Prosiding
ANNUAL RESEARCH SEMINAR 2016
6 Desember 2016, Vol 2 No. 1

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (*PENTEST*)

Yunanri W.[1] , Imam Riadi[2], Anton Yudhana[3]
Magister Teknik Informatika
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
yunanriw@gmail.com[1], S2.imamriadi@mti.uad.ac.id[2], eyudhana@mti.uad.ac.id[3]

Abstrak- Pengujian penetrasi adalah serangkaian kegiatan yang di lakukan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan. Hal Ini akan membantu mengkonfirmasi efektivitas langkah-langkah keamanan yang telah dilaksanakan. Memberikan gambaran tentang pengujian penetrasi. Pembahasan ini membahas mamfaat, strategi dan metodologi melakukan pengujian penetrasi. Metodologi pengujian Penetrasi mencakup tiga fase: persiapan ujian, tes dan analisis tes. Tahap uji coba melibatkan langkah-langkah berikut: pengumpulan informasi, analisis kerentanan, dan kerentanan mengeksploitasi. Penelitian di lakukan untuk menguji pada aplikasi Web server

Kata kunci : Pengujian penetrations,Web server, Keamanan jaringan , Kerentanan

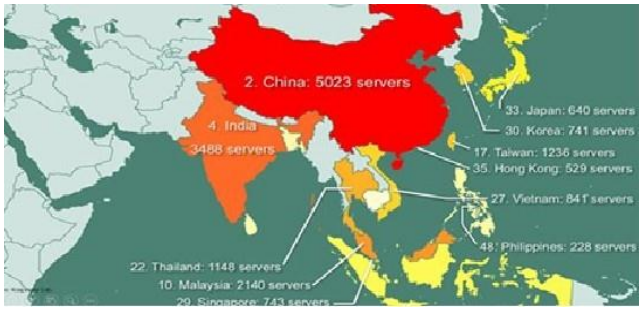
I. PENDAHULUAN

Keamanan sistem informasi adalah salah satu isu utama dalam perkembangan teknologi informasi dan komunikasi saat ini. Selain itu, bisnis penting untuk melindungi aset informasi organisasi dengan mengikuti pendekatan yang konprehensif dan terstruktur untuk memberikan perlindungan dari resiko organisasi yang mungkin di hadapi. Dalam upaya memecahkan masalah keamanan dibutuhkan penerapan metode yang dapat menjamin keamanan data, transaksi, dan komunikasi.

Dengan tidak adanya keamannya pada sistem maka akan banyak para *Hacker* yang dengan mudah dapat mengambil alih sistem yang dibangun. Hal ini menimbulkan keterbukaan untuk mengakses data pribadi maupun data penting sebuah perusahaan atau lembaga yang seharusnya tidak diketahui oleh orang lain. *Hacker* merupakan seseorang yang memiliki kemampuan dalam pemrograman serta jaringan komputer. Seiring pesatnya perkembangan teknologi maka para *Hacker* juga semakin pintar dalam menjalankan pola kegiatan ilegal ini. Dengan kata lain semakin banyak para *Hacker* yang memanfaatkan kelemahan pada sebuah *Web server* untuk mendapatkan keuntungan pribadi maupun organisasi yang dijalankannya. Melihat kondisi ini seharusnya kita dapat mengambil langkah cepat untuk mengamankan Web server dan apabila di abaikan maka web server yang di miliki oleh suatu badan institusi baik milik perintah, swasta, maupun perseorangan dapat mengalami kerugian yang diakibatkan oleh para *Hacker*.

Dalam studi kasus keamanan *web server* ini bertujuan untuk mencari kerentanan atau kelemahan dari sebuah *Web server*, karena banyak sekali para *Hecker* akan mencoba untuk membobol *web server* milik setiap institusi milik pemerintah, institusi swata, maupun perseorangan.

