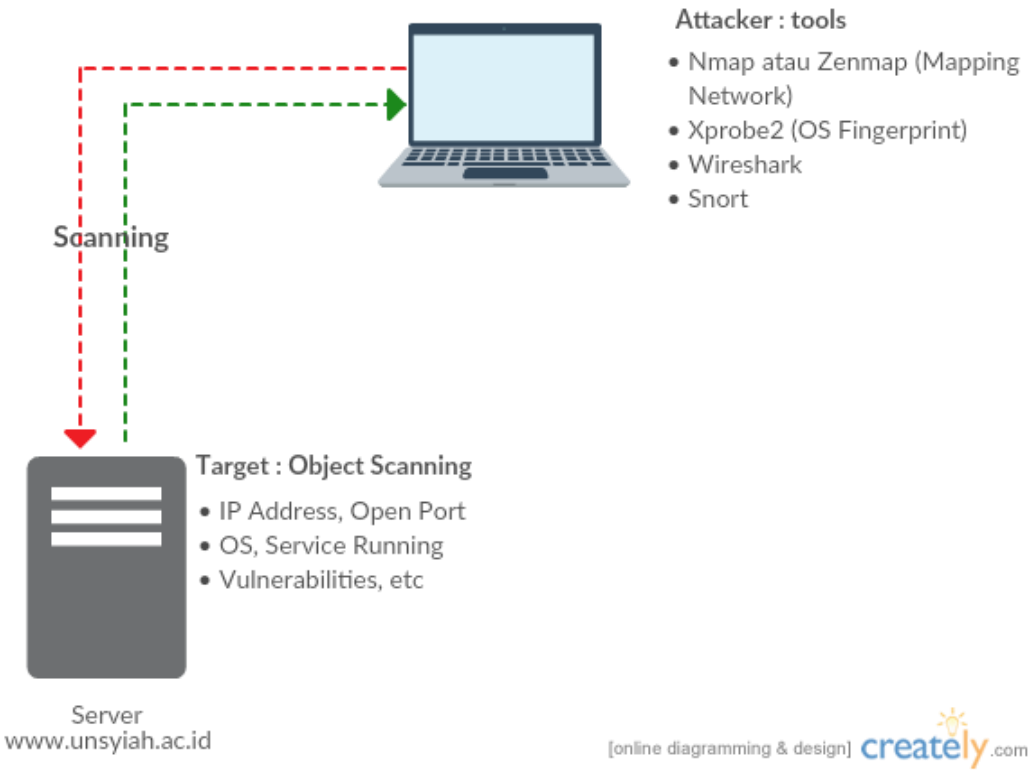
Snort

Dasar Teori : *Snort*

Snort merupakan *tool* atau aplikasi *open source* dari *Intrusion Detection System* (IDS). *Snort* dirancang untuk beroperasi pada *command line* dan telah diintegrasikan ke beberapa aplikasi pihak ketiga serta mendukung *cross platform*. *Snort* menganalisis semua lalu lintas jaringan untuk melakukan *sniffing* dan mencari beberapa jenis penyusupan maupun serangan dalam sebuah jaringan. Secara umum *snort* dapat di operasikan dalam tiga (3) buah mode, yaitu :

1. *Sniffer mode* : untuk melihat paket yang lewat di jaringan.
2. *Packet logger mode* : untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
3. Intrusion Detection mode : pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan setup dari berbagai *rules* / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

