Intrusion Detection System

Intrusion Detection System (IDS) adalah suatu tindakan untuk mendeteksi adanya trafik paket yang tidak diinginkan dalam sebuah jaringan atau device. Sebuah IDS dapat diimplementasikan melalui software atau aplikasi yang terinstall dalam sebuah device, dan aplikasi tersebut dapat memantau paket jaringan untuk mendeteksi adanya paket-paket ilegal seperti paket yang merusak kebijakan rules keamanan, dan paket yang ditujukan untuk mengambil hak akses suatu pengguna.

Beberapa jenis dari teknologi IDS adalah *Network-Based, Wireless IDS, Network Behavior Anomali Detection* dan *Host-Based.*

1. *Network-Based* : Tipe ini menganalisa paket-paket jaringan pada semua lapisan *Open System Interconnection* (OSI) dan membuat sebuah tindakan kepada paket tersebut.
2. *Wireless Local Area Network* (WLAN) : WLAN ini dapat menganalisa paket wireless secara spesifik, termasuk pemindaian pengguna eksternal yang mencoba untuk terhubung ke Access Point (AP).
3. *Network Behavior Anomaly Detection* (NBAD) : tipe ini berfungsi untuk memantau paket pada segmen-segmen jaringan untuk menentukan anomali-anomali dalam jumlah paket atau tipe paket.
4. *Host-based Intrusion Detection System* (HIDS) : menganalisa paket jaringan dan pengaturan sistem secara spesifik seperti *software calls*, *local security policy*, *local log audits*, dan sebagainya.

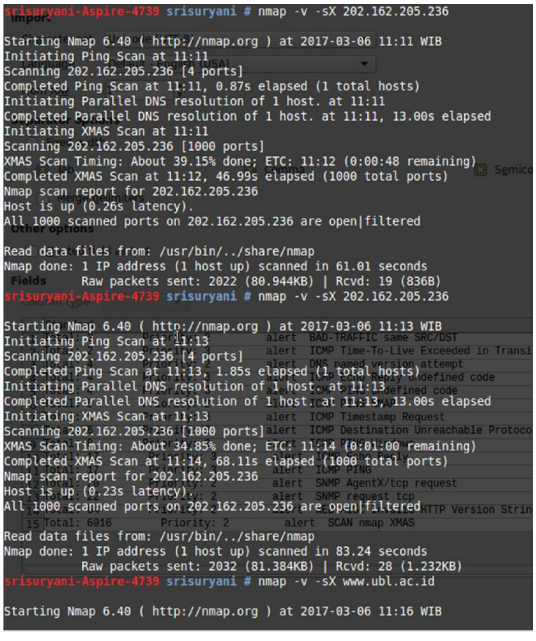
Terdapat beberapa jenis-jenis pendeteksian dalam implementasi IDS, diantaranya :

1. *Signature-Based Detection*, Sebuah IDS dapat menggunakan pendeteksian *Signature-Based Detetection* dari sebuah paket, tergantung data paket yang diketahui untuk menganalisa potensi terjadinya paket ilegal. Tipe pendeteksi ini sangat cepat dan mudah dikonfigurasi.
2. *Anomaly-Based Detection*, IDS yang dapat memantau paket jaringan dan mendeteksi data yang tidak valid, atau umumnya tidak normal menggunakan jenis deteksi Anomaly-Based.

3. *Stateful Protocol Inspection*, menyerupai pendeteksi berbasis anomali, tetapi jenis ini dapat menganalisa paket lapisan 3 OSI yaitu lapisan Network dan lapisan 4 yaitu lapisan protokol.
4. *Open System Interconection Model*, *Model Open System Interconnection* (OSI) diciptakan oleh *International Organization for Standarization* (ISO) yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan.

