BAB II
TINJAUAN PUSTAKA

Dalam bab ini akan di jelaskan teori-teori yang mendukung penelitian, penelitian sebelum nya yang meneliti kerentanan *website* dengan menggunakan *penetration testing, ISSAF, OWASP versi4.*

2.1 Perbandingan Penelitian Sebelumnya

Bedasarkan permasalahan yang ada, yaitu mengenai pengujian ketahanan *website*, penulis menggunakan beberapa referensi terkait dengan penelitian yang sudah dilakukan sebelumnya. Pertama, penulis Fajaryanto Adi Cobantoro, 2016 melakukan pengujian menggunakan *OWASP* versi 4 terlihat bahwa pada tahapan *OTG-AUTHN-001, OTG-AUTHN-004, OTG-AUTHN-005, OTG AUTHN-006*, dan *OTGAUTHN-008* aplikasi tidak lolos pengujian, sehingga proses otentifikasi pemakai berpotensi untuk diendus oleh pihak yang tidak bertanggung jawab dalam proses pengiriman data penting. Hasil yang sama juga ditunjukkan pada aplikasi SIA Universitas Diponegoro Semarang yang menunjukkan bahwa pengiriman data *username* dan *password* tidak di enkripsi sebelum dikirim ke *server* SIA (Satoto, Isnanto, & Masykur, 2008). Pada pengujian otorisasi, tahapan *OTGAUTHZ-002* dan *OTG-AUTHZ-004* tidak lulus pengujian dan ini merupakan *false* alarm sehingga untuk pengujian otorisasi aplikasi ini lolos uji. Tahapan *OTG-SESS-007* dan *OTG-SESS-008* dilakukan pengujian mengenai *session* yang ada. Pada *OTG-SESS-007 session timeout* tidak ada sehingga memungkinkan apabila pemakai meninggalkan komputer maka ada kemungkinan session yang ditinggalkan dimanfaatkan oleh pemakai lain yang tidak berhak. Pada *OTG-SESS-008*, aplikasi ini menggunakan *variabel session* yang sama selama lebih dari satu tujuan sehingga penyerang dapat mengakses halaman secara acak[3]

Referensi yang kedua, penulis Dr. Raden Teduh Dirgahayu, S. T, M. Sc, dkk, pada tahun 2015, melakukan pengujian dan analisa dengan *framework ISSAF* pada sistem *web server* IKIP PGRI Madiun. Hasilnya menunjukkan bahwa masih dapat ditembus dan hak akses *administrator* dapat diambil alih, sedangkan dengan *framework OWASP VERSI 4* menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik[4].

Referensi yang ke tiga, Bambang pujiarto, ema utami, sudarmawan, pada tahun 2013, mengevaluasi keamanan wireless local area network menggunakan metode penetration testing universitas Muhammahdiyah Magelang menunjukkan bahwa Hasil pengujian jaringan *WLAN* di universitas Muhammadiyah Magelang diperoleh empat jenis pengujian yang menunjukkan rata-rata tingkat kerentanan sebesar 0.8, dengan kata lain secara keseluruhan jaringan *WLAN* di Universitas Muhammadiyah Magelang memiliki tingkat kerentanan *(vulnerability).* Metodologi yang meliputi fase *planning and prepration, assessment* dan *reporting* dapat dijadikan pedoman untuk melakukan *penetration testing* pada institusi. Keluaran tiap fase pada fase *planning and preparation* menghasilkan dokumen kebijakan dan *agreement,* pada fase *assessment* menghasilkan dokumen *assessment,* dan yang terakhir pada fase *reporting* menghasilkan dokumen evaluasi keluaran yang dihasilkan oleh tiap fase berikutnya sehingga ketiga fase tersebut merupakan satu rangkaian proses yang tidak dapat dipisahkan[5].

Referensi yang keempat, penulis Mohmmad muhsin dan Adi fajaryanto tahun 2015, melakukan pengujian keamanan *web server* Ujian *Online* menggunakan *framework OWASP Versi 4,* menunjukkan bahwa pada proses otentifikasi terdapat kerentanan yaitu pada pengujian OTG-AUTHN-001, OTGAUTHN-003, OTG-AUTHN-004, OTGAUTHN-005, OTG-AUTHN-006 sehingga proses ini perlu mendapat perbaikan. Pada proses pengujian otorisasi terdapat kerentanan pada OTG-AUTHZ-002, OTGAUTHZ-004, namun setelah dilakukan pengecekan diatas hasilnya adalah false alarm sehingga proses otorisasi sudah berjalan dengan baik, sedangkan pada manajemen sesi terdapat kerentanan pada OTG-SESS-001, OTG-SESS-005, OTGSESS-007, OTG-SESS-008. Tidak adanya session timeout memungkinkan pemakai yang meninggalkan komputer dimanfaatkan oleh pemakai lain yang tidak berhak. Pada OTG-SESS-008, aplikasi ini menggunakan variabel session yang sama selama lebih dari satu tujuan sehingga penyerang dapat mengakses halaman secara acak [6]

