BAB 1

PENDAHULUAN

1.1 Latar Belakang

Lembaga XYZ adalah Lembaga pemerintah nonkementerian Indonesia yang melaksanakan tugas pemerintahan di bidang pengawasan keuangan dan pembangunan yang berupa Audit, Konsultasi, Asistensi, Evaluasi, Pemberantasan KKN serta Pendidikan dan Pelatihan Pengawasan sesuai dengan peraturan yang berlaku.

Hasil pengawasan keuangan dan pembangunan dilaporkan kepada Presiden selaku kepala pemerintahan sebagai bahan pertimbangan untuk menetapkan kebijakan-kebijakan dalam menjalankan pemerintahan dan memenuhi kewajiban akuntabilitasnya. Hasil pengawasan Lembaga XYZ juga diperlukan oleh para penyelenggara pemerintahan lainnya termasuk pemerintah provinsi dan kabupaten/kota dalam pencapaian dan peningkatan kinerja instansi yang dipimpinnya. Lembaga XYZ juga senantiasa berkomitmen untuk memberikan pelayanan yang terbaik dan perlindungan data informasi kepada pengguna jasa mereka, menerapkan praktik tata kelola perusahaan yang baik, meningkatkan kesejahteraan karyawan dan keluarganya serta meningkatkan kepedulian sosial terhadap masyarakat umum dan lingkungan sekitar lembaga XYZ melalui program Social Responsibility.

Banyak Instansi Pemerintah yang berlomba-lomba untuk *go-online* demi perluasan bisnis yang mereka lakukan. Selain itu dengan internet, banyak biaya yang dapat dipangkas oleh Instansi Pemerintah yang akan menggunakan teknologi internet sebagai media penjualannya seperti biaya kertas, biaya promosi fisik dan biaya-biaya lainnya.

Website xyz.co.id yang juga merupakan salah satu pengembangan dalam pengaplikasian teknologi informasi pada umumnya dan internet khususnya pada Instansi Pemerintah menjadi salah satu faktor penting dalam menjalin hubungan antara Instansi Pemerintah dan costumer.

Menurut (jelajahinternet.com,2016), Website atau situs adalah halaman web yang saling berhubungan yang umumnya terletak di pelayanan yang sama berisi kumpulan informasi yang diberikan oleh seorang individu, kelompok, atau organisasi.

Menurut (Yuhefizar,2015), web adalah metode untuk menampilkan informasi internet, baik itu berupa teks, gambar, video dan suara maupun interaktif memiliki keuntungan yang menghubungkan (link) dari dokumen dengan dokumen lainnya (*hypertext*) yang dapat diakses melalui browser.

Dengan melihat peluang yang baik ini, lembaga XYZ sebagai Instansi pemerintah berusaha membangun sebuah *website* sebagai sarana pemberi informasi kepada setiap orang yang mengaksesnya. Setiap orang dapat mengakses informasi Instansi Pemerintah secara umum ataupun secara khusus. *Website* ini juga berguna untuk memberikan informasi mengenai pelayanan-pelayanan yang diberikan Instansi Pemerintah, selain itu dalam penerapanya secara tidak langsung lembaga XYZ sudah merapkan *e-government* bagi birokrasi pemerintahan dan

diharapkan dapat menjadi alternatif bagi reformasi birokrasi menuju pelayanan yang lebih baik

Menurut informasi dari kepala divisi IT pada penerapan website Lembaga XYZ selama 2 tahun terakhir ini telah mendapatkan serangan seperti pada Table 1.1 :

No	Tahun	Serangan
1	2019	*DDOS (Distributed Denial of Service*
2		*host header attack*
3	2018	*SQL Injection*
4		*Bruteforce Attack*

Table 1.1 Daftar Serangan Selama Tahun 2018 - 2019

Dengan merujuk pada Table 1.1 dapat dilihat banyaknya serangan yang ditimbulkan dalam pengaplikasian website maka diperlukan manajemen risiko sistem informasi terhadap website. Dengan melihat kerentanan tersebut dan hasil yang ditimbulkan dari serangan tersebut merugikan lembaga XYZ seperti hilangnya data perusahaan, laporan cabang Lembaga XYZ bocor, tampilan website berubah tanpa sebab, dan. Akses yang terganggu untukckaryawan dalam melakukan transaksi dan komunikasi antar kayawan, maka diperlukan manajemen risiko dengan pengukuran CVSS sistem informasi terhadap website.

