Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM)

Yendri Ikhlas Fernando[1], Rahmad Abdillah[2]
[1,2]Teknik Informatika UIN Sultan Syarif Kasim Riau
Jl. H.R. Soebrantas no. 155 KM. 18 Simpang Baru, Pekanbaru 28293
yendri.ikhlas.fernando@students.uin-suska.ac.id[1], rahmad.abdillah@uin-suska.ac.id[2]

***Abstrak* – Teknologi aplikasi web berkembang pesat sehingga digunakan untuk berbagai tujuan seperti keperluan akademik pada suatu universitas. Namun teknologi ini tidak bisa lepas dari tingginya ancaman kemanan yang tinggi sehingga bisa merugikan pihak-pihak tertentu. Pada dunia keamanan informasi dikenal security testing yakni suatu proses yang menguji seberapa tinggi tingkat kemanan suatu aplikasi yakni aplikasi web sehingga dapat diketahui nilai dan tingkat keamanan dan rekomendasi yang berguna. Salahsatu metode security testing yang efektif adalah Open Source Security Testing Methodology Manual (OSSTMM). OSSTMM adalah metode tertentu untuk melakukan security testing dan menyajikan hasil berupa RAV dan STAR. Aplikasi web yang diteliti adalah Sistem Penerimaan Mahasiswa Baru Universitas XYZ sehingga didapatkan hasil dan rekomendasi yang berguna dalam pengembangan lebih lanjut dimasa yang akan datang. Hasil penilaian yang didapatkan yakni dengan nilai Actual Security 74,5877.**

Kata kunci – Aplikasi Web, OSSTMM, Security Testing, RAV, STAR

PENDAHULUAN

Perkembangan teknologi informasi semakin cepat dari hari ke hari. Kemajuan teknologi ini memudahkan manusia dalam melakukan berbagai aktivitas salah satunya dengan adanya aplikasi web. Universitas XYZ sebagai salah satu universitas yang sedang berkembang pesat banyak memanfaatkan teknologi aplikasi web.

Disisi lain kemajuan teknologi ternyata selalu diiringi dengan sisi negatif. Berkembangnya teknologi aplikasi web juga diiringi dengan tingginya serangan keamanan [1] dan meningkatnya celah keamanan pada aplikasi web [2]. Menurut [2] penting untuk mengamankan sebuah aplikasi web dengan melakukan *security testing* (pengetesan keamanan).

Sistem PMB sebagai salah satu sistem Universitas XYZ memegang peranan penting dalam kelangsungan aktivitas perkuliahan. Sistem ini baru saja diimplementasikan oleh pihak kampus. Saat ini keamanan yang masih diterapkan masih terbatas salahsatunya pada penerapan protokol http yang terdapat kekurangan dan kelemahan. Sistem ini begitu penting karena dalam penggunaannya hanya orang tertentu saja yang bisa mengaksesnya. Basisdata yang dimiliki juga sangat penting terkait proses pembayaran dan penerimaan mahasiswa baru. Pernah terjadi redundansi data yakni satu akun namun memiliki tiga buah data yang sama. Dan juga belum ada jalur alternatif dan cadangan pada sistem PMB apabila sistem ini mati saat digunakan. Jika ini terkendala maka dapat bisa mengakibatkan terhambatnya aktivitas ketika adanya gangguan pada sistem. Oleh karena itu perlunya dilakukan *security testing* (pengetesan keamanan) pada sistem ini dibanding sistem yang lain berdasarkan rekomendasi dari pihak kampus.

Dari berbagai cara untuk mengetes suatu aplikasi web, terdapat banyak metode diantaranya NIST, ISSAF, OSSTMM [3]. Namun metode yang lebih baik, efisien dan lebih tuntas dalam *security testing* (pengetesan keamanan) adalah OSSTMM [4] [5]. OSSTMM juga dinilai sebagai sebuah metode global komprehensif untuk *security testing* (pengetesan keamanan) [6].

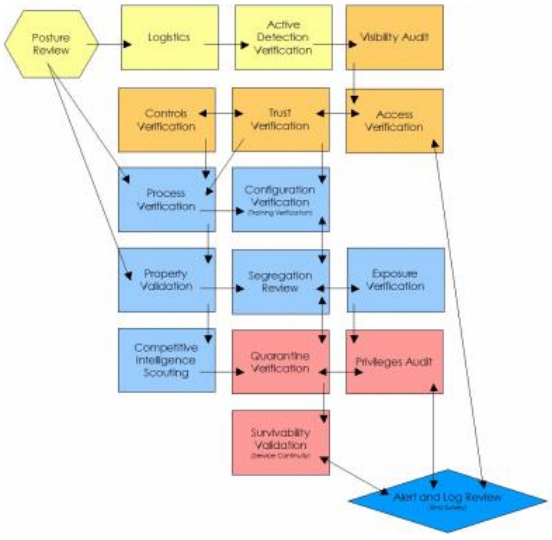
Berdasarkan hal ini maka penulis melakukan penelitian *security testing* (pengetesan keamanan) pada Sistem PMB yang baru difungsikan dengan metode OSSTMM untuk mengetahui tingkat keamanannya sehingga berguna bagi pihak pengembang.

LANDASAN TEORI

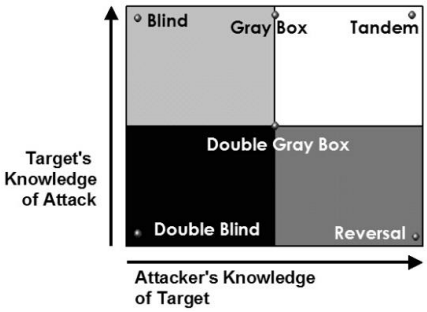
A. Open Source Security Testing Methodology Manual (OSSTMM)

Menurut [4] ada beberapa penting yang harus diketahui sebelum melakukan *security testing* (pengetesan keamanan) menggunakan OSSTMM yaitu :

1. Mendefinisikan apa yang akan diproteksi yang disebut dengan **Aset.**
2. Mengetahui lingkungan sekitar Aset yang dapat berupa mekanisme proteksi, proses atau *service* yang berada disekitar Aset. Disini akan terjadi interaksi dengan Aset. Ini disebut dengan **Zona *Engagement.***
3. Mengetahui segala sesuatu yang berada diluar Zona *Engagement* yang diperlukan untuk menjaga Asset. Semua ini disebut dengan **Skop.**
4. Bagaimana skop berinteraksi dengan dirinya sendiri dan dunia luar. Aset yang berada dalam skop dikelompokkan melalui arah interaksi .Bisa dipahami sebagai arah darimana dilakukan *security testing* (pengetesan keamanan) pada penelitian. Hal ini disebut dengan **Vektor.** *Masing-masing* vektor harus dites secara terpisah.
5. Identifikasi perlengkapan yang diperlukan untuk melakukan tes. Pada Vektor, interaksi bisa terjadi pada berbagai level. Level-level ini bisa dibagi dalam banyak jalan, semuanya dibagi berdasarkan fungsi dan disebut dengan ***Channel*** yakni *Human, Physical, Wireless, Telecommunication* dan *Data Network.* Masing-masing *channel* harus dites terpisah untuk masing-masing vektor. Setiap *channel* memiliki 17 modul yang sama. Setiap modul memiliki *task* yang berbeda-beda tergantung *channel* masing-masing.
6. Menentukan **Tipe Tes.** Tentukan informasi apa yang ingin dihasilkan dari sebuah tes. Apakah hanya sekedar melakukan tes pada interaksi dengan Aset atau jangkauan yang lebih seperti mendapatkan respon dari penanganan keamanan. Ini disebut dengan **Tipe Tes**. Tipe Tes ditentukan setiap kali ingin melakukan tes.



Gambar 1. 17 Modul pada *Channel*[4]



Gambar 2. Tipe Tes[4]

B. Risk Assesment Value (RAV)

RAV berfungsi untuk analisa hasil tes dan menghitung nilai keamanan yang aktual pada tiga faktor yaitu *: Operational Security* (OpSec), *Loss Control* dan *Limitations*. Nilai ini disebut dengan ***RAV Score***. Dengan menggunakan *RAV Score* seorang auditor bisa dengan mudah merangkum (*extract*) dan menjabarkan (*define*) standar berdasarkan nilai kemaanan yang ada untuk meningkatkan pertahanan selanjutnya. RAV adalah *security metric* yang menunjukkan seberapa baiknya proteksi dari sebuah sistem atau lingkungan dari sebuah ancaman. RAV bersifat kuantitatif maka hasilnya akan berupa angka [4].

Tabel 1. Nilai RAV [2]

Hasil	Keterangan
100	*Security* stabil/sempurna. Antara *interaction* (interaksi) dan *control* (kontrol) seimbang.
<100	*Security* masih lemah. Sehingga serangan (*Attack Surface*) lebih besar. *Control* (kontrol) masih sedikit dibanding *interaction* (interaksi) yang ada.
>100	*Security* berlebihan. *Control* (kontrol) lebih banyak daripada *interaction* (interaksi) yang ada. Bisa menimbulkan masalah baru seperti *complexity* (kompleksitas) dan *maintenance* (pemeliharaan).

Category		OpSec	Limitations
Operations		Visibility	Exposure
		Access	Vulnerability
		Trust	
Controls	Class A - Interactive	Authentication	Weakness
		Indemnification	
		Resilience	
		Subjugation	
		Continuity	
	Class B - Process	Non-Repudiation	Concern
		Confidentiality	
		Privacy	
		Integrity	
		Alarm	
			Anomalies

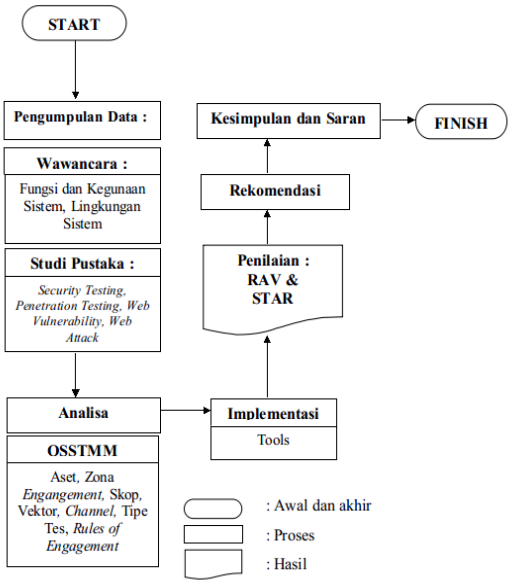
Gambar 3. Hubungan Opsec, Kontrol dan Limitation [4]

C. Security Testing Audit Report (STAR)

Menurut [4], STAR adalah sebuah dokumen yang berfungsi sebagai laporan tes yang menunjukkan secara rinci apa yang dilakukan dalam penelitian. Berikut ini informasi yang terkandung dalam STAR, yaitu :1.Tanggal dan waktu tes, 2. Durasi tes, 3. Nama analis, 4.Tipe tes, 5. Ruang lingkup tes, 6. Index, 7. Channel, 8. Vektor Tes, 9. Metrik Attack Surface, 10. Selesai atau tidaknya suatu tes, 11. Isu terkait tes dan validitas hasil, 12. Proses yang mempengaruhi *Limitations.*

Kesuksesan hasil dari penelitian OSSTMM menunjukkan pengukuran yang actual (*actual measurement*) terhadap *security* dan *control.* Contoh STAR ada dilampiran.

METODOLOGI PENELITIAN



Gambar 4. Metodologi Penelitian

1. Wawancara

Wawancara dilakukan kepada pihak Akademik Rektorat Universitas XYZ dan Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) Universitas XYZ untuk menggali informasi seputar Sistem Penerimaan Mahasiswa Baru yang akan diteliti.

2. Studi Pustaka

Studi pustaka dilakukan untuk mendapatkan pengetahuan tentang kajian-kajian ilmu yang akan digunakan pada saat penelitian berlangsung seperti *security testing, web penetration testing, web vulnerability, web attack* dan sebagainya.

3. Analisa

Pada tahap ini dilakukan analisa tentang hal-hal yang diperlukan sebelum sebelum melakukan *security testing* (pengetesan keamanan). Informasi-informasi yang didapat dari hasil wawancara dan studi pustaka kemudian digunakan untuk menetukan Aset (apa yang akan diproteksi), Zona *Engangement* (lingkungan sekitar aset), Skop (lingkungan diluar Zona *Engangement* yang diperlukan untuk menjaga sperasional asset tetap berjalan), Vektor (arah interaksi skop), *Channel* (kanal pengujian), Tipe Tes, dan *Rules of Engagement*. OSSTMM yang digunakan adalah OSSTMM versi 3.0.

4. Implementasi

Setelah mengetahui informasi yang dibutuhkan pada tahap analisa selanjutnya tahap ini adalah tahap implementasi *security testing* (pengetesan keamanan). Implementasi dilakukan dengan menggunakan Sistem Operasi Kali Linux 1.05 64 bit dengan kumpulan aplikasi *opensource* yang sudah tersedia dan terinstal didalamnya seperti Nmap, Zenmap, Nping, Nikto, Whois daln sebagainya. Dan ada juga yang menggunakan alplikasi gratis yang berjalan di sistem operasi Windows seperti Nettools 5. Semua tool yang digunakan tergantung dari hasil task yang ada.

5. Penilaian RAV dan STAR

Setelah semua *security testing* dilakukan kemudian hasil dan temuan *security testing* digunakan untuk membuat Penilain berbentuk *Risk Assessment Value* (RAV) dan *Securtity Testing Audit Report* (STAR). RAV menghasilkan suatu nilai keamanan sedangkan STAR mengasilkan dalam bentuk status dan komentar terhadapa *security testing* yang dilakukan.

6. Rekomendasi

Setelah dilakukan penilaian dalam bentuk RAV dan STAR maka dirumuskan beberapa rekomendasi terhadap hasil penelitian yang dilakukan. Rekomendasi dibuat dalam dua jenis yang pertama rekomendasi yang ditulis pada setiap modul *channel* yang dilakukan tes dan yang kedua rekomendasi secara keseluruhan. Diharapkan rekomendasi ini menjadi informasi dan pengetahuan yang berguna dari pihak yang bersangkutan.

7. Kesimpulan dan Saran

Pada tahap ini ditentukan kesimpulan berupa hasil akhir dari penelitian yang berguna bagi pihak yang bersangkutan dimasa yang akan

datang dan saran yang berguna untuk pihak lain yang ingin melanjutkan penelitian yang sama dengan masalah yang baru.

ANALISA

Untuk bisa melakukan security testing harus dianalisa dan ditentukan poin-poin yang dibutuhkan dalam penelitian terlebih dahulu. Poin-poin yang dimaksud adalah sebagai berikut ini :

1.Aset

Sistem PMB dengan perangkat terkait yakni web server, database server dan web service inilah yang disebut dengan Aset. Aset sebagai objek penelitian pada penelitian ini.

2. Zona Engangement

Zona Engangement adalah lingkungan yang dibangun disekitar aset yang menyangkut mekanisme proteksi, proses/layanan yakni sebagai berikut:

a. *Mekanisme Proteksi*
   Mekanisme proteksi dapat diartikan sebagai apa-apa saja proteksi yang saat sekarang ini ada pada Sistem PMB. Dengan pengamatan dan wawancara proteksi-proteksi yang ada saat sekarang ini adalah dari segi protokol hanya menggunakan protocol HTTP. Dari segi enkrispi hash menggunakan MD5. Pihak owner sistem PMB belum melakukan analisa keamanan dan evaluasi terkait keamanan yang saat sekarang ini diterapkan di Sistem PMB. Pihak owner beasumsi Sistem PMB aman berdasarkan walaupun belum dilakukan upaya pegecekan secara serius. Kemudian sistem memberikan hak akses kepada orang-orang tertentu yakni orang yang diberi akses seperti pegawai akademik dan pengguna yang memiliki pin dan password. Selanjutnya sistem terinstal di lingkungan server Pusat Teknologi dan Pangkalan Data Universitas XYZ. Lebih lanjut trafik di sistem PMB masih tergolong kecil karena ruang lingkupnya masih Provinsi Riau dan tambahan beberapa dari Provinsi sekitar.
b. *Proses/Layanan*
   Proses berupa penerimaan mahasiswa baru di Sistem PMB dan mahasiswa abru mencetak kartu ujian. Layanan berupa Jalur Mandiri, Jalur Paskasarjana dan Jalur Pindahan (Pindahan Jurusan dan Universitas).

