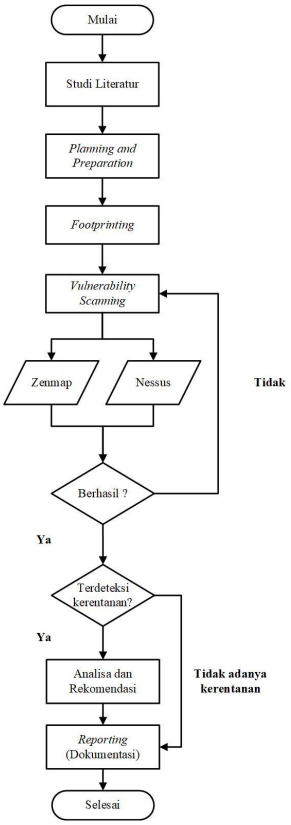
BAB 3
METODOLOGI PENELITIAN

Jenis penelitian ini menggunakan metodologi kuantitatif untuk penyelidikan. Menentukan fokus penelitian pada server web repository IT Telkom Purwokerto, mengidentifikasi dan mendefinisikan permasalahan, melakukan uji coba, dan menganalisis hasil yang dilakukan. Langkah-langkah tersebut antara lain studi literatur, *planning and preparation*, *footprinting, Vulnerabilities scanning,* menganalisis hasil, dan *reporting.*



Gambar 3.1 Diagram Alir Penelitian

3.1. Studi Literatur

Pada tahap awal, studi literatur dilakukan untuk menjelaskan tinjauan literatur terhadap teori-teori pendukung yang mendasari pengembangan penelitian. Kegiatan ini dilakukan melalui membaca buku, jurnal, artikel, laporan penelitian, dan *website*.

3.2. Planning and Preparation

Dalam penelitian ini membuat perencanaan tindakan (*Action Planning*) Pada langkah ini, peneliti melakukan pemahaman masalah utama dan merumuskan rencana tindakan yang efektif untuk mengatasinya. Berikut persiapan dalam pengumpulan data, alat dan bahan yang digunakan, yaitu:

A. Pengumpulan Data

1. Menentukan lokasi penelitian yaitu di IT Telkom Purwokerto.
2. Menentukan *Website* yang diteliti yaitu repository Institut Teknologi Telkom Purwokerto
3. Melakukan koordinasi, dan permohonan izin terhadap unit SISFO dan unit Perpustakaan Institut Teknologi Telkom Purwokerto

B. Perangkat Keras (*Hardware*)

Tabel 3.1 Spesifikasi *Hardware* yang digunakan

Spesifikasi	
Processor	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz
RAM	10.0 GB
Hardisk	1 TeraByte

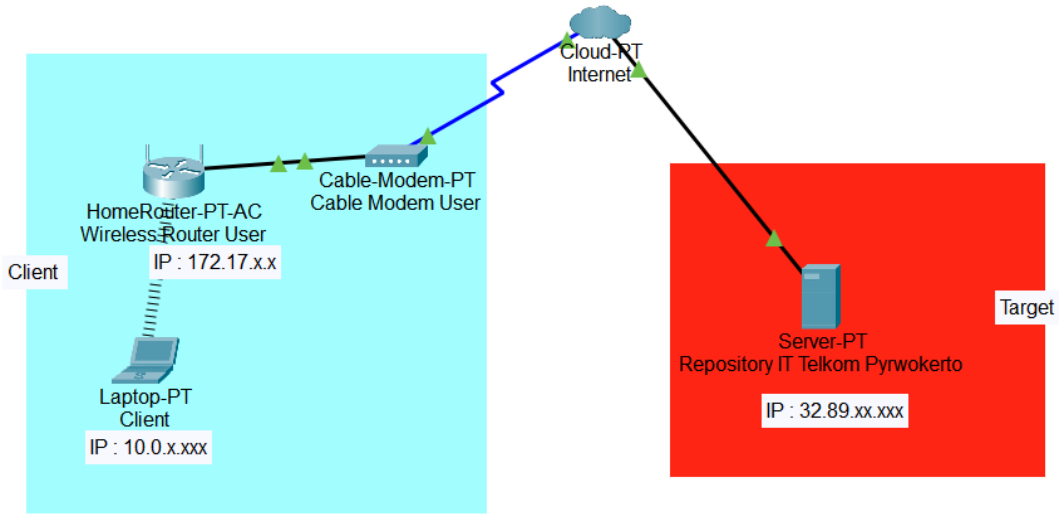
C. Perangkat Lunak (*Software*)

Tabel 3.2 Spesifikasi *Software* yang akan digunakan

No	***Software***	**Fungsi**
1.	Oracle VM VirtualBox	Solusi virtualisasi, dirancang untuk server, desktop, dan aplikasi tertanam, memudahkan pengguna dan administrator untuk menjalankan banyak sistem operasi tamu pada satu host.