Langkah-langkah yang dilakukan pada tugas ini adalah sebagai berikut :

1. Install aplikasi wireshark dan nmap pada terminal, dimana comment install aplikasi wireshark ialah [*apt-get install wireshark*] dan comment install aplikasi nmap ialah [*apt-get install nmap*].
2. Lakukan scanning dengan menggunakan alamat domain yang sama dengan tugas sebelumnya, dimana alamat domain yang digunakan adalah ubl.ac.id dengan ip 202.162.205.236. pada gambar 1 menunjukan command scanning serta hasil scanning pada terminal, dimana pada tugas ini dilakukan scanning sebanyak tiga kali.

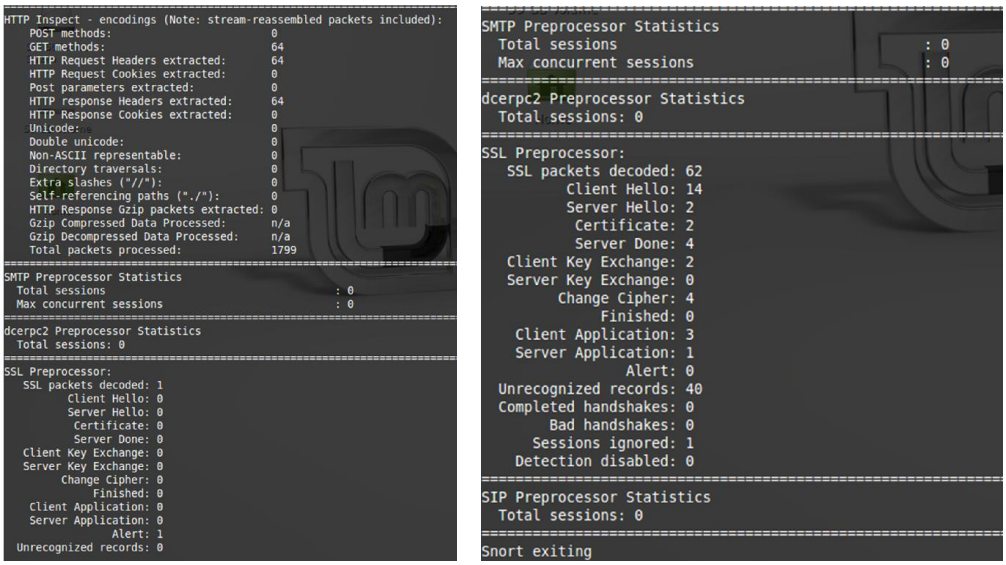


Gambar 1. Hasil scanning pada terminal

3. Paket yang tercapture pada wireshark disimpan untuk kemudian dikompile dengan menggunakan command *snort –A fast –c /etc/snort/snort.conf –r [letak file pcap]*, seperti gambar dibawah ini.

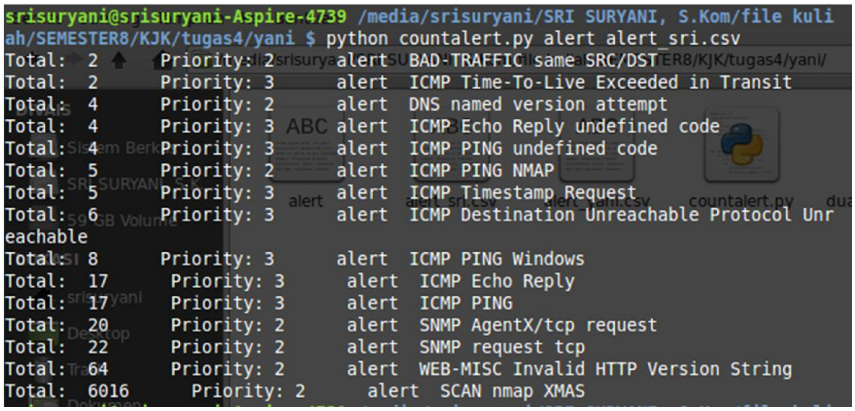
```
srisuryani-Aspire-4739 srisuryani # snort -A fast -c /etc/snort/snort.conf -r /home/srisuryani/Dokumen/ubl.ac.id.pcapng
```

Pada gambar 2 merupakan hasil dari perintah command diatas.



