ANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK DENGAN *WEB PENETRAION TESTING*

Oleh:
Aufan Imron Rosadi
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul
Email: aufanimron@gmail.com
Pembimbing I: Ari Pambudi, S.Kom, M.Kom
Pembimbing II: Nugroho Budhisantosa, S.T, MMSI

Abstrak – Universitas XYZ merupakan Universitas yang melakukan pertukaran informasi melalui sistem berbasis *web*. Mengingat *website* ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan *website*. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap kemanan *website*. Salah satunya adalah dengan melakukan *Web Penetration Testing.* Alasan dilakukannya penelitian ini adalah karena peneliti mendengar dari beberapa sumber baik dosen maupun temen mahasiswa, bahwa sistem informasi akademik yang dimiliki oleh Universitas XYZ tidaklah aman atau dapat di *hacking* atau dijebol sewaktu – waktu. Alasan lain mengapa dilakukannya penelitian ini adalah untuk mengetahui pula seberapa tingginya tingkat keamanan sistem informasi akademik yang ada di Universitas XYZ. Dari penelitian diatas, peneliti dapat menarik kesimpulan bahwa untuk jenis serangan *sql injection* yang dilakukan terhadap target yaitu sistem informasi akademik Universitas XYZ, sistem tersebut telah AMAN. Perlu digaris bawahi kembali peneliti dapat menyimpulkan sistem telah aman HANYA UNTUK JENIS SERANGAN *SQL INJECTION*. Untuk jenis serangan yang lainnya, peneliti dapat menyimpulkan bahwa sistem target BELUM AMAN.

Kata kunci: Universitas XYZ, *web penetration testing*

Abstract *– XYZ University is a University that conducts information flow through a web-based system. Given this website can be accessed widely, it needs to be respected website security. There are several ways you can test your security site. One of them is by doing Web Penetration Test. The reason of this research is because researchers from several sources both lecturers and students, namely academic information owned by XYZ University safe or can be hacked or uprooted at any time. Another reason why this research is to know also the quality of information available at XYZ University. From the above research, researchers can draw conclusions for the type of sql injection attacks conducted against the target of academic information system XYZ University, this system has been SAFE. It should be underlined again the directors can ONLY FOR TYPE OF SQL INJECTION ATTACKS. For other types of attacks, researchers can be divided target system is NOT SAFE.*

Keywords: XYZ University, web penetration testing

Latar Belakang

Perkembangan dunia teknologi yang semakin canggih membuat pekerjaan berjalan dengan sangat mudah dan cepat. Kemudahan yang ditawarkan teknologi tentunya beriringan dengan bahaya yang dapat disisipkan melalui berbagai hal. Terlebih lagi, jika bahaya tersebut tersistem sehingga membuat pengguna tidak menyadari dengan adanya bahaya yang sudah masuk dan mengintainya. Selain itu, *human behavior* dari mahasiswa maupun karyawan ini sendiri juga perlu dilihat mengingat bahwa pelaku *hacking* ini adalah orang dalam itu sendiri. Terkadang, *human behavior* yang kurang baik ini dapat membawa dampak buruk baik secara langsung maupun tidak langsung.

Dengan semakin majunya ilmu dan teknologi, semakin banyak pula masyarakat yang bergantung pada teknologi tersebut, terutama dalam hal yang berhubungan dengan internet. “Perkembangan dan evolusi dari komputer, internet dan teknologi *web* telah membuat masyarakat lebih bergantung pada layanan jaringan komputer lebih dari sebelumnya” (Shrestha, 2012). Hal ini dapat dilihat dengan semakin banyaknya jumlah pengguna media sosial dan layanan internet yang ada saat ini. Dari hasil laporan Asosiasi Penyelanggara Jasa Internet Indonesia (APJII) pada tahun 2012 menunjukkan sudah terdapat

63 juta pengguna internet di seluruh Indonesia yang mana meningkat sekitar 24,23% dari tahun sebelumnya (Asosiasi Penyelenggara Jasa Internet Indonesia, 2012). Pengguna internet di Indonesia diperkirakan masih akan terus meningkat hingga mencapai 123 juta orang pada tahun 2018 (Emarketer, 2014).

Di seluruh dunia terdapat sekitar 640 *Terabytes* data *transfer* dan 204 juta *email* dikirim melalui jaringan internet setiap menitnya (Rick, 2013). Informasi sendiri menjadi hal penting di era digital ini baik untuk setiap individu ataupun organisasi. Semakin banyak individu yang peduli dengan bagaimana informasi pribadi mereka digunakan dan semakin banyak pula organisasi yang sadar bahwa resiko keamanan informasi dapat memberi dampak buruk pada keberlangsungan proses bisnis, citra publik, relasi, menyebabkan kerugian materil, mempengaruhi hubungan dengan pelanggan atau mitra dan juga dapat menyebabkan masalah dengan pihak berwajib. Oleh karena itu untuk melindungi informasi yang ada diperlukan sistem yang baik.

Sistem dapat didefinisikan sebagai seperangkat komponen (sumber daya) terkait, dengan batas yang jelas dan bekerjasama untuk mencapai tujuan tertentu melalui sebuah inputan dalam proses transfromasi yang teroganisir (Brien dan Marakas, 2010). Sedangkan Sistem Informasi lebih menekankan pada pengelolaan sumber daya (*resource*) yang ada menjadi produk informasi. Jadi, sistem informasi akademik adalah sebuah sistem khusus untuk keperluan pengeloaan data-data akademik dengan penerapan teknologi komputer baik *hardware* maupun *software*.

