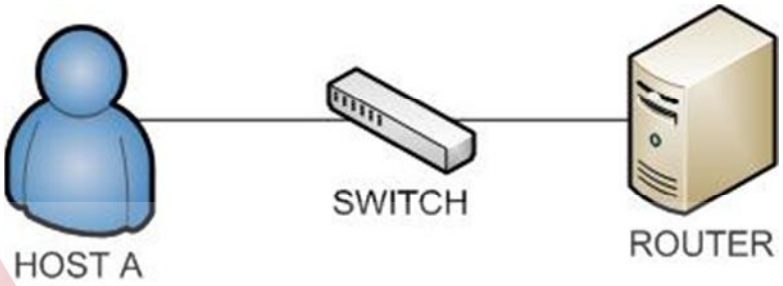
BAB IV

PENGUJIAN DAN ANALISIS SISTEM

Pengujian sistem terhadap aplikasi IDS dilakukan dari *host* a yang melakukan serangan langsung kepada *host* b seperti yang ditunjukkan pada Gambar 4.1.



Gambar 4.1. Skema Serangan DoS

Gambar 4.1 merupakan contoh skema serangan yang dilakukan oleh satu *host* (*host* A) menuju router. Tujuan dari serangan tersebut adalah menghentikan *service* yang diberikan oleh router sehingga seluruh jaringan yang tersambung oleh router akan *down.*

4.1 Pengujian Authentifikasi

Autentifikasi diperlukan supaya tidak sembarang user dapat melihat *log* serangan IDS. Proses autentifikasi dilakukan dengan memasukkan *username* dan *password* pada halaman *login*. Jika *username* dan *password* dikenali oleh database maka user dapat melihat *log* serangan ids, jika tidak maka user disuruh memasukkan ulang *password*.

4.1.1 Tujuan

Tujuan pengujian autentifikasi adalah untuk melihat proses autentifikasi sudah berjalan dengan benar atau tidak.

4.1.2 Alat Pengujian

Berikut ini adalah beberapa alat yang digunakan:

1. PC Router

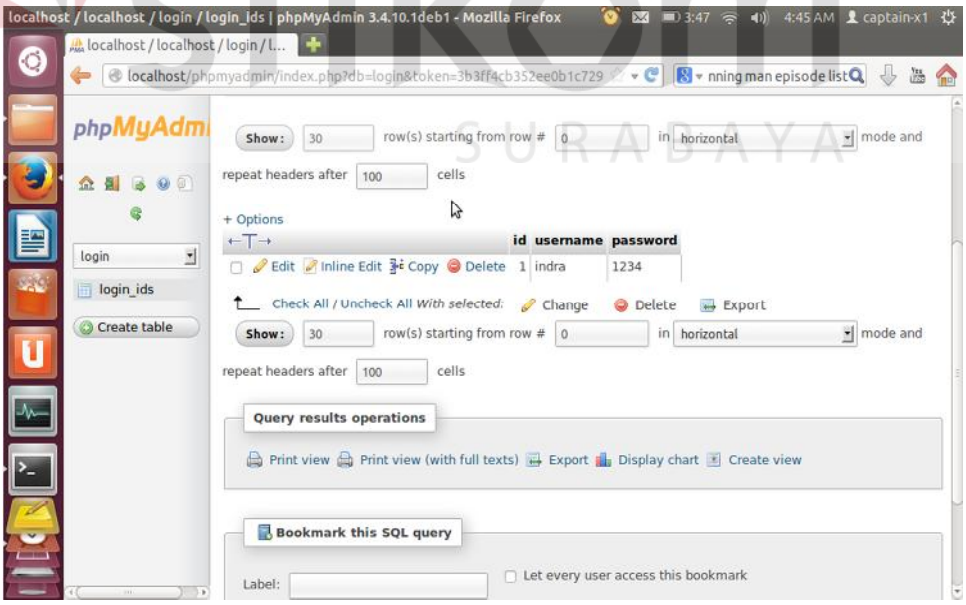
4.1.3 Prosedur Pengujian

Berikut adalah beberapa tahapan prosedur pengujian:

1. Hidupkan PC Router
2. Daftarkan *username* dan *password* pada *database login*
3. Masukkan *username* dan *password* pada halaman *login*

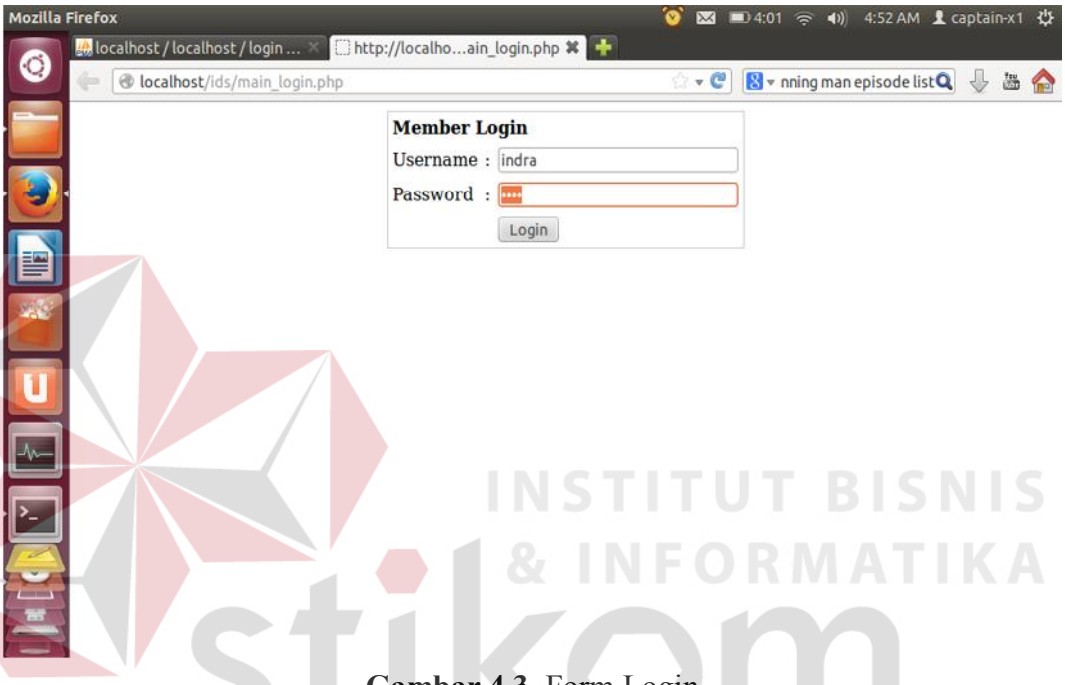
4.1.4 Hasil Pengujian

Untuk mendaftarkan *username* dan *password* dilakukan dengan menggunakan aplikasi *phpmyadmin*. Berikut contoh *username* dan *password* yang telah didaftarkan pada database login yang ditunjukkan pada Gambar 4.2.



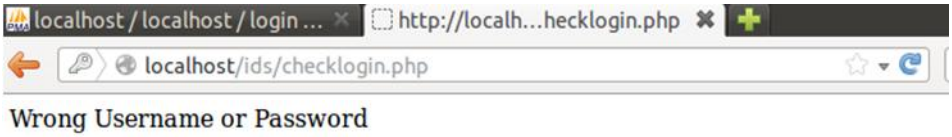
Gambar 4.2. Database *Username* dan *Password*

Gambar 4.2 menunjukkan *database* login yang berisikan *id 1*, *username indra* dan *password 1234* . Apabila *username* dan *password* sudah terdaftar pada *database login* maka user dapat melakukan proses *autentifikasi*. Pertama-tama user diarahkan untuk masuk pada *form login* pada halaman *main_login*. Berikut ini adalah *form login* yang tersedia:



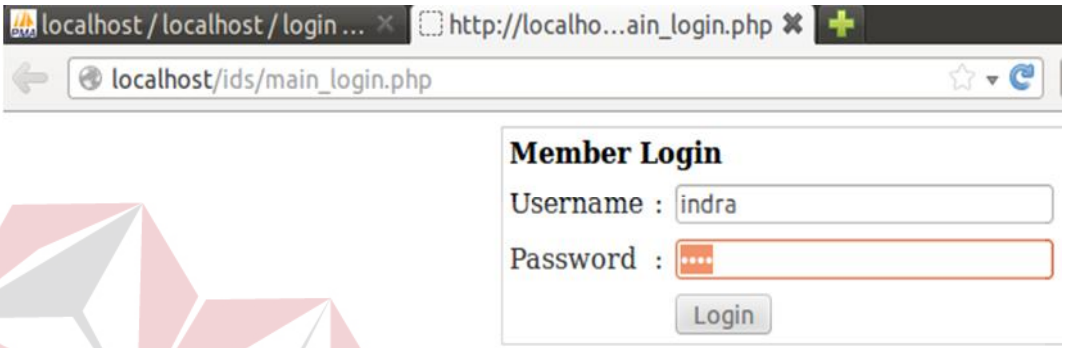
Gambar 4.3. Form Login

Gambar 4.3 menunjukkan form login , proses login dapat berhasil jika user memasukkan *username* dan *password* sesuai dengan data yang ada pada database login. Jika salah maka secara otomatis browser akan mengarahkan ke halaman *checklogin* untuk menunjukkan bahwa *username* dan *password* yang dimasukkan salah. Berikut contoh login tidak sesuai dengan database:



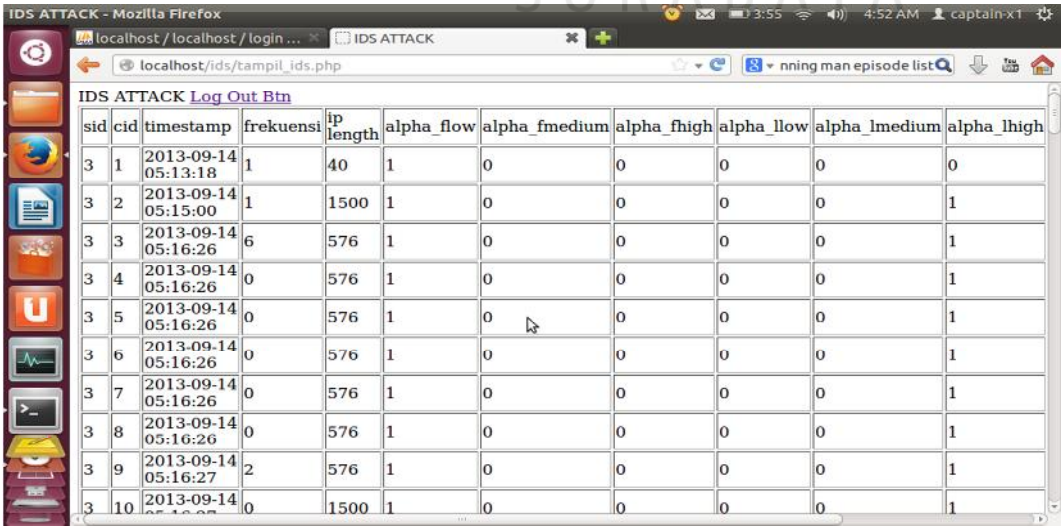
Gambar 4.4. Login Gagal

Gambar 4.4 menunjukkan user salah dalam memasukkan *username* atau *password.* Halaman *checklogin* berfungsi untuk menunjukkan bahwa user salah memasukkan *username* dan *password*. Halaman ini akan langsung secara otomatis muncul apabila user salah login. Sementara itu apabila login benar maka browser akan mengarahkan pada halaman *log* IDS. Berikut ini adalah pengisian data login yang benar.



Gambar 4.5. Login sesuai dengan Database

Gambar 4.5 menunjukkan pengisian *username* dan *password* yang benar. Jika data *login* diisi dengan benar maka browser akan mengarahkan pada halaman *tampil_ids* untuk menampilkan hasil *log* serangan. Berikut ini adalah halaman tampil_ids:



sid	cid	timestamp	frekuensi	ip length	alpha_flow	alpha_fmedium	alpha_fhigh	alpha_llow	alpha_lmedium	alpha_lhigh
3	1	2013-09-14 05:13:18	1	40	1	0	0	0	0	0
3	2	2013-09-14 05:15:00	1	1500	1	0	0	0	0	1
3	3	2013-09-14 05:16:26	6	576	1	0	0	0	0	1
3	4	2013-09-14 05:16:26	0	576	1	0	0	0	0	1
3	5	2013-09-14 05:16:26	0	576	1	0	0	0	0	1
3	6	2013-09-14 05:16:26	0	576	1	0	0	0	0	1
3	7	2013-09-14 05:16:26	0	576	1	0	0	0	0	1
3	8	2013-09-14 05:16:26	0	576	1	0	0	0	0	1
3	9	2013-09-14 05:16:27	2	576	1	0	0	0	0	1
3	10	2013-09-14	0	1500	1	0	0	0	0	1

Gambar 4.6. Login Sukses

Gambar 4.6 menunjukkan halaman web log IDS, halaman ini akan muncul jika user berhasil memasukkan *username* dan *password* dengan benar.

4.2 Pengujian Serangan DoS

Pengujian serangan DoS dilakukan oleh *host* A seperti skema serangan pada gambar 4.1. *Host* A melakukan serangan dengan menggunakan *tools* DoS Longcat versi 2.2 dan melalui *command prompt* Windows. Terdapat beberapa jenis pengujian serangan yaitu penyerangan melalui protokol ICMP, UDP dan TCP, selain itu juga dilakukan pengujian terhadap pengiriman paket normal.

4.2.1 Tujuan

Tujuan yang dilakukan adalah untuk mengetahui apakah aplikasi dapat mendeteksi serangan yang dilakukan oleh host dari beberapa protokol yaitu ICMP, UDP dan TCP. Dari pengujian ini juga melihat apakah sistem IDS yang telah dibuat mampu membedakan paket biasa atau serangan.

4.2.2 Alat Pengujian

Berikut adalah beberapa alat yang digunakan:

1. PC Router
2. PC Client
3. Switch
4. Kabel UTP
5. Tools DoS Longcat
6. Command Prompt Windows

7. Command Shell Linux
8. Browser Internet

4.2.3 Prosedur Pengujian

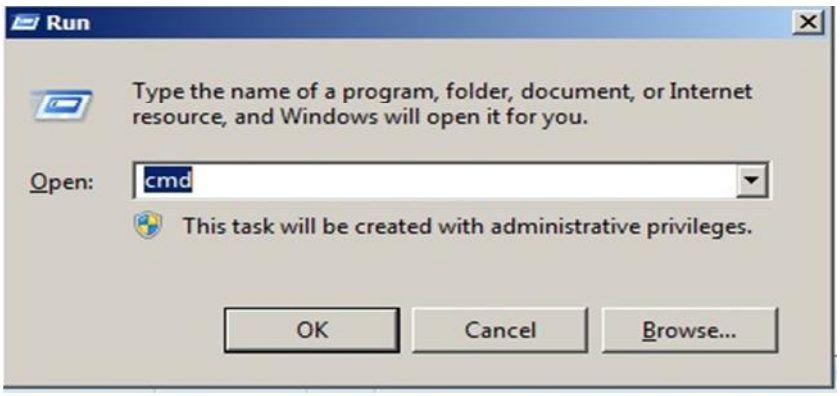
Berikut beberapa tahap-tahap prosedur pengujian:

1. Menghidupkan PC Router
2. Menghidupkan PC Client
3. Menyambungkan masing-masing kabel UTP PC Router dan PC Client ke switch
4. Menjalankan *service* snort pada PC Router
5. Memulai serangan dengan menggunakan DoS *tools* yang sudah disediakan.

4.2.4 Hasil Pengujian

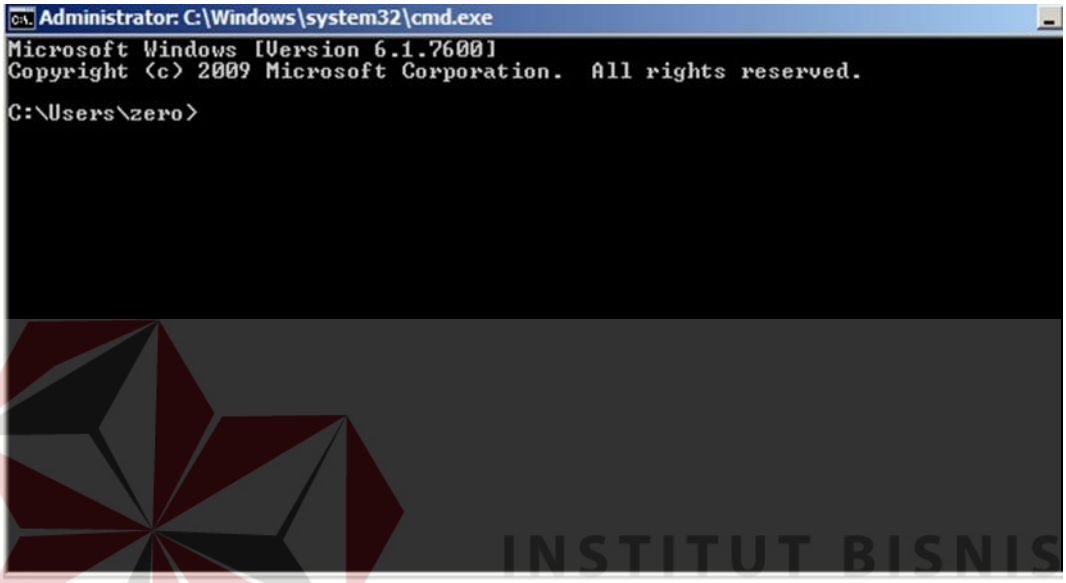
A. Hasil Pengujian Paket Normal

Pengujian pengiriman paket normal dilakukan melalui *command prompt* Windows. Langkah pertama adalah memanggil *command prompt window* melalui jendela *run* kemudian ketikkan perintah cmd seperti yang ditunjukkan pada Gambar 4.7.



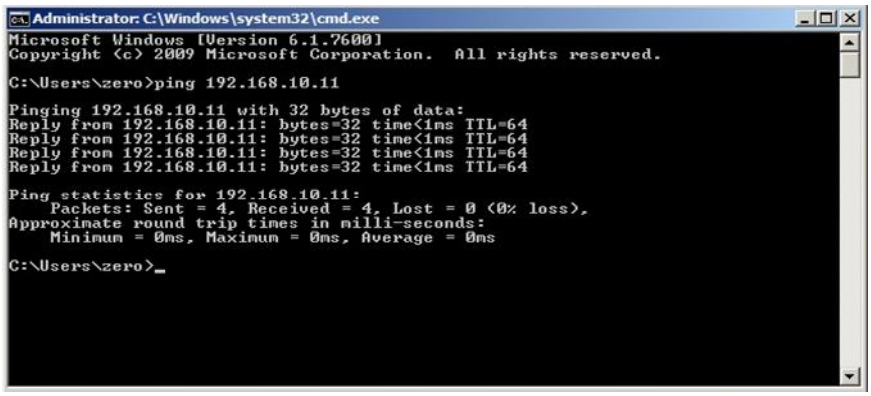
Gambar 4.7. Jendela Run

Gambar 4.7 merupakan jendela *run* yang berfungsi untuk memunculka *command prompt* Windows. Jendela *run* akan muncul dengan menekan logo windows + R pada keyboard. Dengan menekan tombol OK selanjutnya akan muncul jendela *command prompt* seperti yang ditunjukkan pada Gambar 4.8:



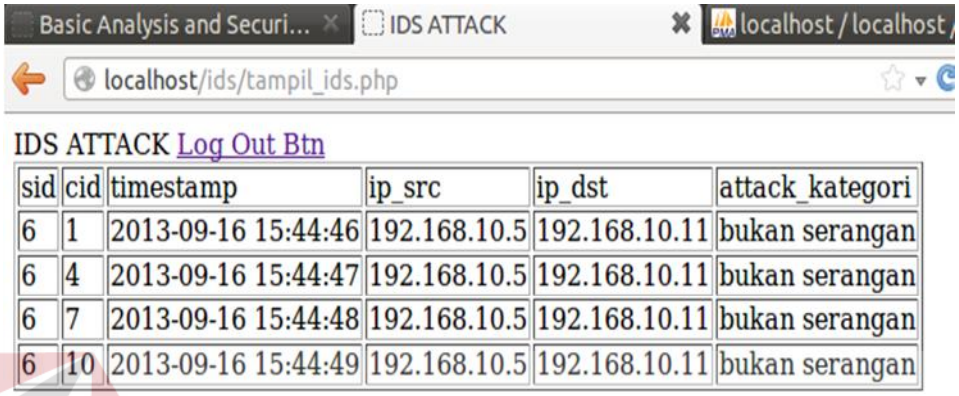
Gambar 4.8. Jendela Command Prompt Windows

Gambar 4.8 menunjukkan tampilan jendela *command prompt* Windows. Melalui *command prompt* seperti yang ditunjukkan pada Gambar 4.8 dapat dilakukan pengiriman paket normal melalui protokol ICMP. Pengiriman dilakukan dengan mengetikkan perintah c:\>*ping 192.168.10.11* dimana 192.168.10.11 adalah alamat *host* target.



Gambar 4.9. Ping Host Target

Gambar 4.9 menunjukkan bahwa *host* target 192.168.10.11 tersambung dengan host pengirim. Indikasi tersebut ditunjukkan dengan pesan *reply from 192.168.10.11*. Adapun hasil weblog pada pc router ditunjukkan oleh Gambar 4.10.



sid	cid	timestamp	ip_src	ip_dst	attack_kategori
6	1	2013-09-16 15:44:46	192.168.10.5	192.168.10.11	bukan serangan
6	4	2013-09-16 15:44:47	192.168.10.5	192.168.10.11	bukan serangan
6	7	2013-09-16 15:44:48	192.168.10.5	192.168.10.11	bukan serangan
6	10	2013-09-16 15:44:49	192.168.10.5	192.168.10.11	bukan serangan

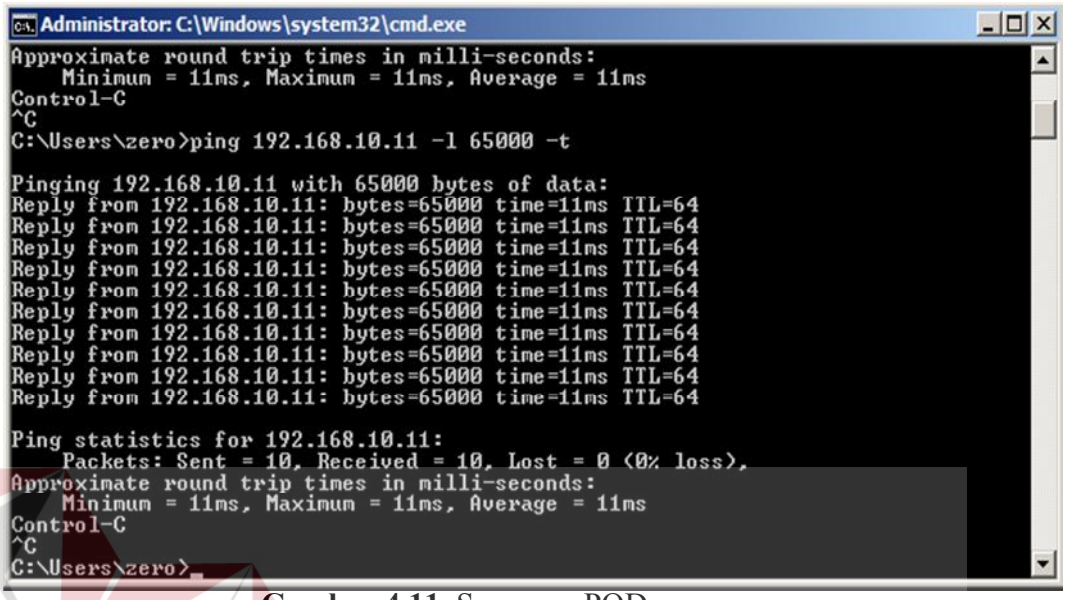
Gambar 4.10. Hasil Web Log IDS

Pada Gambar 4.10 terdapat beberapa kolom yaitu *timestamp, ip_src, ip_dst* dan *attack_kategori*. Kolom *timestamp* berfungsi untuk menunjukkan waktu paket diterima oleh *packet sniffing* snort, kolom *ip_src* berfungsi untuk menunjukkan alamat ip pengirim paket, kolom *ip_dst* berfungsi untuk menunjukkan alamat ip tujuan dan *attack_kategori* berfungsi untuk menunjukkan jenis serangan. Pada gambar 4.10 menunjukkan terdapat 4 paket data dengan masing-masing paket berasal dari host 192.168.10.5 dengan alamat tujuan 192.168.10.11 dengan masing-masing waktu seperti yang ditunjukkan pada gambar. Keempat paket data tersebut mempunyai *attack_kategori* yang sama yaitu bukan serangan.

B. Hasil Pengujian Paket Serangan Protokol ICMP

Ping of Death (POD) adalah salah satu teknik serangan DoS yang bekerja dengan cara mengirim paket ICMP dalam frekuensi dan panjang paket data yang besar secara berkelanjutan. Teknik POD dapat dilakukan melalui *command*

prompt windows. Gambar dibawah ini merupakan perintah POD yang dijalankan dalam jendela *command prompt.*



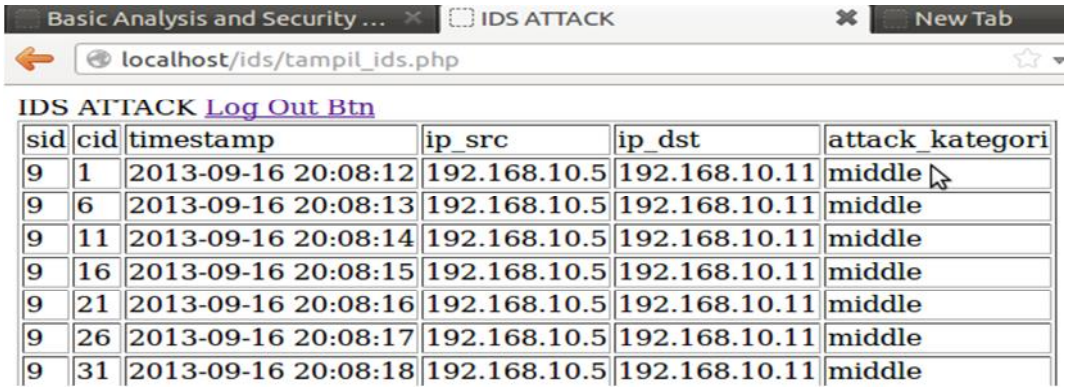
```
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 11ms, Average = 11ms
Control-C
^C
C:\Users\zero>ping 192.168.10.11 -l 65000 -t

Pinging 192.168.10.11 with 65000 bytes of data:
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64
Reply from 192.168.10.11: bytes=65000 time=11ms TTL=64

Ping statistics for 192.168.10.11:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 11ms, Average = 11ms
Control-C
^C
C:\Users\zero>_
```

Gambar 4.11. Serangan POD

Pada Gambar 4.11 untuk melakukan serangan POD perintah yang dijalankan adalah *ping 192.168.10.11 –l 65000 –t.* Ping adalah perintah untuk mengecek koneksi melalui protokol ICMP, 192.168.10.11 adalah alamat host target, -l adalah opsi ping untuk mengirim paket sebesar 65000 bytes dan –t berfungsi agar komputer mengirim paket 65000 kepada host 192.168.10.11 secara terus-menerus, perintah ini akan berhenti jika user menekan tombol *ctrl+C keyboard*.



