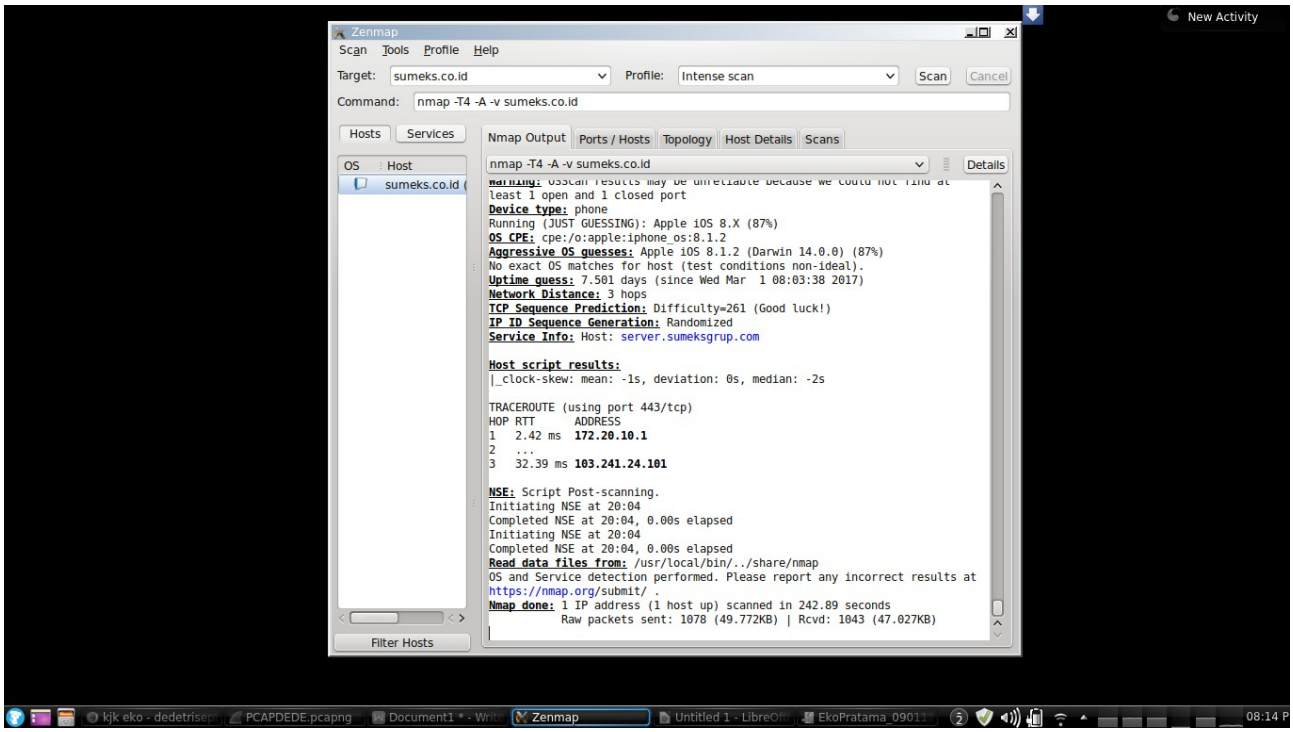
TUGAS KEAMANAN JARINGAN KOMPUTER

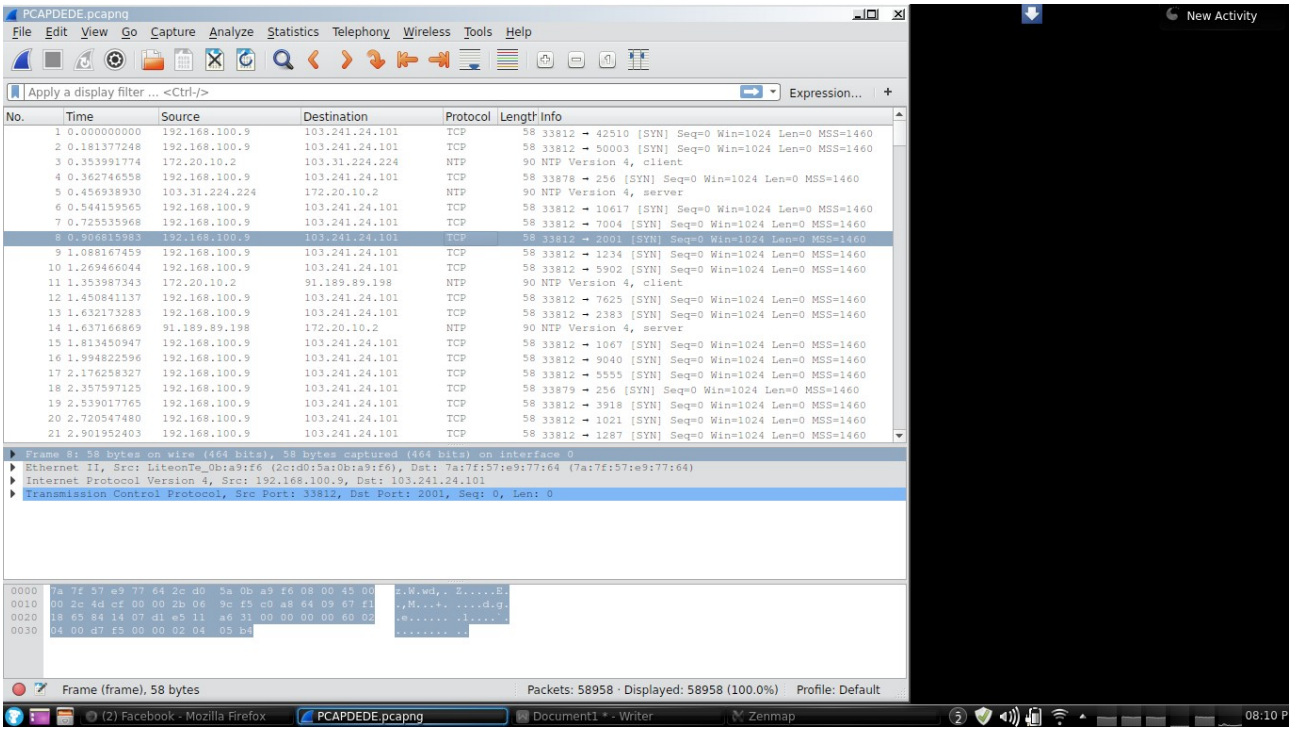
Nama : Dede Triseptiawan
Nim : 09011181320001

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2017

Sebelum kita compile hasil web scanning kita lakukan scan web yang ingin kita scan dalam hal ini menggunakan web sumeks.co.id (103.241.24.101), dengan menggunakan zenmap. zenmap adalah sebuah tool yang kita gunakan untuk melakukan scanning pada ip/web yang sebagai target yang kita tuju. kemudian kita secara bersamaan jalankan aplikasi wireshark adalah aplikasi yang digunakan untuk menganalisa trafic, agar dapat kita gunakan hasil .pcap untuk kita compile di snort untuk memunculkan alert nya.



kita lakukan terlebih dahulu scan sumeks.co.id. pada gambar diatas adalah hasil scan pada sumeks.co.id