No	*Software*	Fungsi
2.	Kali Linux	*Open-Source* berbasis Debian yang ditujukan untuk Pengujian Penetrasi dan Audit Keamanan
3.	Zenmap (Nmap)	Alat pemindaian jaringan digunakan untuk menyelidiki perangkat jaringan, server, dan host untuk *port* TCP atau UDP yang terbuka
4.	Nessus	Perangkat lunak pemindaian kerentanan, berfokus pada akses jarak jauh, kesalahan konfigurasi, dan DoS terhadap tumpukan TCP/IP.

D. Topologi Jaringan



Gambar 3.2 Topologi Jaringan

Berdasarkan Gambar 3.2 bahwa topologi jaringan yang digunakan adalah topologi star, dengan satu perangkat titik pusat yang menggambarkan sistem jaringan yang digunakan untuk memudahkan dan memahami prinsip-prinsip dalam penelitian ini. Pada *core network,* dimana *Repository* Server IT Telkom

Purwokerto dengan ip 32.89.xx.xxx serta *client* yang nantinya akan melakukan prosedur pengujian.

3.3. Footprinting

Data penelitian ini berkaitan dengan website dan server yang berada pada alamat http://repository.ittelkom-pwt.ac.id/ . Tahap ini mengumpulkan informasi sebanyak mungkin tentang inventaris jaringan [22]. Berikut barometer metodologi yang digunakan :

1. Ping *(Packet Internet Groper)*. Perintah ini mengambil sebagai input alamat IP atau URL dan mengirimkan paket data ke alamat yang ditentukan dengan pesan "PING" dan mendapat respons dari server/host kali ini direkam yang disebut latency.

Gambar 3.3 Pengujian Ping

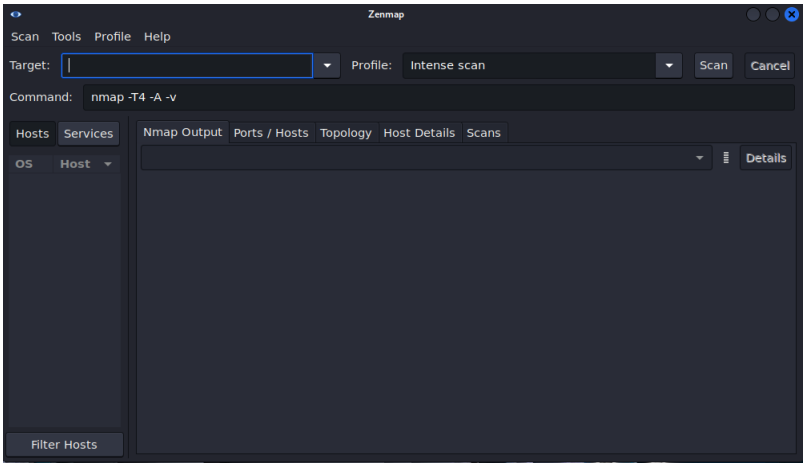
2. *Whois*, protokol permintaan yang didasarkan pada TCP, sering digunakan untuk menawarkan layanan informasi kepada pengguna Internet.

Gambar 3.4 Pengujian *Whois*

3. *Nslookup*, perintah yang berguna untuk mengumpulkan informasi dari server DNS

Gambar 3.5 Pengujian *Nslookup*

4. *Scanning port*, metode aplikasi yang dimaksudkan untuk memeriksa *port host* atau *server* yang terbuka. Administrator sering menggunakan aplikasi untuk menguji keamanan jaringan.



Gambar 3.6 Pengujian *Scanning Port*

3.4. Vulnerabilities Scanning

Tahap pemindaian kerentanan ini memeriksa target untuk keberadaan kerentanan. Ini harus mencakup semua sistem manajemen, server, dan perangkat yang terhubung ke jaringan. Tujuan pemindaian kerentanan untuk mengidentifikasi kerentanan baru atau yang sudah ada untuk mengurangi atau menghilangkan risiko terkait[22]. Perangkat lunak yang digunakan untuk melakukan *Vulnerabilities Scanning* yaitu Nessus.

3.5. Analisa dan Rekomendasi

Tahapan dalam analisis adalah mengumpulkan data yang dibutuhkan dalam teknik analisis Kerentanan. Nessus dan Zenmap melakukan pemindaian kerentanan dalam bentuk kerentanan IP. Selain itu, memberikan solusi untuk mengatasi kerentanan data yang diperoleh.

3.6. Reporting (Dokumentasi)

Tahap ini dirancang untuk membantu penguji dalam mengidentifikasi dan mendokumentasikan data sensitif, hasil konfigurasi, dan hubungan dengan perangkat jaringan lain yang dapat dimanfaatkan untuk akses lebih lanjut[22].
Pada tahap ini kegiatan yang dilakukan adalah sebagai berikut:.

1. Menyiapkan laporan aktivitas yang merinci tahapan, sumber, alat, dan status.

2. Menyerahkan file laporan ke pihak sistem informasi repository.ittelkom-pwt.ac.id untuk dilakukan tindaklanjut terhadap penemuan terhadap *vulnerability* website tersebut.