IMPLEMENTASI TEKNIK HACKING WEB SERVER DENGAN PORT SCANNING DALAM SISTEM OPERASI KALI LINUX

Muhammad Rizqi Rusydianto[1], Edy Budiman[2], Hario Jati Setyadi[3]

Program Studi Teknik Informatika , Jurusan Teknologi Informasi Dan Komunikasi, Universitas Mulawarman,
Jl. Panajam Kampus Gunung Kelua, Samarinda, 75123 Kalimantan Timur
E-Mail: ekirisky6@gmail.com [1)], edibudiman.unmul@gmail.com [2)], hario.setyadi@gmail.com [3)]

ABSTRAK

Port Scanning merupakan sebuah teknik hacking dimana seorang penyerang dapat membobol website atau web server melalui port yang trerbuka untuk dieksekusi. Berdasarkan data dari Pemerintah Meksiko, Amerika Serikat dan Rusia pada tahun 1999-2013, yang melakukan survey mengenai ancaman cybercrime yang sering terjadi pada Port Scanning, carding, Hacking Web Site, dan penyadapan transmisi maka Teknik Port Scanning adalah bug yang kedua paling banyak ditemukan di pada website-website yang berada di Internet. Penelitian ini bertujuan untuk: 1) Bagaimana menguji sistem keamanan web server yang vulnerable open port. Penelitian ini menggunakan metode penelitian kuantitatif berupa eksperimen dimana peneliti menggunakan metode analisis hasil penelitian dengan melakukan penyerangan langsung ke *web server* target. Pengumpulan data dilakukan dengan cara: 1) studi pustaka, 2) studi lapangan. Dalam membuat media pembelajaran ini peneliti menggunakan motode *Network Development Life Structure*. Hasil dari penelitian ini yaitu memudahkan memudahkan admin suatu web server untuk menguji dengan mudah apakah kemungkinan mempunyai celah port yang terbuka atau tidak dan segera menangani masalah yang dihadapi. Dengan demikian tutorial ini memudahkan untuk memeriksa web server apakah mempunyai celah agar dapat segera memperbaikinya dan tidak terjadi pencurian data-data penting dari web server yang di kelola.

Kata Kunci : *Hacking, Kali Linux, Nmap*

1. PENDAHULUAN

Keamanan jaringan komputer sebagai bagian dari sebuah sistem yang sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Perkembangan teknologi informasi yang semakin cepat dengan berbagai macam fungsi dan kebutuhan, menuntut meningkatnya kualitas keamanan jaringan. Terutama dengan semakin terbukanya pengetahuan hacking dan cracking, didukung dengan banyaknya tools yang tersedia dengan mudah dan banyak pula yang gratis, semakin mempermudah para intruder dan attacker untuk melakukan aksi penyusupan ataupun serangan. Pencegahaan yang paling sering dilakukan untuk masalah ini adalah dengan menempatkan seorang administrator. Seorang administrator bertugas untuk mengawasi dan melakukan tindakan reventif ketika terjadi aksi penyusupan dan serangan

Pengertian Server adalah Sebuah system komputer yang menyediakan berbagai jenis layanan yang dapat diakses oleh komputer client yang sedang terhubung pada sebuah jaringan. Server harus didukung dengan baik oleh prosesor dan juga Memori/RAM yang lumayan besar. Server juga harus memiliki System Operasi Kusus atau biasa juga disebut sebagai System Operasi Jaringan.

Belakangan ini berkembang berbagai cara untuk menghack suatu web server tergantung dengan kelemahan dari komputer server tersebut. Salah satu dengan cara hacking web Port Scanning. Port Scanning merupakan teknik web hacking yang sangat populer, bagaimana tidak? Berdasarkan data dari Pemerintah Meksiko, Amerika Serikat dan Rusia pada tahun 1999-2013, yang melakukan survey mengenai ancaman cybercrime yang sering terjadi pada Port Scanning, carding, Hacking Web Site, dan penyadapan transmisi maka Teknik Port Scanning adalah bug yang kedua paling banyak ditemukan di pada website-website yang berada di Internet. [1]. Keamanan komputer digunakan untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. Keamanan komputer yang dimaksud adalah keamanan sebuah komputer yang terhubung ke dalam sebuah jaringan [2]. Jaringan komputer setiap terminal yang terhubung ke dalamnya punya kemampuan untuk saling berkomunikasi. Data dari setiap pengguna dapat disalurkan memalui media transmisi yang tersedia. Data tersebut dapat bersifat umum dan dapat juga bersifat rahasia. [3]. Web server merupakan tulang belakang dari World Wide Web, web server adalah sebuah perangkat lunak server yang berfungsi melayani koneksi tranfser data dalam protokol Hyper Text Transfer Protocol atau Hyper Text Transfer Protocol Secure dari client melalui web browser dan mengirimkan kembali hasilnya dalam

*Corresponding Author

bentuk halaman-halaman web yang umumnya berbentuk dokumen PHP/HTML [4]. TCP/IP adalah sekumpulan protokol yang terdapat di dalam jaringan komputer (network) yang digunakan untuk berkomunikasi atau bertukar data antar komputer. TCP/IP merupakan standard protokol pada jaringan internet yang menghubungkan banyak komputer yang berbeda jenis mesin maupun sistem operasinya agar dapat berinteraksi satu sama lain [5]. Troll terinspirasi oleh trolling konstan dari mesin dalam laboratorium OSCP (Offensive Security Certified Proffesional). Troll adalah sebuah WebServer yang mengacu pada proses instalasi, penyerangan, hingga perbaikan itu sendiri. [6]. Netdiscover merupakan sebuah tool yang dapat digunakan untuk proses scanning dalam pencarian IP [7]. Nmap merupakan sebuah tool yang dapat digunakan untuk melakukan port scanning. [8]. Kali Linux merupakan pembangunan kembali BackTrack Linux secara sempurna. Jika dulunya Backtrack dibuat berdasarkan sistem operasi ubuntu, kini Kali Linux menggunakan Debian sebagai sistem operasinya. Semua infrastruktur baru telah dimasukkan ke dalam satu tempat, semua tools telah direview dan dikemas [9].

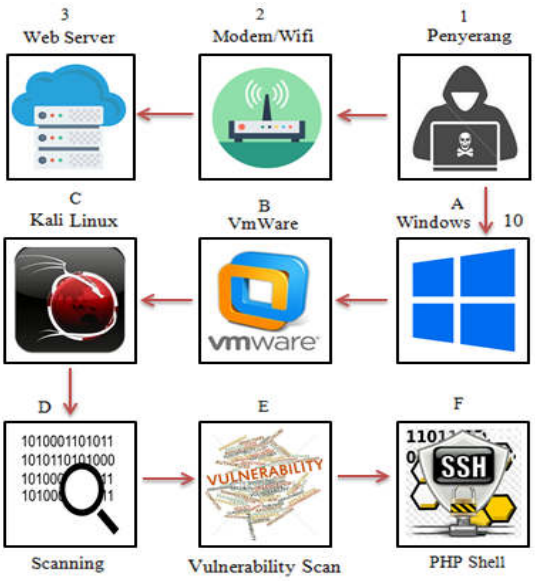
Berdasarkan uraian di atas maka rumusan masalah yang dapat diambil dari penelitian ini, yaitu: Bagaimana cara melakukan hacking dengan port scanning terhadap web server yang vulnerable.
Tujuan dari penelitian ini yaitu: 1) Bagaimana menguji sistem keamanan web server yang vulnerable ftpopen port.

Manfaat dari penelitian ini yaitu: 1) Bagi Penulis, Mengaplikasikan ilmu, wawasan dan pengalaman yang telah diperoleh selama menempuh pendidikan di Perguruan Tinggi dengan membuat laporan penelitian secara ilmiah dan sistematis. 2) Bagi Pembaca, Mengetahui dan memahami implementasi dari setiap proses hacking web server yang vulnerable ftp open port. 3) Bagi Administrator, Terbantu dalam mengetahui kelemahan dari server sehingga mengetahui bagaimana cara penanganannya.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kuantitatif berupa eksperimen dimana peneliti menggunakan metode analisis hasil penelitian dengan melakukan penyerangan langsung ke web server target. Pengumpulan data dilakukan dengan cara: 1) studi pustaka, dengan membaca dan mempelajari buku-buku, laporan penelitian, jurnal yang mendukung penelitian ini, 2) studi lapangan, dengan penyerangan langsung ke web server target. Dalam membuat media pembelajaran ini peneliti menggunakan motode Network Development Life Structure dengan tahapan-tahapan antara lain : 1) scanning, 2) analisis, 3) desain, 4) simulasi, 5) implementasi.

2.1 Design (Perancangan)



Gambar 1. Perancangan Alur Penyerangan

1) Berikut penjelasan dari gambar perancangan alur penyerangan di atas:
2) Penyerang, komputer menggunakan Windows 7 yang di dalam ada VMWare untuk menginstall Kali Linux.
   a. Windows 10, adalah Operating System yang digunakan oleh penyerang yang di Install VMWare.
   b. VMWare, adalah alat yang digunakan untuk menginstall Kali Linux di Operating System Windows 10.
   c. Kali Linux, adalah alat untuk Operating System yang di install di dalam VMWare yang digunakan untuk melakukan hacking terhadap web server target.
   d. Scanning, adalah prosesyang digunakan untuk melakukan pencarian alamat dari target yang akan dilakukan penyerangan.
   e. Vulnerability Scan, adalah proses yang digunakan untuk mencari celah kelemahan dari suatu server.
   f. PHP reverse shell, alat ini adalah shell interaktif yang tepat dimana kita dapat menjalankan program interektif seperti telnet, ssh dan su.
3) Modem, sebagai alat bantu koneksi jaringan agar kita dapat melakukan aktivitas hacking terhadap web server.
4) Server, menggunakan komputer berbasis Ubuntu 14.04.1 yaitu Troll dan sebagai objek target dalam simulasi penyerangan.

3. HASIL DAN PEMBAHASAN

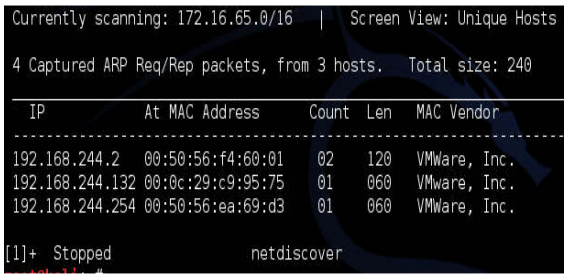
3.1 Hasil

Penelitian ini dilakukan untuk memudahkan admin suatu web server untuk menguji dengan mudah apakah kemungkinan mempunyai celah port yang terbuka atau tidak dan segera menangani masalah yang dihadapi.

3.2 Pengujian

Dalam penelitian ini, sudah dijelaskan mengenai metode pengujian Port Scanning pada web server.

3.2.1 Tampilan Web Server



Gambar 2. Scanning IP

Pada Gambar 2 merupakan tampilan saat melakukan Scanning IP. Jadi pertama penulis memasukkan perintah "Netdiscvoer". Perintah ini ialah untuk mengecek ip manakah yang digunakan pada Web Server yang akan di serang. Setelah melakukan proses Scanning di temukan IP "192.168.244.132" yang meruapakan IP Target yang akan di serang.

3.2.2 Vulnerable Scanning

Pada Gambar 3 pada langkah ini, penulis akan mengecek apakah web tersebut memiliki vulnerable atau tidak. Jadi penulis memasukkan perintah "nmap –T4 –sS 192.168.244.132 -p-". Perintah "nmap –T4 –sS 192.168.244.132 -p-" adalah untuk mengecek vulnerable yang terdapat di dalam web server. Fungsi dari perintah –T4 ialah untuk menaikkan kecepatan dari scanning, sedangkan –sS merupakan type scanning TCP SYN scan yang dipergunakan untuk mendeteksi port apa saja yang terbuka atau biasa disebut scan yang tidak terdeteksi, dan –p ialah untuk memeriksan port tertentu.

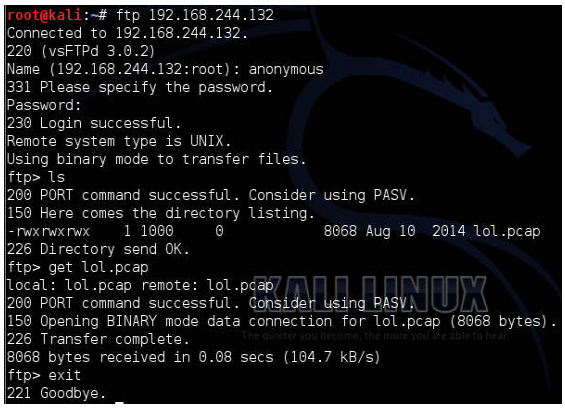
Gambar 3. Vulnerable Scanning

Pada Gambar 3 pada langkah ini, penulis akan mengecek apakah web tersebut memiliki vulnerable atau tidak. Jadi penulis memasukkan perintah "nmap –T4 –sS 192.168.244.132 -p-". Perintah "nmap –T4 –sS 192.168.244.132 -p-" adalah untuk mengecek vulnerable yang terdapat di dalam web server. Fungsi dari perintah –T4 ialah untuk menaikkan kecepatan dari scanning, sedangkan –sS merupakan type scanning TCP SYN scan yang dipergunakan untuk mendeteksi port apa saja yang terbuka atau biasa disebut scan yang tidak terdeteksi, dan –p ialah untuk memeriksan port tertentu.

Gambar 4. Tampilan Web Troll

Pada Gambar 4 merupakan tampilan hasil database dari vulnerable scanning. Di sini terdapat lima informasi yang terdapat dari database web tersebut.

3.2.3 Scanning Open Port



Gambar 5. Scanning Open Port

Pada Gambar 4 merupakan tampilan scanniing untuk melihat vulnerable yang terdapat didalam ftp, di mana terlebih dahulu memasukkan perintah "ftp 192.168.244.132" fungsi perintah ini adalah untuk melihat versi ftp yang digunakan yaitu vsFTPd, setelah itu ketikkan perintah "anonymous" untuk login ke dalam system. Anonymous sendiri ialah id default yang terdapat di dalam system. Lalu memasukkan password secara random, kemudian ketikkan perintah "ls" untuk melihat isi directory yang didalamnya terdapat file yang tersedia bernama lol.pcap. Kemudian memasukkan perintah "get lol.pcap" fungsi perintah ini ialah untuk mendownload paket tersebut.

Gambar 6. Pengecekan File Lol.Pcap

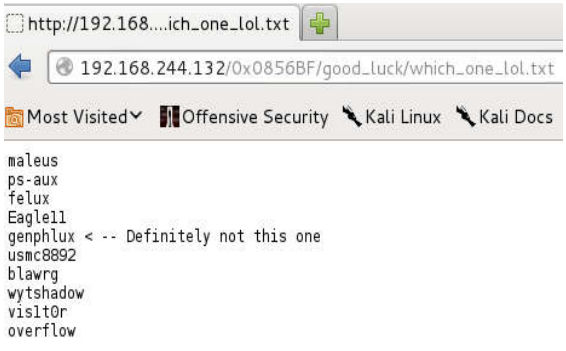
Pada Gambar 6 merupakan tampilan vulnerable yang terdapat didalam file lol.pcap. utnuk melihat isi file tersebut dengan memasukkan perintah "strings lol.pcap" yang didalamnya berisi berbagai infomasi seperti, jenis ftp yang digunakan, nama user, dan juga terdapat file bernama secret_stuff.txt. Di mna di dalam file tersebut terdapat teks yang berisi informasi ke sup3rs3cr3tdirlol kemudian data ini akan dimasukkan ke dalam url untuk melihat apakah terdapat informasi didalamnya.

Gambar 7. Hasil Pengecekan

Pada Gambar 7 diatas merupakan tampilan hasil pengecekan sebelumnya yang didalamnya juga terdapat sebuah file bernama roflmao. Setelah itu download file tersebut dan melakukan analisis untuk melihat informasi di dalam file tersebut.

Pada Gambar 8 dibawah merupakan tampilan untuk melihat isi dari file roflmao dengan memasukkan perintah "strings roflmao". yang setelah di analisis ternyata di dalam file tersebut terdapat sebuah address "0x0856BF" yang kemudian akan di lakukan pengecekan di browser

Gambar 8. Pengecekan File roflmao



Gambar 9. Hasil Pengecekan File Roflmao

Gambar 10 Isi Dari Folder good_luck

Gambar 1. Isi File which_one_lol.txt

Pada Gambar 8 merupakan tampilan hasil dari pengecekan file roflmao yang di dalamnya terdapat 2 folder dan akan di lakukan pengecekan lebih lanjut untuk melihat apakah di dalam folder tersebut terdapat sebuah informasi atau tidak. Pada Gambar 9 merupakan tampilan hasil dari pengecekan folder good_luck yang di dalamnya terdapat sebuah file which_one_lol.txt. Pada Gambar 10 merupakan isi dari file which_one_lol.txt yang di dalamnya berisikan beberapa id.

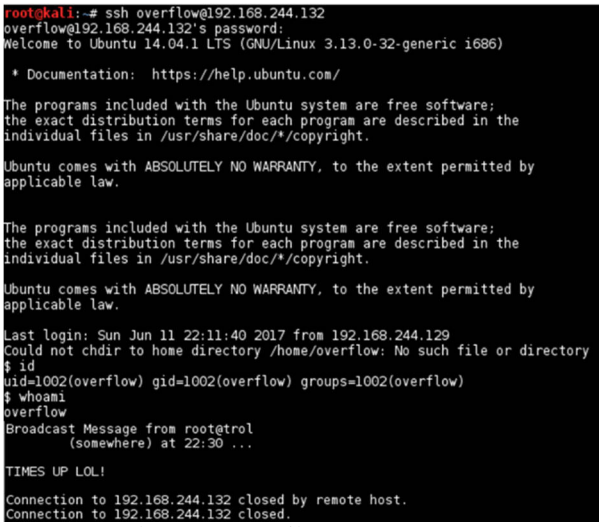
Gambar 12. Isi File Dari Folder this_folder_contains_the_password

Pada Gambar 12 merupakan tampilan hasil daripengecekanfolderthis_folder_contains_ the password kemudian di dalam folder tersebut sebuah file Pass.txt .

Gambar 23. Isi File Pass.txt

Pada Gambar 13 merupakan isi dari file Pass.txt yang di dalamnya terdapat sebuah password yang bernama Good_job_:).

3.2.4 SSH

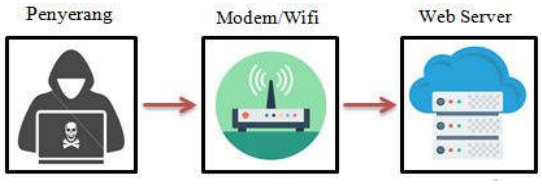


Gambar 34. Tampilan Program SSH

Pada Gambar 13 merupakan tampilan ssh dan di sini kita login sebagai overflow dengan password Pass.txt. Di server ini dapat di amati bahwa target menggunakan Ubuntu Server 14.04.1 lalu terdapat waktu dan tanggal login terakhir. Setelah itu penulis melakukan pengecekan identitas remote server apakah benar berhasil atau tidak dengan cara mengetikan "id" lalu tampil overflow lalu memasukkan perintah selanjutnya yaitu "whoami" fungsinya ialah untuk mengetahui siapa identitas yang login dan muncul overflow, setelah tidak ada lagi dilakukan pengecekan maka system akan mengeluarkannya secara otomatis.

4. ANALISA PENELITIAN

Pada tutorial ini kita mempelajari Teknik Hacking Web Server dengan Port Scanning di Kali Linux. Dalam pengujian ini, penyerang menggunakan Windows 7 dan VMWare yang telah di install Kali Linux. Kemudian, penyerang menggunakan modem/wifi untuk mengkoneksikan ke jaringan internet dan mengeksekusi web server target Netdiscover, Nmap, PHP.



Gambar 15. Alur Penyerangan Web Server

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dalam pengujian sistem keamanan web server yang vulnerable ftp open port terdapat lubang keamanan yang dapat digunakan oleh penyerang untuk melakukan penetrasi pada web server.

5.2 Saran

Dalam tutorial teknik *hacking web server* dengan *Port Scanning* di *Kali Linux* ini, penulis menyarankan agar dapat digunakan secara maksimal sesuai fungsinya sebagai alat penguji *web server* yang *vulnerable* terhadap *SQL Injection.* Berikut ini beberapa saran bagaimana kita bisa menghadapi serangan *Open Port Scanning*: 1) *Menonaktifkan* tampilan kesalahan 2) Gunakan *firewall website*. 3) Menggunakan *source code* yang ditulis dengan baik dan teruji. 5) selalu melakukan peninjauan keamanan aplikasi sebelum menggunakannya.

6. DAFTAR PUSTAKA

[1]. Unggul, STIKOM Insan. *Eptik Carding dan Port Scanning.* n.d. http://ulwishome.blogspot.co.id/2016/12/tugas-makalah-eptik-carding-dan-port.html (accessed Mei 29, 2017).

[2]. Hartiwati, Ertie Nur. "Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet." *Jurnal Ilmiah Informatika Komputer* , 2014: Vol 19, No 3 .

[3]. Kristanto, Andri. "Sistem Keamanan Data Pada Jaringan Komputer." *Magistra*, 2007: Vol 19, No 60.

[4]. Widodo, Andrias Suryo. "Eksploitasi Celah Keamanan Piranti Lunak Web Server Vertrigoservpada Sistem Operasi Windows Melalui Jaringan Lokal." *Prosiding KOMMIT* , 2017: 591/514.

[5]. Syafrizal, Melwin. "TCP/IP." *Networking*, 2010: 4481..

[6]. Overflowsecurity. *overflowsecurity-troll.* n.d. http://overflowsecurity.com/?p=70 (accessed Juni 14, 2017).

[7]. IBTeam. *Attacking Side With Backtrack.* n.d. https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwjJ74GGspTUAhWDyRoKHTOuDbEQFgg8MAM&url=http%3A%2F%2Frepo.unnes.ac.id%2Fdokumen%2Fpentest_hacking%2FASWB.v2.pdf&usg=AFQjCNHNk9RwS

NdtkUzc6gJdL46A7io-qQ&sig2=fHgrSZFQh (accessed Mei 29, 2017).

[8]. BB Halib, E Budiman, HJ Setyadi. " Teknik Hacking Web Server Dengan Sqlmap Di Kali Linux " : 2017: Jurnal Rekayasa Teknologi Informasi 1 (1), 67-72.

[9]. Aulia Rahman & Haviluddin. 2016. *Implementation of Bandwidth Management Authentication*. IJCANDI - International Journal of Computing and Informatics. ISSN: 2502-2334. Vol. 1, No. 1, February 2016. Pg. 1-8.