BAB II
LANDASAN TEORI

2.1. Tinjauan Pustaka

Jurnal penelitian tentang audit keamanan informasi pada 66 sistem informasi milik pemerintah mengungkapkan bahwa web aplikasi yang dikelola pemerintah beberapa masih memanfaatkan *open source framework* yang keamanannya belum terjamin. Pencarian kerentanan keamanan dan rekapitulasi tingkat kerentanan menggunakan *tool software 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 kerentanan 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 kerentanan keamanan. Namun dokumentasi tentang hasil yang didapatkan dirahasiakan karena dikhawatirkan dapat dimanfaatkan oleh penyerang (Harrison, Spahn, Iannacone, Downing, & Goodall, 2012).

Penelitian yang dilakukan oleh Tashia Indah Nastiti mengemukakan bahwa Universitas Gadjah Mada memiliki *website* yang berisi data tentang nomor jaminan sosial, kartu kredit dan data sensitif 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 kerentanan keamanan. Terdapat kurang lebih sepuluh kerentanan keamanan yang ditemukan pada *website* tersebut. Tujuan dari penelitian ini adalah

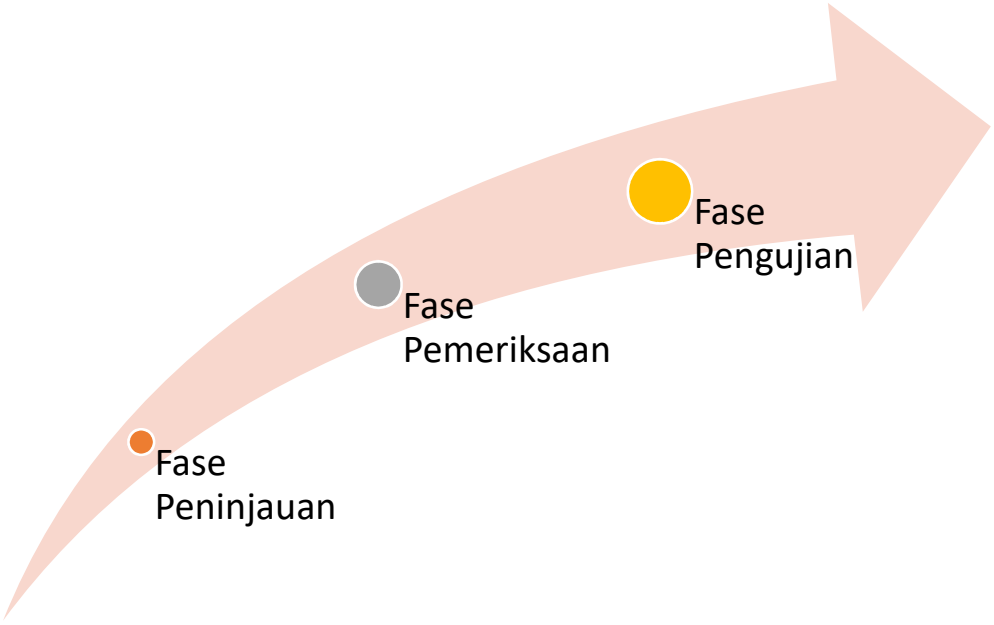
mengevaluasi dan memastikan proses keamanan yang dijalankan oleh website tersebut sudah berjalan dengan baik (Nastiti, 2016).

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 aset yang dimilikinya. 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. Semua aspek Teknis dan Operasional *Net-Nirikshak 1.0* dijelaskan dalam makalah ini bersama dengan *Output* dari sampel uji VAPT yang dilakukan di *www.webscantest.com* menggunakan *Net-Nirikshak 1.0.* Metode ini berhasil mengeksploitasi kerentanan keamanan pada web tersebut (Shah & Mehtre, 2015).

Penelitian Ahmad Fikri Zulfi melakukan kegiatan evaluasi keamanan pada web aplikasi SISTER (Sistem Informasi Terpadu) Universitas Jember, yang dituliskan dalam skripsi berjudul Evaluasi Keamanan Aplikasi Sistem Informasi Mahasiswa Menggunakan *Framework* VAPT (Studi Kasus: SISTER 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 dari penelitiannya adalah untuk mengevaluasi dan memberikan usulan perbaikan pada sistem keamanan web aplikasi SISTER. Beberapa *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 yang didapatkan dari penelitian ini adalah ditemukannya beberapa kelemahan, seperti *SQL Injection*, *Cross Site Scripting*, dll. Kemudian mengusulkan rekomendasi perbaikan keamanan yang diharapkan dapat meningkatkan keamanan web aplikasi SISTER Universitas Jember (Zulfi, 2017).