IDS ATTACK Log Out Btn

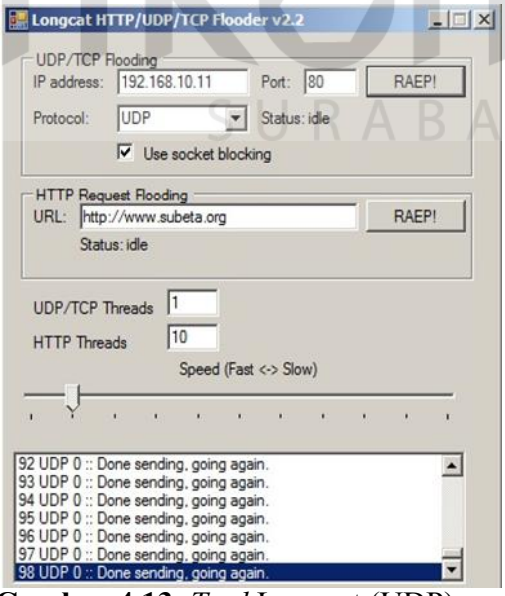
sid	cid	timestamp	ip_src	ip_dst	attack_kategori
9	1	2013-09-16 20:08:12	192.168.10.5	192.168.10.11	middle
9	6	2013-09-16 20:08:13	192.168.10.5	192.168.10.11	middle
9	11	2013-09-16 20:08:14	192.168.10.5	192.168.10.11	middle
9	16	2013-09-16 20:08:15	192.168.10.5	192.168.10.11	middle
9	21	2013-09-16 20:08:16	192.168.10.5	192.168.10.11	middle
9	26	2013-09-16 20:08:17	192.168.10.5	192.168.10.11	middle
9	31	2013-09-16 20:08:18	192.168.10.5	192.168.10.11	middle

Gambar 4.12. Hasil Web *Log* IDS

Pada Gambar 4.12 ditampilkan sebuah tabel dengan beberapa kolom data yaitu *timestamp, ip_src, ip_dst* dan *attack_kategori*. Dari tabel tersebut dapat dilihat bahwa terdapat 7 baris data *ip_src, ip_dst* dan *attack_kategori* yang sama dengan masing-masing data berisi 192.168.10.5, 192.168.10.11 dan *middle* tapi masing-masing mempunyai waktu yang berbeda. Contoh data dari baris pertama berarti host dengan alamat ip 192.168.10.15 mengirim paket pada pukul 20:08:12 tanggal 2013-09-06 dengan tujuan host 192.168.10.11, oleh sistem IDS paket ini diklasifikasikan paket serangan dengan kategori *middle.*

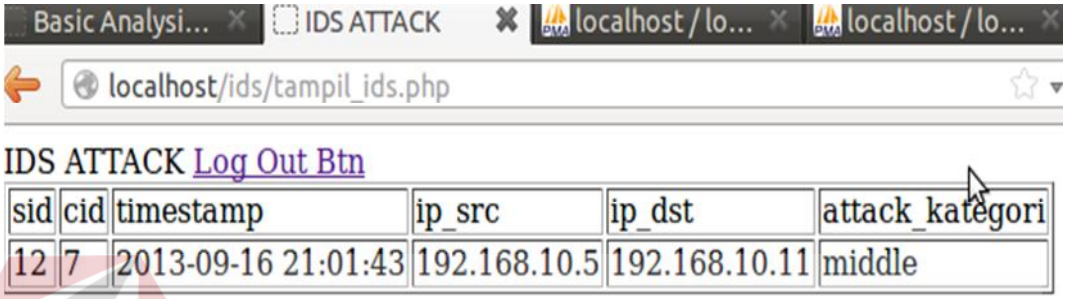
C. Hasil Pengujian UDP *Flooding*

Salah satu teknik serangan DoS UDP yaitu dengan mengirimkan paket UDP sebanyak-banyaknya ke host tujuan atau disebut UDP *flooding*, untuk melakukan serangan ini dapat dilakukan dengan memanfaatkan aplikasi Longcat seperti Gambar 4.13:



Gambar 4.13. *Tool* Longcat (UDP)

Untuk melakukan serangan *udp packet flooding* dimulai dengan mengisi alamat host target pada kolom *ip address* dan memilih protokol serangan seperti yang ditunjukkan pada Gambar 4.13. Untuk mengirim paket serangan dilakukan dengan menekan tombol *RAEP* dan untuk menghentikan pengiriman paket serangan dilakukan dengan menkean tombol STOP.

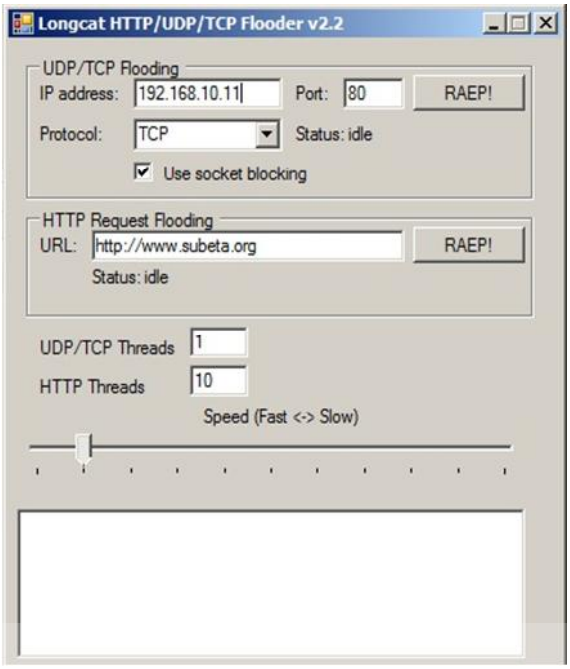


Gambar 4.14. Web Log IDS

Gambar 4.14 menunjukkan web log IDS dari hasil serangan *udp packet flooding* yang dilakukan melalui aplikasi Longcat. Dari gambar tersebut dapat dilihat web log menampilkan satu baris data dengan beberapa kolom yaitu *timestamp, ip_src, ip_dst, attack_kategori*. Dari hasil data yang ditunjukkan host dengan alamat ip 192.168.10.5 mengirim paket data pada host 192.168.10.11 pada pukul 21:01:43 tanggal 2013-09-16 diketahui mempunyai *attack_kategori middle.* Hal ini berarti bahwa host 192.168.10.5 telah melakukan percobaan serangan berskala *middle.*

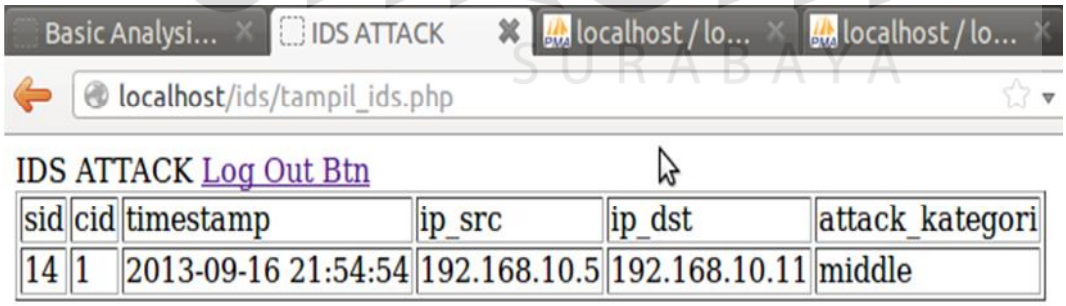
D. Hasil Pengujian TCP *Flooding*

Pengujian serangan *tcp packet flooding* dilakukan dengan menggunakan aplikasi Longcat. Serangan ini dilakukan dengan cara mengirim paket TCP sebanyak-banyaknya pada host target. Berikut ini adalah cara mengirim paket serangan TCP dengan menggunakan aplikasi Longcat, seperti yang ditunjukkan oleh Gambar 4.15.



Gambar 4.15. Tool Longcat (TCP)

Untuk memulai serangan langkah pertama yang dilakukan adalah memasukkan alamat ip target yaitu 192.168.10.11 serta protokol paket yang dikirimkan yaitu TCP pada kolom *ip address* dan *protocol* seperti yang ditunjukkan pada Gambar 4.15. Selanjutnya klik *RAEP* untuk memulai serangan dan klik *STOP* untuk menghentikan serangan.



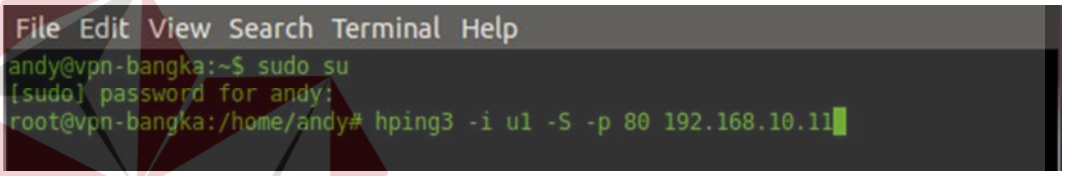
Gambar 4.16. Web Log IDS

Gambar 4.16 menunjukkan satu baris data yang berisikan data *timestamp, ip_src, ip_dst* dan *attack_kategori*. Dari web log tersebut dapat dilihat bahwa terdapat paket dari host alamat 192.168.10.5 menuju host 192.168.10.11 pada pukul

21:54:54 tanggal 2013-09-16 yang diklasifikasikan sebagai serangan skala menengah.

E. Hasil Pengujian Serangan *Syn-ACK*

Serangan *syn-ack* dilakukan dengan mengirim paket *syn* secara terus menerus menuju server untuk menghabiskan sumber daya server sehingga server tidak bisa memenuhi permintaan layanan. Serangan ini dilakukan melalui *command shell* Linux yaitu *hping3*. Berikut ini adalah serangan yang dijalankan *hping3,* seperti yang ditunjukkan pada Gambar 4.17.



Gambar 4.17. Serangan *Syn-ACK*

Gambar 4.17 adalah perintah hping3 untuk melakukan serangan *syn-ack*, serangan ack ditujukan pada alamat host 192.168.10.11 melalui port 80. Berikut ini adalah hasil web log aplikasi yang ditunjukkan oleh Gambar 4.18.

IDS ATTACK Log Out Btn

sid	cid	timestamp	ip_src	ip_dst	attack_kategori
32	1	2014-01-28 04:59:10	192.168.10.80	192.168.10.11	bukan serangan
32	3	2014-01-28 04:59:11	192.168.10.80	192.168.10.11	bukan serangan
32	8	2014-01-28 04:59:15	192.168.10.80	192.168.10.11	bukan serangan
32	11	2014-01-28 04:59:18	192.168.10.80	192.168.10.11	bukan serangan
32	17	2014-01-28 04:59:22	192.168.10.80	192.168.10.11	bukan serangan
32	19	2014-01-28 04:59:26	192.168.10.80	192.168.10.11	bukan serangan
32	23	2014-01-28 04:59:29	192.168.10.80	192.168.10.11	bukan serangan

Gambar 4.18. Web Log Serangan *Syn-ACK*

Pada Gambar 4.18 diketahui terdapat 7 paket yang berasal dari host 192.168.10.80 menuju 192.168.10.11 dengan indikasi *attack_kategori* yang sama yaitu *bukan*

serangan. Ketujuh paket yang ditunjukkan pada Gambar 4.18 dikirim pada tanggal 28-01-2014 pada rentang waktu antara 04:59:10 – 04:59:29.

