BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dunia siber Indonesia di tahun 2023 diramaikan dengan *hacker* bjorka membocorkan 34 juta data paspor warga indonesia. Kejadian awal terpaut insiden siber yang terus menerus menghantam sistem keamanan siber nasional serta kejadian kedua terpaut usaha pemerintah menguatkan kemanan siber nasional itu sendiri. Insiden siber di Indonesia tidak lepas dengan apa yang terjalin di dunia siber global, sebab serangan dapat tiba dari mana saja bukan cuma dari Indonesia.Serangan siber yang bisa jadi saja dari negeri lain yang menjadikan negeri sumber serangan itu selaku pijakan ataupun platform saja[1].Sistem monitoring BSSN pada bulan agustus 2023 mencatat anomali trafik sebanyak 78,464 juta serangan siber yang masuk ke Indonesia sejauh bulan Agustus tahun 2023 ini serangan terbanyak tiba dari IP address berlokasi di Indonesia[2].

Pengguna internet di Indonesia semakin meningkat setiap tahunnya, sehingga keamanan informasi menjadi isu penting sangat penting untuk menjamin kerahasiaan data pengguna, memastikan bahwa hanya data pengguna yang dapat diubah pengguna itu sendiri, dan data yang diperoleh setiap saat oleh pengguna. Namun hal ini belum dilakukan Badan Siber Sandi Negara (BSSN) mencatat paling banyak 1,6 miliar serangan siber pada tahun 2021[3]. Serangan siber tertinggi atau terendah terjadi pada sektor pendidikan, swasta, pemerintah daerah, pemerintah pusat, hukum dan personal.

Seiring dengan meningkatnya kebutuhan akan keamanan siber , perusahaan seperti KSU Postra berperan penting dalam mendukung berbagai sektor. KSU Postra merupakan perusahaan penunjang multibisnis yang berkedudukan di Bandung yang bergerak di bidang keuangan untuk memenuhi kebutuhan pensiunan PNS, TNI/POLRI serta pegawai perusahaan pemerintah dan swasta. Postra sup*Port* berdiri sejak tahun 2019 dan berkembang pesat hingga kini telah memiliki lebih dari 50 pusat layanan yang tersebar di Pulau Jawa dan wilayah

Nusa Tenggara Timur. Dengan banyaknya biro kerja yang ada, perusahaan akan sangat membutuhkan suatu alat untuk memantau kinerja pekerjaannya. Untuk mendukung pengelolaan tersebut, Koperasi Postra telah menerapkan sistem pengenalan yang digunakan oleh karyawannya di seluruh pusat layanan.

Berdasarkan hasil wawancara dengan Bapak Ridwan Panji Akbar selaku kepala depertemen IT di KSU Postra mengatakan bahwa beliau mengelola banyak sistem seperti sistem abensi, sistem pengelolaan dana pensiun, sistem *helpdesk* serta masih banyak sistem lainnya.Berdasarkan sistem yang sudah berjalan dalam hal pemakain terdapat serangan pada sistem helpdesk pada saat user ingin membuat tiket atau bantuan yang dimana seharusnya user hanya bisa mengupload sebuah file gambar yang di filter berekstensi jpg,png dan jpeg tapi user bisa mengupload sebuah extensi diluar dari yang di filter dari sistem yang dimanipulasi atau dibypass dengan cara memakai extensi yang berbeda dari yang difilter sistem .Dari kejadian itu dapat mengupload sebuah *shell backdoor* yang menyebabkan pihak yang tidak bertanggung jawab mampu untuk melakukan tindakan eksploit pada sistem *website* tersebut[4].

Belum adanya pengujian keamanan yang menyeluruh pada sistem yang dikelola oleh KSU Postra menjadi salah satu faktor utama terjadinya insiden ini. Pengujian keamanan, seperti penetration testing dan vulnerability assessment, belum diterapkan secara rutin dan mendalam, sehingga kerentanan seperti yang ditemukan pada sistem helpdesk tidak terdeteksi lebih awal. Pengujian semacam ini penting untuk mengidentifikasi dan memperbaiki celah-celah keamanan sebelum dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Dengan adanya pengujian keamanan yang memadai, perusahaan dapat mengurangi risiko serangan dan melindungi integritas perusahaan.

