KEAMANAN JARINGAN KOMPUTER

TUGAS 4

M RIDUAN FABIO

09121001066

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

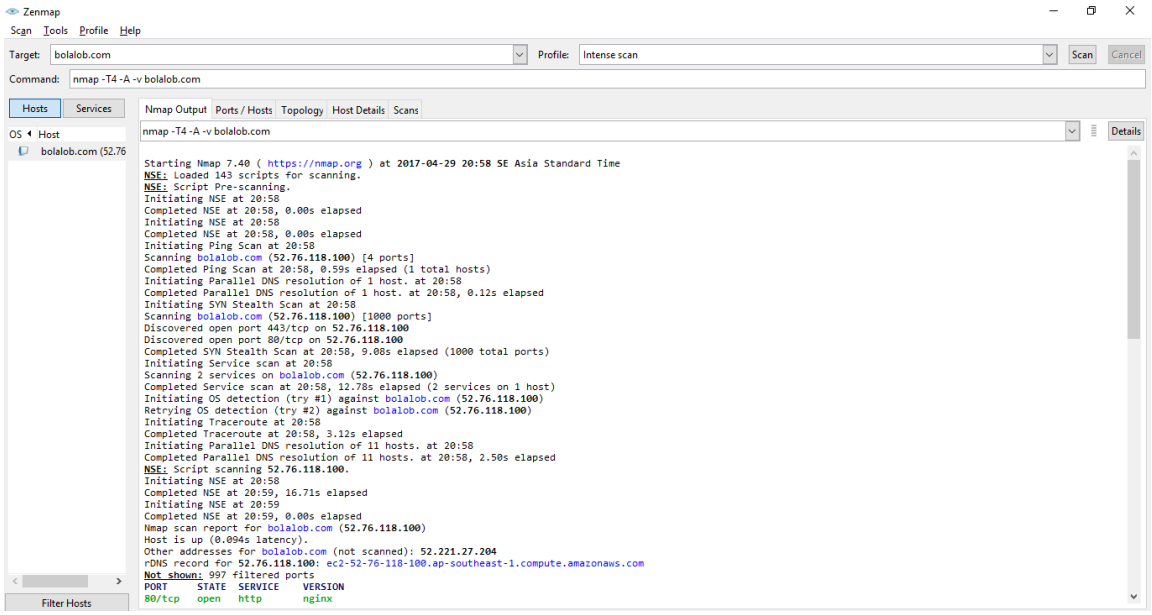
Scanning situs target sambil menjalankan wireshark, kemudian compile menggunakan snort, lihat apa yang terjadi?

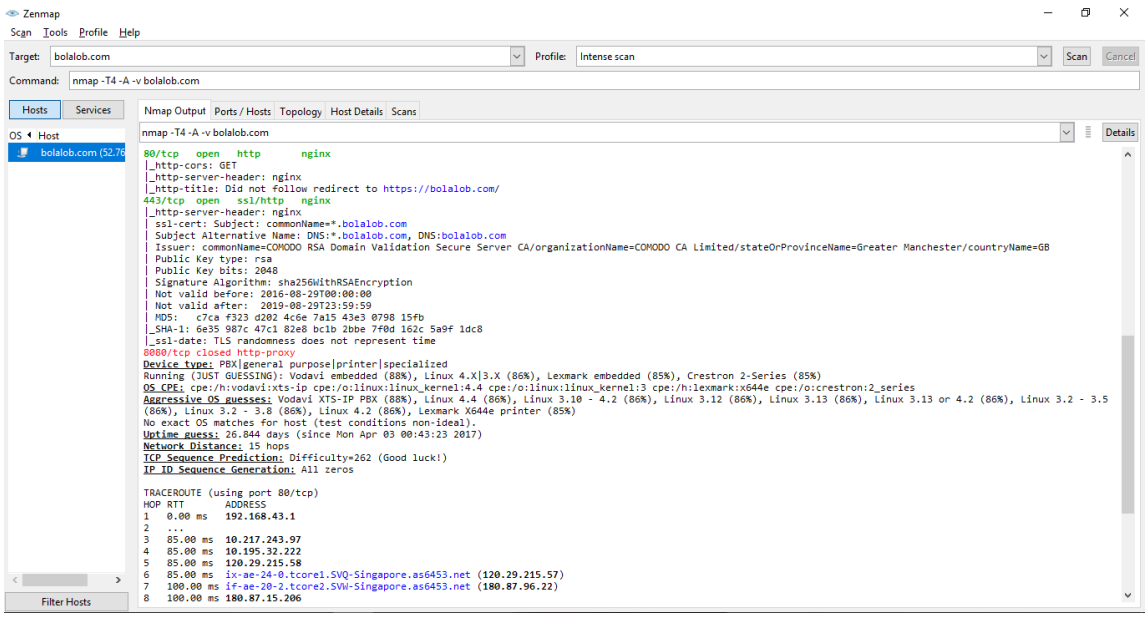
- Buat table dari hasil alert
- Buat grafiknya

