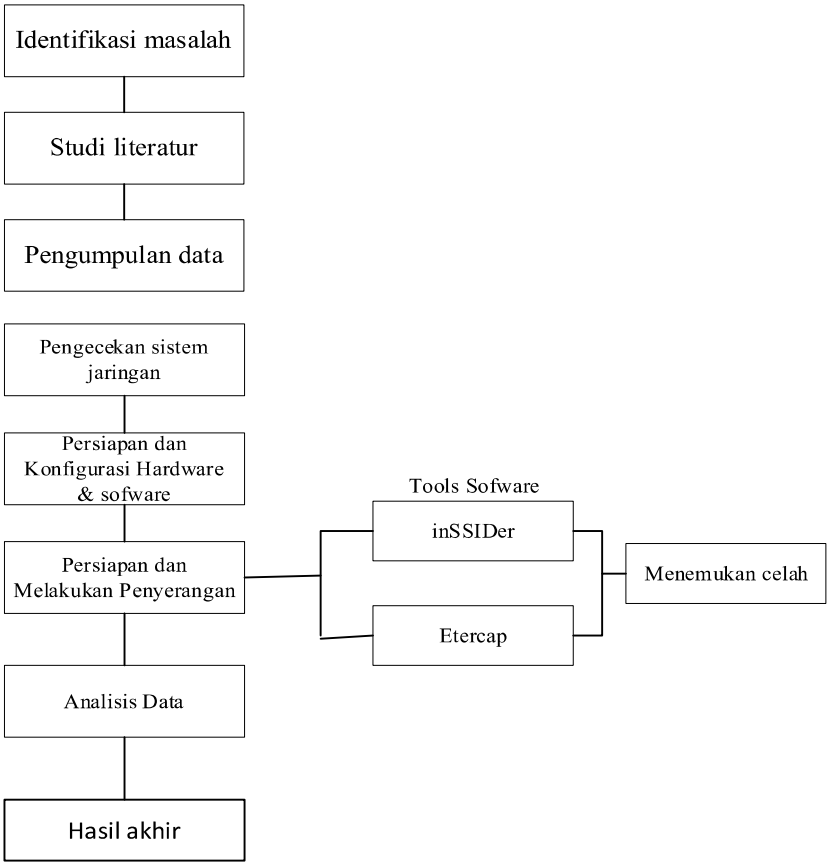
BAB lll

METODE PENELITIAN

3.1 Desain Penelitian

Desain penelitian menyediakan kerangka dan alur kerja mencakup sepanjang proses penelitian. Dalam desain penelitian ini, penulis membagi penelitian menjadi beberapa tahap sebagai berikut :



Gambar 3. 1 Disain Penelitian

Pada Gambar 3.1 desain penelitian didalam sebuah penelitian disajikan dalam bentuk sebuah diagram untuk menghasilkan solusi dari sebuah permasalahan. Berikut penjelasan dari desain penelitian :

1. Identifikasi masalah

   Melakukan identifikasi masalah dengan studi literatur dan pengamatan lapangan (observasi) di tempat penelitian.

2. Studi Literatur

   Melakukan studi literatur yang berhubungan dengan penelitian yaitu data – data yang berasal dari studi pustaka yang berkaitan dengan judul penelitian.

3. Pengumpulan data

   a. Observasi

      Metode ini dilakukan dengan cara pengamatan langsung pada lokasi tempat penelitian yaitu toko services w-elektrik batam dan melakukan pencatatan informasi yang berkaitan dengan obyek penelitian.

   b. Wawancara

      Wawancara adalah salah satu metode yang dilakukan untuk melengkapi hasil pengamatan yang diperoleh melalui observasi. Wawancara dilakukan terhadap pihak-pihak yang mempunyai kapasitas dan informasi yang dibutuhkan dalam hal ini pihak IT pada toko tersebut.

   c. Studi Kepustakaan

      Studi Kepustakaan adalah metode pengumpulan data dengan membaca buku referensi atau dokumentasi yang berhubungan dengan penelitian tentang keamanan jaringan. Dalam hal ini juga dilakukan *browsing* untuk mencari data atau dokumentasi yang berhubungan dengan obyek yang sedang diteliti.

4. Pengecekkan sistem jaringan

   proses memeriksa kondisi atau kinerja jaringan di toko services w-elektrik batam untuk menentukan apakah semua komponen berfungsi dengan baik dan sesuai dengan spesifikasi.

5. Persiapan dan Konfigurasi *Hardware &Software*

   Menyiapkan *hardware* dan *software* yang dibutuhkkan untuk menunjang pelaksanaan penelitian.

6. Persiapan dan melakukan penyerangan

   Menyiapkan alat dan bahan yang akan digunakan untuk melakukan percobaan penyerangan. Melakukan Penyerangan. Melangkah untuk melakukan sebuah percobaan penyerangan kepada jaringan Wi-Fi untuk mendapatkan informasi tentang keamanannya. Dan *tools* yang akan di gunakan yaitu *Inssider* dan Ettercap, saat melakukan penyerangan terdapat celah seperti accun *username* dan *password* yang mudah di dapat.

7. Menganalisa Data

   Analisa dilakukan untuk mengetahui tingkat keamanan yang diterapkan.

8. Hasil akhir

   Membuat laporan sesuai dengan hasil penelitian yang telah dilakukan.

3.2 Analisis Jaringan

3.2.1 Analisis Sistem jaringan

Analisis sistem jaringan adalah proses mengevaluasi kinerja, konfigurasi, dan topologi jaringan komputer untuk menemukan masalah dan meningkatkan kinerja. Analisis ini dapat dilakukan pada jaringan lokal (LAN) atau jaringan luas

(WAN). Berikut adalah beberapa elemen yang dapat di analisis dalam sistem jaringan:

1. *Hardware*: Meliputi perangkat keras seperti router, switch, firewall, server, dan perangkat keras lainnya yang digunakan dalam jaringan.
2. *Software*: Meliputi sistem operasi, aplikasi jaringan, dan perangkat lunak lainnya yang digunakan dalam jaringan.
3. *Topologi*: Meliputi arsitektur jaringan, seperti topologi bus, star, atau mesh, dan konfigurasi koneksi fisik antara perangkat keras.
4. Kinerja: Meliputi kecepatan jaringan, pemakaian bandwidth, dan kapasitas jaringan.
5. Keamanan: Meliputi keamanan fisik, keamanan logika, dan keamanan aplikasi dari jaringan.
6. Dokumentasi: Meliputi dokumentasi jaringan yang diperlukan untuk mengelola dan mengkonfigurasi jaringan.

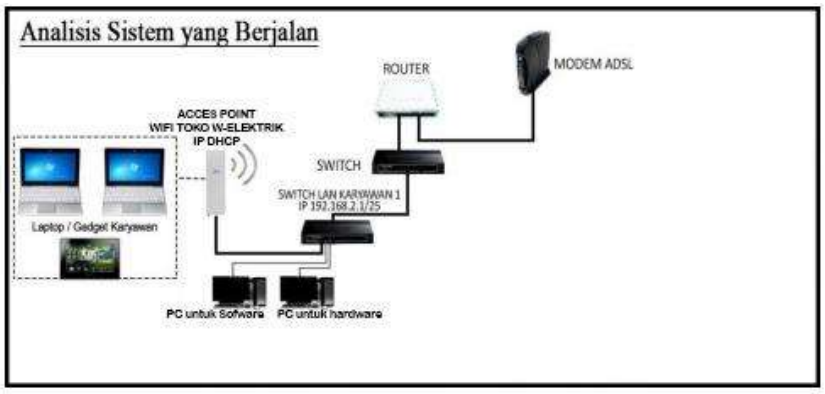
Berikut ini tabel yang dapat digunakan untuk melakukan analisis sistem jaringan:

Tabel 3. 1 Elemen analisis jaringan topologi Star

Elemen	**Deskripsi**	**Status**	**Tindakan**
Hardware	Router	Rusak	Ganti router baru
Software	Sistem operasi	Versi lama	Upgrade ke versi terbaru
Topologi	Star	Konfigurasi salah	Perbaiki konfigurasi
Kinerja	Kecepatan jaringan	Lambat	Tambahkan switch baru
Keamanan	Firewall	Kerentanan	Instal patch keamanan
Dokumentasi	Dokumentasi jaringan	Belum ada	Buat dokumentasi jaringan

Dalam tabel 3.1 Elemen analisis jaringan , setiap elemen dianalisis diberikan status dan tindakan yang diperlukan untuk mengatasi masalah yang ditemukan salah satunya topologi Star.

Sistem keamanan jaringan pada saat ini masih kurang efektif dan efisien dalam mensimulasikan tingkat keamanan pada jaringan internet di toko w-elektrik batam. Dimana keamanan jaringannya masih memiliki celah yang dapat disusupi oleh trojan dan pihak-pihak yang tidak memiliki kewenangan.



Gambar 3. 2 Analisis Sistem berjalan

Gamar 3.2 Menunjukkan analisis sistem yang sedang berjalan atau yang sedang digunakan. alat yang digunaka berupa Modem ADSL,Router,Switch, Wi-Fi Hostpot,PC,Laptop. Untuk keluhan di toko services w-elektrik batam yaitu sering terjadinya *system failure* di komputer untuk software dampaknya software atau tools yang akan di gunakan dalam bekerja tidak berjalan dengan normal, dari gambar tersebut menunjukkan PC 1 untuk software,PC 2 untuk Hardware dan Acces point untuk bebas pakai di gabungkan satu Switch hal ini sangat rentang terjadinya serangan baik virus mau pun trojan.

3.2.2 Analisis data pada jaringan

3.2.2.1 Analisi jaringan menggunakan tools ettercap

Analisis jaringan menggunakan tools Ettercap. ettercap adalah alat open-source yang digunakan untuk melakukan analisis data jaringan dan man-in-the-middle (MITM) attacks. Berikut ini tabel yang dapat digunakan untuk melakukan analisis data jaringan menggunakan tools Ettercap:

Tabel 3. 2 Tools ettercap

Elemen	Deskripsi	Hasil	Tindakan
Target IP	Alamat IP target	192.168.2.1/25	-
Filter	Filter yang digunakan	-	-
Protokol	Protokol yang digunakan	HTTP	-
Data yang ditangkap	Data yang ditangkap dari paket jaringan	Login dan password	-
Serangan	Serangan yang dilakukan	MITM	-
Hasil serangan	Hasil dari serangan	Berhasil mendapatkan Username dan password	-

Bahwa atribut pada tabel 3.2 tools ettercap berupa elemen, Deskripsi, Hasil dan Tindakan. Pada tabel diatas merupakan aktifitas Ettercap mencari celah keamanan.

Tabel 3. 3 celah keamanan menggunakan Ettercap

IP Address	Nama Host	Jenis Perangkat	Konfigurasi Firewall	Routing	Protokol jaringan	Patch dan Update	Status
192.168.1.1	Router	ACER	Aktif	Static	TCP/IP	v1.0.2	• Aman
192.168.1.2	Server	Lenovo	Aktif	Dynamic	TCP/IP	v1.0.3	• Aman
192.168.1.3	Workstation	Dell	Non- Aktif	-	TCP/IP	v1.0.1	• Tidak aman

Bahwa atribut pada tabel 3.3 berupa dari tools Ettercap. Setelah itu dapat ditentukan rule atau aturan suatu hostpot aman atau tidak yang menyebabkan *system failure*, penentuan rule sebagai berikut :

1. IF 192.168.1.1 Router and Konfigurasi firewall Aktif Routing Static TCP/IP patch update v1.0.2 then Status Aman
2. IF 192.168.1.2 Server and Konfigurasi firwall Aktif Routing Dynamic TCP/IP patch update v1.0.3 then Status Aman
3. IF 192.168.1.3 Workstation and Konfigurasi firwall Off Routing there isn't any TCP/IP Patch update v1.0.1 then Status Tidak Aman

Analisis ini menunjukan potensi celah keamanan. Tabel ini menunjukkan beberapa informasi penting mengenai perangkat jaringan, konfigurasi jaringan, patch dan update yang digunakan dan ancaman yang di temukan dalam jaringan.

3.2.2.2 Cara kerja Trojan

Trojan umumnya bergerak melalui tahapan berikut:

1. Pengiriman: Trojan dikirimkan ke komputer korban, biasanya disamarkan sebagai aplikasi yang sah atau disertakan dalam email yang tampaknya tidak berbahaya.
2. Instalasi: Dengan membuka lampiran email yang terinfeksi atau menjalankan program yang disamarkan, korban tanpa sadar menginstal trojan di komputer mereka.
3. Eksekusi: Trojan akan mulai mengeksekusi kode jahatnya di komputer korban setelah diinstal.
4. Kontrol dan Perintah: Trojan terhubung ke server perintah dan kontrol penyerang, memungkinkan penyerang untuk mengontrol komputer yang terinfeksi dari jarak jauh.
5. Ekstraksi dan pengumpulan data: Kata sandi, data keuangan, dan informasi pribadi hanyalah beberapa dari data sensitif yang mulai dicuri trojan dari komputer yang terinfeksi. Server perintah dan kontrol penyerang menerima data ini setelah dieksfiltrasi (ditransfer).
6. Panel kontrol: Komputer yang terinfeksi dapat diakses dari jarak jauh oleh penyerang, yang kemudian dapat menggunakannya untuk melancarkan serangan tambahan, menyebarkan malware, atau bahkan menggunakannya

sebagai titik pivot untuk menyerang sistem jaringan lain. Penting untuk diingat bahwa tidak semua trojan dibuat sama, dan beberapa dirancang untuk tujuan yang berbeda. Akibatnya, langkah-langkah yang disebutkan di atas mungkin tidak selalu diperlukan.

3.2.2.3 Identifikasi Trojan

Tujuan dari identifikasi trojan di toko services w-elektrik batam adalah untuk mengetahui apakah ada trojan yang menyebar di jaringan komputer tersebut, dan jika ada, mengidentifikasi trojan tersebut agar dapat diambil tindakan pencegahan dan penanganan yang tepat. Identifikasi trojan juga bertujuan untuk mencegah penyebaran virus ke sistem lain di jaringan, serta untuk mengurangi risiko keamanan yang disebabkan oleh trojan.

Ada beberapa tools atau perangkat lunak yang dapat digunakan untuk mengidentifikasi trojan pada komputer:

1. Antivirus: Antivirus adalah perangkat lunak yang dirancang untuk mendeteksi dan menghapus virus, Trojan, dan ancaman lain yang mungkin ada pada komputer. Banyak antivirus memiliki fitur pemindaian yang dapat memindai sistem komputer dan menemukan ancaman yang terdeteksi.
2. Malware scanner: Malware scanner adalah perangkat lunak yang dirancang untuk mendeteksi dan menghapus malware, termasuk trojan. Beberapa malware scanner hanya menyaring file yang terinfeksi, sementara yang lain juga dapat memindai sistem untuk menemukan ancaman yang tersembunyi.

3. Security suite: Security suite adalah perangkat lunak yang menyediakan pelindung keamanan lengkap untuk komputer, Termasuk antivirus, firewall, dan fitur-fitur keamanan lainnya. Security suite dapat membantu mengidentifikasi dan menghapus virus trojan yang mungkin ada pada komputer.
4. Online virus scanner: Online virus scanner adalah layanan yang menyediakan pemindaian virus secara online. Dapat menggunakan online virus scanner untuk memindai komputer tanpa perlu menginstall perangkat lunak tambahan.
5. Command-line tools: Command-line tools adalah perangkat lunak yang dapat dijalankan dari command prompt atau terminal. Beberapa command-line tools yang dapat digunakan untuk mengidentifikasi trojan termasuk ClamAV, Chkrootkit, dan Rootkit Hunter.

   Jika mencurigai adanya trojan pada computer.

Tabel 3. 4 Indentifikasi Trojan

Nama Trojan	Lokasi File	Tanggal di Temukan	Tingkat Kerentanan	Tindakan
Trojan.FakeAV	C:\Windows\System32\	01/20/2023	Tinggi	Dihapus dan dihapus
Trojan.Banker	C:\Users\Public\	01/19/2023	Sedang	Dihapus dan dihapus
Trojan.Ransomware	C:\Program Files\	01/18/2023	Tinggi	Dihapus dan dihapus

Untuk mengetahui aktifitas pada tabel 3.4 ada beberapa atribut yang di tampilkan seperti, Nama trojan yang ditemukan, lokasi file, tanggal ditemukan, tingkat kerentanan trojan, dan tindakan yang diambil semuanya ditampilkan di tabel. Maka penentuan rule atau aturan sebagai berikut :

1. IF Trojan.FakeAV Detected Aktif C:\Windows\System32\ and hard to remove. Maka Tingakat kerentanan Tinggi,Tindakan Install ulang Windows
2. IF Trojan.Banker Detected Aktif C:\Users\Public\ and can be deleted.

   Maka Tingkat Kerentanan Sedang Tindakan Upgrade Antirus
3. IF Trojan.Ransomware Detected Aktif C:\Program Files\ and can be deleted but come back.

   Maka Tingkat Kerentanan Tinggi, Tindakan Upgrade windows atau Update antivirus.

3.2.2.4 Analisis jaringan menggunakan tools InSSIDer

Analisis jaringan menggunakan tools InSSIDer, adalah alat yang digunakan untuk menganalisis jaringan nirkabel (Wi-Fi) dan menemukan masalah yang mungkin terjadi. Berikut ini adalah contoh tabel yang dapat digunakan untuk melakukan analisis jaringan menggunakan alat InSSIDer:

Tabel 3. 5 Rule atau aturan pada tools InSSDer

SSID	Signal	Chanel	Security	MAC.Addres	802.11
	-85	10	Wpa2/personal	OC:37:47:92:DF:97	n
	-85	10	Wpa2/personal	OE:37:47:B1:DF:97	n
Rumah putri	-80	11	Wpa2/personal	FC:A6:CD:BB:37:CO	n
Toko w-lektrik	-25	11	Open	36:E9:11:3A:75:99	n
Doraemon	-76	1	Open	68:37:47:92:DF:97	n
	-80	3	Wpa2/personal	C4:A3:66:B1:75:14	n

Untuk mengetahui aktifitas pada tabel 3.5 ada beberapa atribut yang di tampilkan seperti SSID,Signal, Chanel, Security, MAC Addres dan 802.11. Adapun penjelasan atribut pada table,

1. SSID (*Service Set Identifier*) adalah nama unik yang diberikan kepada setiap jaringan wireless. SSID digunakan untuk mengidentifikasi jaringan wireless yang spesifik dan membedakannya dari jaringan wireless lain yang ada di lingkungan yang sama.
2. Signal adalah Kekuatan dan kualitas transmisi data antar perangkat dalam jaringan disebut sebagai sinyal. Istilah "sinyal" digunakan untuk menggambarkan kekuatan sinyal yang diterima perangkat yang terhubung ke jaringan nirkabel.

3. Chanel atau kanal adalah Jalur komunikasi yang digunakan jaringan untuk mengirim dan menerima data dikenal sebagai saluran dalam konteks jaringan internet.
4. Security adalah menjaga kerahasiaan dan integritas data yang dikirimkan jaringan, keamanan jaringan sangat penting. Keamanan jaringan dapat dicapai melalui berbagai teknologi dan pendekatan, WPA2 (Wi-Fi Protected Access 2) adalah standar keamanan jaringan wireless yang digunakan untuk mengamankan jaringan wireless dengan menggunakan metode enkripsi yang kuat. OPEN adalah konfigurasi jaringan nirkabel yang tidak menggunakan keamanan atau enkripsi. Ini menunjukkan bahwa tidak ada kunci enkripsi atau kata sandi untuk jaringan dan siapa pun yang memiliki akses fisik dapat mengaksesnya.
5. MAC (Media Access Control) Address adalah alamat unik yang diberikan kepada setiap perangkat yang terhubung ke jaringan. Alamat ini digunakan untuk mengidentifikasi perangkat yang spesifik dalam jaringan dan membedakannya dari perangkat lain yang terhubung ke jaringan yang sama.
6. "n" dalam konteks InSSIDer merujuk ke jenis jaringan wireless yang menggunakan standar IEEE 802.11n. Standar ini meningkatkan kecepatan data hingga sekitar 300Mbps dan meningkatkan jangkauan sinyal dibandingkan dengan standar sebelumnya, seperti 802.11g.

Maka penentuan rule atau aturan sebagai berikut :

1. IF Rumah putri signal -80 chanel 11 Security Wpa2/personal and MAC Addres 802.11.n then status aman
2. IF Toko w-elektrik -25 chanel 11 security Open And MAC.Addres 802.11n then Status Tidak aman
3. IF Doraemon -75 chanel 1 security Open And MAC.Addres 802.11.n then Status Tidak aman

Tabel 3. 6 Analisis jaringan menggunakan tools InSSIDer

Elemen	**Deskripsi**	**Hasil**	**Tindakan**
Nama jaringan (SSID)	Nama dari jaringan nirkabel	w-eletrik	-
Kanal	Kanal jaringan nirkabel	6	-
Keamanan	Jenis keamanan yang digunakan	WPA2	-
Signal Strength	Kekuatan sinyal	-60dBm	-
Interference	Gangguan yang terdeteksi	Adanya jaringan yang lain pada kanal yang sama	Ganti Kanal jaringan
Kinerja	Kecepatan jaringan	5Mbps	-

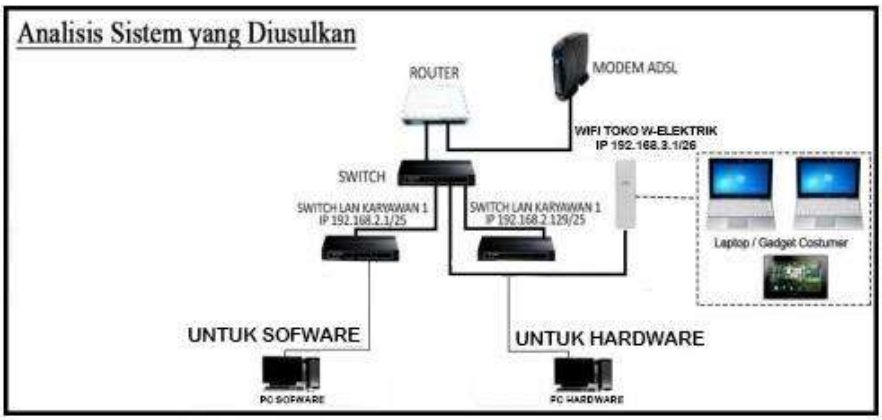
Dalam tabel diatas, setiap elemen dianalisis dan diberikan hasil dan tindakan yang diperlukan untuk mengatasi masalah yang ditemukan. InSSIDer memberikan informasi yang cukup detail mengenai jaringan yang dianalisis, seperti SSID, kanal, keamanan, signal strength, interference dan kinerja, yang dapat membantu mengidentifikasi masalah dan memberikan solusi yang tepat. Untuk menentukan apakah jaringan internet aman atau tidak, beberapa informasi dalam

tabel perlu diperiksa. Beberapa tabel dapat digunakan untuk memeriksa data apakah jaringan aman atau tidak.

3.3 Rancangan Jaringan yang Dibangun/ Diusulkan

3.4.1. Analisis Sistem yang Diusulkan

Analisis sistem yang diusulkan yaitu identifikasi celah keamanan jaringan Wi-Fi dengan tools NetStumbler mengaudit keamanan jaringan dan memblokir lalulintas jaringan yang dianggap sebagai ancaman dalam jaringan internet serta melakukan pengecekan terhadap kesalahan pada bagian media, wireless, dan media koneksinya.



Gambar 3. 3 Analisis sistem yang di usulkan

Gambar 3.3 berupa analisis sistem jaringan yang diusulkan ada beberapa komponen yang di tampilkan berupa Modem ADSL,Router,Switch, Wi-Fi Hotspot, Komputer, laptop. Sebelum peneliti menemukan analisis sistem yang diusulkan, perlu ditentukan tujuan dari jaringan tersebut dan kebutuhan yang harus dipenuhi. Kemudian, perlu dilakukan studi kelayakan untuk menentukan konfigurasi jaringan yang sesuai dan memenuhi kebutuhan tersebut. Setelah itu, perlu dilakukan analisis

kinerja jaringan untuk menentukan kapasitas yang diperlukan dan untuk mengidentifikasi potensi masalah yang mungkin terjadi.

3.4 Lokasi dan Jadwal Penelitian

3.4.1 Lokasi Penelitian

Adapun lokasi yang dijadikan tempat penelitian yaitu toko services w-elektrik batam, di Jl. Kavling Mandiri blok A no 13-14. Waktu penelitian berlangsung pada bulan September 2022 hingga Febuari 2023.

3.4.2 Jadwal Penelitian

Tabel 3. 7 Tabel Penelitian

No	Jenis Kegiatan	Bulan					
		September 2022	Oktober 2022	November 2022	Desember 2022	Januari 2023	Februari 2023
1	Studi Pustaka						
2	Penyusunan Proposal						
3	Pengumpulan Data						
4	Analisis Hasil Penelitian						
5	Penyusunan Laporan						
6	Penyerahan Hasil						
7	Hasil Sidang						

***Sumber** : (Peneliti 2022)*