BAB III

METODOLOGI PENELITIAN

3.1 Subjek dan Objek penelitian

Subjek penelitian ini adalah SMA Negeri 1 Sokaraja, khususnya pada sistem informasi SMA Negeri 1 Sokaraja yang digunakan untuk analisis kerentanan yang ada dalam sistem informasi tersebut. Supaya nantinya sistem informasi SMA Negeri 1 Sokaraja yang digunakan lebih aman dan terhindar dari penyusup yang masuk tanpa sepengetahuan dari admin. Adapun objek penelitian ini yaitu analisis sistem informasi *website* yang ada di SMA Negeri 1 Sokaraja.

3.2 Alat dan Bahan Penelitian

3.2.1 Alat :

Kebutuhan alat yang digunakan peneliti dalam pelaksanaan penelitian yaitu perangkat keras (*hardware*) dan perangkat lunak (*software*) yang masing-masing terdiri untuk kebutuhan analisis dan kebutuhan operasional yaitu:

1. Perangkat keras

a. Kebutuhan Operasional

1) Laptop Lenovo G40-45

Laptop digunakan peneliti untuk menganalisis keamanan sistem informasi *website* SMA Negeri 1 Sokaraja. Selain itu laptop juga digunakan untuk mengolah data penelitian.

2. Perangkat lunak

a. Kebutuhan Analisis

1. Sistem Operasi

Sistem Operasi yang digunakan peneliti adalah *Kali Linux* versi 2021, untuk melakukan kegiatan seperti mencari dan melakukan pentest terhadap celah keamanan sistem informasi *website* SMA Negeri 1 Sokaraja.

2. OWASP ZAP

OWASP ZAP digunakan sebagai alat dalam membantu menganalisa kerentanan pada sistem informasi *website* SMA Negeri 1 Sokaraja.

b. Kebutuhan *Information Gathering*

1. DNS Scan

DNS Scan digunakan sebagai alat untuk membantu proses identifikasi alamat domain dan subdomain.

2. Infoga

Infoga digunakan sebagai alat untuk membantu proses identifikasi alamat email.

3. NMAP

NMAP digunakan sebagai alat untuk membantu proses identifikasi port.

c. Kebutuhan *Penetratiton Testing*

1. SQL *Injection*

SQL *Injection* digunakan untuk melakukan teknik penyerangan terhadap sistem informasi *website* SMA Negeri 1 Sokaraja.

2. SQL *MAP*

SQL *MAP* merupakan *tool* yang digunakan untuk melakukan penetrasi serangan terhadap sistem informasi *website* SMA Negeri 1 Sokaraja.

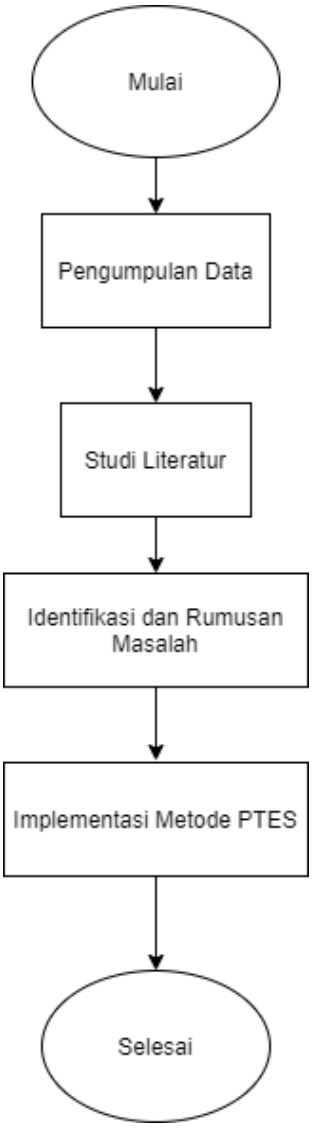
3.2.2 Bahan

Bahan yang peneliti gunakan dalam pelaksanaan penelitian adalah sistem informasi SMA Negeri 1 Sokaraja yang akan dilakukan analisis keamanan dan kerentanannya, di antaranya yaitu:

1) Website

website ini berupa sistem informasi SMA Negeri 1 Sokaraja dengan alamat *website* (https://www.sman1sokaraja.sch.id)

1.3 Diagram Alir Penelitian



Gambar 3.1 Diagram Alir Penelitian

Pada diagram alir penelitian terdiri 6 proses seperti :

1.3.1 Pengumpulan Data

Pada tahap ini peneliti mengumpulkan data yang digunakan untuk kebutuhan keamanan serangan seperti data serangan siber terbaru di Indonesia. Data tersebut didapatkan dengan cara membaca penelitian sebelumnya yang bersumber dari jurnal penelitian. Selain itu peneliti melakukan observasi dengan mencari sumber informasi pada *website* resmi.

3.3.2 Studi Literatur

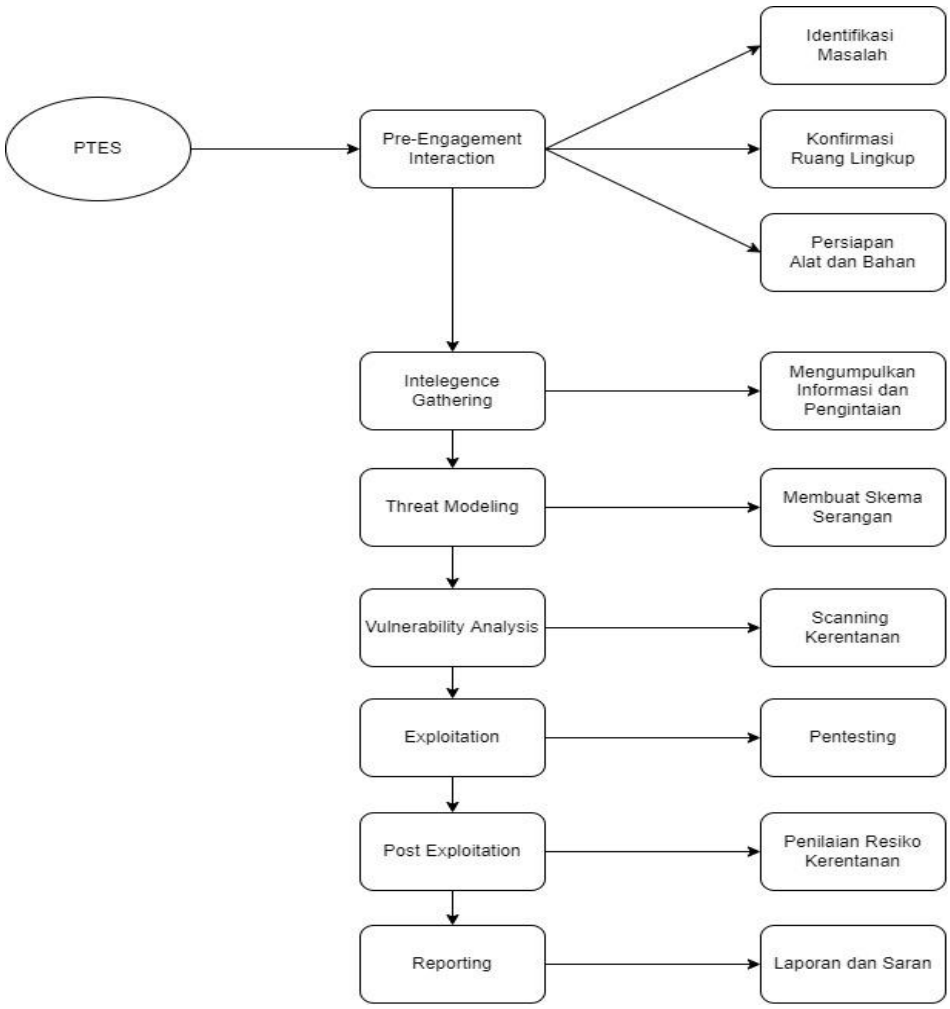
Pada tahapan ini peneliti mulai mencari referensi seperti informasi serangan terbaru di Indonesia yang bersumber dari situs resmi yang ada di internet.