Negara-negara yang *Web servernya* di bobol atau di ambil alih oleh *Hacker* baik sekala nasional maupun Internasional. [1]



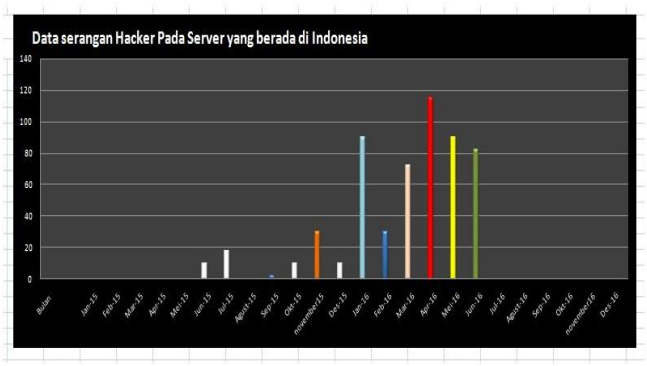
Gambar 1. Data negera-negara yang *server* nya di serang *para Hacker*.

10 Negara terkena dampak dari serangan para, yaitu:

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

- Brazil.
- China.
- India.
- Spanyol.
- Italia.
- Australia
- Afrika
- Malaysia
- Indonesia
- Prancis

Indonesia menduduki peringkat ke-37 dengan 549 *server* dalam daftar *XDedic* pada Mei 2016. Seperti pada gambar 2 [1]



Gambar 2. Sebanyak 549 *server* di Indonesia masuk dalam daftar *XDedic*

Web server memiliki layanan untuk menerima permintaan (*Request*) berupa halaman *web Protokol HTTP* atau *HTTPS* dari *client* yang di kenal dengan *browser* dari sinilah celah yang dapat di susupi oleh seorang *Hacker* tanpa di sadari pemilik *web server*. Hal ini digunakan untuk menargetkan pemilik infrastruktur atau sebagai launch-pad untuk serangan yang lebih luas tanpa disadari sebelumnya.
Indonesia tercatat sebagai negara peringkat 13 yang paling banyak terinfeksi *ransomware* di Asia Tenggara dengan jumlah rata-rata 14 kasus terjadi setiap hari, menurut riset yang dilakukan perusahaan perangkat lunak antivirus *Symantec*. Program jahat yang masuk dalam kategori *ransomware* merupakan sistem kerja dari *Hacker dengan* mengunci data, kemudian melalui notifikasi *Hacker* akan meminta bayaran berupa *Bitcoin* kepada pemilik web server jika menginginkan aksesnya kembali atau pemilik web server harus menunggu layanan dari pihak seperti perusahaan Antivirus untuk membasmi malware dari *ransomware* tersebut.[1]

II. KAJIAN PUSTAKA

Beberapa penelitian sebelumnya melakukan penelitian dengan judul:

a. Penggabungan teknik penetrasi secara manual dengan *tools* yang di miliki oleh sistem operasi (CPAT) oleh Darrien Rushing, Jason Guidry, Ihssan Al Kadi.
b. Teknik Penetrasi *Proxy* jaringan pada Warnet oleh Adam Ghifari Nuskara.
c. Teknik penetrasi pada Portal website kota lubuklinggau oleh Ike Nirmala.

Pada penelitian ini menggunakan metode penetrasi testing atau pencarian kelemahan dari sebuah aplikasi yang digunakan pada *web server*, baik di sebuah institusi pemerintah, institusi swasta, maupun perseorangan. Dengan melakukan penelitian ini dapat diamati pola serangan dari para *Hacker*, serta tindakan yang dapat dilakukan dalam mengamankan *Web server* .

2.1. Pengertian Penetrasi *Testing*

Penetrasi *testing* adalah metode evaluasi keamanan pada sistem komputer atau jaringan dengan mengidentifikasikan kelemahan, *vulnerabilities* dan *the absence of patches*. Identifikasi berupa celah keamanan, konfigurasi *firewall* dan *wireless point.* Simulasi dan identifikasi dilakukan dalam jaringan internal maupun jarak jauh. Tujuannya adalah menentukan dan mengetahui macam-macam serangan yang mungkin dilakukan pada sistem serta akibat yang bisa terjadi karena adanya kelemahan keamanan pada sistem komputer atau jaringan yang dimiliki.[2]

