

**KEAMANAN JARINGAN KOMPUTER**

**TUGAS 4**



**M RIDUAN FABIO**

**09121001066**

**JURUSAN SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA**

**2017**

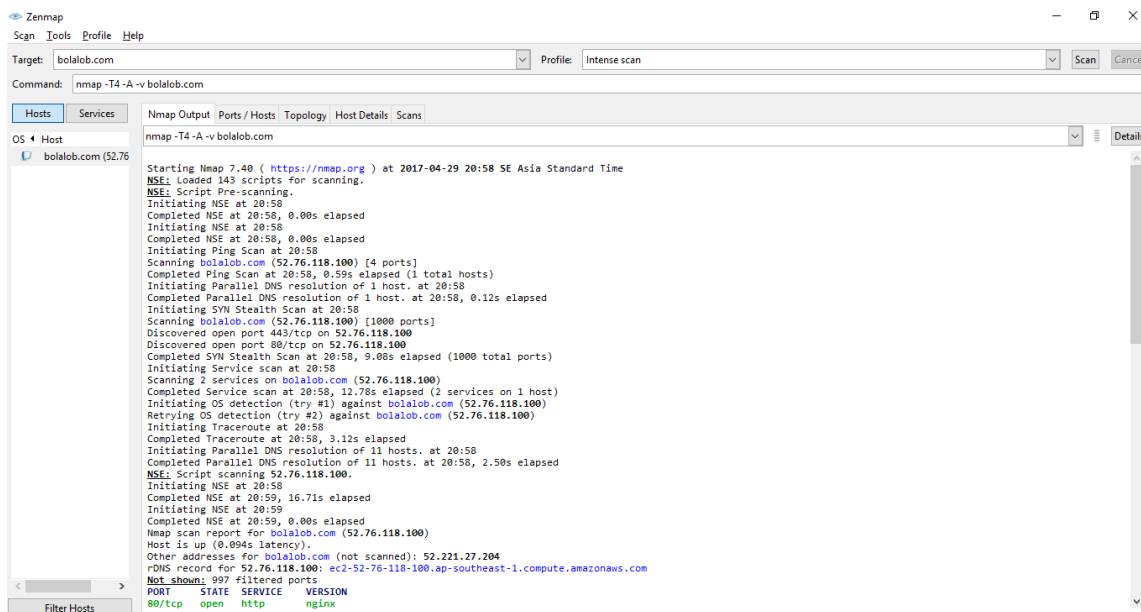
Scanning situs target sambil menjalankan wireshark, kemudian compile menggunakan snort, lihat apa yang terjadi?

- Buat table dari hasil alert
- Buat grafiknya

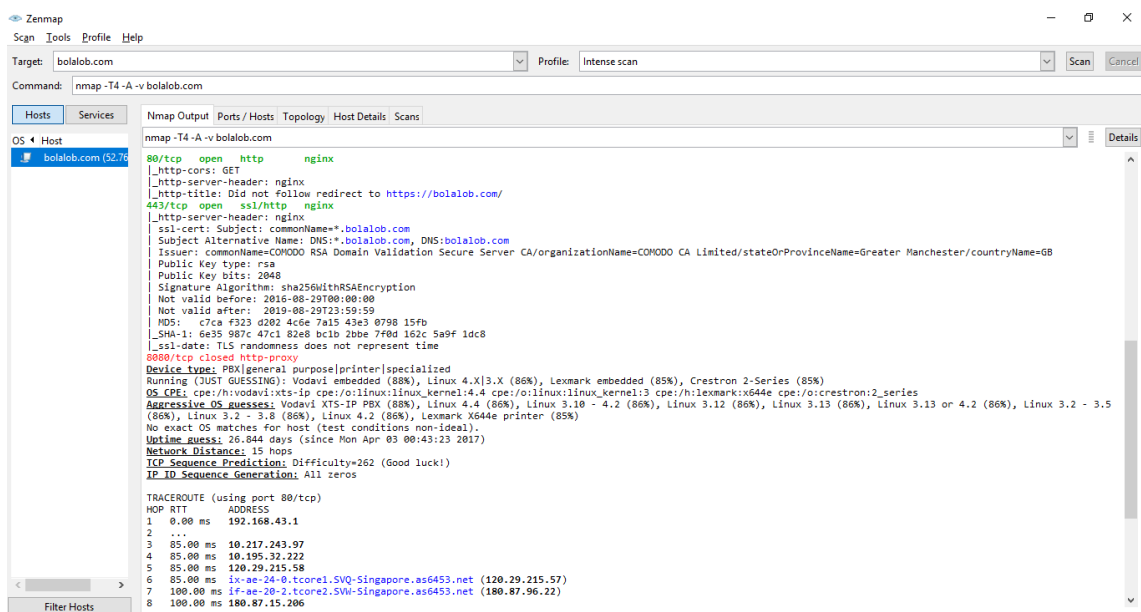
Aplikasi yang disiapkan : Nmap dan Wireshark

