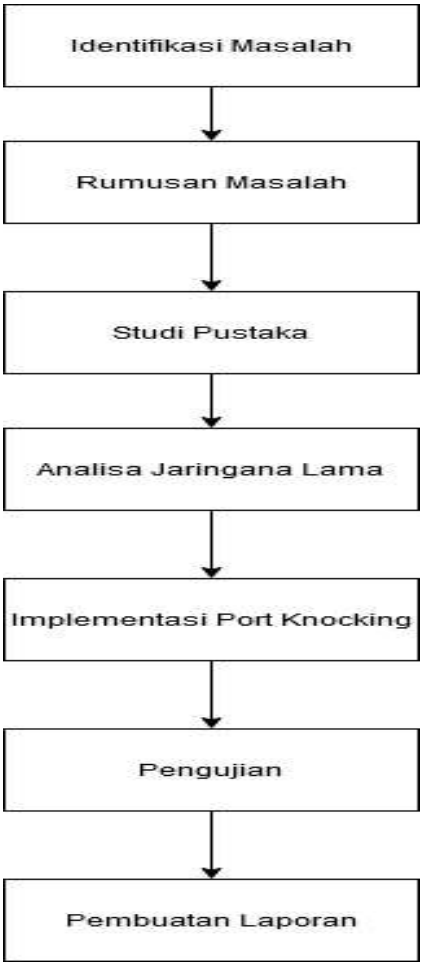
BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Proses pada metode penelitian menggunakan beberapa tahapan yang dalam melakukan penelitian seperti digambarkan pada gambar berikut :



Gambar 3.1 Metode Penelitian
Sumber : (Data Penelitian, 2023)

Penjelasan mengenai proses pada metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Identifikasi masalah

   Pada fase ini pendekatan dilakukan berkenaan dengan hal yang berkaitan dengan permasalahan yang sering terjadi di perusahaan atau instansi. Penelitian ini meliputi hal yang berkaitan dengan perangkat keras *(hardware),* perangkat lunak (*software)* dan berbagai bentuk ancaman serangan terhadap keamanan jaringan komputer sehingga masalah tersebut nantinya dapat diselesaikan dalam penelitian ini.

2. Perumusan masalah

   Pada tahapan ini peneliti merumuskan masalah yang ada menjadi bagian yang lebih rinci sehingga masalah yang ada dapat diurutkan secara spesifik dan terperinci yang mana nantinya masalah tersebut dapat dijawab dengan melalui penelitian yang dilakukan.

3. Studi pustaka

   Melakukan penelitian terhadap keamanan jaringan mikrotik sehingga dapat ditentukan langkah dalam rancang bangun jaringan mikrotik dan didapatkan gambaran komprehensif tentang hal apa saja yang telah ada sebagai teori yang mendasari dalam penelitian ini

4. Analisis jaringan lama

   1. Melakukan analisis terhadap ancaman serangan terhadap sistem jaringan lama, dan pemodelan terhadap sistem jaringan baru.

2. Menjelaskan sistem kinerja jaringan lama sehingga dapat diambil kesimpulan untuk perbaikan terhadap sistem baru yang akan diusulkan
3. Perancangan desain antarmuka untuk sistem keamanan jaringan mikrotik yang baru yang akan dibangun.

5. Implementasi port knocking

Melakukan perencanaan dan langkah langkah yang dapat digunakan dalam menjaga keamanan jaringan sesuai dengan prinsip dasar dari *port knocking* yakni mendefinisikan suatu metode komunikasi antara dua komputer, yang mana suatu informasi dikirimkan secara *encode* dalam bentuk koneksi ke *port port* dalam urutan tertentu. Langkah langkah implementasi port knocking :

1. Dengan menentukan urutan *port knocking* yang akan digunakan seorang *administrator* jaringan akan dengan mudah dalam menjaga keamanan jaringan.
2. Dengan memberi ketentuan seperti memberikan durasi waktu terhadap hak izin dalam mengakses *port knocking* dengan benar, sehingga ketika terjadinya percobaan serangan maka seorang *administrator* jaringan dapat mengantisipasinya.
3. Menbuka port tertentu untuk pihak yang berhak mengaksesnya saja, sehingga untuk keamanan akan berfokus pada port yang terbuka saja.

