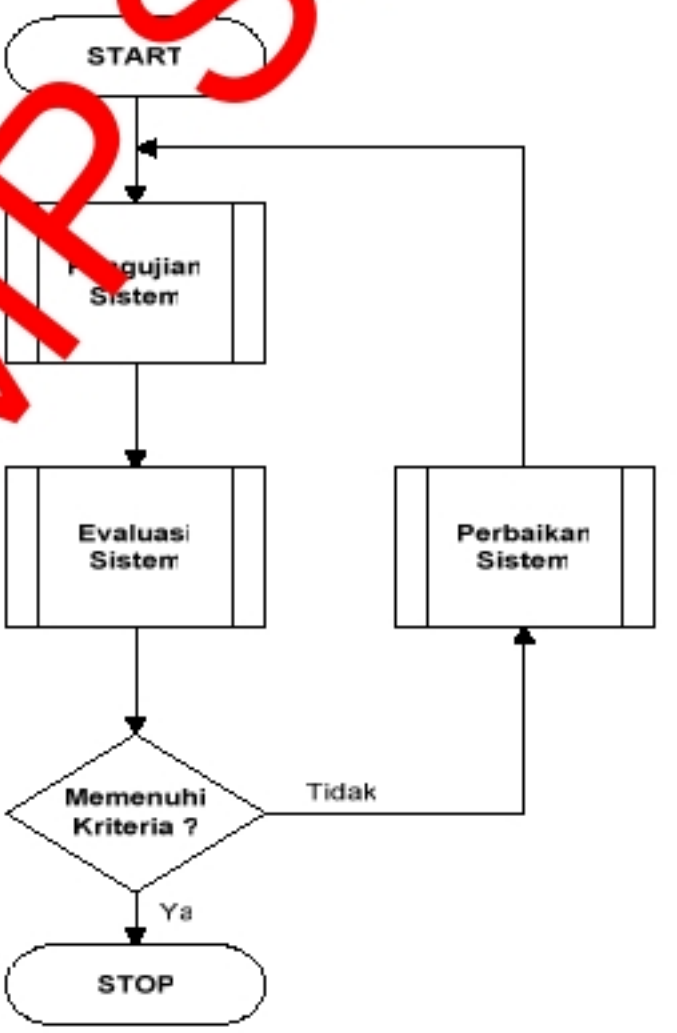
BAB IV

PENGUJIAN DAN EVALUASI SISTEM

4.1. Prosedur Pengujian

Untuk mengetahui apakah sistem yang dibuat sudah memenuhi kriteria yang diinginkan maka diperlukan suatu pengujian dan evaluasi sistem. Dalam proses pengujian dan evaluasi sistem sangat dimungkinkan adanya perbaikan-perbaikan, dalam hal ini pada sistem perangkat lunak, apabila dalam pengujian hasil yang ingin dicapai tidak dapat dipenuhi oleh sistem yang ada, tentu saja harus dilakukan investigasi sistem agar dapat diketahui letak kesalahannya. Secara umum, algoritma pengujian dan evaluasi sistem disajikan pada gambar 4.1 dibawah ini :



Gambar 4.1 Flowchart pengujian dan evaluasi sistem

4.2. Hasil Pengujian

Pada proses pelatihan data yang digunakan yaitu data serangan dan data normal. Pada tahap pelatihan, data dilatih oleh jaringan dengan parameter jaringan yang berbeda-beda hingga didapatkan parameter jaringan yang diinginkan yaitu dapat menghasilkan keluaran yang membedakan data normal dan data abnormal sehingga pengelompokan dapat dilakukan. Pada tahap pelatihan ini masih ada perhitungan *error* dan bila keluaran yang dihasilkan belum sama atau belum mendekati keluaran yang diharapkan, maka jaringan akan mengadakan perhitungan dan perbaikan faktor bobot hingga menghasilkan keluaran yang mendekati atau sama dengan keluaran yang diharapkan. Pada tahap ini terdapat pembatasan iterasi maksimum dan pembatasan *error* agar jaringan tidak terjebak dalam *looping* yang panjang.

