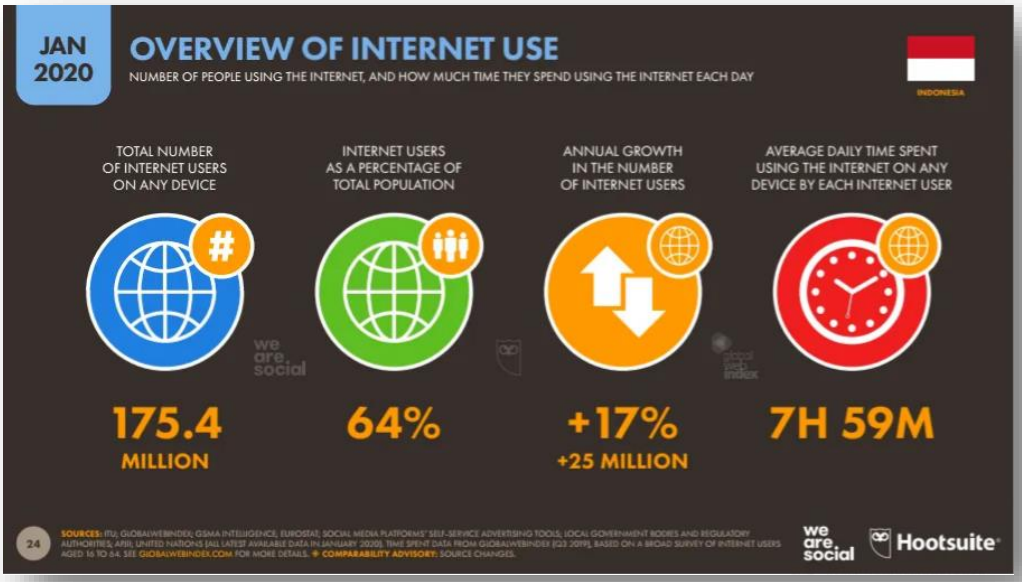
BAB 1

PENDAHULUAN

1.1 Latar Belakang

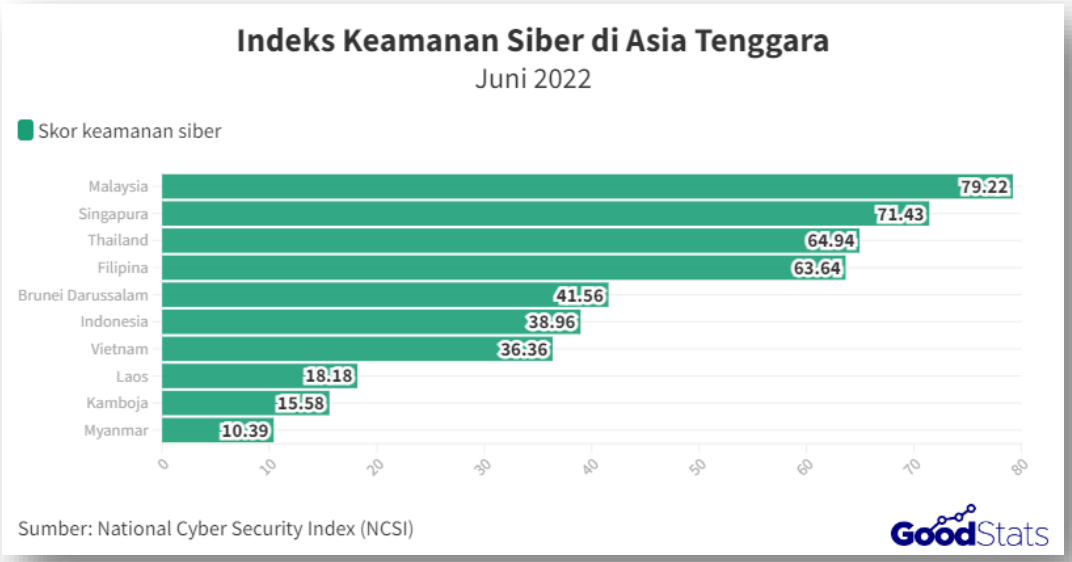
Perkembangan teknologi saat ini memberikan dampak positif di berbagai bidang, termasuk internet. Situs *website* adalah alternatif bagi korporasi untuk berkomunikasi, media promosi dan berinteraksi. *Website* ini dapat dengan mudah diakses oleh banyak orang dari mana saja dan kapan saja. Menurut laporan *digital We Are Social (Hootsuite)*, jumlah pengguna internet di Indonesia mencapai 175 juta pengguna pada awal Januari 2020. Jumlah pengguna yang menggunakan internet meningkat 17 persen atau 25 juta pengguna dalam setahun terakhir (Bagus Ramadhan, 2020).



