BAB III METODOLOGI PENELITIAN

3.1 Subjek Dan Objek Penelitian

Subjek penelitian mengenai *Penetration Testing web* ini dilakukan di IT Telkom Purwokerto yang merupakan salah satu Perguruan Tinggi swasta di Purwokerto. Sementara itu, objek penelitian ini yakni untuk menganalisis keamanan website *Tracer Study* pada IT Telkom Purwokerto melalui *penetration testing*.

1.2 Alat dan Bahan Penelitian

Berikut adalah alat dan bahan yang digunakan dalam melakukan penelitian ini, yaitu:

Alat Peneltian:

Dalam penelitian ini, terdapat dua komponen utama yang digunakan, yaitu perangkat lunak dan perangkat keras. Perangkat lunak yang digunakan adalah sistem operasi Kali Linux, sementara perangkat keras yang digunakan adalah sebuah *laptop*. Kali Linux merupakan salah satu Linux *distribution* yang berbasis Debian, dan memiliki berbagai fitur dan alat yang sesuai untuk melakukan pengujian penetrasi. Dalam penelitian ini, laptop yang digunakan memiliki spesifikasi sebagai berikut:

Tabel 3.1 Spesifikasi Laptop

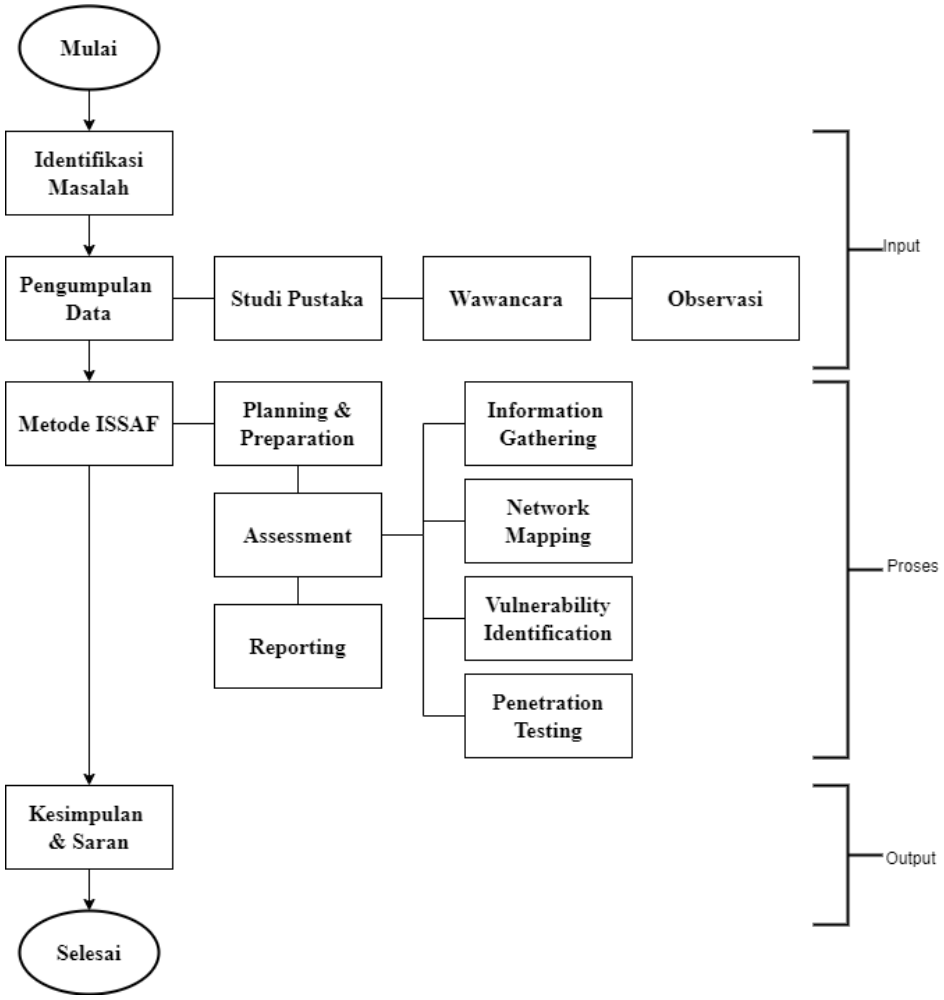
Merk	Asus X441U
Sistem Operasi	Kali Linux
Processor	Intel Core i3-6006U, 2.0GHz
Memori RAM	4 GB
Hardisk	500 GB

Bahan Penelitian:

Bahan penelitian ini diperoleh melalui berbagai studi literatur tentang sistem keamanan web dan uji penetrasi. Selain itu, bahan penelitian juga dikumpulkan melalui diskusi dengan dosen yang memiliki keahlian dalam bidang keamanan informasi.

1.3 Diagram Alir Penelitian

Berikut ini terdapat *flowchart* yang menggambarkan tahapan penelitian ini.



