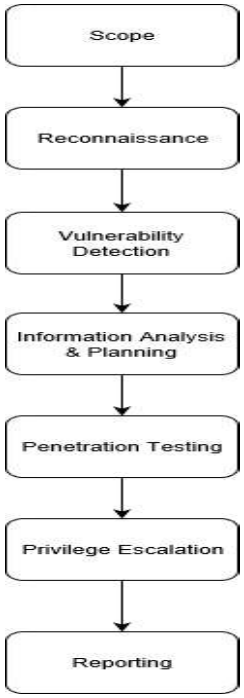
BAB III
METHODOLOGI PENELITIAN

3.1 Metode Penelitian

Pada bagian ini peneliti akan membahas mengenai metode yang akan digunakan selama mengerjakan penelitian. Metode tersebut akan dijadikan sebagai panduan sistematis dalam proses penelitian. Metode yang akan digunakan yaitu VAPT (*Vulnerability Assessment & Penetration Testing*). Gambaran metode penelitian akan digambarkan pada gambar 3.1 :



Gambar 3. 1 Metode VAPT

Gambar 3.1 menjelaskan tentang proses penelitian yang akan dilakukan. Tahapan yang dilakukan antara lain menentukan ruang lingkup penelitian(*scope*), pengintaian sistem(*reconnaissance)*, pencarian celah keamanan*(vulnerability detection)*, analisis informasi dan perencanaan(*information analysis and planning)*, *penetration testing*, eksploitasi celah keamanan(*privilege escalation)*, dan laporan(*reporting)*. Setiap tahapan akan dijelaskan sebagai berikut.

3.1.1. *Scope*

Scope adalah tahapan peneliti menentukan ruang lingkup penelitian, seperti yang dijabarkan sebelumnya pada batasan masalah. Penelitian ini berfokus pada menemukan dan mengeksploitasi kerentanan web aplikasi MoU milik perguruan tinggi XYZ. Metode yang digunakan pada penelitian ini adalah VAPT (*Vulnerability Assessment and Penetration Testing*).

3.1.2. *Reconnaissance*

Reconnaisance adalah proses mengumpulkan informasi awal tentang sistem pada web aplikasi MoU. Informasi itu dapat berupa sistem operasi yang dipakai web server, alamat IP, *database* yang digunakan dan *port* yang terbuka pada target yang akan diuji.

3.1.3. *Vulnerability Detection*

Vulnerability detection adalah pencarian celah keamanan pada target. Hasil dari temuan celah keamanan ini terbatas pada *tool* Nessus yang nantinya akan digunakan sebagai dasar perencanaan pada tahap berikutnya.

3.1.4. *Information Analysis & Planning*

Pada tahap ini penulis melakukan analisis pada hasil pencarian celah dan melakukan perencanaan pengujian yang didasarkan pada celah yang didapatkan. Hasil analisis kemudian akan dilanjutkan dengan perencanaan simulasi penyerangan.

3.1.5. *Penetration testing*

Pada tahap ini peneliti melakukan serangan terhadap target berdasarkan analisis dan perencanaan yang dirancang pada fase sebelumnya.

3.1.6. *Privilege Escalation*

Privilege Escalation adalah memanfaatkan celah keamanan yang berhasil dilakukan pada proses *penetration testing*. Pemanfaatan celah yang dimaksud adalah manajemen data dan pemanfaatan hak akses.

3.1.7. *Reporting*

Reporting adalah tahap penulisan laporan hasil penelitian yang nantinya akan diserahkan kepada pihak Perguruan Tinggi XYZ.