BAB 1. PENDAHULUAN

1.1 Latar Belakang

Keamanan *Website* perlu menjadi perhatian di tengah banyaknya kasus peretasan *Website* dari pihak yang tidak bertanggung jawab. Keamanan *Website* merupakan upayauntuk melindungi *Website* dari serangan hacker yang terhubung melalui suatu jaringan.Situs *Website* yang dapat diakses secara online dapat menciptakan kerentanan terhadapancaman dari serangan hacker((Muhyidin dkk., 2020). Di era modern saat ini sudah banyak software *Website* atau aplikasi web yang di buat dengan berbagai macam jenis contohnya yaitu E-Commerce, Sosial Media Web, Blogging *Website*, *Port*al berita *Website*, E- learning, Web aplikasi platform dan masih banyak lainnya. Pengujian adalah suatu proses pelaksanaan suatu program dengan tujuan menemukan suatu kesalahan(Permatasari dkk., 2020).

Berdasarkan fungsinya *Website* sebagai media yang menyampaikan informasi, membutuhkan sebuah keamanan agar informasi utuh diterima oleh penerima informasi(Mulyanto dkk., 2022). Dengan adanya pengujian *Website* para development dapat mengetahui kelemahan *Website* yang telah dibuat, salah satu tahap pengujian yang akan saya bahas yaitu keamanan *Website*, karena *Website* juga dapat menjadi sasaran serangan oleh pihak yang tidak bertanggung jawab. Tidak adanya keamanan pada sistem *Website* akan berdampak buruk hacker dengan mudah dapat mengambil alih sistem yang dibangun(Riadi dkk., 2020). Oleh karena itu, analisis keamanan *Website* sangat penting dilakukan untuk mengindentifikasi potensi celah keamanan pada webiste dan mencegah serangan dari pihak yang tidak bertanggung jawab, kerentanan pada *Website* disebabkan oleh banyak hal, salah satunya tidak melakukan testing keamanan sebelum *Website* diluncurkan(Pratama dkk., 2022) .

Keamanan *Website* merupakan satu hal penting dalam perancangan sebuah *Website*. Kurangnya pemahaman dan kesadaran terhadap keamanan sistem dapat menjadi ancaman terutama bagi para pengembang(Hafsari, 2024). Apabila development melupakan tahapan pengujian keamanan *Website* akan berakibat fatal

untuk para pengguna yang telah mengisi data diri atau data pribadi, akan sangat mudah untuk para *hacker* membobol situs *Website* tersebut karena tidak dilakukan pengujian keamanan pada *Website* tersebut.

Terdapat beberapa metode untuk melakukan analisis keamanan, yaitu: vulnerability untuk strategi yang mengikuti pendekatan sistematis dan proaktif untuk menemukan sebuah kerentanan, jaringan atau aplikasi (Fachri dkk., 2021) Penetration Testing adalah metode penilaian dengan cara menguji kelemahan dari keamanan sistem, jaringan komputer ataupun kelemahan program aplikasi web(Prasetyo & Hassanah, 2021), *risk assessment* untuk menentukan prioritas tindakan keamanan yang perlu diambil, *code review* untuk mengidentifikasi kerentanan keamanan dan cacat potensial, *Port Scanning* untuk mengidentifikasi *Port* yang terbuka atau dapat diakses pada sistem atau jaringan.

Metode yang akan saya gunakan yaitu *Port Scanning* salah satu metode analisis keamanan *Website* yang umum digunakan, *Port Scanning* suatu proses memeriksa *Port-Port* yang terbuka atau dapat diakses pada suatu sistem atau jaringan. Dengan cara ini saya dapat mengetahui keterangan *Port* yang terbuka, tertutup dan terfilter. Terdapat 3 kategori status *Port* yaitu, "*Open*" atau terbuka berarti *Port* tersebut aktif dan siap untuk menerima koneksi dari jaringan ekternal, hal ini menunjukan adanya potensi titik masuk yang rentan terhadap serangan, "*Close*d" diklasifikasikan *Port* tidak aktif dan sistem menolak permintaan koneksi ke *Port* tersebut status tertutup menunjukan bahwa *Port* tersebut tidak dapat digunakan untuk mengirim atau menerima data, "Filtered" dapat diartikan sebagai filter, berarti koneksi ke *Port* tersebut diblokir atau diarahkan oleh firewall atau perangkat jaringan lainnya, status terfilter ini dapat terjadi ketika paket yang dikirim ke *Port* tidak diterima atau direspon oleh sistem target karena diblokir oleh kebijakan keamanan jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, dapat dituliskan rumusan masalah dalam penelitian ini yaitu sebagai berikut :

1. Bagaimana keadaan keamanan *Port Website* ?

2. Bagaimana mengetahui *Port* yang terbuka dan tertutup pada *Website* secara *automation*
3. Bagaimana sistem operasi *Host* yang digunakan oleh *Website*

1.3 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengidentifikasi keadaan keamanan *Website*
2. Mengidentifikasi *Port* yang terbuka dan tertutup pada *Website* secara *automation*
3. Mengidentifikasi sistem operasi *Host* yang digunakan oleh *Website*

1.4 Manfaat

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Bagi Akademisi
    a. Penelitian ini dapat digunakan sebagai bahan referensi untuk penelitian selanjutnya dan bisa lebih dikembangkan lagi dikemudian hari seiring berjalannya zaman
2. Bagi Peneliti
    a. Peneliti ini sangat bermanfaat untuk menambah ilmu pengetahuan atau wawasan mengenai metode *Port Scanning* pada KaliLinux
    b. Mahasiswa dapat mengetahui bagaimana langkah-langkah pengecekan *Port* yang terbuka dan tertutup.
    c. Mahasiswa dapat membuat GUI pengujian *Port* secara otomatis

1.5 Batasan Masalah

1. Penelitian ini hanya membahas keamanan *Port* pada *Website* yang terdiri dari :
    a. Pengujian menggunakan bantuan *tools* Gui Zenmap, KaliLinux untuk contoh awal pelaksanaan *scan Port*.
    b. Pengujian menggunakan cara *Port Scanning.*
    c. Rancangan pengujian dilakukan secara *automation.*

d. Pengujian keadaan direktori *Port* terbuka dan tertutup.
e. Pembuatan *automation* menggunakan NetBeans IDE 8.