JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1768-1775

Analisis Kerentanan Web Server Metasploitable Menggunakan Metasploit Framework

Fazar Maulana[1], Muhamad Rayhan[2], Dion Nathanael Hutapea[3], Muchammad Ricky Alamsyah[4], Saprudin[5*]

[1,2,3,4,5]Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1]zarmaull179@gmail.com, [2]mraihanfatur21@gmail.com,[3]dion_hutapea12@gmail.com, [4]rikialamsyah48@gmail.com,[5*]dosen00845@unpam.ac.id
(* : coressponding author)

Abstrak − Keamanan adalah elemen krusial yang perlu diperhatikan saat mendirikan saat mendirikan sebuah server web. Pengujian penetrai merupakan suatu kegiatan yang sah dan resmi yang bertujuan untuk memperkuat perlindungan perlindungan sistem informasi, baik di dalam konteks akademis maupun lingkungan bisnis. Penelitian ini memanfaatkan Metasploit Framework sebagai instrumen utama dalam melaksanakan pengujian penetrasi terhadap server Metasploitable2. Metode yang diterapkan mencakup pengumpulan informasi (*information gathering),* analisis (*scanning),* penilaian kerentanan (*vulnarablity assessment),* eksploitasi (*exploitation),* pembersihan jejak (*cleanup),* pelaporan (*reporting).* Temuan dari penelitian ini mengidinkasikan bahwa di web server terdapat celah keamanan yang bervariasi dalam tingkat kerentanan yaitu tinggi *(critical),* sedang *(medium risk)* dan rendah *(low risk).* Selama proses penelitian ini, terindifikasi sejumlah port yang terbuka pada server web, yang memberikan keluasaan bagi peretas untuk masuk ke dalam sistem dan memanfaatkan data yang terdapat didalamnya. Dengan menggunakan simulasi ini, Metasploit Framework berhasil dimanfaatkan untuk mengeksploitasi celah keamanan, yang mengakibatkan pengambilan username dan password dari sistem yang diuji.

Kata Kunci: Web Server; Eksploitasi; Kerentanan Sistem; Metasploit Framework

Abstract *- Security is a crucial element to consider when setting up a web server. Penetration testing is a legitimate and authorized activity that aims to strengthen the protection of information system protection, both in the context of academic and business environments. This research utilizes the Metasploit Framework as the main instrument in carrying out penetration testing against Metasploitable2 servers. The methods applied include information gathering, scanning, vulnarablity assessment, exploitation, cleanup, and reporting. The findings of this research indicate that there are security gaps in web servers that vary in vulnerability levels of high, medium and low. During the process of this research, a number of open ports on the web server were identified, which gives hackers the flexibility to enter the system and utilize the data contained therein. Using this simulation, the Metasploit Framework was successfully utilized to exploit the security holes, resulting in the retrieval of usernames and passwords from the tested system..*

Keywords*: Web Server; Penetration Testing; Exploitation; Metasploit Framework*

1. PENDAHULUAN

Seiring dengan meningkatnya jumlah data yang ditransmisikan melalui internet, keamanan siber menjadi masalah yang sangat penting. Sesuai dengan persyaratan keamanan nasional dan internasioanl, perusahaan dan organisasi harus menjaga kerahasiaan, keamanan dan integritas server web mereka. Karena ketergantungan masyarakat terhadap sistem informasi berbasis internet *(online)* terus meningkat, keamanan sistem harus terus dipantau dan ditingkatkan.

Berbagai metode, seperti metode atau cara Suricata (Nazwita, 2017) dan SSE-CMM ISO 27002, telah diteliti sebelumnya untuk mengevaluasi keamanan server web. Selain itu, sistem yang tidak berfungsi (Setiawan et al., 2016). Web server *Metasploitable2* dipilih sebagai objek pengujian untuk penelitian ini karena strukturnya mirip dengan sistem yang digunakan oleh perusahaan, organisasi dan lembaga pendidikan. Sistem informasi sering menjadi sasaran pembobolan, yang daoat menghancurkan data penting seperti transaksi, data keanggotaan, akademik atau keputusan strategis. Seringkali pintu belakang *(backdoor)* dipasang yang dapat digunakan oleh orang yang tidak berwenang untuk mengganggu sistem.