3.3.3 Identifikasi dan Rumusan Masalah

Pada tahapan ini peneliti mulai melakukan identifikasi suatu permasalahan yang terjadi dilapangan yang dianggap bisa untuk dilakukan penelitian, peneliti kemudian menemukan sebuah permasalahan pada kerentanan sebuah sistem informasi *website* SMA Negeri 1 Sokaraja yang belum diketahui oleh seorang admin web. Kemudian peneliti merumuskan masalah tersebut dengan penelitian tentang analisis keamanan sistem informasi *website* SMA Negeri 1 Sokaraja menggunakan metode *penetration testing execution standard*.

3.3.4 Implementasi Metode PTES

Pada tahap ini peneliti mulai melakukan pengujian dengan menggunakan metode *Penetration Testing Execution Standard* (PTES). Metode tersebut menggunakan 7 tahapan yang nantinya akan dilakukan oleh peneliti seperti *Pre-engagement Interaction, Intelegence Gathering, Threat Modeling, Vulnerabillity Analysis, Exploitation, Post Exploitation, Reporting*. Berikut kerangka kerja dari PTES.



Gambar 3.2 Kerangka Kerja PTES

Pada tahapan *Pre-engagement Interaction* peneliti melakukan beberapa kegiatan seperti identifikasi masalah yang terdapat pada sistem informasi *website* SMA Negeri 1 Sokaraja. Selanjutnya peneliti melakukan konfirmasi terhadap pihak SMA Negeri 1 Sokaraja dengan membuat surat izin penelitian. Setelah itu peneliti menyiapkan alat dan bahan yang diperlukan untuk melakukan PTES terhadap sistem informasi *website* SMA Negeri 1 Sokaraja. Selanjutnya pada tahapan *Intelegence Gathering* peneliti mengumpulkan beberapa informasi yang dibutuhkan pada saat melakukan PTES. Informasi yang dibutuhkan seperti nama *domain* dan subdomain, alamat ip, domain info, alamat email serta DNS.

Selanjutnya pada tahapan *Threat Modeling* peneliti melakukan tahapan untuk pendekatan pemodelan dari pengujian yang akan dilakukan. Pemodelan

ini digunakan untuk memudahkan peneliti untuk memahami kerentanan keamanan yang akan ditemukan pada pengujian dalam penelitian ini. Selanjutnya pada tahapan *Vulnerabillity Analysis* peneliti mulai melakukan analisa kerentanan keamanan sistem informasi *website* SMA Negeri 1 Sokaraja dengan menggunakan *tool* OWASP ZAP. *Tool* ini dapat memberikan informasi mengenai kerentanan (*vulnerability*) yang ada didalam *website*.

Selanjutnya pada tahapan *Exploitation* dilakukan penetrasi serangan menggunakan teknik SQL *Injection* terhadap sistem informasi *website* SMA Negeri 1 Sokaraja. *Tool* yang digunakan peneliti dalam melakukan penetrasi serangan yaitu dengan menggunakan bantuan SQL *MAP*. Teknik tersebut dilakukan untuk menguji keamanan pada sistem informasi *website* SMA Negeri 1 Sokaraja. Selanjutnya pada tahapan *Post Exploitation* dilakukan penilaian tingkat risiko terhadap sistem yang memiliki celah keamanan setelah dilakukan pengujian pada tahapan sebelumnya. Dengan ini peneliti membuat tabel untuk memberikan penelian untuk melihat risiko serangan yang telah ditemukan pada tahapan sebelumnya.

Setelah dilakukan pengujian, tahapan terakhir yang peneliti lakukan adalah *Reporting*. Tahapan tersebut dilakukan dengan menuliskan laporan hasil analisis dan pengujian yang sudah dilakukan sebelumnya.

3.4 Analisis Keamanan Website

Pada tahap ini yang peniliti lakukan adalah menganalisis keamanan website dari hasil pengujian yang telah dilakukan pada tahap implementasi PTES. Tahapan tersebut diambil dari hasil pengujian *vulnerability analysis* dengan menggunakan bantuan *tools* OWASP ZAP. Dari tools tersebut akan didapatkan kerentanan yang ada didalam website sehingga celah keamanan pada sebuah website dapat diketahui.