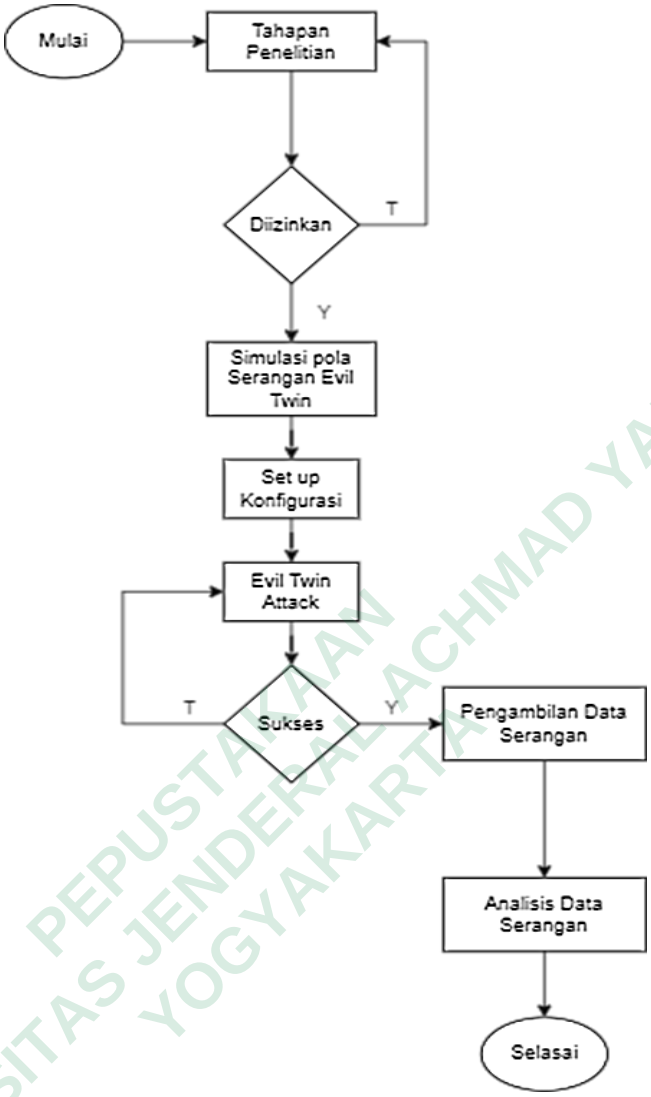
BAB 3
METODE PENELITIAN

Pada metode penelitian ini menggunkan metode *ETSniffer* (Song et al., 2010). Metode *ETSniffer* yaitu tahapan yang terdiri dari ITA (ITA adalah interval waktu antara dua paket data TCP yang berurutan yang tiba disisi pengguna), kemudian menyambungkan perangkat komputer untuk terhubung ke *Access Point ITA* dan Server IAT. Dalam penelitian ini akan melakukan modifikasi dari metode penelitian sebelumnya dengan melakukan analisis serangan *Evil Twin*. Tujuan serangan *Evil twin* untuk mengelabui pengguna dengan membuat *Access Point* palsu, sehingga pengguna tidak menyadari bahwa telah terhubung perangkatnya pada *Access Point* palsu di Gedung Universitas Jenderal Achmad Yani Yogyakarta Unit 1. Penelitian ini dilaksanakan dalam beberapa tahapan, diantaranya Tahapan Penelitian, Simulasi Pola Serangan *Evil Twin*, *Setup* Konfigurasi, *Evil Twin Attack*, Pengambilan Data Serangan, Analisis Data Serangan. Dalam pelaksanaan tahapan penelitian dibutuhkan beberapa perizinan untuk melakukan penelitian, perizinan tersebut berupa perizinan penelitian Studi Kasus Pengerjaan Skripsi dan perizinan peminjaman alat. Lalu tahap berikutnya melakukan implementasi simulasi pola serangan *Evil Twin* untuk menentukan skema serangan dan target pada jaringan nirkabel. Tahap selanjutnya mempersiapkan *setup* konfigurasi Rasberry Pi3 dan komputer. Setelah setup konfigurasi berhasil, kemudian melakukan serangan *Evil Twin*. Jika dalam melakukan serangan *Evil Twin* gagal, maka akan diulang kembali sampai serangan *Evil Twin* berhasil. Jika dalam tahapan serangan *Evil Twin* berhasil dan mendapatkan data dari pengguna yang mengakses *Access Point* palsu, maka tahapan selanjutnya menganalisis data serangan untuk mengetahui jumlah pengguna yang terjebak pada *Access Point* palsu. Untuk lebih jelas dapat dilihat pada Gambar 3.1.



Gambar 3.1 Alur Penelitian

3.1 BAHAN DAN ALAT PENELITIAN

Pada penelitian ini memerlukan beberapa alat yang akan digunakan dalam melakukan penelitian tentang analisis dan serangan jaringan nirkabel dengan *Evil Twin* di Gedung Universitas Jenderal Achmad Yani Yogyakarta Unit 1. Adapun alat yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Laptop yang spesifikasi (Ram 4GB, Processor: AMD Radeon 3, Windows 11, SSD 250GB)
2. Rasberry Pi 3

3. Tenda W311M
4. Kartu SD

3.2 JALAN PENELITIAN

Secara garis besar penelitian ini terdiri atas 4 tahap. Tahapan tahapan tersebut dilakukan guna menganalisi serangan *Evil Twin.* Berikut ini tahapan yang dilakukan dalam penelitian yaitu:

1. Tahap penelitian, pada tahapan ini ada beberapa langkah yang dilakukan diantaranya:
    a. Menentukan lokasi untuk serangan *Evil Twin* yang akan dilancarkan.
    b. Menyampaikan permohonan izin penelitian dan peminjaman alat kepada pihak yang bertanggung jawab.
    c. Memahami terhadap hukum terkait tentang tindakan ini.
2. Tahap simulasi pola serangan *Evil Twin*. Terdiri dari:
    a. Menentukan skema serangan *Evil Twin*
    b. Menentukan target atau pengguna jaringan nirkabel.
    c. Melakukan konfigurasi di Rasberry PI 3
3. Tahap uji coba dilakukan serangan *Evil Twin Attack* di Gedung Universitas Jenderal Achmad Yani Yogyakarta Unit 1 sesuai dengan target yaitu yang mengakses pada *Access Point* dengan SSID Rektorat (poin 2).
4. Tahap analisis merupakan tahap terakhir pada penelitian ini yang dilakukan dengan menggunakan *WiFi-Pumpkin*. *WiFi-Pumpkin* merupakan sekumpulan aplikasi untuk mendukung serangan *MITM* dan merebut kendali atas aliran data ke setiap pengguna yang terhubung. Tujuan dari analisis itu sendiri adalah untuk mengetahui berapa banyak pengguna yang terjebak pada *Access Point* palsu dengan *WiFi-Pumpkin* di Gedung Universitas Jenderal Achmad Yani Yogyakarta Unit 1.

Penelitian dilakukan berdasarkan tiga tahapan utama, yaitu tahap persiapan, kemudian tahap implementasi, dan yang terakhir adalah tahap analisis. Pada tahap persiapan kegiatan yang di lakukan adalah install sistem operasi untuk perangkat Raspberry Pi 3, juga melakukan konfigurasi *WiFi Pumpin 3*. untuk melakukan installasi pada perangkat tersebut membutuhkan sistem operasi Ubuntu 20.04. Untuk memindahkan sistem operasi membutuhkan MicroSD SanDisk yang berukuran 16GB, yang nantinya akan di burn. Pada penelitian versi yang digunakan adalah 20.04 karena menggunakan *Command Line Interface (CLI*) yang biasa di sebut dengan *headless interface*. Hal lain yang perlu dipersiapkan adlah terminal emulator. Terminal emulator berfungsi dalam melakukan konfigurasi lanjutan yang nantinya akan dijalankan pada perangkat komputer secara *remote*. Untuk dlalam melakuakn *remote* menggunakan perangkat lunak PuTTY. PuTTY berfungsi dalam mempermudah mengimplementasikan *WiFi Pumpkin 3* pada perangkat Raspberry Pi 3. Dalam melakukan konfigurasi *WiFi Pumpkin 3* menggunakan beberapa command line yang dijalankan.

Tahap kedua adalah tahap implementasi. Pada tahap ini hal perlu dilakukan konfigurasi jaringan di Raspberry Pi 3. Guna untuk memudahkan peretas meremote menggunkan PuTTY, setelah peretas bisa meremote *WiFi Pumpkin 3* di raspberry pi 3 maka akan melakukan penginstall lajut sebagai pendukung dalam *WiFi Pumpkin 3* yaitu menginstall Driver TP Link AC600 Archer T2u Plus untuk memudahkan peretas menggunakan *access point* yang digunakan dalam proses *Evil Twin*. Kemudian melakukan uji coba *acces point* yang akan digunakan. Sebelum melakukan uji coba *access point*, perlu melakukan pengaturan atau menduplikat ssid yang akan dijadikan target dalam serangan *Evil Twin* dan perlu mengatur *interface* untuk memilih *access point* yang akan digunakan.

Tahapan implementasi dilanjutkan dengan melakukan pengujian sistem pada Raspberry Pi 3 yang sudah terpasang aplikasi *WiFi Pumpkin 3*, yaitu sebagai aplikasi untuk melakukan serangan *Evil Twin*. Pada penelitian ini, serangan *Evil Twin* digunakan pada area gedung Universitas Jenderal Achmad Yani Yogyakarta

Unit 1 dan disematkan dalam jaringan nirkabel gedung Universitas Jenderal Achmad Yani Yogyakarta unit 1.

Pada tahapan ini, selain melakukan uji coba *acces point* palsu membutuhkan pendukung lainya yaitu menduplikasi *captive portal login* yang sama pada jaringan nirkabel di Universitas Jenderal Achmad Yani Yogyakarta supaya serangan *Evil Twin*, tidak ada yang mengetahui bahwa serangan tersebut merupakan serangan *access point* palsu. Agar proses pengambilan data dapat dilakukan perlu dipastikan proses pengujian sistem dilakukan dengan seksama sehingga sistem berjalan sesuai dengan yang direncanakan.

Tahapan terakhir yaitu melakukan analisis data dari serangan *Evil Twin* pada tanggal 15 Juni sampai dengan 22 juni 2023 denga retan waktu 1x 24 jam. Pertama-tama, tahapan analisis dimulai dengan data pydns server dan *captive portal login*. Data yang tersimpan merupakan data pengaksesan yang dilakukan pengguna pada saat menggunakan jaringan nirkabel pada gedung Universitas Jenderal Achmad Yani Yogyakarta unit 1. Monitoring dilakukan bersamaan dengan pengumpulan data akses internet pengguna yang dicatat oleh pydns server dan ditampilkan jumlah yang masuk ke captive portal login palsu. Sehingga peretas dapat melihat data tersebut secara langsung melalui *WiFi Pumpkin 3*. Data ini terdiri atas seluruh situs web yang diakses dan jumlah perangkat yang mengakses.