BAB 3
METODE PENELITIAN

Dalam proses pelaksanaan pengujian keamanan Sistem Informasi Portal Akademik Universitas Jendral Achmad Yani Yogyakarta, metode yang di gunakan adalah metode pendekatan dari Standard *PTES (Penetration Testing Execution Standard).* Berikut tahapan dari metode *PTES (Penetration Testing Execution Standard)* yaitu: dimulai dari *Pre-Engagement Interaction* dengan tujuan untuk mempersiapkan teknik yang akan digunakan dan *tools* yang di butuhkan. Tahap kedua *Intelligence Gathering* merupakan tahapan pengumpulan informasi umum mengenai target yang akan dilakukan *penetration testing*. *Threat Modelling* merupakan sebuah teknik dalam melakukan pemodelan ancaman yang diperlukan dalam *penetration testing*.

Vulnerability Analysis adalah proses pengujian celah keamanan yang digunakan untuk menemukan kerentanan suatu sistem. *Exploitation* merupakan fase *penpenetration testing* yang bertujuan melewati batasan keamanan dengan memaksa untuk mengakses sistem maupun sumber daya. *Post Exploitation* merupakan proses menentukan nilai kerentanan sistem dengan tujuan agar sistem dapat mempertahankan kontrol. *Reporting* merupakan langkah pembuatan sebuah laporan yang berisi hasil pengujian. Berikut tahapan *PTES (Penetration Testing Execution Standard)* ditunjukan pada Gambar 3.1

Gambar 3.1 Tahapan PTES (Penetration Testing Execution Standard)

3.1 TAHAP PENETRATION TESTING PTES

1. *Pre-engagement*

Bagian ini merupakan tahap dari proses mengidentifikasi yang bertujuan untuk menyediakan, menjelaskan alat dan teknik yang membantu dalam proses *penetration testing*. Biasanya informasi dapat di peroleh dari berbagai sumber, termasuk dari pengalaman penguji *(penetration tester)*. Tahap ini sangat penting sebelum melakaukan *penetration testing*.

2. *Intelligence Gathering*

Bagian ini merupakan tahap mengumpulkan informasi yang akan di tuangkan dalam sebuah dokumen dalam melakukan *penetration testing.* Tujuan dari dokumen tersebut adalah untuk memberikan *standard* yang dirancang khusus untuk seorang penguji *(penetration tester)* ,melakukan pengintaian *(reconnaissance)* terhadap target. Isi dari dokumen tersebut merinci dari kerangka proses berfikir dan tujuan dari pengintaian *(reconnaissance)* untuk melakukan penetration testing. Jika hal ini digunakan secara tepat, bisa membantu pembaca menentukan rencana yang sangat strategis untuk menyerang target.

3. *Threat Modeling*

Bagian ini merupakan tahap untuk mengidentifikasi pendekatan pemodelan ancaman yang dibutuhkan untuk *penetration testing.* Fokus dari standard pendekatan ini tergantung pada proses bisnis perusahaan dan asset pada perusahaan. Fase threat modeling sangat penting bagi penguji *(penetration tester)* dan perusahaan karena, pemodelan ini dapat memberikan kejelasan tentang resiko, sasaran secara transparasi.

4. *Vulnerability analysis*

Bagian ini merupakan tahap proses menemukan celah kemanan dalam sistem dan aplikasi yang dapat dimanfaatkan oleh penyerang. *Vulnerability analysis* bagian dari siklus *vulnerability assement.*

Vulnerability assement merupakan implementasi dari tahap *intelligence gathering* dan *threat modeling* untuk mengidentifikasi kemungkinan teknik *exploitation* dan celah keamanan pada sistem.