Perlu diterapkan suatu keamanan yang lebih baik, dengan melakukan analisis keamanan website dengan metode *Scanning vulnerability assessments* menggunakan aplikasi acunetix untuk menganalisis keamanan pada suatu website.

Setelah itu dilakukan perhitungan *CVSS (Common Vulnerability Scoring System) base metrics.* Alasan utama dalam penerapan CVSS adalah karena CVSS

merupakan standar industri bebas dan terbuka untuk menilai tingkat kerentanan keamanan sistem computer yang terbaru. CVSS berupaya untuk menetapkan skor tingkat keparahan untuk kerentanan, memungkinkan responden untuk memprioritaskan respons dan sumber daya sesuai ancaman.

Hasil dari perhitungan *CVSS base metrics* dengan menggunakan formula base score menunjukkan nilai pengukuran untuk menilai suatu kerentanan terhadap sistem. CVSS akan menilai kerentanan dariskor 0.0 – 10.0 yang dimana terbagi menjadi 3 aspek, yaitu :

- Low (0.0 – 3.9)

  Kerentanan dalam kelas rendah biasanya memiliki dampak yang sangat kecil pada bisnis organisasi. Eksploitasi kerentanan semacam itu biasanya memerlukan akses sistem lokal atau fisik.

- Medium (4.0 – 6.9),

  1. Kerentanan yang membutuhkan penyerang untuk memanipulasi korban individu melalui taktik rekayasa sosial.
  2. DOS yang sulit diatur.
  3. Eksploitasi yang membutuhkan penyerang untuk berada di jaringan lokal yang sama dengan korban.
  4. Kerentanan di mana eksploitasi hanya menyediakan akses yang sangat terbatas.
  5. Kerentanan yang memerlukan hak pengguna untuk eksploitasi yang berhasil.
  6. Eksploitasi dapat menyebabkan kehilangan atau downtime data yang signifikan.

- High (7..0 – 10.0) (first.org).

  Merupakan kerentanan yang mempunyai pengaruh kemungkinan menghasilkan kompromi tingkat dasar dari server atau perangkat infrastruktur. Dan Eksploitasi biasanya mudah, dalam arti bahwa penyerang tidak memerlukan kredensial otentikasi khusus atau pengetahuan tentang korban individu, dan tidak perlu membujuk pengguna target, misalnya melalui rekayasa sosial, untuk melakukan fungsi khusus apa pun.

Setelah pengukuran *CVSS* sudah dilakukan kemudian langkah selanjutnya adalah pemetaan risiko kerentanan yang dimungkinkan terjadi dengan menggunkan Standar baru *ISO 31000: 2009* untuk yang bersifat memfasilitasi perbaikan dan pengembangan berkelanjutan bagi *website* XYZ

Kebutuhan organisasi pada masa kini yang berada di lingkungan persaingan yang sangat ketat memerlukan sistem keamanan yang mampu menjaga keberlangsungan kehidupan organisasi dalam jangka panjang. Oleh karena itu, pada tanggal 13 November 2009, di *Genewa Switzerland*, organisasi *ISO* (*International Organization for Standardization*) menerbitkan Standar baru *ISO* 31000: 2009 yang mengatur pedoman suatu standar implementasi manajemen risiko. Manajemen risiko bersifat memfasilitasi perbaikan dan pengembangan berkelanjutan sebagai organisasi.