Universitas XYZ merupakan salah satu universitas dengan jumlah civitas akademik yang banyak. Hal tersebut tentunya mengakibatkan banyaknya informasi yang dipertukarkan dalam organisasi ini. Pertukaran informasi menggunakan jaringan komputer sebagai medianya dimana informasi tersebut dapat berupa informasi penting atau pribadi dimana hak aksesnya hanya diperuntukkan untuk orang-orang tertentu. Mengingat *website* ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan *website*. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap kemanan *website*. Salah satunya adalah dengan melakukan *Web Penetration Testing*.

Berdasarkan definisi dalam modul CEH, *Web Penetration Testing* merupakan metode evaluasi keamanan sistem komputer atau dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari *security audit*. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh *black hat hacker*, *cracker*, dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin dilakukan pada sistem beserta akibat yang bisa terjadi karena kelemahan sistem. Dalam melakukan *penetration testing*, diperlukan analisa intensif untuk setiap kerentanan yang diakibatkan oleh kelemahan sistem. Uji penetrasi dalam penelitian ini akan menggunakan *Kali Linux*. *Kali Linux* menggabungkan lebih dari 300 *tools* untuk uji penetrasi dan audit keamanan dengan sistem operasi *Linux*, memberikan sebuah solusi yang memungkinkan *administrator IT* dan profesional keamanan untuk menguji efektivitas keamanan sistem.

Alasan dilakukannya penelitian ini adalah karena peneliti mendengar dari beberapa sumber baik dosen maupun temen mahasiswa, bahwa sistem informasi akademik yang dimiliki oleh Universitas XYZ tidaklah aman atau dapat di *hacking* atau di jebol sewaktu – waktu. Alasan lain mengapa dilakukannya penelitian ini adalah untuk mengetahui pula seberapa tingginya tingkat keamanan sistem informasi akademik yang ada di Universitas XYZ. Oleh karena itu, prioritas utama kebutuhan yang penting saat ini adalah membantu meminimalisir dan mengantisipasi para *hacker* yang ada dari kejahatan *hacking*. Salah satu hal yang dapat dilakukan adalah dengan melakukan uji *Penetration* (*Web Penetration Testing*). Dari hasil pengujian ini, laporan atau hasilnya akan diberikan kepada pihak *administrator IT* agar pengembangan terhadap keamanan sistem bisa dapat dipertahankan atau ditingkatkan kembali.

Tujuan Penelitian

Adapun tujuan dari penelitian pengujian tingkat keamanan sistem informasi akademik di Universitas XYZ ini adalah sebagai berikut:

1. Untuk mengetahui tingkat keamanan sistem informasi akademik yang ada di Universitas XYZ.
2. Untuk mengetahui hasil dari pengujian tingkat keamanan sistem informasi akademik di Universitas XYZ.
3. Untuk mengetahui solusi atau saran dari kerentanan yang dapat ditembus selama proses pengujian.

Batasan Masalah

Batasan masalah pada penelitian tingkat keamanan sistem informasi akademik di Universitas XYZ adalah sebagai berikut:

1. Penelitian ini hanya untuk menguji tingkat keamanan sistem informasi akademik yang ada di Universitas XYZ.
2. Hanya menggunakan metode *black – hat* yaitu metode *penetration testing* yang serupa dengan yang dilakukan aslinya karena peneliti hanya diberikan nama perusahaan saja dan informasi mengenai jaringan maupun informasi lainnya harus dicari sendiri oleh peneliti.
3. Uji coba yang digunakan pada penelitian ini adalah menggunakan uji coba non destruktif, yaitu uji coba yang tidak membuat kerusakan sistem.
4. Metodologi *penetration testing* yang digunakan hanya menggunakan metode *Information Systems Security Assessment Framework (*ISSAF*) penetration testing*.
5. Pada tahapan penetrasi, serangan yang dilakukan hanya untuk mengetahui informasi *database* yang digunakan, tidak merubah atau mengambil data – data yang ada dalam *database* tersebut. Serangan ini biasa disebut dengan *sql injection*.

Manfaat

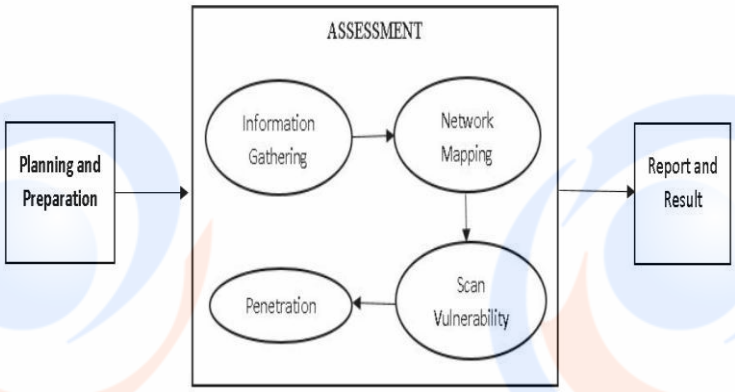
Manfaat yang diperoleh dari penelitian pengujian tingkat keamanan sistem informasi akademik di Universitas XYZ ini adalah dapat mengembangkan dan meningkatkan keamanan sistem informasi akademik yang dimiliki oleh Universitas XYZ sehingga kegiatan civitas akademika tetap terjaga kerahasiaan datanya.