2.2. *Information Technology Security Assessment*

Security Assessment adalah pengukuran postur keamanan dari suatu sistem atau organisasi (Russ Miles, Rogers, Fuller, & Dykstra, 2004). Postur keamanan merupakan cara keamanan informasi untuk diimplementasikan. Seperti pada **Gambar 2.1** menurut (Abdel-Aziz, 2011) penilaian keamanan bergantung pada tiga fase penilaian yaitu Fase Peninjauan, Fase Pemeriksaan, Fase Pengujian.



Gambar 2. 1 Fase *Security Assessment*

2.2.1. Fase Peninjauan

Fase peninjauan merupakan proses melakukan pengumpulan informasi terkait sistem yang akan dilakukan proses *assessment*. Proses ini dapat berupa wawancara kepada pihak organisasi. Informasi yang dikumpulkan mencakup evaluasi kebijakan, prosedur, aplikasi, dan jaringan untuk menemukan kerentanan. Fase ini dilakukan untuk memahami bagaimana sistem bekerja (Abdel-Aziz, 2011).

2.2.2. Fase Pemeriksaan

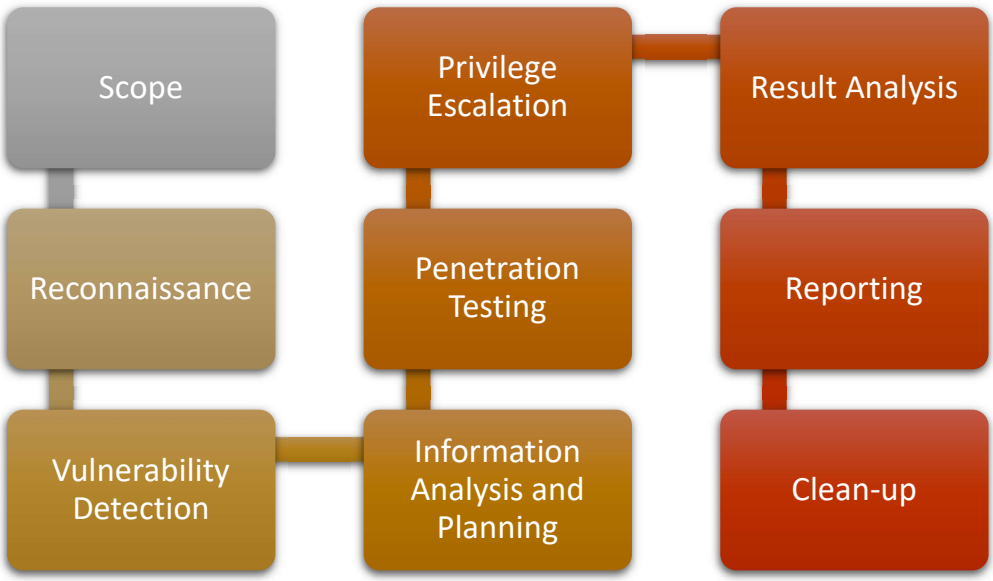
Fase pemeriksaan adalah proses teknis langsung yang melihat organisasi secara khusus dari tingkat sistem atau jaringan untuk mengidentifikasi kerentanan keamanan yang ada adalah sistem tersebut. Ini termasuk melakukan analisis teknis dari *firewall*, sistem deteksi, dan *router*. Ini juga mencangkup pemindaian kerentanan jaringan pelanggan (Abdel-Aziz, 2011).

2.2.3. Fase Pengujian

Fase pengujian sering disebut juga *penetration testing* adalah proses di mana seseorang menirukan seorang musuh yang mencari kerentanan keamanan, yang memungkinkan masuk ke sistem atau jaringan (Abdel-Aziz, 2011).

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

VAPT (Vulnerability Assessment and Penetration Testing) adalah kerangka kerja dalam melakukan uji keamanan terhadap suatu sistem web application (Goel & Mehtre, 2015). VAPT merupakan gabungan dari dua aktivitas *Vulnerability Assessment dan Penetration Testing*. *Vulnerability Assessment* merupakan aktivitas yang meliputi proses pemeriksaan sebuah kerentanan keamanan dari suatu web application. Sedangkan *Penetration Testing* adalah suatu proses simulasi penyerangan terhadap kerentanan yang terdapat pada web application dan mengeksploitasinya. Proses pengujian menggunakan kerangka kerja VAPT terdapat 9 tahapan yang perlu dilakukan (Goel & Mehtre, 2015). Penjabaran mengenai 9 tahapan tersebut ada pada **Gambar 2.2**.