6. Pengujian

Jalankan pengujian terhadap sistem yang telah dirancang seperti melakukan percobaan untuk masuk ke sistem keamanan jaringan dengan paksa dan melihat ketika hal tersebut dilakukan apakah ada notifikasi ke aplikasi telegram kita yang kita gunakan sebagai pihak ketiga dalam pengujian ini. Uji semua konten yang ada apakah bekerja sesuai fitur dan fungsinya masing masing. Adapun langkah langkah dalam skenario pengujian sebagai berikut :

1. Menyiapkan skenario ancaman terhadap keamanan jaringan dan melakukan pengujian terhadap sistem keamanan jaringan untuk memastikan keberhasilan port knocking dan notifikasi telegram
2. Memantau *log* keamanan mikrotik dalam upaya mendeteksi serangan atau percobaan akses yang mencurigakan.

7. Pembuatan laporan

Membuat laporan mengenai rancangan dan hasil dari pengujian dengan menyertakan lampiran dari penelitian.

3.1.1 Teknik Pengumpulan Data

Dalam penelitian ini peneliti meggunakan dua cara dalam menggali informasi yaitu dengan melakukan observasi dan wawancara dengan tujuan untuk mendapatkan informasi yang berkaitan dengan tujuan penelitian ini. Dalam penelitian ini yang menjadi narasumber merupakan Bpk. Suwanda yang merupakan

direktur dari perusahaan PT. Shanaya Creativo Innovation adapun hal yang menjadi acuan dalam pengumpulan data ini adalah sebagai berikut :

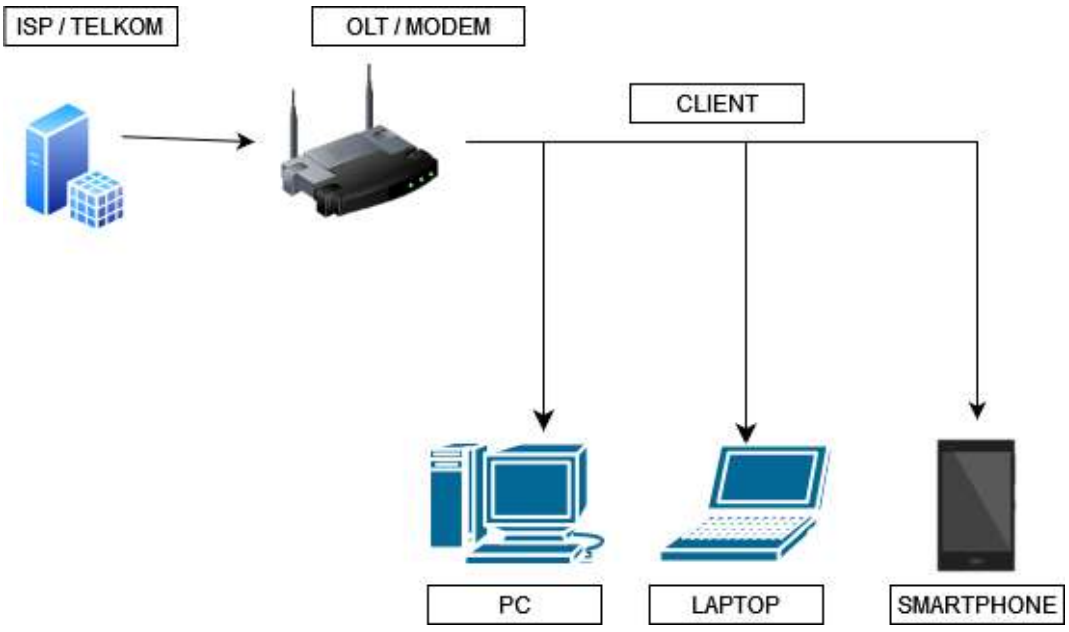
1. Observasi

   Tahapan observasi dengan mendatangi perusahaan untuk melakukan pengamatan guna mendapatkan informasi yang diperlukan dalam penelitian ini. Pada tahapan observasi peneliti langsung mendatangi PT Shanaya Creativo Innovation guna untuk melihat dan mengamati kemungkinan resiko yang berkaitan dengan keamanan mikrotik di perusahaan ini serta mengumpulkan informasi yang menjadi titik fokus dalam penelitian.

2. Wawancara

   Dalam penelitian ini, penulis melakukan wawancara bersama bapak Suwanda selaku direktur perusahaan, dengan mengajukan beberapa pertanyaan secara lisan dan tertulis guna untuk memperoleh informasi mendalam dan lengkap mengenai hal yang berkaitan dengan hal yang akan diteliti.