Metodologi

Berikut penjelasan mengenai langkah – langkah yang digunakan (metodologi) oleh peneliti:

1. Perumusan Masalah: merupakan tahapan awal dari penelitian ini. Masalah yang dirumuskan adalah Bagaimana menganalisis tingkat keamanan sistem informasi akademik di Universitas XYZ dengan menggunakan metode *Web Penetration Testing* dan Bagaimana hasil dari pengujian tingkat keamanan sistem informasi akademik di Universitas XYZ dengan *Web Penetration Testing.*
2. Studi Pustaka: mencari pengetahuan dasar yang didapat dari buku, jurnal, artikel, internet, karya ilmiah dan media lainnya untuk melengkapi landasan teori dan sebagai acuan dasar dalam menyelesaikan penelitian ini.
3. Metode Pentest: pada tahapan ini dilakukan pengujian penetrasi tingkat keamanan sistem informasi akademik yang dimiliki oleh Universitas XYZ dengan *web penetration testing* dengan metode pentest yang biasa digunakan. Untuk metode pentest biasanya terdiri dari 3 tahapan yaitu *planning and preparation, assessment, report and result*. Untuk tahapan *assessment* terdiri dari *information gathering, network mapping, vulnerability scanning, penetration*. Penetrasi menggunakan teknik serangan yang hanya untuk mengetahui informasi *database* yang dimiliki oleh sistem tersebut. Jenis serangan ini biasa disebut *SQL injection*. Adapun *tools* pendukung yang digunakan dalam metode tersebut antara lain *who is, SSL scan, nmap, zenmap, SQLmap, havij, skipfish, httrack, vega, maltego, owasp zap*. Berikut dibawah ini merupakan gambar keterkaitan metode pentest

Gambar 1: Metode *Pentest*



4. Dokumentasi dan Laporan: pada tahapan dokumentasi dan pembuatan laporan merupakan tahapan dimana peneliti memaparkan hasil penelitian yang dilakukan dari tahap awal hingga akhir dan diimplementasikan kedalam bentuk skipsi atau proposal tugas akhir. Laporan hasil penelitian diserahkan ke 5 penerima yaitu bagian penanggung jawab IT, dosen pembimbing selama penelitian, dosen penguji ketika sidang, perpustakaan dan fakultas yang bersangkutan.

Landasan Teori

Pengertian Analisis

Analisis adalah aktivitas yang memuat sejumlah kegiatan seperti mengurai, membedakan, memilah sesuatu untuk digolongkan dan dikelompokkan kembali menurut kriteria tertentu kemudian dicari kaitannya dan ditafsirkan maknanya. Dalam pengertian yang lain, analisis adalah sikap atau perhatian terhadap sesuatu (benda, fakta, fenomena) sampai mampu menguraikan menjadi bagian – bagian, serta mengenal kaitan antarbagian tersebut dalam keseluruhan. Analisis dapat juga diartikan sebagai kemampuan memecahkan atau menguraikan suatu materi atau informasi menjadi komponen-komponen yang lebih kecil sehingga lebih mudah dipahami. Berikut beberapa pengertian analisis menurut para ahli:

a. Kamus Besar Bahasa Indonesia: penguraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan.
b. Anne Gregory: langkah pertama dari proses perencanaan.
c. Dwi Prastowo Darminto & Rifka Julianty: penguraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri, serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan.
d. Syahrul & Mohammad Afdi Nizar: melakukan evaluasi terhadap kondisi dari pos-pos atau ayat-ayat yang berkaitan dengan akuntansi dan alasan-alasan yang memungkinkan tentang perbedaan yang muncul.
e. Wiradi: aktivitas yang memuat sejumlah kegiatan seperti mengurai, membedakan, memilah sesuatu untuk digolongkan dan dikelompokkan kembali menurut kriteria tertentu kemudian dicari kaitannya dan ditaksir maknanya.
f. Kamus akuntansi: melakukan evaluasi terhadap kondisi dari pos-pos atau ayat – ayat yang berkaitan dengan akuntansi dan alasan-alasan yang memungkinkan tentang perbedaan yang muncul.
g. Komaruddin: kegiatan berfikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu.

Jadi, dari pengertian analisis diatas, dapat disimpulkan bahwa analisis adalah sekumpulan aktivitas dan proses. Salah satu bentuk analisis adalah merangkum sejumlah besar data yang masih mentah menjadi informasi yang dapat diinterpretasikan. Semua bentuk

analisis berusaha menggambarkan pola-pola secara konsisten dalam data sehingga hasilnya dapat dipelajari dan diterjemahkan dengan cara yang singkat dan penuh arti.

Sistem Informasi Akademik

Sistem informasi akademik adalah sebuah sistem khusus untuk keperluan pengeloaan data – data akademik dengan penerapan teknologi komputer baik hardware maupun software. Yang dimaksud hardware (perangkat keras) adalah peralatan-peralatan seperti komputer (PC computer), printer, CD ROM, hardisk, dan sebagainya. Sedang Software (perangkat lunak) merupakan program komputer yang memfungsikan hardware tersebut yang dibuat khusus untuk keperluan pengelolaan data – data akademik diatas. Hardware komputer yang akan digunakan dapat dijumpai (dibeli) di pasaran, di tempat – tempat penjualan komputer. Sedang software, harus dibuat dengan teknik pemrograman tertentu. Data yang dikelola adalah data mahasiswa, data dosen, data mata kuliah, data nilai akademik, data Alumni, data Keuangan dan sebagainya. Bagian-bagian sistem antara lain:

a. *Administrator*, yaitu orang yang sangat mengetahui kerja sistem secara keseluruhan, bertanggung jawab atas keberjalanan sistem, pengatur sistem keamanan dan perawatan data dengan mengatur hak akses sistem, dan satu – satunya orang yang bertanggung jawab jika terjadi kecurangan pengaksesan data oleh yang tidak berhak.
b. *Operator*, orang yang sedang memakai komputer.
c. Sistem jaringan, yaitu teknologi yang menyebabkan satu komputer dengan komputer lainnya (di universitas yang sama maupun dengan universitas lain), dapat saling berhubungan.
d. Bagian administrasi, yaitu bagian sistem yang mengelola data-data administrasi.
e. Bagian akademik, yaitu bagian sistem yang mengelola data – data yang berhubungan dengan akademik, baik penyusunan jadwal, ruangan, dosen pengajar, dll.

