Analisis Keamanan *Website E-Learning* SMKN 1 Cibatu Menggunakan Metode *Penetration Testing Execution Standard*

Setyo Utoro [1], Bayu Andi Nugroho [2], Meinawati [3], Septian Rheno Widianto[4]
Jurusan Sistem Informasi Bisnis,
Sekolah Tinggi Manajemen Ilmu Komputer LIKMI /
Jl. Ir. H. Juanda No.96, Lebakgede, Kecamatan Coblong, Kota Bandung, Indonesia
info@likmi.id[1,2], meinawatiwijay@gmail.com[3], septian.rheno@yahoo.de[4]

Diterima : 12 November 2020. Disetujui : 28 Desember 2020. Dipublikasikan : 28 Desember 2020.

Abstract - The Vocational High School 1 of Cibatu (SMKN) 1 Cibatu provides information for public through a website based information system. Considering the online information distribution has been increased during the COVID-19 pandemic, and many prospective students registering on the school, it is very important for SMKN 1 Cibatu to pay attention to the security system and keep users data safe. There are several methods which can be used to conduct a security information system and one we used in this test is Penetration Testing Execution Standard (PTES). PTES method could be used as a standard for web-based application security assessment for belajar.smkn1cibatu.sch.id e-learning website that includes seven phases; pre-engagement interactions, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post exploitation, and reporting. Based on the test conducted on the website, several vulnerabilities were found, such as Web Server Transmits Cleartext Credentials, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF). At the end of the research, several recommendations have been made to repair the vulnerabilities. Based on this research, it has also been concluded that website application security test by using PTES could help the school to improve information system security level in order to face incoming threats from internal or external environments.

Keywords: security; information; website; e-learning; penetration testing execution standard

Abstrak*-- Sekolah Menengah Kejuruan Negeri (SMKN) 1 Cibatu merupakan sekolah yang menyediakan informasi kepada masyarakat melalui sistem informasi berbasis *website*. Mengingat distribusi informasi secara *online* meningkat di tengah pandemi COVID-19 dan banyaknya calon siswa yang akan melakukan pendaftaran pada sekolah, maka sangatlah penting bagi SMKN 1 Cibatu untuk memperhatikan keamanan sistem informasi yang digunakan serta menjaga data-data para penggunanya. Terdapat beberapa metode yang dapat dipergunakan untuk melakukan pengujian keamanan suatu sistem informasi, dan salah satunya adalah *Penetration Testing Execution Standard* (PTES). Metode PTES ini dapat dijadikan sebagai standar penilaian keamanan aplikasi yang berbasis *web* pada *website e-learning* di alamat belajar.smkn1cibatu.sch.id yang terdiri dari tujuh tahapan atau fase yaitu dimulai dari tahap *pre-engagement interactions, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post exploitation,* dan *reporting*. Berdasarkan hasil pengujian yang dilakukan pada *website*, ditemukan celah keamanan, di antaranya adalah *Web Server Transmits Cleartext Credentials, Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF). Pada akhir penelitian dibuat rekomendasi atau usulan perbaikan untuk memperbaiki celah keamanan yang telah ditemukan. Dari hasil penelitian, dapat disimpulkan bahwa pengujian keamanan *website* milik SMKN 1 Cibatu dengan menggunakan metode PTES mampu membantu sekolah meningkatkan keamanan sistem informasi di dalam menghadapi ancaman peretasan *website* yang berasal dari lingkungan internal maupun eksternal.

Kata kunci: keamanan; informasi; website; e-learning; penetration testing execution standard

I. PENDAHULUAN

Sistem informasi di tengah Pandemi *Covid-19* ini memiliki peranan yang sangat penting di dalam membantu tercapainya pembelajaran yang dilaksanakan secara daring dan mendukung program pemerintah yang mengharuskan siswa-siswi sekolah, khususnya Sekolah Menengah Kejuruan Negeri (SMKN) 1 Cibatu untuk belajar di rumah sementara sekolah tetap harus melaksanakan pembelajaran. Pada tahun 2016, Tim *Information and Communication of Technology* (ICT) membangun *website* SMKN 1 Cibatu untuk memberikan informasi kepada masyarakat umum mengenai SMKN 1 Cibatu yaitu tentang informasi umum sekolah, visi, misi, tujuan, kegiatan – kegiatan di sekolah, struktur organisasi, jumlah guru dan staf tata usaha serta jumlah siswa aktif di SMKN 1 Cibatu.

Website SMKN 1 Cibatu juga menyediakan media pembelajaran *online* atau disebut dengan *e-learning* yang sangat dibutuhkan bagi guru dan siswa terutama ditengah kondisi Pandemi *Covid 2019*. *E-learning* atau pembelajaran *online* adalah pembelajaran yang memanfaatkan teknologi informasi sebagai alat komunikasi antara pendidik dengan siswa. Guru dan siswa bisa berinteraksi secara berkelanjutan dalam melakukan kegiatan belajar mengajar tanpa harus bertatap muka [1].

E-learning telah mendorong proses pembelajaran yang memberikan kendali lebih besar kepada siswa. Banyak manfaat yang diperoleh dengan menerapkan pembelajaran online diantaranya adalah: 1) Meningkatkan motivasi siswa, 2) Sebagai Portofolio Digital yang efektif dan efisien, 3) Menambah wawasan dan cakrawala berpikir, 4) Menumbuhkan jiwa kebersamaan, 5) Menjadi tolak ukur konsep kegiatan belajar mengajar.