Referensi yang kelima, penulis Bambang Supradono, tahun 2009 melakukan manajemen risiko keamanan informasi dengan menggunakan metode *Octave Allegro* dan Kontrol *ISO 2700* pada Instansi Pelayanan Penyelenggara Publik. Latar belakang keamanan dari penelitian ini adalah informasi yang tidak bisa hanya disandarkan pada *tool*s atau teknologi keamanan informasi saja, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan seacara tepat solusi dalam menangani permasalahan kebutuhan keamanan informasi. Pemerintah Kulonprogo dipilih sebagai objek atas dasar Peraturann Daerah Bupati Kulon Progo Nomor 65 Tahun 2012 tentang Penerapan Manajemen Resiko pada Pemerintah Daerah. Masalah dalam penelitian ini adalah kerentanan yang ada dalam sistem informasi penting terkait dengan jaringan lokal dan *online*, resiko pencurian, serta bahaya kebakaran pada aset fisik mereka. Sehingga diperlukan kamera pengawas, sensor panas, alat pemadam kebakaran, dan penyemprotan air luar ruangan. Penerapan metode *Octave Allegro* telah menghasilkan pemetaan dampak dengan hasil pendekatan *mitigasi* untuk sistem *database* layanan informasi di *server* dikurangi. Dari hasil identifikasi risiko ada 12 kontrol dalam *ISO 27001* yang dapat digunakan sebagai referensi untuk menentukan rekomendasi mitigasi risiko. Keduabelas kontrol itu adalah, Identfikasi risiko, Identifikasi risiko *backup* data *failure*, identifikasi risiko *human,* identifikasi risiko *memory,* identifikasi risiko serangan *hacker,* identifikasi risiko *hardware failure*, Identifikasi *software failure,* identifikasi risiko *power failure,* Identifikasi risiko *network failure,* identifikasi risiko kebakaran, serta identifikasi risiko pencurian media atau dokumen penting. Hasil dari penelirian ini adalah merekomendasi kepada manajemen tingkat atas untuk mengubah pola kerja operator layanan untuk lebih menigkatkan kesadaran keamanan data[8].

Tabel 2.1.1 Perbandingan penelitian sebelumnya

No	Judul	Penulis	Tahun	Isi	Perbandingan
1	Penerapan *OWASP VERSI 4* untuk uji kerentanan *web server*, Studi kasus: *ejurnal server kampus X madiun*	Adi Fajaryanto Cobantoro	2016	Hasil identifkasi kerentanan dengan menggunakan *framework OWASP* versi 4 menunjukkan bahwa *web server* ejurnal kampus X Madiun memiliki tingkat kerentanan medium. Hasil pengujian dan analisa dengan *framework OWASP* versi 4 menunjukkan bahwa manajemen otentifikasi, dan manajemen sesi belum diimplementasikan dengan baik. Rekomendasi untuk menutup celah kerentanan diatas adalah dengan menerapkan *OWASP Top Ten*	Objek penelitian *web server*, lokasi penelitian, menggunakan *framework OWASP Versi 4*
2	Penerapan Metode *ISSAF* dan *OWASP* VERSI 4 Untuk Uji Kerentanan *Web server*	Dr. Raden Teduh Dirgahayu , S. T, M. Sc, Yudi Prayudi, S.Si., M. Kom, Adi Fajaryanto	2015	Hasil pengujian dan analisa dengan *framework ISSAF* menunjukkan bahwa sistem *web server* IKIP PGRI Madiun masih dapat ditembus dan mengambil alih hak akses administrator, sedangkan dengan *Framework OWASP* versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik	Objek penelitian *web server*, lokasi penelitian dan menggunakan *framework ISSAF* dan *OWASP Versi 4*
3	Evaluasi keamanan *wireless local* area *network* menggunakan metode *penetration testing* Studi kasus: Universitas Muhammadiyah Magelang	Bambang pujiarto, ema utami, sudarmawan	2013	Hasil keseluruhan yang didapat dari empat jenis pengujian menunjukkan rata-rata tingkat kerentanannya adalah 0.8 dengan kata lain secara keseluruhan jaringan *WLAN* di Universitas Muhammadiyah Magelang memiliki tingkat kerentanan *(vulnerability)* tinggi.	Objek penelitian jaringan *Wlan*, menggunakan *framework ISSAF*
4	Penerapan pengujian keamanan *web server* menggunakan metode *OWASP* VERSI 4, studi	Mohmmad muhsin dan Adi fajaryanto	2015	Hasil pengujian menggunakan *framework OWASP* versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi danmanajemen sesi belum diimplementasikan	Objek penelitian web server, menggunakan *framework OWASP Versi 4*

No	Judul	Penulis	Tahun	Isi	Perbandingan
	kasus: web server ujian online			dengan baik sehingga perlu dilakukan perbaikan lebih lanjut oleh pihak *stake holder* Fakultas Teknik Universitas Muhammadiyah Ponorogo	
5	Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metoda *Octave (Operationally Critical Threat, Asset, And Vulnerability Evaluation)*	Bambang Supradono	2009	Metode *OCTAVE* memberikan panduan secara sistemik dan komprehensif dalam manajemen risiko keamanan informasi. Metode ini lebih menekankan pengelolaan risiko berbasis ancaman *(threat)* dan kelemahan *(vulnerability)* terhadap aset-aset informasi organisasi meliputi perangkat keras, lunak, sistem, informasi dan manusia.	Objek penelitian Sistem informasi, menggunakan metode *Octave*

2.2 Dasar Teori

Dalam bab ini akan dijelaskan mengenai teori-teori yang mendukung dalam penelitian, diantaranya mengenai *Internet*, keamanan jaringan, *Penetration testing, ISSAF,* dan *OWASP VERSI 4*.

2.2.1 Internet

Internet adalah jaringan besar yang saling berhubungan dari jaringan-jaringan komputer yang menghubungkan orang-orang dan komputer-komputer di seluruh dunia melalui telepon, satelit, dan sistem-sistem komunikasi yang lain. *Internet* dibentuk oleh jutaan komputer yang terhubung bersama dari seluruh dunia, memberi jalan bagi informasi (mulai teks, gambar, audio, video, dan lainnya) untuk dapat dikirim dan dinikmati bersama. Untuk dapat bertukar informasi, digunakan protokol standar yaitu *Transmision Control Protocol internet Protocol* yang lebih dikenal sebagai *TCP/IP***.**

TCP bertugas untuk memastikan bahwa semua hubungan bekerja dengan benar, sedangkan *IP* bertugas untuk mentransmisikan data dari satu komputer ke komputer lain. *TPC/IP* secara umum berfungsi memilih rute terbaik untuk transmisi data, memilih rute alternatif jika suatu rute tidak dapat digunakan, serta mengatur dan mengirimkan paket-paket pengiriman data. Pada era global ini, keamanan sistem informasi berbasis *Internet* harus sangat diperhatikan, karena jaringan komputer *Internet* yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu terminal asal menuju ke terminal tujuan dalam internet, data itu akan melewati sejumlah terminal yang lain yang berarti akan memberi kesempatan pada *user* Internet yang lain untuk menyadap atau mengubah data tersebut[9].

