P-ISSN :2580-4316
E-ISSN :2654-8054
https://doi.org/10.37817/ikraith-informatika.v8i1

Pengujian Keamanan Sistem Operasi Linux Studi Kasus : Celah Keamanan FTP pada Metasploitable2

Muhammad Anis Al Hilmi[1], Fauziah Herdiyanti[2],
Renol Burjulius[3], Sonty Lena[4]

[1,2,3,4]Politeknik Negeri Indramayu
E-mail : alhilmi@polindra.ac.id[1], fauziahherdi16@gmail.com[2],
burjuliusrenol@gmail.com[3], sontylena18@gmail.com[4]

ABSTRAK

Metasploitable2 merupakan sistem operasi Linux yang sengaja dibuat rentan untuk diserang, tujuannya untuk menjadi bahan percobaan. Penelitian ini dilakukan dengan pengujian pada sistem operasi Metasploitable2 yang menjadi target serangan dan Kali Linux sebagai penyerang. Dengan menggunakan NMAP, celah keamanan Metasploitable2 dapat diketahui dan dimanfaatkan untuk melakukan exploit. Jenis exploit yang dipakai adalah backdoor, karena backdoor dapat berfungsi untuk menembus sistem, program, atau network tanpa harus melewati proses autentikasi. Dalam hal ini, Metasploitable2 memiliki celah keamanan di port FTP-nya. Celah tersebut dicoba untuk dilakukan serangan exploit. Dalam kasus ini, cara penanganan serangan yaitu dengan proses menutup semua jalur masuk yang memungkinkan untuk menjadi celah serangan, dalam hal ini pada Metasploitable2 adalah port 6200 dan menonaktifkan izin akun anonim dalam melakukan upload file menggunakan FTP.

Kata kunci : ***Metasploitable2, Backdoor, Linux, FTP, NMAP, Kali Linux***

ABSTRACT

Metasploitable2 is a Linux operating system that is intentionally made vulnerable to attack; the aim is to be experimental material. This research was conducted by testing the Metasploitable2 operating system, which was the target of the attack, and Kali Linux as the attacker. Using NMAP, Metasploitable2 security vulnerabilities can be identified and exploited to perform exploits. The type of exploit used is a backdoor because a backdoor can function to penetrate systems, programs, or networks without going through the authentication process. In this case, Metasploitable2 has a security hole in its FTP port. The loophole is tried to be exploited. In this case, the way to handle the attack is by closing all possible entry points to be an attack loophole; in this case, Metasploitable2 is port 6200 and disabling anonymous account permissions to upload files using FTP.

Keyword : Metasploitable2 , Backdoor , Linux , FTP , NMAP , Kali Linux

1. PENDAHULUAN

Banyak celah yang dapat dieksploitasi oleh para pelaku kriminal siber. Mereka memanfaatkan celah keamanan demi mencuri data atau mengambil keuntungan dari peretasan ke dalam sistem. Para peretas memanfaatkan ketidaksiapan dari pengelola sistem web maupun

https://doi.org/10.37817/ikraith-informatika.v8i1
P-ISSN :2580-4316
E-ISSN :2654-8054

pengguna publik itu sendiri (Cahyanto, 2021). Implementasi pengamanan sangat penting untuk menjamin sistem tidak diinterupsi dan diganggu. Proteksi dan pengamanan terhadap perangkat keras dan sistem operasi sama pentingnya. Sistem operasi hanya satu bagian kecil dari seluruh perangkat lunak di suatu sistem.

Linux merupakan sebuah sistem operasi seperti Unix yang menggunakan *kernel* sebagai inti dan disertakan aplikasi juga modul pendukung lain agar dapat dipakai dengan baik. Linux bersifat bebas digunakan dan termasuk sumber kode terbuka, sehingga dapat digunakan dan dikembangkan oleh semua pihak (Mair, 2018).

2. DASAR TEORI

2.1 Sistem Operasi

Secara umum, sistem operasi adalah *software layer* pertama yang diletakkan pada memori komputer pada saat komputer dinyalakan, sedangkan *software* lainnya dijalankan setelah sistem operasi bekerja. Sistem operasi akan melayani kebutuhan seperti akses ke *disk*, kelola memori, penjadwalan *task,* dan tampilan/ *user interface* (Mair, 2018).

