BAB I

PENDAHULUAN

1.1. Latar Belakang

Pesatnya perkembangan sebuah teknologi informasi saat ini, serta mudahnya dalam mengakses suatu informasi yang kita inginkan secara cepat. Dalam hal ini informasi sangat penting untuk membangun potensi sebuah institusi yang dikolaborasikan dengan teknologi internet sehingga dapat memajukan dan menjadi animo magnetik untuk mengundang penduduk dunia untuk tertarik melihat informasi tersebut. Perkembangan informasi era digital ini bukanlah lagi komunikasi dalam satu arah melainkan komunikasi dua arah atau disebut *dynamic communication*, dimana penduduk dunia dapat merespons dengan cepat terhadap informasi yang didapatkan dengan lahirnya teknologi web 2.0 yang tren saat ini.

Kita mengetahui perkembangan dan kemajuan web yang sangat cepat dimulai dari web 1.0, web 2.0 sampai web 3.0 bahkan web 4.0 , dimana teknologi yang dikeluarkan tersebut mempunyai sebuah kemajuan yang berbeda-beda pada teknologi yang dikeluarkannya. Penyebaran informasi dalam era digital ini menyentuh seluruh lapisan masyarakat mulai dari kalangan individual, organisasi sampai komunitas serta kepentingan yang berbeda-beda pula sepertihalnya untuk kepentingan bisnis (*business*), Pemerintahan (*government*) , perorangan (*individual*) hingga jaringan pertemanan (*social networks*) . Kita sadar dibalik teknologi yang ada tersebut serta penyampaian informasi yang sangat mudah dengan adanya teknologi web aplikasi terhubung internet sehingga seluruh dunia dapat menjamah ataupun mengakses dengan mudah itu terdapat kerugian yang sangat besar nilainya jika kita tidak sadar yaitu ancaman keamanan suatu informasi (*information security threat*), tanpa kita sadaripun informasi yang kita *publish* untuk khalayak umum dalam dunia maya tersebut terancam nilai

informasinya.

Saat ini menurut statistik jumlah web portal informasi Pemerintah dari jenis *public domain* sampai subdomain hampir sudah berjumlah kurang lebih ada 1000 domain web portal Pemerintah yang berdomainkan .go.id. Pada tahun belakangan ini juga sering kita dengar insiden-insiden kriminal dalam dunia maya atau di sebut *cyber crime* ataupun *cyber war* (perang dunia cyber) . Salah satunya yang sering kita dengar adalah *web defacement* / perubahan halaman utama suatu web portal.

Seperti kita ketahui dan kita dengar insiden *cyber war* atau perang dunia cyber antara indonesia vs malaysia maupun dalam lokal sendiri kita juga dengar amat sering terdengar perubahan halaman web / *defacement* yang dilakukan oleh *hacker* maupun *cracker* dalam negri maupun luar negri. Dimana kejadian tersebut di latarbelakangi berbagai versi antara lain : politik, ekonomi, sosial, budaya yang ada pada permasalahan dalam negri tersebut ataupun hanya mencari sensasi untuk menjadi terkenal didunia maya..Tak hanya itu saja terkait juga masalah hukum dan undang-undang informasi transaksi elektronik (UU ITE) No. 11 tahun 2008, yaitu pasal 16 ayat (1) huruf b Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengamanatkan kewajiban penyelenggara sistem elektronik, baik privat maupun publik untuk mengoperasika sistem elektronik yang dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan , dan keteraksesan Informasi Elektronik [BSU10].

Oleh karena itu c*onfidentiality, integrity, availabillity* serta *non repudation* suatu web harus dijaga terlebih pada situs web portal Pemerintah, dimana informasi tersebut harus dijaga seoptimal mungkin jangan sampai jatuh ketangan yang bukan haknya dalam hal ini adalah pelaku yang berada dalam negeri maupun luar negri. Perlu kita ketahui juga bahwa keamanan dalam menjaga informasi bukanlah sebuah produk maupun teknologi tapi adalah sebuah proses yang berkepanjangan serta *awareness* pada sisi *user* atau sering disebut *security is process and security is not product or technology*.

1.2. Masalah Penelitian

Seperti Penulis sudah paparkan diatas melalui latar belakang dari penelitian ini, sebuah kemajuan teknologi informasi yang sangat pesat, pentingnya sebuah keamanan untuk menjaga infomasi yang dapat di akses ke seluruh dunia sehingga nilai c*onfidentiality, integrity, availabillity,authenticatioan* serta *non repudation* pun harus dijaga pada suatu web portal Pemerintah. Salahsatunya ialah minimnya kesadaran (*awareness*) serta kurang *care* arti menjaga sebuah keamanan informasi di sebuah institusi Pemerintah yang tertuang dalam web portal.