Keamanan *internet* merupakan suatu usaha untuk menghindari timbulnya atau adanya ancaman kejahatan yang ada di *internet*. Keamanan

internet sebaiknya memiliki unsur-unsur seperti adanya *proteksi, intergitas*, keaslian suatu data, serta memiliki hak akses, dimana kecanggihan *internet* pada keamanan jaringan harus sangat diperhatikan. Karena jaringan *internet* menjadi suatu kebutuhan pokok pada setiap instansi atau perusahaan, maka segala upaya akan dilakukan untuk bisa mengikuti perkembangan teknologi *internet* yang sangat luas dan terhubung satu sama lain yang dapat menimbulkan kekhawatiran akan keamanan jaringan pada sistem informasi. Keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang salah dari jaringan. Tujuan keamanan jaringan ini agar memastikan sistem benar-benar aman dari *attacker* yang akan menembus keamanan sistem[10].

2.2.2 Keamanan Jaringan

Sistem keamanan jaringan komputer yang terhubung ke *Internet* harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif. Menurut para ahli, John D. Howard dalam bukunya *"An Analysis of security incidents on the internet"* menyatakan bahwa keamanan jaringan adalah suatu tindakan pencegahan perangkat dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. [11] Keamanan jaringan dapat dilakukan dengan menerapakan perlindunga sistem yaitu:

1. *TCP/IP (Transmission Control Protokol/Internet Protocol)*

   Protokol adalah spesifikasi formal yang mendefinisikan prosedur-prosedur yang harus diikuti ketika mengirim dan menerima data (Werner, 1996). Protokol mendefinisikan jenis, waktu, urutan dan pengecekan kesalahan yang digunakan dalam jaringan. *TCP/IP* merupakan protokol untuk mengirim data antarkomputer pada jaringan. Terdapat 5 *layer* dalam protocol *TCP/IP* yaitu:

a. *Layer Internet*, layer ini mengambil paket dari layer trans*port* dan menambahkan informasi alamat sebelum mengirimkannya ke *layer network interface*.

b. *Layer Network Interface*, di dalam layer ini data dikirim ke *layer physical* melalui *device* jaringan.

c. *Layer Physical*, layer ini merupakan sistem kabel yang digunakan untuk proses mengirim dan menerima data.

d. *Layer Transport*, di dalam layer ini *TCP* dan *UDP* menambahkan data transport ke paket dan melewatkannya ke layer Internet.

e. *Layer Application*, di dalam layer ini aplikasi seperti *FTP, Telnet, SMTP*, dan *NFS* dilaksanakan.

TCP/IP dikirimkan ke setiap jaringan lokal sebagai subnet yang masing-masing subnet telah diberi alamat. IP yang menggunakan pengalamatan disebut dengan *IP Address*. *IP Address* ini digunakan untuk mengidentifikasi subnet dan *host* secara logik di dalam *TCP/IP (Staff of Linux Journal, 2004).*

2. *Firewall*

Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah *access control policy* terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas *firewall* adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. *Firewall* bertanggung jawab untuk memastikan bahwa *acces control policy* yang diikuti oleh semua pengguna di dalam jaringan tersebut. *Firewall* sama seperti alat-alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun tidak seperti alat-alat jaringan lain, sebuah *firewall* harus mengontrol lalu lintas *network* dengan memasukkan faktor pertimbangan bahwa tidak semua paket-paket data yang dilihatnya adalah apa yang seperti terlihat. *Firewall* digunakan untuk

mengontrol akses antara *network internal* sebuah organisasi *Internet.* Sekarang ini *firewall* sudah menjadi fungsi standar yang ditambahkan untuk semua *host* yang berhubungan dengan *network* (Purbo, 2000). Fungsi-fungsi umum *firewall* adalah sebagai berikut:

a. *Static packet filtering* (penyaringan paket secara statis)

b. *Dynamic packet filtering* (penyaringan paket secara dinamis)

c. *Stateful filtering* (penyaringan paket berdasarkan status)

d. *Proxy.*

3. *Network Address Translation*

Network Address Translation (NAT) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan *internet* menggunakan satu alamat *IP*. *NAT* merupakan teknologi yang memungkinkan *IP Private* dapat membagi koneksi akses *internet* jaringan yang didesain untuk menyederhanakan *IP address*, *NAT* juga berperan untuk melindungi jaringan, serta untuk kemudahan dan fleksibilitas dalam administrasi jaringan. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat *IP Address* yang terbatas. *NAT* berlaku sebagai penerjemah antara dua jaringan (Taringan, 2009). *IP address* sebagai sarana pengalamatan di *internet* semakin menjadi barang mewah dan ekslusif. Tidak sembarangan orang sekarang ini bisa mendapatkan *IP address* yang valid dengan mudah. Oleh karena itulah dibutuhkan suatu mekanisme yang dapat menghemat *IP address*. Logika sederhana untuk penghematan *IP address* adalah dengan membagi suatu nomor *IP address valid* ke beberapa *client IP address* lainnya. Atau dengan kata lain, beberapa komputer bisa mengakses *internet* walau hanya memiliki satu *IP address* yang valid. Salah satu mekasnisme itu disediakan oleh *NAT*. *NAT* bekerja dengan cara mengkonversikan *IP address* ke satu atau lebih *IP address* lain. *IP address* dikonversi adalah *IP address* yang diberikan

untuk tiap mesin dalam jaringan internal. *IP address* yang menjadi hasil konversi terletak di luar jaringan internal tersebut dan merupakan *IP address* legal yang valid.

4. *Traffic Filtering*

   Traffic filtering adalah teknik untuk mengontrol lalu lintas data yang di *forward* dari sebuah jaringan melintasi *router* (Rafiudin, 2006). Fungsi ini melibatkan perancangan *policy* keamanan. Jaringan berbeda seringkali memiliki level keamanan yang berbeda pula. Pada implementasinya pemfilteran lalu lintas data dapat dirancang untuk membentuk lingkungan *firewall*. Adapun implementasi sederhana *IP filtering* dapat berupa sebuah *rule access list* yang mengizinkan *("permit")* atau memblok *("deny")* tipe data tertentu berdasarkan *IP address* sumbernya (Faulkner,2001).