3. Skop

Hal-hal yang tidak bisa dipengaruhi secara langsung. Diantaranya adalah sebagai berikut:

a. *Energi Listrik*
   Energi listrik yang digunakan oleh aset yakni Sistem PMB agar bisa dioperasikan.
b. *Kebijakan/Legislasi/Regulasi*
   Kebijakan/Legislasi/Regulasi yang sekarang ini ada yang mengatur aset. Saat ini tidak ada kebijakan khusus yang melindungi aset. Hanya Kode Etik Mahasiswa untuk tidak merusak aset universitas. Selain itu terdapat regulasi secara umum di Indonesia terkait penggunaan perangkat elektronik dan teknologi informasi yakni UU-ITE Tahun 2008.
c. *Hosting dan Bandwith Internet*
   Hosting dan Bandwith internet mempengaruhi keberlangsungan aset yang harus selalu diperpanjangan atau diperbesar agar tidak mengganggu fungsi dan kerja aset.
d. *Kualitas Jaringan*
   Kualitas jaringan juga mempengaruhi keberlangsungan aset. Kwalitas jaringan harus mencapai kwalitas yang memadai.
e. *Budaya*
   Budaya bisa berupa pelatihan yang dilakukan dalam penggunaan aset. Sistem PMB saat ini tidak ada pelatihan penggunaan hanya pedoman pengunaan berbentuk dokumen.

Hal-hal yang ada kerjasama saat penelitian dikerjakan. Diantaranya adalah sebagai berikut:

a. *Bagian Akademik Rektorat Universitas XYZ*
   Bagian Akademik Rektorat menjadi partnership (teman) ketika melakukan penelitian karena Akademik Rektorat bertindak sebagai owner (pemilik) aset.
b. *Pusat Teknologi dan Pangkalan Data Universitas XYZ*
   PTIPD juga menjadi partnership (teman) saat melakukan penelitian karena aset berada dan disimpan didalam gedung PTIPD.

Dalam hal menjaga operasional infrastruktur, Web Service tidak termasuk dalam skop karena web service dibuat oleh pihak ketiga antara pihak Universitas XYZ dan pihak BNI Syariah. Jadi web service tidak termasuk kedalam skop.

4. Vektor

Vektor berarti bagaimana skop berinteraksi dengan dirinya sendiri dan dunia luar. Aset yang berada dalam skop dikelompokkan melalui arah interaksi. Bisa dipahami sebagai arah darimana dilakukan *security testing* pada penelitian. Vektor jenis ini berarti pengetesan keamanan dilakukan dari arah luar ke skop. Karena Sistem PMB digunakan oleh calon mahasiswa dan mengaksesnya menggunakan jaringan internet

maka vektor yang ditetapkan pada penelitian ini adalah dari luar ke skop yakni dari jaringan internet/intranet ke Sistem PMB.

5. Channel

Berdasarkan pemaparan rinci terkait ruang lingkup pada semua channel maka untuk pembahasan aset, zona engangement dan skop yang telah diketahui sebelumnya yakni Sistem PMB maka channel yang paling tepat yang membahas hal tersebut adalah *Data Network Channel.*

6. Tipe Tes

Tipe tes ditentukan sesuai dengan kondisi yang paling tepat bagi analis dalam melakukan penelitian. Tipe tes dipilih salahsatu dari yang semua tipe tes yang ada. Oleh karena itu tipe tes yang paling tepat dalam penelitian ini adalah *Double Gray Box (Black Box).*

IMPLEMENTASI

Setelah melakukan security testing terhadap semua task yang ada maka dirangkum semua nilai tersebut yakni sebagai berikut:

Tabel 2. Rangkuman *Visibillity*

No	Keterangan	Jumlah
1	2 Akses ke aset	2
2	Web server	1
3	Database server	1
4	Port	1
Total		**5**

Tabel 3. Rangkuman Akses

No	Keterangan	Jumlah
1	Port-port yang berstatus Open sebanyak 15 port yakni 21, 22, 23, 25, 53, 80, 110, 119, 143, 443, 465, 563, 587, 993, 995	15
Total		15

Tabel 4. Rangkuman *Trust*

No	Keterangan	Jumlah
1	Spoofing IP Address	1
Total		1

Tabel 5. Rangkuman *Authentication*

No	Keterangan	Jumlah
1	Penyaringan data masuk oleh server.	1
2	Penyaringan data keluar oleh server.	1
3	SNMP versi 3 yang membutuhkan authentication.	1
4	Sistem login pengguna.	1
5	Sulitnya dilakukan teknik *brute force*	1
Total		5

Tabel 6. Rangkuman *Non-Repudiation*

No	Keterangan	Jumlah
1	Tidak bisa menlanjutkan pada langkah selanjutnya pada pengisian form pengguna sebelum semua form yang wajib selesai diisi.	1
Total		1

Tabel 7. Rangkuman *Confidentiality*

No	Keterangan	Jumlah
1	IP ID Sequence Generation yang bernilai *Randomized*	1
2	Rahasia dalam parameter yang digunakan dalam sistem login sehingga menyulitkan untuk menerka parameter	1
Total		2

Tabel 8. Rangkuman *Vulnerability*

No	Keterangan	Jumlah
1	Terdapat 9 port yang berstatus Open namun tidak digunakan maka dinilai sebagai Vulnerbility yakni port 25 (SMTP), 110 (POP3), 119 (NNTP), 143 (IMAP), 465 (SMTPS), 563 (SNEWS), 587 (SUBMISSION), 993 (IMAPS), 995 (POP3S)	9
2	Menggunakan protokol HTTP dan HTTPS terutama pada sistem login sehingga akun login bisa dilacak secara plaintext.	1
3	*Cookie ci_session* tanpa *httponly flag*	1
4	Tidak ada *anti-clickjacking x-frame option header*	1
5	PHP/5.2.9 bukan versi terbaru. Versi terbaru saat dilakukan *scanning* adalah PHP 5.4.4.	1
6	Debug HTTP menampilkan informasi *debugging server*	1

No	Keterangan	Jumlah
7	OSVDB-877 - HTTP Trace Aktif. Rentan diserang dengan teknik XST	1
8	OSVDB-12184 - Terdapat Informasi PHP yan sensitive yakni HHTP Request yang bersi Query yang spesifik	1
9	OSVDB-3233 - Terdapat file asli Apache 2.0 yang executable dan memberikan informasi tentang lingkungan server. Semua file asli seharusnya dihapus. Berpotensi diserang dengan teknik XSS	1
10	OSVDB-3268 - Ditemukan folder *indexing*	1
11	OSVDB-3092 - Ditemukan file License.txt yang bisa berisi informasi sensitive seperti situs aplikasi	
12	OSVDB-756 dan CVE-2002-0082 - Beberapa versi mod_ssl/2.2.11, OpenSSL/0.9.8k, PHP/5.2.9, mod_apreq2-20051231/260, mod_perl/2.0.4, perl/v5.10.0, mod_ssl 28.7 dinilai rentan diserang dengan teknik buffer overflow melalui remote karena versinya tidak *update*	1
Total		20

Tabel 9. Rangkuman *Weakness*

No	Keterangan	Jumlah
1	Tidak ada *notification* (pemberitahuan) atau peringatan ketika proses login berhasil atau gagal	1
2	Ketiadaan tanggapan kerusakan dan forensik berupa dokumentasi yang baik.	1
Total		2

Tabel 10. Rangkuman *Concern*

No	Keterangan	Jumlah
1	Tidak adanya sistem integritas yang baik seperti halaman *backend* database	1
Total		1