Dengan semakin meningkatnya penggunaan media *e-learning* yang dimiliki oleh SMKN 1 Cibatu di dalam menunjang kegiatan belajar mengajar yang dilaksanakan, maka sangatlah penting untuk dilakukan pengujian keamanan dari sistem informasi tersebut dalam menghadapi maraknya ancaman peretasan yang diterima pihak sekolah yang berdampak pada kebocoran informasi atau gangguan layanan sistem. Informasi atau aset kritikal perlu diamankan dengan cara melakukan teknik enkripsi atau steganografi [2], [3] agar dapat terhindar dari upaya peretasan sistem yang berasal dari pihak luar [4]. Sebagai salah satu bentuk upaya dalam mengamankan data atau aset kritikal maka Tim *Information and Communication of Technology* (ICT) di SMKN 1 Cibatu membutuhkan suatu metode standar pengujian keamanan sistem informasi secara lengkap dan menyeluruh, salah satunya dapat berupa penggunaan metode *penetration testing* untuk mendeteksi berbagai kerentanan yang saat ini sulit dilacak disertai dengan rekomendasi perbaikan.

Saat ini sudah banyak penelitian yang menggunakan *framework penetration testing* sebagai standar di dalam pengujian keamanan sistem informasi, salah satunya dilakukan oleh [5], yaitu pengujian keamanan aplikasi berbasis *web* menggunakan *framework Open Web Application Security Project* (OWASP) versi 4, dengan hasil penelitian ditemukan celah keamanan sistem seperti autentikasi yang tidak dienkripsi dan rentan terhadap serangan SQL *injection*. Penelitian berikutnya yang dilakukan oleh [6] yaitu evaluasi keamanan *Website* lembaga X menggunakan *framework Information Systems Security Assessment Framework* (ISSAF), dengan hasil pengujian yang diperoleh masih terdapat celah keamanan yang berbahaya seperti SQL *Injection* dan *Cross Site Scripting* (XSS).

Framework Penetration Testing Execution Standards (PTES) merupakan salah satu *framework penetration testing* yang dibangun pada tahun 2010 dengan menyediakan panduan pengujian yang terstruktur dan mendetail serta mampu memberikan acuan bagi penggunanya terhadap setiap kualitas pengujian yang dilakukan [7]. Beberapa penelitian yang telah menggunakan *framework* PTES salah satunya dilakukan oleh [8] yaitu pengujian aplikasi berbasis *web* milik Diskominfo XYZ menggunakan *framework* PTES, hingga fase *Vulnerability Assessment* (VA) menggunakan alat uji Nikto dan OWASP-ZAP. Hasil akhir pengujiannya ditemukan beberapa celah keamanan seperti XSS, SQL *Injection* dan *Remote* OS *Command Injection*. Penelitian berikutnya dilakukan oleh [9], yaitu pengujian keamanan jaringan pada layanan internet publik di Klinik Pratama Bhakti Medika dengan menggunakan *framework* PTES hingga fase *Vulnerability Assessment* (VA) menggunakan alat uji TuxCut, MacChanger, dan Keylogger. Hasil akhir pengujian ditemukan serangan *bypassing* MAC *Address*, ARP *Spoofing*, dan serangan *Man In The Middle* (MITM).

Dari penelitian-penelitian yang telah dilakukan, pengujian keamanan sistem informasi menggunakan metode PTES mampu memberikan hasil analisis yang komprehensif terhadap para penggunanya serta mudah untuk dilakukan. Melengkapi penelitian-penelitian terdahulu yang hanya dilakukan hingga fase *Vulnerability Analysis*, maka penulis melanjutkan penelitian hingga pada fase *Exploitation*, *Post Exploitation* dan *Reporting* yang mengusulkan saran dan rekomendasi perbaikan pada sistem informasi yang diuji.

Tujuan penelitian yang akan dilakukan oleh penulis adalah menguji keamanan sistem aplikasi berbasis *web* SMKN 1 Cibatu dengan menggunakan metode PTES yang terdiri dari tujuh tahapan dengan menggunakan alat pengujian yang telah ditentukan di setiap tahapannya dan pada akhir penelitian dibuat laporan berupa rekomendasi dan saran perbaikan yang akan diinformasikan kepada pihak SMKN 1 Cibatu. Melalui laporan tersebut diharapkan SMKN 1 Cibatu dapat meningkatkan keamanan sistem informasinya secara lebih efektif.

II. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian *Penetration Testing Execution Standards* (PTES) sebagai kerangka acuan untuk menganalisa kerentanan yang dimiliki oleh *website* SMKN 1 Cibatu dan menggunakan jenis pengujian penetrasi

eksternal pada sistem informasi tersebut secara *remote*.

A. *Penetration Testing*

Penetration Testing atau uji penetrasi adalah suatu simulasi serangan terkontrol yang membantu mengidentifikasi kerawanan terhadap aplikasi, jaringan, dan cabang sistem operasi [10]. Uji penetrasi ini melibatkan analisis aktif mengenai seluruh kerentanan pada sistem yang potensial, termasuk sistem konfigurasi yang lemah dan tidak sesuai, celah pada perangkat lunak atau perangkat keras, serta kelemahan operasi di bagian proses atau penanganan teknisnya [11].

Dengan menyediakan informasi yang dibutuhkan untuk mengisolasi dan memprioritaskan kerentanan sistem secara efektif dan efisien, suatu uji penetrasi dapat membantu organisasi di dalam mengatur dan menguji perubahan konfigurasi atau *patch* untuk secara proaktif menghapus risiko ancaman yang teridentifikasi [12]. Dalam melakukan uji penetrasi, suatu organisasi dapat mengikuti standar atau regulasi yang dipilih sebelumnya untuk dijadikan acuan agar strategi pengelolaan sistem keamanannya bisa diimplementasikan secara lebih efektif.

Berdasarkan cara pengujiannya [10] uji penetrasi dapat dilakukan melalui 2 (dua) cara, yaitu:

1. Uji Penetrasi Internal, yaitu jenis pengujian yang dilakukan melalui *Local Area Network* (LAN) milik organisasi, yang berarti pengujian dilakukan pada aplikasi *web* yang di-*host* di intranet. Hal ini berfungsi untuk mengetahui apakah ada kerentanan yang dimiliki pada *firewall* milik organisasi
2. Uji Penetrasi Eksternal, yaitu jenis pengujian yang dilakukan dari luar atau eksternal organisasi dan mencakup pengujian internet dari aplikasi *web*. Penguji dapat bertindak sebagai peretas yang tidak terlalu familiar dengan sistem internal. Pengujian ini pada dasarnya juga mencakup pengujian server, *firewall* dan *Intrusion Detection System* (IDS).

