BAB III
METODE PENELITIAN

3.1 Objek Penelitian

Objek penelitian ini mengenai keamanan jaringan dengan studi kasus di Cimun Net, dan bahan penelitian berupa topologi jaringan, konfigurasi jaringan, pengumpulan data dengan pihak terkait akan dilambil dari hasil wawancara dengan pemilik Cimun Net.

3.2 Lokasi Dan Waktu penelitian

Cimun Net yang beralamat di Jl. Kp. Lamaran No.6, Palumbonsari, Kec. Karawang Timur, Kabupaten Karawang adalah lokasi tempat penelitian yang akan dilakukan karena berdasarkan pendekatan lapangan. Rincian penelitian yang akan dilakukan dapat dilihat pada tabel 3.1.

Tabel 3. 1 Tabel Rincian Waktu Penelitian

No	Uraian	Bulan Pertama				Bulan Kedua				Bulan Ketiga				Bulan Keempat			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	*Analysis*																
2	*Design*																
3	*Simulation Prototyping*																
4	*Implementation*																
5	*Monitoring*																
6	*Management*																

3.3 Prosedur Penelitian

Prosedur penelitian ini mengacu pada Metode yang digunakan yaitu *Network Development Life Cycle* (NDLC), adapun tahapan yang dilakukan adalah :

1. Analysis

Pada tahapan awal ini dilakukan analisa kebutuhan, terhadap permasalahan yang muncul, serta kekurangan sistem yang akan diteliti, metode yang digunakan adalah seperti pada gambar 3.1

Gambar 3. 1 Metode *Analysis*

a) Wawancara

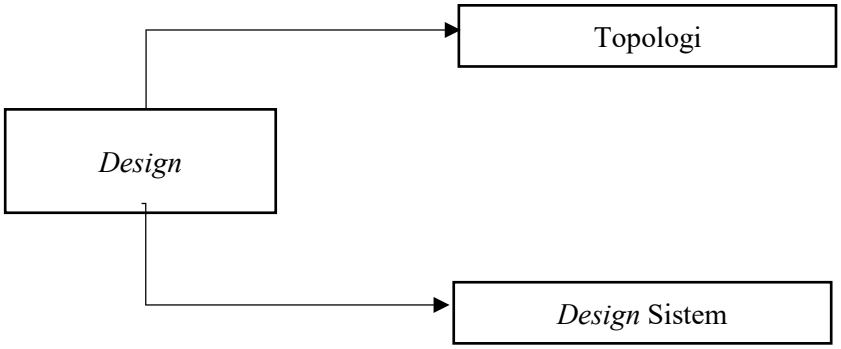
Melakukan wawancara dengan *administrator* jaringan dalam hal ini pemilik Cimun Net dengan maksud untuk mengetahui manajemen jaringan dan harapan yang diinginkan pemilik tentang keamanan jaringan.

b) Studi Pustaka

Melakukan kegiatan mencari referensi yang bersumber baik dari buku, jurnal ilmiah yang disesuai dengan keperluan analisis data.

2. *Design*

Pada Tahap ini akan membuat perencanaan desain topologi, dan *design* sistem.



Gambar 3. 2 *Design* perencanaan

a) Topologi

Berikut gambaran akan dipaparkan Topologi sistem berjalan dan Topologi sistem usulan, tahapan desain topologi menggunakan aplikasi simulator *Cisco Packet Tracer,* jaringan yang dibuat berdasarkan data yang didapat pada proses analisisa.

Berdasarkan topologi (Gambar 3.3),dengan menggunakan IP *class* C dengan menggunakan network 192.168.1.0/27, dan 192.168.1.1 sebagai host yang tersambung dengan *modem* dengan *akses internet* dengan IP 172.8.6.40 dari ISP untuk menyalurkan internet ke mikrotik untuk disebarkan melewati *switch*, lalu switch bertugas meneruskan paket baik itu langsung ke PC *client* maupun untuk dipancarkan kembali melalu *Acces Point* pada perangkat yang menggunakan media *WiFi*.