Keamanan Sistem Informasi

Sistem keamanan informasi (*information security*) memiliki empat tujuan yang sangat mendasar adalah:

1. Kerahasiaan (*Confidentiality*): Informasi pada sistem komputer terjamin kerahasiaannya, hanya dapat diakses oleh pihak-pihak yang diotorisasi, keutuhan serta konsistensi data pada sistem tersebut tetap terjaga. Sehingga upaya orang-orang yang ingin mencuri informasi tersebut akan sia-sia.
2. Ketersediaan (*Availability*): Menjamin pengguna yang sah untuk selalu dapat mengakses informasi dan sumber daya yang diotorisasi. Untuk memastikan bahwa orang-orang yang memang berhak untuk mengakses informasi yang memang menjadi haknya.
3. Integritas (*Integrity*): Menjamin konsistensi dan menjamin data tersebut sesuai dengan aslinya, sehingga upaya orang lain yang berusaha merubah data akan segera dapat diketahui.
4. Penggunaan yang sah (*Legitimate Use*): Menjamin kepastian bahwa sumberdaya tidak dapat digunakan oleh orang yang tidak berhak

Ancaman terhadap sistem informasi dibagi menjadi 2 macam, yaitu ancaman aktif dan ancaman pasif

a. Ancaman aktif mencakup: pencurian data, penggunaan sistem secara illegal, penghancuran data secara illegal, modifikasi secara illegal.

b. Ancaman pasif mencakup: kegagalan sistem, kesalahan manusia, bencana alam.

Web Penetration Testing

Berdasarkan definisi dalam modul CEH, Web Penetration Testing merupakan metode evaluasi keamanan sistem komputer dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari security audit. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh black hat hacker, cracker, dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin dilakukan pada sistem beserta akibat yang bisa terjadi karena kelemahan sistem. Dalam melakukan penetration testing, diperlukan analisa intensif untuk setiap kerentanan yang diakibatkan oleh kelemahan sistem. Nantinya setelah seluruh analisa selesai dilakukan, akan didokumentasikan dan diberikan kepada IT yang bersangkutan beserta solusi dan dampak yang dapat diakibatkan dari celah keamanan yang ada. Hal – hal yang perlu diuji dalam penetration testing ada banyak, hal ini dibutuhkan untuk mengidentifikasi ancaman – ancaman utama seperti kegagalan komunikasi, e-commerce, dan kehilangan informasi rahasia. Selain itu ketika berhadapan dengan infrastruktur publik, seperti situs, gateway e-mail, akses jarak jauh, DNS, kata sandi, FTP, IIS, dan server situs, pengujian dilakukan pada semua perangkat keras dan lunak di sebuah sistem keamanan jaringan. Adapun faktor – faktor pendukung seperti tujuan, batasan, dan penyesuaian prosedur yang diperlukan untuk membuat web penetration testing lebih maksimal. Selain hal tersebut diperlukan orang yang professional untuk melakukannya serta pertimbangan biaya yang sesuai dengan kebutuhan. Pada akhirnya diperlukan juga dokumentasi yang jelas serta penjelasan mengenai potensi resiko dan hasil penemuan dari hasil analisa dan uji coba kepada klien. Bersumber pada modul Licensed Penetration Tester, beberapa teknik yang umum digunakan dalam penetration testing adalah sebagai berikut:

a. *Passive research*: digunakan untuk mencari semua informasi umum yang digunakan sebuah organisasi.
b. *Open source monitoring*: keterbukaan sebuah perusahaan untuk integritas informasi dan kerahasiaan informasinya.
c. *Network mapping* dan *OS Fingerprinting*: digunakan untuk mendapatkan konfigurasi jaringan yang akan diuji coba.
d. *Spoofing*: uji coba penyamaran sistem yang disamarkan seperti sebuah komputer yang sudah terdaftar dalam sistem, serta diuji coba dari sisi internal maupun eksternal.
e. *Network sniffing*: penangkapan data yang berjalan dalam sebuah jaringan.
f. *Trojan attacks*: kode jahat yang biasanya dikirim dalam sebuah jaringan berupa *attachment* pesan elektronik atau dikirim melalui pesan instan di sebuah ruang chat.
g. *Brute force attack*: teknik yang umum untuk membuka kata sandi dan dapat membuat sebuah sistem *overload* maupun berhenti merespon ke semua permintaan akses.
h. *Vulnerability Scanning*: pemeriksaan menyeluruh pada sebuah area target dari infrastruktur jaringan perusahaan.
i. *Scenario Analysis*: pengujian akhir yang melibatkan pengujian dan penilaian resiko celah keamanan lebih akurat dengan sebuah kasus.