B. *Penetration Testing Execution Standard (PTES)*

Metode *Penetration Testing Execution Standards* (PTES) dibangun pada tahun 2010 oleh para praktisi *information security* dengan tujuan menciptakan standar yang akan membantu klien dan penguji dalam menyediakan petunjuk mengenai *tools* atau peralatan, teknik, dan elemen lainnya yang dilingkupi oleh uji penetrasi secara keseluruhan. Di dalam implementasinya, PTES dibagi menjadi tujuh fase utama, seperti yang ditunjukkan pada Gambar 1.

1. *Pre-engagement Interactions*

Fase *Pre-engagement interactions* bertujuan untuk menyediakan dan menjelaskan peralatan atau teknik-teknik yang tersedia untuk membantu di dalam langkah memulai suatu uji penetrasi. Memilih alat yang tepat untuk uji penetrasi akan bergantung pada tipe dan kedalaman pengujian.

Gambar 1. Fase *Penetration Testing Execution Standards* [10]

2. *Intelligence Gathering*

Fase *Intelligence Gathering* adalah fase di mana data intelijen dikumpulkan dengan tujuan membantu memberikan arahan pada setiap tindakan pemeriksaan. Pada sudut pandang yang lebih luas, pengumpulan data intelijensi ini mencakup informasi pekerja, fasilitas, produksi, dan perencanaan. Secara garis besar, intelijensi ini juga memuat rahasia potensial dari kompetitor, atau informasi yang mungkin relevan dari target.

3. *Threat Modeling*

Threat Modeling adalah fase yang mendefinisikan suatu pendekatan terhadap model ancaman yang dibutuhkan untuk memberikan tindakan eksekusi yang tepat pada suatu uji pemetrasi. Pada standar PTES, tidaklah digunakan sebuah model yang spesifik, melainkan membutuhkan sebuah model yang konsisten dalam kaitannya dengan representasi ancaman, kapabilitasnya, kualifikasinya pada masing-masing organisasi yang diuji, serta kemampuannya untuk diaplikasikan pada pengujian di masa mendatang secara berulang dengan hasil yang sama.

4. *Vulnerability Analysis*

Vulnerability Analysis atau analisis kerentanan digunakan untuk mengidentifikasi dan mengevaluasi risiko keamanan yang ditimbulkan oleh faktor kerentanan yang teridentifikasi. Pekerjaan analisis ini dibagi menjadi dua area, yaitu identifikasi dan validasi. Upaya penemuan kerentanan ini merupakan komponen kunci dari fase

identifikasi, sementara validasi bertujuan mengurangi jumlah banyaknya kerentanan yang teridentifikasi menjadi yang hanya valid saja.

5. *Exploitation*

Fase eksploitasi dari uji penetrasi berfokus hanya pada membangun akses pada sistem atau sumber dengan menerobos keamanan yang ada. Jika pada fase sebelumnya, yaitu fase analisis kerentanan dilakukan dengan kurang baik, maka pada fase ini harus dilakukan dengan terencana dan dengan tingkat presisi yang tinggi. Fokus utama dari fase ini adalah untuk mengidentifikasi akses masuk utama pada organisasi dan mengidentifikasi aset-aset yang berharga.

6. *Post Exploitation*

Fase *Post Exploitation* bertujuan untuk menentukan nilai dari sistem yang terekspos dan untuk menjaga kontrol sistem agar dapat terus berjalan. Nilai dari sistem akan ditentukan dari sensitivitas data yang disimpan di dalamnya dan peranan sistem tersebut di dalam jaringan yang diekspos.

7. *Reporting*

Fase *reporting* merupakan fase terakhir untuk melaporkan dan mendokumentasikan bagian-bagian penting yang terjadi selama uji penetrasi dan berguna untuk menjelaskan kepada organisasi mengenai apa saja yang dilakukan, resiko yang dapat terjadi, dan bagaimana langkah-langkah selanjutnya untuk memperbaiki sistem organisasi tersebut menjadi lebih baik.

III. HASIL DAN PEMBAHASAN

Pada bab ini akan dilakukan tahapan pengujian keamanan aplikasi *website e-learning* SMKN 1 Cibatu beserta analisisnya dengan menggunakan metode PTES dan *tools* yang berbeda di setiap fasenya.

A. *Pre-Engagement Interaction.*

Pada fase ini, kegiatan uji penetrasi dilakukan dengan terlebih dahulu mempersiapkan peralatan dan teknik, jadwal dan durasi pelaksanaan, serta melakukan wawancara kepada pihak klien terkait sistem informasi yang akan diuji [8].

1. Kuesioner

Dalam wawancara menentukan lingkup pengujian, pertanyaan yang diajukan kepada klien dilampirkan pada Tabel 1 yang menyangkut pertanyaan seputar uji penetrasi sistem informasi, Tabel 2 menyangkut pertanyaan mengenai uji penetrasi aplikasi *web*, dan Tabel 3 menyangkut pertanyaan yang ditujukan kepada admin sistem.

2. Peralatan Yang Digunakan

Peralatan atau *tools* perangkat lunak yang digunakan pada penelitian ini, yaitu :

1. Sistem operasi *KALI Linux*. Perangkat yang diturunkan dari *Debian GNU/Linux* ini khusus dikembangkan oleh *Offensive Security* sejak tahun 2013 untuk melakukan forensik digital dan uji penetrasi [13].
2. TheHarvester. Program ini digunakan untuk mengumpulkan *email*, subdomain, *host*, nama karyawan, *port* terbuka, dan spanduk dari berbagai sumber publik seperti mesin pencari, *server* kunci PGP dan *database* komputer SHODAN [14].

