p-ISSN: 2252-3006
e-ISSN: 2685-2411

Evaluasi Keamanan Website Lembaga X Melalui *Penetration Testing* Menggunakan Framework ISSAF

I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, Dewa Made Sri Arsa
Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana
Bukit Jimbaran, Bali, Indonesia, telp. (0361) 701806
e-mail: suta.arry@gmail.com, aryasasmita@it.unud.ac.id, dewamsa@unud.ac.id

Abstrak

Lembaga X adalah lembaga pemilihan umum yang memiliki situs web sebagai media penyampaian informasi dan penataan data pemilih. Sebagai situs web yang menyimpan data sensitif, perlu dilakukan peningkatan keamanan untuk mencegah terjadinya serangan pihak luar. Metode yang dapat digunakan untuk menguji keamanan sistem adalah pengujian penetrasi. Framework ISSAF adalah standar pengujian penetrasi yang digunakan untuk menguji ketahanan situs web, yang memiliki beberapa keunggulan dibandingkan kontrol keamanan lainnya, dan berfungsi sebagai jembatan antara pandangan teknis dan manajerial. Tujuan penelitian ini adalah untuk mengetahui celah keamanan website Lembaga X dengan menggunakan metode penetration testing dengan Framework ISSAF. Framework ISSAF meliputi sembilan asesmen pengujian yang meliputi Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromise Remote User/Sites, Maintaining Access, dan Covering Tracks. Hasil dari penelitian ini adalah diperoleh 18 celah keamanan yang terdapat pada website Lembaga X. Pemberian rekomendasi diberikan untuk meningkatkan keamanan website Lembaga X.

Kata kunci: *Framework ISSAF, Penetration Testing, Website*

Abstract

Institution X is an electoral institution that has a website for delivering information and organizing voter data. It is necessary to increase security to prevent outsiders moving. Penetration testing is one of method which user to test system security. The ISSAF Framework is a penetration testing standard used to test website robustness, which has several advantages over other security controls, and serves as a bridge between technical and managerial views. The purpose of this study is to determine the security holes of the Institution X website using ISSAF penetration testing Framework. ISSAF Frameworks contains of Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Enhanced Privilege, Further Mention, Compromising Remote User/ Sites, Maintaining Access, and Covering Tracks. The results of this study obtained 18 security holes in the Institution X website. Providing recommendations is given to improve Institution X website's security.

Keywords : *Framework ISSAF, Penetration Testing, Website*

1. Pendahuluan

Website merupakan layanan informasi yang banyak diakses oleh pengguna yang terhubung dalam suatu jaringan internet. Suatu *website* dituntut untuk mampu menangani permintaan pengguna dengan baik, sehingga dalam pembangunannya tidak jarang terdapat celah keamanan yang dapat dimanfaatkan hacker untuk merusak sistem didalamnya. Keamanan pada teknologi informasi merupakan kebutuhan yang penting bagi suatu lembaga untuk menjamin kerahasiaan, integritas dan ketersediaan informasi [1].

Informasi merupakan salah satu aset penting pada sistem informasi sebuah organisasi. Ini dikarenakan informasi merupakan sumber daya strategis dalam meningkatkan nilai usaha. Penting untuk melindungi informasi, sehingga terbebas dari ancaman dan bahaya dari pihak luar. Keamanan pada sistem informasi perlu untuk diperhatikan, hal ini bertujuan untuk mencegah ancaman terhadap sistem dan mendeteksi segala kerusakan sistem. Keamanan informasi memiliki beberapa aspek yang harus dipahami dan dilindungi. Aspek keamanan

sistem informasi antara lain *confidentiality* (kerahasiaan) yaitu informasi haruslah dapat diakses hanya oleh mereka yang memiliki wewenang untuk memperolehnya serta menjamin kerahasiaan data, *integrity* (integritas) yaitu keakurasian informasi yang dilindungi melalui beberapa metodologi pengolahan yang baik, dan *availability* (ketersediaan) yaitu memastikan bahwa informasi dapat diakses sesuai dengan kebutuhan [2].

Lembaga X merupakan lembaga yang bertugas sebagai penyelenggara pemilihan umum, yang memiliki situs *website* sebagai media dalam penyampaian informasi kepada masyarakat dan sebagai media untuk pengelolaan dan penataan data pemilih pada domisili terkait. Sebagai lembaga yang memanfaatkan website, tidak jarang situs Lembaga X terjadi serangan dari pihak luar. Kasus yang cukup berdampak pada Lembaga X adalah serangan *deface* yang dilakukan pada tahun 2014, yang menyebabkan website tidak dapat diakses. Berdasarkan kasus serangan tersebut, maka perlu adanya pengujian keamanan website Lembaga X yang bertujuan untuk mengetahui celah keamanan pada website sehingga dapat dilakukan peningkatan pada aspek keamanan website Lembaga X.

Terdapat dua jenis metode dalam pencarian celah keamanan pada *website*, yaitu *vulnerability identification* dan *penetration testing* [3]. *Vulnerability identification* merupakan proses *scanning*/ pemindaian sistem pada perangkat lunak atau jaringan yang bertujuan mengetahui kelemahan dan celah di dalam sistem tersebut. Sedangkan, *penetration testing* merupakan pengujian dengan mengeksploitasi ke dalam sistem dengan tujuan mengetahui kemungkinan eksploitasi dalam sistem. Penguji pada metode *penetration testing* berwenang untuk melakukan pengujian penetrasi untuk mengeksploitasi sistem dan mencari tahu kemungkinan adanya celah keamanan yang dapat dimanfaatkan untuk eksploitasi. Keduanya merupakan metode yang baik digunakan untuk menguji keamanan sistem. Namun, *penetration testing* memiliki kelebihan dan disarankan untuk melakukan pengujian keamanan sistem [4].

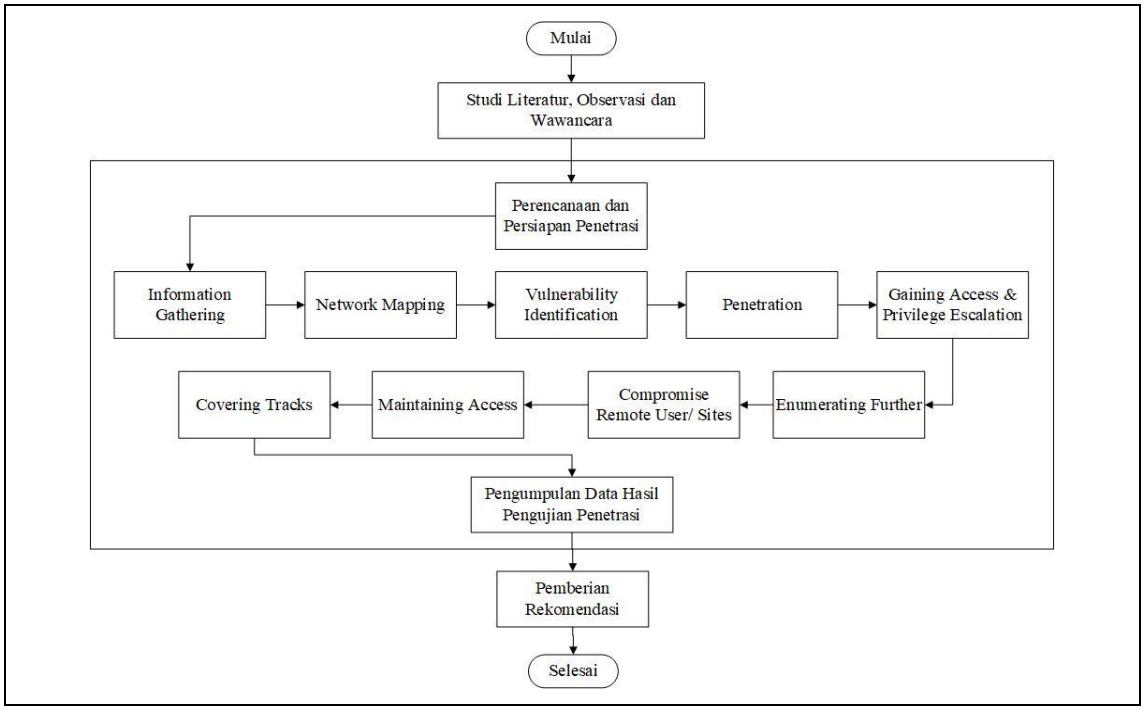
Terdapat beberapa *framework* yang disarankan dalam melakukan *penetration testing*. ISSAF (*The Information System Security Assessment Framework*) adalah kerangka pengujian penetrasi yang memiliki beberapa keunggulan kontrol keamanan, memiliki struktur intuitif yang dapat memberikan arahan kepada penguji sistem melalui langkah-langkah yang kompleks. ISSAF pada pedomannya menjelaskan proses uji penetrasi dilakukan untuk memberikan arahan pengujian secara benar dan lengkap, serta menghindari adanya kesalahan umum yang terkait dengan metode serangan yang dilakukan secara acak [5].

Penelitian mengenai *penetration testing* pernah dilakukan sebelumnya oleh Akhyar Lubis, yang menjelaskan mengenai pengujian keamanan sistem informasi website Universitas Pembangunan Panca Budi. Penelitian dilakukan melalui pengujian *penetration testing* dengan beberapa tahapan umum pengujian *penetration testing* yang dilakukan pada sisi aplikasi website [6]. Framework ISSAF cukup banyak digunakan untuk pengujian keamanan sistem melalui metode *penetration testing*. Bambang Pujiarto pada penelitiannya melakukan pengujian *penetration testing* pada jaringan WLAN pada Universitas Muhammadiyah Magelang menggunakan Framework ISSAF [7].

Penelitian ini berfokus pada pengujian keamanan *website* lembaga X yang dilakukan melalui metode pengujian *penetration testing* menggunakan Framework ISSAF. Tujuan dilakukannya penelitian ini adalah mengetahui celah keamanan pada *website* berdasarkan pada pengujian *penetration testing* Framework ISSAF, sehingga dapat diberikan rekomendasi untuk peningkatan keamanan pada *website* Lembaga X.

2. Metodologi Penelitian

Tahapan *penetration testing* merupakan tahapan pengujian berupa serangan beruntun pada website KPU Kota Denpasar. *Penetration testing* pada penelitian diawali dengan studi literatur mengenai pengujian yang dilakukan dan melakukan diskusi dan wawancara terhadap pihak pengelola *website*. Selanjutnya, dilakukan pengujian *penetration testing* dengan menggunakan tahapan *assessment* pada Framework ISSAF. Setelah pengujian dilakukan, tahap terakhir adalah melakukan pemberian rekomendasi berdasarkan hasil pengujian *penetration testing* menggunakan Framework ISSAF. Pemberian rekomendasi dilakukan untuk meningkatkan keamanan website Lembaga X. Adapun, penggambaran tahapan penelitian yang dilakukan dapat dilihat pada Gambar 1.



Gambar 1. Gambaran Umum Penelitian

2.1 *Information Gathering*

Tahap *information gathering* merupakan tahapan pengumpulan informasi secara umum yang dilakukan pada target. Informasi yang dikumpulkan meliputi informasi mengenai IP target, informasi mengenai *registrant* dan admin, informasi mengenai *reverse* DNS dan IP *lookup*, dan informasi umum lainnya.

2.2 *Network Mapping*

Tahap *network mapping* merupakan tahapan pengumpulan informasi secara spesifik mengenai jaringan pada target. Salah satu informasi yang dikumpulkan pada tahap ini meliputi informasi mengenai *port* TCP dan UDP pada sistem target.

2.3 *Vulnerability Identification*

Tahap *vulnerability identification* merupakan tahapan pemindaian *website* target untuk mengetahui kerentanan keamanan didalamnya. Pengujian pada penelitian ini menggunakan Vega Vulnerability Tools sebagai proses *scanning* untuk mengetahui kerentanan keamanan pada *website*.

2.4 *Penetration*

Tahap *penetration* merupakan tahapan simulasi serangan yang dilakukan pada *website* target yang bertujuan untuk memperoleh celah pada keamanan sistem. Jenis serangan yang dilakukan pada tahap ini yaitu serangan Cross-Site Scripting (XSS) dan serangan SQL Injection yang dilakukan pada *website* target.

2.5 *Gaining Access and Privilege Escalation*

Tahap *gaining access and privilege escalation* merupakan tahapan pengujian dengan mencoba akses ke dalam sistem target. Jenis akses yang dilakukan pada penelitian ini adalah akses ke dalam sistem *user* admin dan akses ke dalam sistem Cpanel.

2.6 *Enumerating Further*

Tahap *enumerating further* merupakan tahapan pengujian dengan melakukan pengambilan dan pemecahan seluruh informasi mengenai *password* yang diperoleh dari *website* target.

2.7 *Compromise Remote User/Sites*

Tahap *compromise remote user/sites* merupakan tahapan pengujian dengan melakukan eksploitasi akses ke dalam *user root* melalui hubungan jarak jauh/ *remote* pada *website.*

2.8 *Maintaining Access*

Tahap *maintaining access* merupakan tahapan pengujian dengan melakukan penanaman *backdoor* ke dalam sistem *website* target. Penanaman *backdoor* dapat dilakukan dengan memanfaatkan fitur file upload yang tersedia pada *website* target.

2.9 *Covering Tracks*

Tahap *covering tracks* merupakan tahapan terakhir dari pengujian *penetration testing*. Pengujian tahap ini yaitu dengan melakukan penghapusan *log* serangan yang telah dilakukan pada tahapan-tahapan sebelumnya.

3. Kajian Pustaka

Studi literatur yang digunakan pada penelitian ini merupakan literatur yang menjadi referensi pada penelitian ini. Beberapa literatur yang digunakan adalah *penetration testing* dan Framework ISSAF.

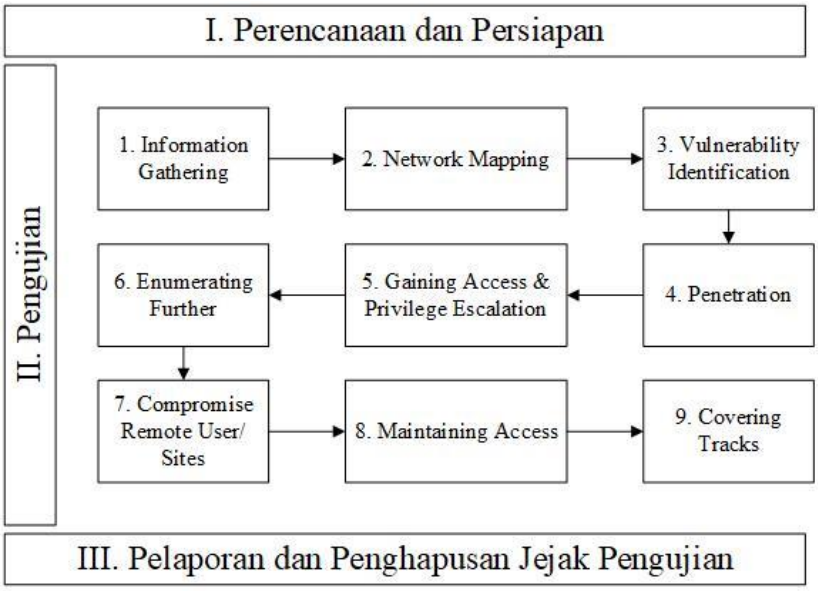
3.1 *Penetration Testing*

Penetration testing adalah metode untuk menguji kerentanan dalam sistem, identifikasi konfigurasi sistem yang buruk, kecacatan perangkat keras dan perangkat lunak serta kelemahan teknis pada sistem informasi yang diujikan [8]. *Penetration testing* berguna untuk menemukan dan mengatasi kerentanan dalam infrastruktur jaringan, menunjukkan betapa rentannya serangan berbahaya pada jaringan tersebut [9]. Melakukan pengujian secara *real-time* pada aplikasi *web* telah terbukti membantu dalam memperkuat keamanan situs *web* [10]. Tujuan utama pengujian *penetration testing* adalah untuk mengidentifikasi kelemahan keamanan sistem. Selain itu, *penetration testing* juga dapat digunakan untuk menguji kebijakan keamanan organisasi, kesadaran karyawan organisasi tentang persyaratan keamanan, dan kemampuan organisasi untuk mengidentifikasi dan menanggapi insiden keamanan [11].

Penetration testing memberikan hasil terperinci mengenai ancaman keamanan yang berisiko adanya eksploitasi apabila diimplementasikan ke dalam keamanan pada organisasi. Pengujian penetrasi membantu pihak terkait untuk melakukan identifikasi kerentanan potensial yang cepat dan akurat. Proses *penetration testing* secara umum terdiri dari pengumpulan informasi, pengidentifikasian celah-celah keamanan, dan melaporkan hasil pengujian [12]. Implementasi pengujian keamanan dengan metode *penetration testing* direkomendasikan untuk menggunakan kerangka kerja terkait sehingga tahapan serangan yang dilakukan terhadap sistem memiliki standardisasi yang telah dikembangkan dan diakui oleh organisasi tertentu yang ahli di bidang pengujian keamanan [6]. Shanley pada penelitiannya mnemukan beberapa metode yang mengulas mengenai tahapan *penetration testing*, yang meliputi ISSAF, OWASP OTG, OSSTMM, BSIMM, PTES, dan MSF [13]. Berdasarkan hasil penelitian yang dilakukan, diperoleh bahwa ISSAF dan OWASP OTG merupakan metode pengujian *penetration testing* yang memberikan kontrol keamanan yang baik dalam pelaksanaannya. ISSAF memiliki kelebihan pada sisi *domain coverage*, dimana pengujian dilakukan secara mendalam untuk menemukan celah keamanan baik dari bagian luar sistem maupun pada bagian dalam sistem.

3.2 *Framework* ISSAF

Framework ISSAF dikembangkan oleh OISSG (Open Information System Security Group). Metodologi uji penetrasi melalui *Framework* ISSAF dibuat untuk mengevaluasi jaringan, sistem dan kontrol aplikasi [14]. *Framework* ISSAF memberikan tahapan proses pengujian penetrasi secara optimal yang bertujuan memberikan arahan kepada auditor melakukan pengujian secara lengkap dan benar, serta menghindari kesalahan dalam melakukan pengujian serangan yang bersifat acak [15]. Ada tiga langkah dalam kerangka kerja ISSAF yang meliputi persiapan dan perancangan, pengujian, serta pelaporan dan pembersihan jejak serangan. Tahapan pengujian *penetration testing* menggunakan *Framework* ISSAF dapat dilihat pada Gambar 2.



Gambar 2. Metodologi Kerangka ISSAF

Tahap pertama merupakan tahapan persiapan pengujian yang dilakukan, mulai dari pembelajaran lingkup target dan penentuan aspek penyerangan yang dilakukan. Tahap *assessment* merupakan tahapan utama dari pengujian *penetration testing* yang meliputi sembilan tahap pengujian. Tahap pertama yaitu *information gathering* merupakan tahap pengumpulan informasi umum mengenai *website* target. Tahap kedua yaitu *network mapping* merupakan tahap pengumpulan informasi spesifik tentang jaringan *website* target. Tahap ketiga yaitu *vulnerability identification* merupakan tahap pemindaian kerentanan pada *website* target. Tahap keempat yaitu *penetration* merupakan tahapan simulasi serangan yang bertujuan untuk menemukan celah keamanan *website* target. Tahap kelima yaitu *gaining access and privilege escalation* merupakan tahap pengujian akses ke sistem target. Tahap keenam yaitu *enumerating further* merupakan tahapan pencarian informasi mengenai password dari *website* target. Tahap ketujuh yaitu *compromise remote user/sites* merupakan tahap untuk melakukan *remote* ke sistem target. Tahap kedelapan yaitu *maintaining access* merupakan tahapan penanaman backdoor ke dalam sistem. Tahap kesembilan yaitu *covering tracks* merupakan tahap terakhir dari pengujian, yaitu dengan menghapus *log* dari serangan yang telah dilakukan sebelumnya pada sistem target. Setelah tahap assessment dilakukan, tahap terakhir adalah pelaporan dan penghapusan jejak pengujian. Semua informasi yang tersimpan pada sistem yang diuji harus dihapus pada tahap ini, dan pelaporan hasil pengujian dilakukan.

4. Hasil dan Pembahasan

Hasil dan pembahasan pada penelitian ini meliputi pembahasan hasil pengujian *penetration testing* menggunakan *Framework* ISSAF serta rekomendasi yang diberikan berdasarkan hasil pengujian.

4.1 Hasil Pengujian *Penetration Testing*

Pengujian *penetration testing* dilakukan melalui sembilan tahap pengujian berdasarkan pedoman *Framework* ISSAF yang dilakukan pada *website* target, yang meliputi tahap *information gathering*, tahap *network mapping*, tahap *vulnerability identification*, tahap *penetration*, tahap *gaining access and privilege escalation*, tahap *enumerating further*, tahap *compromise remote user/sites*, tahap *maintaining access*, dan tahap *covering tracks*. Pengujian dilakukan pada website utama Lembaga X dan subdomain *website* yang terkait dengan situs Lembaga X. Penggunaan *tools* pada setiap tahapan dijelaskan pada tabel 1.

p-ISSN: 2252-3006
e-ISSN: 2685-2411

Tabel 1: Tools/ Metode yang Digunakan pada Setiap Tahapan

No.	Tahapan	Tools/ Metode	Fungsi
1	*Information Gathering*	a. Whois Domain b. IP lookup Scanner	a. Mengumpulkan informasi umum website b. Memperoleh domain lain yang terkait dengan website target
2	*Network Mapping*	NMap	Melakukan port scanning
3	*Vulnerability Identification*	Vega	Melakukan pemindaian vulnerability
4	*Penetration*	Manual Test	Melakukan serangan SQL Injection dan XSS
5	*Gaining Access and Privilege Escalation*	a. Manual Test b. Vega, Owaspzap, Web Site Analysis	a. Memperoleh informasi akun pada website b. Memperoleh halaman login page
6	*Enumerating Further*	a. Manual Test b. Vega	a. Memperoleh informasi password b. Memperoleh informasi cookies
7	*Compromise Remote User/Sites*	Manual Test	Memperoleh akses remote ke dalam website
8	*Maintaining Access*	Manual Test	Melakukan penanaman backdoor
9	*Covering Tracks*	Manual Test	Menghapus log serangan

Tabel 1 menjelaskan *tools* yang digunakan pada setiap tahapan pengujian penetrasi menggunakan *Framework* ISSAF. Pengujian dengan *manual test* dilakukan dengan menguji langsung ke dalam sistem *website* melalui eksekusi *script*, pemanfaatan *bug* pada *website*, dan metode lainnya tanpa menggunakan *tools.*

4.1.1 *Information Gathering*

Pengujian pada tahap *information gathering* dilakukan dengan mengumpulkan informasi umum mengenai *website* target dengan menggunakan *tool* Whois Domain, dengan memasukkan domain *website* target. Hasil dari pengujian dapat dilihat pada Tabel 2.

Tabel 2: Hasil Pemindaian Whois Domain

WHOIS Domain Result	
Domain ID	PANDI-DO45001
Domain Name	(Domain website)
Create On	2013-01-10
Expiration Date	2021-01-10
IP Address	(IP website)
IP Location	Yogyakarta
Name Servers	ns1.rumahmedia.com ns2.rumahmedia.com
Registrant ID	-
Registrant Name	-
Registrant Organizaton	-
Admin ID	-
Admin Name	-
Admin Organization	-

Berdasarkan Tabel 2, dapat dilihat bahwa pada hasil pemindaian *tool* Whois Domain diperoleh informasi mengenai IP dan *domain* target berhasil diperoleh, namun informasi mengenai admin dan *registrant* gagal diperoleh. Pengujian berikutnya yaitu dengan melakukan *reverse* IP *lookup* untuk mengetahui *subdomain website* yang terhubung pada target. Berdasarkan hasil IP *lookup* menggunakan Reverse IP Lookup Scanner, didapat hasil yang dapat dilihat pada Tabel 3.

Tabel 3: Hasil Pemindaian Reverse IP Lookup Scanner

IP	Domain
IP Target	Xyz.go.id
	Subdomain1.xyz.go.id
	Subdomain2.xyz.go.id

Berdasarkan Tabel 3, dapat dilihat bahwa hasil pemindaian pada *tool* Reverse IP Lookup Scanner diperoleh dua *subdomain* yang terkait dengan *website* target. Dengan demikian, pengujian pada tahap berikutnya dapat dilakukan pada *domain* utama dan kedua *subdomain* yang telah diperoleh pada Tabel 3.

4.1.2 *Network Mapping*

Pengujian pada tahap *network mapping* merupakan tahapan mengumpulkan informasi secara spesifik mengenai jaringan *website* target. Dilakukan *port scanning* pada *website* target menggunakan *tool* NMap. Adapun, hasil dari pengujian tahap *network mapping* dapat dilihat pada Tabel 4.

Tabel 4: Hasil Pemindaian Port Scanning

Port	Status	Services
21	Open	FTP
22	Open	SSH
23	Open	Telnet
25	Open	SMTP
80	Open	HTTP
110	Open	Pop3
142	Open	IMAP
443	Open	HTTPs
993	Open	IMAPS
3306	Open	MySQL

Berdasarkan Tabel 4, dapat dilihat hasil pemindaian *tool* NMap menunjukkan bahwa hampir seluruh *port* TCP yang penting pada *website* target terbuka. Hal ini cukup berbahaya karena beberapa *port* tersebut merupakan celah bagi *hacker* untuk dapat melakukan penyerangan. Namun, pada pemindaian port UDP tidak ditemukan adanya *port* yang terbuka.

4.1.3 *Vulnerability Identification*

Pengujian pada tahap *vulnerability identification* dilakukan dengan memindai kerentanan keamanan yang terdapat pada website target. Pemindaian kerentanan dilakukan dengan menggunakan *tool* Vega Vulnerability Scanner yang diuji pada *domain* utama dan dua *subdomain website* target. Hasil pengujian dapat dilihat pada Tabel 5.

p-ISSN: 2252-3006
e-ISSN: 2685-2411

Tabel 5: Hasil Pengujian *Vulnerability Identification*

Domain	Kerentanan	Level
xyz.go.id	Session Cookie without Secure Flag	High
	Directory Listing Detected	Low
Subdomain1.xyz.go.id	Session Cookie without Secure Flag	High
	Local Filesystem Path Found	Medium
Subdomain2.xyz.go.id	Session Cookie 2ithout Secure Flag	High
	Shell Injection Vulnerability	High
	SQL Injection Vulnerability	High
	Local Filesystem Path Found	Medium

Berdasarkan Tabel 5, dapat dilihat bahwa hasil pemindaian *tool* Vega Vulnerability Scanner menunjukkan lima kerentanan pada *website* dengan level *high*, dua kerentanan dengan level *medium*, dan satu kerentanan dengan level *low*. Hal ini perlu diperhatikan dalam keamanan sistem infomasi, karena celah dengan kerentanan tinggi memiliki risiko yang cukup besar akan adanya serangan oleh pihak yang tidak bertanggungjawab.

4.1.4 *Penetration*

Pengujian pada tahap *penetration* dilakukan melalui simulasi serangan pada *website* target, yang pada pengujian ini dilakukan beberapa jenis serangan yaitu SQL Injection dan Cross-Site Scripting (XSS). Domain yang diuji pada tahap *penetration* meliputi *domain* utama dan dua *subdomain website* target. Hasil pengujian serangan SQL Injection dan XSS yang dilakukan pada *domain* utama dan dua *subdomain website* dapat dilihat pada Tabel 6.

Tabel 6: Hasil Pengujian *Penetration*

Jenis Serangan	Domain	Celah
SQL Injection	Subdomain1.xyz.go.id/	Subdomain1.xyz.go.id// home /get_warga/51xxx12101xxxxxx/
XSS	xyz.go.id/	Input Form “No. Identitas/ KK” pada halaman utama
	Subdomain2.xyz.go.id/	Input Form “Kata Kunci”

Berdasarkan Tabel 6, dapat dilihat bahwa pada domain utama terdapat celah XSS yang dapat dimanfaatkan pada form *input* nomor KK yang tersedia. Sama halnya dengan *subdomain2*, form input kata kunci dapat digunakan sebagai celah serangan XSS. Pada *subdomain1*, celah SQL Injection dapat ditemukan ketika server memberikan hasil dari *request* yang diminta. Celah SQL Injection ini tergolong berbahaya, karena dengan diperolehnya celah SQL Injection maka informasi mengenai *database* dapat diperoleh.

4.1.5 *Gaining Access and Privilege Escalation*

Pengujian pada tahap *gaining access and privilege escalation* dilakukan dengan melakukan akses kedalam sistem *website* target. Pada tahap ini, dilakukan dua jenis pengujian akses yang meliputiakses kedalam *user admin* website dan akses kedalam Cpanel *website*. Hasil pengujian dapat dilihat pada Tabel 7.

p-ISSN: 2252-3006
e-ISSN: 2685-2411

Tabel 7: Hasil Pengujian *Gaining Access and Privilege Escalation*

Jenis Akses	Target	Status	Hasil
Akses Admin Pengelola Website	*Username* dan *Password*	Berhasil diperoleh melalui SQL Injection	Gagal
	Scanning Halaman *Login* Admin	Gagal diperoleh dengan Vega, Owaspzap, dan Web Site Analisys	
Akses Cpanel Website	*Username* dan *Password*	Gagal diperoleh	Gagal
	Scanning Halaman *Login* Cpanel	Berhasil diperoleh melalui port 2086	

Berdasarkan Tabel 7, dapat dilihat bahwa pengujian akses kedalam *user admin* gagal dilakukan. Informasi mengenai *username* dan *password* telah berhasil diperoleh, namun pencarian halaman *admin login* pada *website* target melalui pemindaian menggunakan *tools* Vega, Owaspzap, dan Web Site Analysis gagal diperoleh. Pengujian akses kedalam Cpanel juga gagal dilakukan, hal ini karena informasi mengenai *username* dan *password* Cpanel gagal diperoleh.

4.1.6 *Enumerating Further*

Pengujian pada tahap *enumerating further* dilakukan dengan memperoleh seluruh informasi pada *website* target yang berkaitan dengan *password*. Pengujian dilakukan dengan pengambilan informasi *password* admin dan informasi *cookies* pada website target. Hasil pengujian dapat dilihat pada Tabel 8.

Tabel 8: Hasil Pengujian *Enumerating Further*

Jenis Informasi	Target	Status	Hasil
Informasi Password	Password Admin	Berhasil diperoleh melalui seragan SQL Injection, namun terenkripsi	Gagal
	Dekripsi Password	Gagal, proses dekripsi password menggunakan MD5, SHA, RSA tidak berhasil dilakukan	
Informasi Cookies	Random Cookies	Berhasil memperoleh informasi session _ga, _gid, _gat _gtag dan informasi ci_session	Berhasil

Berdasarkan Tabel 8, dapat dilihat bahwa informasi *password* gagal diperoleh. *Password* dapat diperoleh melalui serangan SQL Injection, namun masih berupa enkripsi. Proses dekripsi melalui MD5, SHA, RSA, dan jenis enkripsi lainnya gagal dilakukan, sehingga pengujian dinyatakan gagal. Pada informasi *cookies*, pengujian berhasil dilakukan dengan memperoleh informasi *_ga*, *_gid*, dan *_gat_gtag* melalui serangan Cross-Site Scripting dengan menggunakan script menampilkan *alert document cookies* serta memperoleh informasi ci_session melalui tools Vega Vulnerability Scanner.

4.1.7 *Compromise Remote User/Sites*

Pengujian pada tahap *compromise remote user/sites* dilakukan dengan melakukan akses *remote* pada *website* target. Metode yang digunakan untuk memperoleh akses *remote* pada tahap *compromise remote user/sites* adalah dengan melakukan penanaman file *shell* dan pemanfaatan celah Remote File Inclusion (RFI) yang terdapat pada *website* target. Hasil pengujian dapat dilihat pada Tabel 9.

Tabel 9: Hasil Pengujian *Compromise Remote User/Sites*

Pengujian	Metode	Status	Hasil
Akses remote pada website	Penanamann file *shell* pada web server	Gagal, fitur file upload tidak berfungsi dengan baik.	Gagal
	Pemanfaatan celah Remote File Inclusion	Gagal, tidak adanya celah pada Remote File Inclusion	Gagal

Berdasarkan Tabel 9, dapat dilihat bahwa pengujian tahap ini gagal dilakukan. Pada metode penanaman *shell*, gagal dilakukan karena fitur *file upload* yang tidak berfungsi dengan baik. Selain itu, celah RFI pada website tidak ditemukan sehingga pengujian ini gagal dilakukan.

4.1.8 *Maintaining Access*

Pengujian pada tahap *maintaining access* dilakukan dengan penanaman *backdoor* ke dalam server website. Hal ini bertujuan untuk memperoleh akses ke dalam *server website*. Hasil pengujian dapat dilihat pada Tabel 10.

Tabel 10: Hasil Pengujian *Maintaining Access*

Pengujian	Status	Hasil
Penanaman Backdoor	Gagal, fitur file upload tidak berfungsi dengan baik	Gagal

Berdasarkan Tabel 10, dapat dilihat bahwa pengujian tahap ini gagal dilakukan. Hal ini fitur *file upload* yang tidak berfungsi dengan baik. Proses *upload file* berekstensi *php* berhasil dilakukan, namun berdasarkan hasil pengecekan *database* menggunakan SQL Injection, ketika dilakukan upload file berekstensi *php* kedalam sistem maka file tersebut akan berubah ekstensinya menjadi *jpg*. Sehingga, pengujian tahap ini gagal dilakukan.

4.1.9 *Covering Tracks*

Tahap *covering tracks* merupakan tahap terakhir dari *penetration testing*. Pengujian pada tahap ini dilakukan dengan menghapus seluruh *log file* serangan yang telah dilakukan pada tahapan sebelumnya. Hasil pengujian dapat dilihat pada Tabel 11.

Tabel 11: Hasil Pengujian *Covering Tracks*

Pengujian	Status	Hasil
Penghapusan log file	Gagal, akses kedalam root tidak dapat dilakukan	Gagal

Berdasarkan Tabel 11, dapat dilihat bahwa pengujian tahap ini gagal dilakukan. Hal ini karena akses *root* tidak diperoleh sehingga *log* serangan tidak dapat dihapus, yang berarti pengujian ini gagal dilakukan.

4.2 Pemberian Rekomendasi

Pemberian rekomendasi terhadap hasil pengujian penetrasi yang telah dilakukan sebelumnya diberikan berdasarkan hasil literatur yang diperoleh dari pedoman *Framework* ISSAF dan literatur lainnya. Berdasarkan dari hasil pengujian *penetration testing* menggunakan *Framework* ISSAF yang telah dilakukan pada subbab 4.1, maka diperoleh beberapa rekomendasi yang dapat diberikan untuk peningkatan keamanan *website* Lembaga X, yaitu sebagai berikut.

1. SQL Injection merupakan jenis serangan yang tergolong berbahaya pada *website*. Pencegahan serangan SQL Injection yang dapat dilakukan adalah proses validasi sebaiknya dilakukan pada level *php*, bukan *query*. Validasi level php yang digunakan dipastikan tidak terdapat *query inject*, sehingga ketika skrip validasi mendeteksi adanya string query (select, #, -- -, from, where) maka sistem akan menolak *request*.

Pencegahan lain yang dapat dilakukan adalah dengan mengenkripsi semua parameter POST sehingga penyerang akan cukup sulit menemukan celah serangan SQL Injection.

2. Jenis serangan Cross-Site Scripting (XSS) tergolong cukup berbahaya karena apabila dimanfaatkan dengan baik, cukup mengancam keamanan pada *website*. Celah XSS memanfaatkan *form input* untuk mengeksekusi *script* yang dijalankan. Pencegahan yang dapat dilakukan adalah dengan memberikan validasi pennggunaan simbol (seperti "<>", "/") pada *form input*, sehingga *script* XSS tidak dapat berjalan didalamnya
3. Port TCP merupakan salah satu celah keamanan pada *website*. Peningkatan keamanan dapat dilakukan dengan menutup seluruh *port* TCP yang terbuka pada sistem atau membuat *custom port* dengan mengubah *port* penting agar tidak berada pada *port default*.
4. Fitur *file upload* merupakan celah yang dapat digunakan untuk penanaman file *backdoor*. Proses pengubahan ekstensi file menjadi *jpg* cukup baik digunakan dalam implementasi. Namun, sebaiknya validasi mengenai ekstensi file sebaiknya diberikan sebelum file tersebut berhasil diunggah.
5. *Port* 2086 merupakan *port* yang umum digunakan sebagai akses ke dalam halaman Cpanel *login*. Namun, sebaiknya menggunakan *custom port* pada halaman Cpanel *login* untuk menghindari adanya kemungkinan serangan dari pihak luar.