5. ***Exploitation***

Bagian ini merupakan tahap yang memiliki tujuan untuk membangun akses ke dalam sistem atau mencoba mendapatkan akses kedalam server, dengan melewati batas keamanan sebuah sistem. Fokus utamanya adalah untuk mengidentifikasi titik lemah keamanan pada suatu perusahaan atau organisasi dan mempertimbangkan resiko terhadap serangan yang berdampak pada asset, data atau target yang *privacy.*

6. ***Post Exploitation***

Bagian ini merupakan tahap penguji *(penetration tester)* mencari objek yang terekspos dari proses eksplotasi seperti menemukan *sensitive data, unauthorized process, privilege escalation*. Tujuan dari *post exloitatation* untuk menentukan *value* dari sebuah layanan *(website,apps).*

7. ***Reporting***

Bagian ini merupakan tahap terakhir dalam melakukan *penetration testing*. Seorang penguji *(penteration tester)* akan melaporkan segala jenis hasil temuan dari *penetration testing* yang akan dituangkan dalam sebuah dokumen laporan *(reporting).* Hal yang dicantumkan atau di tuangkan adalah hasil proses dari tahapan yang sudah di lakukan. Tujuannya dilakukan *reporting* adalah untuk mengurangi resiko dampak celah keamanan dari sebuah organisasi yang memiliki layanan teknologi informasi.

3.2 BAHAN PENELITIAN

Dalam melakukan penelitian ini, penulis mengkategorikan menjadi 2 kebutuhan bahan yaitu *tools hardware* (perangkat keras) & *tools software* (perangkat lunak).

3.3 ALAT PENELITIAN

3.3.1 Tools Hardware

Perangkat keras yang digunakan dalam penelitian ini yaitu laptop. Adapun spesifikasi minimum dan spesifikasi yang ditujukan pada Tabel 3.1

Tabel 3.1 Komponen Tools Hardware

Komponen	Spesifikasi Umum	Spesifikasi yang digunakan
CPU	1.3 GHz	Intel core 15-11 2.500 Ghz (8CPUs), 2.5 Ghz
RAM	2GB	16 GB (dual channel)
Storage	20GB	SSD 512 GB
VGA	Nvdia GT 9600 512 MB or better	Intel ® Iris ® Xe Graphics

3.3.2 Tools Software

Dalam penelitian ini, penulis menggunakan Kernel Kali Linux:

A. Kernel Kali Linux

1. Terminal Kali Linux, digunakan untuk melakukan beberapa perintah untuk menjalankan suatu sistem atau perintah.
2. *Whois* perintah dalam kali linux untuk mengetahui sebuah informasi nama pemilik domain
3. *Dirbuster* digunakan untuk melihat *hidden directory* pada sebuah *website*

4. *Wpscan,* karena portal akademik mengggunakan CMS wordpess jadi untuk melihat scaning tersebut menggunakan perintah sesuai CMS (*vulnerability assement*)
5. *Nikto tool scaning* untuk melihat sebuah *vulnerability* yang ada pada *website.*(*vulnerability assement*)
6. *Nmap* digunakan untuk menscan sebuah *port* yang terbuka dan tertutup. Hal ini dilakukan untuk scaning sebuah jaringan.(*vulnerability assement*)
7. *Burp suite*, *tools* yang digunakan dalam *penetration testing (exploitaion)*
8. *Foxyproxy*, *tool* ekstensi konfigurasi *web browser* dengan *burp suite*
9. *Wappalyze*r, sebuah *tools* ekstensi untuk melihat secara terpatri sebuah website menggunakan arsitektur yang digunakan.
10. *Mozila Firefox*
11. *Shodan*
12. *Netcraft*
13. *Google Hacking dan Google dork*

