sudo
Jurnal Teknik Informatika
https://jurnal.ilmubersama.com/index.php/sudo

Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box

Studi Kasus Web Server Diva Karaoke.co.id

Marzuki Hasibuan, Andi Marwan Elhanafi

Fakultas Teknik dan Komputer, Program Studi Teknik Informatika, Universitas Harapan Medan, Medan, Indonesia

INFORMASI ARTIKEL

Diterima Redaksi: 5 Desember 2022
Revisi Akhir: 7 Desember 2022
Diterbitkan *Online*: 8 Desember 2022

KATA KUNCI

Penetration Testing; Kali Linux; Keamanan Jaringan; Web Server

KORESPONDENSI

Phone: +62 823-6399-9245
E-mail: amarhsb7@gmail.com

A B S T R A K

Sebuah perusahaan yang berkembang memerlukan sebuah *website* untuk menunjang kegiatan operasionalnya, namun yang sering menjadi permasalahan adalah bagaimana cara mengamankan data yang ada di *web server* agar terhindar dari pihak yang tidak bersangkutan. Dalam penelitian ini akan ditulis bagaimana cara mengetahui tingkat keamanan pada *web server* diva karaoke dengan melakukan pengujian penetrasi dalam suatu sistem dengan menggunakan perangkat lunak virtualisasi *virtualbox* untuk mengeksekusi sistem operasi *kali linux.* Pengujian penetrasi ini hanya untuk menguji tingkat keamanan sistem jaringan *web server* diva karaoke dengan menggunakan uji coba non destruktif yaitu uji coba yang tidak membuat kerusakan sistem. Penelitian ini dilakukan dengan melakukan analisis dan perancangan dengan menggunakan tools-tools yang ada di *kali linux*. Hasil penelitian ini menunjukkan tingkat kerentanan pada *web server* diva karaoke masih rendah, dibuktikan dengan adanya beberapa port TCP yang terbuka, situs web beresiko terhadap serangan *clickjacking.* Selain itu penelitian ini juga dapat menjadi tolak ukur sejauh mana perusahaan yang dievaluasi ini sudah bisa mengamankan data dari pihak yang seharusnya tidak mendapatkan akses terhadap data.

PENDAHULUAN

Penetration testing adalah seni semua orang dapat mempelajari banyak teknik dan memahami semuanya, tetapi kenyataannya perangkat lunak itu komplek, terutama ketika mulai meletakkan banyak sistem pada perangkat lunak secara bersama [1]. Perusahaan akan menggunakan banyak waktu dan potensi untuk menyingkirkan diri mereka sendiri dari gangguan *hacker*, untuk terhindar dari kerugian yang disebabkan oleh para *hacker* langkah yang harus dikembangkan adalah melakukan evaluasi terhadap keamanan *server* yang ada. Hal ini bermaksud untuk meredam resiko terjadinya penyalahgunaan terhadap sumber daya yang ada pada organisasi [2]. *Penetration testing* adalah alat penilaian jaminan bernilai yang menguntungkan baik bisnis dan operasinya. Dari segi operasional, *penetration testing* membantu membentuk strategi keamanan informasi melalui identifikasi kerentanan yang cepat dan akurat [3]. Perangkat lunak *web server* dikenal dapat melayani permintaan pengguna berupa *http* dari *client* yang terhubung dalam jaringan dan memberikan pelayanan kepada yang meminta informasi berkaitan dengan *website* dan memberikan suatu hasil berupa halaman *web* yang ditampilkan dalam *browser*. Seringkali kita dapati bahwa masalah pada umumnya *server down* ataupun permintaan paket yang dikirim ke *server* terasa sangat lama dan lambat dan bisa jadi *server* tidak bisa di akses dikarenakan *web server* mengalami kerusakan yang disebabkan oleh *hacker* [4]. Oleh karena itu dibutuhkan suatu cara untuk mencari suatu kerentanan pada sistem *web server* yang bisa mengakibatkan para *hacker* masuk untuk merusak sistem *web server*. Salah satunya dengan melakukan *penetration testing* pada *web server* agar permasalahan yang sering terjadi bisa diantisipasi [5]. Seiring berkembangnya dunia teknologi dan untuk memudahkan pelanggan mencari informasi tentang diva karaoke, diva karaoke memiliki *website* sendiri yang diberi nama *www.divakaraoke.co.id* dimana *website* tersebut

https://doi.org/10.56211/sudo.v1i4.160

menjadi tempat promosi untuk para pelanggan melihat fitur – fitur yang tersedia di diva karaoke. Pelanggan bisa melihat sejarah berdirinya diva karaoke, sistem yang digunakan, *room*, dan *outlet* diva karaoke yang tersebar di indonesia. Dengan memiliki *website* tentu diva karaoke ingin menjaga keamanan *website* nya dari serangan *hacker*. Maka dari itu diva karaoke memberikan izin kepada penguji penetrasi untuk menguji kelemahan *website* tersebut [6].