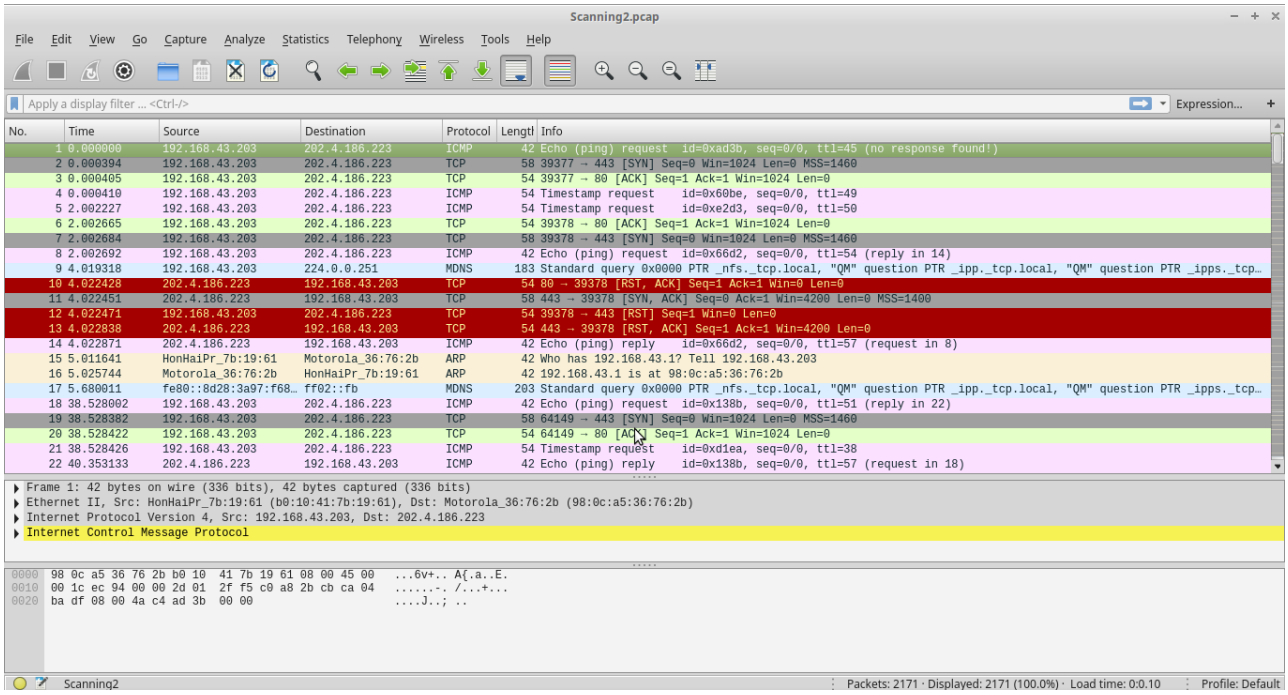
Topologi : *Snort*



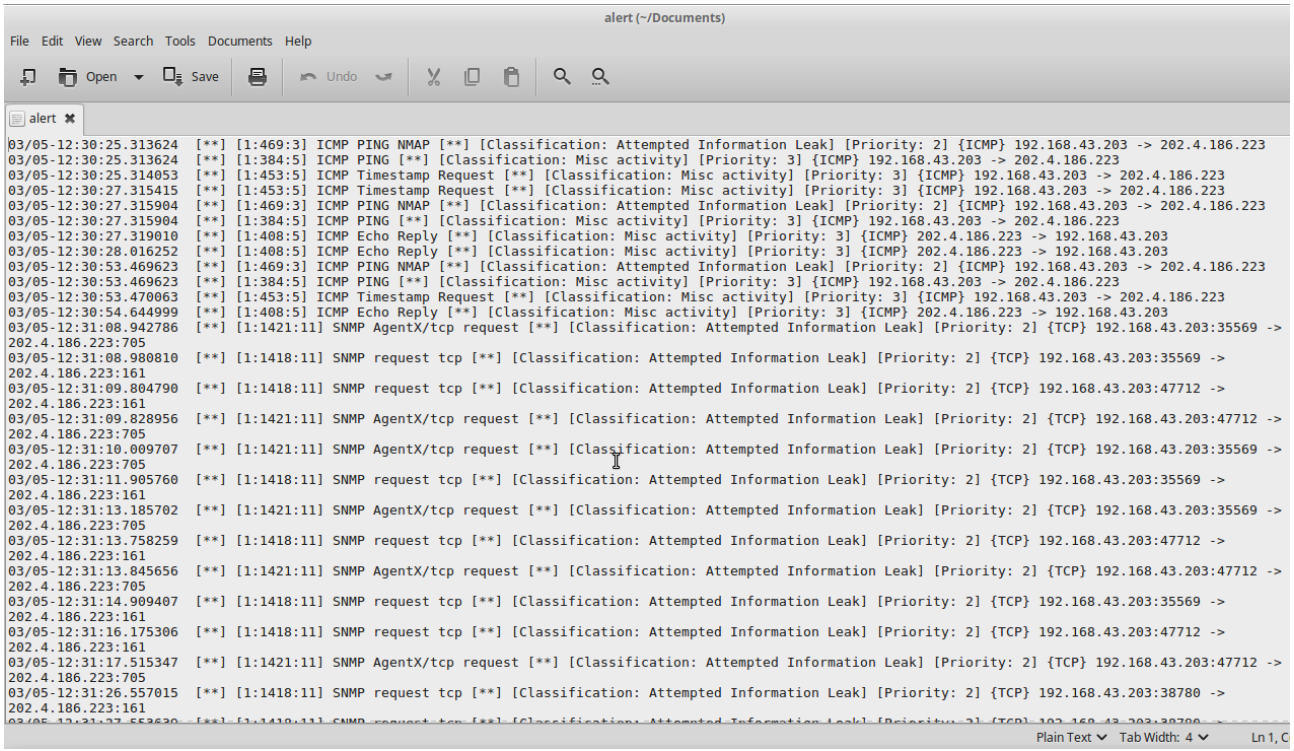
Gambar 3. Topologi *Scanning*

Pada kegiatan ini *scanning* dilakukan pada target (www.unsyiah.ac.id). Proses *scanning* di*capture* menggunakan *wireshark* untuk memproleh data berupa pcap. Proses selanjutnya data pcap di*import* pada *snort* untuk memproleh alertdari proses *scanning* target.

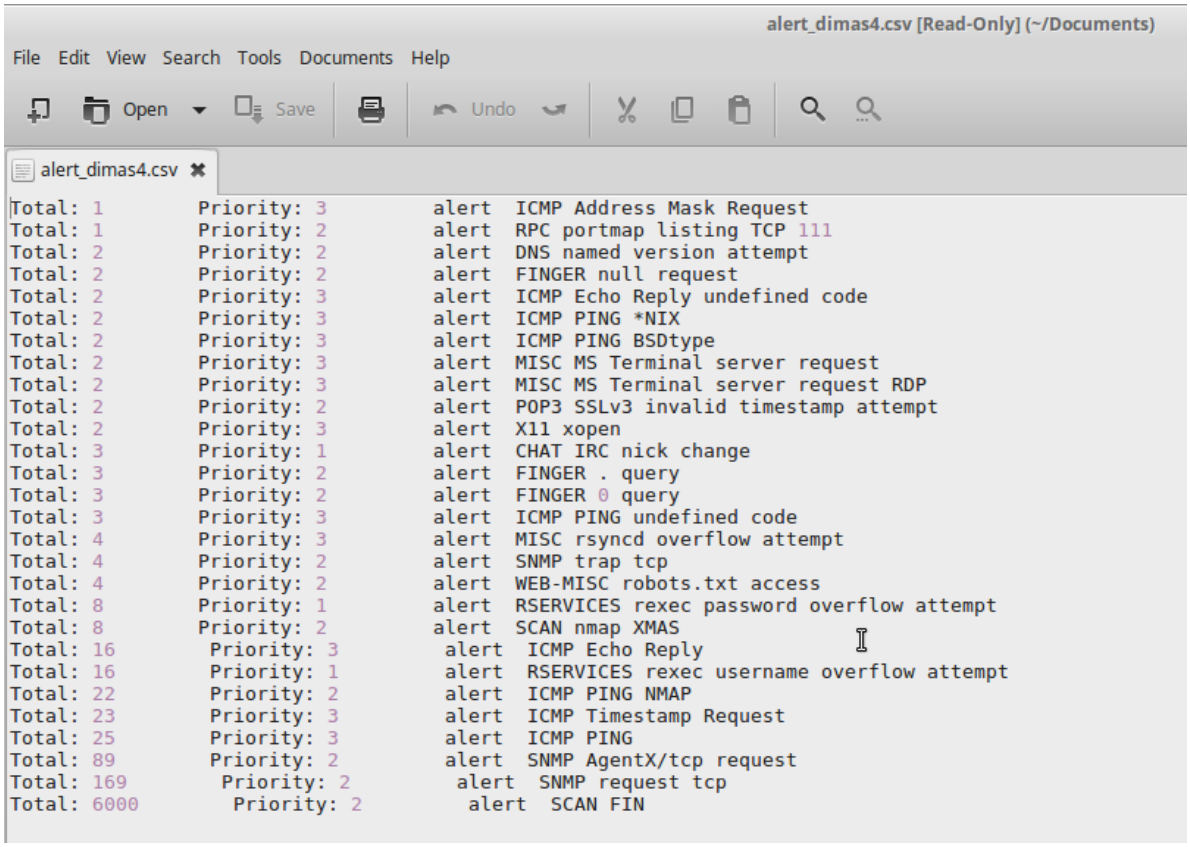
Tahap : Capture proses *scanning* menggunakan *wireshark*



