BAB 3
METODE PENELITIAN

Penelitian ini menerapkan metode pengumpulan dan analisis data jaringan dengan teknik *Port Mirroring*. Alat dan bahan yang dipakai meliputi switch jaringan yang mendukung fitur *Port Mirroring*, perangkat lunak tcpdump untuk menangkap data dalam format PCAP, dan DynamiteLab untuk melakukan analisis lebih mendalam.

3.1 BAHAN DAN ALAT PENELITIAN

File PCAP merupakan format yang digunakan untuk menyimpan data trafik jaringan yang diperoleh melalui teknik *Port Mirroring*. Data dalam format PCAP menjadi komponen utama dalam analisis penelitian ini, memungkinkan pemeriksaan secara detail terhadap pola trafik dan potensi ancaman.

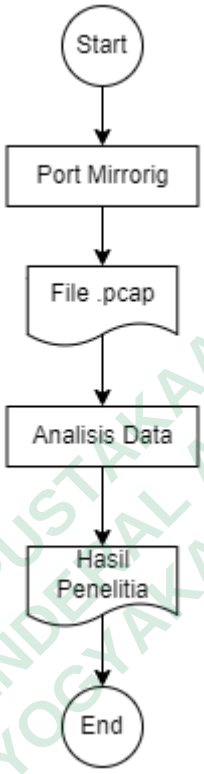
Alat yang digunakan dalam penelitian ini adalah komputer dengan spesifikasi yang memadai untuk menjalankan sistem operasi dan pengembangan perangkat lunak serta konektivitas Internet.

1. Laptop

   Sistem operasi : *Windows 11 Home Single Language 64 bit*
   Processor : *Intel® Core™ i5-8250U*
   RAM : 4 GB
   SSD : 256 GB
2. Tcpdump alat baris perintah yang digunakan untuk menangkap dan menyimpan data lalu lintas jaringan dalam format PCAP. Alat ini memungkinkan pengumpulan data secara langsung dari jaringan yang terhubung ke switch.
3. DynamiteLab perangkat lunak yang digunakan untuk melakukan analisis mendalam terhadap file PCAP yang dihasilkan oleh tcpdump. Alat ini membantu dalam mendeteksi aktivitas mencurigakan melalui berbagai fitur analisi.

3.2 JALAN PENELITIAN

Pada Gambar 3.1 menunjukkan diagram alur penelitian yang menggambarkan langkah-langkah dari pengaturan Port Mirroring hingga penulisan laporan akhir.



Gambar 3.1 Alur Penelitian

Jalan penelitian ini melibatkan langkah-langkah berikut untuk menganalisis trafik jaringan di Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA):

1. Pengaturan *Port Mirroring* : *Port Mirroring* dikonfigurasi pada switch jaringan di Kampus 1 UNJAYA untuk menangkap seluruh trafik jaringan yang relevan..
2. Pengumpulan Data : Pada langkah ini, trafik jaringan ditangkap menggunakan tcpdump dalam jangka waktu tertentu dan disimpan dalam format PCAP. Dalam penelitian ini, data yang dikumpulkan selama 8 detik menghasilkan file berukuran 70 MB dengan 84.311 paket. Mengingat batasan ukuran file unggahan DynamiteLab yang

maksimal 75 MB, periode pengumpulan data disesuaikan untuk memastikan efisiensi analisis.

3. Analisis Data : Dalam langkah ini, File PCAP yang terkumpul diunggah dan dianalisis menggunakan DynamiteLab. Tujuannya untuk mengidentifikasi pola trafik, mendeteksi anomali, dan mengungkap potensi ancaman keamanan.
4. Evaluasi dan Validasi : Akurasi deteksi DynamiteLab diuji dengan membandingkan hasil analisis terhadap data jaringan yang dianggap normal. Teknik cross-check digunakan untuk memverifikasi temuan dari DynamiteLab, memastikan bahwa deteksi anomali dan ancaman yang teridentifikasi relevan dan akurat.
5. Penulisan Laporan : Langkah terakhir adalah menyususn laporan yang menjelaskan metodologi, hasil, dan analisis penelitian secara rinci, serta merumuskan kesimpulan.