TABEL I. PERTANYAAN MENGENAI UJI PENETRASI SISTEM INFORMASI

No	Pertanyaan
1	Mengapa klien membutuhkan uji penetrasi terhadap sistem informasinya?
2	Pada saat kapan klien dapat mengizinkan uji penetrasi untuk dilakukan?
3	Berapa banyak alamat IP yang akan diuji?
4	Apakah ada sistem keamanan yang saat ini sudah diterapkan oleh klien yang mungkin akan berdampak pada hasil uji penetrasi?

TABEL II. PERTANYAAN MENGENAI UJI PENETRASI APLIKASI *WEB*

No	Pertanyaan
1	Berapa banyak sistem login yang akan diuji?
2	Berapa banyak halaman statik yang akan diuji?
3	Berapa banyak halaman dinamis yang akan diuji?
4	Apakah klien mengizinkan scan informasi kredensial pada aplikasi *web*?

TABEL III. PERTANYAAN KEPADA ADMIN SISTEM

No	Pertanyaan
1	Apakah ada sistem yang dapat digolongkan rentan?
2	Apakah ada sistem pada jaringan yang tidak dimiliki oleh klien dan membutuhkan persetujuan pihak ketiga terlebih dahulu sebelum diuji?
3	Apakah prosedur manajemen perubahan sudah tersedia?
4	Berapa lama waktu yang biasa dibutuhkan untuk memperbaiki kerusakan sistem?

3. Nessus *Vulnerability Scanner*. Perangkat lunak yang digunakan untuk memindai kerentanan suatu sistem yang dikembangkan oleh Tenable, Inc. Pemindaian mencakup berbagai teknologi termasuk sistem operasi, perangkat jaringan, *hypervisor*, basis data, *web server*, dan infrastruktur lainnya [15].
4. NMAP (*Network Mapper*). Sebuah utilitas *open source* yang digunakan untuk melakukan pemindaian *port* dan enumerasi atau mengumpulkan informasi berharga dari target

hacking. *Tools* ini dapat dijalankan di multi *platform* seperti Windows, Linux, MAC OS, dan varian UNIX [16].

5. *Wireshark*. Program ini merupakan perangkat lunak yang digunakan untuk menganalisis protokol jaringan yang paling terkemuka dan banyak digunakan di dunia [17].
6. OWASP *Zed Attack Proxy* (ZAP). Perangkat lunak ini merupakan aplikasi pemindai keamanan *web* yang banyak digunakan di seluruh dunia dan secara aktif dikembangkan oleh banyak relawan profesional secara *dedicated* [18].

3. Jadwal Pengujian

Pengujian penetrasi sistem informasi SMKN 1 Cibatu dilakukan pada tanggal 25 September sampai dengan tanggal 10 Oktober 2020 dan dilakukan di luar jam operasional sekolah.

B. Intelligence Gathering

Tahap pengujian dilakukan terhadap *website e-learning* milik SMKN 1 Cibatu. Hasil pengujian terhadap target dengan nama domain belajar.smkn1cibatu.sch.id mendapatkan informasi yang dapat dilihat pada Tabel 4.

TABEL IV. HASIL PENGUJIAN *INTELLIGENCE GATHERING*

Parameter Pengujian	Informasi yang diperoleh
Alamat IP domain belajar.smkn1cibatu.sch.id	46.17.173.126
Port yang aktif atau statusnya *open*.	TCP Port 21, 53, 80, 110, 143, 443, 465, 587, 993, 3306
Sistem operasi yang digunakan.	OpenBSD 4.x
Service atau protokol yang berjalan.	FTP, DNS, HTTP, IMAP, POP3, SMTP, dan MYSQL
Masa berlaku domain	hingga 28 Nov 2020
DNS *Server* yang digunakan	ns1.niagahoster.com dan ns2.niagahoster.com
Web platform yang digunakan	Moodle
Alamat sekolah SMKN 1 Cibatu	Jln. Raya Sadang-Subang KM 15, Desa Cipinang Kec. Cibatu, Purwakarta
Email yang dapat dihubungi	info@smkn1cibatu.sch.id
Sistem proteksi *website*	Imunify360

Tahap pengumpulan data intelijen mengenai target, yaitu aplikasi *website e-learning* SMKN 1 Cibatu dilakukan melalui *Open Source Intelligence* (OSINT), *Footprinting*, dan Identifikasi Mekanisme Proteksi.

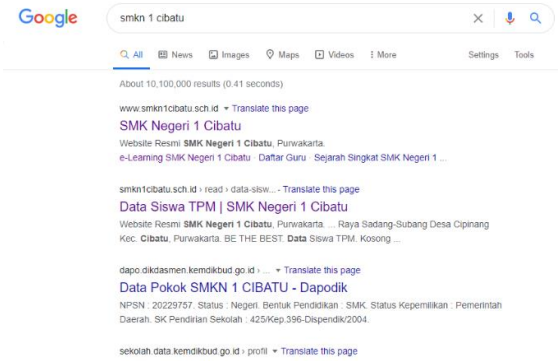
1. Open Source Intelligence (OSINT)

Pengumpulan data intelijen *open source* dilakukan menggunakan *Google Search* pada Gambar 2 yaitu mencakup pengumpulan informasi *website* sekolah seperti yang ditunjukkan pada Gambar 3, data lokasi fisik sekolah, kerjasama pihak sekolah dengan lingkungan eksternal, hubungan kemasyarakatan sekolah, jumlah murid aktif, dan calon pendaftar [9].

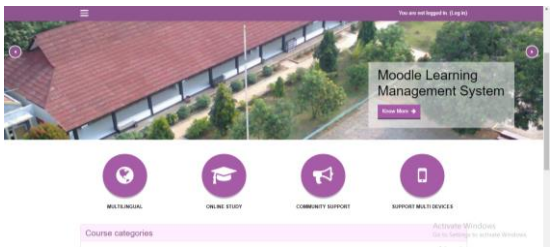
2. Footprinting

Pengumpulan data secara eksternal dengan melakukan pelacakan informasi menggunakan *tools* theHarvester, WHOIS, dan NMAP.

