BAB II

LANDASAN TEORI

2.1. Tinjauan Pustaka

Penelitian sebelumnya menjadi salah satu bahan yang digunakan sebagai referensi dan landasan pemikiran dalam melakukan penelitian ini. Bekti Cahyo Hidayanto dkk melakukan penelitian berupa kegiatan evaluasi keamanan pada web aplikasi SISTER (Sistem Informasi Terpadu) Universitas Jember. Penelitian ini mengacu pada metode VAPT (*Vulnerability Assessment and Penetration Testing*) untuk mengetahui kelemahan yang dapat menyebabkan kegagalan proses bisnis pada web aplikasi SISTER. Tujuan penelitian ini adalah untuk mengevaluasi dan memberikan usulan perbaikan pada sistem keamanan web aplikasi SISTER. *Tools* pendukung yang digunakan pada penelitian ini adalah W3af dan OWASP ZAP yang digunakan untuk pemindaian kelemahan pada web aplikasi SISTER, Metasploit yang digunakan untuk mengendalikan komputer jarak jauh dan Nmap yang digunakan untuk mendeteksi port yang digunakan pada web aplikasi tersebut. Hasil dari penelitian ini adalah temuan beberapa kelemahan, seperti *SQL Injection*, *Cross Site Scripting* dan lain lain. Kemudian mengusulkan rekomendasi perbaikan keamanan yang diharapkan dapat meningkatkan keamanan web aplikasi SISTER Universitas Jember (Hidayanto, 2017).

Penelitian lain yang juga menggunakan metode VAPT adalah penelitian dari *Institute for Development and Research in Banking Technology*. Penelitian tersebut menjelaskan bahwa peningkatan konektivitas sistem Informasi di seluruh dunia, juga dapat meningkatkan ancaman terhadap integritas dan kerahasiaan data. Untuk menjaga keamanan dan meminimalisir ancaman yang ada, maka dilakukan pengujian kerentanan secara berkala pada sebuah aset. Penelitian ini menggunakan *tool* Net-Nirikshak 1.0 yang digunakan untuk menganalisis sistem keamanan yang sedang berjalan. *Tool* tersebut dapat mendeteksi kerentanan pada web aplikasi. Metode ini berhasil mengeksploitasi celah keamanan pada web tersebut. (Net-nirikshak, 2014).

Penelitian yang dilakukan oleh Tashia Indah Nastiti mengemukaan bahwa Universitas Gadjah Mada memiliki website yang berisi data tentang nomor jaminan sosial, kartu kredit dan data sesnitif lainnya. Oleh sebab itu dibutuhkan sebuah kegiatan untuk melakukan pengujian keamanan untuk mengevaluasi sistem keamanan pada website tersebut. Kegiatan ini menggunakan tool OWASP ZAP untuk mencari celah keamanan. Terdapat kurang lebih sepuluh celah keamanan yang ditemukan pada website tersebut. Tujuan dari penelitian ini adalah mengevaluasi dan memastikan proses keamanan yang dijalankan oleh wesite tersebut sudah berjalan dengan baik (Nastiti, 2016).

Jurnal penelitian tentang audit keamanan informasi pada 66 sistem informasi milik pemerintah mengungkapkan bahwa web aplikasi yang dikelola pemerintah beberapa masih memanfaatkan *opensource framework* yang keamanannya belum terjamin. Pencarian celah keamanan dan rekapitulasi tingkat kerentanan menggunakan *tool* Nessus. Hasil yang didapatkan adalah 37 web aplikasi menghasilkan tingkat High, 20 web aplikasi mendapat tingkat medium dan 9 lainnya mendapat tingkat low. Jumlah tersebut terus meningkat seiring berjalannya waktu karena banyak instansi pemerintah yang mulai beralih menggunakan sistem informasi untuk pengelolaan data. Tujuan dari jurnal ini adalah untuk evaluasi untuk meminimalisir peluang terjadinya serangan pada web aplikasi yang dikelola oleh pemerintah. (Anggrahito, 2018).

Penelitian tentang penggunaan *tool* Nessus untuk pencarian celah keamanan dalam rangka pelengkapan dokumentasi sebagai bahan pengembangan web yang dilakukan oleh Lane Harrison dkk dari Oak Ridge National Laboratory. Hasil dari scanning vulnerability menggunakan tool Nessus menunjukkan bahwa web localhost memiliki berbagai celah keamanan. Namun dokumentasi tentang hasil yang didapatkan dirahasiakan karena dikhawatirkan dapat dimanfaatkan oleh penyerang (Harrison, Spahn, Iannacone, Downing, & Goodall, 2012).

