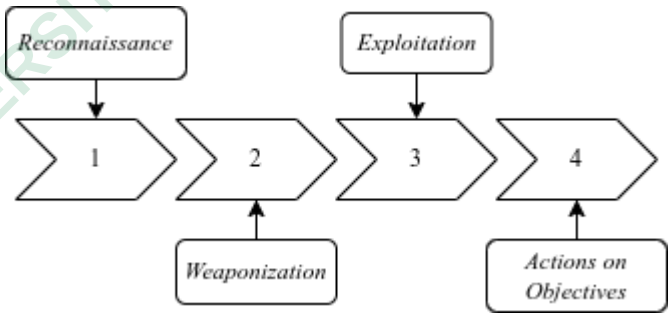
BAB 3
METODE PENELITIAN

Penelitian ini adalah penelitian rancang-bangun alat pengujian jaringan Wi-Fi berbasis Raspberry Pi dan OpenWRT yang diintegrasi untuk dapat diakses secara *remote* menggunakan Tailscale yang dapat menangkap paket data dalam format .pcap, selanjutnya dilakukan analisis paket data jaringan Wi-Fi menggunakan Arkime. Penelitian ini menggunakan jenis penelitian eksperimen dengan mengadopsi metode *Cyber Kill Chain* (CKC). Metode CKC adalah kerangka dari Lockheed Martin yang bertujuan untuk mengidentifikasi dan mencegah serangan siber (Martin, 2015). Dengan mengadopsi metode CKC untuk penelitian ini, terdapat 4 tahapan meliputi *Reconnaissance*, *Weaponization*, *Exploitation*, dan *Actions on Objectives*, sebagaimana yang ditampilkan pada Gambar 3.1.



Gambar 3.1 Tahapan Penelitian

3.1 Bahan dan Alat Penelitian

Pada penelitian ini dibutuhkan bahan dan alat untuk mendukung proses penelitian berlangsung. Berikut bahan dan alat penelitian yang diperlukan dalam penelitian ini sebagaimana ditampilkan pada poin 3.1.1 dan 3.1.2.

3.1.1 Bahan Penelitian

Bahan penelitian yang digunakan adalah paket data jaringan Wi-Fi dalam format .pcap. Paket data dalam format .pcap ini didapat ketika alat pengujian melakukan penangkapan lalu lintas jaringan yang selanjutnya paket data ini diteruskan ke dalam Arkime untuk proses analisis.

3.1.2 Alat Penelitian

Alat penelitian merupakan perangkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan selama proses penelitian. Pada alat penelitian yang digunakan terbagi menjadi 3 bagian meliputi *Controller*, *Agent*, dan *Analyzer*. *Controller* adalah komponen pusat kendali yang bertugas untuk mengatur jalannya proses pengujian, mengirim perintah ke *Agent*, dan mengelola hasil analisis dari *Analyzer*. *Agent* adalah komponen yang dirancang untuk menjalankan proses dari pengujian pada penelitian ini. *Analyzer* adalah komponen yang dapat melakukan identifikasi dan analisis terhadap paket data yang digunakan dalam penelitian ini. Berdasarkan 3 bagian tersebut, berikut alat – alat yang digunakan dalam penelitian ini:

1. Laptop merek HP-EliteBook-840-G1 dengan *processor* Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz RAM 8GB (*Controller*)

   Laptop tersebut digunakan penguji untuk melakukan pengujian keamanan jaringan Wi-Fi dengan cara menangkap dan menganalisis paket data .pcap. Selain itu, Laptop berfungsi sebagai perangkat utama untuk mengakses dan mengelola Raspberry Pi yang terintegrasi dengan OpenWRT

melalui koneksi Tailscale serta menyimpan hasil data pengujian yang diperlukan dalam proses analisis dan dokumentasi penelitian.

2. *Smartphone* (*Controller*)

   Smartphone digunakan penguji untuk melakukan *scan barcode* pada saat identifikasi jaringan Wi-Fi sebagai objek penelitian.

3. Sistem pengoperasian Linux Mint 22 Wilma (*Controller*)

   Sistem pengoperasian Linux Mint 22 Wilma digunakan penguji sebagai sistem pengoperasian utama pada Laptop yang dipakai untuk semua kebutuhan penelitian.

