Penetration Testing Keamanan Sistem Informasi Berbasis Web dengan Metode OSSTMM

I Wayan Ardiyasa[1], Alce Theresia Ndok[2]
Fakultas Informatika dan Komputer
Institut Teknologi dan Bisnis STIKOM Bali
Denpasar, Indonesia
e-mail: [1]ardi@stikom-bali.ac.id, [2]nonaalce@gmail.com

Abstrak

Keamanan merupakan suatu hal yang sangat penting didalam berbagai aspek kehidupan manusia terlebih lagi saat ini merupakan era penggunaan IPTEK. Pesatnya perkembangan IPTEK di era saat ini menjadikan informasi digital mengalami peningkatan akses yang begitu pesat terlebih lagi infrastruktur jaringan internet sudah sangat mendukung dengan dukungan broadband yang begitu cepat untuk mengakses informasi digital. Disisi lain keunggulan dari IPTEK ini memiliki ancaman terhadap keamanan sistem dan jaringan komputer yang dapat menimbulkan kejahatan siber (cybercrime) yang menggunakan komputer. Kejahatan dunia maya yang semakin meningkat mencakup kejahatan komputer, misalnya, SQL Injection, Cross Site Scripting dan Exploitasi sistem komputer. Untuk meminimalisir kejahatan cyber pada sistem informasi berbasis web perlu dilakukan simulasi serangan untuk mengukur keamanan pada sebuah sistem atau penetration testing. Pada proses penetration testing untuk menguji keamanan sistem dan jaringan komputer menggunakan metode Open-Source Security Testing Methodology Manual (OSSTMM). Metode ini untuk menguji seberapa tinggi tingkat keamanan suatu aplikasi terhadap serangan. Hasil dari penelitian ini adalah sebagai rekomendasi untuk membantu administrator jaringan didalam meningkatkan keamanan sistem dan jaringan komputer melalui celah keamanan yang berhasil diketahui.

Kata kunci: penetration testing, security, cyber.

Abstract

Security is very important in various aspects of human life, especially now is the era of the use of science and technology. The rapid development of science and technology in the current era has made digital information experience a rapid increase in access, moreover the internet network infrastructure is very supportive with broadband support which is so fast to access digital information. On the other hand, the superiority of science and technology poses a threat to the security of computer systems and networks which can lead to cyber crimes using computers. Increasingly cybercrimes include computer crimes, for example, SQL Injection, Cross Site Scripting and Exploitation of computer systems. To minimize cybercrime on web-based information systems, it is necessary to carry out attack simulations to measure the security of a system or penetration testing. In the penetration testing process to test the security of computer systems and networks using the Open-Source Security Testing Methodology Manual (OSSTMM) method. This method is to test how high the security level of an application is against attacks. The results of this study are recommendations to assist network administrators in improving the security of computer systems and networks through known security holes.

Keywords*: penetration testing, security, cyber.*

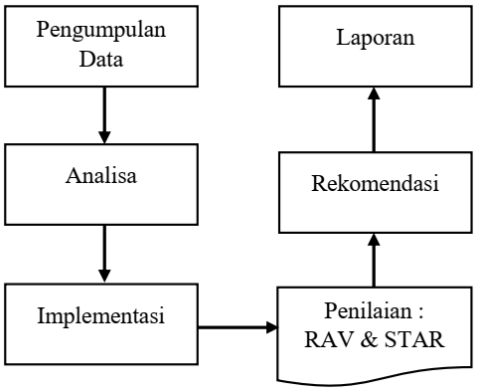
1. Pendahuluan

Perkembangan ilmu pengetahuan dan teknologi (ISTEK), khususnya teknologi informasi (*information technology*) seperti internet, sangat mendukung setiap orang dalam mencapai tujuan hidupnya dalam waktu yang singkat, baik legal maupun ilegal, menghalalkan segala cara dengan kenyataan bahwa mereka ingin menerima manfaat material atau tidak berwujud. Perkembangan teknologi informasi dan komunikasi (TIK) di dunia sangat bermanfaat bagi berbagai sektor industri, perbankan dan usaha kecil dan menengah (UKM). Sektor-sektor ini mendapat manfaat dari efisiensi dan efektivitas dalam hal operasi serta peningkatan pengalaman pengguna. Namun perkembangan ini menimbulkan masalah baru dengan munculnya berbagai *cybercrime* oleh pihak-pihak yang mencoba memanfaatkan kelemahan sistem dan kesadaran pengguna tentang sistem informasi[1]. *Cybercrime* adalah istilah untuk kejahatan yang menggunakan komputer untuk perampokan dan tindakan kriminal. Daftar

kejahatan dunia maya yang semakin meningkat mencakup kejahatan komputer, misalnya, penyebaran intrusi jaringan dan virus komputer. Selain itu, varian kejahatan yang tak terbantahkan berbasis komputer dapat berupa pencurian, penguntitan, intimidasi, dan pemaksaan. Sejak teknologi memainkan peran penting dalam kehidupan sehari-hari masyarakat dengan perkembangan teknologi, kejahatan dunia maya akan meningkat[2]. Untuk meminimalisir kejahatan *cyber* pada sistem dan jaringan komputer perlu dilakukan simulasi serangan untuk mengukur keamanan pada sebuah sistem atau *penetration testing*. *Penetration testing* adalah serangan jaringan yang disimulasikan pada sistem komputer untuk menemukan kerentanan, ancaman, dan resiko dalam sistem dan aplikasi perangkat lunak, jaringan atau aplikasi web yang dapat digunakan penyerang[3]. Didalam *penetration testing* untuk menguji keamanan sistem informasi berbasis web dengan menggunakan metode *Open Source Security Testing Methodology Manual* (OSSTMM) Metode OSSTM merupakan metode global komprehensif untuk *security testing* dan merupakan metode yang mampu menguji seberapa tinggi tingkat keamanan suatu aplikasi dan sistem dan jaringan melalui diketahuinya nilai dan tingkat keamanan dan rekomendasi yang berguna[4]. Tujuan menggunakan metode OSSTMM ini adalah sebagai *framework* didalam tahapan-tahapan pengujian suatu keamanan sistem untuk mendapatkan informasi *vulnerability* dari sistem informasi berbasis web. Hasil dari penelitian ini adalah sebagai rekomendasi untuk dasar acuan bagi pengelola dan pengembang perangkat lunak ataupun pengembang sistem didalam meningkatkan keamanan sistem dan atau memperbaiki celah keamanan pada system yang berhasil diketahui.

2. Metode Penelitian

Adapun metode pada penelitian ini adalah sebagai berikut :



Gambar 1. Metode Penelitian[5]

Berikut adalah penjelasan masing-masing alur pada gambar 3.1 yaitu :

1. Pengumpulan Data
   Pengumpulan data dilakukan dengan melakukan wawancara dengan pihak IT (puskom) yang memegang dan bertanggungjawab pada web prodi khususnya teknologi informasi, kemudian melakukan observasi dan pengumpulan informasi secara pasif pada hardware dan software[5]
2. Analisa
   Pada tahap Analisa dilakukan tahap Analisa permasalahan dan data pendukung sebelum tahap pengujian (*penetration testing*). Data-data yang ditemukan dari studi literatur akan digunakan untuk menentukan aset (apa yang akan diproteksi), *Zona Engangement* (lingkungan sekitar aset), Skop (lingkungan diluar *Zona Engangement* yang diperlukan untuk menjaga operasional *asset* tetap berjalan), *Vektor* (arah interaksi skop), *Channel* (kanal pengujian), Tipe Tes, dan *Rules of Engagement.*
3. Implementasi
   Pada tahap ini adalah tahap implementasi *security testing* (pengetesan keamanan). Implementasi dilakukan dengan menggunakan Sistem Operasi Kali Linux dan aplikasi testing yang sudah ada didalamnya seperti Nmap, Zenmap, Nping, Nikto, Whois dan sebagainya.
4. Penilaian RAV dan STAR
   Setelah semua *security testing* dilakukan kemudian hasil dan temuan *security testing* digunakan untuk membuat Penilaian berbentuk *Risk Assessment Value* (RAV) dan *Securtity Testing Audit*

Report (STAR). RAV menghasilkan suatu nilai keamanan sedangkan STAR mengasilkan dalam bentuk status dan komentar terhadap *security testing* yang dilakukan.

5. 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
6. Laporan
   Pada tahap ini adalah tahap laporan atau dokumentasi. Secara keseluruhan hasil penelitian akan dituangkan kedalam bentuk laporan

3. Hasil dan Pembahasan

3.1 Gambaran Umum Sistem

3.2 Hasil Pengujian dan Pembahasan

1. Pengumpulan Data

Pengumpulan data didapatkan dengan melakukan wawancara dengan pengelola web yaitu bagian/unit PUSKOM untuk mendapatkan informasi seputar web dan dan jaringan internet lokal, sehingga di tetapkan pada penelitian ini menggunakan dua arah interaksi[6]

2. Analisa

Penetration Testing dengan menggunakan Metode Open source Security Testing Manual Metodology menggunakan Sistem informasi berbasis web yaitu menggunakan website Program Studi Teknologi ITB STIKOM Bali yang beralamat di https://ti.stikom-bali.ac.id/. Pada web tersebut menggunakan wordpress versi 6.0.1 dengan IP Address 103.148.191.63. Pada web ti.stikom-bali.ac.id merupakan subdomain dari stikom-bali.ac.id.

3. Implementasi

A. Pengujian

Tahapan pengujian keamanan pada sistem informasi web dilakukan beberapa tahap yang bertujuan untuk mengetahui tingkat keamanan dan celah keamanan pada sistem informasi tersebut. Adapaun tahapan tersebut adalah sebagai berikut :

Tabel 1.Tabel Tahap Pengujian

No	Tahapan/Proses	Aplikasi	Keterangan
1	Reconnaisance/Information gathering	1. Netcraft 2. Maltego 3. Whois 4. Nslookup	Proses mengumpulkan informasi pada sistem yang dijadikan sebagai target.
2	Scanning Network	Nmap	Proses melakukan Scanning port pada sistem target
3	Scanning Vulnerability	1. WPscan 2. Nikto	Proses scanning vulnerability pada web target
4	Penetration Test	1. Manual test 2. Nikto 3. Acunetix	Melakukan serangan SQL injection dan XSS dan membuild up serangan

B. Tahap Reconnaisance

Tahap reconnaissance dilakukan untuk mendapatkan informasi pada website yang dijadikan target. Tahap ini menggunakan tools antara lain : Netcraft, Maltego, Whois dan Nslookup. Hasil dari tahap ini adalah informasi untuk tabel Risk Assesment Value (RAV).

C. Scanning Network

Tahap scanning network bertujuan untuk mendapatkan informasi jaringan dan pemetaan jaringan awal. Informasi yang didapatkan adalah informasi port number, IP Address. Tools yang digunakan adalah Nmap.

D. Scanning Vulnerability

Tahap scanning untuk mendapatkan suatu informasi dari data-data yang dibutuhkan untuk penelitian agar mencapai tujuan yang diharapkan[7]. Tahapan yang dilakukan adalah analisis keamanan pasif (*non-intrusif*), User Enumeration, Direktori Indexing, Linked Javascript.

4. Rangkuman

Setelah melakukan pengujian keamanan sistem, berikut akan dirangkum kedalam nilai yang menggunakan metode Open Source Security Testing Metodology Manual yang digunakan untuk penilaian *Risk Assesment Value* (RAV). Berikut adalah rangkumannya :

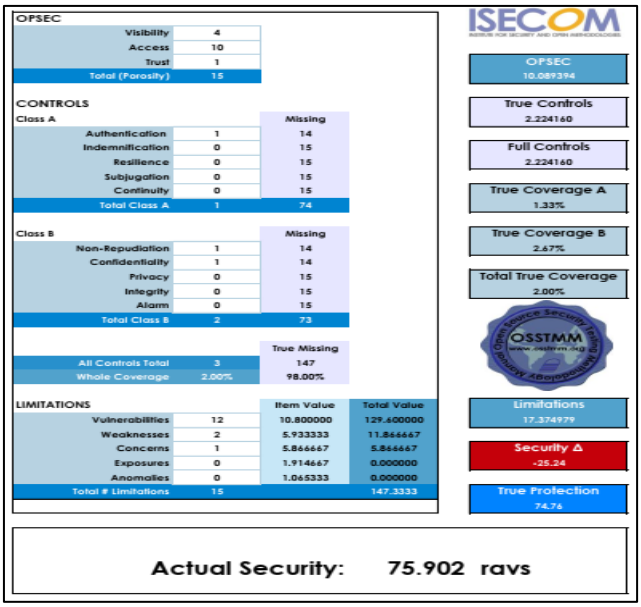
Tabel 2.Tabel Rangkuman *Risk Assesment Value (RAV)*

Tabel Visibility		
No	**Keterangan**	**Jumlah**
1	Web Server	1
2	Database	1
3	Port	1
4	Akses ke Aset	1
Jumlah		4
Tabel Akses		
No	**Keterangan**	**Jumlah**
1	21, 22, 53, 80, 110, 143,443, 587, 993, 995	10
Jumlah		10
Tabel Autentikasi		
No	**Keterangan**	**Jumlah**
1	Login Akses user pada situs	1
2	Sulit melakukan Bruteforce password	1
Jumlah		2
Tabel Non-Repudiaton		
No	**Keterangan**	**Jumlah**
1	Menggunakan login akses apabila melakukan update berita pada web. Apabila tidak memiliki akses, user tidak bisa melakukan update berita	1
Jumlah		1
Tabel Confidentiality		
No	**Keterangan**	**Jumlah**
1	Menggunakan https pada situs. Sehingga informasi dienkripsi	1
Jumlah		1
Tabel Vulnerability		
No	**Keterangan**	**Jumlah**

1	Terdapat beberapa port yang terindikasi bisa melakukan serangan kedalam server antara lain : 110 (POP3), 143 (IMAP), 587 (SUBMISION), 993 (IMPAS), 995 (POP3S)	5
2	Terdapat plugin yang belum diupdate, antara lain : slider-revolution, keydesign-addons, revslider, js_composer, contact-form-7, chaty, woocommerce.	7
Jumlah		12
Tabel Weakness		
No	**Keterangan**	**Jumlah**
1	Tidak didisable informasi user pada sistem. Dimana terdapat 2 user yang menggunakan sistem tersebut	2
Jumlah		2
Tabel Concern		
No	**Keterangan**	**Jumlah**
1	Tidak adanya sistem integritas yang baik pada halaman backend database	1
Jumlah		1

5. Penilaian RAV

Setelah dilakukan rangkuman dari hasil pengujian tersebut, selanjutnya dilakukan memasukan nilai pada RAV tabel untuk mendapatkan nilai *actual security*nya, sebagai berikut :



Gambar 2. Penilaian RAV

Pada penilaian diatas didapatkan dari rumus penghitungan RAV. Yang menjadi dasar adalah *Actual Security* yang memiliki nilai RAV = 75,902. Jika dilihat pada peraturan penilaian RAV maka nilai 75,902 menunjukkan keamanan yang diterapkan masih belum bisa menyeimbangi interaksi atau layanan yang ada. Berarti keamanan pada sistem tersebut perlu ditingkatkan sebesar 25,42 agar mencapai nilai 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 nilai 100 ketika nilai *Limitation* bernilai 0. Jika nilai *Actual Security* diatas nilai 100 maka kontrol yang dianggap tidak perlu bisa dihilangkan atau dimaksimalkan.

4. Kesimpulan

Adapun kesimpulan pada penelitian ini adalah sebegai berikut :

Hasil dari penelitian ini adalah telah dilakukan proses pentesting pada sistem informasi berbasis web dengan menggunakan metode OSTMM pada sistem keamanan pada website ti.stikom-bali.ac.id yang memiliki nilai *actual security* sebesar 75.902 ravs yang memiliki kekurangan nilai 25.10 untuk mendapatkan nilai 100. Sistem keamanan pada website tersebut masih memiliki kelemahan dan perlu dilakukannya evaluasi perbaikan.

Daftar Pustaka

[1] A. Muftiadi, T. P. Mulyani Agustina, and M. Evi, "Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking," *Jurnal Ilmiah Teknik,* vol. 1, 2022.

[2] S. K. Rahayu, S. Ruqoyah, S. Berliana, S. B. Pratiwi, and H. Saputra, "Cybercrime dan dampaknya pada teknologi e-commerce," *Journal of Information System, Applied, Management, Accounting and Research,* vol. 5, no. 3, p. 632, Aug. 2021, doi: 10.52362/jisamar.v5i3.478.

[3] J. S. Komputer, K. Buatan, M. A. Adiguna, and B. W. Widagdo, "Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)."

[4] Y. I. Fernando and R. Abdillah, "Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM)," 2016.

[5] A. Ilmi, H. B. Seta, I. Wayan, and W. Pradnyana, "Evaluasi Risiko Celah Keamanan Menggunakan Metodologi Open-Source Security Testing Methodology Manual (OSSTMM) Pada Aplikasi Web Terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta", [Online]. Available: http://new-fik.upnvj.ac.id

[6] E. Surmana, P. Tarigan, M. Fajar Sidiq, I. F. Adam, and R. Adhitama, "Security Testing Dengan Menggunakan Metode OSSTMM Pada Web Institut Teknologi Telkom Purwokerto," 2018. [Online]. Available: http://ittelkom-pwt.ac.id.

[7] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," *Jurnal Informasi dan Teknologi,* pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.