Gambar 2. Sebagian tampilan dari command pada langkah ketiga

4. Setelah paket dikompile, maka file alert pada folder snort dijumlahkan/count dengan menggunakan perintah *python countalert.py [nama file sebelumnya] [nama file baru] dengan format file csv*, seperti yang ditampilkan pada gambar 3 dan gambar 4 adalah tampilan file alert sebelum dijumlahkan/count ke file csv.



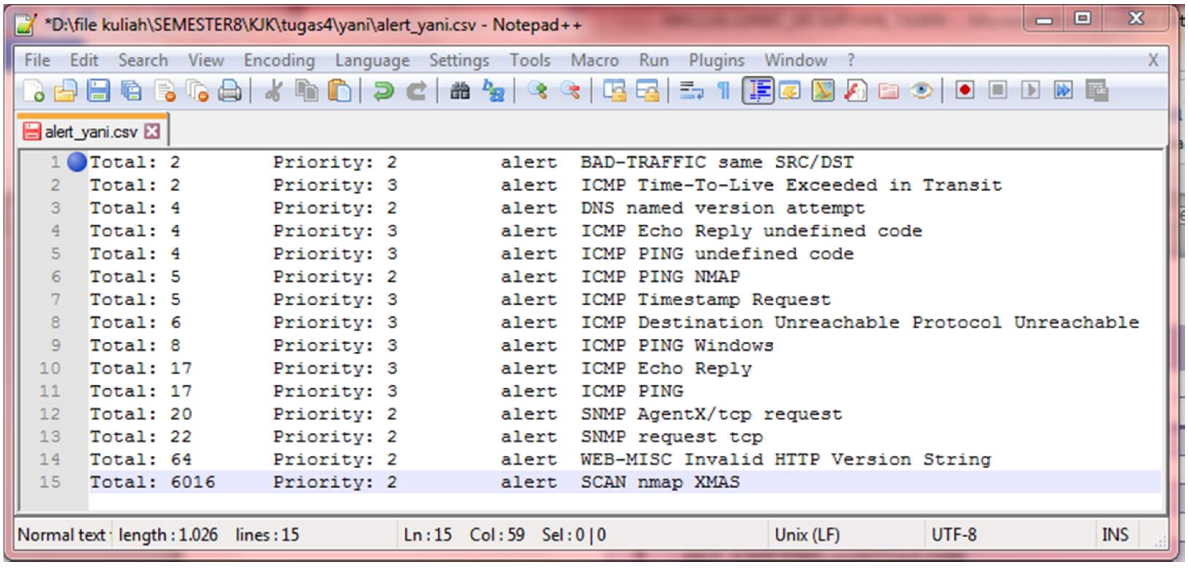
Gambar 3. Tampilan ketika menjumlahkan/count file alert ke file csv dengan menggunakan aplikasi countalert.py

```
03/04-14:31:24.225959  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.74 -> 202.162.205.236
03/04-14:31:24.225959  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.74 -> 202.162.205.236
03/04-14:31:24.318640  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 202.162.205.236 -> 192.168.43.74
03/04-14:31:25.237836  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.74 -> 202.162.205.236
03/04-14:31:25.237836  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.74 -> 202.162.205.236
03/04-14:31:25.336588  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 202.162.205.236 -> 192.168.43.74
03/04-14:31:26.236133  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.74 -> 202.162.205.236
03/04-14:31:26.236133  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.74 -> 202.162.205.236
03/04-14:31:26.326651  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 202.162.205.236 -> 192.168.43.74
03/04-14:31:27.250131  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.74 -> 202.162.205.236
03/04-14:31:27.250131  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.74 -> 202.162.205.236
03/04-14:31:27.346581  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 202.162.205.236 -> 192.168.43.74
03/04-14:33:19.816896  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
03/04-14:33:41.709256  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:64489 ->
```

```
03/06-11:11:49.110197  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:1972
03/06-11:11:49.110221  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:389
03/06-11:11:49.110244  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:8290
03/06-11:11:49.110267  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:7007
03/06-11:11:49.110290  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:37
03/06-11:11:49.110314  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:1030
03/06-11:11:49.110337  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:464
03/06-11:11:49.110360  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:8082
03/06-11:11:49.110382  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:5815
03/06-11:11:49.110404  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:1024
03/06-11:11:49.110427  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:5054
03/06-11:11:49.110449  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:1099
03/06-11:11:49.110473  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:1719
03/06-11:11:49.110496  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:1234
03/06-11:11:49.110520  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 ->
202.162.205.236:55056
03/06-11:11:49.110545  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 -> 202.162.205.236:1117
03/06-11:11:49.110631  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 ->
202.162.205.236:20000
03/06-11:11:49.110656  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.74:42424 ->
```