Planning and Preparation

Fase ini berisi langkah-langkah untuk bertukar informasi, merencanakan dan mempersiapkan tes. Sebelum dimulainya melakukan pengujian, peneliti akan memberikan surat ijin untuk melakukan penelitian terkait yang akan disetujui dari kedua pihak. Tujuannya adalah memberikan perlindungan hukum pada kedua belah pihak. Pada tahapan ini juga menentukan tim yang terlibat, tanggal, waktu dan ketentuan lainnya. Pada fase ini, peneliti mempersiapkan *tools* untuk mendukung penelitian dan mengajukan permohonan penelitian kepada pihak yang terkait dengan penelitian ini.

Assessment

Information Gathering

Pengumpulan informasi pada dasarnya menggunakan internet untuk mencari semua informasi mengenai target (perusahaan / orang) menggunakan dua metode yakni teknis (*DNS* / *WHOIS*) dan non-teknis (mesin pencari, kelompok berita, dll). Metode ini adalah tahap awal dari setiap audit keamanan informasi yang banyak orang cenderung mengabaikannya. Ketika melakukan pengujian apapun pada sistem informasi, pengumpulan informasi dan data *mining* sangat penting menyediakan semua informasi untuk melanjutkan tes. Terlebih lagi, melakukan pengumpulan informasi sangat penting dari beberapa kejadian yang mungkin. Pengumpulan informasi ini menjadi jalan untuk mendapatkan lebih banyak pemahaman atau informasi dari target dan sumber daya yang dimiliki. Pengumpulan informasi bisa diperoleh dari: brosur perusahaan, kartu nama, *leaflet*, iklan, koran, dokumen internal dan sebagainya. Pengumpulan informasi tidak mengharuskan peneliti menetapkan kontak dengan sistem target. Informasi dikumpulkan dari sumber – sumber publik di internet dan organisasi yang memegang informasi publik (misalnya lembaga pajak, perpustakaan, dll). Penilaian pada bagian ini sangat penting bagi peneliti, penilaian umumnya terbatas dalam waktu dan sumber daya tertentu. Oleh karena itu, sangat penting untuk mengidentifikasi poin – poin yang paling rentan dan fokus pada kerentanan tersebut. Bahkan alat terbaik akan sia – sia jika tidak digunakan dengan tepat dan di tempat dan waktu yang tepat pula. Itu sebabnya peneliti yang berpengalaman sangat bersungguh – sungguh dalam waktu pengumpulan informasi. Dalam tahapan ini, peneliti menggunakan *tools* bawaan *kali linux* yaitu *who is*, *dmitry*, *dig*, *nslookup*, *maltego* dan sebuah *website* yang menyediakan informasi dari target yaitu www.searchdns.netcraft.com. Berikut dibawah ini informasi yang didapatkan oleh peneiti dari target yang ingin diserang:

Tabel 1: Hasil dari *Information Gathering*

Site rank	850015
Date first seen	April 2010
Primary language	*english*
Site	(*link* situs target)
Domain	(domain situs target)
Ip address / DNS	(*IP* server situs target)
Domain register	*Pandi.or.id*
Netblock owner	*PT Telkom Indonesia's Customer*
Name server organization	*Whois.pandi.or.id*
Name server	*Ns5.dnet.net.id / Ns5.dnet.net.id*
DNS admin	*Noc2@dnet.net.id*
Hosting company	PT Telekomunikasi Indonesia Tbk
Reverse DNS	subnet.static.astinet.telkom.net.id
Organization	(alamat situs target)
Top level domain	Indonesia (*ac.id*)
OS	*Linux*
Web server	*Apache* / 2.4.7 *ubuntu*
Last seen	10 feb 2017
Netcraft risk rating	1 dari 10 yang belum diamankan
Registrant phone	0215674223
Domain ID	PANDI-D0116131
Status	*Client – server transfer prohibited*
Router	(*IP* router target)
Admin name	Supriyadi
Admin ID	3supriy
Admin email	*Supriyadi_mk@yahoo.com*
Hosting country	ID

Network Mapping

Pertama, ketika semua informasi tentang target telah diperoleh yang membutuhkan teknik lebih, dibawa ke *footprint network* dan sumber daya yang dimaksud. Jaringan informasi dari bagian sebelumnya diambil dan diperluas untuk menghasilkan topologi

jaringan target. Agar efektif, *network mapping* harus dilakukan sesuai dengan rencana. Rencana ini mencakup kerentanan atau poin yang paling penting untuk dinilai organisasi atau perusahaan, dan akan mempertimbangkan semua informasi yang diperoleh dari bagian sebelumnya. *Network mapping* akan membantu peneliti untuk *fine tune* informasi sebelumnya yang diperoleh dan untuk mengkonfirmasi atau menolak beberapa hipotesis mengenai sistem yang ditargetkan (seperti tujuan, merek *software / hardware*, konfigurasi, arsitektur, hubungan dengan sumber lain dan hubungan dengan proses bisnis). Pada tahapan ini, peneliti menggunakan *tools zenmap*. Berikut hasil informasi yang didapat oleh peneliti dari tahapan *network mapping* ini:

Tabel 2: Hasil dari *Network Mapping*

Status	*Up*
Open ports	844
Closed port	156
Scanned port	1000
Up time	677889
Last boot	*Sun mar 19 23:08:46 2017*
Ipv4	(*IP* situs target)
Hostnames	(*link* situs target)
TCP sequence difficulty	*Good luck*
TCP sequence index	264
Ip id sequences	*Randomized*
TCP TS sequence class	*Other*
Route	(*router* situs target)
Topology	*Localhost* - (*router* situs target) - (*IP* situs target)
Services	*Jetdirect, postgresql, tcpwrapped, squid-http, domain, ftp, http, http-proxy, smpt, ssh, unknown*

Scan Vulnerability

Sebelum memulai tahapan ini, peneliti akan memilih titik – titik tertentu untuk menguji dan bagaimana untuk menguji sistem yang ditargetkan. Pada tahapan ini *tools* yang digunakan oleh peneliti terdiri dari *vega*, *OWASP ZAP*, *skipfish* dan *vega*. Berikut dibawah ini hasil *scan vulnerability* yang dilakukan oleh peneliti dengan target situs sistem.

