BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan jaman dalam dunia komputer, internet, dan teknologi *website* telah begitu pesatnya berkembang sehingga masuk dalam segala hal kehidupan masyarakat kini masyarakat bergantung pada layanan jaringan komputer melebihi masa sebelumnya. Hal ini dapat dilihat dengan semakin banyaknya pengguna media sosial dan layanan internet saat ini.

Menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2021 jumlah pengguna internet di Indonesia tahun 2021 adalah 274,9 juta user. Jika dibandingkan dengan tahun sebelumnya mengalami kenaikan hingga 15,5%. Pada tahun 2020 adalah 266,9 juta *user* dari total jumlah penduduk Indonesia sebesar 271,3 juta. Jika dibandingkan penggunaan internet Indonesia pada tahun 2019 sebesar 171 juta *user*, maka terjadi kenaikan sebesar 25,5 juta dalam waktu setahun (2019 - 2020). Pengguna internet di Indonesia diprediksi akan terus meningkat setiap tahun.

Dengan semakin banyak bertambahnya pengguna internet maka semakin banyak informasi yang dapat diperoleh dari internet. Teknologi informasi sekarang banyak diterapkan pada institusi pendidikan yang ada di Indonesia. Pemanfaatan teknologi informasi menjadi sebuah kebutuhan, bukan hanya sekedar *lifestyle* (Indrayani, 2011). Teknologi informasi diartikan sebagai teknologi yang mendukung kegiatan manusia dalam melakukan pengelolaan dan penyebaran informasi. Informasi yang dikelola dan disebarkan ke publik harus memiliki integritas atau dapat dipercaya, oleh sebab itu keamanan terhadap informasi juga menjadi hal yang penting, ancaman pada kemananan informasi dapat berupa serangan dari luar maupun dari dalam intitusi, karena hal tersebut dapat mengancam keberlangsungan teknologi informasi dan dapat menyebabkan gangguan bahkan terjadi kegagalan proses bisnis. Penyerang dapat memanfaatkan celah keamanan untuk menyadap hak akses dan menggunakannya untuk mengambil data penting.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka rumusan masalah dari penelitian ini adalah sebagai berikut :

1. Bagaimana hasil pengujian *penetration testing* dan analisis kerentanan terhadap *website* yang ada?

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah melakukan pengujian terhadap *website* yang ada, untuk menemukan kerentanan keamanan dan memberitahu dampak yang akan terjadi jika terjadi serangan dan membuat hasil *pentest* ke dalam laporan pengujian kerentanan pada website.

1.4 Manfaat Penelitian

Dengan adanya penelitian ini dapat mengetahui celah keamanan pada *website*, mengetahui dampak yang akan terjadi jika terjadi serangan, dan mengetahui cara mengatasi dampak terjadi.

1.5 Sistematika Penulisan

Sistematika penulisan tugas akhir dibagi menjadi lima bab. Berikut penjelasan masing-masing bab:

BAB I PENDAHULUAN

Pada bab ini menjelaskan mengenai latar belakang masalah, batasan masalah, tujuan, dan manfaat penelitian, serta sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Mengenai dasar teori yang mendukung masalah yang sedang diteliti, antara lain *Keamanan Sistem, Ubuntu Server, Kali Linux,* & *Penetration Testing*, OWASP ZAP, Nmap, Metasploit.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan mengenai metode penelitian, berupa Alat dan Bahan, Skenario Pengujian, Topologi Jaringan, Installasi *Ubuntu Server, Installasi Kali Linux, Installasi* OWASP ZAP, *Installasi Nmap, Installasi Metasploit* dan Kriteria Pengujian *Website.*

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan tentang penerapan metode penelitian pencarian celah keamanan, berupa *Scope*, Hasil analisis celah keamanan menggunakan tiga *tools* yaitu OWASP ZAP, Nmap, dan Metasploit.

BAB V KESIMPULAN

Pada bab ini menjelaskan tentang kesimpulan dari hasil penelitian dan saran yang diberikan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Mengenai rujukan dari berbagai macam, seperti jurnal, tesis, atau alamat *website* yang digunakan dalam penulisan skripsi.