BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan yang terhubung dengan internet yang sifatnya publik dan global pada dasarnya tidak aman apalagi berkaitan dengan informasi atau data. Keberadaan suatu informasi atau data sangatlah berharga, maka tidaklah heran jika kemudian bermunculan beberapa pihak yang tidak bertanggung jawab, dimana pihak tersebut berusaha mencuri maupun merusak dan mengubah data atau informasi.[1]. Berbagai cara dapat digunakan untuk mendeteksi serangan atau penyusupan. Dengan teknik-teknik tersebut kita dapat memblok, mengizinkan, atau menyaring paket yang mencoba masuk ke dalam jaringan atau ingin mengakses sumberdaya.[2]

Pengukuran atau assessment adalah hal yang mutlak dilakukan untuk mendapatkan peningkatan kualitas. Suatu perusahaan dapat meningkatkan penjualannya bila mengetahui bagaimana tingkat penjualannya, bagaimana efisiensinya. Dengan adanya pengukuran maka perusahaan dapat mengetahui kelemahan yang ada, membandingkannya dengan contoh penerapan di perusahaan lain dan ujungnya adalah peningkatan keuntungan perusahaan.[3]

Salah satu cara meningkatkan sistem keamanan informasi adalah dengan *vulnerability assessment* (penilaian kerentanan). Melakukan penilaian kerentanan merupakan proses mengidentifikasi, mengukur, dan memprioritaskan (memberi peringkat) sebuah kerentanan dalam suatu sistem yang meliputi information *technology systems, energy supply systems, water supply systems, transportation systems,* dan *communication systems.*

Penilaian kerentanan juga memberikan gambaran terkait kelemahan keamanan dalam lingkungan organisasi, memberikan arahan dalam menilai risiko dan ancaman yang terus berkembang. Proses ini memberikan pemahaman mengenai aset organisasi, sistem keamanan dan risiko yang dihadapi, serta mengurangi kemungkinan adanya *cyber crime attack* yang akan menyerang sistem organisasi, perusahaan dan institute.[4]

Menurut *GOV-CSIRT (Government Computer Security Incident Response Team)* pada tahun 2021,. *Vulnerability* atau kerentanan dibagi menjadi beberapa penilaian yaitu; *High* (tinggi) pada *level* ini terdapat kelemahan yang berpotensi tinggi menjadi ancaman, sedangkan fitur atau langkah untuk tingkat pencegahan maupun penaganannya tidak memadai, *Medium* (sedang) pada *level*

ini tingkatan kelemahan bersifat lokal dan upaya penanganan dan pencegahan bersifat lokal juga. *Low* (rendah) *level* kelamahan ini adalah rendah, upaya pencegahan dan penaganan yang diharapkan sangat memadai, *informational* (info) *level* kerentanan ini adalah menunjukan informasi, upaya pencegahan dan penanganan yang diharapkan sangat memadai.[5]

Oleh karena itu pada tugas akhir ini penulis membuat usulan untuk melakukan penilaian vulnerability website menggunakan *scanning tools* untuk meningkatkan sistem keamanan untuk membantu dan juga mencari solusi agar terhindar dari *cyber crime attack* pada sebuah organisasi, perusahaan, dan juga institute.

1.2 Rumusan Masalah

Dari uraian latar belakang masalah yang telah dijabarkan diatas maka penulis merumuskan beberapa pokok – pokok masalah yang akan diteleti :

1. Bagaimana langkah pengerjaan dari penilaian kerentanan untuk memberikan gambaran terkait kelemahan sistem keamanan dengan menggunakan aplikasi *Owasp Zap (Zed Attack Proxy)* dan *Nmap (Network Mapper)*
2. Bagaimana hasil dari langkah pengerjaan dari penilaian kerentanan menggunakan aplikasi *Owasp Zap (Zed Attack Proxy)* dan *Nmap (Network Mapper)*

1.3 Batasan Masalah

Beberapa batasan masalah peneliti angkat dalam penelitian untuk menyelesaikan tugas akhir ini adalah :

1. Tools yang digunakan untuk melakukan penilaian kerentanan adalah *Znmap(Nmap) dan Pentest-Tools.com (Web Scanning Online).*
2. Pengujian terhadap *website* yang diteliti dilakukan dengan pengujian otomatis dari *vulnerability tools* yang meliputi *Scanning Port, Website Fingerprinting, Version-based Vulnerability Detection dan Common Consequenses Issues.*

1.4 Tujuan Penelitian

Dalam melakukan kegiatan penelitian tugas akhir penulis mempunyai tujuan yang ingin dicapai yaitu :

1. Menemukan Celah Keamanan yang dimiliki pada Website menggunakan *tools Owasp Zap (Zed Attack Proxy)* dan *Nmap (Network Mapper).*

2. Memberikan rekomendasi tindakan yang harus dilakukan setelah dilakukannya *scanning vulnerability*.
3. Meminimalisir ancaman yang dapat merugikan perangkat yang dimiliki.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat :

1. Hasil penelitian dapat digunakan sebagai bahan referensi terhadap upaya peningkatan keamanan pada website
2. Dapat memberikan masukan dalam mengembangkan kemampuan akademis dalam menerapkam teori penilaian vulnerability pada website.

1.6 Metodologi Penelitian

Pada pembuatan penelitian tugas ini, penulis melakukan metodologi penelitian dengan menggunakan metode sebagai berikut :

1. Studi Literatur

   Metode ini dilakukan dengan membaca beberapa referensi buku dari berbagai sumber yang terdapat di perpustakaan kampus atau perpustakaan lain dan membaca beberapa jurnal Nasional maupun Intenasional yang berhubungan dengan permasalahan yang akan dibahas serta mencari data dari berbagai situs internet yang diharapkan dapat mendukung perancangan tugas ini.
2. Observasi

   Pada tahap ini akan dilakukan pengamatan terkait dengan data yang dibutuhkan untuk proyek akhir nantinya.
3. Analisa

   Merupakan metode yang dilakukan untuk mengetahui permasalahan yang terjadi secara detail berdasarkan data yang telah dilakukan sebelumnya dengan menggunakan parameter yang sudah ada sehingga bisa mendapatkkan sebuah informasi yang akan dijadikan acuan.

1.7 Sistematika Penulisan

Secara umum sistematika penulisan proyek akhir ini terdiri dari bab-bab dengan metode penyampaian sebagai berikut :

BAB I PENDAHULUAN

Bab pendahuluan mendeskripsikan mengenai latar belakang, rumusan masalah, batasan penelitian, tujuan penelitian, manfaat, metodologi dan sistematika penelitian.

BAB II DASAR TEORI

Bab ini berisi tentang penelitian yang merupakan penelitian-penelitian terdahulu yang berkaitan dengan yang dikerjakan dan juga landassan pustaka yang berisi teori-teori yang mendasari landasan.

BAB III PERANCANGAN ANTENA DAN SIMULASI

Dalam bab ini penulis mengemukakan perancangan serta analisa penelitian yang dilakukan dalam implementasi vulnerability assessment tools untuk meningkatkan sistem keamanan informasi.

BAB IV HASIL PENGUKURAN DAN ANALISIS HASIL PENGUKURAN

Dalam bab ini berisi tentang langkah dari implementasi beserta hasil dari implementasi vulnerability tools untuk meningkatkan sistem keamanan informasi

BAB V PENUTUP

Pada bab ini menjelaskan kesimpulan dari penelitian dan saran-saran sebagai pertimbangan untuk penelitian selanjutnya.