Pengujian penetrasi dianggap sebagai metode terbaik untuk mengevaluasi status keamanan data organisasi. Peneliti keamanan dapat menemukan masalah baru dengan strategi ini (Zeebare et al., 2020). Data menunjukan bahwa, meskipun Indonesia tidak berada diantara 10 negara dengan

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1768-1775

pelanggaran data tertinggi, negara ini masih mengalami trend kebocoran data. Beberapa peristiwa besar yang melibatkan lembaga pemerintahan, bisnis e-commerce, dan penyedia layanan swasta harus bekerja sama untuk mengembangkan rencana dan sistem keamanan siber karena adopsi teknologi digital yang cepat.

Penelitian ini bertujuan untuk mengeksplorasi kelemahan dan kerentanan server web *Metasploitable2* melalui pengujian penetrasi. Selain itu, ancaman yang mungkin terjadi pada keamanan sistem informasi akan diperiksa dan saran akan dibuat tentang carra memperkuat perlindungan data dan integritas sistem. Penelitian ini diharapkan dapat membantu meningkatkan standar keamanan web server, terutama di Indonesia.

2. METODE

2.1 Jenis Penelitian

Pendekatan yang digunakan pada penelitian ini adalah eksperimental dengan memanfaatkan Metasploitable2 untuk melaksanakan uji penetrasi secara menyeluruh pada webserver dan menilai tingkat kerentanan. Melalui serangkaian uji penetrasi, penelitian ini bertujuan mengidentifikasi, mengeksploitasi dan menganalisis celah keamanan potensial, serta memberikan rekomendasi langkah pencegahan yang efektif untuk meningkatkan sistem.

2.2. Metode yang digunakan

Metode yang diterapkan dalam penelitian ini adalah pendekatan uji penetrasi untuk mendeteksi kerentanannya pada server web. Pendekatan ini mensimulasikan serangan untuk menguji seberapa efektif pertahanan server web Metasploitable2 terhadap potensi ancaman. Penetration testing yang dilakukan bersifat manual dan otomatis, menggunakan berbagai alat untuk memindai dan mengeksploitasi celah-celah keamanan.

2.3 Tahapan Penelitian

Tahap pengujian penetrasi merupakan tahap pengujian berupa serangan secara terus menerus terhadap suatu sistem informasi (I Gede Ary Suta Sanjaya & Gusti Made Arya Sasmita 2020) menyampaikan pendapat mereka. Penelitian ini diawali dengan kajian literatur terkait metode pengujian yang relevan, kemudian dilanjutkan dengan simulasi pengujian kerentanan pada *web server Metasploitable*. Penelitian dilakukan dalam lingkungan virtual menggunakan VirtualBox dengan sistem operasi Kali Linux 2023.4. Target pengujian adalah *web server Metasploitable2*, Dengan uraian perangkat keras *(hardware*) dan perangkat lunak *(software)* yang kami gunakan sebagai berikut:

Tabel 1. *Hardware*

Nama	Keterangan Spesifikasi
Laptop Acer Aspire 3	- Processor i3-1115G4 - Ram 6gb ddr 4 - SSD 256gb

Tabel 2. *Software*

No	Nama Tools	Fungsi
1	Kali Linux	Operating System
2	Nmap	Information Gathering
3	Metasploit	Exploitation Framework

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1768-1775

Teknik yang digunakan pada simulasi serangan yaitu :

Gambar 1. Tehnik Penetration Testing

a. *Information Gathering*

Pada tahap ini, dilakukan pengumpulan informasi dasar mengenai web server, seperti alamat IP dan nama domain, menggunakan alat seperti Nmap dan WHOIS.

b. *Scanning dan Vulnerability*

Pemindaian dilakukan untuk mendeteksi kerentanan dengan menggunakan alat seperti Nmap atau Nuclei. Alat ini digunakan untuk mengidentifikasi port terbuka dan layanan yang rentan pada server.

c. *Exploitation*

Setelah kerentanan ditemukan, tahap eksploitasi dilakukan untuk menguji apakah celah tersebut dapat dimanfaatkan menggunakan tools seperti Metasploit, yang memungkinkan pengaksesaan atau perusakan sistem target.

d. *Reporting*

Setelah eksploitasi, laporan disusun mengenai temuan kerentanan dan rekomendasi mitigasi untuk memperbaiki masalah yang ada pada server

3. ANALISA DAN PEMBAHASAN

3.1 Instalasi Lingkungan Pengujian

Penelitian ini dilakukan dalam lingkungan laboratorium yang disimulasikan menggunakan VirtualBox sebagai platform virtualisasi. Lingkungan ini terdiri dari dua mesin virtual, yaitu ***Metasploitable2*** sebagai target pengujian (web server) dan ***Kali Linux*** sebagai mesin untuk menjalankan penetration testing.