3.2 Analisis Jaringan Lama/ sedang berjalan



Gambar 3.2 Analisis Jaringan Lama
Sumber : (Data Penelitian, 2023)

Pada gambar diatas, proses keamanan yang berjalan pada PT. Shanaya Creativo Innovation pada bagian IT yang bertugas pada keamanan jaringan perusahaan, yang mana sistem yang diterapkan masih menggunakan sistem yang lama yaitu melakukan keamanan sistem yang masih menggunakan Laptop/PC (*Personal Computer)* dalam memantau lalu lintas jaringan yang sedang berjalan.

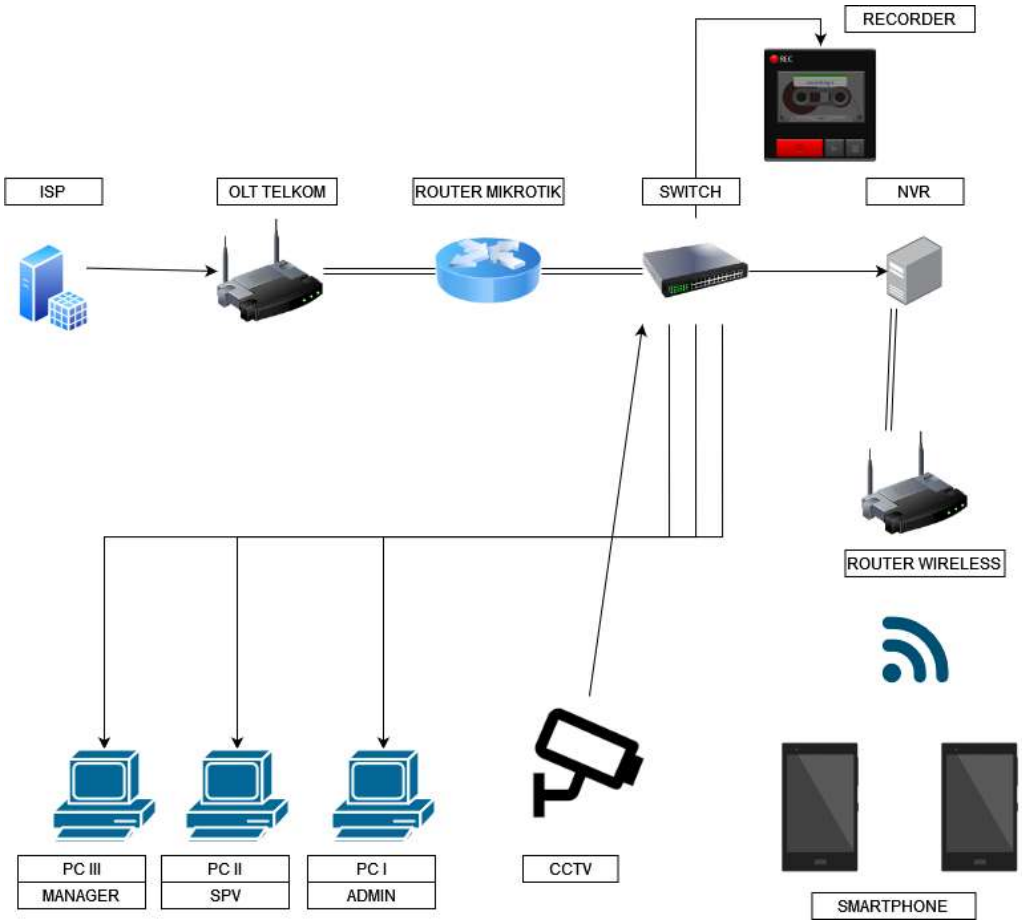
Proses pemantauan keamanan jaringan mikrotik untuk keperluan sebuah event pada PT. Shanaya Creativo Innovation masih menggunakan *personal computer* (PC) dengan langkah langkah sebagai berikut :

1. Langkah pertama para administrator jaringan akan masuk ke sistem server untuk memantau keamanan jaringan.
2. Selama memantau keamanan jaringan, para administrator harus selalu *standby* di depan komputer
3. Para administrator jaringan harus selalu ada di kantor untuk memantau keamanan jaringan.

Beberapa kelemahan ketika memonitoring keamanan jaringan menggunakan jaringan yang sedang berjalan diantaranya sebagai berikut :

1. Jaringan lama tidak menggunakan router mikrotik
2. Hanya megandalkan layanan dari ISP *(Internet Service Provider)*
3. Adanya potensi percobaan pembobolan keamanan jaringan di perusahaan.