Dalam penerapanya, kerentanan dalam suatu website dapat terjadi dan menimbulkan impack yang cukup membuat proses kegiatan perusahaan mengalami suatu kendala, Dengan memperhatikan hal–hal tersebut, Pemerintah dalam hal ini telah berupaya melakukan pengendalian dengan mengeluarkan

peraturan pemerintah yang di dalam peraturan tersebut terdapat ketentuan yang mengatur rencana keberlangsungan kegiatan (Business Continuity Plan) yang salah satunya adalah tata kelola TI (IT Governance). Pemenuhan atas peraturan–peraturan tersebut tertuang pada:

a) Peraturan Presiden RI No. 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika.

Berdasarkan uraian diatas, maka dari itu Instansi Pemerintah memerlukan sebuah mekanisme agar Instansi Pemerintah tetap dapat menjaga keamanan website. Berkaitan dengan hal itu, penulis memberi judul skripsi ini "PENGUKURAN KINERJA SISTEM KEAMANAN PADA WEBSITE XYZ MENGGUNAKAN PERHITUNGAN CVSS BASE MATRIKS", dan menggunakan website lembaga XYZ sebagai media penlitian dan diharapkan mampu memberikan rekomendasi terhadap Instansi Pemerintah dalam hal sistem pengamanan website dengan memertimbangkan risiko dan ancaman yang ada.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, perumusan masalah pada penelitian ini adalah sebagai berikut:

1. Mengapa terjadi serangan pada *Website* XYZ ?
2. Apa saja kerentanan dan tingkatan risiko yang dapat menggangu keamanan *website* XYZ?
3. Apakah Penanganan yang harus dilakukan oleh Lembaga XYZ terhadap kerentanan yang ada?

1.3 Tujuan Penelitian

Berdasarkan permasalahan yang telah disebutkan diatas, tujuan penelitian yang hendak penulis capai ialah sebagai berikut:

1. Mengidentifikasi Faktor apa saja penyebab terjadinya jadi serangan pada *Website* XYZ.
2. Menganalisa dan mengukur pengaruh kerentanan website terhadap dampak yang ditimbulkan.
3. Memberikan rekomendasi penanganan dampak yang ditimbulkan.

1.4 Manfaat Penelitian

Manfaat yang hendak dicapai dalam penelitian ini adalah sebagai berikut:

a. Memberikan manfaat praktis bagi lembaga XYZ, khususnya pemangku kepentingan dan penegelola sistem informasi dalam manajemen risiko keamanan sistem informasi sesuai standar sistem informasi.
b. Memberikan pemahaman yang benar kepada lembaga XYZ tentang pentingnya keamanan sistem informasi khususnya management IT.
c. Mendapatkan informasi dari hasil analisa dan evaluasi untuk perbaikan manajemen risiko keamanan sistem informasi lembaga XYZ di waktu mendatang.

1.5 Ruang Lingkup Penelitian

Berikut merupakan batasan masalah yang bertujuan mempermudah agar lebih terarah dan berjalan dengan baik. Adapun ruang lingkup yang akan dibahas dalam penulisan ini, yaitu:

1. Penelitian dilakukan dengan mengandalkan *Computer Assisted Audit Techniques (CAATs) yaitu software Acunetix Web Vulnerability Scanner 9.5* dengan pengujian keamanan terhadap *website* dari aspek *web* dan *port*.
2. Pengukuran menguunakan alat bantu CVSS Calculator
3. Dalam penelitian berfokus hanya sampai tahap pengukuran dan rekomendasi atas temuan kerentanan dalam website tersebut.
4. Analisa keamanan dilakukan terhadap *website* dengan alamat *domain* yang telah disepakati oleh pihak perusahaan.
5. Nama perusahaan dan alamat domain *website* dirahasiakan dan dikarenakan bersifat sensitif dan dapat mengganggu keamanan informasi perusahaan.
6. Berfokus pada Base Matriks CVSS