BAB I
PENDAHULUAN

1.1. Latar Belakang

Saat ini kemajuan teknologi di bidang sistem informasi *website* sudah menyebar hingga ke pelosok tanah air, desa, kabupaten, dan kota yang sudah menyebarluaskan informasi kepada masyarakat melalui situs *website*[1]. Dengan semakin meningkatnya pertukaran data melalui Internet, setiap instansi dituntut untuk selalu menjaga kerahasiaan, integritas dan *otentikasi* data pada suatu *website* sesuai standar internasional. Hal ini sebagian disebabkan oleh meningkatnya serangan siber. Belakangan ini banyak orang yang mulai menyadari bahwa informasi yang mereka berikan bisa saja disalah gunakan. Inilah sebabnya mengapa semakin banyak organisasi mulai memperhatikan risiko keamanan informasi yang dapat berdampak negatif dan merugikan terhadap proses bisnis, citra, dan instansi[2].

Perlu disadari bahwa sistem informasi website merupakan sumber daya yang sangat penting dalam sistem informasi suatu instansi. Karena ini adalah sumber daya untuk meningkatkan nilai bisnis. Data penting ini juga perlu dicadangkan agar terhindar dari Ancaman dan kerusakan kredensial. Tujuannya adalah untuk terhindar dari ancaman terhadap sistem dan mendeteksi kebocoran sistem informasi serta kerusakan pada web server. Salah satu ancaman yaitu serangan *hacking*. *Hacking* ini dapat meretas dan merusak serta membocorkan informasi yang dimiliki oleh pihak instansi.

Instansi Rumah Sakit Umum Daerah Provinsi NTB salah satu lembaga yang bergerak pada bidang kesehatan yang memanfaatkan jaringan internet yaitu web sebagai media yang digunakan untuk menyampaikan informasi kepada pihak luar dengan menghubungkan integritas yang dapat memudahkan dalam menyampaikan informasi, Namun pihak instansi rumah sakit umum daerah provinsi perlu menyadari bahwa tidak hanya pihak yang memiliki akses saja yang dapat mengakses sistem informasi *website*. Namun, ada pihak-pihak lain yang tidak bertanggung jawab dapat mengakses dan menyalahgunakan

informasi yang ada sehingga menyebabkan pihak instansi memiliki kerugian[3].

Sehingga langkah yang dapat dilakukan adalah dengan melakukan analisa keamanan pada website tersebut dengan melakukan pengujian penetration testing yang dapat mengumpulkan informasi yang sensitif pada website. Mengingat pentingnya data-data tersebut maka perlu di terapkan pengujian keamanan pada instansi Rumah Sakit Umum Daerah Provinsi NTB untuk mengetahui kondisi dan pengukuran tingkat keamanan pada Rumah Sakit Umum Daerah dengan menggunakan framework Penetration Testing Execution Standard (PTES) sebagai acuan dalam penelitian ini.

1.2. Rumusan Masalah

Berdasarkan permasalahan yang telah diidentifikasi sebelumnya maka dapat di rumuskan masalah yaitu:

a. Seberapa efektifkah metode yang digunakan dalam melaksanakan *penetration testing* pada sistem keamanan web lembaga RSUD Provinsi NTB?
b. Apa yang perlu diupayakan setelah melakukan *penetration testing* pada sistem *website* tersebut?
c. Bagaimana cara untuk mengetahui kondisi dan pengukuran tingkat kerentanan pada sistem *website* RSUD Provinsi NTB?

1.3. Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini bertujuan untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah agar penelitian ini lebih terarah adalah sebagai berikut:

1. Penelitian ini melakukan analisis terhadap celah keamanan sistem *website* yang ada pada instansi RSUD Provinsi NTB.
2. Penelitian ini menggunakan sistem operasi Kali Linux dan Windows dalam pengujiannya, distro (2023, (64-bit) untuk kali Linux dan OS Windows 10.

3. Membahas tentang metode yang akan digunakan yaitu metode *PTES (Penetration Testing Execution Standard)* dijadikan sebagai acuan dalam melakukan *penetration testing*.
4. Hasil pada penelitian ini bukan untuk melakukan serangan yang berbahaya agar situs *website* mengalami kendala dan berbagai kerusakan lainnya. melainkan untuk memberikan solusi agar sistem *website* tersebut aman dari serangan *hacker*.
5. Hasil penerapan dari rekomendasi akan diserahkan sepenuhnya pada kewenangan instansi terkait yaitu RSUD Provinsi NTB.

1.4. Tujuan Penelitian

1. Untuk mengetahui celah keamanan pada website RSUD NTB dan dapat dilakukan tindakan penanggulangan.
2. Mengimplementasikan metode *PTES (Penetration Testing Execution Standard)* pada *website* RSUD NTB.
3. Dapat membantu pihak instansi Rumah Sakit dalam melakukan evaluasi keamanan pada *web server* yang mereka miliki.
4. Memberikan media informasi atau edukasi yang baru tentang bagaimana mengamankan suatu sistem *website* yang akan berguna untuk melindungi sistem dari serangan *hacker*.

1.5. Manfaat Penelitian

a) Bagi Peneliti
   1. Menyampaikan informasi terkait tentang kelemahan dan kekurangan pada keamanan website kepada pihak instansi RSUD Provinsi NTB.

b) Bagi instansi RSUD Provinsi NTB
   1. Mengetahui seberapa jauh tingkat keamanan website terhadap serangan yang dapat merugikan pihak instansi RSUD NTB.
   2. Mengetahui celah keamanan pada sistem *website* RSUD NTB, Sehingga dapat melakukan tindakan penanggulangan celah keamanan yang berbahaya.

1.6. Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini merupakan bagian pengantar dari pokok permasalahan yang dibahas dalam skripsi ini. Adapun hal-hal yang di bahas berisikan latar belakang(1), rumusan masalah(2), batasan masalah(3), tujuan penelitian(4), manfaat penelitian(5), dan sistematika penulisan(6).

BAB II LANDASAN TEORI

Bab yang berisi tentang tinjauan pustaka(1), dasar teori(2),

Pengertian metode *PTES (Penetration Testing Execution Standard)* yang menguraikan konsep dasar yang mendukung dalam perencanaan dan analisis sistem *website*, serta teori-teori yang berkaitan dengan topik penelitian dari sumber pustaka dan referensi yang menjadi landasan dasar dalam analisis keamanan, dan implementasi, serta hal-hal yang berguna dalam proses analisis permasalahannya.

BAB III METODE PENELITIAN

bab yang berisi tentang metode penelitian(1), objek penelitian(2), alur penelitian(3), tahap dalam melakukan penetration testing(4), alat dan bahan yang digunakan untuk pentes (perangkat keras (Hardware) dan perangkat lunak (Software))(5), perencanaan dan skenario pengujian(6). yang dilakukan secara sistematis yang memberikan gambaran dan alur dari penelitian yang akan dilakukan.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini membahas tentang hasil dan pembahasan tentang landasan teori yang berkaitan dalam penelitian ini seperti, Langkah-langkah untuk dalam pengujian penetration

testing dan hasil yang didapatkan dari proses penetration testing yang dilakukan kepada website target yang sudah di tentukan.

BAB V PENUTUP

pada bab ini yang berisi tentang kesimpulan dari hasil analisis dan pengujian pada *web server* serta saran yang dapat diberikan untuk mengembangkan aplikasi web dan menjadi masukan pihak instansi maupun penelitian selanjutnya dalam analisis keamanan sistem *website*.