Gambar 1 . 1 Jumlah Pengguna Internet di Indonesia menurut *We Are Social* dan *Hootsuite* pada Januari 2020
Sumber : (Bagus Ramadhan, 2020)

Setiap instansi harus memperhatikan keamanan data informasi yang tersimpan pada jaringan internet untuk mencegah gangguan dan tindak kejahatan. Gangguan tersebut dapat berupa serangan *Eksploitasi, Malware* dan *Injeksi database*. Menurut laporan *National Cyber Security Index* (NCSI), keamanan

siber Indonesia menempati urutan keenam di ASEAN dan ke-83 dari 160 negara di dunia (Naurah Nada, 2022).



Gambar 1 . 2 Indeks kemanan siber
Sumber:(Naurah Nada, 2022)

Negara Malaysia berada pada peringkat pertama memuncaki ASEAN *Best Cyber Security* dengan skor 79,22 dari 100 dan peringkat ke-19 secara global, sedangkan indeks keamanan Indonesia hanya 38,96 per Juni 2022 (Naurah Nada, 2022).

Dari data *National Cyber Security Index* (NCSI) tahun 2022, sebagian besar pengguna internet di indonesia masih belum menyadari akan pentingnya menjaga keamanan data dan informasi dalam beraktifitas di ruang siber. Pada dasarnya keamanan data sangat penting karena berkaitan dengan data pribadi *(privacy),* hak akses atau verifikasi *(autentication),* integritas *(integritiy),* ketersediaan *(availability)* dan kerahasiaan *(confidentiality)*. Seiring meningkatnya sumber daya manusia pemahaman dan kesadaran akan masalah pada sistem keamanan selalu menjadi ancaman setiap saat, terutama bagi pengembang aplikasi. Solusi untuk melindungi jaringan dari gangguan atau serangan hacker dapat dilakukan dengan *self-test*, yaitu pengujian yang dilakukan pada web server dengan tindakan yang sah seperti *hacker* salah satu metode *selftest* ini adalah *Penetration test* (Pentest).

Pengujian penetrasi aplikasi web adalah metode komprehensif untuk mendeteksi kerentanan sistem dalam pengujian penetrasi. Ada Beberapa metode dapat digunakan, salah satunya adalah *Open Web Application Security Project* (OWASP). Pada penelitian ini menggunkan metode OWASP *Top* 10 sebagai metode implementasi untuk pengujian penetrasi, metode OWASP dipilih karena bersifat *open sourc*e dan gratis untuk semua orang. *Open Web Application Security Project* (OWASP) didirikan pada tahun 2004 oleh OWASP *Foundation,* sebuah organisasi *non-profit* di Amerika Serikat. OWASP adalah organisasi internasional dan OWASP mendukung upaya OWASP di seluruh dunia. Mengingat keamanan *website* cukup penting untuk mencegah dari tindak kejahatan yang dilakukan oleh pihak yang tidak bertanggung jawab*,* Penelitian ini dilakukan uji penetrasi testing Mail Server lokal, Mail server adalah sebuah server yang bertugas untuk mengelola dan mengirimkan email di dalam suatu jaringan. Fungsi utama dari mail server adalah menerima, menyimpan dan mengirimkan pesan email antara pengguna yang menggunakan aplikasi email atau klien email. Penelitian ini dilaksanakan di Universitas Muhammadiyah Kalimantan Timur (UMKT) . Hasil dari penelitian akan direkomendasikan sebagai saran dan langkah-langkah untuk meminimalisir tingkat kerentanan pada sistem yang ada.

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang masalah sebelumnya, maka rumusan masalah dalam penulisan tugas akhir ini adalah menguji tingkat keamanan sistem pada *website mail server* lokal dengan uji penetrasi menggunakan metode OWASP *Top* 10.

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah Melakukan uji penetrasi pada domain *website mail server local* sebagai salah satu bentuk evaluasi sistem keamanan *website*.

1.4 Batasan Masalah

Batasan masalah ini dibuat agar tidak menyimpang dari pokok pembahasan penelitian, adapun batasan masalahnya sebagai berikut:

1. Metode yang digunakan pada penelitian ini adalah *Open Web Application*

Security Project (OWASP) *top* 10.

2. Penelitian ini dilakukan hanya untuk uji penetrasi pada *website mail server* lokal.
3. Hasil Penelitian ini berupa laporan yang tertulis.

1.5 Manfaat

Manfaat dari uji penetrasi bisa dapat mengidentfikasi kelemahan keamanan pada *website mail server*. Hasil dari uji penetrasi akan dijadikan saran maupun rekomendasi untuk perbaikan pada *website mail server*.