Tahap : *Import* hasil *scanning* berupa data pcap dari *wireshark* ke *snort*



Tahap : Pengelompokan *alert snort*



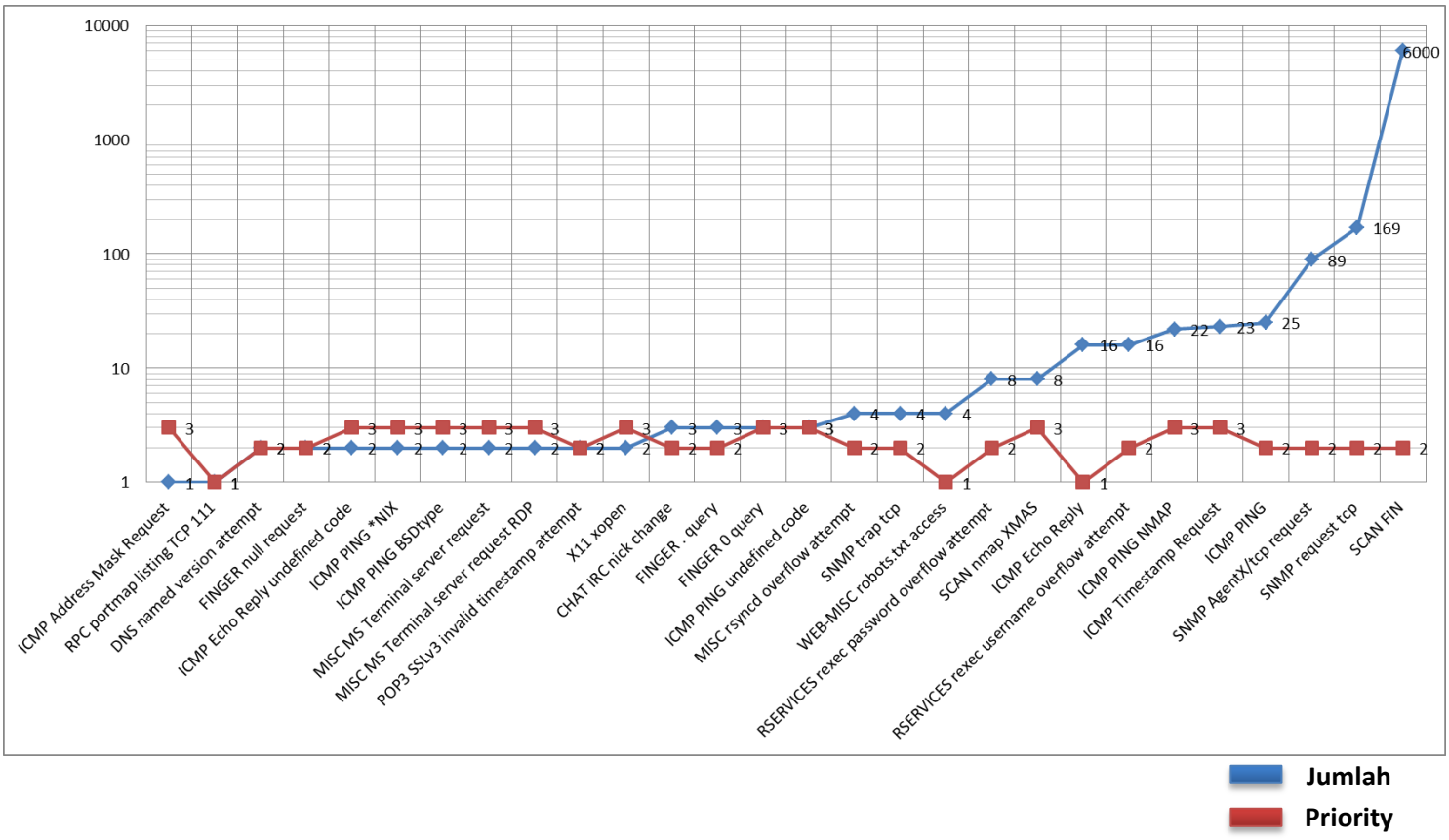

```
Total: 1        Priority: 3         alert  ICMP Address Mask Request
Total: 1        Priority: 2         alert  RPC portmap listing TCP 111
Total: 2        Priority: 2         alert  DNS named version attempt
Total: 2        Priority: 2         alert  FINGER null request
Total: 2        Priority: 3         alert  ICMP Echo Reply undefined code
Total: 2        Priority: 3         alert  ICMP PING *NIX
Total: 2        Priority: 3         alert  ICMP PING BSDtype
Total: 2        Priority: 3         alert  MISC MS Terminal server request
Total: 2        Priority: 3         alert  MISC MS Terminal server request RDP
Total: 2        Priority: 2         alert  POP3 SSLv3 invalid timestamp attempt
Total: 2        Priority: 3         alert  X11 xopen
Total: 3        Priority: 1         alert  CHAT IRC nick change
Total: 3        Priority: 2         alert  FINGER . query
Total: 3        Priority: 2         alert  FINGER 0 query
Total: 3        Priority: 3         alert  ICMP PING undefined code
Total: 4        Priority: 3         alert  MISC rsyncd overflow attempt
Total: 4        Priority: 2         alert  SNMP trap tcp
Total: 4        Priority: 2         alert  WEB-MISC robots.txt access
Total: 8        Priority: 1         alert  RSERVICES rexec password overflow attempt
Total: 8        Priority: 2         alert  SCAN nmap XMAS
Total: 16        Priority: 3         alert  ICMP Echo Reply
Total: 16        Priority: 1         alert  RSERVICES rexec username overflow attempt
Total: 22        Priority: 2         alert  ICMP PING NMAP
Total: 23        Priority: 3         alert  ICMP Timestamp Request
Total: 25        Priority: 3         alert  ICMP PING
Total: 89        Priority: 2         alert  SNMP AgentX/tcp request
Total: 169        Priority: 2         alert  SNMP request tcp
Total: 6000        Priority: 2         alert  SCAN FIN
```