3.3 Rancangan Jaringan yang diusulkan



Gambar 3.3 Sistem Jaringan Baru
Sumber : (Data Penelitian, 2023)

Pada gambar diatas ada beberapa usulan sistem keamanan jaringan di usulkan oleh peneliti, sehingga dapat memudahkan kinerja dari administrator jaringan yaitu dengan cara dengan menambahkan sebuah perangkat tambahan smartphone, yang mana nantinya peneliti akan mengimplementasikan API mikrotik untuk management sebuah router mikrotik yang berfungsi untuk membangun antarmuka antara dua perangkat yang berbeda. Jadi seorang *administrator* jaringan

nantinya dapat memantau sistem keamanan jaringan perusahaan melalui aplikasi telegram. Ketika ada pihak yang mencoba untuk masuk kedalam sistem keamanan jaringan mikrotik maka administrator jaringan akan mendapatkan notifikasi berupa laporan mengenai jenis serangan, port tujuan, IP address penyerang, IP address server serta waktu terjadinya serangan.

3.3.1 Metode demonstrasi

Suatu metode yang digunakan untuk mendemonstrasikan sebuah proses atau langkah langkah dalam penelitian yaitu menyiapkan alat yang akan digunakan dalam uji coba, menyiapkan objek penelitian, melakukan demonstrasi, mengamati serta menganalisis hasil yang didapat. Metode demonstrasi untuk mengetahui sejauh mana sebuah aplikasi dapat membantu seorang administrator ketika mengkonfigurasi suatu jaringan, sehingga dapat mengefisienkan waktu dalam melakukan suatu pekerjaan.

3.3.2 Desain pengiriman alur informasi serangan

Tahapan alur pengiriman informasi jika terjadi serangan terhadap sistem keamanan jaringan mikrotik, alur pengiriman informasi serangan pada perancangan *Intrusion Detection System* (IDS) dengan menggunakan snort yang nantinya akan mengirimkan notifikasi peringatan jika terdapat indikasi serangan dengan mengirimkan notifikasi pada aplikasi telegram, untuk dapat menghubungkan antara sistem dengan snort maka dibutuhkan sebuah *trigger* yakni dengan memanfaatkan sebuah API *(Application Programming Interface).* Aplikasi tersebut dibuat dengan menggunakan bahasa program PHP dengan tujuan supaya telegram dapat

terhubung dan memeriksa informasi mengenai data data penyerang, untuk desain pengiriman informasi dapat kita lihat dari gambar berikut .

Gambar 3.4 Desain Pengiriman Alur Informasi Serangan
Sumber : (Data Penelitian, 2023)

Apps interface dirancang untuk dapat mendapatkan informasi mengenai pihak yang mencoba untuk mengakses sistem keamanan jaringan mikrotik, dengan ketentuan sistem akan memblokir IP pengguna apabila telah salah dapat melakukan login terhadap sistem sebanyak 3 kali. Informasi yang akan dikirimkan ke telegram berdasarkan jenis serangan, port tujuan, IP address penyerang, IP address server serta waktu terjadinya serangan.

3.3.3 Perangkat hardware yang digunakan

Adapun perangkat hardware yang digunakan oleh PT. Shanaya Creativo Innovation dalam konfigurasi jaringan sebagai berikut:

Tabel 3. 1 Perangkat *Hardware* yang digunakan

No	Perangkat keras (*Hardware*)	Model	Keterangan	Gambar
1	Server	OLT Fujitomo E04L3 10G, 4 PON	Sebagai pusat untuk mengkonfigurasi jaringan serta memantau lalu lintas jaringan	
2	Router (mikrotik)	router mikrotik RB941-2nD-TC HAP Lite	Sebuah perangkat keras komputer yang berfungsi sebagai penghubung terhadap dua bahkan lebih terhadap jaringan yang berbeda	

Tabel 3.1 Perangkat *Hardware* yang digunakan (Lanjutan)

3	Smartphone	Infinix Hot 11s	Smartphone berguna untuk membantu dalam memonitoring jaringan komputer	
4	Telephone Analog	KX-TS505MX	Digunakan sebagai telephone analog di meja karyawan	

Sumber : (Data Penelitian, 2023)

3.3.4 Perangkat Software

Adapun beberapa perangkat lunak *(software)* yang digunakan dalam membangun jaringan ini antara lain sebagai berikut :

1. Mikrotik

   Sebuah sistem operasi yang berbasis perangkat lunak yang digunakan untuk mengubah komputer menjadi router jaringan, dari segi biaya router juga lebih hemat. Ada beberapa fitur yang diberikan oleh mikrotik seperti:

1. Mikrotik telah menerapkan sistem *autentifikasi* dan konfigurasi jaringan lokal
2. pengelolaan yang terpusat
3. tidak hanya untuk jaringan kabel saja tapi juga dapat digunakan untuk jaringan *wireless*
4. bisa berperan sebagai hotspot

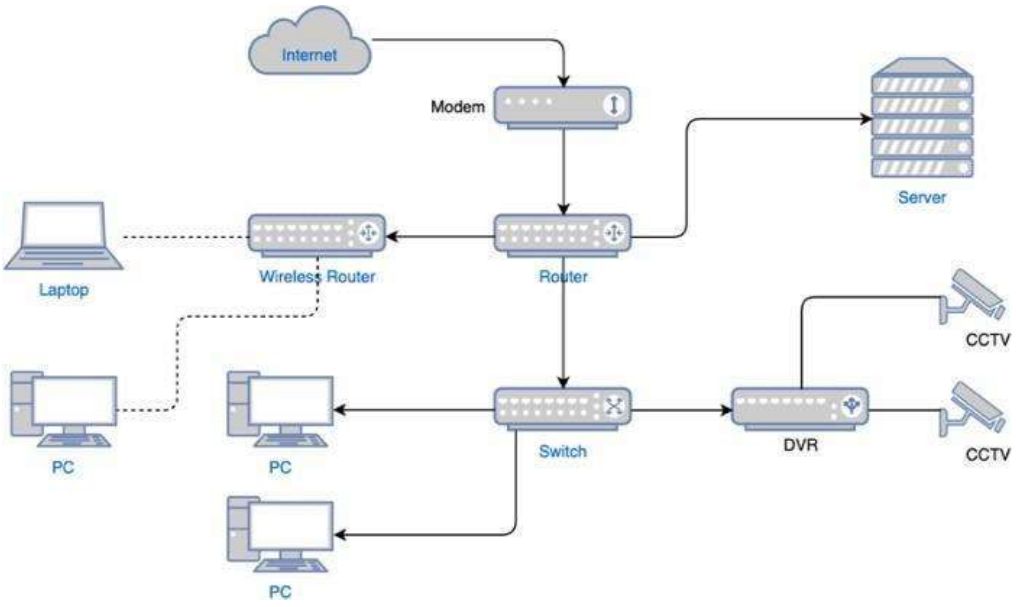
2. Library API

   Digunakan untuk menciptakan sebuah aplikasi berbasis *mobile* yang digunakan management sebuah router mikrotik, yang nantinya dalam membantau jaringan bisa melalui komputer dan secara *mobile.*

3.3.5 Spesifikasi Hardware dan Software

Simulasi sistem keamanan jaringan mikrotik untuk event virtual akan menggunakan beberapa perangkat keras *(hardware)* dan perangkat lunak (*software),* yang mana disini sistem akan dioperasikan dengan 4 user pada virtual mesin sebagai router. Disini menggunakan mikrotik dengan versi 7.1.1, *attacker 1 (FileZilla), attacker 2 (Putty), attacker 3 (Zenmap) log server* dan telegram *gateway,* administratornya (windows 10) dan winbox versi 3.34

3.4 Topologi jaringan



Gambar 3.5 Topologi Jaringan
Sumber : (Data Penelitian, 2023)

Peneliti menggunakan topologi star dalam melakukan konfigurasi jaringan dan melakukan konektivitas antara *smartphone* dengan mikrotik. Topologi star merupakan sebuah topologi jaringan komputer yang terdiri dari konvergensi melalui titik *(node)* tengah ke setiap titik *(node)* yang terhubung. Topologi star memanfaatkan fitur dari mikrotik yang sudah *built-in wifi,* sehingga *smartphone* dapat dengan langsung terkoneksi ke mikrotik, sedangkan komputer/laptop nantinya akan menggunakan kabel UTP untuk mengkoneksikannya yang dapat *memonitoring traffic* pada mikrotik.

3.5 Tahapan rencana implementasi

Beberapa tahapan perencanan dalam mengimplementasikan sistem keamanan yang akan dirancang. Adapun tahapan implementasinya sebagai berikut:

1. Menyiapkan perangkat mikrotik yang akan digunakan sebagai *firewall* serta hak akses *administrator* ke perangkat tersebut.
2. Mengkonfigurasikan mikrotik
    a. Melakukan konfigurasi basic pada mikrotik yaitu membuah *dhcp client* dan *dhcp service* serta melakukan proses NAT *(Network Addressing Translalation)* agar *client* mendapatkan akses internet.
    b. Membuat kebijakan keamanan yang akan diterapkan di *firewall* mikrotik
    c. Membuat aturan untuk pemblokiran bagi pihak yang tidak dapat mengakses dengan valid
    d. Membuat aturan *firewall* dinamis sehingga dapat membuka akses *port knocking* setelah berhasil
3. Mengkonfigurasi *port knocking*

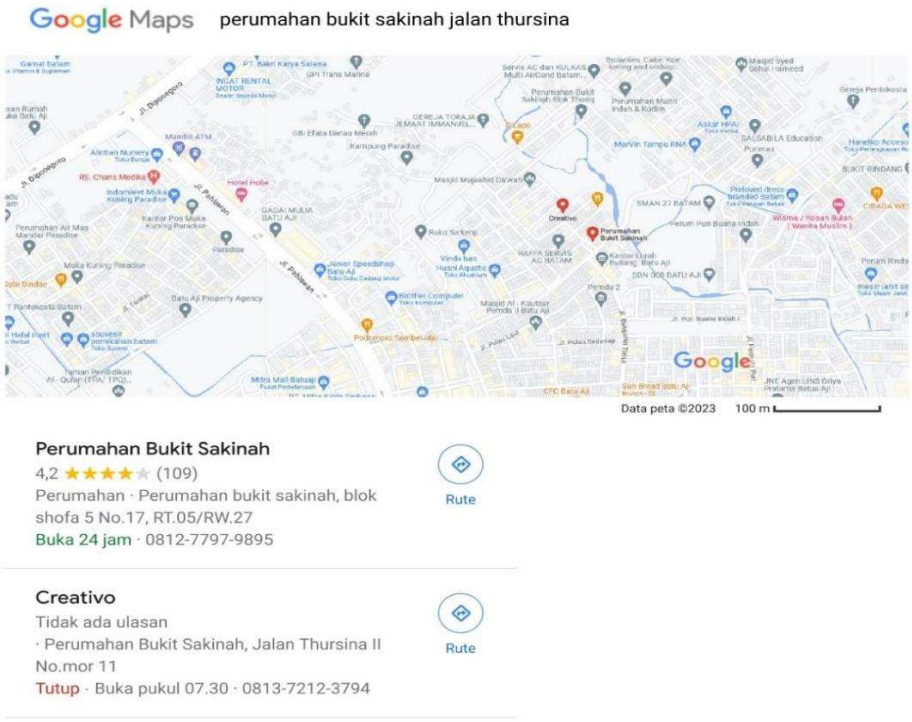
    Mengatur lama waktu yang diizinkan dalam mengakses *port knocking* setelah berhasil
4. Integrasi notifikasi telegram

    Mengkonfigurasikan mikrotik untuk dapat mengirimkan notifikasi melalui telegram menggunakan API bot

3.4 Lokasi dan Jadwal Penelitian

3.4.1 Lokasi penelitian

PT. Shanaya Creativo Innovation merupakan sebuah perusahaan perorangan yang bergerak dibidang *IT Consultant* yang beralamatkan di perumahan bukit Sakinah jalan thursina 2 no 11, kec Sagulung, Kota Batam, Prov. Kepulauan Riau.



Gambar 3.6 Lokasi Penelitian
Sumber : (Data Penelitian, 2023)

3.4.2 Jadwal penelitian

Penelitian ini dilaksanakan di PT Shanaya Creativo Innovation yang beralamat di perumahan Bukit Sakinah jalan thursina 2 no 11, kec Sagulung, Batu Aji. Lokasi ini dipilih karena akan mempermudah peneliti dalam melakukan

penelitian dan perancangan alat. Waktu yang dihabiskan dalam melakukan penelitian ini selama lebih kurang 6 bulan, berawal dari bulan Maret 2023 sampai dengan Agustus 2023. Adapun kegiatan yang dilakukan selama penelitian dapat dilihat dalam tabel 3.2.

Tabel 3. 2 Jadwal Penelitian

Kegiatan	**Waktu pelaksanaan**																							
	Maret 2023				**April 2023**				**Mei 2023**				**Juni 2023**				**Juli 2023**				**Agustus 2023**			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Judul																								
Bab I																								
Bab II																								
Bab III																								
Bab IV																								
Bab V																								
Pengumpulan Skripsi																								

Sumber : (Data Penelitian, 2023)