## PROSES SCANNING

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



```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-29 20:58 SE Asia Standard Time
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:58
Completed NSE at 20:58, 0.00s elapsed
Initiating NSE at 20:58
Completed NSE at 20:58, 0.00s elapsed
Initiating Ping Scan at 20:58
Scanning bolalob.com (52.76.118.100) [4 ports]
Completed Ping Scan at 20:58, 0.59s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:58
Completed Parallel DNS resolution of 1 host. at 20:58, 0.12s elapsed
Initiating SYN Stealth Scan at 20:58
Scanning bolalob.com (52.76.118.100) [1000 ports]
Discovered open port 443/tcp on 52.76.118.100
Discovered open port 80/tcp on 52.76.118.100
Completed SYN Stealth Scan at 20:58, 9.00s elapsed (1000 total ports)
Initiating Service scan at 20:58
Scanning 2 services on bolalob.com (52.76.118.100)
Completed Service scan at 20:58, 12.78s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against bolalob.com (52.76.118.100)
Retrying OS detection (try #2) against bolalob.com (52.76.118.100)
Initiating Traceroute at 20:58
Completed Traceroute at 20:58, 3.12s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 20:58
Completed Parallel DNS resolution of 11 hosts. at 20:58, 2.50s elapsed
NSE: Script scanning 52.76.118.100.
Initiating NSE at 20:58
Completed NSE at 20:59, 16.71s elapsed
Initiating NSE at 20:59
Completed NSE at 20:59, 0.00s elapsed
Nmap scan report for bolalob.com (52.76.118.100)
Host is up (0.094s latency).
Other addresses for bolalob.com (not scanned): 52.221.27.204
rDNS record for 52.76.118.100: ec2-52-76-118-100.ap-southeast-1.compute.amazonaws.com
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx
```



```
80/tcp    open  http    nginx
|_ http-cors: GET
|_ http-server-header: nginx
|_ http-title: Did not follow redirect to https://bolalob.com/
443/tcp   open  ssl/http nginx
|_ http-server-header: nginx
|_ ssl-cert: Subject: commonName=.bolalob.com
| Subject Alternative Name: DNS:*.bolalob.com, DNS:bolalob.com
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-08-29T00:00:00
| Not valid after: 2019-08-29T23:59:59
| MD5: c7ca f323 d282 4c6e 7a15 43e3 0790 15fb
| SHA-1: 6e35 987c 47c1 82e6 bc1b 28be 7f9d 162c 5a9f 1dc8
|_ ssl-date: TLS randomness does not represent time
8080/tcp   closed http-proxy
Device type: PXE[general purpose]printer[specialized]
Running (JUST GUESSING): Vodavi embedded (88%), Linux 4.X[3.X (86%), Lexmark embedded (85%), Crestron 2-Series (85%)
OS_CPE: cpe:/h:vodavi:xts-ip cpe:/o:linux:linux_kernel:14.4 cpe:/o:linux:linux_kernel:13 cpe:/h:lexmark:x644e cpe:/o:crestron:2_series
Aggressive OS guesses: Vodavi XTS-IP PXE (88%), Linux 4.4 (86%), Linux 3.10 - 4.2 (86%), Linux 3.12 (86%), Linux 3.13 (86%), Linux 3.13 or 4.2 (86%), Linux 3.2 - 3.5 (86%), Linux 3.2 - 3.8 (86%), Linux 4.2 (86%), Lexmark X644e printer (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 26.844 days (since Mon Apr 03 00:43:23 2017)
Network Distance: 15 hops
TCP Sequence Predictions: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.00 ms 192.168.43.1
2 ..
3 85.00 ms 10.217.243.97
4 85.00 ms 10.195.32.222
5 85.00 ms 120.29.215.58
6 85.00 ms ix-ae-24-0.tcore1.SVQ-Singapore.as6453.net (120.29.215.57)
7 100.00 ms ix-ae-20-2.tcore2.SWI-Singapore.as6453.net (180.87.96.22)
8 100.00 ms 180.87.15.206
```

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 :

The screenshot shows the Wireshark interface with a packet list table. The table columns are No., Time, Source, Destination, Protocol, Length, and Info. The traffic includes SSL continuation data, TCP keep-alive messages, TCP resets (RST), and ARP requests. A packet of type Transmission Control Protocol (TCP) is highlighted in blue, showing a sequence number of 443 and an acknowledgment number of 1.

