Lampiran

Rule flooding attack yang digunakan untuk deteksi serangan sebagai berikut:

```
#

#----------

# DOS RULES

#----------

#

alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS Jolt attack";
dsize:408; fragbits:M; reference:cve,1999-0345; classtype:attempted-dos;
sid:268; rev:4;)

alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS Teardrop attack";
fragbits:M; id:242; reference:bugtraq,124; reference:cve,1999-0015;
reference:nessus,10279; reference:url,www.cert.org/advisories/CA-1997-
28.html; classtype:attempted-dos; sid:270; rev:6;)

alert udp any 19 <> any 7 (msg:"DOS UDP echo+chargen bomb";
reference:cve,1999-0103; reference:cve,1999-0635; classtype:attempted-dos;
sid:271; rev:5;)

alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS IGMP dos attack";
fragbits:M+; ip_proto:2; reference:bugtraq,514; reference:cve,1999-0918;
classtype:attempted-dos; sid:272; rev:9;)

alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS IGMP dos attack";
fragbits:M+; ip_proto:2; reference:bugtraq,514; reference:cve,1999-0918;
classtype:attempted-dos; sid:273; rev:8;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS ath"; itype:8;
content:"+++ath"; nocase; reference:arachnids,264; reference:cve,1999-1228;
classtype:attempted-dos; sid:274; rev:5;)

alert tcp $EXTERNAL_NET any <> $HOME_NET any (msg:"DOS NAPTHA";
flow:stateless; flags:S; id:413; seq:6060842; reference:bugtraq,2022;
reference:cve,2000-1039;
reference:url,razor.bindview.com/publish/advisories/adv_NAPTHA.html;
reference:url,www.cert.org/advisories/CA-2000-21.html;
reference:url,www.microsoft.com/technet/security/bulletin/MS00-091.mspx;
classtype:attempted-dos; sid:275; rev:12;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 7070 (msg:"DOS Real Audio Server";
flow:to_server,established; content:"|FF F4 FF FD 06|";
reference:arachnids,411; reference:bugtraq,1288; reference:cve,2000-0474;
classtype:attempted-dos; sid:276; rev:5;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 7070 (msg:"DOS Real Server
template.html"; flow:to_server,established;
content:"/viewsource/template.html?"; nocase; reference:bugtraq,1288;
reference:cve,2000-0474; classtype:attempted-dos; sid:277; rev:5;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 8080 (msg:"DOS Real Server
template.html"; flow:to_server,established;
content:"/viewsource/template.html?"; nocase; reference:bugtraq,1288;