Gambar 3.1 Diagram Alir Penelitian

Berikut adalah penjelasan ringkas mengenai tahapan penelitian yang tergambar pada Gambar 3.1

1. Identifikasi Masalah

   Pada tahap awal dilakukan penentuan masalah pada web *Tracer Study* di IT Telkom Purwokerto. Berdasarkan hasil wawancara, didapatkan permasalahan utama yakni *web* Sistem Informasi *Tracer Study* belum pernah dilakukan uji keamanan atau *Penetration Testing*. Masalah tersebut menjadi alasan diambilnya topik penelitian uji keamanan *web* atau *Penetration Testing*. Diharapkan bahwa melalui penelitian mengenai topik tersebut, dapat memberikan kontribusi bagi administrator dalam melakukan audit terhadap kerentanan keamanan pada website Sistem Informasi *Tracer Study* IT Telkom Purwokerto. Serta memberikan hasil *Penetration Testing* dan juga melakukan peningkatan keamanan melalui proses optimalisasi Sistem Informasi *Tracer Study* IT Telkom Purwokerto.

2. Pengumpulan Data

   Langkah berikutnya adalah melakukan pengumpulan data. Ini dilakukan untuk mendapatkan materi atau informasi yang diperlukan untuk penelitian. Pengumpulan data dilakukan melalui tiga langkah, yaitu studi pustaka, observasi, dan wawancara.

   Untuk studi pustaka dilakukan proses pengumpulan informasi dari sumber-sumber literatur yang relevan untuk mendukung penelitian, yaitu dengan cara pencarian, pengumpulan, dan penelaahan berbagai referensi seperti buku, jurnal ilmiah, artikel, laporan penelitian, dan sumber-sumber lainnya yang terkait dengan topik penelitian. Lalu untuk wawancara dilakukan dengan pihak yang terlibat yaitu bagian unit keamanan IT Telkom Purwokerto. Sedangkan untuk obeservasi yaitu dilakukan pengumpulan data dengan melakukan pengamatan langsung terhadap objek penelitian untuk memperoleh informasi dan mengidentifikasi kerentanan pada *web Tracer Study* IT Telkom Purwokerto.

3. Metode ISSAF

   Pada tahap ini, dilakukan uji penetrasi dengan menggunakan *framework* ISSAF yang terbagi menjadi beberapa tahapan. Seperti halnya dalam

pengujian penetrasi yang dilakukan secara umum, setiap tahapan dalam framework ISSAF ini memiliki proses tersendiri untuk menuju tahap selanjutnya.

A. *Planning and Preparation*

Fase *planning and Preparation* merupakan Langkah awal dalam mempersiapkan dan mengumpulkan informasi mengenai target yang akan dilakukan *penetration testing*. Pada tahap ini, penulis akan menyiapkan *Web* Sistem Informasi *Tracer Study* IT Telkom Purwokerto yang akan menjadi objek penelitian ini. Setelah mempersiapkan web Sistem Informasi *Tracer Study*, langkah selanjutnya adalah menyusun rencana pengujian untuk sistem informasi tersebut.

B. *Assessment*

Fase Assessment merupakan tahap yang bertujuan untuk menguji website yang telah dipersiapkan pada tahap planning and preparation.. Pada Fase *Assessment* ini dilakukan 4 tahapan yang mencakup:

a. *Information Gathering* (Pengumpulan Informasi)

Pada tahap ini, dilakukan pengumpulan informasi umum terkait sistem sebagai tahapan persiapan *penetration testing*. Informasi yang dikumpulkan antara lain seperti SSL, DNS, info *domain*, dan identifikasi CMS.

b. *Network Mapping* (Pemetaan Jaringan)

Mengumpulkan informasi secara spesifik mengenai jaringan pada target seperti informasi tentang *port* TCP dan UDP pada sistem target.

c. *Vulnerability Identification* (Identifikasi Keterangan)

Melakukan pemindaian atau *scanning* terhadap website target dengan tujuan untuk mengidentifikasi kerentanan keamanan yang ada dalam sistem target.

d. *Penetration* (Penetrasi)

Pada tahap ini dilakukan simulasi serangan pada website target bertujuan untuk memperoleh kerentanan keamanan pada sistem.

C. *Reporting*

Setelah menyelesaikan tahap assessment, langkah selanjutnya adalah tahap *reporting, Clean Up & Destroy Artifacts* bertujuan untuk mendokumentasikan segala aktivitas dan hasil uji penetrasi. Laporan ini akanberbentuk laporan tertulis yang secara rinci menjelaskan semua kegiatan uji penetrasi, dan juga memasukkan hasil uji penetrasi bersama dengan tools-tools yang dipakai. Laporan tersebut juga akan mencakup temuan celah keamanan yang ditemukan dan tindakan yang diambil untuk menanganinya.

4. Kesimpulan & Saran

Tahap ini bertujuan untuk melaporkan secara lengkap seluruh aktivitas dan hasil uji penetrasi. Laporan yang disusun yaitu berupa tulisan yang secara detail menjelaskan semua kegiatan yang telah dilakukan. Selain itu, laporan juga mencakup lampiran berisi hasil pengujian, *tools* yang digunakan, celah keamanan yang ditemukan serta solusi untuk mengatasinya.