Tujuan keamanan jaringan komputer yaitu *Availability* (ketersediaan), *Reliability* (Kehandalan), dan *Confidentiality* (Kerahasian). Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman *(threat)* yang harus diatasi dan resiko ancaman yang harus diambil maupun yang harus dihindari. Ancaman merupakan salah satu bentuk usaha yang bersifat untuk mengubah atau merombak kebijaksanaan yang dilakukan secara konsepsional melalui segala tindak kriminal dan politis. Beberapa bentuk ancaman jaringan yang membahayakan keamanan jaringan antara lain adalah hal-hal sebagai berikut. .[12]

a. *Probe*

   Probe atau yang biasa disebut *probing* adalah suatu usaha untuk mengakses sistem atau mendapatkan informasi tentang sistem. Contoh sederhana dari *probing* adalah percobaan *log in* ke suatu *account* yang tidak digunakan. *Probing* dapat dianalogikan dengan menguji kenop-kenop pintu untuk mencari pintu yang tidak dikunci sehingga dapat masuk dengan mudah[12].

b. *Scan*

Scan adalah *probing* dalam jumlah besar menggunakan suatu *tool. Scan* Biasanya merupakan awal dari serangan langsung terhadap sistem yang oleh pelakunya ditemukan mudah diserang

c. *Packet Sniffer*

Packet sniffer adalah sebuah program yang menangkap *(capture)* data dari paket yang lewat di jaringan. Data tersebut bisa termasuk *user name, password,* dan informasi-informasi penting lainnya yang lewat di jaringan dalam bentuk teks. Paket yang dapat ditangkap tidak hanya satu paket tapi bisa berjumlah ratusan bahkan ribuan, yang berarti pelaku mendapatkan ribuan *user name* dan *password.*

d. Denial of Service (DoS)

Denial of Service adalah sebuah metode serangan yang bertujuan untuk menghabiskan sumber daya sebuah peralatan jaringan komputer sehingga layanan jaringan komputer menjadi terganggu. Salah satu bentuk serangan ini adalah *'Ping Flood Attack'*, yang mengandalkan kelemahan dalam sistem *'three-way-handshake'*.

Pada keamanan jaringan akan semakin banyak ancaman yang terus berkembang pesat oleh orang-orang yang tidak bertanggung jawab atau pun ingin mengambil alih. Dengan pertumbuhan *internet* di zaman yang serba teknologi akan memberikan kekhawatiran terhadap keamanan jaringan dari sistem informasi baik perusahaan, instansi, sekolah-sekolah dan Perguruan tinggi. Berikut adalah kegiatan seseorang yang ingin mengambil alih [13]

1. *Cracker*

Cracker bisa dikategorikan sebagai orang yang memahami jenis pemrograman tingkat tinggi dan sedikit pengetahuan jaringan. Umumnya kabanyakan *craker* membuat sebuah program untuk mendisfungsikan atau memanipulasi jalur yang seharunya.

2. *Hacker*

Hacker merupakan golongan profesional komputer atau IT, mereka terdiri dari daripada trutera komputer, pengatur cara dan sebagainya yang memiliki pengetahuan tinggi dalam sesuatu sistem komputer. Di dalam sistem keamanan perlu penjagaan dari orang-orang yang tidak bertanggung jawab. *Hacker* adalah seseorang atau sekelompok orang yang mempelajari, menganalisa, dan selanjutnya bila menginginkan, bisa membuat, memodifikasi, atau bahkan mengeksploitasi sistem yang terdapat di sebuah perangkat lunak dan keras seperti program komputer atau administrasi. *Hacker* dibagi menjadi 3 yaitu:

a) *White-Hat Hacker*

Istilah dalam bahasa inggris *White-hat* yaitu memfokuskan aksinya bagaimana melindungi sebuah sistem. Bertentangan dengan *black-hat* yang lebih memfokuskan aksinya kepada bagaimana menerobos sistem. *White-Hat Hacker* adalah *attacker* beretika yang mencoba mebobol keamanan tetapi untuk tujuan altruistik ataupun sekurang - kurangnya tidak berniat jahat.

b) *Black-Hat Hacker*

Istilah dalam bahasa inggris yang mengacu kepada peretas yaitu mereka yang menerobos keamanan sistem komputer tanpa izin, umumnya dengan maksud untuk mengakses komputer-komputer yang terkoneksi ke jaringan tersebut.

Tujuan dari setiap serangan yang dilakukan oleh *hacker* adalah mengambil informasi penting dari *database* sistem informasi. *Hacker* akan melakukan berbagai cara untuk menembus keamanan dari sistem informasi dengan bantuan sumber dan tutorial untuk membobol, sehingga tidak akan mustahil bagi *hacker* untuk *bias* masuk ke dalam sistem informasi.

2.2.3 *Information System Security Assessment Framework (ISSAF)*

ISSAF adalah kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi dalam berbagai *domain* dan rincian kriteria

evaluasi atau pengujian spesifik untuk masing-masing *domain. ISSAF* digunakan untuk memenuhi persyaratan penilaian keamanan system informasi. *Framework* ini terdiri atas tiga fase pendekatan dan Sembilan langkah penilaian. Pendekatan tersebut meliputi tiga tahap sebagai berikut:[14]

1. *Fase I: Planing*

   Fase ini berisi langkah-langkah untuk bertukar informasi, merencanakan dan mempersiapkan tes. Sebelum melakukan pengujian Perjanjian *Assessment* resmi akan ditandatangani oleh kedua belah pihak. Perjanjian ini akan memberikan perlindungan hukum bagi kedua belah pihak. Perjanjian ini akan ditentukan tim yang terlibat, tanggal, waktu, dan ketentuan lainnya. Langkah-langkah utama dalam fase ini adalah:

   a. *Information Gathering* yaitu pengumpulan informasi secara luas tentang sistem informasi.
   b. *Project Chartering* yaitu pembuatan dokumen projek/perjanjian proyek.
   c. *Resource Identication* yaitu proses mengidentifikasi sumber daya sistem
   d. *Budgeting* yaitu proses penentuan anggaran proyek.
   e. *Cash Flow* yaitu pelaporan anggaran atau arus kas.
   f. *Work Breakdown Structure* yaitu proses memecah-mecah pekerjaan menjadi lebih kecil.
   g. *Project kick-off* yaitu proses langkah awal pengujian.

