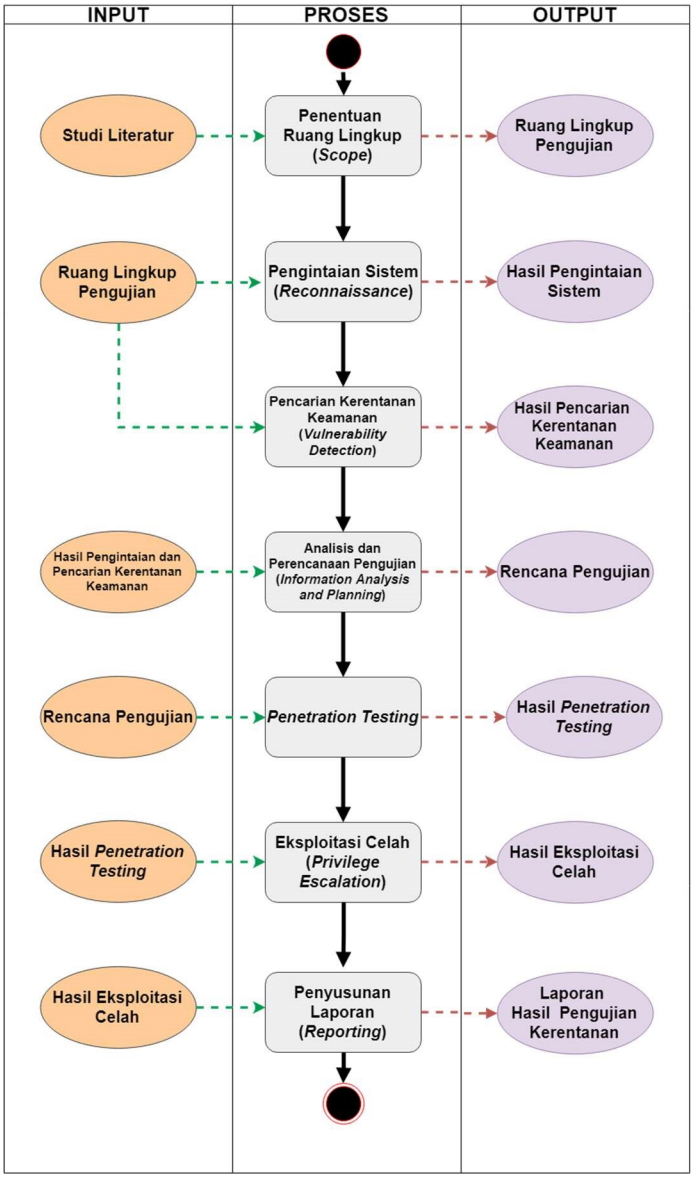
BAB III

METODOLOGI PENELITIAN

3.1. Metode Penelitian

Berikut ini pada **Gambar 3.1** merupakan Tahapan Penelitian yang digunakan oleh peneliti:



Gambar 3. 1 Tahapan Penelitian

Dalam penelitian ini menggunakan kerangka kerja VAPT (*Vulnerability Assessment and Penetration Testing*) digunakan untuk menguji keamanan pada Web KRS Daring (Kartu Rencana Studi Daring).

3.1.1. Studi Literatur

Pada langkah awal penulis melakukan studi literatur terkait kerangka kerja yang digunakan yaitu VAPT (*Vulnerability Assessment and Penetration Testing*), selanjutnya hasil dari studi literatur adalah pengetahuan bagi peneliti untuk menjadi gambaran dari ruang lingkup pengujian.

3.1.2. Penentuan Ruang Lingkup (*Scope*)

Pada penelitian ini telah ditentukan Ruang Lingkup (*Scope*) seperti yang tertera pada subbab Batasan Masalah. Pengujian akan berfokus pada Web Aplikasi milik Institusi Pendidikan XYZ yaitu KRS Daring (Kartu Rencana Studi Daring).

3.1.3. Pengintaian Sistem (*Reconnaissance*)

Pada tahap ini penulis akan mencari informasi dasar target dan mengumpulkan informasi terkait sistem seperti *IP Address* dan *Port* dengan menggunakan *tool software* Nmap.

3.1.4. Pencarian Kerentanan Keamanan (*Vulnerability Detection*)

Pada tahap ini penulis akan melakukan proses pencarian kerentanan keamanan dengan menggunakan *tool software* yaitu OWASP ZAP, nantinya digunakan untuk mendeteksi berbagai kerentanan dari Web KRS Daring. Dari hasil pencarian tersebut akan didapatkan daftar kerentanan yang nantinya akan digunakan sebagai bahan untuk perencanaan pengujian ke tahap berikutnya.

3.1.5. Analisis Perencanaan dan Perencanaan Pengujian (*Information Analysis and Planning*)

Pada tahap ini penulis akan menganalisis dan membuat rencana pengujian hasil dari Pengintaian Sistem dan Pencarian Kerentanan Keamanan yang telah dilakukan sebelumnya, analisis dan perencanaan dibuat untuk menentukan bagaimana *Penetration Testing* nantinya akan dilaksanakan.

3.1.6. *Penetration Testing*

Pada tahap ini penulis akan melakukan simulasi penyerangan terhadap target yang diuji yaitu Web KRS Daring. Simulasi penyerangan akan dilakukan sesuai hasil rencana pengujian dari tahap sebelumnya.

3.1.7. Eksploitasi Kerentanan (*Privilege Escalation*)

Setelah selesai melakukan tahap *penetration testing* selanjutnya adalah tahap Eksploitasi Kerentanan (*Privilege Escalation*) yaitu pemanfaatan kerentanan dari hasil *penetration testing*. Pemanfaatan yang dimaksud adalah untuk mengambil informasi, merubah informasi, dan merubah hak akses.

3.1.8. Penyusunan Laporan (*Reporting*)

Pada tahap ini penulis menyusun laporan hasil dari pengujian yang sudah dilakukan pada Web KRS Daring.

3.2. Alat Penelitian

Alat penelitian yang digunakan adalah sebagai berikut:

1. Laptop (Sistem Operasi: Windows 10 Pro dan Parrot).
2. OWASP ZAP.
3. *Nmap*.
4. *Arpspoof*.
5. *SSLStrip*.