2.2. Linux

Linux adalah sistem UNIX yang dapat digunakan untuk kebutuhan jaringan (*networking*), pengembangan perangkat lunak, dan untuk digunakan sehari-hari seperti di kantor. Linux adalah sistem operasi alternatif yang murah karena biasanya bersifat gratis, jika dibandingkan dengan sistem operasi lain yang bersifat komersial (Purnama, 2018). Sistem operasi Linux sendiri memiliki fitur *true-multitasking*, *shared libraries*, *demand-loading*, *proper memory management*, dan *multi* pengguna. Linux mendukung banyak perangkat lunak mulai dari pengolah kata, tampilan X-Windows, GNU C/C++, hingga ke TCP/IP.

Gambar 1. *Logo Linux*

2.3. Metasploitable2

Metasploitable2 adalah sistem operasi berbasis Linux yang sengaja dibuat rentan. OS ini dapat digunakan untuk melakukan pelatihan keamanan, menguji alat keamanan, dan mempraktikkan teknik pengujian penetrasi umum.

2.4. FTP

FTP (*File Transfer Protocol*) umumnya berfungsi sebagai media tukar menukar file atau data dalam suatu *network* yang menggunakan TCP koneksi. FTP yang digunakan menggunakan berbasis *open-source* guna menunjang tingkat stabilitas tinggi dan tidak mudah terinfeksi virus dan *malware*. FTP merupakan metode protokol pilihan yang paling tepat dalam penyimpanan file/data secara cepat dalam proses *upload* dan *download* dari komputer *server* ke klien tanpa menggunakan flashdisk untuk mengambil data dari komputer *server* (Ruwaida dan Kurnia, 2018). *File Transfer Protocol* (FTP) adalah protokol jaringan standar yang digunakan untuk mentransfer file komputer dari satu *host* ke *host* lain melalui jaringan berbasis TCP, seperti Internet. FTP dibangun di atas arsitektur *server* klien dan menggunakan kontrol terpisah dan koneksi data antara klien dan *server*. Pengguna aplikasi dapat melakukan autentikasi dirinya dengan menggunakan protokol *login* yang jelas, biasanya dalam bentuk nama pengguna dan kata sandi, namun dapat terhubung secara anonim jika server dikonfigurasi untuk mengizinkannya.

P-ISSN :2580-4316
E-ISSN :2654-8054
https://doi.org/10.37817/ikraith-informatika.v8i1

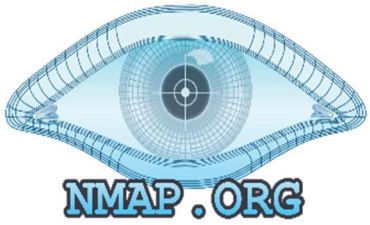
Untuk transmisi aman yang melindungi *username* dan *password*, dan mengenkripsi isinya, FTP sering diamankan dengan SSL / TLS (FTPS) (Radivilova dkk, 2018).

2.5 IP

Internet Protocol (IP) adalah protokol atau seperangkat aturan perutean dan pengalamatan paket data sehingga mereka dapat melakukan perjalanan melalui jaringan dan mencapai tujuan yang tepat. Fungsi atau tujuan *Internet Protocol* adalah untuk memindahkan *datagram* melalui serangkaian jaringan yang saling berhubungan. Ini dilakukan dengan melewati datagram dari satu modul *internet* ke modul *internet* lainnya sampai tujuan tercapai. Modul *internet* berada di *host* dan *gateway* dalam sistem *internet*. *Datagram* dirutekan dari satu modul *internet* ke yang lain melalui jaringan individu berdasarkan interpretasi alamat internet. Jadi, salah satu mekanisme penting protokol *internet* adalah alamat *internet* (Lencse dan Kadobayashi, 2019).

2.6. Nmap

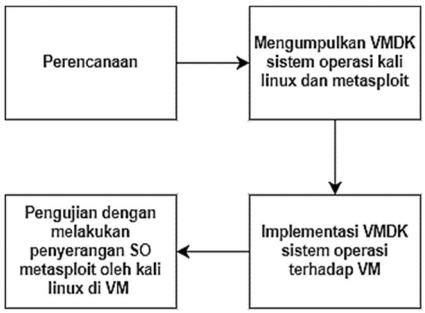
Nmap adalah sebuah *network scanner* yang banyak digunakan oleh para profesional di bidang *network security*, walaupun ada *tool* khusus dibuat untuk tujuan *hacking*, tetap belum dapat mengalahkan kepopuleran Nmap (Bagyalakshmi dkk, 2018). Nmap ("Network Mapper") merupakan sebuah *tool open source* untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap *host* tunggal. Nmap menggunakan paket IP *raw* dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal *upgrade* layanan, dan melakukan *monitoring uptime host* atau layanan (Bagyalakshmi dkk, 2018). Nmap sendiri biasanya sudah *include* terinstal pada Kali Linux, yang mana sering digunakan untuk melakukan pengujian keamanan sistem (Johansen dkk, 2016), (Mahtuf dkk, 2019).



Gambar 2. *Logo Website NMAP*

3. METODOLOGI PENELITIAN

Tahap penelitian dapat dilihat pada gambar 3.

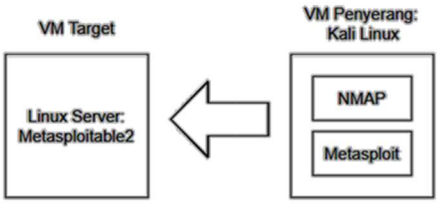


Gambar 3. *Tahapan Penelitian*

Penelitian ini diawali dengan perencanaan pengujian sistem operasi, dimana disiapkan sistem operasi Kali Linux sebagai penyerang dan sistem operasi Metasploitable2 sebagai target serangan. Setelah itu, mengumpulkan sistem operasi yang dibutuhkan yaitu, Kali Linux dan Metasploitable2. Ekstensi sistem operasi yang dipakai berupa

https://doi.org/10.37817/ikraith-informatika.v8i1
P-ISSN :2580-4316
E-ISSN :2654-8054

VMDK (*Virtual Machine Disk*), yaitu *format file* yang menjelaskan wadah untuk *drive hard disk virtual* untuk digunakan di mesin virtual seperti VMware *Workstation* atau VirtualBox. Kedua file VMDK tersebut kemudian dijalankan di dalam *virtual machine* dan mulai melakukan konfigurasi jaringan.

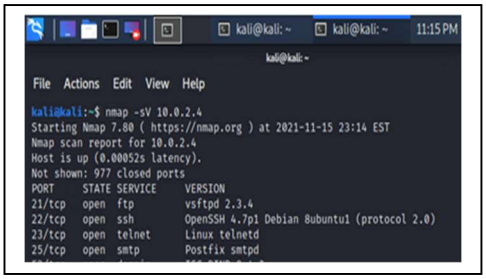


Gambar 4. *Ilustrasi Pengujian*

Skenario pengujian diawali dengan melakukan *scanning* melalui IP target menggunakan Nmap untuk mengetahui celah keamanan si target (Metasploitable2). Setelah mengetahui celah keamanan target, barulah mulai melakukan *exploit* terhadap target.

4. PENGUJIAN & PEMBAHASAN

Penelitian ini dilakukan dengan pengujian pada sistem operasi Metasploitable2 yang menjadi target serangan dan Kali Linux sebagai penyerang. Dengan bermodalkan alamat IP target, dapat dilakukan *scanning* menggunakan Nmap untuk mengetahui kondisi dan peluang adanya celah keamanan di sisi target.



Gambar 5. *Informasi Celah Keamanan Target*

Dari hasil scanning di atas, terlihat bahwa target menggunakan FTP versi vsftpd 2.3.4 yang mana mengandung celah keamanan di port 21/TCP (Khera dkk, 2019), (Xie dkk, 2016). Dengan memanfaatkan informasi tersebut, kemudian dapat dilakukan serangan atau exploit dengan menggunakan Kali Linux. Adapun langkah dilakukannya serangan adalah sebagai berikut:

1. Menjalankan Metasploit pada Kali Linux dengan perintah "`mfsconsole`".
2. Eksploit yang digunakan bertipe exploit *backdoor* yang bertujuan untuk mengakses sistem tanpa harus menangani proses autentikasi.
3. Penggunaan perintah `set RHOSTS <IP target>` bertujuan untuk mengatur IP target tersebut agar bisa dilakukan *remote.*
4. *Payload* di set `cmd/unix/interact` atau menentukan bahwa payload `cmd/unix/interact` yang akan digunakan.
5. Perintah "`exploit`" dijalankan untuk mengeksekusi modul atau serangan kepada target.

Serangan yang diujikan ternyata berhasil, dibuktikan dengan munculnya keterangan "session 1 opened". Dampak dari serangan tersebut yaitu, penyerang dapat melakukan *remote code execution* (RCE) pada sistem yang diserang (Metasploitable2). Adapun RCE yang dilakukan yaitu menambahkan *library* dan merubah hak akses beberapa *file*. Adapun hasil serangan tersebut disajikan di dalam tabel dibawah ini.