Pada proses pelatihan digunakan 30 data serangan dan 20 data normal. Adapun kegiatan normal yang dilakukan adalah dengan mencoba mengakses komputer server dengan kegiatan yang dilakukan antara lain melakukan *browsing file*, *sharing data (copy and saving data to client)*. Sedangkan untuk data serangan digunakan NMAP dengan variasi serangan NMAP Fin Scan, NMAP Null Scan dan NMAP X-Mas Scan. Adapun hasilnya ditunjukkan pada tabel-tabel dibawah ini :

4.2.1. Masukan (*Input*) Data Normal

A. Browsing dan copy data pada tabel status

Pada tahap ini dilakukan proses perhitungan dan penyimpanan data normal hasil keluaran dari software final.c yaitu memberikan nilai bobot atas kondisi yang melibatkan *browsing data* dan *copy data* yang kemudian disimpan pada tabel status. Untuk data-data pada tabel status ditunjukkan pada tabel 4.1 dan tabel 4.2, pada kedua tabel tersebut terdapat 9 buah field yaitu :

- no berisikan nomor urut data yang terurut secara *ascending*.
- usr berisikan nilai bobot yang dipengaruhi oleh kegiatan user dilihat dari ip-address yang coba masuk ke server.
- port berisikan nilai bobot yang dipengaruhi oleh kegiatan user dilihat dari port yang digunakan untuk masuk ke server oleh suatu ip-address.
- payload berisikan nilai bobot yang dipengaruhi oleh kegiatan user dilihat dari *string* yang terkandung saat sebuah ip-address masuk ke dalam server.
- flags berisikan nilai bobot yang dipengaruhi oleh kegiatan user dilihat dari *flags* apa saja yang aktif selama sebuah ip-address mencoba ataupun masuk ke server.
- ack berisikan jumlah *acknowledgement number* yang terjadi saat sebuah user mencoba ataupun masuk ke server.

- window berisikan jumlah *window* yang terjadi saat sebuah user mencoba ataupun masuk ke server.
- icmp berisikan nilai bobot yang dipengaruhi oleh kegiatan user dilihat dari jumlah protokol icmp yang aktif.
- udp berisikan nilai bobot yang dipengaruhi oleh kegiatan user dilihat dari jumlah protokol udp yang aktif.

Tabel 4.1 Output data normal untuk browsing data (tabel status)

no	usr	port	payload	flags	ack	window	icmp	udp
1	0	0	1	0	4[illegible]110036.[illegible]956	30626.0121	0	0
2	0	0	1	0	5[illegible]60[illegible]045.9968	32671.015	0	0
3	0	0	1	0	[illegible]948358.391	32670.2482	0	0
4	0	0	1	0	532294383.5312	32671.0586	0	0
5	0	0	1	0	535845078.0183	32669.0515	0	0
6	0	0	1	0	536237071.7131	32670.0246	0	0
7	0	0	1	0	524035011.2981	32671.0452	0	0
8	0	0	1	0	535517143.0013	32669.0251	0	0
9	0	0	0	0	525528172.7351	32670.3433	0	0
10	0	0	0	0	525711823.4917	32671.0143	0	0

Tabel 4.2 Output data normal untuk copy data (tabel status)

no	usr	port	payload	flags	ack	window	icmp	udp
1	0	0	1	0	521901438.0021	32625.0133	0	0
2	0	0	1	0	525179460.3826	32671.0901	0	0
3	0	0	0	0	525519405.1987	32671.13[illegible]5	0	0
4	0	0	0	0	523551289.0109	326[illegible].[illegible]712	0	0
5	0	0	1	0	525713947.0341	32[illegible].0347	0	0
6	0	0	1	0	535019776.675[illegible]	32[illegible].1881	0	0
7	0	0	1	0	525419880[illegible]28[illegible]	[illegible]2669.0016	0	0
8	0	0	0	0	5104791[illegible].0[illegible]90	32671.4603	0	0
9	0	0	1	0	52739618[illegible].6934	32670.1124	0	0
10	0	0	0	0	5[illegible]9392[illegible].4752	32671.975	0	0

Untuk output data normal pada tabel 4.1 dan 4.2 diatas, dapat dilihat bahwa :

- Nilai kolom usr seluruhnya bernilai 0, hal ini menandakan *source ip-address* yang masuk merupakan ip-address yang *trusted* (diperbolehkan mengakses server) sehingga dapat disimpulkan kondisi yang menyangkut parameter user (usr) masuk dalam kategori normal.
- Nilai kolom port seluruhnya bernilai 0, hal ini menandakan hal-hal yang menyangkut parameter port, baik itu merupakan *source port* dan *destination port* yang digunakan selama user mencoba masuk ke server tidak ditemukannya sesuatu yang menyimpang (abnormal), sehingga dapat dikategorikan kondisi parameter port berada dalam kondisi normal.