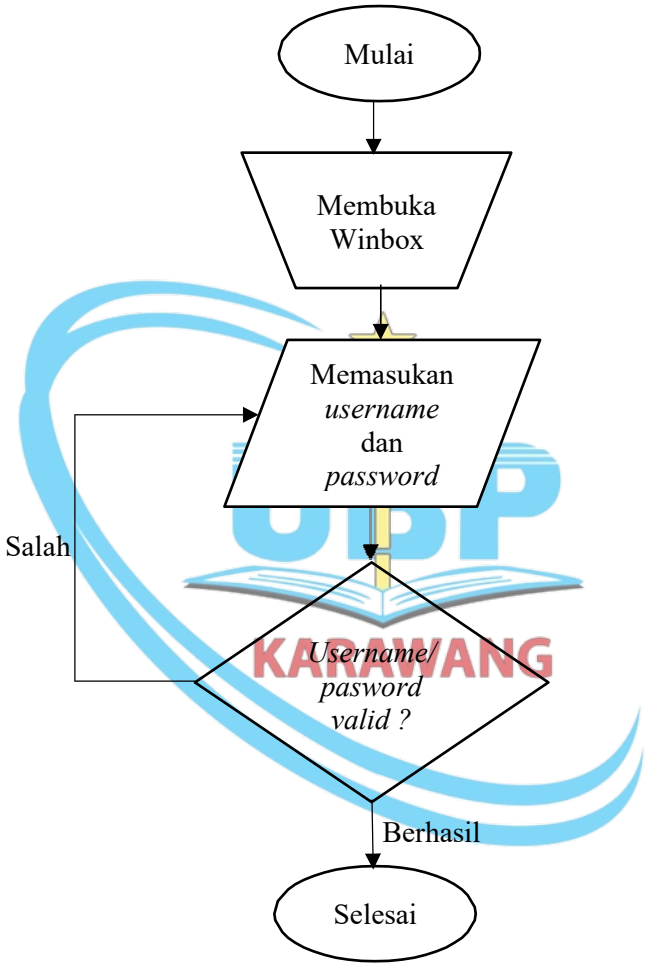
Gambar 3. 3 Topologi Sistem Berjalan

Pada Topologi (Gambar 3.4) ditambahkan sebuah firewall yang bertugas untuk mengamankan jaringan komputer, dengan menerapkan metode *port knocking* diharapkan dapat menambah keamanan *server* jaringan komputer.