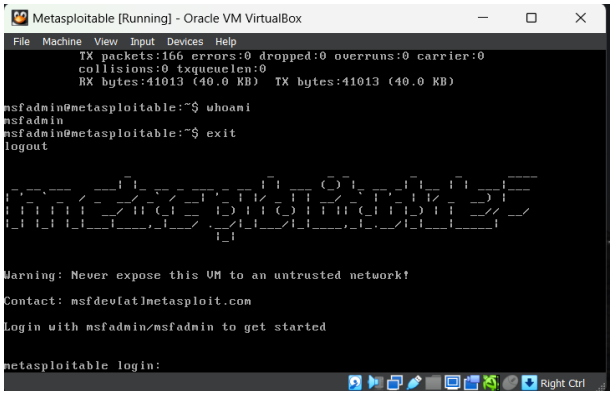
3.1.1 Instalasi Metasploitable

a. unduh file iso melalui link berikut https://sourceforge.net/projects/metasploitable/

b. Buat host baru pada virtualbox dengan nama Metasploitable2, pilih Linux (Ubuntu 32-bit) sebagai sistem operasi, tetapkan ram 512Mb, dan tentukan hard disk 8Gb.

c. Ubah pengaturan jaringan menjadi Host-Only Adapter agar mesin ini hanya terhubung dengan mesin virtual Kali Linux.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1768-1775



Gambar 2. Tampilan Metasploitable

3.1.2 Instalasi Kali Linux

a. Unduh file iso melalui link berikut *https://www.kali.org/*

b. Buat host baru pada virtualbox dengan nama Kali Linux, pilih Linux (Debian 64bit) sebagai sistem operasi, tetapkan ram 2048Mb, dan tentukan hard disk 20Gb.

c. Ubah pengaturan jaringan menjadi Host-Only Adapter agar mesin ini hanya terhubung dengan mesin virtual lainnya.

Gambar 3. GUI Kali Linux

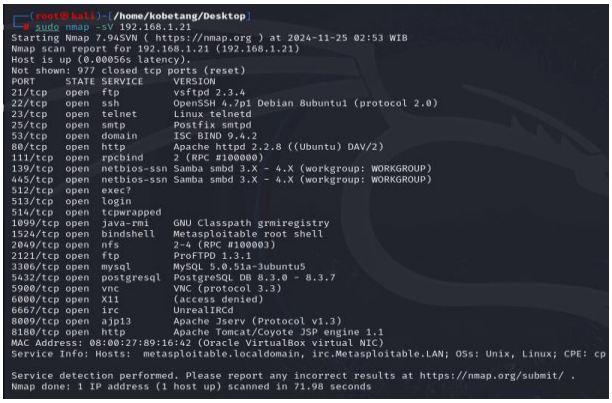
3.2 Tahapan Penetration Testing

3.2.1 Information Gathering

Dua metode pemindaian yang termasuk dalam sistem operasi Kali linux digunakan untuk mengumpulkan informasi untuk penelitian ini yaitu : Pemindaian keamanan dan jaringan (Nmap) dan *Whatweb*.

Gambar 4. Hasil dari whatweb

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1768-1775



Gambar 5. Hasil dari Nmap

Pada gambar 3 dan 4 itu merupakan hasil dari pemindaian menggunakan *tools* Nmap dan Whatweb yang dihasilkan dari Kali Linux sebagai *attacker*, dari hasil pemindaian ini mendapatkan hasil :

a. Informasi dari Whatweb

Pemindaian WhatWeb pada http://192.168.1.21 mengidentifikasi server Apache 2.2.8 yang berjalan di Ubuntu Linux dengan WebDAV aktif. Server ini juga menjalankan PHP 5.2.4-2ubuntu5.10. Layanan yang terdeteksi termasuk Apache HTTP Server, PHP, dan WebDAV. Judul halaman menunjukkan "Metasploitable2 - Linux," yang mengindikasikan sistem ini sebagai target uji penetrasi dengan potensi kerentanannya.

b. Informasi dari Nmap

Pemindaian Nmap terhadap IP 192.168.1.21 (alamat ip target) menunjukkan sejumlah port terbuka yang menandakan berbagai layanan aktif, seperti FTP (vsftpd), SSH (OpenSSH), Telnet, SMTP, DNS, HTTP (Apache), serta MySQL. Terdapat juga port untuk VNC, IRC, dan Java RMI.