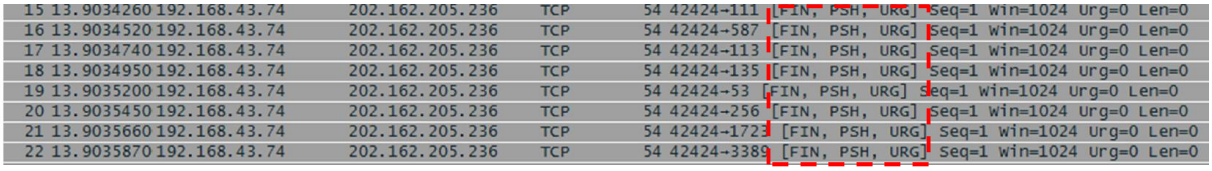
Gambar 4. Tampilan file alert sebelum dijumlahkan/count dengan menggunakan aplikasi countalert.py

Pada gambar 5 menampilkan alert yang dihasilkan dari scanning menggunakan aplikasi nmap dengan domain : **ubl.ac.id** dan memiliki ip **202.162.205.236,** scanning tersebut dicapture dengan menggunakan aplikasi wireshark kemudian paket tersebut dikompile dengan menggunakan snort.



Gambar 5. Tampilan alert setelah dijumlahkan/count dengan menggunakan aplikasi countalert.py

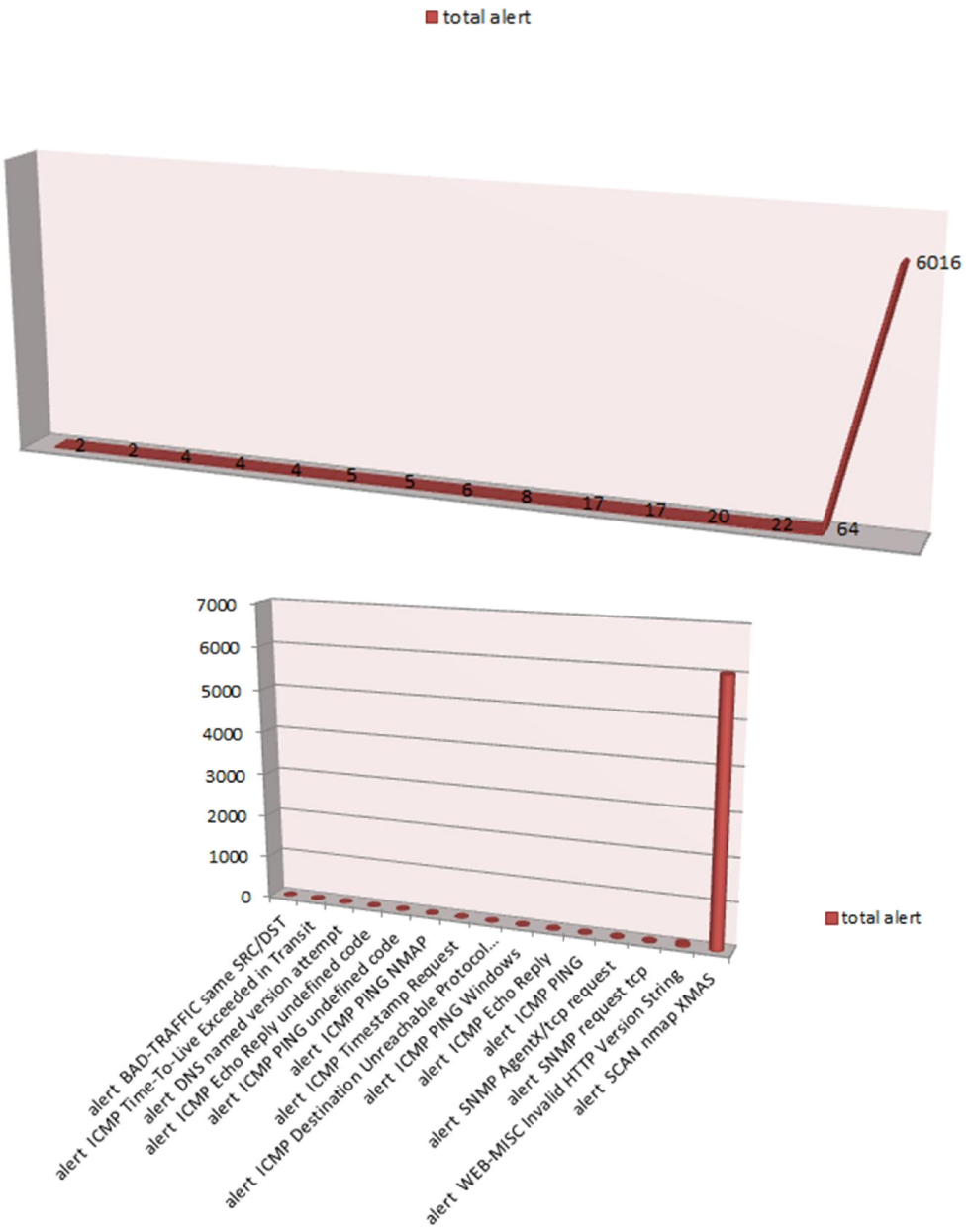
Gambar 6b merupakan tabel yang berisi alert dan jumlah dari masing-masing alert yang dihasilkan dari scanning dan capture paket menggunakan aplikasi wireshark. Pada tabel dibawah (gambar 6b) menunjukan alert SCAN nmap XMAS menghasilkan jumlah paling besar dibandingkan dengan alert yang lainnya. Jika pada wireshark alert XMAS ditunjukan dengan ciri memiliki [FIN, PSH, URG] seperti gambar 6a. Xmas scan akan mengirim frame TCP pada remote device dengan memanfaatkan pesan URG, ACK, RST, SYN dan FIN. Port akan dianggap open jika ia tak memberikan respon, sebaliknya port akan dianggap tertutup ketika ia merespon dengan menggunakan pesan reset. Dengan menggunakan pesan FIN, attacker mengirim TCP frame pada remote device.



gambar 6a. Menapilkan paket dengan alert XMAS

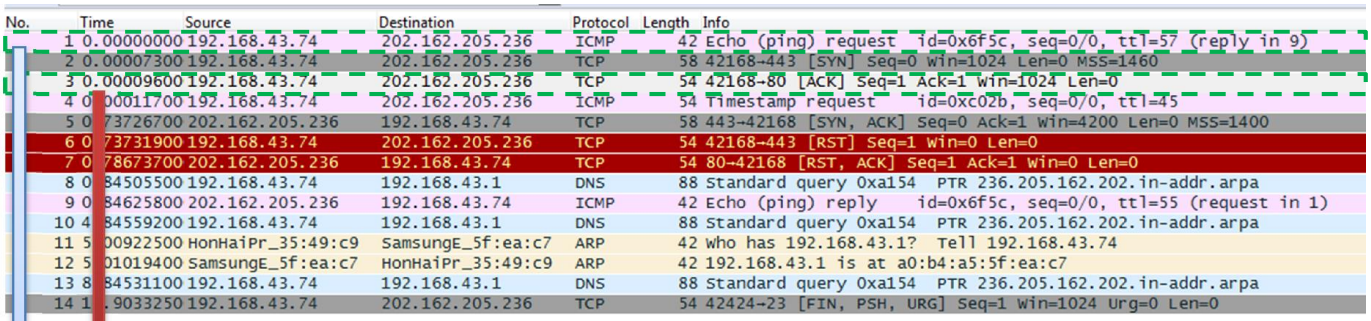
No	Alert	Jumlah Alert
1	alert BAD-TRAFFIC same SRC/DST	2
2	alert ICMP Time-To-Live Exceeded in Transit	2
3	alert DNS named version attempt	4
4	alert ICMP Echo Reply undefined code	4
5	alert ICMP PING undefined code	4
6	alert ICMP PING NMAP	5
7	alert ICMP Timestamp Request	5
8	alert ICMP Destination Unreachable Protocol Unreachable	6
9	alert ICMP PING Windows	8
10	alert ICMP Echo Reply	17
11	alert ICMP PING	17
12	alert SNMP AgentX/tcp request	20
13	alert SNMP request tcp	22
14	alert WEB-MISC Invalid HTTP Version String	64
15	alert SCAN nmap XMAS	6016

Gambar 6b. Tabel hasil alert



Gambar 7. Grafik alert

Gambar 7 merupakan grafik dari tabel pada gambar 6b, dimana pada grafik menunjukan alert SCAN namp XMAS memiliki nilai tertinggi dibandingkan dengan alert lainnya.

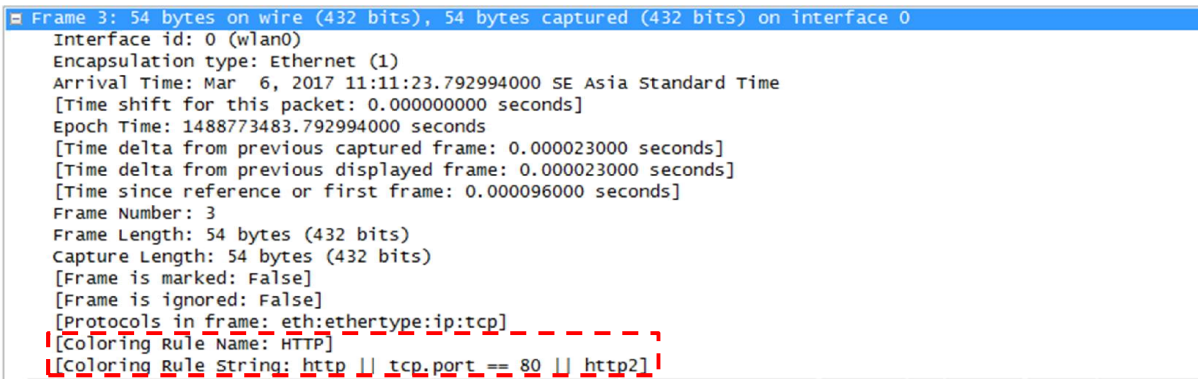


No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.43.74	202.162.205.236	ICMP	42	Echo (ping) request id=0x6f5c, seq=0/0, ttl=57 (reply in 9)
2	0.00007300	192.168.43.74	202.162.205.236	TCP	58	42168→443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.00009600	192.168.43.74	202.162.205.236	TCP	54	42168→80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
4	0.00011700	192.168.43.74	202.162.205.236	ICMP	54	Timestamp request id=0xc02b, seq=0/0, ttl=45
5	0.73726700	202.162.205.236	192.168.43.74	TCP	58	443→42168 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400
6	0.73731900	192.168.43.74	202.162.205.236	TCP	54	42168→443 [RST] Seq=1 Win=0 Len=0
7	0.78673700	202.162.205.236	192.168.43.74	TCP	54	80→42168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	0.84505500	192.168.43.74	192.168.43.1	DNS	88	Standard query 0xa154 PTR 236.205.162.202.in-addr.arpa
9	0.84625800	202.162.205.236	192.168.43.74	ICMP	42	Echo (ping) reply id=0x6f5c, seq=0/0, ttl=55 (request in 1)
10	4.84559200	192.168.43.74	192.168.43.1	DNS	88	Standard query 0xa154 PTR 236.205.162.202.in-addr.arpa
11	5.00922500	HonHaiPr_35:49:c9	SamsungE_5f:ea:c7	ARP	42	Who has 192.168.43.1? Tell 192.168.43.74
12	5.01019400	SamsungE_5f:ea:c7	HonHaiPr_35:49:c9	ARP	42	192.168.43.1 is at a0:b4:a5:5f:ea:c7
13	8.84531100	192.168.43.74	192.168.43.1	DNS	88	Standard query 0xa154 PTR 236.205.162.202.in-addr.arpa
14	1.9033250	192.168.43.74	202.162.205.236	TCP	54	42424→23 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

Gambar 8. Hasil capture paket menggunakan aplikasi wireshark

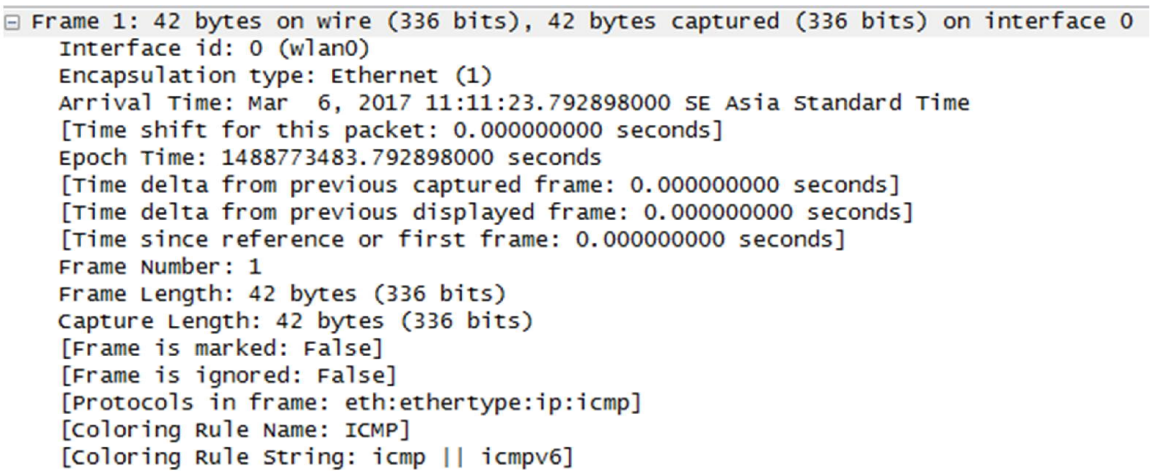
Pada gambar 8 menunjukan port 80 yang open, dimana port 80 tersebut menggunakan protokol TCP. Isi dari protokol TCP dapat dilihat pada gambar 9.

Pada gambar 8 juga menunjukan protokol ICMP, dimana protokol tersebut berfungsi untuk Membantu proses error handling atau melaporkan apabila terjadi error pada sebuah jaringan, membantu control procedure atau prosedur pengaturan pada sebuah jaringan, menyediakan pengendalian error dan pengendalian arus pada network layer atau lapisan jaringan, dan mendeteksi terjadinya error pada jaringan, seperti connection lost, kemacetan jaringan. Isi dari protokol ICMP dapat dilihat pada gambar 10.



```
Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
    Interface id: 0 (wlan0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  6, 2017 11:11:23.792994000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1488773483.792994000 seconds
    [Time delta from previous captured frame: 0.000023000 seconds]
    [Time delta from previous displayed frame: 0.000023000 seconds]
    [Time since reference or first frame: 0.000096000 seconds]
    Frame Number: 3
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

Gambar 9. Hasil dari protokol TCP dengan port 80



Gambar 10. Hasil dari protokol ICMP

Referensi :

D. Stiawan, A. H. Abdullah, and M. Y. Idris, “Classification of Habitual Activities in Behavior-based Network Detection,” vol. 2, no. 8, pp. 1–7, 2010.