4. Raspberry Pi 4 Model B (*Agent*)

   Raspberry Pi 4 Model B digunakan penguji sebagai perangkat keras (*hardware*) untuk integrasi OpenWRT dan sebagai alat pengembangan dalam penelitian.

5. OpenWRT (*Agent*)

   OpenWRT digunakan sebagai sistem operasi untuk mengubah perangkat keras Raspberry Pi menjadi Router dan *Access Point* (AP) untuk mendukung proses pengembangan alat pada penelitian ini

6. Tailscale (*Agent*)

   Tailscale digunakan sebagai penghubung antara perangkat keras Raspberry Pi yang diinstall OpenWRT dengan laptop penguji melalui teknologi Mesh VPN sehingga OpenWRT dapat diakses secara *remote*.

7. *Tcpdump* (*Agent*)

   Tcpdump digunakan untuk menangkap (*capture*) paket data pada jaringan Wi-Fi selama proses pengujian.

8. Server (*Agent*)

Server dengan sistem pengoperasian Ubuntu Server 22.04.5 LTS, virtual CPU 6 *Core*, virtual RAM 12GB, dan *storage* 60GB digunakan untuk proses instalasi dan konfigurasi Arkime.

9. *Secure Shell File System* (SSHFS) (*Agent*)

SSHFS digunakan untuk mengakses file yang tersimpan di server sehingga dapat dikelola langsung dari perangkat lokal melalui koneksi *Secure Shell* (SSH). Hal ini dilakukan untuk melakukan tangkapan data yang langsung disimpan di server selama proses pengujian.

10. SD *Card* 128GB (*Agent*)

SD *Card* dengan kapasitas 128GB digunakan untuk menyimpan data instalasi OpenWRT yang dijalankan pada perangkat keras Raspberry Pi.

11. *Card Reader* (*Agent*)

Card Reader digunakan untuk menstransfer data instalasi OpenWRT dari laptop ke SD *Card* sebelum digunakan pada perangkat keras Raspberry Pi.

12. Modem *Global System for Mobile Communication* (GSM) (*Agent*)

Modem GSM digunakan sebagai sumber koneksi internet berbasis jaringan seluler dengan menggunakan kartu *Subscriber Identity Module* (SIM) untuk dipasang pada perangkat keras Raspberry Pi yang menjalankan OpenWRT.

13. Kartu *Subscriber Identity Module* (SIM) (*Agent*)

Kartu SIM digunakan untuk menyediakan akses koneksi internet melalui Modem GSM yang terpasang pada perangkat keras Raspberry Pi

14. IP5310 Modul *Power Bank* (*Agent*)

Modul *Power Bank* dengan spesifikasi IP5310 digunakan untuk menyediakan sumber daya listrik portabel yang stabil dan efisien dalam mendukung proses pengujian selama penelitian

15. Baterai Sony ORD 18650 22000mAh 4.2V Li-ion (*Agent*)

Baterai Sony ORD 18650 dengan kapasitas 22000mAh dan tegangan 4.2V tipe Li-ion digunakan untuk menyuplai daya listrik secara stabil pada perangkat keras Raspberry Pi agar dapat beroperasi selama proses pengujian.

16. USB *Image Writer* (*Agent*)

USB *Image Writer* digunakan penguji untuk melakukan proses *burning file image* OpenWRT pada SD Card berkapasitas 128GB.

17. Kabel *Local Area Network* (LAN) (*Agent*)

Kabel LAN digunakan sebagai media penghubung antara Raspberry Pi, Laptop, dan Router pada saat dilakukan proses konfigurasi OpenWRT.

18. WiGLE Wi-Fi (*Analyzer*)

WiGLE Wi-Fi digunakan sebagai alat untuk mendukung proses analisis dan identifikasi jaringan Wi-Fi yang dijadikan objek penelitian.

19. Arkime (*Analyzer*)

Arkime digunakan sebagai alat untuk mendukung proses analisis paket data jaringan Wi-Fi dalam penelitian ini.

3.2 Jalan Penelitian

Jalan penelitian berisi tahapan dari penelitian yang dilakukan dengan mengadopsi metode *Cyber Kill Chain* (CKC) untuk pengujian sistem yang dibangun. Tahapan dari metode CKC yang diadopsi terdiri dari 4 tahapan yang dapat dilihat pada Gambar 3.1.