Berdasarkan masalah yang ditemui dan berdiskusi bersama pihak terkait dalam menentukan sebuah solusi.Hasil diskusi tersebut ialah perlu adanya pencegahan bug dengan mencari celah keamanan yang dapat di eksploitasi agar terhindar dari hal-hal yang tidak diinginkan .Untuk uji keamanan disini peneliti menggunakan metode Zero entry Hacking (ZEH) karena memiliki tahapan sederhana dan sangat cocok untuk pemula untuk pendekatan celah keamanan yang

bisa di *Exploit*asi pada sistem *Website*[5].Maka akan dilakukan *penetration testing* pada sistem *helpdesk* untuk mengetahui celah keamanan dan mencegah *hacker* yang dapat mengekploitasi kedalam *Website* tersebut.Sehingga diharapkan mampu memberi solusi untuk masalah yang ada di KSU Postra.

Dengan demikian untuk mengambil topik penelitian tentang keamanan sistem dengan judul penelitian "IMPLEMENTASI PENETRATION TESTING DENGAN METODE ZERO ENTRY HACKING (ZEH) PADA SISTEM KOPERASI SERBA USAHA POSTRA" diharapkan dapat memberikan manfaat terutama bagi KSU Postra.

1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang, maka didapat identifikasi masalah yaitu sistem pada *website helpdesk* postra masih rentan terhadap serangan.

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah untuk mengidentifikasi, menganalisis, dan memitigasi celah keamanan pada sistem *helpdesk* KSU Postra dengan mengimplementasikan *penetration testing* memenggunakan metode *Zero Entry Hacking* (ZEH). Penelitian ini mencoba untuk memahami secara mendalam bagaimana kerentanan pada sistem helpdesk dapat dieksploitasi, dan potensial merugikan integritas.Adapun tujuan dari penelitian ini adalah dengan melakukan *Assesment* pengujian keamanan *website helpdesk* postra melalui implementasi *penetration testing* menggunakan metode Zero Entry Hacking (ZEH) dengan menghasilkan resiko keamanan dari analisis kerentanan dan rekomendasi perbaikan.

1.4 Batasan Masalah

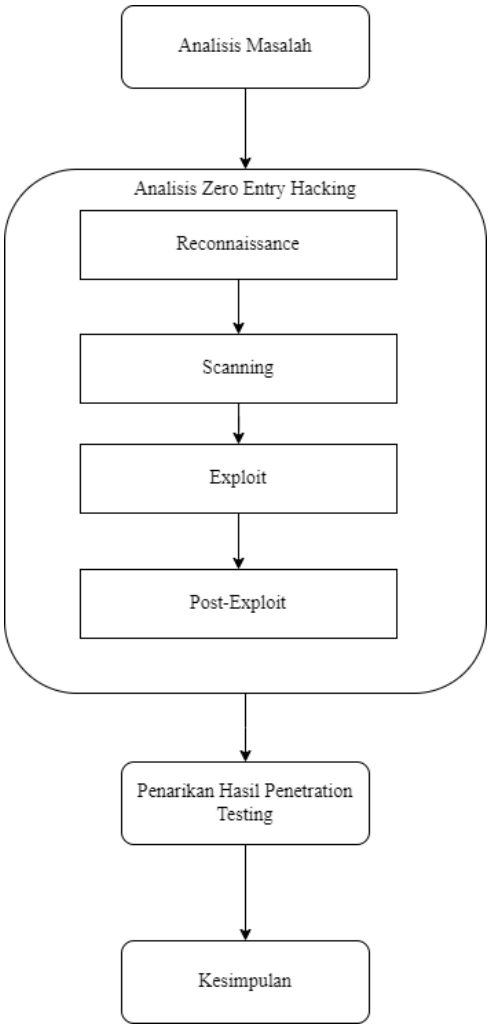
Penelitian ini dibatasi pada beberapa aspek tertentu agar dapat fokus pada tujuan yang ingin dicapai. Pembatasan ini dilakukan agar penulisan skripsi dapat memberikan pemahaman yang jelas dan sesuai dengan harapan. Adapun batasan masalah dalam pengujian sistem ini adalah sebagai berikut.