5. Kesimpulan

Metode *penetration testing* merupakan pengujian keamanan sistem yang komprehensif untuk menguji basis komputasi yang lengkap. *Framework* ISSAF merupakan metodologi *penetration testing* yang dirancang untuk mengevaluasi jaringan, sistem dan kontrol aplikasi. *Penetration testing* pada *website* Lembaga X menggunakan Framework ISSAF dilakukan melalui sembilan tahap yang meliputi *information gathering*, *network mapping*, *vulnerability identification*, *penetration*, *gaining access and privilege escalation*, *enumerationg further*, *compromise remote user/sites*, *maintaining access*, dan *covering tracks*. Berdasarkan sembilan tahapan tersebut diperoleh hasil bahwa terdapat celah keamanan yang berbahaya seperti SQL Injection dan XSS pada *website* Lembaga X. Celah lainnya adalah *port* TCP yang terbuka sehingga berisiko terhadap adanya serangan dari pihak luar, serta adanya *bug* pada sistem yang dapat digunakan sebagai celah keamanan. Rekomendasi yang dapat diberikan adalah validasi pada level *php* yang bertujuan untuk mencegah serangan SQL Injection dan XSS yang merupakan sumber celah keamanan terbanyak, penutupan *port* TCP yang terbuka, serta perbaikan *bug* pada sistem yang dapat dimanfaatkan penyerang sebagai celah keamanan. Kedepannya, penelitian mengenai *penetration testing* pada Lembaga X dapat dilakukan setelah dilakukan perbaikan berdasarkan rekomedasi yang diberikan, serta penggunaan *framework penetration testing* lainnya dapat digunakan sebagai perbandingan hasil pengujian.

Daftar Pustaka

[1] A. D. Purba, I. K. A. Purnawan, and I. P. A. E. Pratama, "Audit Keamanan TI Menggunakan Standar ISO / IEC 27002 dengan COBIT 5," *J. MERPATI*, vol. 6, no. 3, pp. 148–158, 2018.

[2] Y. C. N. Bless, G. Made, A. Sasmita, and A. A. K. A. Cahyawan, "Audit Keamanan SIMAK Berdasarkan ISO 27002 (Studi Kasus : FE UNUD)," *Merpati*, vol. 2, no. 2, pp. 157–166, 2014.

[3] J. N. Goel and B. M. Mehtre, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology," *Procedia Comput. Sci.*, vol. 57, pp. 710–715, 2015.

[4] J. Doshi, "Comparison of Vulnerability Assessment and Penetration Testing," no. June 2017, 2015.

[5] F. R. Mahtuf, P. Hatta, and E. S. Wihidiyat, "Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan," *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 4, no. 1, p. 17, 2019.

[6] A. Lubis and A. Tarigan, "Security Assessment of Web ApplicationThrough Penetration System Techniques," *Jend. Gatot Subroto Km*, vol. 4, no. 100, pp. 296–303, 2017.

[7] B. Pujiarto, E. Utami, and S. Sudarmawan, "Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode Penetration Testing (Kasus : Universitas Muhammadiyah Magelang)," *Data Manaj. dan Teknol. Inf.*, vol. 14, no. 2, p. 16, 2013.

[8] M. Z. Hussain, M. Z. Hasan, M. Taimoor, A. Chughtai, M. Taimoor, and A. Chughtai, "Penetration Testing In System Administration," *Int. J. Sci. Technol. Res.*, vol. 6, no. 6, pp. 275–278, 2017.
[9] D. Stiawan, M. Y. Idris, A. H. Abdullah, F. Aljaber, and R. Budiarto, "Cyber-attack penetration test and vulnerability analysis," *Int. J. Online Eng.*, vol. 13, no. 1, pp. 125–132, 2017.
[10] K. Nagendran, A. Adithyan, R. Chethana, P. Camillus, and K. B. Bala Sri Varshini, "Web application penetration testing," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 10, pp. 1029–1035, 2019.
[11] I. Riadi, S. Sunardi, and E. Handoyo, "Security Analysis of Grr Rapid Response Network using COBIT 5 Framework," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 10, no. 1, p. 29, 2019.
[12] A. Wiradharma and A. Sasmita, "IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study : X Company)," no. December, pp. 17–29, 2019.
[13] A. Shanley and et al Johnstone, "Selection of penetration testing methodologies: A comparison and evaluation," *AISMC - Aust. Inf. Secur. Manag. Conf.*, vol. 2015, pp. 65–72, 2015.
[14] B. Ratore *et al.*, *Information System Security Assessment Framework (ISSAF) Draft 0.2.1B*. OISSG, 2005.
[15] R. H. Hutagalung, L. E. Nugroho, and R. Hidayat, "Analisis Uji Penetrasi Menggunakan ISSAF," *Hacking Digit. Forensics Expo.*, pp. 32–40, 2017.