Gambar 3.1 menunjukkan 4 tahapan yang dilakukan pada penelitian ini untuk mengembangkan alat uji keamanan jaringan Wi-Fi berbasis Raspberry Pi dan OpenWRT dengan menerapkan teknik *Evil Twin Attack* untuk menangkap paket data dalam format .pcap yang dilakukan secara *remote* menggunakan Tailscale, selanjutnya akan dilakukan analisis paket data jaringan Wi-Fi menggunakan Arkime. Pengujian dilakukan di Kampus 1 Universitas Jenderal

Achmad Yani Yogyakarta. Sementara itu, 4 tahapan yang dilakukan dalam penelitian ini, sebagai berikut:

1. *Reconnaissance* (Pengintaian), tahap ini dilakukan dengan beberapa langkah, diantaranya:
   a) Menentukan jaringan Wi-Fi yang dijadikan objek penelitian.
   b) Mengajukan permohonan izin penelitian kepada pihak terkait di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta.
   c) Mencari informasi dan mengidentifikasi jaringan Wi-Fi yang dijadikan objek penelitian.
2. *Weaponization* (Persiapan Alat Uji dan Sistem Pengujian), tahap ini dilakukan dengan beberapa langkah, diantaranya:
   a) Mempersiapkan alat dan bahan untuk mendukung proses penelitian.
   b) Membangun sumber daya berbasis Baterai dan IP5310 Modul *Power Bank* sebagai sumber daya untuk alat uji selama proses pengujian.
   c) Merancang dan membangun alat uji jaringan Wi-Fi berbasis Raspberry Pi yang dikonfigurasikan dengan OpenWRT dengan teknik *Evil Twin Attack* untuk pembuatan *Service Set Identifier* (SSID) palsu yang dikendalikan secara *remote* menggunakan Tailscale agar alat uji dapat dikendalikan jarak jauh menggunakan internet.
   d) Mengintegrasikan Arkime pada Server agar dapat menerima, memproses, menyimpan dan menganalisis paket data jaringan Wi-Fi dalam format .pcap.
   e) Melakukan *mounting Secure Shell File System* (SSHFS) pada Laptop agar dapat menerima dan mengirimkan file ke Arkime Server.
3. *Exploitation* (Eksploitasi atau Pengujian), tahap ini dilakukan dengan beberapa langkah, diantaranya:

a) Pengujian dilakukan pada jaringan Wi-Fi pada Lantai 1, Lantai 2, Lantai 3, Lantai 4, dan Gazebo di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta dengan SSID bernama "UNJAYA".
b) Alat uji yang sudah dirancang diaktifkan dan diletakkan pada tempat pengujian.
c) Penguji melakukan *remote* terhadap alat uji menggunakan Tailscale dari mana saja melalui koneksi internet.
d) Penguji dapat melihat perangkat korban yang terhubung ke SSID palsu. Ketika ada perangkat dari korban yang terhubung ke SSID palsu maka penguji melakukan penangkapan paket data dengan menggunakan *tools tcpdump*.
e) Penangkapan paket data dilakukan dalam format .pcap dan tersimpan ke Arkime Server melalui *mounting Secure Shell File System* (SSHFS).
f) Paket data dalam format .pcap yang sudah tersimpan di Arkime Server akan diproses ke *Elasticsearch* yang merupakan *database* dari Arkime agar dapat ditampilkan di Arkime *Viewer* oleh penguji.
g) Pengujian dilakukan selama sumber daya baterai habis di setiap masing – masing lokasi pengujian.