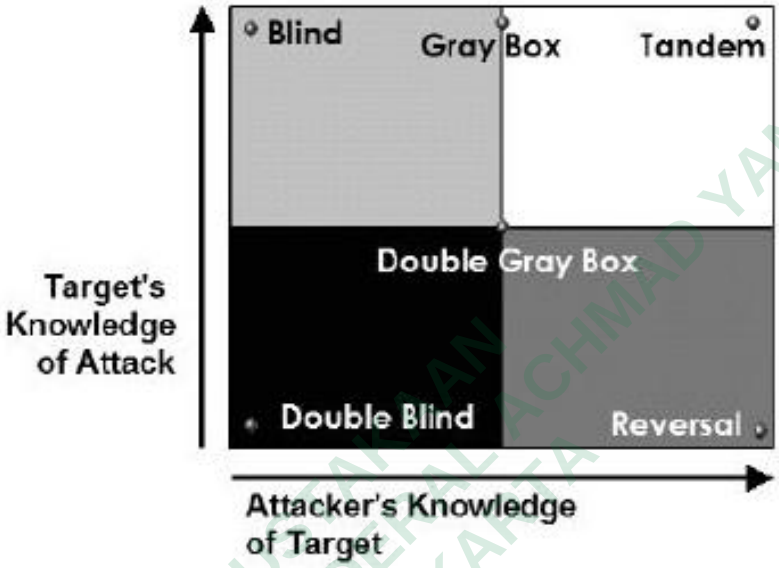
3.4 METODE PENGUJIAN

Pada metode pengujian sistem yang dilakukan oleh penulis adalah menggunakan PTES *(Penetration Testing Execution Standard)* (Dewi & Setiawan, 2022),(PTES Team, 2022). Berikut tahapan-tahapan pengujian keamanan Sistem Informasi Akademik Universitas Jenderal Achmad Yani Yogyakarta yang akan dilakukan.

3.4.1 Jenis Pengujian

Berdasarkan data dari *OSSTMM (Open Source Security Testing Methodology Manual)* terdapat 6 jenis pengujian keamanan. Jenis *penetration testing* yang dilakukan dalam penelitian ini menggunakan jenis pengujian *Gray Box penetration testing*, di kenal juga sebagai *Vulnerability testing* dan pada akhirnya sebagai data *assement*

personal. Maksud dari pengujian tersebut, penguji *(penetration tester)* hanya mengetahui beberapa *flow* dari sebuah layanan atau *website* (Herzog, 2010). Dijelaskan dalam Gambar 3.2



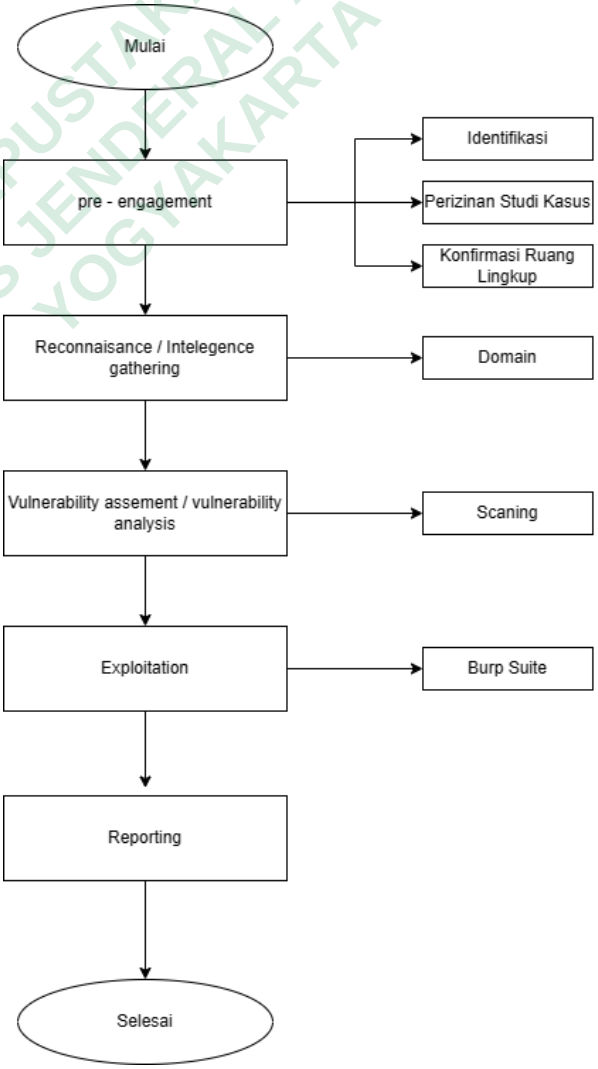
Gambar 3.2 Jenis Pengujian OSSTMM (Open Source Security Testing Methodology Manual)

3.4.2 Alur Pengujian

Berikut fase atau tahapan melakukan *penetration testing* berdasarkan pendekatan Standards *PTES (Penetration Testing Execution Standard)* sebagai berikut:

1. *Pre – engagement* (a.identifikasi ; b.konfirmasi ; c.pengambilan data)
2. *Reconnasisance / Intellegence Gathering (use tools* terminal Kali Linux, *Whois, Nmap)*
3. *Vulnerability Assement / Vulnerabilitty Analysis* (*use tools Wpscan, Nikto, Nmap)*
4. *Exploitation (use tools Burp Suite)*
5. *Reporting*

Tahapan *penetration testing* seperti pada Gambar 3.3



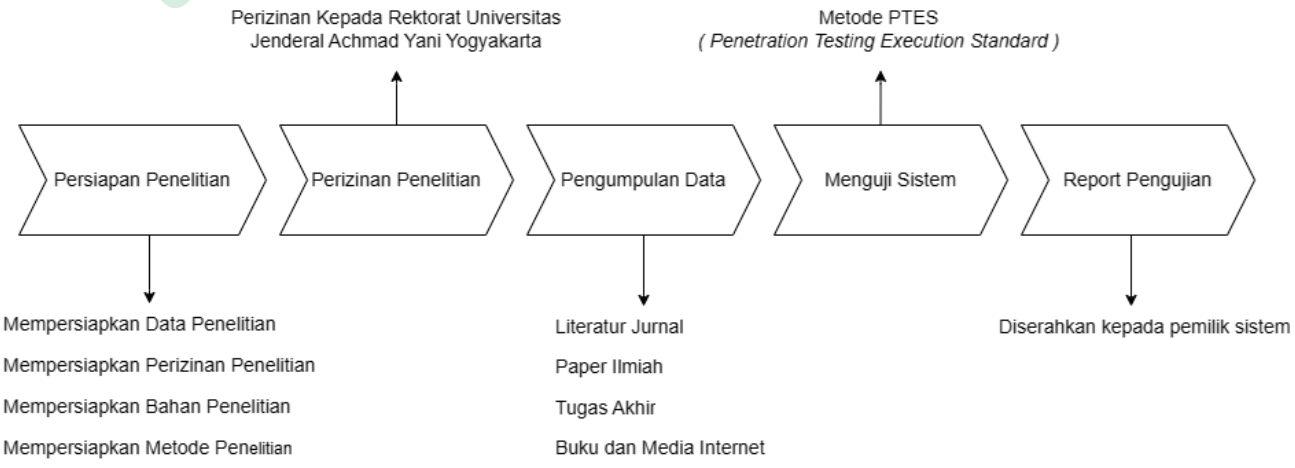
Gambar 3.3 Alur Pengujian pendekatan Standards PTES

(Penetration Testing Execution Standard)

3.5 JALAN PENELITIAN

Dalam melakukan penelitian Pengujian Keamanan Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta ini terdapat beberapa tahapan. Tahapan pertama dimulai dari persiapan penelitian. pada tahapan persiapan penelitian, penulis mempersiapkan apa saja kebutuhan yang diperlukan dari awal penelitian sampai selesai. Setelah tahapan persiapan selesai, tahapan selanjutnya melakukan perizinan. Perizinan di tujukan kepada pihak Rektorat Universitas Jenderal Achmad Yani Yogykarta guna untuk mendapat izin penelitian. Setelah tahapan perizinan disetujui, tahapan selanjutnya tahapan pengumpulan data.

Pada tahapan pengumpulan data terdapat dari beberapa sumber seperti melalui literatur jurnal, paper ilmiah, tugas akhir, buku, termasuk juga media digital seperti internet. Setelah tahapan pengumpulan data di lakukan, tahapan berikutnya menguji sistem. Dalam tahapan menguji sistem penulis menggunakan metode standard dari PTES *(Penetration Testing Execution Standard)* dan semua tahapan dalam pengujian akan didokumentasikan dalam satu laporan. Tahapan yang terakhir adalah melakukan *report*. Tahapan *report* atau laporan berisi mengenai dokumentasi baik ditemukan sebuah celah atau tidak ditemukan celah pada Sistem Informasi Portal Akademik Universitas Jendral Achmad Yani Yogyakarta. Sebagaimana ditunjukan pada Gambar 3.4



Gambar 3.4 Jalan Penelitian