Gambar 3. 4 Topologi Sistem Usulan

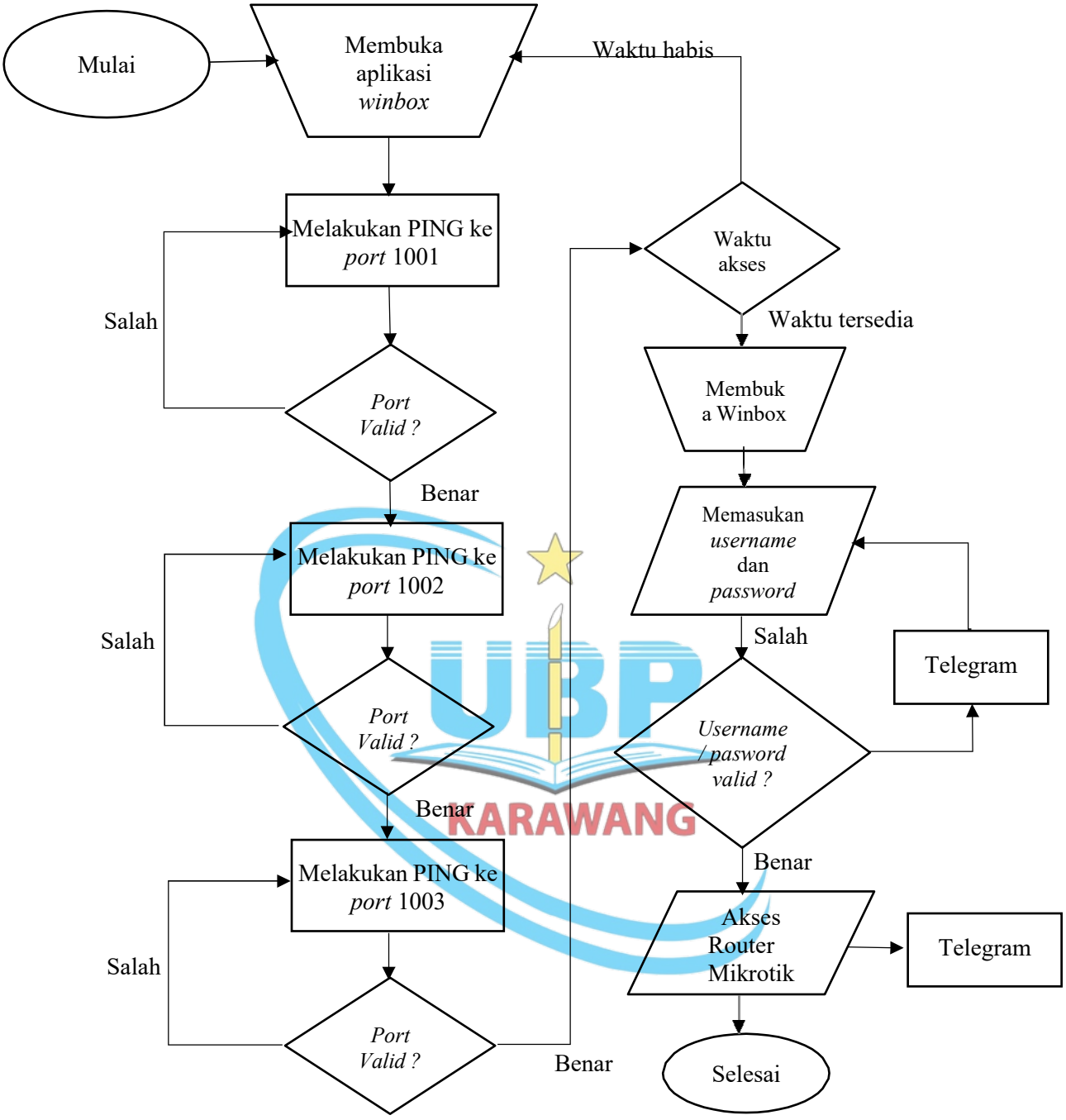
b) *Design* Sistem

Berdasar hasil pada proses Analisis maka dapat disimpulkan bahwa *design* keamanan sistem yang saat ini sedang berjalan adalah yang mengandalkan keamanan pada proses *login*, sehingga memungkinkan untuk diretas apabila mengetahui kombinasi *username* dan *password*, berikut adalah *design* sistem berjalan saat ini.



Gambar 3. 5 *Design* sistem berjalan

Berdasar *design* sistem berjalan maka perlu ditambahkan autentikasi berlapis yang bisa menambah keamanan pada proses *Login* sehingga memungkinkan untuk mengamankan sistem jaringan dari para pengguna yang tidak bertanggung jawab. Berikut adalah *design* sistem usulan yang akan diterapkan pada Gambar 3.6.



Gambar 3. 6 *Design* sistem usulan

3. Simulation Prototype

Pada tahap ini akan dilakukan simulasi *port knocking* pada perangkat mikrotik berdasarkan Gambar 3.6 yang dimaksudkan untuk melihat fungsionalitas pada sistem kemanan jaringan .

4. Implementation

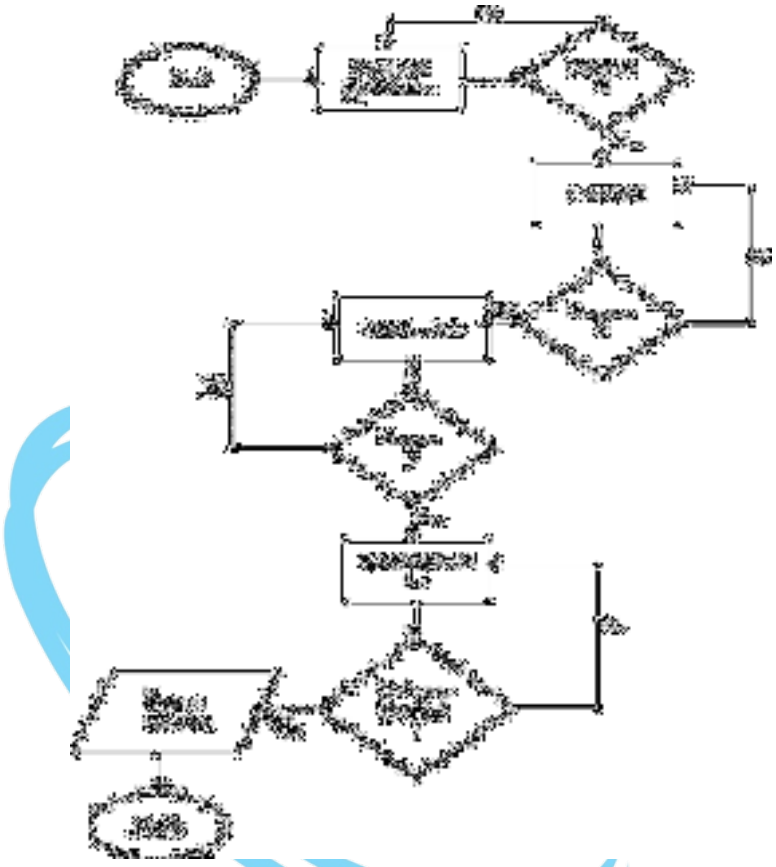
Pada tahap ini akan dilakukan penerapan sistem keamanan jaringan dengan berdasarkan hasil analisa dari tahap sebelumnya yang dilakukan pada sistem dengan metode *port knocking* yang mempunyai cara kerja menutup *port* yang ditentukan sehingga *user* hanya bisa mengakses *server* dengan cara mengetuk (*knock*) terlebih dahulu. Maka, dibutuhkan data seperti tertera pada Tabel 3.2.