TINJAUAN PUSTAKA

Diva Karaoke

Outlet diva karaoke pertama kali berdiri di jl. Mangga besar raya no.96 jakarta barat pada bulan april 2011, *outlet* tersebut juga sebagai kantor pusat dari diva karaoke. Didirikan langsung oleh artis 'Rossa' sebagai *brand ambassador* yang meningkatkan *brand awareness family* karaoke. Sesuai *value* diva terkonsep memberikan keistimewaan kepada pelanggan wanita, tidak sebagai pelanggan tetapi juga bisa merasakan jadi seorang diva. Sampai saat ini *outlet* diva karaoke sudah tersebar mencapai 41 outlet di seluruh indonesia. Mulai dari jakarta, sukabumi, karawang, bandung, cirebon, malang, madiun, pontianak, banjarmasin, makassar, manado, kendari, palembang, pekanbaru, jambi, medan, bangka, batam, bali dan Lombok.

Sistem Jaringan Komputer

Mendapatkan dua atau lebih komputer untuk berkomunikasi dan mengirimkan data adalah proses yang sederhana dalam konsep jaringan. Semua faktor yang terlibat di suatu jaringan perlu terhubung secara fisik ke komputer [7][8]. Koneksi ini biasanya memerlukan kabel yang dihubungkan ke komputer lain atau perangkat jaringan. Jaringan lain adalah komunikasi *nirkabel*, komunikasi *nirkabel* digunakan dengan frekuensi lebih banyak, dan koneksi *nirkabel* jelas tidak membutuhkan kabel. Namun komunikasi *nirkabel* bergantung pada perangkat fisik untuk mengirimkan data

Keamanan Jaringan

Keamanan jaringan sangat vital bagi sebuah jaringan komputer. Kelemahan - kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan kerugian berupa kehilangan data, kerusakan sistem *server*, tidak maksimal dalam melayani *user* atau bahkan kehilangan aset - aset berharga di suatu organisasi [9]. Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan meskipun terkadang beberapa organisasi lebih mendahulukan tampilan dan lain sebagainya dibandingkan masalah keamanannya, dan ketika sistem mendapat serangan dan terjadi kerusakan sistem, masalah dan kerugiannya akan lebih besar untuk melakukan perbaikan sistem. Maka sudah selayaknya keamanan jaringan harus lebih diperhatikan untuk melindungi sistem dari ancaman serangan yang semakin canggih dan beragam, terlebih lagi ketika jaringan lokal sudah terhubung ke *internet* maka ancaman keamanan jaringan akan semakin meningkat. Misalnya *ddos attack* dan sebagainya, juga serangan *hacker*, *virus*, *trojan* yang semuanya merupakan ancaman yang tidak bisa di abaikan.

Penetration Testing

Penetration testing adalah alat penilaian jaminan bernilai yang menguntungkan baik bisnis dan operasinya. Dari segi operasional, *penetration testing* membantu membentuk strategi keamanan informasi melalui identifikasi kerentanan yang cepat dan akurat. *Penetration testing* membagikan informasi rinci tentang ancamanan keamanan secara aktual, yang dapat dieksploitasi jika tercakup dalam aliran dan proses keamanan organisasi [10][11]. Hal ini akan membantu organisasi untuk mengidentifikasi dengan cepat dan akurat, potensi kerentanan yang nyata

Tujuan mendasar dari evaluasi kerentanan adalah mengidentifikasi kerentanan keamanan di bawah keadaan yang dikendalikan, sehingga dapat diantisipasi sebelum pengguna yang tidak berhak mengeksploitasi sistem suatu organisasi. Ahli sistem penetrasi menggunakan uji penetrasi untuk mengatasi masalah yang menyangkut dalam penilaian kerentanan, dengan fokus pada kerentanan dengan tingkat keparahan yang tinggi.
Tes *penetrasi* dianggap bagian dari proses manajemen resiko keamanan IT yang mungkin digerakkan oleh persyaratan internal atau eksternal sesuai dengan situasi individu. Penting untuk diingat bahwa tes penetrasi hanya satu komponen dalam mengevaluasi keamanan sistem jaringan. Dan yang paling utama tes penetrasi dapat memberikan bukti nyata masalah keamanan, namun harus menjadi bagian dari sebuah tinjauan komprehensif tentang keamanan organisasi.
Berikut ini adalah item yang diharapkan untuk diuji selama tes penetrasi:

1. Aplikasi
2. Infrastruktur IT
3. Perangkat Jaringan
4. Tautan komunikasi
5. Keamanan dan tindakan fisik
6. Masalah psikologis
7. Masalah kebijakan

Dalam banyak kasus, tes penetrasi merupakan tipe tes paling agresif yang bisa dilakukan pada suatu organisasi. Sedangkan tes lain menghasilkan informasi tentang kekuatan dan kelemahan suatu organisasi. Hanya penetrasi yang beresiko menyebabkan gangguan pada sebuah lingkungan produksi. Secara mendasar *penetration testing* memiliki beberapa jenis pengujian, berikut di bawah ini jenis - jenis pengujian *penetration testing* [10]:

1. *Black Box* adalah jenis tes yang paling mirip dengan tipe situasi yang merupakan serangan luar dan kadang - kadang dikenal sebagai tes eksternal. Untuk melakukan jenis tes ini penguji penetrasi akan menjalankan tes dari lokasi yang jauh. penguji penetrasi sangat terbatas dalam informasi dan biasanya hanya memiliki informasi berupa situs *web* yang akan di *pentest*.
2. *Gary Box* dalam jenis tes ini, penguji penetrasi diberi pengetahuan terbatas yang mungkin berjumlah semua informasi seperti sistem operasi atau data lainnya.
3. *White Box* dalam jenis tes ini, pihak organisasi memberi pengetahuan tentang struktur dan susunan lingkungan target, karenanya jenis tes ini juga kadang – kadang dikenal sebagai tes internal. Jenis tes ini memungkinkan untuk analisis yang lebih dekat dan lebih mendalam daripada jenis tes *black box* atau *gray box*.

Web Server

Web server adalah sebuah software yang memberikan layanan berbasis data dengan menggunakan *protokol HTTP* atau *HTTPS* dari *client* menggunakan aplikasi *web browser* untuk *request* data dan *server* akan mengirim data dalam bentuk halaman *web* dan pada umumnya berbentuk halaman *HTML*. Halaman *web* yang diminta bisa terdiri dari berkas *teks*, video, gambar, *file* dan banyak lagi.

Serangan Clickjacing

Serangan *clickjacking* yaitu jenis serangan pada aplikasi web yang membuat pengguna web aplikasi secara tidak sengaja mengklik elemen halaman web yang sebenarnya tidak ingin di klik.

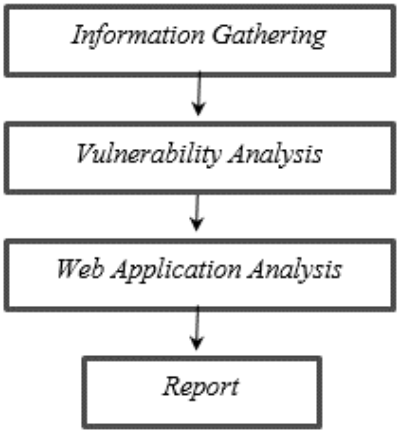
Sniffing MIME

Sniffing MIME adalah teknik yang digunakan oleh beberapa browser web (terutama Internet Explorer) untuk memeriksa konten aset tertentu. Ini dilakukan untuk tujuan menentukan format file aset. Teknik ini berguna jika tidak ada informasi metadata yang cukup untuk aset tertentu, sehingga memungkinkan browser menafsirkan aset secara tidak benar. Meskipun pengendapan MIME dapat berguna untuk menentukan format file aset yang benar, hal ini juga dapat menyebabkan kerentanan keamanan. Kerentanan ini bisa sangat berbahaya baik bagi pemilik situs maupun pengunjung situs. Ini karena penyerang dapat memanfaatkan *MIME sniffing* untuk mengirimkan serangan XSS (*Cross Site Scripting*).

METODOLOGI

Tahapan Penelitian

Merupakan langkah-langkah pekerjaan yang akan dilakukan oleh peneliti dalam suatu penelitian.