Aplikasi yang disiapkan : Nmap dan Wireshark

PROSES SCANNING

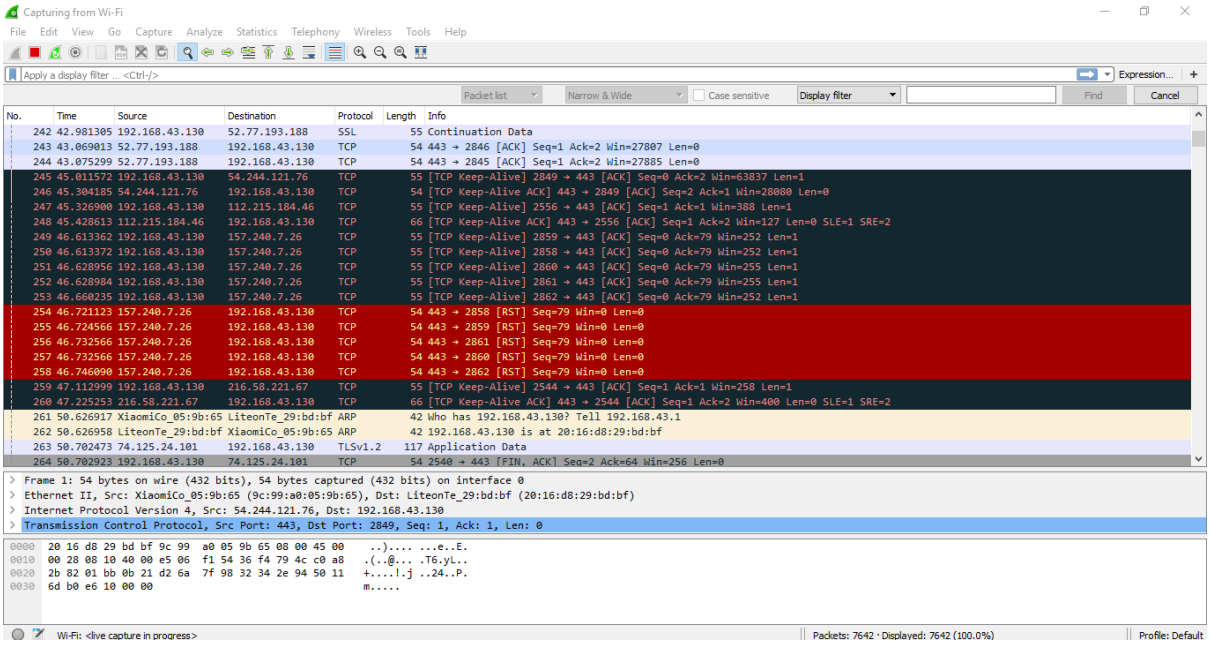
Berikut ini adalah hasil scanning web bolalob.com dari aplikasi Nmap :





Pada saat melakukan scanning pada web bolalob.com, secara bersamaan saya menyalakan aplikasi wireshark.