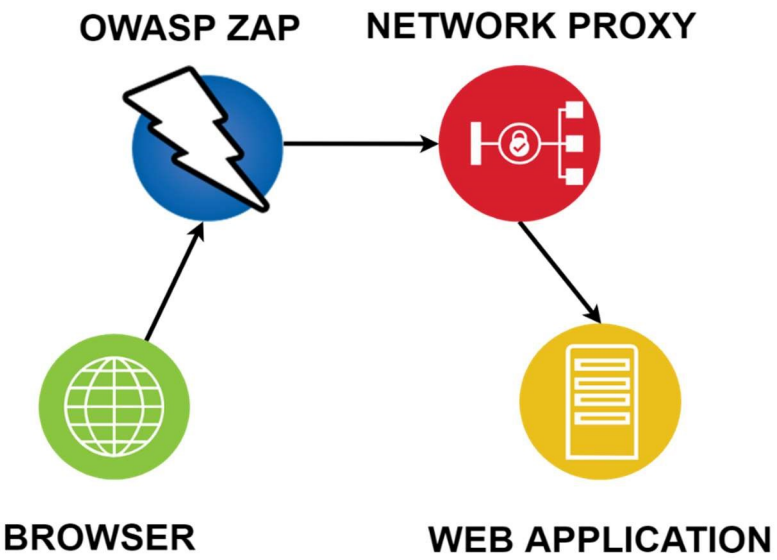
Gambar 2. 2 Tahapan VAPT

2.4. OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*)

OWASP (*Open Web Application Security Project*) merupakan organisasi atau komunitas terbuka yang didirikan pada tanggal 1 Desember 2001 berfokus pada bidang keamanan aplikasi. OWASP tidak berafiliasi dengan perusahaan mana pun demi kebebasan dari tekanan dan mampu bersifat objektif dalam memberikan informasi mengenai keamanan yang erat kaitannya dengan dunia teknologi informasi (OWASP (Open Web Application Security Project), 2001).

Sedangkan ZAP (*Zed Attack Proxy*) adalah aplikasi *open source* untuk melakukan pencarian kerentanan pada *website* dengan cara *scanner* otomatis pada aplikasi ZAP tersebut (OWASP (Open Web Application Security Project), 2001).

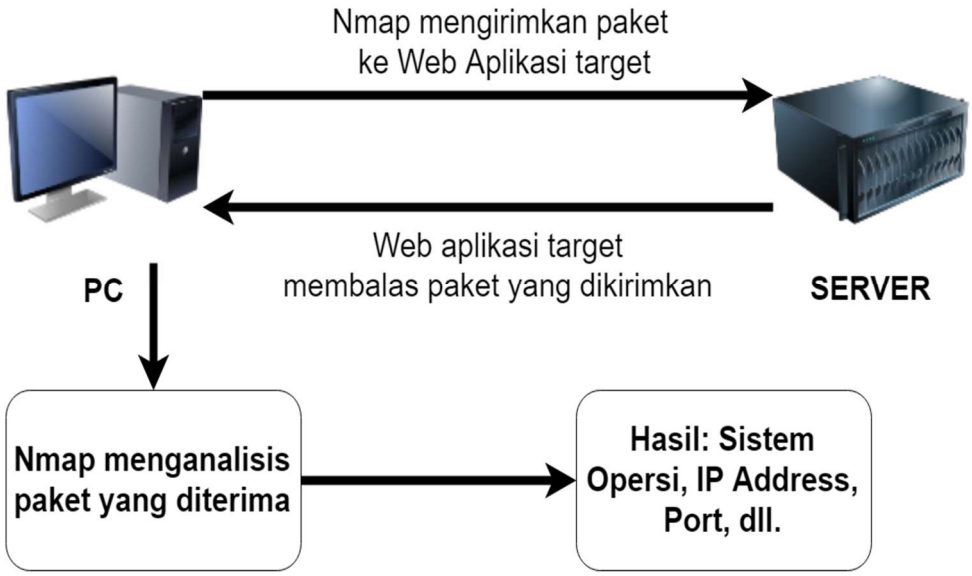
ZAP dirancang khusus untuk pengujian aplikasi web dan *flexible* dan *extensible*. Pada intinya, ZAP adalah apa yang dikenal sebagai "*Proxy Man-in-the-Middle*." Ini berdiri antara tester browser dan aplikasi web sehingga dapat mencegat dan memeriksa pesan yang dikirim antara browser dan aplikasi web, memodifikasi isi jika diperlukan, dan kemudian meneruskan paket-paketnya mereka ke tujuan. Seperti **Gambar 2.3**, jika ada jaringan lain *proxy* yang sudah di gunakan, seperti di banyak lingkungan perusahaan, ZAP dapat dikonfigurasi untuk terhubung ke *proxy*.