1.2.1. Identifikasi Masalah

Kejadian yang bermunculan atau insiden yang pernah kita dengar ketika terjadinya manipulasi tabulasi suara dalam pemilihan umum yang di selenggarakan oleh KPU secara online di http://www.kpu.go.id yang mengakibatkan perubahan konten, seperti penambahan item partai yang dilakukan oleh *unauthorized user* akibat adanya celah kelemahan terhadap sistem tersebut. Celah keamanan tersebut salah satunya adalah *SQL Injection, Cross Site Scripting, HTTP Directory Listing, System Path Discloser*, dan lain sebagainya. Tetapi yang marak terjadi yaitu serangan *web defacement* pada situs-situs web portal Pemerintah di Indonesia, entah itu situs web portal Pemerintah Pusat maupun Daerah serta hampir setiap harinya serangan *web defacement* tersebut terjadi, ternyata insiden atau kejadian hal tersebut dapat dilihat di beberapa situs yang mempublikasikan kejadian tersebut, yaitu di http://www.zone-h.org/ , http://www.deface.us , http://wappsec.wordpress.com . Sampai saat ini instansi Pemerintah yang bertanggungjawab hal tersebut, belum mempunyai sistem yang mengukur keamanan informasi pada web portal tersebut, serta menganalisa keamanan web portal Pemerintah. Sebagai contoh jika kita melihat di suatu situs keamanan informasi seperti http://www.whitehatsec.com dalam *website security statistic report* 9 th *Edition Spring* 2010 [WHS10] telah dilakukan *review* tentang keamanan website dari data 1 Januari 2006 sampai 25 Maret 2010 menyatakan :

- Hampir tiap bulannya terdapat *multiple* kelemahan pada website portal
- Dari 1,659 total *website* , sebanyak 300 organisasi yang baru memulai keamanan website dan serius menangani tentang keamanan website
- 24, 286 website telah diverifikasi rentan terhadap keamanan

Kita bisa melihat hasil dari *review* tersebut, masih rentannya keamanan terhadap website yang tidak hanya tertuju pada sisi teknis saja tetapi pada tingkat pengelolaannya. Lalu bagaimana di Indonesia saat ini, mungkin serangan yang masih sering dalam bentuk *web defacement* saja. Tetapi ketika sudah menuju *e-government* dimana semua aplikasi sudah terintegrasi dalam *on line system„* kita bisa bayangkan ketika sistem tersebut diserang, yang terjadi di belahan eropa dimana sistem pembangkit listriknya ataupun sistem penerbangannya di susupi oleh *cracker,* maka lumpuhlah semua sistem tersebut, dengan demikian lumpuh pula perekonomian negara tersebut dalam sekejap. Mungkin Indonesia belum masuk pada tahap tersebut dimana layanan strategis suatu negara tersentralisasi pada suatu sistem berbasis aplikasi. Tetapi kita sebagai warga negara harus memikirkan hal tersebut sejak dini.

1.2.2. Batasan Masalah

Penulis dalam hal ini mempunyai batasan masalah riset mengenai sejauh mana kerentanan terhadap ancaman (*threat*) atau serangan pada keamanan web portal Pemerintah, seperti : *web defacement, sql injection, cross site scripting (xss), cross site forgery request (csrf),* menganalisa ancaman (*threat*) web portal Pemerintah dan *attack model* (model serangan). Terkait waktu, tenaga, dan keterbatasan akses, penulis hanya membataskan pada batasan masalah tersebut diatas.

1.2.3. **Rumusan Masalah**

Setelah mengidentifikasi masalah dan batasan masalah dalam penelitian, maka perumusan beberapa masalah untuk riset ini, adalah sebagai berikut :

- Faktor – faktor yang diperlukan untuk mendukung pembangunan keamanan web portal Pemerintah
- Bagaimana membangun model keamanan web portal Pemerintah

1.3. Tujuan Penelitian

Berdasarkan dari rumusan masalah dari penelitian atau riset ini, maka tujuan dari penelitian ini adalah, sebagai berikut :

- Identifikasi kelemahan-kelemahan yang ada pada web portal Pemerintah.
- Membangun model keamanan web portal Pemerintah, berdasarkan ancaman pada kelemahan web portal Pemerintah

1.4. Manfaat Penelitian

Sedangkan manfaat dari penelitian ini adalah sebagai berikut :

- Sektor Pemerintah

Semoga dengan adanya penelitian ini bisa dijadikan sebagai tolok ukur untuk merumuskan kebijakan (*policy*), strategi (*strategy*), panduan (*guidance*), *best practice* kedepannya agar terwujud konsep keamanan informasi pada instansi Pemerintah serta *user* maupun pemangku kebijakan lebih *aware* dan *care* terhadap pentingnya keamanan informasi.