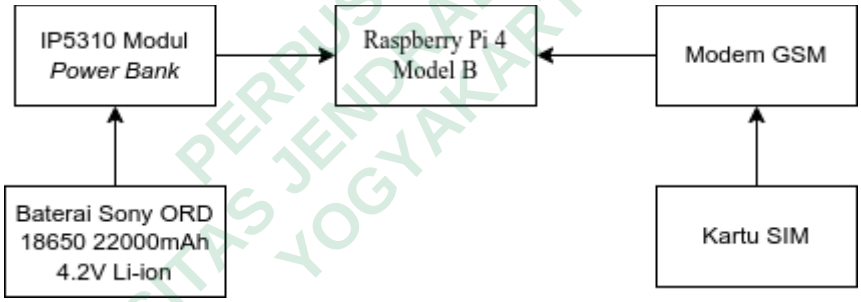
4. *Actions on Objectives* (Tindakan untuk Tujuan Akhir), tahap ini dilakukan dengan tujuan akhir dalam penelitian ini yaitu analisis paket data jaringan Wi-Fi yang telah dilakukan pada tahap *Exploitation*. Paket data yang telah diproses dan ditampilkan di Arkime *Viewer* akan dianalisis oleh penguji dengan tujuan mengidentifikasi jumlah korban yang terjebak ke jaringan Wi-Fi palsu dan mengidentifikasi protokol yang rentan atau berbahaya. Protokol yang rentan atau berbahaya tersebut diidentifikasi oleh penguji untuk mencari data sensitif dari korban seperti *username* dan *password*.

3.3 Rancangan Sistem

Selanjutnya pada subbab ini menjelaskan mengenai rancangan sistem yang dikembangkan dari solusi terhadap permasalahan yang telah diuraikan pada bab sebelumnya. Rancangan sistem mencakup diagram blok pengembangan alat dan topologi sistem yang dapat dilihat pada Gambar 3.2 dan Gambar 3.3.

3.3.1 Diagram Blok Pengembangan Alat

Diagram blok pengembangan alat adalah gambaran umum mengenai susunan komponen perangkat keras dan alur kerja sistem secara keseluruhan untuk pengembangan alat dalam penelitian ini. Diagram blok ini bertujuan untuk menunjukkan bagaimana setiap komponen saling terintegrasi dalam satu kesatuan sistem. Diagram blok pengembangan alat dapat dilihat pada Gambar 3.2.



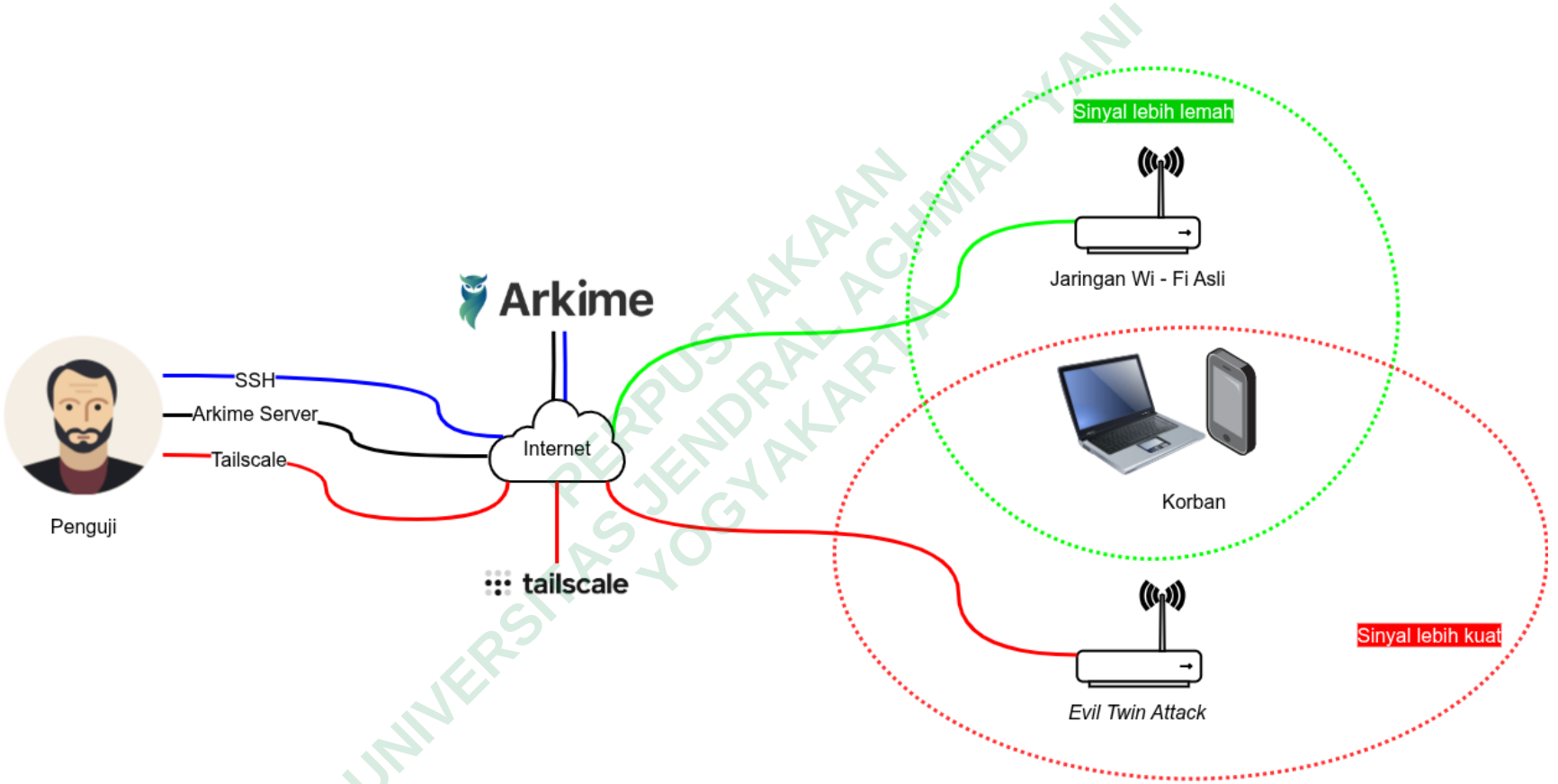
Gambar 3.2 Diagram Blok Pengembangan Alat