F. Pengujian Akses Data HTTP

Pengujian data http dilakukan dengan mengakses salah satu *website* melalui *browser* internet, hal ini bertujuan untuk mengetahui apakah sistem dapat membedakan paket tcp serangan dan bukan serangan. Berikut salah satu *website* yang diakses:

Gambar 4.19. Akses Website Internet

Gambar 4.19 menunjukkan salah satu *website* yang diakses melalui *browser* internet. Dari gambar tersebut didapatkan hasil weblog sebagai berikut.

IDS ATTACK Log Out Btn

sid	cid	timestamp	ip_src	ip_dst	attack_kategori
33	1	2014-01-28 05:10:22	202.80.220.100	192.168.10.11	middle

Gambar 4.20. Web Log Data HTTP

Gambar 4.20 menunjukkan bahwa terdapat satu paket data yang berasal dari host 202.80.220.100 menuju host 192.168.10.11 pada tanggal 28-01-2014 pada jam 05:10:22 yang dikategorikan sebagai *attack_kategori middle.*

4.3 Pengujian Data Fuzzy

Data yang diterima dan telah diolah oleh sistem IDS perlu diuji apakah data tersebut sesuai dengan perhitungan secara manual. Pada pengujian ini akan disajikan kedalam dua tabel antara tabel database dan tabel perhitungan manual.

4.3.1 Tujuan

Tujuan utama yang dilakukan adalah untuk mengetahui seberapa akurat perhitungan data menurut metode fuzzy yang dilakukan oleh sistem IDS.

4.3.2 Alat Pengujian

Berikut adalah beberapa alat yang digunakan:

1. PC Router
2. PC Client
3. Switch
4. Kabel UTP
5. Tools DoS Longcat
6. Command Prompt Windows
7. Command Shell Linux
8. Browser Internet

4.3.3 Prosedur Pengujian

Berikut beberapa tahap-tahap prosedur pengujian:

1. Menghidupkan PC Router
2. Menghidupkan PC Client

3. Menyambungkan masing-masing kabel UTP PC Router dan PC Client ke switch
4. Menjalankan *service* snort pada PC Router
5. Memulai serangan dengan menggunakan DoS tools yang sudah ada

4.3.4 Hasil Pengujian

A. Data Fuzzy Paket Normal

Dari pengiriman paket ICMP yang telah dilakukan didapatkan hasil database sebagai berikut:

timestamp	ip_src	ip_dst	frekuensi	iplen	ip_proto	alphaflow	alphafmid	alphafhigh	alphallow
2013-09-17 04:13:24	192.168.10.5	192.168.10.11	3	60	0	1	0	0	0
2013-09-17 04:13:25	192.168.10.5	192.168.10.11	3	60	0	1	0	0	0
2013-09-17 04:13:26	192.168.10.5	192.168.10.11	3	60	0	1	0	0	0
2013-09-17 04:13:27	192.168.10.5	192.168.10.11	3	60	0	1	0	0	0

Gambar 4.21. Database Sistem IDS 1

Dimana:

alphaflow : nilai alpha frekuensi ip src kategori low

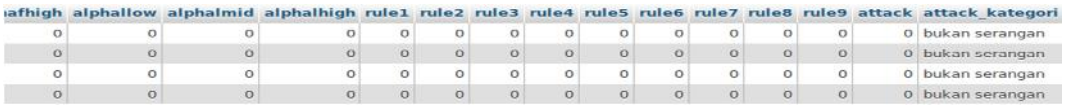
alphafmid : nilai alpha frekuensi ip src kategori middle

alphafhigh : nilai alpha frekuensi ip src kategori high

alphahllow : nilai alpha length ip src kategori low

Gambar 4.21 merupakan hasil pengolahan database paket normal oleh sistem IDS. Dalam Gambar 4.21 host 192.168.10.5 mempunyai data *frekuensi, iplen, alphaflow, alphafmid, alphafhigh, alphallow* dimana nilai dari *alphaflow, alphafmid, alphafhigh* dan *alphallow* didapatkan dari hasil pengolahan data fuzzy. Gambar 4.22 merupakan lanjutan dari hasil database pada gambar 4.21, pada Gambar 4.22 terdapat kolom *alphalmid, alphalhigh, rule1, rule2, rule3, rule4,*

rule5, rule6, rule7, rule8, rule9, attack dan attack_kategori. Nilai dari masing-masing kolom tersebut diperoleh dari hasil perhitungan fuzzy.



afhigh	alphallow	alphalmid	alphalhigh	rule1	rule2	rule3	rule4	rule5	rule6	rule7	rule8	rule9	attack	attack_kategori
0	0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan

Gambar 4.22. Database Sistem IDS 2

Dimana :

alphalmid : nilai alpha length ip src kategori middle

alphalhigh : nilai alpha length ip src kategori high

rule1 : nilai rule 1 fuzzy

rule2 : nilai rule 2 fuzzy

rule3 : nilai rule 3 fuzzy

rule4 : nilai rule 4 fuzzy

rule5 : nilai rule 5 fuzzy

rule6 : nilai rule 6 fuzzy

rule7 : nilai rule 7 fuzzy

rule8 : nilai rule 8 fuzzy

rule9 : nilai rule 9 fuzzy

attack : nilai z fuzzy atau nilai defuzzyfikasi

Nilai frekuensi dan iplen didapatkan dari hasil perhitungan jumlah ip_src dan ip_len dalam satu detik dari tabel ip_hdr pada database snort. Tabel 4.1 merupakan hasil perhitungan fuzzyfikasi secara manual.

Tabel 4.1. Fuzzyfikasi Paket Normal

IP SRC	Frekuensi	IP Len	alphaf low	alphaf mid	Alphafhigh	alphallow	alphalmid
192.168.10.5	3	60	1	0	0	0	0
192.168.10.5	3	60	1	0	0	0	0
192.168.10.5	3	60	1	0	0	0	0
192.168.10.5	3	60	1	0	0	0	0

Tabel 4.1 menunjukkan nilai fuzzyfikasi paket normal yang dihitung secara manual. Nilai 1 menunjukkan bahwa ip src menjadi anggota dalam kategori frekuensi low sedangkan nilai 0 menunjukkan bahwa ip src bukan anggota dalam kategori frekuensi middle, frekuensi high, length low, length middle dan length high.

Tabel 4.2. Fuzzyfikasi Paket Normal (lanjutan)

Alpha lhigh	rule 1	rule 2	rule 3	rule 4	rule 5	rule 6	rule 7	rule 8	rule 9	Attack	attack_kategori
0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	bukan serangan

Tabel 4.2 menunjukkan nilai rule1 sampai nilai rule 9 adalah 0 sehingga nilai defuzzyfikasi serangan (attack) adalah 0. Nilai defuzzyfikasi 0 dikategorikan sebagai bukan serangan.

B. Data Fuzzy Paket POD

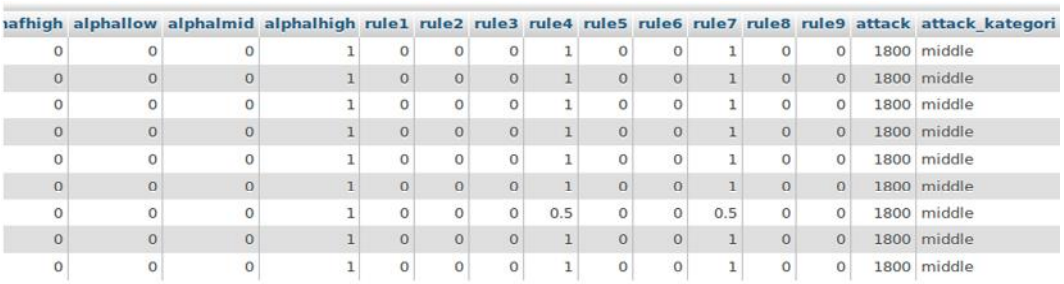
Adapung hasil database dari serangan *ping of death* yang telah ditunjukkan pada Gambar 4.11 adalah sebagai berikut:

timestamp	ip_src	ip_dst	frekuensi	iplen	ip_proto	alphaflow	alphafmid	alphafhigh	alphallow
2013-09-17 04:19:42	192.168.10.5	192.168.10.11	5	65028	0	1	0	0	0
2013-09-17 04:19:43	192.168.10.5	192.168.10.11	5	65028	0	1	0	0	0
2013-09-17 04:19:44	192.168.10.5	192.168.10.11	5	65028	0	1	0	0	0
2013-09-17 04:19:45	192.168.10.5	192.168.10.11	5	65028	0	1	0	0	0
2013-09-17 04:19:46	192.168.10.5	192.168.10.11	5	65028	0	1	0	0	0
2013-09-17 04:19:47	192.168.10.5	192.168.10.11	5	65028	0	1	0	0	0
2013-09-17 04:19:48	192.168.10.5	192.168.10.11	7	1500	0	0.5	0.5	0	0
2013-09-17 04:19:49	192.168.10.5	192.168.10.11	5	65028	0	1	0	0	0
2013-09-17 04:19:50	192.168.10.5	192.168.10.11	5	65028	0	1	0	0	0

Gambar 4.23. Database Sistem IDS

Pada Gambar 4.23 terdapat 2 perbedaan nilai alpha hal ini dipengaruhi oleh perbedaan nilai frekuensi dan iplen. Untuk ip src dengan frekuensi 5 dan iplen

65028 nilai 1 terdapat pada alphaflow sedangkan nilai alpha lainnya adalah 0. Untuk ip src dengan frekuensi 7 dan iplen 65028 nilai alphaflow dan alphafmid adalah 0.5 sedangkan nilai alpha lainnya adalah 0.



afhigh	alphallow	alphalmid	alphalhigh	rule1	rule2	rule3	rule4	rule5	rule6	rule7	rule8	rule9	attack	attack_kategori
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle
0	0	0	1	0	0	0	0.5	0	0	0.5	0	0	1800	middle
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle

Gambar 4.24. Database Sistem IDS (Lanjutan dari gambar 4.23)

Gambar 4.24 menunjukkan ip src mempunyai nilai alpha yang sama meskipun terdapat nilai frekuensi dan iplen berbeda. IP src dengan frekuensi 5 dan iplen 65028 mempunyai nilai 1 pada rule4 dan rule7 sehingga nilai defuzzyfikasi yang diperoleh adalah 1800. Nilai defuzzyfikasi ini dikategorikan dalam kategori serangan *middle*. IP src dengan nilai frekuensi 7 dan iplen 1500 mempunyai nilai 0.5 pada rule4 dan rule7 sehingga nilai defuzzyfikasi serangan adalah 1800 dengan kategori serangan *middle*.