reference:cve,2000-0474; classtype:attempted-dos; sid:278; rev:5;)

alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"DOS Bay/Nortel Nautica
Marlin"; dsize:0; reference:bugtraq,1009; reference:cve,2000-0221;
classtype:attempted-dos; sid:279; rev:4;)

alert udp $EXTERNAL_NET any -> $HOME_NET 9 (msg:"DOS Ascend Route";
content:"NAMENAME"; depth:50; offset:25; reference:arachnids,262;
reference:bugtraq,714; reference:cve,1999-0060; classtype:attempted-dos;
sid:281; rev:5;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 617 (msg:"DOS arkiea backup";
flow:to_server,established; dsize:>1445; reference:arachnids,261;
reference:bugtraq,662; reference:cve,1999-0788; classtype:attempted-dos;
sid:282; rev:8;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 135:139 (msg:"DOS Winnuke attack";
flow:stateless; flags:U+; reference:bugtraq,2010; reference:cve,1999-0153;
classtype:attempted-dos; sid:1257; rev:10;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 3372 (msg:"DOS MSDTC attempt";
flow:to_server,established; dsize:>1023; reference:bugtraq,4006;
reference:cve,2002-0224; reference:nessus,10939; classtype:attempted-dos;
sid:1408; rev:10;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 6004 (msg:"DOS iParty DOS attempt";
flow:to_server,established; content:"|FF FF FF FF FF FF|"; offset:0;
reference:bugtraq,6844; reference:cve,1999-1566; classtype:misc-attack;
sid:1605; rev:6;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 6789:6790 (msg:"DOS DB2 dos
attempt"; flow:to_server,established; dsize:1; reference:bugtraq,3010;
reference:cve,2001-1143; reference:nessus,10871; classtype:denial-of-service;
sid:1641; rev:10;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"DOS Cisco attempt";
flow:to_server,established; dsize:1; content:"|13|"; classtype:web-
application-attack; sid:1545; rev:8;)

alert udp $EXTERNAL_NET any -> $HOME_NET 500 (msg:"DOS ISAKMP invalid
identification payload attempt"; content:"|05|"; depth:1; offset:16;
byte_test:2,>,4,30; byte_test:2,<,8,30; reference:bugtraq,10004;
reference:cve,2004-0184; classtype:attempted-dos; sid:2486; rev:5;)
```

```
alert tcp $EXTERNAL_NET any <> $HOME_NET 179 (msg:"DOS BGP spoofed connection
reset attempt"; flow:established; flags:RSF*; threshold:type both,track
by_dst,count 10,seconds 10; reference:bugtraq,10183; reference:cve,2004-0230;
reference:url,www.uniras.gov.uk/vuls/2004/236929/index.htm;