Actual Security			**Total Nilai**
Opsec		*Visbility*	5
		Access	15
		Trust	1
Kontrol	Kelas A (Interaktif)	*Authentication*	5
		Indemnification	0
		Resilience	0
		Subjugation	0
		Continuity	0
	Kelas B (Proses)	*Non-Repudiation*	1
		Confidentiality	2
		Privacy	0
		Integrity	0
		Alarm	0
Limitations		*Vulnerability*	20
		Weakness	2
		Concerns	1
		Exposures	0
		Anomaly	0

Gambar 5. Nilai RAV

Nilai *Opsec* adalah : 11.038515
Nilai Kontrol
True Controll : 3,642315
Full Controll : 3,642315
Nilai *Limitations*
Limitations : 19,020911
Nilai Security
Security Delta : -26,42
True Protection : 73,58
Actual Security **: 74,5877**

Nilai-nilai diatas didapatkan dari rumus penghitungan RAV sebelumnya. Yang menjadi patokan adalah *Actual Security* yang memiliki nilai **74,5877**. Jika dilihat pada peraturan penilaiN RAV maka nilai **74,5877** menunjukkan keamanan yang diterapkan masih belum bisa menyeimbangi interaksi atau layanan yang ada. Berarti keamanan pada sistem tersebut perlu ditingkatkan sebesar **26,42** agar mencapai 100.

Untuk bisa mencapai Actual Security bernilai 100 maka semua nilai limitations yakni Vulnerability, Weakness dan Concern harus bernilai 0 maka seluruh kondisi yang menyebabkan naiknya nilai Limitation harus diperbaiki. Sedangkan untuk kontrol tetap dipertahankan walaupun akan menaikkan nilai Actual Security menjadi diatas 100 ketika nilai Limitation bernilai 0. Jika nilai Actual Security diatas 100 maka kontrol yang dianggap tidak perlu bisa dihilangkan atau dimaksimalkan.

ID Laporan		Tanggal	6 April 2015
Pimpinan Auditor		Durasi Tes	1 Nov 2014 – 1 April 2015
Skop and Indek	Sistem PMB	Vektor	Dari Client ke Server via Jaringan Internet
Channels	Data Network	Tipe Tes	Double Blind

Saya bertanggung jawab atas informasi dalam laporan ini dan mengakui semua informasi didalamnya faktual dan benar.

TANDA TANGAN	STEMPEL PERUSAHAAN
Sertifikat ISECOM #	Sertifikat ISECOM #

OPERATIONAL SECURITY VALUES		CONTROLS VALUES	
Visibility	5	Authentication	5
Access	15	Indemnification	0
Trust	1	Resilience	0
		Subjugation	0
LIMITATIONS VALUES		Continuity	0
Vulnerability	20	Non-Repudiation	1
Weakness	2	Confidentiality	2
Concern	1	Privacy	0
Exposure	0	Integrity	0
Anomaly	0	Alarm	0
OpSec	11.038515	True Control	3,642315
Limitations	19,020911	Security Δ	-26,42
True Protection	73,58	Actual Security	74,5877

Gambar 6. Nilai RAV

REKOMENDASI

Beberapa rekomendasi dari penelitian ini adalah:

A. Rekomendasi Umum

1. Terdapat pembahasan rinci dan khusus terkait kebijakan/peraturan pemeliharaan aset Sistem PMB.
2. Adanya pemeliharaan secara berkala atau sosialisasi dalam penggunaan Sistem PMB.
3. Terdapat sistem cadangan seperti Backup Data Computer (BDC) dan jalur alternatif ketika Sistem PMB mati atau rusak seperti pelaksanaan secara manual terkait fungsi Sistem PMB.
4. Ketika jumlah pengguna cukup besar maka dapat menggunakan IDPS, menggunakan Load Balancing dan Loose Source Routing pada server dan memasang sistem alarm untuk keperluan pengawasan sistem.