Penelitian yang dilakukan di institusi pendidikan XYZ menggunakan metode VAPT untuk melakukan serangkaian penilaian dan pengujian terhadap web aplikasi repositori yang dimilikinya. Pencarian celah keamanan dilakukan dengan menggunakan *tool* Nessus.

2.2. *Information Technology Security Assessment*

Information Technology Security Assessment atau dalam bahasa Indonesia disebut sebagai penilaian keamanan teknologi informasi adalah sebuah penilaian yang berorientasi kepada risiko (Abdel-Aziz, 2011). Konsentrasi penilaian keamanan adalah terdapat pada celah keamanan yang dapat menimbulkan risiko beragam jika terjadi kegagalan proses teknologi informasi yang bisa terjadi karena beberapa faktor, seperti; faktor *hardware*, *software*, lingkungan bahkan serangan dari dalam maupun luar organisasi. Fokus analisis risiko adalah mengacu pada aset-aset yang menjalankan proses teknologi informasi (Sosonkin, 2005). Aset-aset tersebut perlu diperhatikan karena berperan penting dalam proses teknologi informasi yang berlangsung secara terus menerus.

2.3. Metode VAPT (*Vulnerability Assessment and Penetration Testing*)

Sesuai dengan namanya, metode ini terdiri dari dua kegiatan utama, yaitu *Vulnerability Assessment* dan *Penetration Testing* serta beberapa kegiatan pendukung lainnya. *Vulnerability Assessment* adalah pemindaian pada sebuah web aplikasi untuk mencari celah keamanan yang kemungkinan dapat digunakan oleh penyerang dan menimbulkan dampak yang beragam. *Penetration testing* adalah kegiatan percobaan untuk melakukan penetrasi atau masuk kedalam sebuah sistem dengan memanfaatkan celah keamanan atau hak akses yang sah untuk eksploitasi sesuatu. Tujuannya adalah untuk mendapatkan informasi penting pada sebuah web aplikasi (Goel & Mehtre, 2015).

2.4. NESSUS

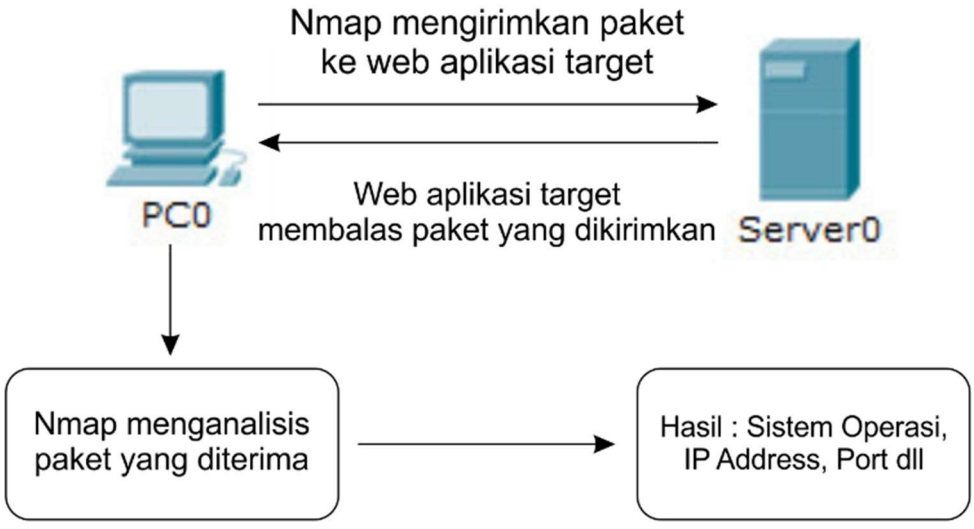
Nessus adalah sebuah *tool* untuk mencari celah keamanan pada perangkat lunak atau halaman web. *Tool* ini memungkinkan seseorang untuk dapat menemukan cara untuk menembus keamanan pada sebuah software atau halaman web. Nessus pertama kali dirilis tahun 1998 oleh Renaud Deraison menjadi salah satu produk *scanning* untuk mencari celah keamanan yang banyak digunakan. Nessus menampilkan hasil *scanning* berkecepatan tinggi, penemuan data sensitif dan analisis celah keamanan (Kumar, 2014).