Tabel 4.3. Fuzzyfikasi Paket POD

IP SRC	Frekuensi	IP Len	Alpha flow	alphaf mid	alphaf high	alphal low	alphal mid
192.168.10.5	5	65028	1	0	0	0	0
192.168.10.5	5	65028	1	0	0	0	0
192.168.10.5	5	65028	1	0	0	0	0
192.168.10.5	5	65028	1	0	0	0	0
192.168.10.5	5	65028	1	0	0	0	0
192.168.10.5	5	65028	1	0	0	0	0
192.168.10.5	7	1500	1	0	0	0	0
192.168.10.5	5	65028	1	0	0	0	0
192.168.10.5	5	65028	1	0	0	0	0

Tabel 4.3 menjelaskan ip src 192.168.10.5 merupakan anggota dari kategori himpunan frekuensi low, hal ini ditunjukkan melalui nilai 1 pada alphaflow.

Tabel 4.4 dibawah ini menjelaskan bahwa ip src 192.168.10.5 merupakan anggota dari himpunan length high, hal ini ditunjukkan melalui nilai 1 pada alphalhigh. Dari nilai-nilai alpha frekuensi dan length diperoleh nilai 1 pada rule4 dan rule7, sehingga nilai defuzzyfikasi attack adalah 1800 dengan kategori serangan adalah *middle.*

Tabel 4.4. Fuzzyfikasi Paket POD (Lanjutan)

alpha lhigh	rule 1	rule 2	rule 3	rule 4	rule 6		rule 7	rule 8	rule 9	attack	attack_ kategori
1	0	0	0	1	0	0	1	0	0	1800	Middle
1	0	0	0	1	0	0	1	0	0	1800	Middle
1	0	0	0	1	0	0	1	0	0	1800	Middle
1	0	0	0	1	0	0	1	0	0	1800	Middle
1	0	0	0	1	0	0	1	0	0	1800	Middle
1	0	0	0	1	0	0	1	0	0	1800	middle
1	0	0	0	0.5	0	0	0.5	0	0	1800	middle
1	0	0	0	1	0	0	1	0	0	1800	middle
1	0	0	0	1	0	0	1	0	0	1800	middle

C. Data Fuzzy Paket TCP Flooding

Adapung hasil database dari serangan *tcp packet flooding* yang telah ditunjukkan pada Gambar 4.15 adalah sebagai berikut:

timestamp	ip_src	ip_dst	frekuensi	iplen	ip_proto	alphaflow	alphafmid	alphafhigh	alphallow	alphalm
2013-09-16 21:54:54	3232238085	3232238091	1	668	0	1	0	0	0	

Gambar 4.25. Database Sistem IDS

Dari gambar 4.25 diketahui nilai alpha frekuensi dan length. IP src 192.168.10.5 mempunyai frekuensi 1 dan iplen 668 sehingga diperoleh nilai alphaflow = 1, alphafmid = 0, alphafhigh = 0, dan alphallow = 0. Dari nilai-nilai alpha tersebut menunjukkan bahwa ip src 192.168.10.15 merupakan anggota dari himpunan frekuensi low.

hafhigh	alphallow	alphalmid	alphalhigh	rule1	rule2	rule3	rule4	rule5	rule6	rule7	rule8	rule9	attack	attack_kategori
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle

Gambar 4.26. Database Sistem IDS (Lanjutan gambar 4.25)

Pada Gambar 4.26 nilai alphalmid = 0 dan alphalhigh = 1. Nilai tersebut menunjukkan bahwa ip src 192.168.10.5 merupakan anggota himpunan length high. Dari nilai alpha tersebut diperoleh nilai 1 pada rule 4 dan rule 7 sehingga nilai defuzzyfikasi serangan yang didapatkan adalah 1800 dengan kategori serangan *middle.*

Tabel 4.5. Fuzzyfikasi Paket TCP Flooding

IP SRC	Frekuensi	IP Len	alpha flow	Alphaf mid	alpha fhigh	Alpha llow	alphal mid
192.168.10.5	1	668	0	1	0	0	0

Tabel 4.5 menunjukkan data yang diperoleh secara manual. Nilai ip src 192.168.10.5 mempunyai frekuensi 1 dan iplen 668 merupakan anggota himpunan alphafmid, hal ini ditunjukkan oleh nilai 1 pada alphafmid. Tabel 4.6 menunjukkan ip src 192.168.10.5 merupakan anggota dari himpunan alphalhigh. Dari nilai alpha tersebut diperoleh nilai 1 pada rule 1 dan 7 sehingga nilai defuzzyfikasi serangan yang diperoleh adalah 1800 dengan kategori serangan *middle.*

Tabel 4.6. Fuzzyfikasi Paket TCP Flooding (Lanjutan)

Alphal high	rule 1	rule 2	rule 3	rule 4	rule 5	rule 6	rule 7	rule 8	rule 9	Atta ck	attack _kateg ori
1	0	0	0	1	0	0	1	0	0	1800	middle

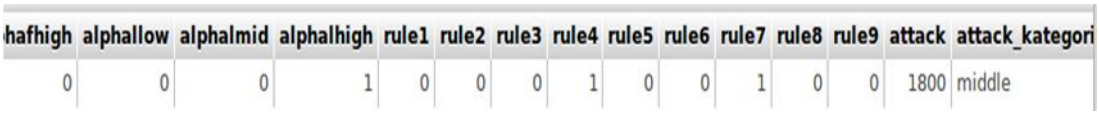
D. Data Fuzzy Paket UDP Flooding

Adapun hasil database dari serangan *udp packet flooding* yang telah ditunjukkan pada Gambar 4.13 adalah sebagai berikut:

timestamp	ip_src	ip_dst	frekuensi	iplen	ip_proto	alphaflow	alphafmid	alphafhigh	alphallow
2013-09-17 04:24:00	192.168.10.5	192.168.10.11	0	1500	0	1	0	0	0

Gambar 4.27. Database Sistem IDS

Pada Gambar 4.27 menunjukkan bahwa ip src 192.168.10.5 merupakan anggota himpunan frekuensi low. Gambar 4.28 menunjukkan ip src juga termasuk anggota himpunan frekuensi high. Dari alpha tersebut diperoleh nilai rule4 dan rule7 adalah 1 sehingga didapatkan defuzzyfikasi serangan adalah 1800 dengan kategori serangan adalah *middle.*



hafhigh	alphallow	alphalmid	alphalhigh	rule1	rule2	rule3	rule4	rule5	rule6	rule7	rule8	rule9	attack	attack_kategori
0	0	0	1	0	0	0	1	0	0	1	0	0	1800	middle

Gambar 4.28. Database Sistem IDS (Lanjutan dari gambar 4.23)

Tabel 4.7. Fuzzyfikasi paket UDP Flooding

IP SRC	Frekuensi	IP Len	alpha flow	Alphaf mid	alphaf high	Alpha llow	alphal mid
192.168.10.5	0	1500	1	0	0	0	0

Tabel 4.7 menunjukkan perhitungan manual dengan hasil frekuensi = 0 dan iplen = 1500. Dari Tabel 4.7 juga ditunjukkan bahwa ip src 192.168.10.5 merupakan anggota dari himmpunan frekuensi low dan himpunan length high yang ditunjukkan oleh Tabel 4.8. Dari nilai alpha yang didapatkan diperoleh nilai 1 pada rule 4 dan 7 sehingga nilai defuzzyfikasi serangan yang diperoleh adalah 1800 dengan kategori serangan *middle*.