Tabel 3. 2 Tabel *Port*

No	*Port* di *knock*	Urutan Port Knocking			Waktu akses
		1	2	3	
1	1001				60 Detik
2	1002				60 Detik
3	1003				60 Menit

Berdasarkan Tabel 3.2 proses implementasi akan diterapkan pada *router* Mikrotik yang akan mengamankan *port* winbox dan www dengan skenario pengetukan dimulai dari knock ke 1-2-3 dengan masing-masing *knock* mempunya waktu akses yang berbeda.

Bot telegram merupakan salah satu pilihan untuk mengintegrasikan perangkat mikrotik sehingga dapat dimonitoring secara *mobile*, cara membuat bot telegram berdasarkan diagram alir pembuatan token *bot* pada gambar 3.7.



Gambar 3. 7 Pembuatan *token bot* telegram

Untuk itu diperlukan *hardware* dan *software* sebagai berikut :

a) Hardware

1) Laptop Lenovo B490
2) Mikrotik RB941-2nD-TC

b) Software

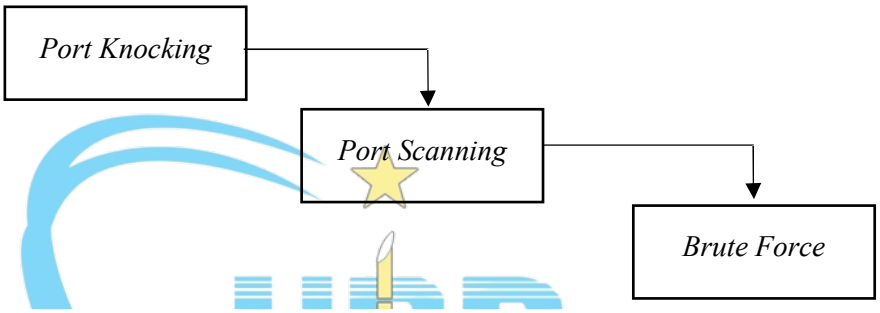
1) Sistem operasi windows 7.
2) Winbox untuk *remote access* server mikrotik.
3) *Microsoft office word* untuk membuat laporan.
4) Putty untuk melakukan *remote access* pada jaringan.

5) Zenmap Scanner untuk melakukan proses *scanning* pada jaringan.

6) Telegram untuk menerima notifikasi dari mikrotik.