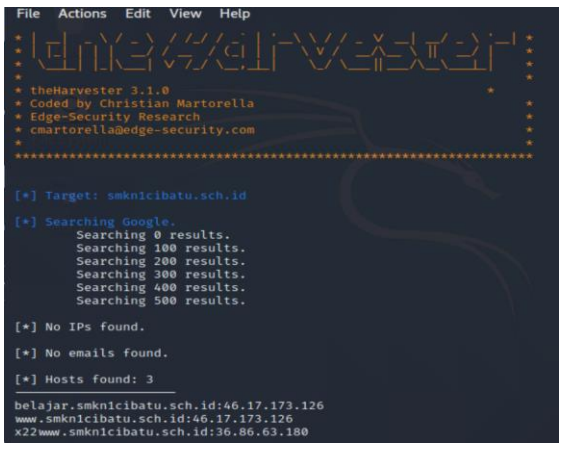
Hasil pengujian dengan menggunakan *tools theHarvester* seperti yang ditunjukkan pada Gambar 4, didapatkan informasi *host* sebanyak 3 (tiga) *hostname* dengan dua diantaranya merupakan domain *web* aplikasi yang dimiliki SMKN 1 Cibatu.



Gambar 2. Hasil Pencarian Data SMKN 1 Cibatu



Gambar 3. Tampilan Muka *Website E-Learning* SMKN 1 Cibatu

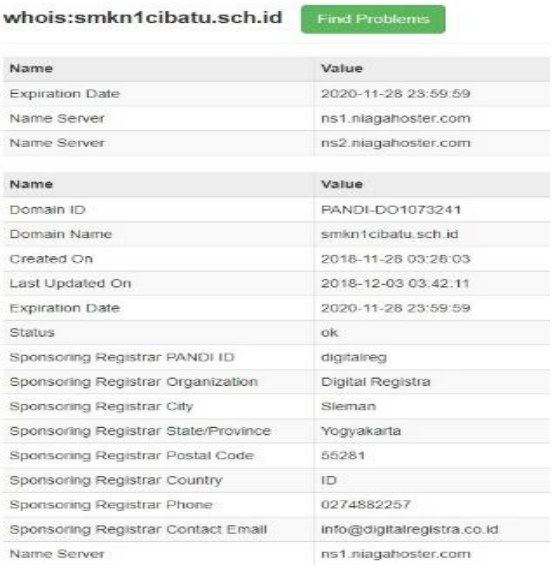


Gambar 4. Hasil Pelacakan *TheHarvester*

Hasil pengujian menggunakan WHOIS terhadap target domain yang telah ditentukan didapatkan berbagai informasi terkait pendaftaran nama domain, masa berlakunya, serta DNS *server* yang digunakan seperti yang ditunjukkan pada Gambar 5.

Hasil pengujian menggunakan NMAP didapatkan informasi penting mengenai *port* apa saja yang statusnya aktif atau *open* dan *banner* yang berisi informasi mengenai jenis *engine* atau *platform* yang digunakan untuk setiap *port service* yang digunakan seperti yang ditunjukkan pada Gambar 6.

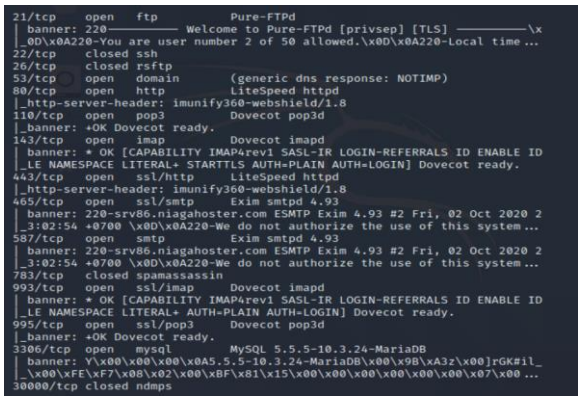
Hasil pengujian menggunakan NMAP juga didapatkan informasi mengenai sistem operasi yang digunakan pada *web server* seperti dapat dilihat pada Gambar 7.


whois:smkn1cibatu.sch.id Find Problems

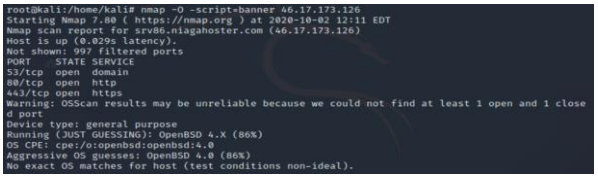
Name	Value
Expiration Date	2020-11-28 23:59:59
Name Server	ns1.niagahoster.com
Name Server	ns2.niagahoster.com

Name	Value
Domain ID	PANDI-DO1073241
Domain Name	smkn1cibatu.sch.id
Created On	2018-11-28 03:28:03
Last Updated On	2018-12-03 03:42:11
Expiration Date	2020-11-28 23:59:59
Status	ok
Sponsoring Registrar PANDI ID	digitalreg
Sponsoring Registrar Organization	Digital Registra
Sponsoring Registrar City	Sleman
Sponsoring Registrar State/Province	Yogyakarta
Sponsoring Registrar Postal Code	55281
Sponsoring Registrar Country	ID
Sponsoring Registrar Phone	0274882257
Sponsoring Registrar Contact Email	info@digitalregistra.co.id
Name Server	ns1.niagahoster.com

Gambar 5. Hasil Pelacakan WHOIS



Gambar 6. Hasil *Port Scanning* dan *Banner Grabbing* NMAP



Gambar 7. Hasil OS *Fingerprinting* NMAP

3. Identifikasi Mekanisme Proteksi

Pada tahap ini dilakukan pengumpulan informasi mengenai jenis perlindungan keamanan yang dimiliki oleh SMKN 1 Cibatu. Berdasarkan hasil pengujian yang telah dilakukan dan informasi yang didapatkan pada fase sebelumnya bahwa aplikasi *web* SMKN 1 Cibatu menggunakan layanan sewa *hosting* yang telah dilengkapi dengan fitur pengamanan yaitu dengan mengimplementasikan Imunify360 seperti dapat dilihat pada Gambar 8.