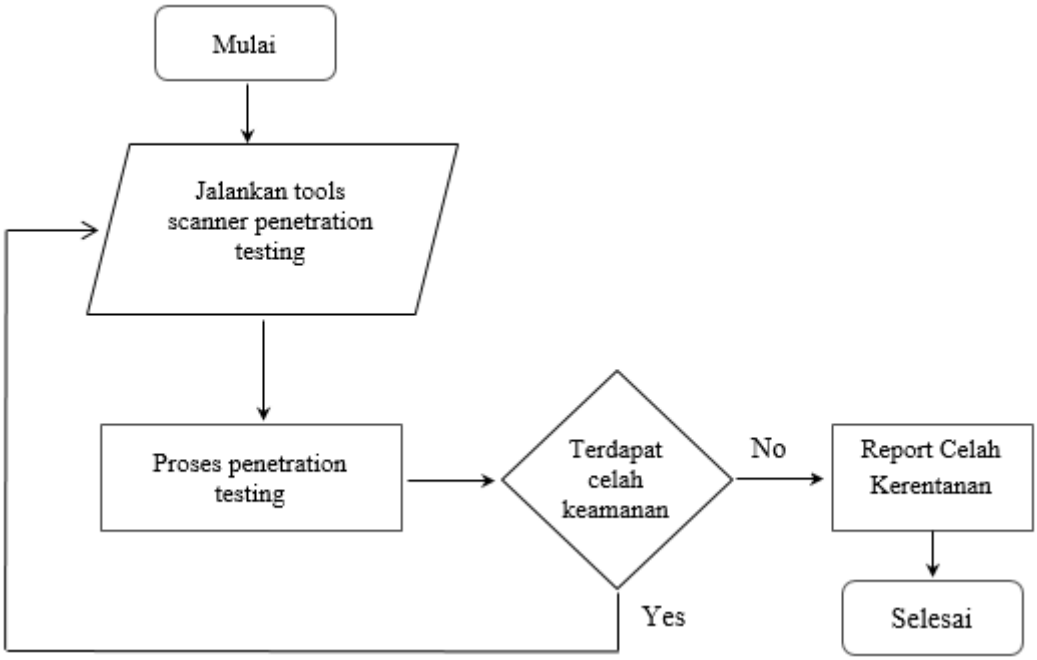


Gambar 1. Tahap Penelitian

Gambar diatas meruapakan tahapan penelitian yang akan dilakukan mulai dari Studi Litertur, Analisa kebutuhan sistem, Implementasi sistem, dan pengujian sistem. Semua tahapan diatas sudah mencakup langkah awal yaitu pengumpulan data, implementasi dan evaluasi sistem.

Flowchart

Flowchart sistem merupakan gambaran grafis yang memperlihatkan aliran data dari sumbernya dalam objek kemudian melewati proses yang mentransformasikan ke tujuan yang lain.



Gambar 2. Flowchart

Tahapan melakukan penetration testing

1. Buka terminal pada kali linux
2. Lalu jalankan *tools information gathering* untuk mendapatkan sebanyak mungkin informasi awal tentang *web server www.divakaraoke.co.id*
3. Setelah mendapatkan informasi awal
4. Lalu lakukan pengujian kerentanan
5. Buka terminal jalankan tools pengujian kerentanan
6. Selanjutnya masuk proses *penetration testing*
7. Jika terdapat celah kerentanan lakukan proses *penetration testing* menggunakan informasi yang lain
8. Jika sudah semua data informasi awal yang di dapat dan uji tidak menambah hasil laporan kerentanan

 https://doi.org/10.56211/sudo.v1i4.160

9. Buat laporan hasil kerentanan yang di dapat

HASIL DAN PEMBAHASAN

Adapun hasil yang di dapat dari proses *penetration testing* pada *web server* www.divakaraoke.co.id di temukan beberapa kerentanan. Di bawah ini table laporan hasil penetrasi testing menggunakan kali linux pada web server www.divakaraoke.co.id

Tabel 1. Laporan Information Gathering

Information Gathering			
Target HostName	www.divakaraoke.co.id		
Tools	**HostName**	**TCP/UDP**	**Port**
Dmitry	www.divakaraoke.co.id	*tcp*	21/open
		tcp	22/open
		tcp	80/open
		tcp	110/open
		tcp	111/open
		tcp	143/open
Whatweb	www.divakaraoke.co.id	*Plugin*	*Adobe-Flash*
		Webserver	*Apache*
		HTML	*HTML Version 5*
		Http Server	*Apache*
		Jquery	*Ajax*
		Metagenerator	*Serif Web Plus X7*
		Script	*Javascript*

Tabel 2. Jenis Kerentanan

Vulnerability Analysis		
Target HostIp	49.50.8.234	
Port	80	
Tools	**Jenis Kerentanan**	**Tingkat Kerentanan**
Owasp-zap	*X-Frame-Options Header Not Set*	*Medium*
	Cross-Domain JavaScript Source File Inclusion	*Low*
	X-Content-Type-Options Header Missing	*Low*

