BAB III
METODOLOGI PENELITIAN

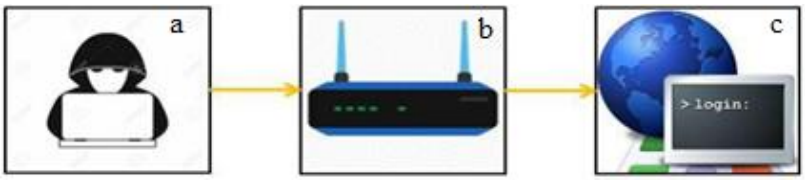
3.1 Metodologi Penelitian

Berdasarkan bab sebelumnya, tujuan penelitian ini untuk mengaudit sistem informasi akademik Universitas Sultan Ageng Tirtayasa menggunakan metode COBIT 5, agar dapat melakukan analisis penelitian perlu adanya pengambilan data secara langsung. Sebelum pengambilan data ada beberapa tahap yang harus diselesaikan sampai dengan penelitian ini selesai, berikut merupakan penjelasan alur penelitian antara lain:

1. Studi literatur yang dilakukan yaitu dengan mencari referensi-referensi seperti jurnal, buku-buku mengenai penelitian terkait dengan pokok permasalahan yang akan diteliti. Referensi-referensi yang dipergunakan kemudian dipelajari serta diimplementasikan.
2. Observasi ke lokasi penelitian untuk mengetahui proses layanan teknologi informasi.
3. Menyusun kuesioner berdasarkan COBIT 5.
4. Menyebar kuesioner COBIT 5 pada responden.
5. Menyiapkan *tools* untuk *penetration testing.*
6. Melakukan *penetration testing.*
7. Menghitung dan analisa hasil dari kuesioner berdasarkan COBIT 5 menggunakan *capability level* serta menganalisa hasil *penetration testing.*
8. Membuat rekomendasi berdasarkan hasil dari kuesioner dan hasil *penetration testing.*
9. Membuat kesimpulan dan saran untuk hasil pengujian yang di peroleh.

3.2 *Penetration Testing*

Tahap *penetration testing* dilakukan untuk menguji kerentanan keamanan layanan Siakad. Layanan tersebut dipilih karena umum digunakan untuk layanan akademik dan layanan informasi. Berikut merupakan alur *penetration testing,* ditunjukan di Gambar 3.2.



(a) Penyerang (b) Koneksi internet (c) *Web server*

Gambar 3.1 Alur *Penetration Testing*

Berdasarkan Gambar 3.1 merupakan penjelasan *penetration testing* menggunakan sistem operasi Kali linuk, koneksi internet dan beberapa *tools* serta menggunakan 4 tahapan ISSAF, antara lain:

1. *Information gathering*, pengujian ini menggunakan *tools Whois* untuk mengetahui registrasi dan sistem administrator, *DNSrecon* untuk mengetahui DNS target, *whatweb* untuk mendapatkan informasi tentang teknologi web, sslscan untuk mendapatkan informasi tentang SSL/TSL target.
2. *Network mapping* dalam pengujian ini menggunakan *tools* Nmap digunakan untuk mencari *port* yang terbuka.
3. *Vulnerability identification* dalam melakukan pengujian menggunakan *tools* Vega *vulnerability* dan owasp ZAP sebagai proses mencari celah kerentanan.
4. *Penetration testing* mensimulasikan serangan terhadap *website* yang ditargetkan. Pengujian ini akan melakukan serangan SQL *injection* atau menambahkan injeksi pada *website* target menggunakan *tools* Sqlmap.

3.3 Kuesioner COBIT 5

Sebelum penyebaran kuesioner, perlu dilakukan pemetaan RACI dengan tujuan untuk mendapati siapa saja responden yang akan menjawab kuesioner setara dengan tugasnya, sehingga perlu dilakukan pemetaan antara RACI *Chart* dengan struktur di Pusdainfo yang dipetakan, seperti terlihat pada Tabel 3.1 responden yang akan mengisi jawaban kuesioner pada penelitian ini.

Tabel 3.1 Responden Penelitian

No	Fungsional Struktur COBIT 5	Fungsional Struktur Pusdainfo
1	*Information security manager*	Kepala sub koordinator pengembangan sistem
2	*Bussiness process owners*	Kepala sub koordinator jaringan
3	*Head development*	Admin server
4	*Head IT operations*	Spv *engineering* PT. MMD

Berdasarkan Tabel 3.1 merupakan pemetaan RACI *chart* dan struktur Pusdainfo. Kuesioner yang akan digunakan dalam penelitian ini yaitu *key management practices* (KMP). Pada penelitian ini hanya difokuskan pada 2 sub-domain yaitu pengelolaan keamanan (APO13) dan pengelolaan layanan keamanan (DSS05). Hasil kuesioner tersebut didapatkan nilai kapabilitas level setiap proses. Pasca perhitungan hasil kapabilitas level akan dilakukan analisis *gap.* Analisis *gap* digunakan untuk mengetahui jarak dari nilai kapabilitas yang didapatkan dengan target yang diharapkan. Memberikan saran yang diperlukan agar pengelolaan serta pelayanan keamanan Siakad menjadi lebih baik dari sebelumnya.