B. Rekomendasi untuk Mengatasi Vulnerability

1. Menutup port-port yang tidak dibutuhkan karena port-port ini tidak digunakan dan tidak mendukung fungsi Sistem PMB sehingga dapat menjadi celah penyerangan yakni port 25 (SMTP), 110 (POP3), 119 (NNTP), 143 (IMAP), 465 (SMTPS), 563 (SNEWS), 587 (SUBMISSION), 993 (IMAPS), 995 (POP3S).
2. Menggunakan protokol yang dienkripsi seperti protokol HTTPS terutama pada halaman login agar tidak bisa dicuri Password dan PIN pengguna saat login. Karena berdasarkan penelitian akun login pengguna dapat diketahui oleh orang lain secara *plaintext.*
3. Memperbaiki cookie ci_session yang tanpa httponly flag.
4. Mengadakan anti-clickjacking x-frame option header .
5. Melakukan pembaruan versi PHP, mod_ssl, openSSL, mod_apreq2, mod_perl, perl yang berpotensi diserang dengan teknik buffer overflow secara remote.
6. Menyembunyikan informasi debugging server pada Debug HTTP
7. Menonaktifkan HTTP Trace Aktif.
8. Menyembunyikan atau menghapus informasi PHP yang sensitif seperti HTTP Request yan berisi query yang spesifik.
9. Menghapus file asli apache 2.0 yang executable karena berpotensi diserang dengan teknik XSS.
10. Menghapus folder indexing dan file License.txt yang berisi informasi sensitif.

C. Rekomendasi untuk Mengatasi Weakness

1. Pada sistem login ketika terjadi terjadi kesalahan sebaiknya dibuat sebuah pemberitahuan (*alert*) yang memberitahu pengguna bahwa akun yang digunakan salah.
2. Sebaiknya terdapat dokumentasi yang baik terhadap tanggapan kecelakaan dan forensik pada sistem jika dibutuhkan.

D. Rekomendasi untuk Mengatasi Concerns

Sebaiknya terdapat sistem integritas data yang baik. Salah satunya dapat membuat tampilan *backend* database sehingga pengubahan terhadap

database tidak langsung mengakses server (phpMyAdmin).

KESIMPULAN

Beberapa kesimpulan penelitian ini adalah sebagai berikut:

1. Dari semua *security testing* yang ada terdapat beberapa task yang tidak dikerjakan karena task tersebut berada diluar skop dan tipe tes yang bisa dilihat pada STAR.
2. Sistem Penerimaan Mahasiswa Baru Universitas XYZ memiliki nilai RAV 74,5877 dari nilai sempurna 100 dan memiliki kekurangan nilai 26,42. Berdasarkan teori OSSTMM hal ini berarti keamanan atau kontrol yang saat ini diterapkan pada Sistem PMB belum bisa menyeimbangi interaksi yang ada sebanyak nilai kekurangan diatas.
3. Terdapat beberapa rekomendasi setelah dilakukan security testing yang bisa dijadikan acuan oleh pihak pemilik Sistem PMB.
4. OSSTMM dinilai memiliki kekurangan dalam hal penentuan hasil analisa. Hasil analisa bisa berbeda setiap analis.
5. Metode OSSTMM masih perlu ditambahkan langkah-langkah dalam security testing secara lebih rinci dan jelas.

Adapun saran adalah sebagai berikut:

1. Penelitian dapat menggunakan channel, test type (tipe tes), dan vektor, lainnya yang belum digunakan.
2. Menggunakan metode yang lain untuk menutupi kekurangan OSSTMM.

REFERENSI

[1] Cenzic. 2014. *Application Vulnerability Trends Report*

[2] Erdogan, Gencer. 2009, *Security Testing of Web Based Applications.* Norwegia: University of Science and Technology.

[3] Guiomar Corral, Xavier Cadenas, Agustín Zaballos, M.Teresa Cadenas. "A Distributed Vulnerability Detection System for WLANs", *Proceedings of the First International Conference on Wireless Internet*. 2005.

[4] Herzog, Pete. 2010, *Open Source Security Testing Methodology Manual 3.0*. United States of America: ISECOM.

[5] Prandini dan Ramili. 2010, "Towards a practical and effective security testing methodology", *Computers and Communications (ISCC)*. 2010.

[6] Guiomar Corral, Xavier Cadenas, Agustín Zaballos, M.Teresa Cadenas. "A Distributed Vulnerability Detection System for WLANs", *Proceedings of the First International Conference on Wireless Internet*. 2005.