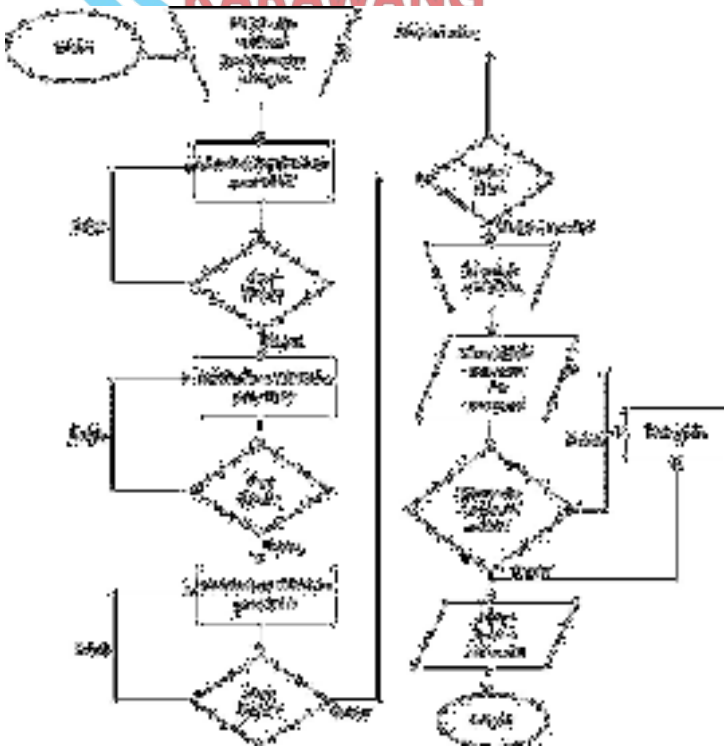
5. Monitoring

Pada tahap ini dilakukan *monitoring* terhadap hasil yang telah di implementasikan dengan melakukan *monitoring* pada *Log* mikrotik secara teratur dan juga dilakukan pengujian berdasarkan alur seperti pada Gambar 3.8.



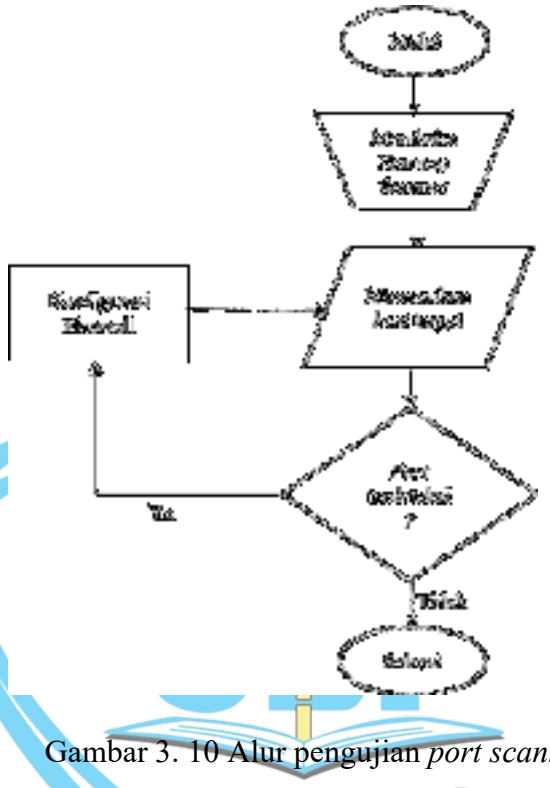
Gambar 3. 8 Alur pengujian

Alur pengujian yang pertama adalah *firewall* yang bermaksud untuk menguji dengan *port knocking* berdasarkan Gambar 3.8.



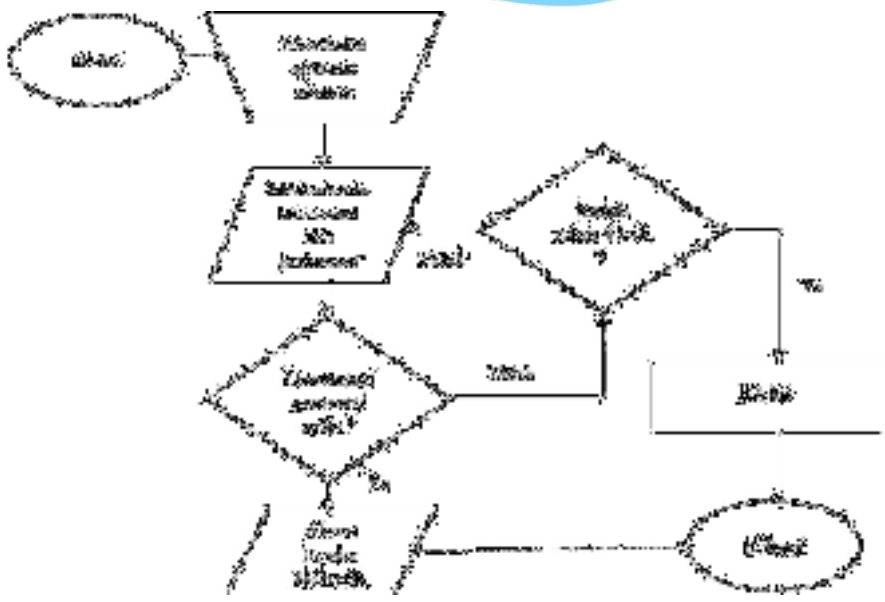
Gambar 3. 9 Alur pengujian *port knocking*

Alur pengujian yang kedua adalah *port scanning* yang bermaksud untuk mendeteksi port yang telah di *knocking* seperti pada Gambar 3.9.