2. *Fase II: Assessment*

   Fase ini merupakan fase pelaksanaan uji penetrasi. Pada fase *assessment* dilakukan pendekatan bertingkat. Setiap tingkatan akan memberikan akses lebih luas ke aset informasi yang diinginkan. Fase fokus pada proses penilaian resiko dan alamat setiap komponen yang di uji. Kegiatan pada fase ini terdiri dari:

a. *Identification of Assessment Entities*: Identifikasi enitas-entitas yang akan diuji, misalnya proses, aset, fasilitas, dll.)
b. *Identification of Threats and Vulnerabilities:* kegiatan ini menjelaskan bagaimana caranya mengidentifikasi ancaman dan kerentanan sistem informasi.
c. *Impact Assessment:* Menilai dampak kerentanan terhadap sistem informasi yang di eksploitasi.
d. *Likelihood Assessment:* Mengevaluasi kemungkinan kerentanan yang terjadi.

3. *Fase III: Control Assessment*

Semua informasi yang dibuat atau disimpan pada sistem yang diuji harus dihapus. Jika tidak mungkin menghapus dari *remote system*, semua file ini (dengan lokasi mereka) harus disebutkan dalam laporan teknis sehingga staf teknis klien dapat menghapus setelah laporan diterima[3].

a. *Evaluation of Legal and Regulatory Compliance:* Kegiatan ini mengevaluasi keadaan sistem informasi dengan memperhatikan peraturan dan perundang-undangan saat ini.
b. *Evaluation of Enterprise Information Security Policy:* Kegiatan ini mengevaluasi kebijakan keamanan sistem informasi *enterprise.*
c. *Evaluation of Enterprise Information Security Organization and Managament:* Mengevaluasi organisasi dan manajemen keamanan sistem.
d. *Assessment of Enterprise Information System Security and Controls:* Meninjau aspek keamanan dari sistem infomasi yang berbeda, Misalnya keamanan fisik, keamanan lingkungan, kontrol teknis (misalnya: keamanan jaringan, keamanan host dll).
e. *Evaluation of Enterprise Security Operations Management:* (Kegiatan yang mengevaluasi manajemen operasi keamanan sistem informasi).

f. *Evaluation of Enterprise Business Continuty Management:* Mengevaluasi kemampuan sistem informasi untuk memastikan ketersedian informasi secara berkelanjutan saat terjadi serangan. Hasil dari pengujian ini akan diimplementasikan untuk penanggulangan dan pengambilan keputusan. Pada fase ini akan diputuskan apakah akan menerima, mengurangi, atau menghindari kerentanan dan risiko terkait yang telah diidentifikasi dalam fase sebelumnya. Pada bagian ini akan ditiinjau metodologi pengujian penetrasi *ISSAF* yang mengevaluasi jaringan dan sistem informasi yang terdiri dari tiga fase dan sembilan langkah penilaian. Tiga fase ini adalah: *Planning and Preparation, Assessment,* serta *Reporting, Clean-up and Destroy Artifacts.*

a) *Fase Planning and Preparation*

Fase ini melakukan perencanaan dan persiapan penelitian, tahapan ini mencakup kegiatan berkoordinasi dengan pihak pengelola yang bertanggung jawab terhadap sistem informasi di Institut Teknologi Telkom Purwokerto terkait izin

b) *Fase Assessment*

Fase ini adalah tahap pengujian terhadap sistem informasi dengan sembilan langkah operasi:

1. *Information Gathering:* Pengumpulan informasi secara luas tentang sistem informasi seperti: IP target, *Domain Info*, DNS.
2. *Network Mapping:* Pengumpulan informasi dengan melakukan pendekatan yang lebih teknis dan mengidentifikasi perangkat yang berkerja. Tiap-tiap pendekatan dibedakan tindakan yang harus dilakukan yaitu:
    1) *Find Live Host* (Mencari *Host)*
    2) *Port and service Scanning* (Pemindaian *port* dan layanan)
    3) *Perimeter network mapping* (Pemetaan Jaringan Sistem Informasi)

4) *Identifying Critical Services* (Mengidentifikasi informasi layanan penting)
5) *Operating System Printing* (Mengidentifikasi sistem operasi yang digunakan)
6) *Identifying Routes Using Management Information Base (MIB)* (Mengidentifikasi rute yang menggunakan basis informasi manajemen)
7) *Service Printing* (Mengidentifikasi layanan)

3. *Vulnerability Identification:* Mengidentifikasi kerentanan sistem informasi dengan beberapa langkah untuk mendeteksi kelemahan, yaitu:
   1) Identify vulnerable services using service banners (Mengidentifikasi celah kerentanan)
   2) Perform vulnerability scans (Melakukan pemindaian kerentanan)
   3) Perform false positive and false negative verification (Melakukan verifikasi *false positive* dan *false negative*)
   4) Enumerate discovered vulnerabilities (Mencatat celah kerentanan yang ditemukan)
   5) Estimate probable impact (Perkiraan dampak yang akan terjadi)
   6) Identify attack paths and scenarios for exploitation (Mengidentifikasi alur *attacker* dan cara untuk mengeksploitasi)
4. *Penetration,* melakukan pengujian terhadap sistem keamanan yang menekan kan pada:
   1) Develop new tools/scripts if needed (Pengembangan alat untuk melakukan *penetration*)

2) *Test proof of concept code/tools before use them to avoid problems during the actual pentesting* (Melakukan pengecekan terhadap *tools* yang akan digunakan agar terhindar dari masalah)
3) *Use proof of concept code against* target (Menggunakan konsep dalam *attacker*)
4) *Verify or disprove the existence of vulnerabilities* (*Verifikasi* celah kerentanan)
5) *Document findings* (Laporan)

5. *Gaining Access & Privileges Escalation:*

Dalam fase ini pentester akan terkoneksi untuk mengakses target. Dalam tahapan ini *hacker* akan melakukan penetrasi ke dalam komputer atau sistem. Tentunya tahap ini dilakukan setelah mendapatkan informasi kelemahan pada tahap *scanning*.