classtype:attempted-dos; sid:2523; rev:7;)

alert udp $EXTERNAL_NET any -> $HOME_NET 2048 (msg:"DOS squid WCCP I_SEE_YOU
message overflow attempt"; content:"|00 00 00 08|"; depth:4;
byte_test:4,>,32,16; reference:cve,CAN-2005-0095; reference:bugtraq,12275;
classtype:attempted-user; sid:3089; rev:1;)
```

Lampiran tabel rule flooding attack:

No.	RULE	KETERANGAN
1	Alert	Tanda peringatan
	Ip	Alamat IP
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS Jolt attack"; dsize:408;	Pesan yang akan diterima apabila terjadi sebuah event
	fragbits:M;	Ukuran data
	reference:cve,1999-0345;	Merupakan referensi ke system pengidentifikasian
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:268;	Merupakan id dari aturan snort
	rev:4;)	Refisi aturan snort ke 4
2	Alert	Tanda peringatan
	Udp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	(msg:"DOS Teardrop attack";	Pesan yang akan diterima apabila terjadi sebuah event
	fragbits:M;	Ukuran data
	id:242;	Merupakan id dari aturan snort
	reference:bugtraq,124; reference:cve,1999-0015; reference:nessus,10279; reference:url,www.cert.org/advisories/CA-1997-28.html;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:270;	Merupakan id dari aturan snort
	rev:6;)	Refisi aturan snort ke 6
3	Alert	Tanda peringatan
	Udp	Jenis protokol transport
	any 19	Host tujuan port 19
	<>	Aliran host
	any 7	Host tujuan port 7
	(msg:"DOS UDP echo+chargen bomb";	Pesan yang akan diterima apabila terjadi sebuah event
	reference:cve,1999-0103; reference:cve,1999-0635;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:271;	Merupakan id dari aturan snort
	rev:5;)	Refisi aturan snort ke 5
4	Alert	Tanda peringatan
	Ip	Alamat IP
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS IGMP dos attack";	Pesan yang akan diterima apabila terjadi sebuah

		event
	fragbits:M+;	Ukuran data
	ip_proto:2;	IP Protokol 2
	reference:bugtraq,514; reference:cve,1999-0918;	Merupakan referensi ke system pengidentifikasian serangan
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:272;	Merupakan id dari aturan snort
	rev:9;)	Refisi aturan snort ke 9
5	Alert	Tanda peringatan
	Ip	Alamat IP
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS IGMP dos attack"; fragbits:M+;	Pesan yang akan diterima apabila terjadi sebuah event
	ip_proto:2;	IP Protokol 2
	reference:bugtraq,514; reference:cve,1999-0918;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:273;	Merupakan id dari aturan snort