Imunify360 diketahui sebagai *tool* keamanan yang dapat melindungi server *web* hosting dengan fitur antara lain: *advanced firewall, malware detection, intrusion detection and protection system, proactive defense, patch management, reputation management* dan notifikasi serangan *malware*.

Gambar 8. Proteksi Imunify360

C. *Threat Modelling*

Pada fase *Threat Modelling*, dilakukan pemodelan bentuk ancaman yang berfokus pada dua elemen utama, yaitu aset (aset bisnis dan proses bisnis) dan penyerang (komunitas ancaman dan kapabilitas).

1. Analisis Aset

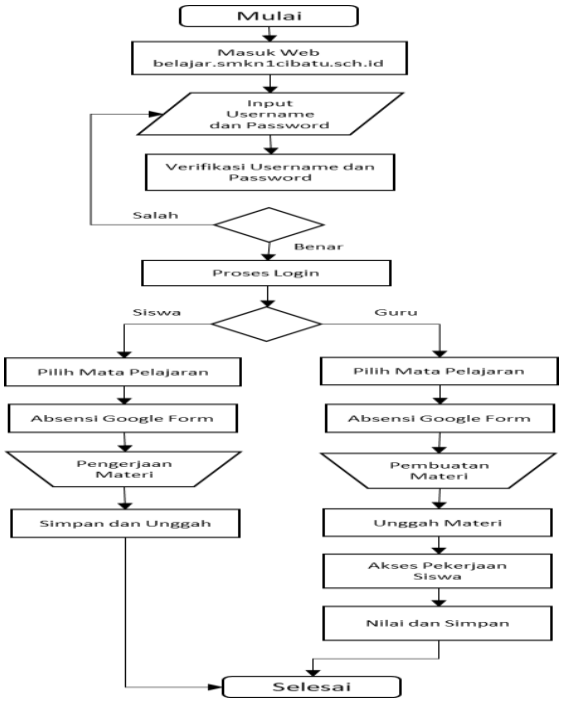
Analisis data dan informasi yang merupakan aset bisnis berharga pada *website e-learning* SMKN 1 Cibatu dan diuraikan pada Tabel 5.

TABEL V. ANALISIS DATA *WEBSITE E-LEARNING*

No	Nama Aset	Jenis Data	Tingkat Kerahasiaan
1	Data Siswa	Nama	Rendah
		Nomor Siswa	Rendah
		Data Nilai	Tinggi
		Alamat *Email*	Sedang
2	Data Guru	Nama	Rendah
		NIP	Sedang
		Alamat *Email*	Sedang
3	Data *Login*	*Username*	Sedang
		Password	Tinggi

2. Alur Proses SMKN 1 Cibatu

Proses penggunaan *website e-learning* SMKN 1 Cibatu mengikuti alur seperti yang ditunjukkan pada gambar 9. *Website e-learning* SMKN 1 Cibatu dapat diakses baik oleh guru maupun murid sekolah SMKN 1 Cibatu. Dengan menggunakan username masing-masing yang telah ditentukan, sesi akan dibagi menjadi dua, yaitu sesi murid dan sesi guru. Guru dapat mengakses dan melakukan perubahan isi form pada materi pelajaran, sementara murid mengakses isinya dan dapat mengunggah hasil pekerjaan pada *website.*



Gambar 9. Alur Proses *Website E-Learning*

3. Analisis *Threat Community*

Analisis dilakukan pada komunitas ancaman yang berpotensi melakukan tindakan peretasan *website* dan ditunjukkan pada Tabel 6.

TABEL VI. ANALISIS KOMUNITAS ANCAMAN

No	Jenis Komunitas	Tingkat Risiko
1	Internal Sekolah	Rendah
2	Eksternal Sekolah	Tinggi

4. Matriks Identifikasi Risiko Ancaman

Berdasarkan hasil analisis aset, proses bisnis dan komunitas ancaman maka jenis ancaman dapat dimodelkan seperti pada Tabel 7.

TABEL VII. HASIL ANALISIS RISIKO ANCAMAN

No	Nama Aset	Potensi Jenis Ancaman	Tingkat Risiko
1	Data Siswa	*SQL Injection*	Sedang
2	Data Guru	*SQL Injection*	Sedang
3	Data Nilai	*SQL Injection*	Tinggi
4	Aplikasi *Web*	*Defacement, XSS Attack, CSRF Attack, Brute Force*	Tinggi
5	Jaringan dan Server	*Denial of Service, Eavesdropping.*	Tinggi

D. *Vulnerability Analysis*

Pada fase ini dilakukan analisis kerentanan dari sistem informasi yang dimiliki oleh SMKN 1 Cibatu dengan menggunakan beberapa *tools* antara lain Nesus VS, Pentesting Online (pentest-tools.com) dan OWASP ZAP.

1. Nessus *Vulnerability Scanner*

Hasil analisis kerentanan menggunakan Nessus yaitu ditemukan celah keamanan pada *website e-learning* SMKN 1 Cibatu seperti yang dapat dilihat pada Gambar 10.

Gambar 10. Hasil Analisis Kerentanan Oleh Nessus Pada *Website E-Learning* SMKN 1 Cibatu

Jenis kerentanan *website e-learning* yang ditemukan menggunakan *Nessus* dapat dilihat pada Tabel 8.