Tabel 4.8. Fuzzyfikasi paket UDP Flooding (Lanjutan)

Alpha lhigh	rule1	rule 2	rule 3	rule 4	rule 5	rule 6	rule 7	rule 8	rule 9	attac k	attack_k ategori
1	0	0	0	1	0	0	1	0	0	1800	Middle

E. Data Fuzzy Paket *Syn-ACK*

Berikut ini adalah data fuzzy serangan *syn-ack* yang telah ditunjukkan pada Gambar 4.29.

sid	cid	id	timestamp	ip_src	ip_dst	frekuensi	iplen	ip_proto	alphaflow	alphafmid	alphafhigh
32	1	1	2014-01-28 04:59:10	3232238160	3232238091	2	40	0	1	0	0
32	3	3	2014-01-28 04:59:11	3232238160	3232238091	4	40	0	1	0	0
32	7	7	2014-01-28 04:59:15	3232238091	3232238160	4	40	0	1	0	0
32	11	11	2014-01-28 04:59:18	3232238160	3232238091	5	40	0	1	0	0
32	16	16	2014-01-28 04:59:19	3232238091	3232238160	1	40	0	1	0	0
32	17	17	2014-01-28 04:59:22	3232238160	3232238091	2	40	0	1	0	0
32	19	19	2014-01-28 04:59:26	3232238160	3232238091	4	40	0	1	0	0
32	23	23	2014-01-28 04:59:29	3232238160	3232238091	2	40	0	1	0	0

Gambar 4.29. Data Tabel Fuzzy Serangan *Syn-Ack*

Gambar 4.29 menunjukkan data dari *ip_src* 3232238160 mempunyai *frekuensi* paket sebanyak satu per satu detik dengan panjang paket sebanyak 40 Byte dengan nilai alphaflow = 1, alplhafmid dan alphafhigh = 0.

alphallow	alphalmid	alphalhigh	rule1	rule2	rule3	rule4	rule5	rule6	rule7	rule8	rule9	attack	attack_kategori
0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan
0	0	0	0	0	0	0	0	0	0	0	0	0	bukan serangan

Gambar 4.30. Data Fuzzy Serangan *Syn-Ack* (Lanjutan Gambar 4.29)

Gambar 4.30 menunjukkan nilai *alphallow =0, alphalmid=0, alphalhigh=1* dan sembilan nilai rule yang mempunyai nilai 0 serta nilai *attack = 170* dan *attack_kategori = middle.* Hal ini menunjukkan bahwa paket 3232238160 mempunyai nilai defuzyfikasi 1760 dengan kategori serangan *middle.*

F. Data Fuzzy HTTP

Dari akses *website* yang dilakukan seperti pada Gambar 4.19 didapatkan data fuzzy yang ditunjukkan dalam sebuah tabel database pada Gambar 4.31.

sid	cid	id	timestamp	ip_src	ip_dst	frekuensi	iplen	ip_proto	alphaflow	alphafmid	alphafhigh
33	1	1	2014-01-28 05:10:22	3394296932	3232238091	1	1440	0	1	0	0

Gambar 4.31. Tabel Fuzzy Data HTTP

Gambar 4.31 menunjukkan data dari *ip_src* 3394296932 mempunyai *frekuensi* paket sebanyak satu per satu detik dengan panjang paket sebanyak 1440 Byte dengan nilai alphaflow = 1, alplhafmid dan alphafhigh = 0.

alphallow	alphalmid	alphalhigh	rule1	rule2	rule3	rule4	rule5	rule6	rule7	rule8	rule9	attack	attack_kategori
0	0	1	0	0	0	0	0	0	1	0	0	1760	middle

Gambar 4.32. Tabel Fuzzy Data HTTP (Lanjutan gambar 4.31)

Gambar 4.32 menunjukkan nilai *alphallow =0, alphalmid=0, alphalhigh=1* dan hanya *rule7* yang mempunyai nilai 1 serta nilai *attack = 170* dan *attack_kategori = middle.* Hal ini menunjukkan bahwa paket 3394296932 mempunyai nilai defuzyfikasi 1760 dengan kategori serangan *middle.*

4.4 Analisis Sistem

4.4.1 Pendeteksian Paket Normal

Dari hasil pengujian pada Gambar 4.10 ditunjukkan sistem IDS dapat mengklasifikasikan paket ping koneksi biasa sebagai kedalam kategori bukan serangan. Hal ini menunjukkan bahwa sistem IDS sudah dapat membedakan mana paket serangan dan bukan serangan dengan baik. Pada Gambar 4.9 host 192.168.10.5 mengirim 4 paket data dan oleh pc router atau host 192.168.10.11 4 paket data tersebut diklasifikasian dalam kategori bukan serangan.

Dari hasil perbandingan nilai perhitungan fuzzy yang dilakukan oleh sistem IDS dan manual menunjukkan bahwa nilai fuzzy yang terdapat dalam database IDS adalah sama. Dari tabel database pada Gambar 4.17 nilai frekuensi yang didapat adalah 3 dan iplen adalah 60. Nilai frekuensi termasuk dalam himpunan frekuensi low sebab mempunyai nilai alpha frekuensi low=1. Sedangkan iplen dengan nilai 60 juga bukan bagian dari anggota himpunan fuzzy length low, mid dan high dengan nilai alpha length = 0.

Dengan menggunakan operator *and* pada setiap aturan fuzzy membuat nilai setiap aturan adalah 0 karena operator *and* membandingkan nilai minimal dari 2 himpunan kategori frekuensi dan length. Berikut perhitungan defuzzyfikasi serangan:

Rule 1 : min (alphafhigh;alphalhigh)

: min (0;0) = 0

attack = high

Rule 2 : min (alphafhigh;alphalmid)

: min (0;0) = 0

attack = high

Rule 3 : min (alphafhigh;alphallow)

: min (0;0) = 0

attack = high

Rule 4 : min (alphafmid;alphalhigh)

: min (0;0) = 0

attack = high

Rule 5 : min (alphafmid;alphalmid)

: min (0;0) = 0

attack = middle

Rule 6 : min (alphafmid;alphallow)

: min (0;0) = 0

attack = middle

Rule 7 : min (alphaflow;alphalhigh)

: min (1;0) = 0

attack = middle

Rule 8 : min (alphaflow;alphalmid)

: min (1;0) = 0

attack = middle

Rule 9 : min (alphaflow;alphallow)

: min (1;0) = 0

attack = low

dimana : attack low = 760

attack middle =1200

attack high =2400

nilai kategori attack diperoleh dari perkalian batas bawah himpunan 2 kategori.

Dari nilai rule diatas diperoleh nilai defuzzyfikasi serangan:

attack = rule 1 * 2400 + rule 2 * 2400 + rule 3 * 2400 + rule 4 * 2400 + rule 5 * 1200 + rule 6 * 1200 + rule 7 * 1200 + rule 8 * 1200 + rule 9 * 760 / (rule 1 + rule 2 + rule 3 + rule 4 + rule 5 + rule 6 + rule 7 + rule 8 + rule 9)

=0 * 2400 +0 * 2400 + 0 * 2400 + 0 * 2400 + 0 * 1200 + 0 * 1200 + 0 * 1200 + 0 * 1200 + 0 * 760 / (0)

=0 / 0= *0*

Dengan didapatkan nilai defuzzyfikasi = *0* membuat nilai attack termasuk kedalam kategori bukan serangan.

4.4.2 Pendeteksian Serangan Paket PoD

Berdasarkan hasil serangan yang ditunjukkan oleh Gambar 4.12 sistem IDS dapat mendeteksi serangan paket PoD. Pada web log terdapat 7 baris data yang menunjukkan adanya serangan kategori middle dari host 192.168.10.5 pada pukul 20:18 tanggal 2013-09-16. Data fuzzy yang diperoleh sistem IDS juga menunjukkan kesesuaian dengan penghitungan manual seperti yang terlihat dari Gambar 4.19 dan 4.20 dengan Tabel 4.3 dan Tabel 4.4. Dari perbandingan pengujian data fuzzy sistem IDS dan data fuzzy sistem manual (Gambar 4.18 dan 4.19 dengan Tabel 4.3 dan 4.4) dapat dilihat bahwa data fuzzy yang diperoleh adalah sama sehingga keakuratan hasil web log sistem IDS dapat dibuktikan.

Dari Gambar 4.19 diketahui frekuensi serangan per detik = 5 dengan iplen = 65028. Nilai frekuensi tersebut termasuk kedalam anggota himpunan frekuensi low karena mempunyai nilai alpha frekuensi low = 1 sedangkan iplen termasuk kedalam anggota himpunan length high. Berikut ini adalah perhitungan defuzzyfikasi serangan:

Rule 1 : min (alphafhigh;alphalhigh)

: min (0;1) = 0

attack = high

Rule 2 : min (alphafhigh;alphalmid)

: min (0;0) = 0

attack = high

Rule 3 : min (alphafhigh;alphallow)

: min (0;0) = 0

attack = high

Rule 4 : min (alphafmid;alphalhigh)

: min (0;1) = 0

attack = high

Rule 5 : min (alphafmid;alphalmid)

: min (0;0) = 0

attack = middle

Rule 6 : min (alphafmid;alphallow)

: min (0;0) = 0

attack = middle

Rule 7 : min (alphaflow;alphalhigh)

: min (1;1) = 1

attack = middle

Rule 8 : min (alphaflow;alphalhigh)

: min (1;0) = 0

attack = middle

Rule 9 : min (alphaflow;alphallow)

: min (1;0) = 0

attack = low

Dari nilai rule diatas diperoleh nilai defuzzyfikasi serangan:

attack = rule 1 * 2400 + rule 2 * 2400 + rule 3 * 2400 + rule 4 * 2400 + rule 5 * 1760 + rule 6 * 1760 + rule 7 * 1760 + rule 8 * 1760 + rule 9 * 1200 / (rule 1 + rule 2 + rule 3 + rule 4 + rule 5 + rule 6 + rule 7 + rule 8 + rule 9)

=0 * 2400 +0 * 2400 + 0 * 2400 + 0 * 2400 + 0 * 1760 + 0 * 1760 + 1 * 1760 + 0 * 1760 + 0 * 760 / (1)

=1760 / 1= 1760

Dengan didapatkan nilai defuzzyfikasi = 1760 membuat nilai *attack* termasuk kedalam kategori serangan *middle.*

4.4.3 Pendeteksian Serangan Paket UDP Flooding

Berdasarkan hasil pengujian yang diperlihatkan melalui Gambar 4.14 dapat dilihat sistem IDS dapat mendeteksi serangan paket UDP Flooding (serangan dapat dilihat pada Gambar 4.13). Pada web log tersebut terlihat satu baris data menunjukkan adanya paket serangan kategori *middle* yang dilakukan oleh host 192.168.10.5 pada pukul 21:01 tanggal 2013-09-16. Dari perbandingan pengujian data fuzzy sistem IDS dengan data fuzzy sistem manual (Gambar 4.27 dan 4.28 dengan Tabel 4.7 dan 4.8) dapat dilihat bahwa data fuzzy yang diperoleh adalah akurat.