- Nilai kolom payload bernilai antara 0 dan 1, untuk nilai 0 dapat disimpulkan bahwa payload dalam kondisi normal, sedangkan untuk payload bernilai 1 berarti ditemukannya data payload yang mengandung *string "open port"* atau *"port"* sehingga masuk dalam kategori abnormal dalam level medium. Sehingga dapat disimpulkan kondisi yang menyangkut parameter payload masuk dalam kategori normal dan abnormal.

- Nilai kolom flags seluruhnya bernilai 0, hal ini menandakan hal-hal yang menyangkut parameter flags yang aktif selama user mencoba masuk ke server tidak ditemukannya sesuatu yang menyimpang (abnormal), sehingga dapat dikategorikan kondisi untuk parameter flags yang aktif berada dalam kondisi normal.

- Nilai kolom ack berada di kisaran nilai yang besar yaitu antara 4.9 x 10^8 sampai dengan 5.2 x 10^8, sedangkan nilai window berada di kisaran nilai 3.0 x 10^4 sampai dengan 3.2 x 10^4. Parameter ack dan window masih memerlukan perhitungan lebih lanjut (perhitungan *fuzzy*) guna menentukan parameter tersebut masuk kategori normal atau abnormal.

- Nilai kolom icmp seluruhnya bernilai 0, hal ini menandakan jumlah protokol icmp yang aktif masih dalam batas normal.

- Nilai kolom udp seluruhnya bernilai 0, hal ini menandakan jumlah protokol udp yang aktif masih dalam batas yang normal.

Kesimpulan yang bisa didapatkan dari tabel 4.1 dan 4.2 diatas adalah karakteristik keluaran untuk kondisi data normal dapat dikategorikan menjadi dua yaitu :

- usr bernilai ‘0’, port bernilai ‘0’, payload bernilai ‘0’, flags bernilai ‘0’, ack bernilai antara 4.9×10^8 sampai dengan 5.3×10^8, window bernilai antara 3.0×10^4 sampai dengan 3.2×10^4, icmp bernilai ‘0’, dan parameter udp bernilai ‘0’.

- usr bernilai ‘0’, port bernilai ‘0’, payload bernilai ‘1’, flags bernilai ‘0’, ack bernilai antara 4.9×10^8 sampai dengan 5.3×10^8, window bernilai antara 3.0×10^4 sampai dengan 3.2×10^4, icmp bernilai ‘0’, dan parameter udp bernilai ‘0’.

Data-data yang terdapat pada tabel 4.1 dan 4.2 akan digunakan sebagai masukan untuk perhitungan fuzzy.

B. Browsing dan copy data pada tabel fuzzy

Pada tahap ini dilakukan proses perhitungan dan penyimpanan data normal hasil keluaran dari software fuzzy.c yaitu melakukan perhitungan fuzzy atas data-data yang terdapat pada tabel status diatas (tabel 4.1 dan tabel 4.2). Selanjutnya hasil dari defuzzifikasi disimpan di tabel fuzzy. Untuk data-data pada tabel fuzzy ditunjukkan pada tabel 4.3 dan tabel 4.4, pada kedua tabel tersebut terdapat beberapa field, yaitu :

no berisikan nomor urut data yang terurut secara *ascending*.

- usr_port berisikan nilai hasil defuzzifikasi antara field usr dengan port pada tabel status.

- payload_flags berisikan nilai hasil defuzzifikasi antara field payload dengan flags pada tabel status.
- ack_window berisikan nilai hasil defuzzifikasi antara field ack dengan window pada tabel status.
- icmp_udp berisikan nilai hasil defuzzifikasi antara field icmp dengan udp pada tabel status.

Tabel 4.3 Output data normal untuk browsing data (tabel fuzzy)

no	usr_port	payload_flags	ack_window	icmp_udp
1	0	1	5	0
2	0	1	5	0
3	0	1	5	0
4	0	1	5	0
5	0	1	5	0
6	0	1	5	0
7	0	0	5	0
8	0	1	5	0
9	0	0	5	0
10	0	0	5	0

Tabel 4.4 Output data normal untuk copy data (tabel fuzzy)

no	usr_port	payload_flags	ack_window	icmp_udp
1	0	1	5	0
2	0	1	5	0
3	0	0	5	0
4	0	0	5	0
5	0	1	5	0
6	0	1	5	0
7	0	1	5	0
8	0	0	5	0
9	0	1	5	0
10	0	0	5	0