- Sektor Swasta

Dengan adanya penelitian ini, sektor swasta mungkin sudah lebih baik, sehingga bisa dapat dijadikan referensi untuk bisa mengambil strategi keamanan web site portalnya masing-masing.

- Sektor Peneliti

Mudah-mudahan dengan adannya penelitian ini bisa dijadikan kajian tersendiri untuk bisa lebih berinovasi lagi dalam meneliti tentang keamanan informasi

khususnya web site portal.

- Sektor Pembaca dan Peneliti lainnya

Penelitian ini bisa dijadikan referensi untuk penelitian berikutnya, guna referensi bagi sistem yang akaan dikembangkan mereka supaya lebih baik lagi.

1.6. Tata Urut Penulisan

Naskah ini disusun dengan tata-urut sebagai berikut :

BAB I PENDAHULUAN, yang membahas latar belakang pembuatan pedoman penyusunan tesis, maksud dan tujuan, ruang lingkup, tata-urut dan pengertian yang tercantum dalam naskah ini.

BAB II LANDASAN/PEMIKIRAN, yang membahas dasar-dasar penyusunan tesis yaitu tugas akhir kesarjanaan, metode ilmiah, proses penelitian ilmiah, jenis penelitian dan laporan penelitian.

BAB III DESAIN PENELITIAN, dalam bab ini yang akan membahas langkah-langkah/pentahapan proses penulisan tesis di MKOM beserta aturan-aturan teknis perwajahan naskah dan tertib penulisan.

BAB IV ANALISIS, INTERPRETASI, DAN IMPLIKASI PENELITIAN, berisi hasil proses penelitian, beserta data-data yang didapatkan untuk mencapai hasil hipotesis.

BAB V PENUTUP, yang berisi kesimpulan uraian pembahasan pedoman tesis.

1.7. Daftar Pengertian

Apache	merupakan aplikasi layanan untuk menjalankan scipt-script yang akan diterjemahkan ke dalam browser aplikasi berbasiso*pensource software* (OSS)
Web Server	merupakan layanan untuk menjalankan dan menampilkan statik file maupun *dynamic file* kedalam browser aplikasi

	internet
Database Server	merupakan layanan dari pusat data di berbagai aplikasi, berfungsi sebagai pengumpulan data-data aplikasi yang sifatnya terpusat maupun desentralisasi
Threat	merupakan ancaman-ancaman dalam dunia maya yang di tujukan kepada *object* ataupun seseorang dengan sebuah tools yang mengakibatkan dapat merugikan seseorang.
Defacement	merupakan serangan perang dunia maya yang mengakibatkan merubah halaman depan suatu *home page*
Web Portal	merupakan gerbang informasi suatu perusahaan, lembaga, instansi maupun pribadi yang bertujuan untuk memberikan informasi dalam bentuk halaman web
Sql Injection	merupakan serangan pada suatu halaman web dengan menyisipkan kode-kode sql dan gabungan bilangan operator logika untuk berusaha masuk dalam database suatu aplikasi web biasanya serangan ini berlaku pada f*ield-field* atau form elektronik seperti menu *login* pada suatu aplikasi berbasis web
Cross Site Scripting	merupakan kelemahan dari suatu sistem web aplikasi yang dapat di rubah oleh user dengan menyisipkan *script code* yang sifatnya malware sehingga web tersebut dapat di eksploit oleh *attacker*
Social Engineering	merupkan sebuah serangan hacker dalam rangka meguasai target dengan menggunkan pendekatan secara interaksi dengan musuh atau orang lain yang dijadikan target
Hacker	merupakan seorang ahli yang mempelajari sistem komputer sekaligus ahli dalam bidang programming suatu aplikasi dan mengerti dalam membongkar suatu

	sistem seseorang
Cracker	merupakan seseorang yang ahli mempelajari sistem komputer sekaligus dalam bidang programing serta mahir dalam menguasai sistem target dalam hal kepentingan pribadi