No.	Time	Source	Destination	Protocol	Length	Info
242	42.981305	192.168.43.130	52.77.193.188	SSL	55	Continuation Data
243	43.069013	52.77.193.188	192.168.43.130	TCP	54	443 → 2846 [ACK] Seq=1 Ack=2 Win=27807 Len=0
244	43.075299	52.77.193.188	192.168.43.130	TCP	54	443 → 2845 [ACK] Seq=1 Ack=2 Win=27885 Len=0
245	45.011572	192.168.43.130	54.244.121.76	TCP	55	[TCP Keep-Alive] 2849 → 443 [ACK] Seq=0 Ack=2 Win=63837 Len=1
246	45.304185	54.244.121.76	192.168.43.130	TCP	54	[TCP Keep-Alive ACK] 443 → 2849 [ACK] Seq=2 Ack=1 Win=28080 Len=0
247	45.326900	192.168.43.130	112.215.184.46	TCP	55	[TCP Keep-Alive] 2556 → 443 [ACK] Seq=1 Ack=1 Win=388 Len=1
248	45.428613	112.215.184.46	192.168.43.130	TCP	66	[TCP Keep-Alive ACK] 443 → 2556 [ACK] Seq=1 Ack=2 Win=127 Len=0 SLE=1 SRE=2
249	46.613362	192.168.43.130	157.240.7.26	TCP	55	[TCP Keep-Alive] 2859 → 443 [ACK] Seq=0 Ack=79 Win=252 Len=1
250	46.613372	192.168.43.130	157.240.7.26	TCP	55	[TCP Keep-Alive] 2858 → 443 [ACK] Seq=0 Ack=79 Win=252 Len=1
251	46.628956	192.168.43.130	157.240.7.26	TCP	55	[TCP Keep-Alive] 2860 → 443 [ACK] Seq=0 Ack=79 Win=255 Len=1
252	46.628984	192.168.43.130	157.240.7.26	TCP	55	[TCP Keep-Alive] 2861 → 443 [ACK] Seq=0 Ack=79 Win=255 Len=1
253	46.660235	192.168.43.130	157.240.7.26	TCP	55	[TCP Keep-Alive] 2862 → 443 [ACK] Seq=0 Ack=79 Win=252 Len=1
254	46.721123	157.240.7.26	192.168.43.130	TCP	54	443 → 2858 [RST] Seq=79 Win=0 Len=0
255	46.724566	157.240.7.26	192.168.43.130	TCP	54	443 → 2859 [RST] Seq=79 Win=0 Len=0
256	46.732566	157.240.7.26	192.168.43.130	TCP	54	443 → 2861 [RST] Seq=79 Win=0 Len=0
257	46.732566	157.240.7.26	192.168.43.130	TCP	54	443 → 2860 [RST] Seq=79 Win=0 Len=0
258	46.746090	157.240.7.26	192.168.43.130	TCP	54	443 → 2862 [RST] Seq=79 Win=0 Len=0
259	47.112999	192.168.43.130	216.58.221.67	TCP	55	[TCP Keep-Alive] 2544 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1
260	47.225253	216.58.221.67	192.168.43.130	TCP	66	[TCP Keep-Alive ACK] 443 → 2544 [ACK] Seq=1 Ack=2 Win=400 Len=0 SLE=1 SRE=2
261	50.626917	XiaomiCo_05:9b:65	LiteonTe_29:bd:bf	ARP	42	Who has 192.168.43.130? Tell 192.168.43.1
262	50.626958	LiteonTe_29:bd:bf	XiaomiCo_05:9b:65	ARP	42	192.168.43.130 is at 20:16:d8:29:bd:bf
263	50.702473	74.125.24.101	192.168.43.130	TLSv1.2	117	Application Data
264	50.702923	192.168.43.130	74.125.24.101	TCP	54	2540 → 443 [FIN, ACK] Seq=2 Ack=64 Win=256 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
> Ethernet II, Src: XiaomiCo\_05:9b:65 (9c:99:a0:05:9b:65), Dst: LiteonTe\_29:bd:bf (20:16:d8:29:bd:bf)  
> Internet Protocol Version 4, Src: 54.244.121.76, Dst: 192.168.43.130  
> Transmission Control Protocol, Src Port: 443, Dst Port: 2849, Seq: 1, Ack: 1, Len: 0

```
0000 20 16 d8 29 bd bf 9c 99 a0 05 9b 65 00 00 45 00  ..)...e..E.
0010 00 28 08 10 40 00 e5 06 f1 54 36 f4 79 4c c0 a8  .(.@...T6.yL.
0020 2b 82 01 bb 0b 21 d2 6a 7f 98 32 34 2e 94 50 11  +....!j..24..P.
0030 6d 0b e0 10 00 00  m.....
```

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

```
root@ubuntu:~# snort -l ./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 :