Untuk output data normal pada tabel 4.3 dan 4.4 diatas, dapat dilihat bahwa :

- Nilai kolom usr_port seluruhnya bernilai 0 yang merupakan hasil defuzzifikasi kolom usr dan port pada tabel 4.1 dan 4.2 dimana parameter usr bernilai ‘0’ dan parameter port bernilai ‘0’ sehingga bila dimasukkan ke perhitungan defuzzifikasi didapatkan keluaran bernilai ‘0’. Jadi untuk parameter usr_port masuk dalam kondisi low.
- Nilai kolom payload_flags bernilai 0 dan 1. Nilai tersebut didapatkan dari hasil defuzzifikasi kolom payload dan flags pada tabel 4.1 dan 4.2 dimana parameter payload bernilai antara ‘0’ dan ‘1’ dan parameter flags bernilai ‘0’ sehingga bila dimasukkan ke perhitungan defuzzifikasi didapatkan keluaran

bernilai antara ‘0’ dan ‘1’. Untuk parameter payload_flags masuk dalam dua kondisi yaitu low dan medium.

- Nilai kolom ack_window seluruhnya bernilai 5 yang merupakan hasil defuzzifikasi kolom ack dan window pada tabel 4.1 dan 4.2 dimana parameter ack bernilai antara 4.9×10^8 sampai dengan 5.3×10^8 dan parameter window bernilai antara 3.0×10^4 sampai dengan 3.2×10^4 sehingga bila dimasukkan ke perhitungan defuzzifikasi didapatkan keluaran bernilai ‘5’. Jadi untuk parameter ack_window masuk dalam kondisi high.

- Nilai kolom icmp_udp bernilai 0 yang merupakan hasil defuzzifikasi kolom icmp dan udp pada tabel 4.1 dan 4.2 dimana parameter icmp bernilai ‘0’ dan parameter udp bernilai ‘0’ sehingga bila dimasukkan ke perhitungan defuzzifikasi didapatkan keluaran bernilai ‘0’. Jadi untuk parameter icmp_udp masuk dalam kondisi low.

Kesimpulan yang bisa didapatkan dari tabel 4.3 dan 4.4 diatas adalah karakteristik keluaran untuk kondisi data normal dapat dikategorikan menjadi dua yaitu :

- usr_port bernilai ‘0’, payload_flags bernilai ‘0’, ack_window bernilai ‘5’ dan icmp_udp bernilai ‘0’.
- usr_port bernilai ‘0’, payload_flags bernilai ‘1’, ack_window bernilai ‘5’ dan icmp_udp bernilai ‘0’.

Data-data hasil defuzzifikasi yang terdapat pada tabel 4.3 dan 4.4 akan digunakan sebagai masukan untuk proses pelatihan neural network.

4.2.2. Masukan (*Input*) Data Abnormal

A. Nmap FIN Scan, Null Scan dan X-Mas Scan pada tabel status

Pada tahap ini dilakukan proses perhitungan dan penyimpanan data abnormal hasil keluaran dari software final.c yaitu memberikan nilai bobot atas kondisi yang melibatkan kegiatan *scanning port* yang melibatkan 3 macam tipe yaitu *FIN scan*, *Null scan* dan *X-mas scan* yang menggunakan *tool NMAP Scanning Port*. Hasil dari keluaran software final.c akan disimpan pada tabel status. Untuk data-data pada tabel status ditunjukkan pada tabel 4.5, tabel 4.6 dan tabel 4.7 dibawah ini :

Tabel 4.5 Output pengujian Nmap FIN scan (tabel status)

no	usr	port	payload	flags	ack	window	icmp	udp
1	0	0	1	2	8136311.377	2556.4028	0	0
2	0	0	1	2	7878123.4072	2704.347	0	0
3	0	0	0	2	5503155.3017	2568.5131	0	0
4	0	0	0	2	6874934.8852	2452.2105	0	0
5	0	0	0	2	3409363.1209	2490.9395	0	0
6	1	0	1	2	5091837.0013	2713.827	0	0
7	1	0	1	2	7003285.9371	2419.8744	0	0
8	1	0	1	2	6284618.4296	2519.1739	0	0
9	1	0	0	2	5507348.3674	2649.2394	0	0
10	1	0	0	2	8368411.6493	2719.8375	0	0