Gambar 3.2 menunjukan rangkaian untuk pengembangan alat dari penelitian ini yang terdiri dari 5 komponen utama. Baterai Sony ORD 18650 dengan kapasitas 22000mAh dan tegangan 4.2V Li-ion digunakan sebagai sumber daya pada Raspberry Pi secara portabel. IP5310 Modul *Power Bank* digunakan untuk mengatur dan mengalirkan tegangan dari Baterai ke Raspberry Pi serta digunakan untuk pengisian daya Baterai. Modem *Global System for Mobile Communication* (GSM) digunakan untuk menghubungkan Raspberry Pi ke jaringan seluler GSM agar mendapatkan koneksi internet dengan menggunakan Kartu *Global System for Mobile Communication* (SIM) untuk mendapatkan

jaringan operator. Raspberry Pi 4 Model B digunakan sebagai pusat kendali (otak sistem) untuk memproses dan menjalankan sistem pengoperasian serta alat atau *tools* yang diperlukan dalam proses pengujian.

3.3.2 Topologi Sistem Pengujian

Topologi sistem pengujian adalah gambaran seluruh komponen dari perangkat keras (*hardware*) dan perangkat lunak (*software*) yang saling terintegrasi untuk menjalakan proses pengujian keamanan jaringan Wi-Fi dalam penelitian ini. Gambaran topologi sistem pengujian dalam penelitian ini dapat dilihat pada Gambar 3.3.



Gambar 3.3 Topologi Sistem Pengujian

Gambar 3.3 menujukkan seluruh komponen saling terintegrasi untuk melakukan pengujian keamanan jaringan Wi-Fi yang dimana dikendalikan secara *remote* oleh penguji. Penguji melakukan *remote* menggunakan Tailscale pada OpenWRT yang sudah terintegrasi dengan Raspberry Pi untuk membuat jaringan Wi-Fi palsu. Pada jaringan Wi-Fi palsu menggunakan Modem GSM untuk memberikan internet pada jaringan Wi-Fi palsu yang sudah dibuat. Ketika penguji berhasil mengakses OpenWRT dan membuat jaringan Wi-Fi palsu maka ketika sinyal pada jaringan Wi-Fi palsu lebih kuat, perangkat pengguna atau korban akan terhubung. Ketika korban terhubung maka penguji melakukan penangkapan lalu lintas jaringan Wi-Fi melalui *mounting* SSH *File System* dan alat atau *tools tcpdump* untuk mendapatkan paket data dalam format .pcap dan menyimpannya pada Arkime Server. Pada saat penguji berhasil mendapatkan paket data dalam format .pcap yang tersimpan di Arkime Server maka paket data tersebut akan diproses melalui Arkime Server ke *Elasticsearch* untuk menyimpan paket data dan proses analisis serta identifikasi paket data jaringan Wi-Fi pada Arkime *Viewer*.