Tabel 3: Hasil *Scan Vulnerability*

Kerentanan	Tingkat
Directory browsing	*Medium*
x-frames-options header not set	*Medium*
Cross domain javascript source file inclusion	*Low*
Private IP disclosure	*Low*
Web browser xss protection not enabled	*Low*
x-content-type-options header missing	*Low*
Cleartext password over HTTP	*High*
Session cookie without httponly flag	*High*
Session cookie without secure flag	*High*
Directory listing detected	*Low*
Form password field with autocomplete enabled	*Low*
Html form with no apparent xsrf protection	*Medium*
Limit exceeded, fetch suppressed	*High*
Incorrect or missing charset	*Low*
Incorrect or missing MIME type	*Low*
File upload form	*Low*
Hidden files / directories	*Info*
Server error triggered	*Info*
Resource not directly accessible	*Info*
New 404 signature seen	*Info*
New 'server' header value seen	*Info*
http error detected	*Info*

Penetration

Peneliti mencoba untuk masuk kedalam sistem secara ilegal atau tanpa izin dan mencoba mencapai tingkat akses yang sifatnya *privacy*.*Tools* yang digunakan oleh peneliti antara lain *havij* (versi *windows*), *sqlmap* (versi *linux*), dan *browser* untuk analisa secara manual, *metasploit*, *upload script*, *XSS script*, *tools flooding*. Untuk teknik dan bagaimana cara melakukannya, pihak peneliti tidak memberikan gambarannya di jurnal ini. Peneliti menerangkan tentang bagaimana cara melakukan penetration testing di dalam tugas akhir peneliti. Peneliti melakukan hal tersebut dikarenakan demi alasan keamanan dan kebaikan dari semua pihak yang terlibat didalam penelitian ini. Dari penelitian yang telah dilakukan, peneliti dapat menarik kesimpulan bahwa untuk jenis serangan *sql injection* yang dilakukan terhadap target yaitu sistem informasi akademik Universitas XYZ, sistem tersebut telah **AMAN**. Peneliti dapat menyimpulkan bahwa target sudah tidak memilik *bug* di bagian *sql* nya. Hal tersebut dapat dibuktikan oleh peneliti melalui serangan *sql injection* dengan tiga *tools* dan metode yang berbeda (lihat gambar 30 – 32). Perlu digaris bawahi kembali peneliti dapat menyimpulkan sistem telah aman **HANYA UNTUK JENIS SERANGAN *SQL INJECTION***. Untuk jenis

serangan yang lainnya, peneliti dapat menyimpulkan bahwa sistem target **BELUM AMAN**. Hal ini terlihat dan dibuktikan oleh peneliti dari hasil *scanning* celah keamanan atau *vulnerability*. Oleh karena itu, peneliti dapat menyimpulkan bahwa tingkat kemanan yang dimiliki oleh target belumlah sempurna. Untuk membuat sistem informasi akademik lebih aman maka peneliti memberikan beberapa saran untuk pihak *developer* yang akan diberikan oleh peneliti. Dari hasil pengujian ini, laporan atau hasilnya akan diberikan kepada pihak *administrator IT* agar pengembangan terhadap keamanan sistem bisa dapat dipertahankan atau ditingkatkan kembali. Saran yang akan diberikan oleh peneliti didasarkan pada hasil analisa celah *vulnerability* yang telah ditemukan. Berikut ini solusi atau saran yang diberikan oleh peneliti untuk menambah keamanan sistem target:

- *Cleartext password over http*: ini merupakan celah dimana *form password* untuk *login* ke sistem target masih bersifat *cleartext*. Para *hacker* dapat dengan mudah mengetahui *password* yang dituliskan di *form* tersebut hanya dengan mengirimkan *keylogger* ke dalam situs target. Solusinya adalah *password* tidak boleh dikirim melalui *cleartext*. Bentuknya harus tunduk kepada target HTTPS.
- *Session cookie without httponly flag*: ini merupakan celah dimana *cookie session* pada sistem target tidak menggunakan *httponly*. Akibat dari celah ini *client user* dapat mengontrol *session cookie* sistem target. Diistilah dunia *hacking* biasa disebut dengan serangan XSS atau *cross site script*. Solusinya yaitu dengan mengaktifkan *flag httponly* ketika sedang membuat *script* untuk *session* sistem.
- *Session cookie without secure flag*: ini merupakan celah dimana *developper* sistem tidak mengaktifkan *secure flag* ketika membuat *script* untuk *session cookie*. Padahal *session cookie* merupakan salah satu segi keamanan yang *credential*. Bila berhasil dijebol, sistem akan berhasil disadap oleh *hacker*, jadi setiap kegiatan yang dilakukan target *hacker* dapat memonitoring apa yang sedang dilakukan *user* dalam sistem. Solusi untuk menutup celah tersebut adalah dengan mengaktifkan mode keamanan *secure flag* pada saat membuat *script cookie session*.
- *Limits exceeded, fetch suppressed*: ini merupakan celah dimana ketika sistem memasuki sebuah *web page* tertentu, aksesnya bisa digunakan oleh beberapa *user* sehingga page tersebut mengalami *limits* dan bisa dibuka. *Page* yang mengalami hal tersebut adalah (celah yang ditemukan link situs target). Solusinya adalah menutup beberapa akses yang dapat masuk ke *web page* tersebut.
- *Html form with no apparent XSRF protection*: ini merupakan celah dimana sistem tidak mengaktifkan tingkat proteksi untuk serangan XSRF. Serangan XSRF adalah jenis serangan dimana *hacker* mengirimkan *request* yang berhubungan dengan sistem target ke *user* tanpa disadari oleh *user* itu sendiri bahwa itu merupakan serangan untuk masuk ke target. Solusinya adalah dengan mengaktifkan XSRF *protection* ketika *developper* sedang membuat *script* sistem target. Boleh juga dilakukan ketika sedang *maintenance*
- *Directory browsing*: maksudnya *user* dapat mencari berkas – berkas penting yang telah dimasukkan ke dalam sistem ke dalam *webpages*. Ini sangat berbahaya karena bila sistem berhasil diretas, *hacker* bisa langsung dengan mudah mengambil berkas tersebut. Solusinya menonaktifkan fitur untuk *directory browsing* bagi *user*.
- *X-frames-options header not set*: celah ini disebabkan karena *x – frames options header* tidak dimasukan ke dalam HTTP *response*. Bila tidak dimasukkan maka kemungkinan *hacker* akan menyerang dengan jenis serangan *clickjacking* dapat terlaksana. Solusinya adalah pastikan *X-Frame-Options HTTP header* diatur pada semua halaman web dan dikembalikan

ke situs target. Jika sistem ingin menggunakan *frame* hanya pada *server* maka ubah mode menjadi "*SAMEORIGIN*", untuk sebaliknya ubah mode menjadi "*DENY, ALLOWS-FROM*".

- *Form password field with autocomplete enabled*: ini merupakan celah dimana *services autocomplete* tidak dimatikan di *form input password* dari sistem. Hal ini dapat menyebabkan *password* dapat tersimpan di *browser* sehingga lebih memudahkan *hacker* untuk mendapatkan *password* tersebut. Solusinya yaitu dengan menonaktifkan layanan *autocomplete* pada *form password* yang dimiliki sistem target.
- *Web browser xss protection not enabled*: ini merupakan celah dimana proteksi atau perlindungan terhadap serangan XSS *scripting* dalam keadaan non aktif. Nonaktifnya proteksi XSS bisa disebabkan karena konfigurasi *response header* pada *web servernya*. Solusinya membuat konfigurasi proteksi xss menjadi aktif secara otomatis
- *X – content – type – options header missing*: ini merupakan celah dimana *header anti – MIME – sniffing X – content – type – options* tidak disetel ke *nosniff*. Hal ini menyebabkan *browser* dapat menampilkan isi atau content yang sebenarnya tidak untuk ditampilkan didalam sistem. Solusi untuk mengatasi hal tersebut adalah pastikan bahwa aplikasi / *web server* menetapkan *Content-Type header* yang tepat, dan mengaktifkan *header X-Content-Type- untuk 'nosniff'* untuk semua halaman *web*.
- *Directory listing detected*: ini merupakan celah dimana sistem memiliki list direktori atau daftar isi data – data penting. Biasanya data – data tersebut disimpan dalam bentuk *backup* data. Nah kesalahan yang ditemukan oleh peneliti, *backup* datanya pun diletakkan dalam sistem. Bahaya yang ditimbulkan adalah *server* dapat sewaktu waktu mengeluarkan isi direktori tersebut ke *user*, dapat mengakses file (*htaccess* lama, *backup, source code*), memberikan informasi tentang tata letak dan karakteristik sistem (seperti *naming conventions*), dan meningkatkan kemungkinan untuk serangan *blinds attack* dan *brute force attack*. Solusinya adalah untuk *apache*, lakukan salah satu hal berikut: menambahkan "*indexignore*" untuk file *.htaccess* direktori ini, atau menghapus "*indexes*" dari baris "*options all indexes followsymlinks multiviews*" pada konfigurasi *apache*. Untuk *lighttpd*, perubahan "*dir-listing.activate = enable*" untuk "*dir-listing.activate = disable*" di file konfigurasi *lighttpd* anda.
- *File upload form*: ini merupakan celah dimana sistem menyediakan ruang atau *space* untuk *upload file*. Sebetulnya tidak menjadi masalah bila *upload* hanya untuk orang – orang yang berhak saja. Di sistem ini peneliti dapat melihat *file* yang udah di *upload*. Bagi *hacker*, ini sangat menguntungkan karena *hacker* bisa meyisipkan *shell script* untuk menyerang sistem. Solusinya adalah dengan menutup layanan *upload* hanya untuk beberapa *user* saja seperti *admin* atau yang lainnya.