3.2.2 Eksploitasi Webserver

Proses eksploitasi dilakukan untuk menentukan apakah kerentanan yang ditemukan pada beberapa port yang telah di scanning dapat digunakan untuk akses yang tidak sah. Proses eksploitasi dilakukan pada *web server Metasploitable2* dengan menggunakan *tools Metasploit Framework* pada Kali Linux. Fokus eksploitasi adalah *port* 21 (FTP), 22 (SSH) dan 5900 (VNC).

a. Eksploitasi Port 21

Layanan FTP yang berjalan pada port 21 menggunakan perangkat lunak vsftpd 2.3.4, versi yang diketahui memiliki kerentanan backdoor. Kerentanan ini memungkinkan penyerang untuk membuka koneksi shell jarak jauh tanpa autentikasi tambahan, sehingga memberikan akses penuh ke sistem target.

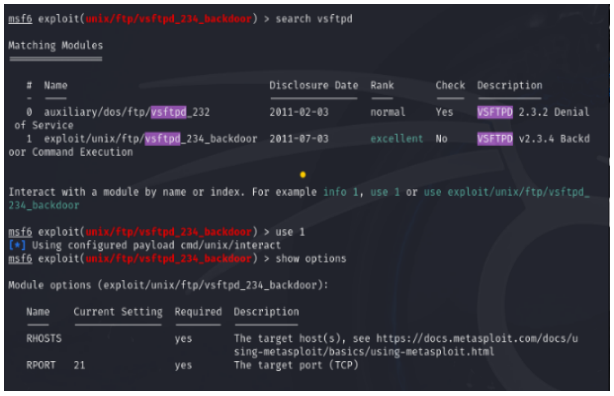
Langkah – langkah eksploitasi :

1. Langkah pertama adalah membuka Metasploit Framework di Kali Linux
2. Langkah kedua yaitu menjalankan modul *(payload)* eskploitasi berikut :
   " use exploit/unix/ftp/vsftpd_234_backdoor"

   "set RHOST 192.168.1.21"

   "exploit"
3. Setelah eksploitasi berhasil, shell korban terbuka dengan hak penuh, dimana memungkinkan pencuri *(attacker)* untuk membuka data, menginstall perangkat lunak seperti *backdoor* maupun *malware*.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1768-1775



Gambar 6. Konfigurasi Modul di Metasploit Framework

Dampak : Serangan ini menimbulkan resiko keamanan tingkat tinggi. Kerentanan ini dapat digunakan untuk mencuri data atau memanipulasi konfigurasi server jika digunakan dalam lingkungan produksi suatu perusahaan atau lembaga.

b. Eksploitasi SSH (Port 22)

Layanan *Secure Shell* (SSH) pada port 22 berfungsi untuk menghubungkan dan mengamankan komunikasi antar perangkat melalui jaringan. Pada port ini ditemukan kredensial default (username : msfadmin, password : msfadmin). Kredensial ini dapat ditemukan dalam waktu yang sangat singkat melalui serangan brute-force Metasploit.

Langkah – langkah eksploitasi port 22 :

1. Langkah pertama adalah membuka Metasploit Framework di Kali Linux
2. Menjalankan modul brute force berikut di Metasploit:

   " use auxiliary/scanner/ssh/ssh_login "

   " set RHOSTS 192.168.1.21 "

   " set USERNAME msfadmin & set PASSWORD msfadmin "

   " exploit "
3. Setelah mendapatkan akses SSH, penyerang dapat mengakses sistem sebagai pengguna resmi ataupun administrator seperti melakukan modifikasi *file* dan *monitoring* server.

Gambar 7. SSH Pentest

Dampak : Eksploitasi ini memungkinkan hacker untuk mengkonfigurasi sistem dengan kredensial *default* yang dapat digunakan secara *real time*. Kerentanan ini dapat digunakan untuk melakukan serangan tipe tinggi seperti memasangkan *ransomware* atau *keylogger*.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1768-1775

c. Eksploitasi VNC (Port 5900)

Tidak adanya authentikasi tambahan untuk layanan *Virtual Network Computing* (VNC) pada port 5900, ini memungkinkan *hacker* (peretas) mengakses antarmuka pengguna grafis server (*UI*) dan mengontrol sistem secara keseluruhan.

Langkah – langkah eksploitasi port 5900 :

1. Langkah pertama adalah membuka Metasploit Framework di Kali Linux.
2. Menjalankan modul eksploitasi berikut di Metasploit:

   " use auxiliary/scanner/vnc/vnc_none_auth "

   " set RHOSTS 192.168.1.21 "

   " exploit "
3. Eksploitasi tersebut berhasil membuka sesi VNC, yang memungkinkan penyerang melihat dan mengontrol desktop server target.