Berikut hasil traffic yang ditampilkan pada wireshark pada saat scanning web :



Setelah selesai melakukan scanning di nmap dan mendapatkan data pcap dari wireshark, lalu compile data di Ubuntu :

```
root@ubuntu:# snort -1 ./log -b -c /etc/snort/snort.conf -r bolalob.pcap
```

Berikut adalah data alert yang didapat :

```
Total:  1      Priority: 2      alert  ICMP PING NMAP
Total:  1      Priority: 3      alert  ICMP Timestamp Reply
Total:  1      Priority: 3      alert  ICMP Timestamp Request
Total:  2      Priority: 3      alert  BAD-TRAFFIC 0 ttl
Total:  2      Priority: 2      alert  WEB-CGI finger access
Total:  3      Priority: 3      alert  ICMP Destination Unreachable Protocol Unr
eachable
Total:  3      Priority: 2      alert  WEB-MISC robots.txt access
Total:  4      Priority: 2      alert  DNS named version attempt
Total:  4      Priority: 3      alert  ICMP Destination Unreachable Port Unreach
able
Total:  4      Priority: 2      alert  SNMP AgentX/tcp request
Total:  4      Priority: 2      alert  SNMP request tcp
Total:  5      Priority: 3      alert  ICMP Time-To-Live Exceeded in Transit
Total:  6      Priority: 3      alert  ICMP Echo Reply undefined code
Total:  6      Priority: 3      alert  ICMP PING undefined code
Total:  7      Priority: 3      alert  ICMP Echo Reply
Total:  7      Priority: 3      alert  ICMP PING
Total:  8      Priority: 3      alert  ICMP Destination Unreachable Communicatio
n Administratively Prohibited
Total:  8      Priority: 3      alert  ICMP Destination Unreachable Host Unreach
able
Total:  24      Priority: 3      alert  COMMUNITY WEB-MISC Proxy Server Access
Total:  24      Priority: 2      alert  SCAN nmap XMAS
Total:  30      Priority: 1      alert  COMMUNITY WEB-MISC mod_jrun overflow att
empt
Total:  45      Priority: 2      alert  BAD-TRAFFIC same SRC/DST
Total:  421      Priority: 2      alert  MISC UPnP malformed advertisement
Total:  811      Priority: 3      alert  SCAN UPnP service discover attempt
```

HASIL DATA

Dari data alert tersebut dapat dibuat table sebagai berikut :

No	Alert	Jumlah
1	ICMP PING NMAP	1
2	ICMP Timestamp Reply	1
3	ICMP Timestamp Request	1
4	BAD-TRAFFIC 0 ttl	2
5	WEB-CGI finger access	2
6	ICMP Destination Unreachable Protocol Unreachable	3
7	WEB-MISC robots.txt access	3
8	ICMP Destination Unreachable Port Unreachable	4
9	DNS named version attempt	4
10	SNMP AgentX/tcp request	4
11	SNMP request tcp	4
12	ICMP Time-To-Live Exceeded in Transit	5
13	ICMP Echo Reply undefined code	6
14	ICMP PING undefined code	6
15	ICMP Echo Reply	7
16	ICMP PING	7
17	ICMP Destination Unreachable Communication Administratively Prohibited	8
18	ICMP Destination Unreachable Host Unreachable	8
19	COMMUNITY WEB-MISC Proxy Server Access	24
20	SCAN nmap XMAS	24
21	COMMUNITY WEB-MISC mod_jrun overflow attempt	30
22	BAD-TRAFFIC same SRC/DST	45
23	MISC UPnP malformed advertisement	421
24	SCAN UPnP service discover attempt	811

Dan dibuat grafik sebagai berikut :