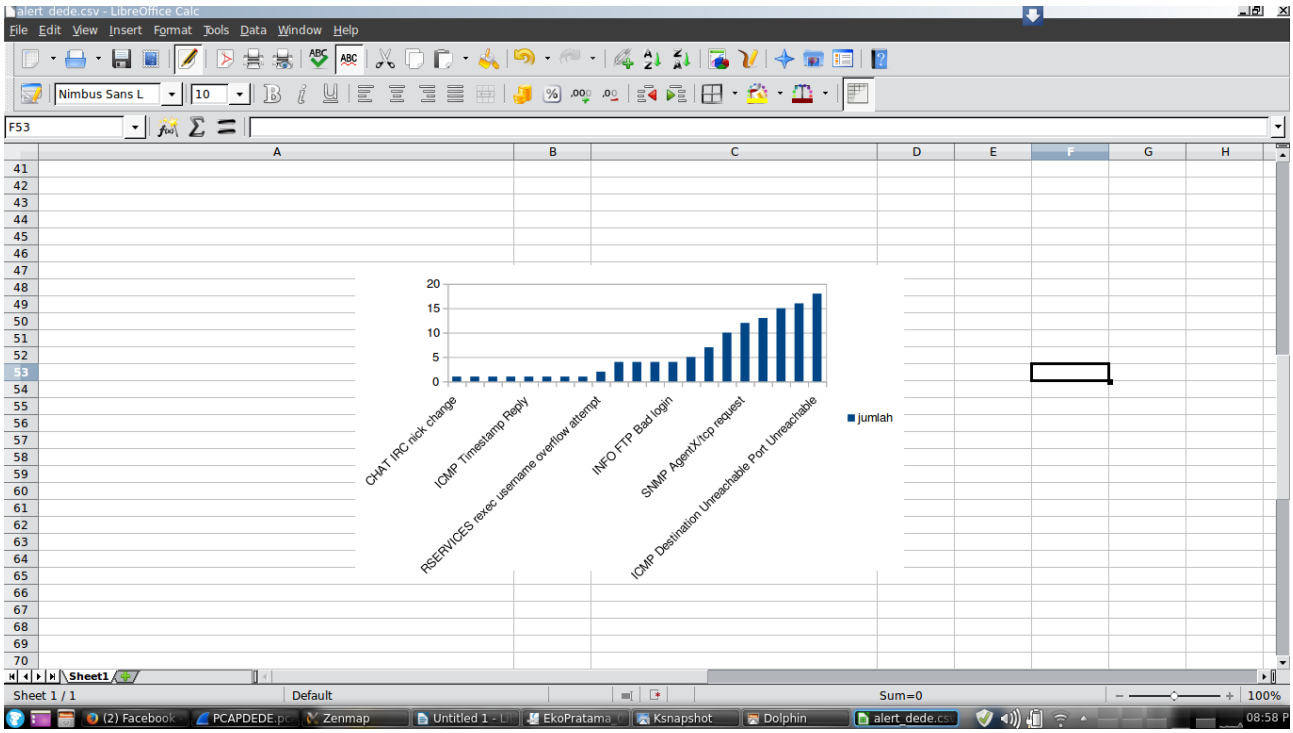


kemudian secara bersamaan kita jalankan wireshark. Dan pada gambar diatas hasil trafic scan dari sumeks.co.id

setelah kita dapat hasil dari wireshark yang tersimpan dalam format .pcap, kemudian kita lakukan compile menggunakan snort, dengan perintah di terminal -A fast -c /etc/snort/snort.conf -r (tempat tersimpannya .pcap)

pada gambar diatas adalah hasil dari compile .pcap di snort. Kemudian setelah berhasil mendapatkan alert dari snort, kita gunakan bantuan countalert.py yang berguna untuk melakukan compile terhadap data alert yang didapatkan tadi, kemudian data tersebut ter-ekstrak dengan bantuan tools tersebut. yang didapatkan berupa ekstrak dari hasil trafic yang dilakukan dengan wireshark. Berikut hasil data yang didapatkan

no	alert	jumlah
1	CHAT IRC nick change	1
2	FINGER null request	1
3	ICMP PING NMAP	1
4	ICMP Time-To-Live Exceeded in Transit	1
5	ICMP Timestamp Reply	1
6	ICMP Timestamp Request	1
7	POLICY PPTP Start Control Request attempt	1
8	RPC portmap listing TCP 111	1
9	RSERVICES rexec username overflow attempt	2
10	X11 xopen	4
11	ICMP Echo Reply undefined code	4
12	DNS named version attempt	4
13	INFO FTP Bad login	4
14	INFO web bug 0x0 gif attempt	5
15	POLICY FTP anonymous login attempt	7
16	ICMP Echo Reply	10
17	SNMP AgentX/tcp request	12
18	ICMP PING	13
19	SNMP request tcp	15
20	SCAN nmap XMAS	16
21	ICMP Destination Unreachable Port Unreachable	18


alert_dede.csv - LibreOffice Calc
File Edit View Insert Format Tools Data Window Help
Nimbus Sans L
10
F53
20
15
10
5
0
CHAT IRC nick change
ICMP Timestamp Reply
RSERVICES rexec username overflow attempt
INFO FTP Bad login
SNMP AgentX/tcp request
ICMP Destination Unreachable Port Unreachable
jumlah
Sheet1
Sheet 1 / 1
Default
Sum=0
100%
(2) Facebook
PCAPDEDE.pc
Zenmap
Untitled 1 - Li
EkoPratama
Ksnapshot
Dolphin
alert_dede.csv
08:58 P