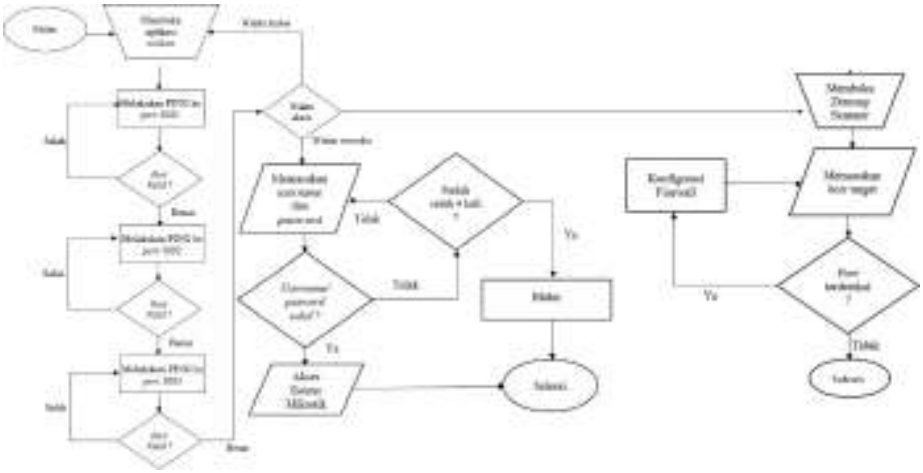
Gambar 3. 10 Alur pengujian *port scanning*

Alur pengujian yang ketiga adalah *brute force* yang bermaksud untuk memblokir *user* yang telah melakukan kesalahan pada proses *login* seperti pada Gambar 3.10.



Gambar 3. 11 Alur pengujian brute force

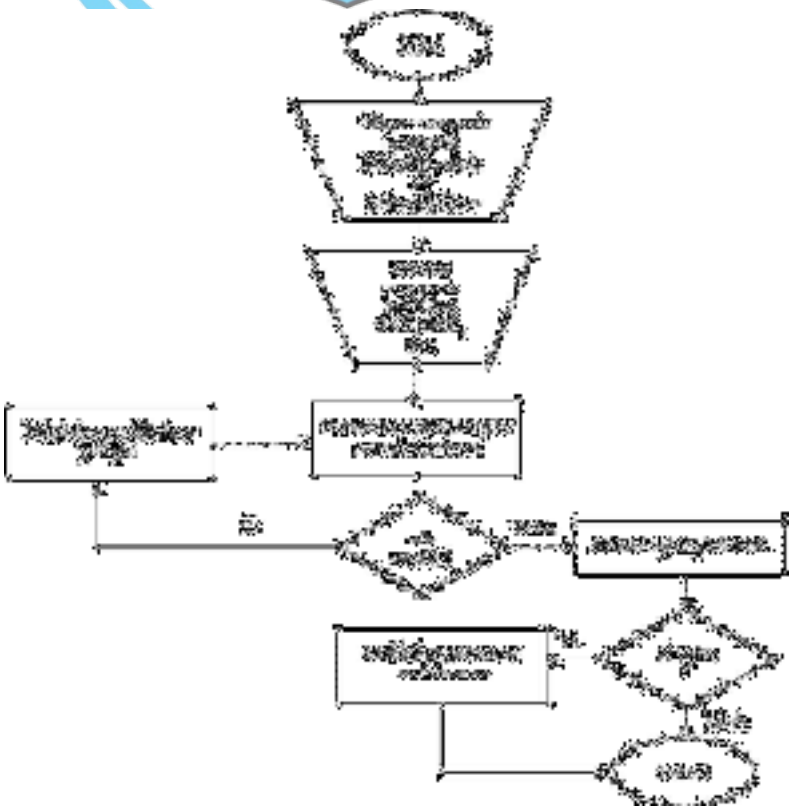
Dengan 3 alur pengujian tersebut, jika digabungkan maka akan seperti Gambar 3.12.



Gambar 3. 12 Alur pengujian gabungan

6. Management

Tahap terakhir ini perlu dibuatkan kebijakan yang mengatur agar sistem yang telah dikembangkan dapat berjalan dengan baik serta dapat mengamankan sistem sehingga dapat bertahan lama, maka akan dibuatkan SOP (*Standard Operating Procedure)* yang akan diterapkan berdasarkan Gambar 3.8 .



Gambar 3. 13 Alur SOP monitoring jaringan