Kerentanan dalam aplikasi *Web server* akan memberikan peluang bagi *hacker* untuk melakukan eksploitasi serangan pada sistem secara bertahap dan tidak menutup kemungkinan sistem yang diserang akan diambil alih sepenuhnya.[3]

Dalam sebuah penetrasi testing, diperlukan batasan-batasan dalam pengujian secara hati-hati untuk menghindari gangguan dan untuk memberikan bukti konsep serangan dapat di lakukan atau tidak, akan tetapi pengujian ini dapat menyebabkan Denial of Service (DOS). Sebaliknya, setelah pengujian destruktif dilakukan dan dipetakan maka serangan Denial of Service dan Buffer Overflow dapat diminimalisir. [4]

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

2.2. Sistem Operasi *BackTrack*

Sistem operasi *BackTrack* seperti yang terdapat pada Gambar 3. Merupakan sistem operasi yang di buat oleh Mati Aharoni, dia seorang yang bekerja sebagai *consulting Security* asal Israel. BackTrack memiliki tools-tools Information Gathering , *Fluxbox* , Exploittations, Vulnerability Assessment dan *auditor security*. *BackTrack* kini menggunakan basis Ubuntu serta , yang memiliki *tools-tools* yang bermamfaat untuk Penetrasi (Pentest).

Menurut Zee Eichel dalam buku nya yang berjudul *Attacking Side With BackTrack*, *BackTrack* merupakan sistem operasi hasil dari kreatifitas para komunitas-komunitas di seluruh negara.[5]

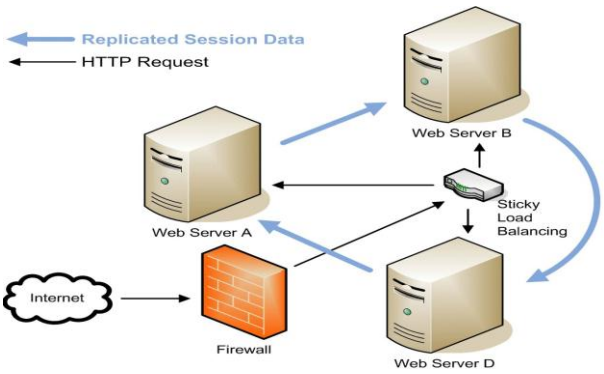
Gambar 3. Sistem Operasi *BackTrack*

BackTrack memiliki *tools* yang dikategorikan dan bisa digunakan dalam melakukan penetrasi *testing, tool-tool* seperti terdapat pada tabel 1

Tabel 1. Penggunaan *tools BackTrack*

Tools yang terkenal dalam *Backtrack* 5	**Kategori dalam *Backtrack* 5**
- *Information Gathering* - *Vulnerability Assessment* - *Exploitation Tools* - *Privilege Escalation* - *Maintaining Access* - *Reverse Engineering* - *RFID Tools* - *Stress Testing* - *Reporting Tools* - *Services* - *Miscellaneous*	- *Networking Exploitation Tools* - *Web Explotation Tools* - *DataBase Explotation Tools* - *Wireless Explotation Tools* - *Social Enginering Tools* - *Physical Explotation* - *Open Source Exploitations*

2.3. Cara kerja atau sitematika penetrasi (pentest) menggunakan *tools BackTrack Linux* yang di tunjukan pada Gambar 4.[6]



Gambar 4. Sistem topologi alur kerja *tools BackTrack*

III. METODOLOGI

3.1. Metodelogi Penelitian

Pada penelitian ini menggunakan metode deskriptif dan kualitatif yang memiliki kemampuan mengimplementasikan dan menggambarkan keadaan atau suatu permasalahan berdasarkan data yang diperoleh dan yang telah dikumpulkan.

3.2. Metode Pengumpulan data

Metode pengumpulan data antara lain :

a. Obsevasi
   Observasi adalah pengumpulan data secara langsung terhadap objek penelitian yang berhubungan dengan judul penelitian
b. Wawancara
   Tujuan dari sebuah wawancara adalah pengumpulan data dengan cara melakukan komunikasi dengan para ahli yang memiliki pemahaman yang mendalam dengan penelitian
c. Studi Pustaka
   Studi pustaka adalah suatu cara pengumpulan data dari sumber sumber tertulis dengan membaca, mempelajari dan mencatat hal hal pengting terkait dengan masalah yang sedang diteliti sehingga diperoleh gambaran yang dapat menunjang penelitian.

3.3. Alat dan Bahan

a. Penelitian ini menggunakan 1 unit laptop dengan sistem operasi untuk penetrasi testing dan sebuah *web server* yang dapat dilihat pada tabel 2 dibawah ini.

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Tabel 2 *hardware* yang digunakan

No	Alat-alat	keterangan
1.	Laptop	1 unit
2.	*Server*	1 unit di ruang control

b. *Software* yang digunakan dalam penelitian antara lain:
   1. Sistem operasi *BackTrack Linux*
   2. Sistem operasi *Windows*

3.4. Demo Penyerangan pada Aplikasi *Web server*

Teknik yang di gunakan dalam simulasi serangan pada *web server* antara lain yaitu: *Reconnaissance*, *Scanning*, *Gaining Access*, *Maintaining Access* dan *Clearing Tracks.* Seperti yang ditunjukan pada Gambar5. [7]

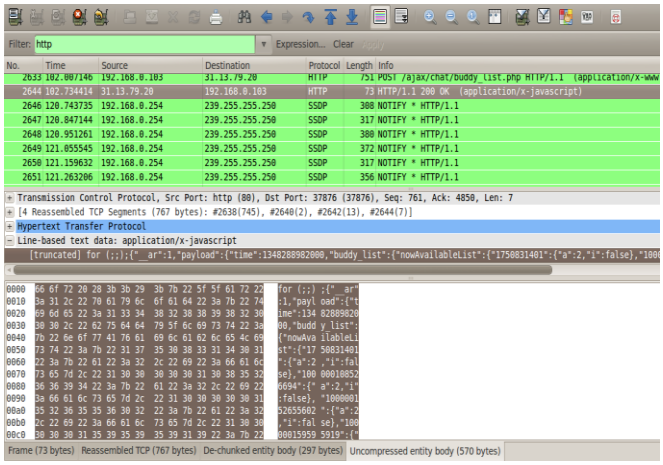
Gambar 5. Bentuk pola dari teknik penetrasi *reconnaissance* untuk tahap awal sistem bekerja sampai *Clearning Track*

A. *Login backtrack*

Langkah awal masuk pada Sistem Operasi *Backtrack* adalah menggunakan *username default root*, sedangkan berjalan *password default* adalah *toor*. Kemudian setelah *login* kita masukan perintah *startx* untuk memulai *Backtrack Graphics Interfaces*.[8]

B. *Scanning* atau mencari

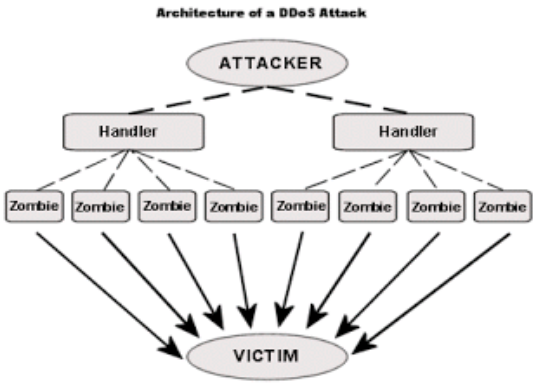
Scanning merupakan salah satu teknik yang bertujuan untuk mengenal karakteristik dari sistem yang menjadi target, teknik ini dapat dilihat pada Gambar 6 [9]



Gambar 6. Proses *Scanning Hypertext Protocol*

C. *Gaining Access*

Gaining Access merupakan teknik mencari *Password* untuk membobol sistem untuk mendapatkan hak akses terhadap sistem. Seperti yang terlihat pada gambar 7.[9]



Gambar 7. Lankah pembobolan *Password*

D. *Maintaining Access*

Eksploitasi yang dilakukan oleh *Attacker* biasanya akan menanamkan *shell* didalam sistem targetnya dengan cara mencari dan mendapatkan *Backdoor*. *Shell* inilah yang ditinggalkan oleh *hacker* yang memiliki tujuan agar dapat melakukan akses kapan saja dengan meninggalkan shell melalui celah-celah yang terdapat pada sistem *web server*. Setelah mendapatkan dan menanampak *shell* hacker akan dengan mudah mendapatkan akses terhadap sistem.[9]

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

E. *Clearing Track*

Clearing track adalah aktivitas penghapusan jejak. Tujuannya agar tidak bisa terlacak oleh *IT Security*. Selain membutuhkan sumber daya yang tidak sedikit, diperlukan pula pengetahuan dan keahlian dalam hal ini. Dengan menerapkan teknik ini membuat berbagai jenis kejahatan *hacking* di webserver jarang sekali terungkap. Adapun modus *hacker* dalam melakukan serangan pada *webserver* menggunakan pola yang beragam, teknik yang di gunakan oleh para *hacker*, misalnya teknik *steganography, tunneling, log filealtering*, dan masih banyak lagi [9]

Manfaat yang diperoleh dengan melakukan simulasi dan identifikasi kengamanan *web server* adalah agar terhindar dari serangan *hacker* dan untuk meminimalisir celah-celah keamanan dan kerentanan pada sistem *web server* [10]

IV. HASIL DAN PEMBAHASAN

4.1. Untuk prosedur atau langkah kerja pada penelitian ini dapat dijabarkan secara singkat sebagai berikut :

- Memetakkan pola serangan dengan memanfaatkan tool yang terdapat pada sistem operasi *BackTrack*.
- Melakukan *reconnaissance* yaitu *information gathering* terhadap sistem yang digunakan pada sebuah *web server.*
- Melakukan *scanning* bertujuan untuk mengenal karakteristik yang di gunakan pada *web server*
- Melakukan teknik *gaining access* yang bertujuan untuk mendapatkan *username* dan *password* yang di gunakan pada *web server*
- Melakukan teknik *maintaining access* yang bertujuan untuk memberikan akses tersendiri kepada *hacker* kapan pun terhadap sistem *web server* dengan cara menanamkan *shell.*
- Melakukan *clearing track* bertujuan untuk menghapus jejak pada *web server.*

DAFTAR PUSTAKA

[1] http://tekno.liputan6.com/read/2534918/459-server-indonesia- diperjualbelikan-hacker-di-pasar-gelap waktu :jam 18:45 WIB tanggal 19 juni 2016

[2] Ankita Gupta, Kavita, kirandeep Kaur. *"Vulnerability Assessment and Penetration Testing". Computer Science Department, PEC University of Technology,India *Electronics and Electrical Communication Depertement, PEC University of Technology, India IJETT Vol 4 Issue3 -2013*

[3] Imam Riadi, Eddy Irawan Aristianto. "*An Analysis of Vulnerability Web Against Attack Unrestricted Image File Upload".* CEA (*Computer Engineering and Aplications*) *Departement of Information System*, Universitas Ahmad Dahlan. 2016

[4] Richard Pangalila, Agustinus Noertjahyana, Justinus Andjarwirawan, "*Penetrasi Testing Server* Informasi Manajemen dan *website* Universitas Kristen Petra", *Jurnal Infra, Vol 3, No* 2. 2015

[5] *Zee Eichel judul ASWB v.2 (Attacking Side With BackTrack). IBT tiemRevolution.* hal 8, Indonesia 2013

[6] Danang Heriyadi. "P*rivate Training X-Code"*. Diakses pada 10 November 2016, diambil dari https://www.scribd.com

[7] *Ravi Kumar "Penetrations Testing & Hacker Toolbox Amplify Mindware" DITM 2013*

[8] Hadi Zayandehroodi, Azah Mohamed, Hussain Shareef. "*A Novel protection Coordination Strategy Using backTrack Algorithm for Distribution System With high Penetration of DG" IEEE june 2012*

[9] *Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982]*.

[10] *Darrien rushing, Jason Guidry, Ihssan Alkadi "Collaborative Penetation-Testing and Analysis Toolkit" IEEE Aerospace Conference 2015.*