1. Jenis uji penetrasi yang dilakukan saat penelitian menggunakan *gray-box testing*.
2. Proses mencari celah keamanan dalam uji penetrasi hanya dilakukan dengan alamat *helpdesk.ksupostra.id*.
3. *Penetration testing* berfokus pada *application layer*.
4. Proses *penetration testing* berakhir pada tahap pemberian laporan rekomendasi perbaikan terhadap celah keamanan yang ditemukan.

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah metodologi penilitian kuantitatif, Dengan mengambil pendekatan penelitian eksperimen yang bersifat *validation* atau menguji yaitu menguji pengaruh satu atau lebih variabel terhadap variabel lain, yang dalam penelitian peneliti yaitu menguji kerentanan pada kemananan sistem *website helpdesk* koperasi postra.

Langkah -langkah penelitian dilakukan dapat dilihat pada Gambar 1.1



Gambar 1.1 Tahapan Metodologi Penelitian

Adapun penjelasan dari langkah-langkah metode penelitian sesuai dengan Gambar 1.1 sebagai berikut:

1.5.1 Analisis Masalah

Tahap ini bertujuan untuk memahami dan merumuskan masalah yang akan diatasi dalam penelitian. Peneliti mengidentifikasi kerentanan yang ada dalam sistem *website helpdesk* Koperasi Serba Usaha Postra.

1.5.2 Analisi *Zero Entry Hacking*

Penelitian ini menggunakan *Zero Entry Hacking* (ZEH) sebagai metode dalam melalukan pengujian dan analisis. Adapun beberapa proses yang akan dilakukan sebagai berikut.

1. Pengitaian Target (*Reconnaisance*)

   Reconnaisance adalah tahapan pertama yang bertujuan untuk menggali informasi sebanyak mungkin mengenai objek yang di uji.
2. Pemindaian (*Scanning*)

   Scanning adalah sebuah tahapan dimana seorang penyerang menggunakan berbagai macam *tools* untuk mencari celah yang akan digunakan sebagai target serangan.
3. Ekploitasi (*Exploitation*)

   Pada tahap ini, celah kerentanan yang telah ditemukan akan di uji untuk memperoleh akses pada sebuah sistem tersebut dengan *tools*.
4. Pasca eksploitasi (*Post Exploitation*)

   Pada tahap ini, celah kerentanan yang telah ditemukan akan di dinilai dan akan memberikan rekomendasi perbaikan.

1.5.3 Penarikan Hasil *Penetration Testing*

Pada tahap ini, hasil dari setiap tahap sebelumnya dievaluasi dan dianalisis. Hasil eksploitasi, kelemahan yang ditemukan, serta langkah perbaikan yang direkomendasikan dicatat untuk dilaporkan.

1.5.4 Kesimpulan

Hasil dan kesimpulan memberikan gambaran dari inti permasalahan yang terjadi berdasarkan hasil *penetration testing* dan analisis. Kesimpulan ini mencakup rekomendasi untuk perbaikan sistem dan hasil temuan dari penetration testing.

1.6 Sistematika Penulisan

Sistematika penulisan ini disusun untuk memberikan gambaran secara umum mengenai penulisan yang akan dilaksankan. Untuk sistematika penulisan tugas akhir sebagai berikut.

BAB I PENDAHULUAN

Menguraikan tentang latar belakang permasalahan, mencoba mengidentifikasi permasalahan yang dihadapi, menentukan tujuan dan kegunaan penelitian, yang kemudian diikuti dengan batasan masalah dan sistematika penulisan.

BAB II LANDASAN TEORI

Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian.

BAB III ANALISIS DAN PERENCANAAN

Bab ini berisi analisis dalam pembangunan sistem yaitu gambaran umum analisis masalah, analisis pengujian, analisis perencanaan.

BAB IV IMPLEMENTASI

Bab ini berisi pembahasan mengenai implementasi dalam menguji keamanan sistem yaitu implemntasi penetration testing sistem dan tahap-tahap dalam melakukan pengujiam perangkat lunak.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil penelitian yang dilakukan dan saran untuk pengembangan penelitian yang dilakukan lebih lanjut.