Tabel : Pengelompokan *alert*

NO	Alert	Jumlah	Priority
1	ICMP Address Mask Request	1	3
2	RPC portmap listing TCP 111	1	1
3	DNS named version attempt	2	2
4	FINGER null request	2	2
5	ICMP Echo Reply undefined code	2	3
6	ICMP PING *NIX	2	3
7	ICMP PING BSDtype	2	3
8	MISC MS Terminal server request	2	3
9	MISC MS Terminal server request RDP	2	3
10	POP3 SSLv3 invalid timestamp attempt	2	2
11	X11 xopen	2	3
12	CHAT IRC nick change	3	2
13	FINGER . query	3	2
14	FINGER 0 query	3	3
15	ICMP PING undefined code	3	3
16	MISC rsyncd overflow attempt	4	2
17	SNMP trap tcp	4	2
18	WEB-MISC robots.txt access	4	1
19	RSERVICES rexec password overflow attempt	8	2

20	SCAN nmap XMAS	8	3
21	ICMP Echo Reply	16	1
22	RSERVICES rexec username overflow attempt	16	2
23	ICMP PING NMAP	22	3
24	ICMP Timestamp Request	23	3
25	ICMP PING	25	2
26	SNMP AgentX/tcp request	89	2
27	SNMP request tcp	169	2
28	SCAN FIN	6000	2

Grafik : Pengelompokan *alert*



Daftar Pustaka

[1] A. H. Abdullah, "Cyber-Attack Penetration Test and Vulnerability Analysis," vol. 13, no. 1, pp. 125–132.

[2] I. C. of E.-C. C. (EC-Council), "Footprinting and Reconnaissance," *Certif. Ethical Hacker V8.00*.