Gambar 8. UI Desktop Webserver Korban

Dampak: Layanan *VNC* yang tidak diautentikasi menimbulkan ancaman serius karena memungkinkan kontrol langsung terhadap sistem. Dalam skenario produksi, hal ini dapat mengakibatkan pelanggaran data atau penghentian layanan secara tiba-tiba.

4. KESIMPULAN

4.1 Kesimpulan

Sebagai hasil dari penyelidikan ini, kami dapat mengidentifikasi kerentanan di server web *Metasploitable2* melalui pengujian penetrasi yang berfokus pada port 21, 22, dan 5900. Data menunjukkan bahwa server web ini rentan terhadap berbagai serangan karena konfigurasi sistem yang buruk, perangkat lunak yang ketinggalan jaman, dan kurangnya mekanisme keamanan. Layanan *FTP* pada port 21 menggunakan *software* vsftpd 2.3.4. Ini berisi kerentanan pintu belakang *(backdoor)* yang memungkinkan penyerang mendapatkan akses shell tanpa otentikasi. Selain itu, layanan *SSH* pada port 22 ditemukan menggunakan kredensial default yang mudah ditebak, sehingga memungkinkan serangan brute force. Fitur *VNC* pada port 5900 tidak menawarkan perlindungan yang ketat, ini memungkinkan penyerang untuk mengakses *GUI* server secara langsung. Dari data tersebut, dapat disimpulkan bahwa keamanan server web sangat bergantung pada pembaruan perangkat lunak secara berkala, konfigurasi sistem yang tepat, dan penerapan kebijakan keamanan tambahan. Penelitian ini menyoroti pentingnya mengidentifikasi kerentanan dan mengambil langkah proaktif untuk melindungi sistem sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1768-1775

4.2 Saran

Berikut adalah beberapa saran untuk meningkatkan keamanan pada webserver berdasarkan penelitian yang sudah dilakukan :

a. Pembaruan Perangkat Lunak: Untuk melindungi terhadap eksploitasi kerentanan yang diketahui, gunakan perangkat lunak server versi terbaru.

b. Keamanan Konfigurasi: Gunakan kombinasi nama pengguna dan kata sandi yang rumit alih-alih kredensial layanan SSH default.

c. Menerapkan kebijakan keamanan tambahan : Gunakan otentikasi dua faktor (2FA) saat menggunakan layanan akses jarak jauh.

d. Pemantauan dan Deteksi: Menerapkan sistem pemantauan jaringan untuk memantau aktivitas mencurigakan seperti akses tidak sah atau serangan brute force.

REFERENCES

Aziz, M. A. 2022. " VULNERABILITY ASSESMENT UNTUK MENCARI CELAH KEAMANAN WEB APLIKASI E-LEARNING PADA UNIVERSITAS XYZ." *Journal of Engineering, Computer Science and Information Technology (JECSIT)* 2(1).

Darmawan, C., Panda, J., & Kweldju, A. D. 2024. " Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021." *EDUMATIC Jurnal Pendidikan Informatika* 272-281.

Fachri, F., Fadlil, A., & Riadi, I. 2021. "Analisis Keamanan Webserver menggunakan Penetration Test." *Jurnal Informatika* 183 - 190.

Hilmi, A., None Fauziah Herdiyanti, None Renol Burjulius, & Lena, N. S. 2023. "Pengujian Keamanan Sistem Operasi Linux Studi Kasus : Celah Keamanan FTP pada Metasploitable2. ." *IIKRA-ITH Informatika Jurnal Komputer Dan Informatika* 110-115.

Maulana Pandudinata, & Farid Ridho. 2024. "Analisis Keamanan Aplikasi Berbasis Web di Lingkungan BPS RI." *Seminar Nasional Official Statistics, 2024* 549–558.

Riadi, I., Umar, R., & Lestari, T. 2020. "Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP." *JISKA (Jurnal Informatika Sunan Kalijaga), 5(3)* 146.

Singh, M., Kumar, S., Garg, T., & Pandey, N. 2020. "Penetration Testing on Metasploitable 2." *International Journal of Engineering and Computer Science* 25014–25022.

Yunus, M. 2019. " ANALISIS KERENTANAN APLIKASI BERBASIS WEB MENGGUNAKAN KOMBINASI SECURITY TOOLS PROJECT BERDASARKAN FRAMEWORK OWASP VERSI 4." *Jurnal Ilmiah Informatika Komputer* 37-48.