Gambar 2. 3 Skema OWASP ZAP

2.5. *Nmap*

Nmap adalah *tool* untuk mengaudit keamanan jaringan. *Nmap* melakukan *scanning* terhadap satu host untuk mengetahui layanan yang digunakan (nama dan versi aplikasi), sistem operasi dan jenis *filter firewall* yang digunakan. *Nmap* berjalan di semua sistem operasi komputer, seperti *Linux*, *Windows*, dan *Mac OS X*. *Nmap* menjalankan setiap baris perintah menggunakan *command prompt* atau terminal. *Nmap* juga tersedia dalam versi *GUI* dengan nama *Zenmap* (Nmap, 1997). Skema Nmap bisa dilihat pada **Gambar 2.4**.



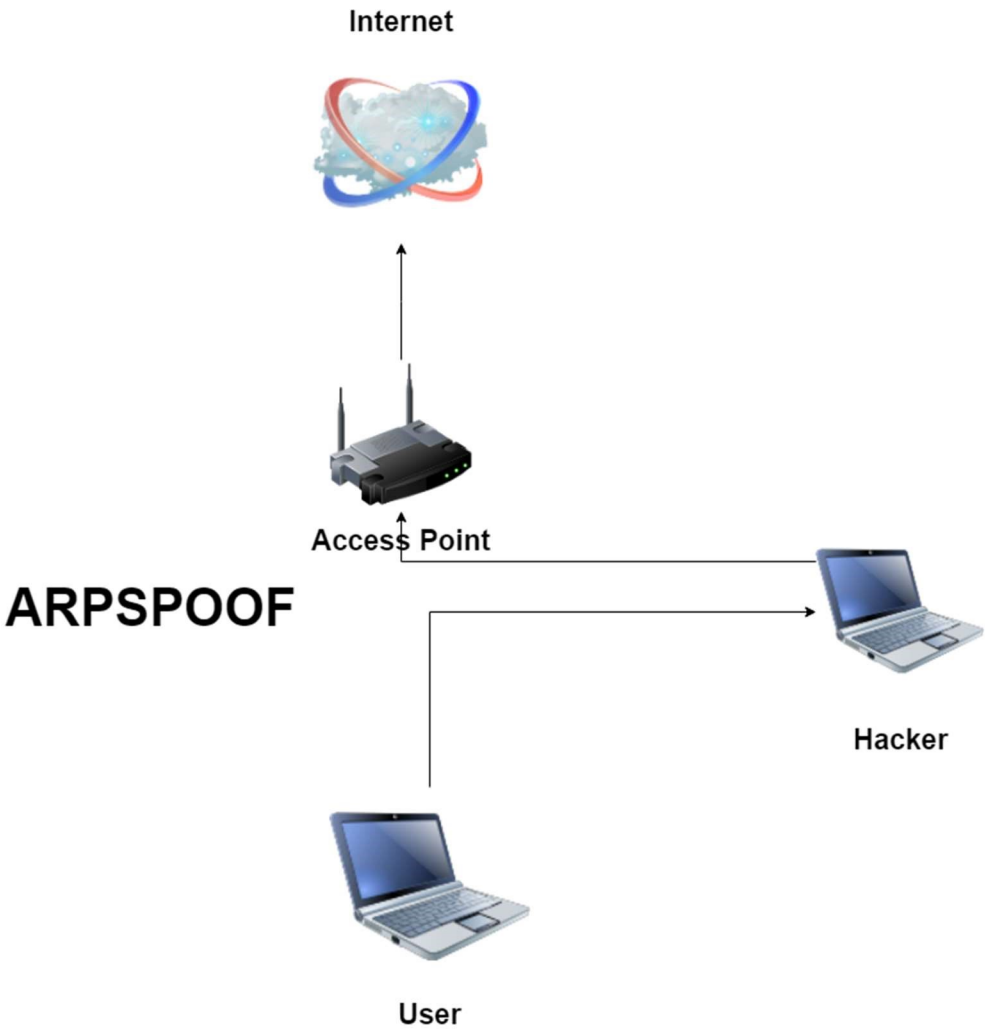
Gambar 2. 4 Skema *Nmap*

2.6. *Man-in-the-Middle*

Man-in-the-Middle adalah jenis serangan *cyber* dimana penyerang memasukkan dirinya ke dalam sebuah komunikasi antara dua perangkat, meniru kedua pihak dan mendapatkan informasi yang kirimkan satu sama lain. 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).

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). Seperti pada **Gambar 2.5**, 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 melewati perangkat yang digunakan oleh penyerang lalu diteruskan ke perangkat tujuan yang sebenarnya.



Gambar 2. 5 Skema *Arpspoof*

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 target atau sebaliknya. Hasil dari penggunaan *tool* ini adalah sebuah *file log* yang berisi data sesi dari interaksi dua perangkat.

2.9. *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).