Report and Result

Pada tahapan ini, semua informasi yang dibuat atau disimpan pada sistem yang diuji harus dihapus. Jika tidak mungkin menghapus dari *remote system*, semua file ini (dengan lokasi mereka) harus disebutkan dalam laporan teknis sehingga staf teknis klien dapat menghapus setelah laporan diterima. Hal ini dilakukan agar tidak terjadi kesalahpahaman dan penumpukan file didalam sistem tersebut. Pada tahapan ini pula, disajikan tentang hasil dari penelitian yang dilakukan oleh peneliti. Lalu, hasil dan laporannya dibuat atau dimuat dalam bentuk dokumen yang akan diberikan kepada pihak *administrator IT* yang bersangkutan agar bila masih terdapat celah segera dapat ditutup dan ditindak lanjuti.

Kesimpulan

Dari penelitian diatas, peneliti dapat menarik kesimpulan bahwa untuk jenis serangan *sql injection* yang dilakukan terhadap target yaitu sistem informasi akademik Universitas XYZ, sistem tersebut telah **AMAN**. Peneliti dapat menyimpulkan bahwa target sudah tidak memilik *bug* di bagian *sql* nya. Hal tersebut dapat dibuktikan oleh peneliti melalui serangan *sql injection* dengan tiga *tools* dan metode yang berbeda (lihat gambar 30 – 32). Perlu digaris bawahi kembali peneliti dapat menyimpulkan sistem telah aman **HANYA UNTUK JENIS SERANGAN *SQL INJECTION***. Untuk jenis serangan yang lainnya, peneliti dapat menyimpulkan bahwa sistem target **BELUM AMAN**. Hal ini terlihat dan dibuktikan oleh peneliti dari hasil *scanning* celah keamanan atau *vulnerability* (lihat gambar 27 – 29).

Daftar Pustaka

Allen, Lee, Shakel Ali dan Tedi Heriyanto. 2014. "Kali Linux – Assuring Security by Penetration Testing". Oktober 2016.

Allen, Lee. 2012. "Advanced Penetration Testing for Highly – Secured Environments: The Ultimate Security Guide". Oktober 2016.

Aristorini, M Aisyah, Sukiswo dan A Ajulian Z. 2015. "Evaluasi Kinerja Protokol AOMDV terhadap Serangan Malicious Node dan Ddos pada Manet dengan menggunakan Network Simulator 2". http://download.portalgaruda.org/article.php?article=365678&val=4717&title=EVALUASI%20KINERJA%20PROTOKOL%20AOMDV%20TERHADAP%20SERANGAN%20MALICIOUS%20NODE%20DAN%20DDOS%20PADA%20MANET%20DENGAN%20MENGGUNAKAN%20NETWORK%20SIMULATOR%202%20(NS-2). Oktober 2016.

Dahlan, A Latubessy dan M Nurkhamid. 2015. "Analisa Keamanan Web Server terhadap Serangan Posibility SQL Injection (Studi Kasus Web Server UMK)". http://jurnal.umk.ac.id/index.php/SNA/article/viewFile/331/348. Oktober 2016.

Daniel, M Ilham, Leon A Abdillah dan Kiky Rizky N. 2015. "Evaluasi Celah Keamanan Web Server pada LPSE kota Palembang". http://arxiv.org/pdf/1508.06069. Oktober 2016.

Dieterle, W Daniel. 2013. "Basic Security Testing With Kali Linux". Oktober 2016.

Eichel, Zee. 2015."Attacking Side With Backtrack". http://www.indonesianbacktrack.or.id/. Oktober 2016.

Fauziah dan Ina Agustina. 2015. "Pencegahan Session Hijacking pada Sistem Jaringan Komputer di Web Server (Studi Kasus Penggunaan Email dan Chatting)". http://repository.upnyk.ac.id/255/1/C-13_PENCEGAHAN_SESSION_HIJACKING_PADA_SISTEM_JARINGAN_KOMPUTER.pdf. Oktober 2016.

Homenta, Johanes Indra dan Rissal Efendi. 2015. "Menganalisa Keamanan Jaringan berbasis Intrusion Prevention System dan Honeypot sebagai Pendeteksi dan Pencegah Malware (Studi Kasus PT Mitra Nugraha)". http://www.provisi.ac.id/ejurnal/index.php/JTIKP/article/download/111/105. Oktober 2016.

Idrus, M R Suryatama. 2015. "Analisis Performa Network Intrusion Detection System (NIDS) Menggunakan Metode Signature Based dalam Mendeteksi Serangan Denial of Service (Ddos) berbasis UDP Flooding". http://journal.bakrie.ac.id/index.php/jurnal_ilmiah_ub/article/view/1208. Oktober 2016.

Kennedy, David, dkk. 2011. "Metasploit". Oktober 2016.

Masyur, Fauzan. 2015. "Analisis Vulnerability WEB Based Aplication Menggunakan Nessus". http://senatekprosiding.ump.ac.id/index.php/snt/article/viewFile/54/53. Oktober 2016.

Muhsin, Muhammad dan Adi Fajaryanto. 2015. "Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP Versi 4 (Studi Kasus Web Server

Ujian Online)". http://jurnal.umpo.ac.id/index.php/MUL/article/download/149/134. Oktober 2016.

Official kali linux. 8 Desember 2013. "Pengenalan Kali Linux". http://docs.kali.org/. Oktober 2016.

OISSG. 01 Mei 2006. "Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1 B". Oktober 2016.

Pangalila, Richad, A Noertjahyana dan J Andjarwirawan. 2015. "Penetration Testing Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra". http://studentjournal.petra.ac.id/index.php/teknik-informatika/article/download/3145/2835. Oktober 2016.

Paryati. 2015. "Keamanan Sistem Informasi". http://repository.upnyk.ac.id/143/1/47_Keamanan_Sistem_Informasi.pdf. Oktober 2016.