	rev:8;)	Refisi aturan snort ke 8
6	Alert	Tanda peringatan
	Icmp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS ath"; itype:8; content:"+++ath"; nocase;	Pesan yang akan diterima apabila terjadi sebuah event
	reference:arachnids,264;	Merupakan referensi ke sistem pengidentifikasian serangan
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:274;	Merupakan id dari aturan snort
	rev:5;)	Refisi aturan snort ke 5
7	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	<>	
	(msg:"DOS NAPTHA"; flow:stateless;	Pesan yang akan diterima apabila terjadi sebuah event
	flags:S;	Serangan
	id:413;	Nomor id
	seq:6060842;	Waktu
	reference:bugtraq,2022; reference:cve,2000-1039; reference:url,razor.bindview.com/publish/advisories/adv_NAPTHA.html; reference:url,www.cert.org/advisories/CA-2000-21.html; reference:url,www.microsoft.com/t	Merupakan referensi ke system pengidentifikasian serangan eksternal

	echnet/security/bulletin/MS00-091.mspx;	
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:275;	Merupakan id dari aturan snort
	rev:12;)	Refisi aturan snort ke 12
8	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS Real Audio Server";	Pesan yang akan diterima apabila terjadi sebuah event
	flow:to_server,established;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	content:"|FF F4 FF FD 06|";	Konten spesifik yang dicari
	reference:arachnids,411; reference:bugtraq,1288; reference:cve,2000-0474;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:276;	Merupakan id dari aturan snort
	rev:5;)	Refisi aturan snort ke 5
9	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS Real Server template.html";	Pesan yang akan diterima apabila terjadi sebuah event
	flow:to_server,established;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	content:"/viewsource/template.html?";	Kontes spesifik yang dicari
	nocase;	Tidak ada aturan
	reference:bugtraq,1288; reference:cve,2000-0474;	Merupakan referensi ke system pengidentifikasian serangan
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:277;	Merupakan id dari aturan snort
	rev:5;)	Refisi aturan snort ke 5
10	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS Real Server template.html";	Pesan yang akan diterima apabila terjadi sebuah event
	flow:to_server,established;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	content:"/viewsource/template.html?";	Konten spesifik yang dicari
	nocase;	Tidak ada aturan
	reference:bugtraq,1288;	Merupakan referensi ke system pengidentifikasian

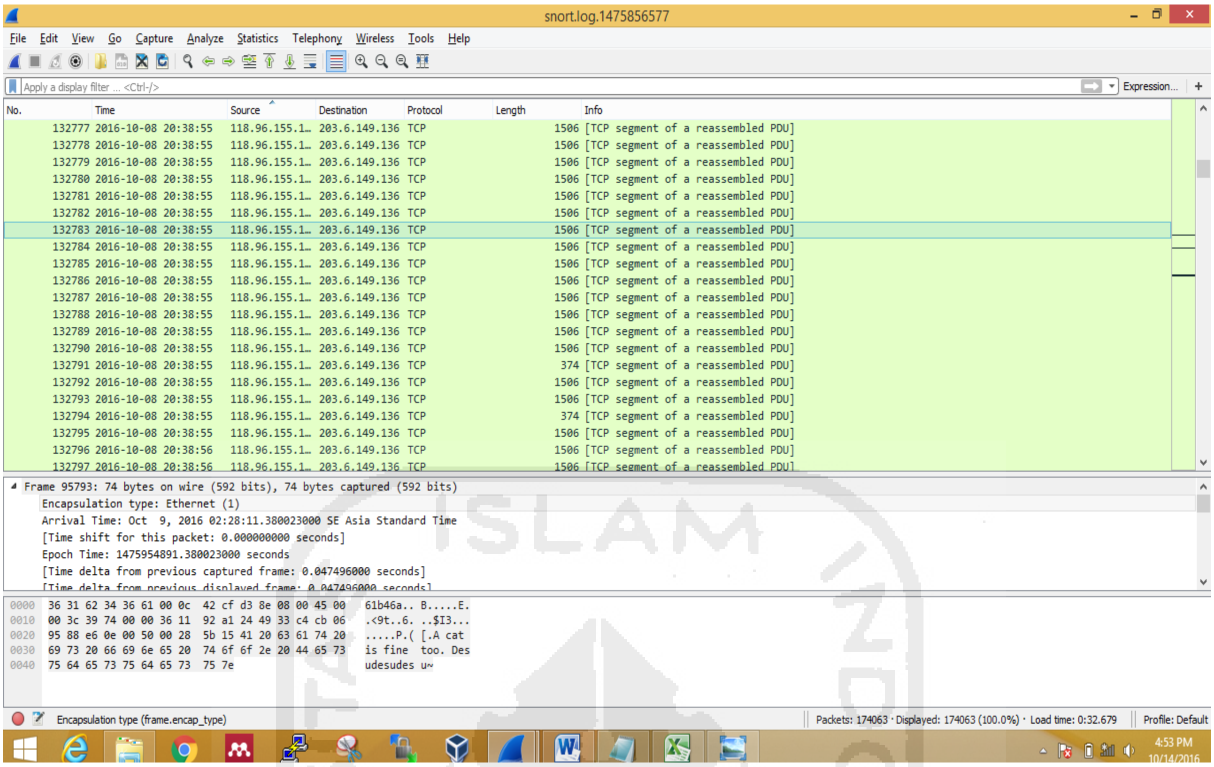
	reference:cve,2000-0474;	serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:278;	Merupakan id dari aturan snort
	rev:5;)	Refisi aturan snort ke 5
11	Alert	Tanda peringatan
	Udp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS Bay/Nortel Nautica Marlin";	Pesan yang akan diterima apabila terjadi sebuah event
	dsize:0;	Ukuran data
	reference:bugtraq,1009; reference:cve,2000-0221;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:279;	Merupakan id dari aturan snort
	rev:4;)	Refisi aturan snort ke 4
12	Alert	Tanda peringatan
	Udp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS Ascend Route"; content:"NAMENAME";	Pesan yang akan diterima apabila terjadi sebuah event
	depth:50;	Untuk mencari pola yang sesuai dengan konten pada 50 byte pertama pada payload
	offset:25;	Akhir data 25
	reference:arachnids,262; reference:bugtraq,714; reference:cve,1999-0060;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:281;	Merupakan id dari aturan snort
	rev:5;)	Refisi aturan snort ke 5
13	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS arkiea backup";	Pesan yang akan diterima apabila terjadi sebuah event
	flow:to_server,established;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	dsize:>1445;	Ukuran host
	reference:arachnids,261; reference:bugtraq,662; reference:cve,1999-0788; classtype:attempted-dos;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:282;	Merupakan id dari aturan snort
	rev:8;)	Refisi aturan snort ke 8

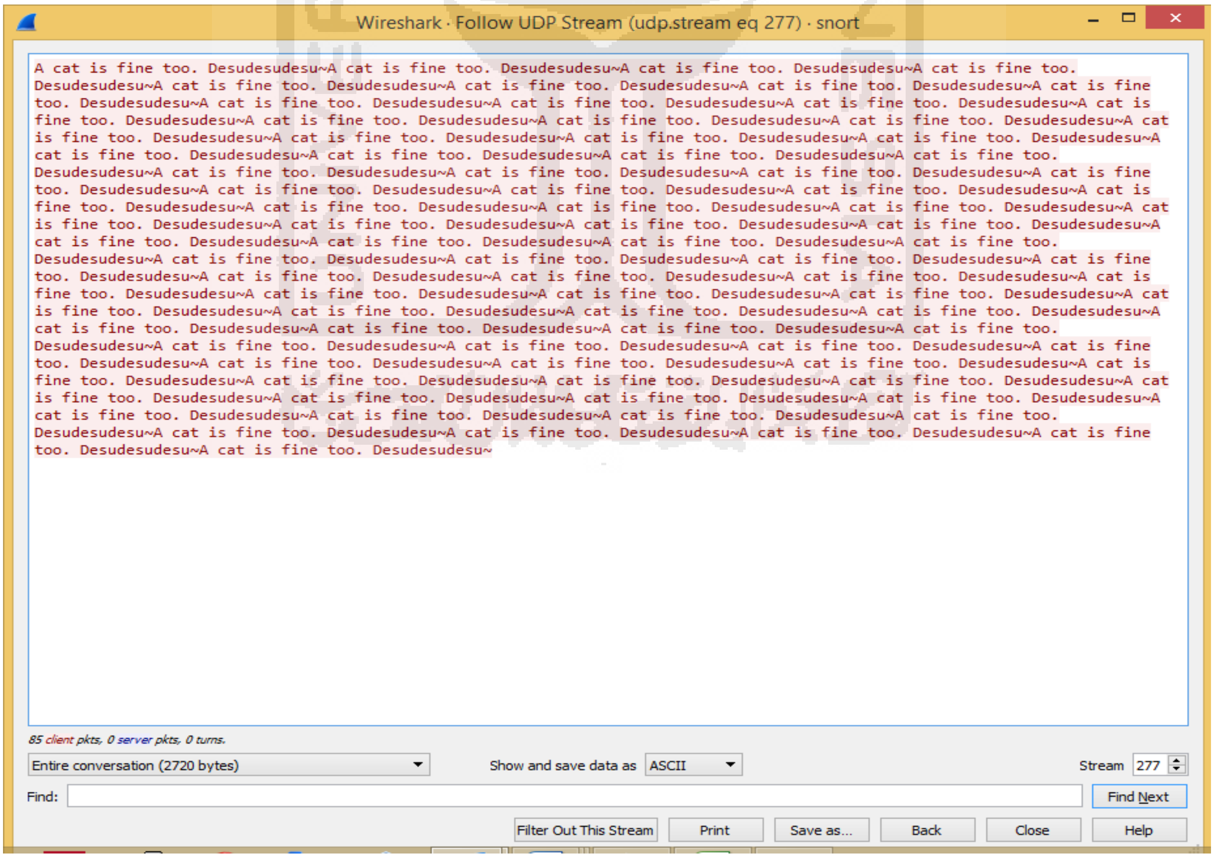
14	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS Winnuke attack";	Pesan yang akan diterima apabila terjadi sebuah event
	flow:stateless;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	flags:U+;	Nama host
	reference:bugtraq,2010; reference:cve,1999-0153;	Merupakan referensi ke sistem pengidentifikasian serangan
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:1257;	Merupakan id dari aturan snort
	rev:10;)	Refisi aturan snort ke 10
15	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS MSDTC attempt";	Pesan yang akan diterima apabila terjadi sebuah event
	flow:to_server,established;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	dsize:>1023;	Ukuran host