Dari Gambar 4.23 diketahui frekuensi serangan per detik = 0 dengan iplen = 1500. Nilai frekuensi tersebut termasuk kedalam anggota himpunan frekuensi low karena mempunyai nilai alpha frekuensi low = 1 sedangkan iplen termasuk kedalam anggota himpunan length high dengan alpha length high = 1. Berikut ini adalah perhitungan defuzzyfikasi serangan:

Rule 1 : min (alphafhigh;alphalhigh)

: min (0;1) = 0

attack = high

Rule 2 : min (alphafhigh;alphalmid)

: min (0;0) = 0

attack = high

Rule 3 : min (alphafhigh;alphallow)

: min (0;0) = 0

attack = high

Rule 4 : min (alphafmid;alphalhigh)

: min (0;1) = 0

attack = high

Rule 5 : min (alphafmid;alphalmid)

: min (0;0) = 0

attack = middle

Rule 6 : min (alphafmid;alphallow)

: min (0;0) = 0

attack = middle

Rule 7 : min (alphaflow;alphalhigh)

: min (1;1) = 1

attack = middle

Rule 8 : min (alphaflow;alphalmid)

: min (1;0) = 0

attack = middle

Rule 9 : min (alphaflow;alphallow)

: min (1;0) = 0

attack = low

Dari nilai rule diatas diperoleh nilai defuzzyfikasi serangan:

attack = rule 1 * 2400 + rule 2 * 2400 + rule 3 * 2400 + rule 4 * 2400 + rule 5 * 1760 + rule 6 * 1760 + rule 7 * 1760 + rule 8 * 1760 + rule 9 * 1200 / (rule 1 + rule 2 + rule 3 + rule 4 + rule 5 + rule 6 + rule 7 + rule 8 + rule 9)

=0 * 2400 +0 * 2400 + 0 * 2400 + 0 * 2400 + 0 * 1760 + 0 * 1760 + 1 * 1760 + 0 * 1760 + 0 * 1200 / (1)

=1760/ 1= 1760

Dengan didapatkan nilai defuzzyfikasi = 1760 membuat nilai attack termasuk kedalam kategori serangan *middle.*

.

4.4.4 Pendeteksian Serangan Paket TCP Flooding

Berdasarkan hasil pengujian yang diperlihatkan melalui Gambar 4.16 dapat dilihat sistem IDS dapat mendeteksi serangan paket TCP Flooding (serangan dapat dilihat dari Gambar 4.15). Pada web log tersebut terlihat satu baris data menunjukkan adanya paket serangan kategori *middle* yang dilakukan oleh host 192.168.10.5 pada pukul 21:54 tanggal 2013-09-16.Dari perbandingan pengujian data fuzzy sistem IDS dengan data fuzzy sistem manual (Gambar 4.21 dan 4.22 dengan Tabel 4.5 dan 4.6) dapat dilihat bahwa data fuzzy yang diperoleh akurat.

Dari Gambar 4.25 diketahui frekuensi serangan per detik = 1 dengan iplen = 668. Nilai frekuensi tersebut termasuk kedalam anggota himpunan frekuensi low karena mempunyai nilai alpha frekuensi low = 1 sedangkan iplen termasuk kedalam anggota himpunan length high. Berikut ini adalah perhitungan defuzzyfikasi serangan:

Rule 1 : min (alphafhigh;alphalhigh)

: min (0;1) = 0

attack = high

Rule 2 : min (alphafhigh;alphalmid)

: min (0;0) = 0

attack = high

Rule 3 : min (alphafhigh;alphallow)

: min (0;0) = 0

attack = high

Rule 4 : min (alphafmid;alphalhigh)

: min (0;1) = 0

attack = high

Rule 5 : min (alphafmid;alphalmid)

: min (0;0) = 0

attack = middle

Rule 6 : min (alphafmid;alphallow)

: min (0;0) = 0

attack = middle

Rule 7 : min (alphaflow;alphalhigh)

: min (0;1) = 1

attack = middle

Rule 8 : min (alphaflow;alphalmid)

: min (1;1) = 0

attack = middle

Rule 9 : min (alphaflow;alphallow)

: min (1;0) = 0

attack = low

Dari nilai rule diatas diperoleh nilai defuzzyfikasi serangan:

attack = rule 1 * 2400 + rule 2 * 2400 + rule 3 * 2400 + rule 4 * 2400 + rule 5 * 1760 + rule 6 * 1760 + rule 7 * 1760 + rule 8 * 1760 + rule 9 * 1200 / (rule 1 + rule 2 + rule 3 + rule 4 + rule 5 + rule 6 + rule 7 + rule 8 + rule 9)

=0 * 2400 +0 * 2400 + 0 * 2400 + 0 * 2400 + 0 * 1760 + 0 * 1760 + 1 * 1760 + 0 * 1760 + 0 * 1760 / (1)

=1760 / 1= 1760

Dengan didapatkan nilai defuzzyfikasi = 1760 membuat nilai *attack* termasuk kedalam kategori serangan *middle*

4.4.5 Pendeteksian Paket Serangan *Syn-ACK*

Berdasarkan hasil pengujian yang ditunjukkan oleh web log pada Gambar 4.18 aplikasi yang dibangun masih belum mampu mendeteksi paket *syn-ack* sebagai serangan. Hal ini dikarenakan nilai variabel frekuensi paket yang dikirim adalah 40 Byte. Nilai ini lebih kecil dari nilai paket ping normal yaitu 60 Byte,

sehingga jika dimasukkan dalam aturan-aturan fuzzy dan fungsi implikasi nilai paket serangan *syn-ack* tidak termasuk serangan kategori *low, middle* dan *high.*Berikut ini adalah nilai perhitungan defuzyfikasi paket serangan:

Rule 1 : min (alphafhigh;alphalhigh)

: min (0;0) = 0

attack = high

Rule 2 : min (alphafhigh;alphalmid)

: min (0;0) = 0

attack = high

Rule 3 : min (alphafhigh;alphallow)

: min (0;0) = 0

attack = high

Rule 4 : min (alphafmid;alphalhigh)

: min (0;0) = 0

attack = high

Rule 5 : min (alphafmid;alphalmid)

: min (0;0) = 0

attack = middle

Rule 6 : min (alphafmid;alphallow)

: min (0;0) = 0

attack = middle

Rule 7 : min (alphaflow;alphalhigh)

: min (1;0) = 0

attack = middle

Rule 8 : min (alphaflow;alphalmid)

: min (1;0) = 0

attack = middle

Rule 9 : min (alphaflow;alphallow)

: min (1;0) = 0

attack = low

attack = rule 1 * 2400 + rule 2 * 2400 + rule 3 * 2400 + rule 4 * 2400 + rule 5 * 1200 + rule 6 * 1200 + rule 7 * 1200 + rule 8 * 1200 + rule 9 * 760 / (rule 1 + rule 2 + rule 3 + rule 4 + rule 5 + rule 6 + rule 7 + rule 8 + rule 9)

=0 * 2400 +0 * 2400 + 0 * 2400 + 0 * 2400 + 0 * 1200 + 0 * 1200 + 0 * 1200 + 0 * 1200 + 0 * 760 / (0)

=0 / 0= *0*

Dengan didapatkan nilai defuzzyfikasi = *0* membuat nilai attack termasuk kedalam kategori bukan serangan.

4.4.6 Pendeteksian Paket HTTP

Berdasarkan hasil pengujian yang ditunjukkan oleh web log pada Gambar 4.20 aplikasi yang dibangun masih belum mampu mendeteksi paket http sebagai paket bukan serangan. Hal ini dikarenakan nilai variabel frekuensi paket yang dikirim adalah 1440 Byte. Nilai ini termasuk dalam variabel *length* kategori *high* yaitu lebih dari 240 Byte , sehingga jika dimasukkan dalam aturan-aturan fuzzy dan fungsi implikasi nilai paket http tidak termasuk serangan kategori *low, middle* dan *high.*Berikut ini adalah nilai perhitungan defuzyfikasi paket serangan:

Rule 1 : min (alphafhigh;alphalhigh)

: min (0;1) = 0

attack = high

Rule 2 : min (alphafhigh;alphalmid)

: min (0;0) = 0

attack = high

Rule 3 : min (alphafhigh;alphallow)

: min (0;0) = 0

attack = high

Rule 4 : min (alphafmid;alphalhigh)

: min (0;1) = 0

attack = high

Rule 5 : min (alphafmid;alphalmid)

: min (0;0) = 0

attack = middle

Rule 6 : min (alphafmid;alphallow)

: min (0;0) = 0

attack = middle

Rule 7 : min (alphaflow;alphalhigh)

: min (0;1) = 1

attack = middle

Rule 8 : min (alphaflow;alphalmid)

: min (1;1) = 0

attack = middle

Rule 9 : min (alphaflow;alphallow)

: min (1;0) = 0

attack = low

Dari nilai rule diatas diperoleh nilai defuzzyfikasi serangan:

attack = rule 1 * 2400 + rule 2 * 2400 + rule 3 * 2400 + rule 4 * 2400 + rule 5 * 1760 + rule 6 * 1760 + rule 7 * 1760 + rule 8 * 1760 + rule 9 * 1200 / (rule 1 + rule 2 + rule 3 + rule 4 + rule 5 + rule 6 + rule 7 + rule 8 + rule 9)

=0 * 2400 +0 * 2400 + 0 * 2400 + 0 * 2400 + 0 * 1760 + 0 * 1760 + 1 * 1760 + 0 * 1760 + 0 * 1760 / (1)

=1760 / 1= 1760

Dengan didapatkan nilai defuzzyfikasi = 1760 membuat nilai *attack* termasuk kedalam kategori serangan *middle.*