6. *Enumerating Further*

Fase ini mencantumkan aktivitas berbahaya yang dapat dilakukan penyerang dalam sistem. Dalam fase ini bertujuan untuk:

1) Mendapatkan *username* dan *password*
2) *Sniff traffic and analyze* (mengujia rute dan menganalisis)
3) *Gather Cookies and use them to exploit sessions and for password attacks* (Pengumpulan informasi histori dalam *attacker)*
4) *E-mail address gathering* (Pengumupulan informasi alamat email)
5) *Identifying new routes and networks* (Mengidentifikasi rute dan jaringan baru)

6) Mapping internal networks (Memetakan jaringan)

7. *Compromise Remote User/Sites*

   Fase ini melakukan kontrol jarak jauh dengan sistem informasi yang sudah diretas.

8. *Maintaining Access*

   Dalam fase ini *hacker* akan menanam sebuah sistem yang akan mengontrol sistem di kemudian hari, karena celah kerentanan sistem akan langsung ditutup.

9. *Covering Tracks*

   Menghapus jejak sang *hacker* agar tidak diketahui dengan menghapus *log* riwayat.

   1) Menyembunyikan *tools* yang digunakan
   2) Menghapus *History and edit log files*
   3) Menghilangkan *scaning sistem*
   4) Menghilangkan anti-virus
   5) Menerapakan *root-kits* yang inginkan

10. *Audit* Melaporkan potensi kerentanan dalam sistem

c) *Reporting, Cleanup and destroy artifacts*

Melaporkan serta menghancurkan semua jejak/bukti aktivitas penetrasi. Laporan ini meliputi dari:

1. Laporan Verbal: Laporan yang disampaikan secara lisan, berisi gambaran yang harus dilakukan oleh sistem informasi setelah dilakukan serangan.
2. Laporan Akhir: Presentasi hasil dari setiap *test* dan dengan solusi penanggulangan. Laporan tersebut terdiri dari:

   1) Management Summary (Ringkasan)

   2) Scope of the project (Cakupan proyek)

   3) Tools that have been used (*Tools* yang digunakan)

4) *Dates and times of the actual tests on the system* (Waktu pengujian sistem)
5) *Outputs of tests performed* (Laporan dari hasil pengujian)
6) *List action* (Daftar Pengujian)
7) *List of Vurnerability* (Daftar celah kerentanan)

Semua informasi yang dibuat ataupun yang disimpan harus dihapus, ataupun diberikan kepada pihak pengelola.

2.2.4 OWAPS versi 4

OWASP merupakan singkatan dari *Open Web Aplication Security Project* yang dikeluarkan oleh *OWASP Foundation* yang sebagai organisasi non-profit (amal) di Amerika Serikat yang didirikan pada tanggal 21 April 2004. *OWASP* berdedikasi untuk membuat *framework* pengujian keamanan yang bebas digunakan oleh siapa saja. Dalam *OWASP*, semua alat, dokumen, forum, dan bab terbuka untuk siapa saja yang tertarik dalam meningkatkan keamanan aplikasi. Adapun *framework* yang digunakan pada *OWASP versi 4* adalah sebagai berikut: [14]

1. *Information gathering*

   Tahap Pengumpulan informasi dari sistem informasi yang akan dilakukan *penetration testing*. Pada tahap ini terdiri atas sepuluh aktivitas untuk mengumpulkan informasi, yaitu:

   1) Mencari kelemahan sistem informasi
   2) Mencari keamanan *web server*
   3) Memantau informasi celah kerentanan
   4) Melihat keamanan yang digunakan *web server*
   5) Memantau aktivitas halaman *web*
   6) Mengidentifikasi aktiviats sistem informasi
   7) Memetakan jalur eksekusi *testing*
   8) Merangkai keaman *web server*

2. *Authentication Testing*

Otentikasi merupakan tindakan membangun dan mengkonfirmasi sesuatu bahwa klaim yang dibuat adalah benar. Otentikasi sebuah objek dapat berarti mengkonfirmasikan sumbernya, sedangkan otentikasi seseorang adalah dengan memverifikasi identitasnya. Otentikasi tergantung pada satu atau lebih faktor *otentikasi.* Dalam keamanan komputer, otentikasi adalah proses mencoba untuk memverifikasi identitas digital pengirim komunikasi. Salah satu contoh umum dari proses otentikasi adalah *log* proses. Pengujian skema otentikasi berarti memahami bagaimana proses otentikasi bekerja dan menggunakan informasi tersebut untuk menghindari mekanisme otentikasi. Kegiatan *testing* yang dilakukan yaitu:

1) Pengujian *Encrypted Channel*
2) Pengujian *Default Credentiasl*
3) Pengujian mekanisme keamanan
4) Pengujian skema *otentikasi*
5) Pengujian fungsi *remember* sandi
6) Pengujian kelemahan *cache browser*
7) Pengujian kelemahan *reset password*
8) Pengujian untuk pertanyan/jawaban keamana yang leamah

3. *Authorization Testing*

Otorisasi merupakan konsep yang memungkinkan akses ke sumber daya bagi mereka yang diizinkan untuk menggunakannya. Pengujian untuk otorisasi berarti memahami bagaimana proses otorisasi bekerja dan menggunakan informasi tersebut untuk menghindari mekanisme otorisasi. Otorisasi adalah proses yang datang setelah *otentikasi*

berhasil, sehingga *tester* akan memverifikasi titik ini setelah ia memegang identitas yang sah. Selama ini jenis penilaian harus diverifikasi apakah mungkin untuk memotong skema otorisasi, menemukan kerentanan jalur *tranversal*, atau menemukan cara untuk meningkatkan hak-hak istimewa yang ditugaskan untuk *tester*. Pengujian sistem ini meliputi :

1) Pengujian file *direktori*
2) Pengujian jalur akses yang dilalui
3) Pengujian izin hak
4) Pengujian langsung terhadap sumber

4. Session Management Testing

Session Management didefinisikan sebagai himpunan semua kontrol yang mengatur interaksi *full state* antara pengguna dan aplikasi berbasis *web* (*Matteo Meucci and Friends*: 2014). Ini secara luas mencakup apa pun dari bagaimana otentikasi pengguna dilakukan, bagaimana mereka logout. Lingkungan aplikasi web yang populer, seperti *ASP* dan *PHP*, memberikan pengembang dengan penanganan sesi yang *built in*. Beberapa jenis identifikasi token biasanya akan dikeluarkan, yang akan disebut sebagai "*ID* Sesi" atau *Cookie*[7]. Kegiatan ini meliputi beberapa pengujian yaitu:

1) *Testing for Bypassing Session Management Schema* (Memverifikasi skema otorisasi yang telah diterapkan)
2) *Testing for Cookies attributes* (Pengujian melalui *cookie* dalam *attacker*)
3) *Testing for Session Fixation* (Pengujian kerentanan *session*)
4) *Testing for Exposed Session Variables* (Pengujian dengan mengakses aplikasi secara tidak sah)

5) *Testing for Cross Site Request Forgery* (Pengujian yang memaksa pengguna melakukan tindakan yang di kontrol *hacker*)

6) *Testing for logout functionality* (Pengujian dengan pemutusan akses)

7) *Test Session Timeout* (Pengujian dengan memeriksa pengguna masuk secara *illegal* untuk dikeluarkan)

8) *Testing for Session puzzling* (Pengujian tingkat kerentanan aplikasi yang memungkinkan *attacker* melakukan berbagai tindakan jahat)

5. *Configuration and Deploy Management Testing*

Fase ini akan melakukan testing terhadap konfigurasi manajemen keamanan yang ada dalam sistem informasi

1) Menentukan apakah ada cacat pada manajemen konfigurasi, seperti penempatan yang salah dan sistem *weakness*
2) Uji untuk kerentanan *platform-spesifik*
3) Uji metode *HTTP* dan *Cross-Site Tracing*

6. *Identity Management Testing*

Melakukan pengujian terhadap manajemen identitas. Pengujian ini meliputi sebagai berkut:

1) *Test Role Definitions* (Pengujian terhadap definisi peran *user*)

2) *Test User Registration Process* (Pengujian proses *registrasi user*)

3) *Test Account Provisioning Process* (Pengujian proses penyediaan akun)

4) *Testing for Account Enumeration and Guessable User Account* (Pengujian *brute force* dan memverifikasi pengguna yang *valid*)

5) *Testing for Weak or unenforced username policy* (Pengujian terhadap akun pengguna yang valid)

6) *Test Permissions of Guest/Training Accounts* (Pengujiaan akses masuk yang di izinkan)

7) *Test Account Suspension/Resumption Process* (Pengujian untuk mengambil alih akun yang di *hack*)

7. *Input Validation Testing*

Pengujian terhadap inputan validasi sistem informasi, meliputi aktivitas sebagai berikut:

1) Uji kemampuan aplikasi untuk menangani masukan berbahaya dan permintaan yang salah
2) Uji fungsionalitas pengodean *input/output* yang ada dalam aplikasi
3) Uji perintah sistem di kolom *input*
4) Tes untuk *Cross-Site Scripting* (Tercermin/DOM/Tersimpan)
5) Uji untuk *SQL Injection*
6) Uji untuk injeksi *LDAP/ORM/XML/SSI/XPATH*/*Code injection*
7) Uji untuk Pemisahan / Penyelundupan *HTTP*
8) Uji fungsi *AJAX*

8. *Error Handling*

Menganalisis *error* yang sering terjadi terhadap sistem, dapat dilakukan dengan cara sebagai berikut:

1) *Analysis of Error Codes* (Menganalisa *program error*)

2) *Analysis of Stack Traces* (Menganalisa jejak masuk nya *hacker* untuk mengetahui informasi *attacker*)

9. *Cryptography*

Tahap ini dilakukan pengujian informasi yang di enkripsi untuk dipecahkan. Pengujian dilakukan dengan tahap sebagai berikut:

1) *Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection*
2) *Testing for Padding Oracle*
3) *Testing for Sensitive information sent via unencrypted channels*

10. *Business Logic Testing*

Pengujian bisnis yang dilakukan dalam *web server* yang dilakukan dengan tahap berikut ini:

1) *Test Business Logic Data Validation*
2) *Test Ability to Forge Requests*
3) Tentukan apakah aliran logika dapat disalahgunakan atau dilewati

11. *ClientSide Testing*

Pengujian situs atau *link* dengan aktivitas sebagai berikut:

1) *Testing for DOM based Cross Site Scripting*
2) *Testing for JavaScript Execution*
3) *Testing for HTML Injection*
4) *Testing for ClientSide URL Redirect*
5) *Testing for CSS Injection*
6) *Testing for ClientSide Resource Manipulation*
7) *Test Cross Origin Resource Sharing*
8) *Testing for Cross Site Flashing*
9) *Testing for Clickjacking*