	reference:bugtraq,4006; reference:cve,2002-0224; reference:nessus,10939;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:1408;	Merupakan id dari aturan snort
	rev:10;)	Refisi aturan snort ke 10
16	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS iParty DOS attempt";	Pesan yang akan diterima apabila terjadi sebuah event
	flow:to_server,established;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	content:"|FF FF FF FF FF FF|";	Isi spesifik konten
	offset:0;	Akhir data
	reference:bugtraq,6844; reference:cve,1999-1566;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:misc-attack;	Percobaan Denial of Service
	sid:1605;	Merupakan id dari aturan snort
	rev:6;)	Refisi aturan snort ke 6
17	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun

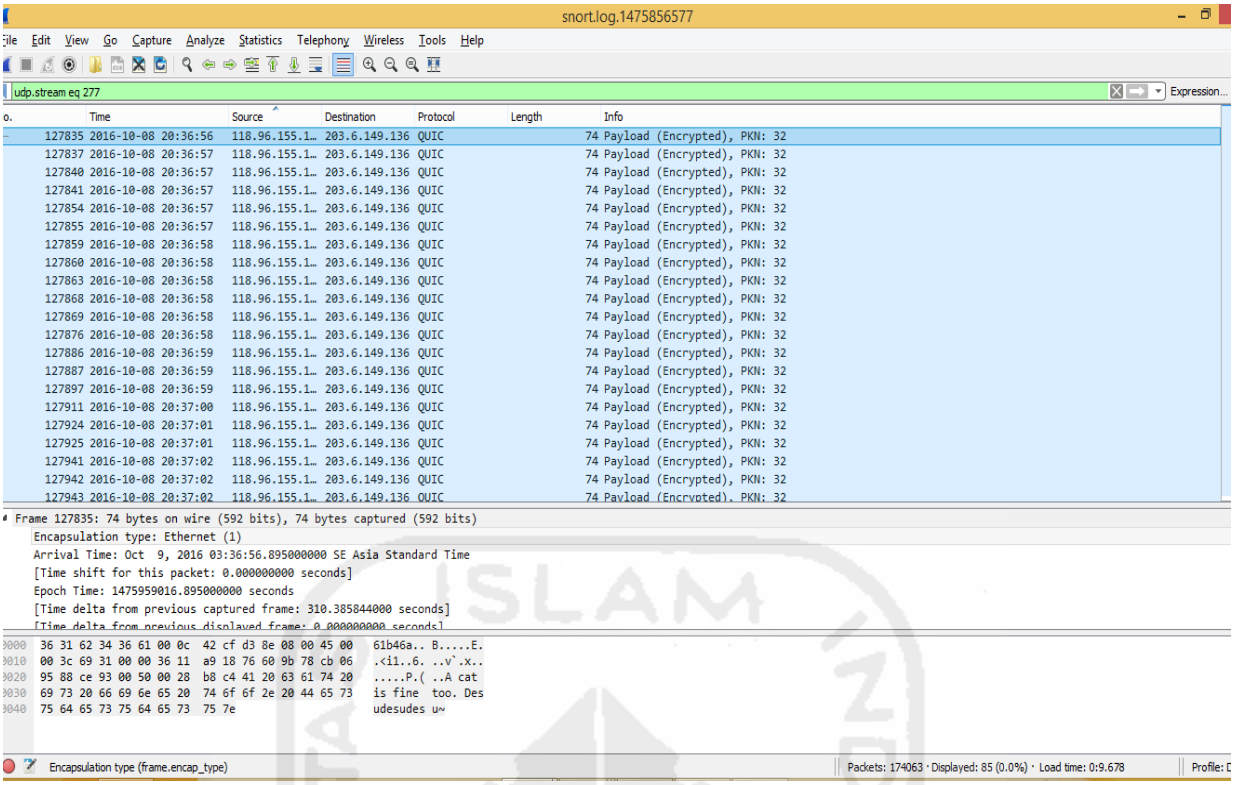
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS DB2 dos attempt";	Pesan yang akan diterima apabila terjadi sebuah event
	flow:to_server,established;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	dsize:1;	Ukuran konten
	reference:bugtraq,3010; reference:cve,2001-1143; reference:nessus,10871;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:denial-of-service;	Percobaan Denial of Service
	sid:1641;	Merupakan id dari aturan snort
	rev:10;)	Refisi aturan snort ke 10
18	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS Cisco attempt";	Pesan yang akan diterima apabila terjadi sebuah event
	flow:to_server,established;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	dsize:1;	Ukuran size
	content:"|13|";	Isi spesifikasi konten
	classtype:web-application-attack;	Serangan aplikasi web
	sid:1545;	Merupakan id dari aturan snort
	rev:8;)	Refisi aturan snort ke 8
19	Alert	Tanda peringatan
	Udp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS ISAKMP invalid identification payload attempt";	Pesan yang akan diterima apabila terjadi sebuah event
	content:"|05|";	Isi spesifikasi konten yang dicari
	depth:1;	Terbuka konten
	offset:16;	Akhir host 16
	byte_test:2,>,4,30;	Ukuran konten
	byte_test:2,<,8,30;	
	reference:bugtraq,10004; reference:cve,2004-0184;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:2486;	Merupakan id dari aturan snort
	rev:5;)	Refisi aturan snort ke 5
20	Alert	Tanda peringatan
	tcp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS BGP spoofed connection reset attempt";	Pesan yang akan diterima apabila terjadi sebuah event

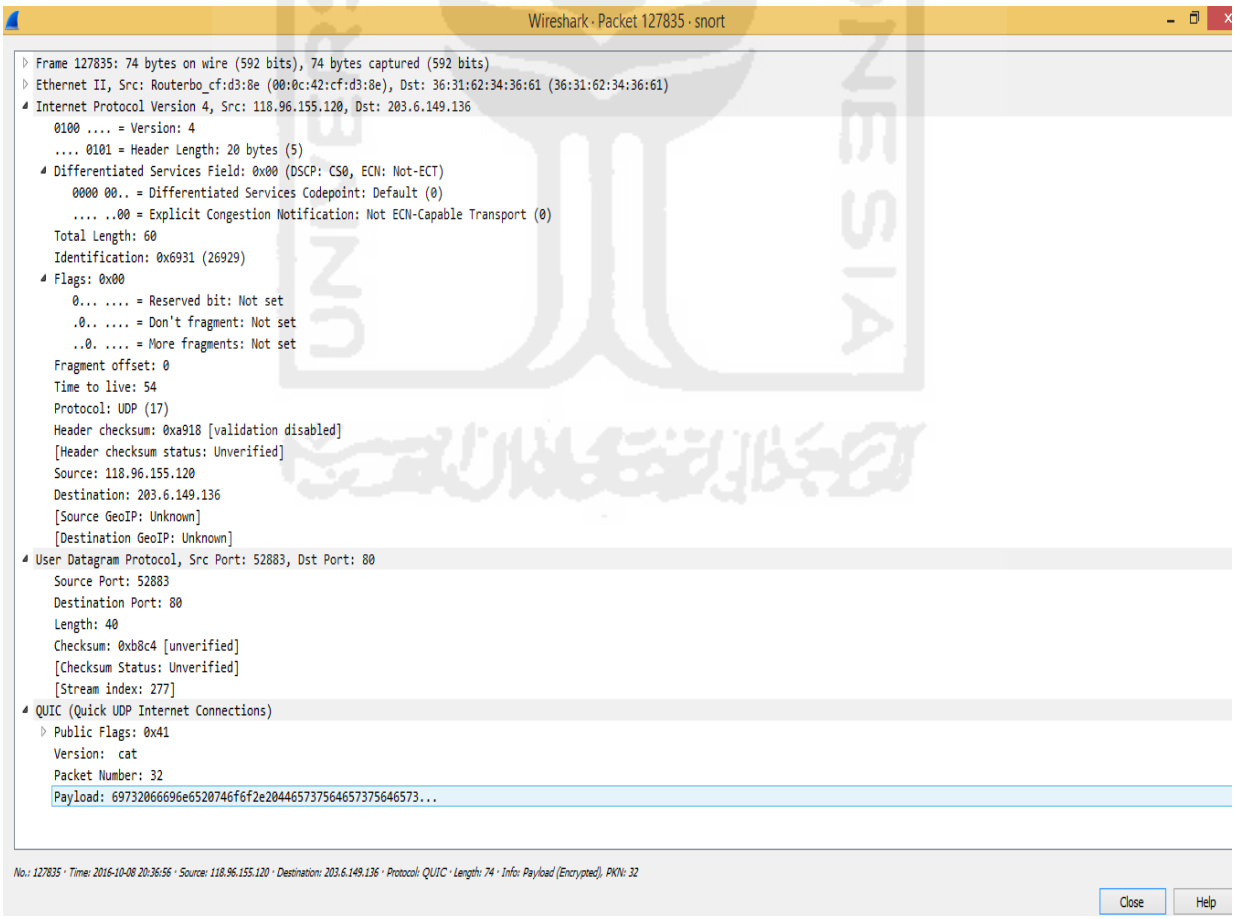
	flow:established;	Koneksi TCP yang terbentuk dalam host sumber ke host tujuan
	flags:RSF*;	Tanda yang dituju
	threshold:type both,track by_dst,count 10,seconds 10;	Tipe yang dipakaidalam waktu detik
	reference:bugtraq,10183; reference:cve,2004-0230; reference:url,www.uniras.gov.uk/vuls/2004/236929/index.htm;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-dos;	Percobaan Denial of Service
	sid:2523;	Merupakan id dari aturan snort
	rev:7;)	Refisi aturan snort ke 7
21	Alert	Tanda peringatan
	Udp	Jenis protokol transport
	$EXTERNAL_NET any	Host asal yang melewati port manapun
	->	Aliran dari host asal ke host tujuan
	(msg:"DOS squid WCCP I_SEE_YOU message overflow attempt";	Pesan yang akan diterima apabila terjadi sebuah event
	content:"|00 00 00 08|";	Isi konten spesifik yang dicari
	depth:4;	Ukuran
	byte_test:4,>,32,16;	Test kecepatan
	reference:cve,CAN-2005-0095; reference:bugtraq,12275;	Merupakan referensi ke system pengidentifikasian serangan eksternal
	classtype:attempted-user;	Mencoba mendapatkan hak user
	sid:3089;	Merupakan id dari aturan snort
	rev:1;)	Refisi aturan snort ke 1

Lampiran gambar analisis bab iv






snort.log.1475856577
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.stream eq 277
No. Time Source Destination Protocol Length Info
127835 2016-10-08 20:36:56 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127837 2016-10-08 20:36:57 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127840 2016-10-08 20:36:57 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127841 2016-10-08 20:36:57 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127854 2016-10-08 20:36:57 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127855 2016-10-08 20:36:57 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127859 2016-10-08 20:36:58 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127860 2016-10-08 20:36:58 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127863 2016-10-08 20:36:58 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127868 2016-10-08 20:36:58 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127869 2016-10-08 20:36:58 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127876 2016-10-08 20:36:58 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127886 2016-10-08 20:36:59 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127887 2016-10-08 20:36:59 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127897 2016-10-08 20:36:59 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127911 2016-10-08 20:37:00 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127924 2016-10-08 20:37:01 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127925 2016-10-08 20:37:01 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127941 2016-10-08 20:37:02 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127942 2016-10-08 20:37:02 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
127943 2016-10-08 20:37:02 118.96.155.1… 203.6.149.136 QUIC 74 Payload (Encrypted), PKN: 32
Frame 127835: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 9, 2016 03:36:56.895000000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1475959016.895000000 seconds
[Time delta from previous captured frame: 310.385844000 seconds]
0000 36 31 62 34 36 61 00 0c 42 cf d3 8e 08 00 45 00 61b46a.. B.....E.
0010 00 3c 69 31 00 00 36 11 a9 18 76 60 9b 78 cb 06 .<i1..6. ..v`.x..
0020 95 88 ce 93 00 50 00 28 b8 c4 41 20 63 61 74 20 .....P.(..A cat
0030 69 73 20 66 69 6e 65 20 74 6f 6f 2e 20 44 65 73 is fine too. Des
0040 75 64 65 73 75 73 64 65 73 75 7e udesudes u~
Encapsulation type (frame.encap_type)
Packets: 174063 · Displayed: 85 (0.0%) · Load time: 0:9.678
Profile:


Wireshark · Packet 127835 · snort
Frame 127835: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Routerbo_cf:d3:8e (00:0c:42:cf:d3:8e), Dst: 36:31:62:34:36:61 (36:31:62:34:36:61)
Internet Protocol Version 4, Src: 118.96.155.120, Dst: 203.6.149.136
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 60
Identification: 0x6931 (26929)
Flags: 0x00
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 54
Protocol: UDP (17)
Header checksum: 0xa918 [validation disabled]
[Header checksum status: Unverified]
Source: 118.96.155.120
Destination: 203.6.149.136
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 52883, Dst Port: 80
Source Port: 52883
Destination Port: 80
Length: 40
Checksum: 0xb8c4 [unverified]
[Checksum Status: Unverified]
[Stream index: 277]
QUIC (Quick UDP Internet Connections)
Public Flags: 0x41
Version: cat
Packet Number: 32
Payload: 69732066696e6520746f6f2e20446573756573756573646573...
No.: 127835 · Time: 2016-10-08 20:36:56 · Source: 118.96.155.120 · Destination: 203.6.149.136 · Protocol: QUIC · Length: 74 · Info: Payload (Encrypted), PKN: 32
Close
Help