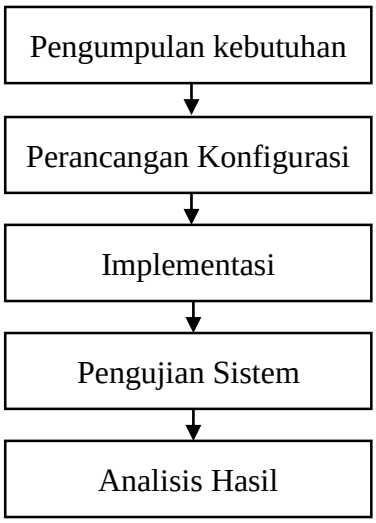
BAB III
METODE PENELITIAN

3.1 Subjek dan Objek Penelitian

Subjek penelitian ini merupakan penerapan sistem HoneyPy dengan Maltrail menggunakan analisis deskriptif dan objek penelitian ini yaitu server CentOs sebagai server tambahan dan Linux Mint sebagai server utama yang diberi pertahanan HoneyPy serta diharapkan dengan adanya sistem keamanan yang berupa HoneyPy dan Maltrail ini akan mengurangi risiko penyerangan terhadap server maupun pengguna.

3.2 Diagram Alir Penelitian

Pada penyusunan tugas akhir ini peneliti melakukan beberapa tahapan penelitian yang sudah ditentukan. Berikut merupakan gambar tahapan yang dilakukan peneliti untuk menyusun tugas akhir ini:



Gambar 3.1 Diagram Alir Penelitian

3.2.1 Studi Literatur

Dalam penelitian ini, peneliti menggunakan studi literatur dengan mencari dan mempelajari berbagai informasi tentang sistem operasi Linux, HoneyPy, Maltrail dan macam-macam serangan pada server melalui referensi makalah, jurnal ilmiah, buku

elektronik (ebook), dokumentasi internet, paper, website, dan tugas akhir mahasiswa lain yang memiliki kesamaan topik pembahasan.

3.2.2 Metode Penelitian

Penelitian ini merupakan penelitian penerapan implementasi metode mengamankan sebuah server dari peretasan dengan menggunakan *virtual machine* yaitu HoneyPy dengan Maltrail. Pendekatan yang digunakan dalam penelitian ini dengan penulis melakukan pengumpulan kebutuhan, perancangan konfigurasi, implementasi, pengujian sistem, dan analisis hasil.

3.3 Pengumpulan Kebutuhan

Adapun yang dibutukan untuk merancang sistem yaitu :

a) Perangkat Keras (Hardware):

1. Laptop ASUS dengan spesifikasi:

   Processor : Intel Core i7

   Memory : RAM 12 GB

   HDD : 1 TB

   VGA : NVIDIA GEFORCE 940M

b) Perangkat Lunak (Software):

1. OS Windows 10 Pro 64-bit
2. **V**irtualBox
3. OS VM Kali Linux, OS VM CentOs dan OS VM Linux Mint

3.4 Perancangan Konfigurasi

Tahap perancangan sistem merupakan tindak lanjut terhadap data yang diperoleh. Pada tahap perancangan konfigurasi sistem yaitu membuat server utama dengan OS Linux Mint serta konfigurasi HoneyPy dengan Maltrail sebagai tempat menampung serangan terhadap Kali Linux serta dapat menangkap aktivitas serangan menggunakan Maltrail dan juga hasil analisis deskriptif yang ditampilkan.

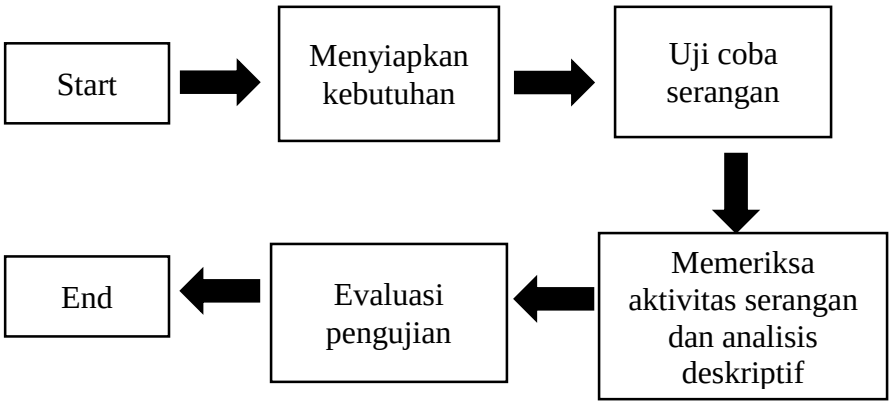
3.5 Implementasi

Tahap ini merupakan tahap tindak lanjut dari perancangan sistem. Berikut merupakan langkah-langkah pembangunan infrastruktur yang akan diimplementasikan:

1) **Instalasi VirtualBox**
2) **Instalasi VM OS Kali Linux, CentOs, dan Linux Mint**
3) **Instalasi dan Konfigurasi HoneyPy pada LinuxMint**
4) **Instalasi dan Konfigurasi Maltrail pada LinuxMint**

3.6 Pengujian Sistem

Dalam penelitian ini dilakukan pengujian sistem yang telah dibangun. Tujuan dari pengujian sistem untuk mengetahui apakah sistem yang dibangun sudah sesuai ataupun adanya kekurangan. Berikut diagram alir pengujian yang dilakukan oleh peneliti:



Gambar 3.2 Diagram Alir Pengujian

1. Menyiapkan kebutuhan berupa *tools* yang digunakan maupun perangkat-perangkat yang sudah dicantumkan pada pengumpulan kebutuhan.
2. Uji coba serangan berupa melakukan serangan dari OS Kali Linux ke OS CentOs dan OS Linux Mint yang tidak diberi maupun sudah diberi pertahanan honeypot. Adapun 3 serangan yang dilakukan dalam penelitian antara lain sebagai berikut:

a) Pengujian *scanning* dengan NMAP yang sebelum dan sesudah diberikan HoneyPy

- Gunakan *command* untuk *scanning* di OS Kali Linux

```
nmap –n –script=vuln <target IP Address>
```

b) Pengujian dengan DoS menggunakan PING yang sudah diubah packetsize "-s 65000"

- Gunakan *command* untuk menjalankan tool tersebut di OS Kali Linux

```
ping <target IP Address> -s 65000
```

c) Pengujian dengan DoS menggunakan serangan *hping3*

- Gunakan *command* untuk menjalankan *tool* tersebut pada Kali Linux

```
sudo hping3 -S <IP penyerang> -a <target IP Address> -flood
```

3. Memeriksa aktivitas serangan berupa pengecekan log pada HoneyPy dengan Maltrail yang dianalisis menggunakan analisis deskriptif untuk menganalisa serangan yang dilakukan terhadap server. Adapun analisis yang dilakukan sebagai berikut:

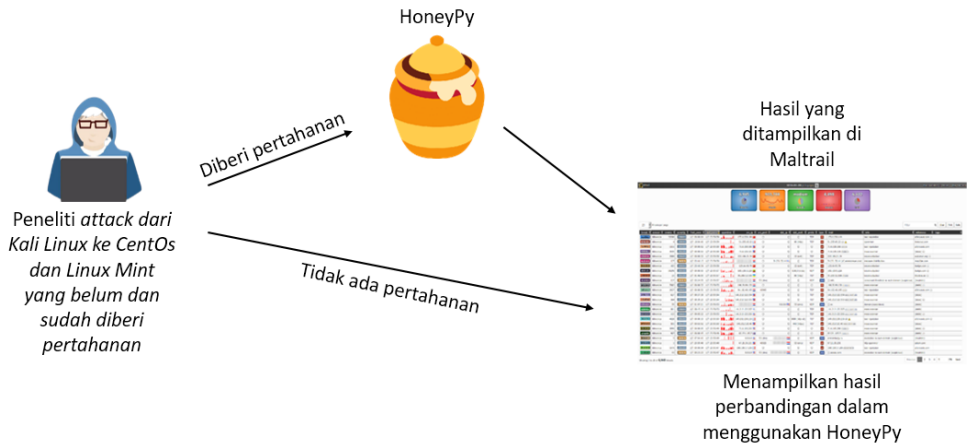
a) Pengambilan data dari Maltrail.

b) Dibandingkan antara serangan yang diberikan maupun tidak diberikan pertahanan HoneyPy.

c) Menyajikan gambar yang didapatkan pada Maltrail.

4. Evaluasi pengujian berupa tahap melakukan perbaikan dalam pengujian yang dilakukan pada sistem. Jika uji coba sudah berjalan dengan baik, tahap selanjutnya yaitu melakukan analisis hasil.

3.7 Analisis Hasil



Gambar 3.3 Simulasi Gambar

Pada tahap ini peneliti melakukan analisis terhadap pengujian yang sudah dilakukan sehingga memperoleh hasil dari pengujian tersebut yaitu seperti pada gambar 3.3 peneliti melakukan uji coba beberapa serangan yang dilakukan bagian awal pengujian dengan scanning Nmap mendapatkan port yang berbeda pada sebelum dan sesudah menggunakan HoneyPy serta akan ditangkap hasilnya pada Maltrail. Bagian kedua pengujian dengan DoS menggunakan PING yang diberi *packetsize* serta mendapatkan hasil serangan yang sudah dapat dilihat pada Maltrail juga, serangan tersebut prinsipnya membanjiri sumber daya target dengan PING yang umumnya mengirim paket secepat mungkin tanpa menunggu balasan sehingga mengakibatkan perlambatan sistem secara keseluruhan yang signifikan. Bagian akhir pengujian dengan DoS menggunakan serangan *hping3* mendapatkan hasil serangan juga yang bisa dilihat pada Maltrail, *hping3* merupakan serangan yang sangat bertarget serta dapat membanjiri sehingga memungkinkan dapat menjatuhkan server. Kemudian serangan tersebut akan dibandingkan dengan yang belum diberikan pertahanan HoneyPy maupun yang sudah diberikan.

Serangan-serangan yang dilakukan oleh peneliti akan di analisis hasilnya menggunakan deskriptif yang datanya diambil pada maltrail guna untuk mendeteksi

serangan yang sudah dilakukan pada pengujian sehingga mendapatkan hasil. Batas kecepatan yang membatasi jumlah permintaan yang dapat diperoleh server dalam jangka waktu tertentu, yaitu pendekatan umum untuk mengurangi serangan DoS. Meskipun ini merupakan strategi yang efektif, namun gagal ketika dihadapkan dengan serangan yang lebih besar dan lebih rumit. Oleh karena itu, peneliti mencoba melakukan uji coba secara virtual.

3.8 Jadwal Penelitian

Berikut ini adalah jadwal pelaksanaan kegiatan penulis lakukan yang dapat dilihat pada table berikut ini :

No	Jenis Kegiatan	Bulan Juni				Bulan Juli				Bulan Agustus				Bulan November				Bulan Desember				Bulan Januari				Indikator
		Minggu ke -				Minggu ke -				Minggu ke -				Minggu ke -				Minggu ke -				Minggu ke -				
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
Tahap I																										
1	Penentuan ide																									Menemukan tema yang sesuai
2	Perumusan masalah																									Kualifikasi sebuah masalah
3	Studi literatur																									Relevansi referensi penelitian
4	Penyusuan proposal																									Menyusun draft proposal
5	Seminar proposal																									Seminar TA 1
6	Revisi proposal																									Perbaikan draft proposal
Tahap II																										
7	Perancangan sistem																									Konfigurasi HoneyPy dan Maltrail

8	Pengujian sistem																								Hasil pengujian
9	Analisis pembahasan																								Menganalisis hasil
10	Publikasi jurnal nasional																								Jurnal nasional telah di submit
11	Penyusuan laporan TA																								Draft laporan TA

Tabel 3.1 Jadwal Penelitian