Table 3. Dampak dan Resiko

Jenis Kerentanan	**Resiko**
X-Frame-Options Header Not Set	Owasp-zap mendeteksi bahwa situs *web* bisa beresiko terhadap serangan *clickjacking.*
Cross-Domain JavaScript Source File Inclusion	Owasp-zap mendeteksi halaman mencakup satu atau lebih *file skrip* dari domain pihak ketiga.
X-Content-Type-Options Header Missing	Owasp-zap mendeteksi *content-type header* ada yang hilang. berarti bahwa situs *web* dapat beresiko terkena serangan *sniffing MIME.*

Tabel 4. Solusi dari Kerentanan

Jenis Kerentanan	Solusi
X-Frame-Options Header Not Set	Gunakan *X-Frame Options. x-frame options* ialah sebuah *header* dari *http* yang disebut juga sebagai *header* keamanan *http. header* akan memberi perintah kepada *web browser* ketika *menghandle* konten di dalamnya. alasan utama untuk menggunakan teknik ini adalah untuk memberikan perlindungan dari *clickjacking* dengan tidak mengizinkan *rendering* bingkai pada halaman. ini termasuk *merender* pada <*frame*>, <*iframe*>, atau <*object*> *iframe* digunakan untuk menyematkan dan mengisolasi konten pihak ketiga ke dalam *website*.
Cross-Domain JavaScript Source File Inclusion	Pastikan *file* sumber *JavaScrip*t diambil dari hanya sumber terpercaya, dan sumbernya tidak dapat dikontrol oleh pengguna akhir aplikasi.
X-Content-Type-Options Header Missing	Pastikan bahwa *server* aplikasi/web menetapkan *header* tipe-konten dengan tepat, bahwa *header* jenis opsi-x menjadi 'nosniff' untuk semua halaman *web*.

Kesimpulan dari hasil laporan *scanning* diatas adalah sebagai berikut:

1. Dari hasil laporan *information gathering* didapatkan beberapa port yang terbuka dan ditemukan informasi *DNS* (*Domain Name Server)* yang digunakan *web server* www.divakaraoke.co.id
2. Dari hasil laporan jenis kerentanan ditemukan 3 jenis kerentanan.
   a. *X-Frame-Options Header Not Set,*
   b. *Cross-Domain JavaScript Source File Inclusion,*
   c. *X-Content-Type-Options Header Missing.*
3. Dari hasil laporan dampak dan resiko *webserver* www.divakaraoke.co.id rentan terhadap serangan *clickjacking* dan serangan *sniffing MIME*

KESIMPULAN DAN SARAN

Pada pengujian pencarian *port tcp web server* www.divakaraoke.co.id masih memiliki banyak *port tcp* yang terbuka untuk dieksploitasi hal ini dibuktikan dengan terbukanya 6 *port tcp* yaitu *port* 21, *port* 22, *port* 80, *port* 110, *port* 111, *port* 143. Melalui pengujian menggunakan *owasp-zap webserver* www.divakaraoke.co.id beresiko terhadap serangan *clickjacking* dan *sniffing.* Dari hasil penelitian ini penulis menyatakan tujuan dari penelitian sudah tercapai, yaitu melakukan *penetration testing* menggunakan *kali linux* dapat memberikan informasi tentang kerentanan *web server* diva karaoke.

DAFTAR PUSTAKA

[1] Pangalila, R. 2015. Penetration Testing Server Sistem Informasi Manajemen Dan Website Universitas Kristen Petra. Jurnal Teknologi Informasi. http://publication.petra.ac.id

[2] Messier, R. 2016. Penetration Testing Basics. In Penetration Testing Basics. https://doi.org/10.1007/978-1-4842-1857-0

[3] Bayu, I. 2017. Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO).

[4] Kizza, J. M. 2016. Computer Network Security Fundamentals. https://doi.org/10.1007/978-3-319-55606-2_2

[5] Kadek, N. 2016. Rancang Bangun Sistem Terdistribusi pada Apotek. Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi).

[6] Chapman, C. 2016. Network performance and security: testing and analyzing using open source and low-cost tools. https://www-oreilly-com

[7] Anugrah, I. 2017. Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone. https://doi.org/10.33558/piksel.v5i2.271

[8] Aziz, A. 2015. Analisis Web Server untuk Pengembangan Hosting Server Institusi: Pembandingan Kinerja Web Server Apache dengan Nginx. https://doi.org/10.32722/vol1.no2.2015.pp12-20

[9] Oriyano, S. 2017. Penetration Testing Essentials. In Penetration Testing Essentials. https://doi.org/10.1002/9781119419358

[10] Athaya. 2016. Mastering The Penetration Testing Distribution.

[11] Tarigan, B. 2017. Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer.