BAB II
TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Dalam penelitian Bairwa, Mewara, & Gajrani (2014) telah melakukan pengujian keamanan aplikasi *web*. Berdasarkan penilitian ini disebutkan *Nmap* adalah pemindai *port* yang digunakan untuk memindai *port*. Dibutuhkan alamat IP atau nama *host* dan kemudian menemukan informasi dasar yang terkait dengannya. Jika alamat IP diberikan, ia kemudian menemukan *host* untuk milik siapa. Ia juga menemukan jumlah *port* yang berjalan pada *host* tertentu, jumlah *port* yang dibuka, jumlah *port* tertutup, layanan yang disediakan oleh port tersebut, untuk misalnya, apakah layanan berorientasi TCP atau berorientasi FTP. Bahkan memprediksi jenis sistem operasi yang digunakan pada host tertentu. Topologi host yang dipindai direkam dalam format grafis yang menunjukkan berbagai gateway yang melaluinya mesin lokal mengakses host jarak jauh tertentu. Mempertimbangkan port yang dibuka, serangan dapat dirancang untuk memiliki yang tidak sah dan akses yang sah ke pemilik dengan tujuan yang ditentukan. Apalagi jika *port* yang dibuka adalah menyediakan layanan yang berorientasi TCP atau FTP, menjadi mudah untuk mendapatkan akses sang pemilik.

Gultom & Harahap (2015) telah melakukan analisis celah keamanan *website* instansi pemerintahan di Sumatera Utara. Berdasarkan penelitian yang dilakukan ini, menunjukkan bahwa *Website* pemerintahan di provinsi

sumatera utara memiliki beberapa celah keamanan seperti SQL injection, Blind SQL Injection, Code Injection, File Inclusion, Remote File Inclusion, Cross Site Request Forgery, Cross Site Scripting, Path Traversal dan Clickjacking. Dari hasil penelitian terdapat beberapa *website* yang memiliki celah keamanan yang terbanyak yaitu : www.binjaikota.go.id, www.taputkab.go.id, www.dairikab.go.id dengan tingkat celah keamanan yang tinggi. Hasil pembahasan dapat dirancang beberapa model penanganan dalam bentuk *use case* diagram. Dimana model ini dapat digunakan oleh pengelola *website* untuk melakukan kegiatan pencegahan dan perbaikan dari setiap celah keamanan yang ditemukan.

Mantra (2015), pada penelitiannya menyatakan bahwa *web defacement* terjadi setiap hari di Indonesia yang melanda beberapa *web* seperti nama domain .go.id, .Ac.id, .co.id, or.id, .net.id. Untuk mengantisipasi hal ini perlu dilakukan keamanan *web* dan anti SOP untuk *web defacement* khusus Indonesia. Karena aktivitas *anti-web defacing* masih sangat sedikit maka perlu dibuat SOP, dikembangkan dengan mudah dan efisien sehingga dapat digunakan sebagai panduan oleh administrator *web* di daerah tersebut. Ada beberapa hal yang harus dicermati agar setidaknya *web defacement* berkurang.

Singh & Tomar (2015) pada penelitian terdahulunya menyatakan bahwa *port scanning* adalah teknik yang digunakan oleh penyusup dan administrator jaringan untuk mengumpulkan informasi dari komputer yang terhubung ke jaringan. Pemindaian *port* diklasifikasikan dalam tiga kategori

berdasarkan berbagai jenis paket yang digunakan untuk pemindaian yaitu buka penuh, pemindaian setengah terbuka, pemindaian siluman.

Akgul (2016) telah melakukan penelitian analisis penilaian aksesibilitas, kualitas dan kerentanan situs *web* pemerintah di Republik Turki. Berdasarkan penelitian ini, menunjukan kerentanan utama tentang situs *web* pemerintah adalah keamanan diberikan prioritas rendah. Selain itu, tes di antara situs *web* menunjukkan bahwa 6% dari situs *web* telah secara kritis mengkonfirmasi kerentanan yang ditandai dan semua situs *web* yang diperiksa memiliki kerentanan yang ditandai sebagai tingkat penting dan rendah. Pada tingkat kritis dan penting, ada kerentanan terhadap serangan skrip lintas situs dan kata sandi yang dikirimkan melalui HTTP. Situs *web* pemerintah sering menjadi sasaran bagi peretas, celah keamanan ini merupakan ancaman nyata, meskipun faktanya sejauh ini ancaman-ancaman ini adalah *cyber* 'terendah' dari tingkat kejahatan dunia maya, peretasan dan penipuan di dunia maya. Keamanan situs *web* sangat penting dan penting, kesiapan situs *web* sangat bergantung pada metrik keamanannya.

Idris (2017) menganalisis 10 *website* kementerian, departemen dan lembaga di Nigeria. Berdasarkan penelitian yang dilakukan, menunjukan demi antarmuka yang ramah pengguna dan aplikasi yang berpusat justru membuat keamanan *website* terlupakan dan banyak kerentanan. Kerentanan dalam situs *web* di antaranya Referensi Objek Langsung A4-Insecure adalah kontributor terbesar risiko keamanan *web* di situs *web*. A4 ditemukan mempengaruhi 49% sumber daya *web* di berbagai situs *web*. Mayoritas

kerentanan adalah milik kelompok risiko informasi, yaitu. tinggi, rendah, informasional dengan masing-masing 17,53%, 27,88%, 45,82%. Kerentanan risiko menengah sangat sedikit dengan 8,77%.