Fitur yang terdapat dalam *tool* ini adalah (EC-Council, 2012):

1. Masing-masing tes keamanan dituliskan dalam bentuk *plugin* agar mempermudah user dalam memilih tes yang diinginkan tanpa harus membaca kode yang dijalankan oleh Nessus.
2. Nessus dapat menjalankan lebih dari satu *vulnerability scanner*, karena Nessus terdiri dari *server* yang melakukan *vulnerability scanning* dari perintah *client* yang ada pada *end device.*

2.5. Nmap

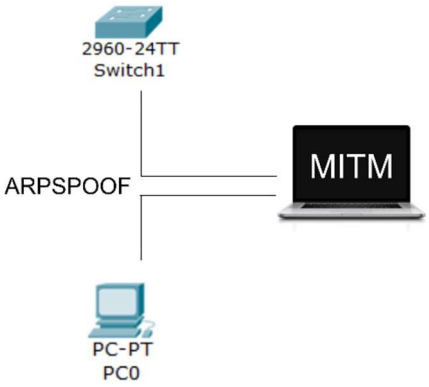
Nmap adalah *tool* untuk mengaudit keamanan jaringan. Nmap melakukan pemindaian terhadap satu *host* untuk mengetahui layanan yang digunakan (nama dan versi aplikasi), sistem operasi dan jenis filter *firewall* yang digunakan. Nmap berjalan disemua sistem operasi komputer, seperti Linux, Windows, dan Mac OS X. Nmap menjalankan setiap baris perintah menggunakan *command prompt* atau terminal (Nmap, 1997). Gambaran mengenai skema kerja *tool* ini dijelaskan pada **Gambar 2.1**.



Gambar 2. 1 Skema Nmap

2.6. *Man In The Middle*

Man in the middle adalah teknik serangan *cyber* dimana penyerang memasukkan dirinya kedalam sebuah komunikasi antara dua perangkat, meniru kedua pihak dan mendapatkan informasi yang kirimkan satu sama lain. Teknik serangan *man in the middle* memungkinkan penyerang untuk mencegat, mengirim dan menerima data yang ditujukan untuk orang lain, kegiatan ini tidak diketahui oleh kedua perangkat yang sedang berkomunikasi tersebut (Shubh & Sharma, 2016). *Tool* yang digunakan untuk mendukung teknik serangan ini adalah arpspoof. Gambaran tentang skema *logic* tentang kegiatan *man in the middle* dijelaskan pada **Gambar 2.2**.



Gambar 2. 2 Skema *Logic Man In The Middle*

2.7. Arpspoof

Arpspoof adalah sebuah *tool* untuk mendukung kegiatan *man in the middle* yang fungsinya adalah untuk membaca data sesi pada dua *host* pada saat yang bersamaan (Puangpronpitag & Masusai, 2009). Cara kerjanya adalah *tool* ini memanipulasi tabel ARP yang berisi *IP Address* dan *Mac Address* dari setiap perangkat yang terhubung ke jaringan. Arpspoof mengirimkan paket palsu yang berisi *Mac Address* dari perangkat penyerang namun tetap dengan *IP address* dari perangkat yang menjadi korban. Sehingga yang terjadi adalah data sesi yang berjalan dari dan menuju *gateway* akan malewati perangkat yang digunakan oleh penyerang lalu diteruskan ke perangkat tujuan yang sebenarnya dan begitu pula sebaliknya.

2.8. SSLStrip

SSLStrip adalah sebuah *tool* yang mendukung kegiatan *man in the middle* melalui protokol HTTP (Wicaksono, 2009). Fungsinya adalah untuk membaca data sesi yang dikirimkan pada sebuah web aplikasi menuju perangkat *client* atau sebaliknya. Hasil dari penggunaan *tool* ini adalah sebuah file log yang berisi data sesi dari interaksi dua perangkat.

2.9. Metasploit

Metasploit adalah salah satu *tool* untuk mengeksploitasi serangan pada server. *Tool* ini menjadi salah satu tool yang paling berguna untuk penguji penetrasi. HD Moore merancang tool ini pada tahun 2003. *Tool* ini digunakan sebagai alat pengujian penetrasi yang digunakan oleh penyerang untuk melakukan eksploitasi sistem (Muniz & Lakhani, 2013).

2.10. *Brute Force*

Brute Force adalah teknik penyerangan untuk menemukan *username* dan *password* legal yang digunakan untuk masuk kedalam sebuah sistem. *Brute Force* berjalan secara otomatis dengan cara mengkombinasikan satu per satu baris *username* dan *password* yang dikumpulkan pada sebuah file. (Karawash et al., 2016). Lalu kombinasi tersebut dicoba satu per satu pada sistem.

2.11. *Social Engineering*

Social Engineering bisa diartikan sebagai penggunaan trik psikologis dari peretas, untuk memperoleh informasi yang dibutuhkannya untuk mendapatkan akses ke sistem atau bisa dikatakan juga sebagai cara untuk mendapatkan informasi yang dibutuhkan (misalnya, kata sandi) dari seseorang, bukan dengan cara membobol sistem (Granger, 2001)