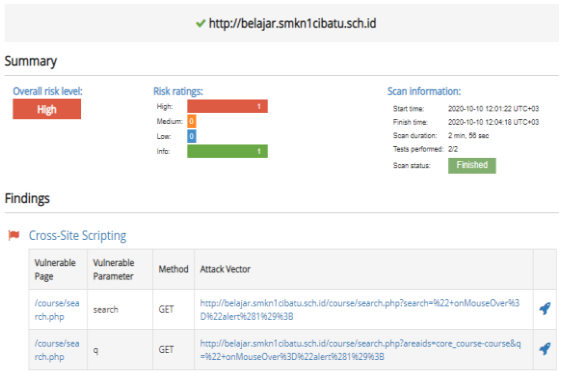
TABEL VIII. HASIL TEMUAN KERENTANAN MENGGUNAKAN NESSUS

Vulnerable	*Description*	*Severity*
Web Server Transmits Cleartext Credentials	*An attacker eavesdropping the traffic between web browser and server may obtain logins and*	*High*

Vulnerable	*Description*	*Severity*
	passwords of valid users.	
Web Application Potentially Vulnerable to Clickjacking	*The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses.*	*Medium*
PHP 7.4.x < 7.4.10 Memory Leak Vulnerability	*According to its self-reported version number, the version of PHP running on the remote web server is 7.4.x prior to 7.4.10.*	*Medium*
PHP 7.4.x < 7.4.9 Use-After-Free Vulnerability	*According to its self-reported version number, the version of PHP running on the remote web server is 7.4.x prior to 7.4.9.*	*Low*

2. *Pentesting Online* (pentest-tools.com)

Hasil analisis kerentanan menggunakan *Pentesting Online* yaitu ditemukan celah keamanan pada *website e-learning* SMKN 1 Cibatu seperti yang dilihat pada Gambar 11.



Gambar 11. Hasil Analisis Kerentanan Oleh Pentesting Online Pada *Website E-Learning* SMKN 1 Cibatu

Jenis kerentanan *website e-learning* yang ditemukan menggunakan *Pentesting Online* dapat dilihat pada Tabel 9.

TABEL IX. HASIL TEMUAN KERENTANAN MENGGUNAKAN *PENTESTING ONLINE* (PENTEST-TOOLS.COM)

Vulnerable Page	*Vulnerable Parameter*	*Method*	*Severity*
Cross-Site Scripting (XSS)	*search*	GET	*High*
Cross-Site Scripting (XSS)	q	GET	*High*

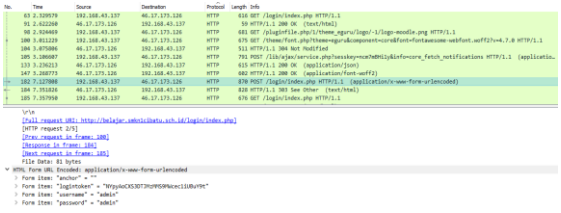
E. *Exploitation*

Pada fase ini akan dilakukan pengujian celah keamanan *website e-learning* SMKN 1 Cibatu yang ditemukan pada fase *Vulnerability Analysis* dengan menggunakan *tools* yang telah ditentukan.

1. *Eavesdropping*

Pengujian terhadap kelemahan pada *web server* ketika mentransmisikan informasi kepada klien tanpa menggunakan protokol yang aman menggunakan *tools* Wireshark.

Hasil dari proses *sniffing* seperti yang terlihat pada Gambar 12, didapatkan informasi nama pengguna dan kata sandi ketika pengguna memasukkan kredensial di form *login* aplikasi *website e-learning*. Kelemahan penggunaan protokol HTTP pada *website* menjadi celah yang dapat dimanfaatkan penyerang untuk mendapatkan informasi penting.



Gambar 12. *Sniffing* Menggunakan *Wireshark*

2. *Cross-Site Scripting* (XSS)

Pengujian eksploitasi yang ditemukan dengan mencari kerentanan terhadap serangan *Cross Site Scripting* (XSS) dengan menggunakan bantuan *tools online* yaitu pentest-tools.com. Terdapat dua vektor serangan terhadap *vulnerable page* yang ditemukan, salah satunya seperti ditunjukkan pada Gambar 13.

Gambar 13. Pengujian Kerentanan XSS

3. *Cross-Site Request Forgery (CSRF)*

Pengujian exploitasi menggunakan *tools* OWASP ZAP menemukan adanya celah keamanan terhadap serangan *Cross-site Request Forgery* (CSRF) seperti ditunjukkan pada Gambar 14.

Gambar 14. Pengujian Kerentanan CSRF

Tingkat risiko masuk ke dalam kategori *Low* dengan bukti atau *evidence* pada *form action* http://belajar.smkn1cibatu.sch.id/course.php dengan metode GET, dimana metode ini akan menampilkan data/nilai pada URL, kemudian akan ditampung oleh *action.* Permasalahan adalah ketika informasi yang ditampikan bersifat rahasia.

F. Post Exploitation

Pada tahap ini dilakukan penilaian profil risiko terhadap sistem yang memiliki celah keamanan setelah dilakukan pengujian pada fase sebelumnya. Terdapat 3 (tiga) jenis serangan atau ancaman yang berhasil diuji terhadap sistem aplikasi *website e-learning* SMKN 1 Cibatu seperti yang dapat dilihat pada Tabel 10.

TABEL X. PENILAIAN RISIKO TERHADAP CELAH KEAMANAN YANG DITEMUKAN

No	Nama Aset	Celah Keamanan	Profil Risiko
1	Aplikasi *Web*	*XSS Attack, CSRF Attack.*	Tinggi
2	Jaringan dan Server	*Eavesdropping.*	Tinggi

Berdasarkan hasil pengujian, maka terdapat celah keamanan yang memiliki profil risiko tinggi. Untuk aplikasi web, celah keamanan berupa serangan *Cross Site Scripting* (XSS), dan serangan *Cross Site Request Forgery* (CSRF). Serangan XSS dan CSRF memiliki potensi ancaman yang tinggi terhadap perubahan atau modifikasi data (integrasi data). Kemudian untuk aset jaringan dan server, memiliki celah keamanan berupa serangan *eavesdropping* yang memiliki potensi ancaman yang tinggi terhadap pencurian akun pengguna.

G. Reporting

Dari seluruh tahap pengujian yang telah dilakukan, maka penulis dapat menyimpulkan hasil pengujian menggunakan metode *Penetration Testing Execution Standard* (PTES) pada aplikasi *website* SMKN 1 Cibatu yang ditunjukkan sebagai hasil laporan pengujian keamanan pada Tabel 11.

TABEL XI. HASIL PENGUJIAN *PENETRATION TESTING*

Jenis Serangan	Tools	Status
Eavesdropping	Wireshark	Berhasil
SQL *Injection*	SQLMap	Gagal
Cross-site Scripting (XSS)	Pentest-tools.com	Berhasil
Cross-site Request Forgery (CSRF)	OWASP ZAP	Berhasil

Dari empat tipe serangan yang diketahui dari tahap *post exploitation*, terdapat tiga serangan yang berhasil dieksploitasi yaitu *Eavesdropping, Cross-Site Scripting*, dan *Cross Site Request Forgery*. Sementara itu, SQL Injection mengalami kegagalan karena hosting yang digunakan oleh sistem memiliki sistem keamanan yaitu proteksi Immunify360 yang dapat mendeteksi perintah SQL Map.

Berdasarkan hasil pengujian keamanan tersebut, maka rekomendasi perbaikan dari temuan celah keamanan pada *website e-learning* SMKN 1 Cibatu dapat dirangkum seperti pada Tabel 12.

TABEL XII. SOLUSI DAN REKOMENDASI PERBAIKAN

Celah Keamanan	Solusi
Web Server Transmits Cleartext Credentials	Pastikan setiap konten penting seperti kredensial pada form login dapat ditransmisikan menggunakan protocol HTTPS (*Hypertext Transfer Protocol Secure*)
Cross-Site Scripting (XSS)	Penggunaan mekanisme terstruktur yang secara otomatis memaksakan pemisahan antara data dan kode.
Cross-Site Request Forgery (CSRF)	Hindari penggunaan metode GET untuk permintaan apa pun yang dapat memicu perubahan status.

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian ini. dapat disimpulkan bahwa analisis kerentanan aplikasi *website* milik SMKN 1 Cibatu dengan menggunakan metode PTES (*Penetration Testing Execution Standard*) mampu mengetahui tingkat kerentanan sistem informasi dengan risiko serangan yang paling tinggi seperti *Cross Site Scripting*, *Cross Site Request Forgery* dan *Eavesdropping* yang sangat berpotensi mengakibatkan kebocoran data penting. Melalui tahapan pengujian keamanan yang telah dilakukan, maka metode PTES dinilai dapat dijadikan sebagai standar penilaian keamanan aplikasi berbasis *web* pada *website e-learning* di alamat belajar.smkn1cibatu.sch.id yaitu mulai dari tahap *pre-engagement interactions* hingga *reporting.*

Untuk pengembangan lebih lanjut maka penulis memberikan saran di antaranya adalah: (1) Perlu menguasai dan mendalami teknik-teknik lainnya dalam pengujian fase eksploitasi agar hasil yang didapat lebih akurat. (2) Perlunya pembahasan mengenai potensi suatu kerentanan yang dapat berakibat terjadinya kerentanan yang lain. (3) Perlu dilakukan penelitian lebih lanjut dengan menggunakan metode yang berbeda seperti ISSAF (*Information System Security Assesment Framework*) atau OWASP (*The Open Web Application Security Project*) untuk dapat diketahui kerentanan lainnya dari sisi *web server*

REFERENSI

[1] P. Agus, "Pengembangan Aplikasi E-Learning Sekolah Menengah Atas," *J. Simetris*, vol. 8, no. 2, pp. 619–628, 2017.

[2] W. R. Septian, "Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK," *J. Multinetics*, vol. 3, no. 2, pp. 32–37, 2017.
[3] W. R. Septian, "Desain Algoritma Steganografi dengan Metode Spread Desain dan Analisa Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK (Permutasi Chaotic Multiputaran Mengecil dan Membesar) Menggunakan Matlab," *J. Elektra*, vol. 3, no. 1, pp. 37–46, 2018.
[4] W. R. & A. Septian, "Analisis Upaya Peretasan Web Application Firewall dan Notifikasi Serangan Menggunakan Bot Telegram pada Layanan Web Server," *J. Elektra*, vol. 3, no. 2, pp. 19–28, 2018.
[5] Y. Moh, "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework OWASP Versi 4," *J. Ilm. Inform. Komput.*, vol. 24, no. 1, pp. 37–48, 2019.
[6] S. S. A. Gede, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *J. Ilm. Merpati*, vol. 8, no. 2, pp. 113–124, 2020.
[7] C. S. D. Bruno, "Using PTES and Open Source Tools as a Way to Conduct External Footprinting Security Assessments for Intelligence Gathering," *J. Internet Technol. Secur. Trans.*, vol. 3, no. 3, 2014.
[8] P. W. Cunong, Denis Nigel, Muhardi Saputra, "Analisis Risiko Keamanan Terhadap Website Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Pemerintahan XYZYZ Menggunakan Standar Penetration Testing Execution Standard (PTES)," *E-Proceeding Eng.*, vol. 7, no. 1, 2020.
[9] N. Yoel, "Analisis Keamanan Jaringan Pada Layanan Internet Publik Menggunakan Metode Penetration Testing Execution Standard (PTES) (Studi Kasus : Klinik Pratama Bhakti Medika)," 2020.
[10] P. Team, "PTES Technical Guidelines," 2020.
[11] D. Mohanty, "Demystifying Penetration Testing HackingSpirits," 2020. .
[12] A. G. Bacudio, "An Overview of Penetration Testing," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 6, 2011.
[13] KALI, "KALI Linux," 2020.
[14] TheHarvester, "About The Harvester," 2020.
[15] T. Nessus, "About Nessus Professional," 2020.
[16] NMAP, "About Network Mapper," 2020.
[17] Wireshark, "About Wireshark," 2020.
[18] O. Z. P. Attack, "About OWASP ZAP," 2020.