Elisa (2017) telah melakukan penelitian analisis kegunaan, aksesibilitas dan penilaian keamanan *web* dari situs *web* e-government di Tanzania. Berdasarkan penelitian ini, menunjukan keamanan utama tentang situs *web* pemerintah Tanzania adalah bahwa 50,6% memiliki satu atau lebih kerentanan dengan tingkat keparahan tinggi (SQL *injection sqli, cross site scripting*-XSS) sementara 64,5% memiliki satu atau lebih kerentanan tingkat keparahan sedang (pemalsuan permintaan situs silang-CSRF, *Denial of Service*-DOS). Beberapa situs tampaknya memiliki kerentanan tingkat keparahan tinggi dan sedang-keparahan dan memiliki kata sandi yang dikirimkan melalui HTTP. Situs *web* pemerintah sering menjadi sasaran peretas, oleh karena itu kerentanan adalah ancaman nyata terhadap keamanan dan privasi informasi yang dibagikan oleh pengguna dan pemerintah. Jika seorang penyerang mengambil keuntungan dari kelemahan-kelemahan ini, itu bisa dengan mudah diserang.

Pada penelitian lain, Ramadhani (2017) telah melakukan penelitian analisis sistem keamanan *web server* dan *database server* menggunakan *suricata*. Berdasarkan penelitian tersebut, sebagai sistem pendeteksi dan pencegah gangguan, *suricata* dapat mendeteksi dan mencegah gangguan seperti *port scanning* atau aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status *port* (biasanya *port* TCP) pada sebuah *host*, dan

brute force atau metode untuk mendapatkan *password* dari *user* yang menjadi target.

Dalam penelitian terdahulu Bhavsar, Sharma, & Gokani (2017) menyatakan status *port* enam yang diakui oleh nmap yaitu *open* (terbuka), *closed* (tertutup), *filtered* (tersaring), *unfiltered* (tidak tersaring), *open filtered* (tersaring terbuka), *closed filtered* (tersaring tertutup).

Pada penelitian sebelumnya Murah & Ali (2018) melakukan analisis terhadap situs pemerintah Libya. Berdasarkan penelitian yang dilakukan ini, menemukan 3 situs *web* dengan lebih dari 9 kerentanan dan, 12 situs *web* memiliki antara 0 dan 8 kerentanan. Dua belas situs *web* menerapkan enkripsi SSL pada tingkat implementasi yang berbeda dengan hanya 3 situs *web* yang memiliki peringkat A. Hanya 3 situs *web* yang telah menerbitkan kebijakan keamanan dan privasi di situs *web* mereka. Peneliti memiliki 1 situs *web* yang sangat tidak aman karena penerapan SSL dan sifat operasinya. Sangat disarankan bagi situs *web* untuk tetap mendapatkan informasi terkini tentang masalah keamanan, patch sistem, dan vektor serangan dunia maya. Situs *web* juga perlu mengembangkan kebijakan keamanan dan privasi untuk penggunanya sehingga pengguna dapat mempercayai situs *web* tersebut.

Selain itu, penelitian ini dapat digunakan sebagai dasar untuk meningkatkan teknik analisis mencari celah keamanan suatu *web*site. Penelitian lebih lanjut dapat mengeksplorasi lebih banyak teknik analisis celah keamanan *website*. Berbagai teknik analisis celah keamanan yang

variatif merupakan bentuk representasi dari pencegahan penyerangan dan evaluasi keamanan *website* yang bertujuan meningkatkan keamanan *website*.

B. Landasan Teori

1. Celah Keamanan

Menurut Merriam & Webster (2019) celah adalah rentan berasal dari kata benda Latin vulnus ("luka"). "Vulnus" mengarah ke kerentanan kata kerja Latin, yang berarti "luka," dan kemudian ke kata Latin latability kerentanan, yang menjadi "rentan" dalam bahasa Inggris di awal 1600-an. "Rentan" awalnya berarti "mampu terluka secara fisik" atau "memiliki kekuatan untuk melukai" (yang terakhir sekarang sudah usang), tetapi sejak akhir 1600-an, itu juga telah digunakan secara kiasan untuk menyarankan ketidakberdayaan terhadap serangan non-fisik. Dengan kata lain, seseorang (atau sesuatu) bisa rentan terhadap kritik atau kegagalan serta luka-luka secara literal.

Berdasarkan penjelasan di atas, celah keamanan dapat diartikan bahwa kerentanan suatu keamanan pada sistem yang bersifat non-fisik yang dapat diakses dan dapat disalahgunakan untuk melakukan sesuatu di luar perizinan.

2. *Website*

Menurut Nurmi (2004) menjelaskan *website* atau situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara dan atau gabungan dari semuanya, baik brsifat statis maupun dinamis yang

membentuk suatu rangkaian bangunan yang saling terkait, yang masingmasing dihubungkan dengan jaring-jaringan

3. *Brute Force*

Menurut Ramadhani (2017) *brute force* merupakan serangan pada password dengan mencoba segala kemungkinan agar password dapat diketahui dan server dapat diambil alih. Cara kerja *brute force* yaitu mencocokkan password dengan list yang telah disediakan. Salah satu kelebihan *brute force* yaitu tidak perlu mengetahui sistem enkripsi yang rumit, namun hanya dengan mencoba segala kemugkinan *username* dan *password* yang digunakan sampai si penyerang mendapatkan *username* dan *password* yang benar.

4. *Port Scanning*

Menurut Gordon (2009) *port scanning* adalah tindakan pengujian jarak jauh dari banyak *port* untuk menentukan statusnya. Kondisi yang paling menarik biasanya terbuka, artinya aplikasi mendengarkan dan menerima koneksi pada *port*. Banyak teknik yang tersedia untuk melakukan pemindaian tersebut.