10) *Testing WebSockets*
11) *Test Web Messaging*
12) *Test Local Storage*

2.2.5 Sitem Informasi

Informasi adalah data yang telah diklasifikasi atau diolah atau diinterprestasi untuk digunakan dalam proses pengambilan keputusan. Sistem pengolahan mengolah data menjadi informasi atau tepatnya mengolah data dari bentuk tak berguna menjadi berguna bagi penerimanya. Nilai informasi berhubungan dengan keputusan. Nilai informasi dilukiskan paling berarti dalam konteks sebuah keputusan. Bila tidak ada keputusan, maka informasi menjadi tidak diperlukan. Keputusan dapat berkisar dari keputusan berulang sederhana sampai keputusan strategis jangka panjang. Fungsi utama informasi adalah menambah pengetahuan atau mengurangi ketidakpastian pemakai informasi. Informasi yang disampaikan kepada pemakai mungkin merupakan hasil data yang dimasukkan ke dalam database dan pengolahan suatu model keputusan. Akan tetapi, dalam pengambilan keputusan yang kompleks, informasi hanya dapat menambah kemungkinan keputusan atau mengurangi bermacam-macam pilihan. Informasi yang disediakan bagi pengambil keputusan memberikan suatu kemungkinan faktor resiko pada tingkat-tingkat pendapatan yang berbeda. Informasi yang dapat ditangani atau dihasilkan dalam fungsi organisasi yang dapat ditentukan banyaknya sangat penting karena sistem informasi memberikan informasi formal mengenai keadaan yang memberikan tingkat kemungkinan meramalkan yang lebih besar kepada pemakai, baik mengenai kejadian maupun mengenai hasil kegiatan (termasuk kegiatan pemakai sendiri) organisasi. Hal-hal yang dapat ditentukan oleh nilai informasi adalah manfaat dan biaya untuk mendapatkannya. Suatu informasi dikatakan bernilai bila manfaat lebih efektif dibandingkan dengan biaya mendapatkannya. Akan tetapi, perlu dipertimbangkan bahwa informasi dapat

digunakan untuk beberapa kegunaan sehingga tidak memungkinkan dan sulit untuk menghubungkan suatu bagian informasi pada suatu masalah tertentu dengan biaya untuk memperolehnya karena sebagian besar informasi dimanfaatkan tidak hanya oleh satu pihak di dalam perusahaan. Sebagian besar informasi tidak dapat persis ditafsir keuntungannya dengan suatu nilai uang, tetapi dapat ditafsir nilai efektivitasnya. Kualitas suatu informasi tergantung dari 3 (tiga) hal yaitu informasi harus akurat, tepat waktu dan relevan.

a. Akurat

   Informasi harus bebas dari kesalahan-kesalahan dan tidak bias atau menyesatkan. Akurat juga bebarti informasi harus jelas mencerminkan maksudnya. Informasi harus akurat karena dari sumber informasi sampai penerima informasi kemungkinan banyak terjadi gangguan *(noise)* yang dapat mengubah atau merusak informasi tersebut.

b. Tepat waktu

   Informasi yang datang pada si penerima tidak boleh terlambat. Informasi yang sudah usang tidak akan mempunyai nilai lagi karena informasi merupakan landasan dalam pengambilan keputusan.

c. Relevan

   Informasi tersebut mempunyai manfaat untuk pemakainya. Relevansi informasi untuk orang satu dengan orang yang lain berbeda, misalnya informasi sebab kerusakan mesin produksi kepada akuntan perusahaan adalah kurang *relevan*, tetapi akan lebih relevan bila ditujukan kepada ahli teknik perusahaan.

Suatu sistem mempunyai satu tujuan *(goal)* atau sasaran *(objective)*. Sasaran dari sistem sangat menentukan masukan yang dibutuhkan sistem dan keluaran yang akan dihasilkan sistem. Sistem keamanan mempunyai tujuan yaitu untuk mengevaluasi keamanan sistem informasi dan mempunyai sasaran yaitu sistem informasi. Oleh

karena itu, dengan tujuan untuk mengevaluasi maka dibutuhkan sebuah *Penetration testing* untuk menguji keamanan sistem informasi.

2.2.6 Penetration Testing

Penetration Testing adalah metode untuk mengevaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya. Sebagai contoh serangan yang dilakukan oleh *black hat, hacke, cracker, dan defacer*. Adapun tahapan untuk melakukukan *penetration testing* yaitu:[15]

a. *Reconnaissance*

Adalah tahap seorang *hacker* mengumpulkan data sebanyak-banyaknya tentang target atau sasaran. Data yang diperlukana baik dari tanggal lahir, nomor rumah, nama istri, hobi, dan plat kendaraan. *Reconnaissance* dibagi menjadi 2, yaitu *Active Reconnaissance* dan *Passive Reconnaissance,* dimana *active reconnaissance* melakukan pengumpulan data dengan cara bertatap muka langsung, sedangkan *passive reconnaissance* melakukan pengumpulan data melalui media informasi

b. *Scanning*

Merupakan tahap dimana *hacker* mulai melakukan serangan. Dalam tahap ini, *hacker* akan mencari kelemahan dari target. Metode ini biasanya menggunakan *tools* seperti *Nmap.*

c. *Gaining Access*

Dalam tahapan ini *gaining access* atau *hacker* akan melakukan penetrasi kedalam komputer atau sistem. Tentunya tahap ini dilakukan setelah mendapatkan informasi kelemahan pada tahap *Scanning.*

d. *Maintenance Access*

Setelah mendapatkan akses komputer target, biasanya hacker ingin tetap menguasai sistem target. Misalkan ketika sang administrator

mengganti semua *password user*, sang *hacker* tidak mau kehilangan control dangan menanam *backdoor, rookit,*dan *trojan.*

e. *Covering Tracks*

Hukuman kepada pelaku kejahatan dunia maya memiliki hukum yang jelas. Pada tahap ini, seorang *hacker* harus menghapus jejaknya sehingga aktivitasnya tidak diketahui dan juga keberadaannya tidak dapat dilacak dengan mudah. Salah satu yang harus dilakukan untuk menghapus jejak adalah dengan menghapus *Log File*

Penetration testing merupakan bagian yang sangat penting jika ingin mengetahui tingkat keamanan dari sistem informasi dan diperlukan sebuah kontrol manajemen. Maka diperlukan *framework* pengujian sistem terhadap kerentanan. Ada beberapa *framework* keamanan sistem informasi yaitu: *EC-Council LPT, OWASP, OSSTMM, ISSAF, CISSP*. Didalam penelitian ini akan menggunakan *framework ISSAF* dan *OWASP VERSI 4.*