P-ISSN :2580-4316
E-ISSN :2654-8054
https://doi.org/10.37817/ikraith-informatika.v8i1

Tabel 1. *Hasil serangan*

Jenis eksploit	Backdoor
Perintah	`exploit/unix/ftp/vsftpd_234_backdoor`
Respon	Session opened
Keterangan	Berhasil

Kali Linux memanfaatkan FTP versi vsftpd 2.3.4 sebagai celah keamanan yaitu pada *port* 21. Celah keamanan tersebut kemudian di-*exploit* menggunakan *backdoor* oleh kali linux sampai berhasil membuka *session* 1. Dari suksesnya serangan ini, Kali Linux dapat mengunggah *file* secara bebas menggunakan FTP di *server*. Dampak dari *exploit* tersebut akan sangat berbahaya bagi sistem operasi Metasploitable2. Namun hal tersebut dapat ditangani dengan beberapa cara. Adapun salah satu cara penanganannya disajikan dalam tabel 2.

Tabel 2. *Proses penanganan*

Tempat konfigurasi	file vsftpd.conf
Perintah	`anon_upload_enable = YES` diberi tanda pagar (#)
Tambahan	Blok port 6200 (karena backdoor menggunakan port ini sebagai alternatif kerja)
Tujuan	Mencegah izin *anonym* melakukan *upload file* secara bebas, sehingga nanti diperlukan proses autentikasi dahulu.

Tujuan diberinya tanda pagar pada perintah `anon_upload_enable = YES` yaitu agar perintah tersebut dianggap sebagai komentar dan tidak aktif. Celah keamanan tersebut diakibatkan oleh konfigurasi default yang memperbolehkan akun anonim (tanpa proses autentikasi) dalam melakukan *upload file* menggunakan FTP.

5. KESIMPULAN

Setelah dilakukan perencanaan, implementasi, dan pengujian, maka dapat disimpulkan sebagai berikut:

1. Sistem operasi Metasploitable2 mempunyai kerentanan di *port* 21 atau protokol FTP versi 2.3.4. Celah keamanan tersebut dimanfaatkan untuk dilakukan serangan *exploit* menggunakan *backdoor* agar penyerang dapat memasuki sistem tanpa harus melalui proses autentikasi.
2. Serangan tersebut dapat ditangani dengan proses menutup semua jalur masuk yang memungkinkan untuk menjadi celah serangan, yaitu dengan mengaktifkan fitur autentikasi dalam penggunaan FTP, atau menonaktifkan akun anonim melakukan *upload file* dan memblok port 6200 (karena dimanfaatkan *backdoor*).

DAFTAR PUSTAKA

Bagyalakshmi, G., Rajkumar, G., Arunkumar, N., Easwaran, M., Narasimhan, K., Elamaran, V., ... & Ramirez-Gonzalez, G. (2018). Network vulnerability analysis on brain signal/image databases using Nmap and Wireshark tools. *Ieee Access*, *6*, 57144-57151.

Bök, P. B., Noack, A., Müller, M., & Behnke, D. (2020). Computernetze und Internet of Things. *Technische Grundlagen und Spezialwissen, Wiesbaden*.

Cahyanto, K. A., Al Hilmi, M. A., & Mustamiin, M. (2022). Pengujian Rule-Based pada Dataset Log Server Menggunakan Support Vector Machine Berbasis Linear Discriminat Analysis untuk Deteksi Malicious Activity. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, *9*(2).

Cozzi, E., Graziano, M., Fratantonio, Y., & Balzarotti, D. (2018, May). Understanding linux malware. In *2018 IEEE symposium on security and privacy (SP)* (pp. 161-175). IEEE.

D. Ruwaida and D. Kurnia. (2018). Rancang Bangun File Transfer Protocol (FTP) dengan Pengamanan Open SSL pada Jaringan VPN Mikrotik di SMK Dwiwarna. *CESS (Journal of Computer Engineering, System and Science), 3*(1), 45–49.

Johansen, G., Allen, L., Heriyanto, T., & Ali, S. (2016). *Kali Linux 2–Assuring Security by Penetration Testing*. Packt Publishing Ltd.

Khera, Y., Kumar, D., & Garg, N. (2019, February). Analysis and impact of vulnerability assessment and penetration testing. In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)* (pp. 525-530). IEEE.

Lencse, G., & Kadobayashi, Y. (2019). Comprehensive survey of IPv6 transition technologies: A subjective classification for security analysis. *IEICE Transactions on Communications*, *102*(10), 2021-2035.

M. Arman. (2017). Rancang Bangun Pengamanan FTP Server dengan Menggunakan Secure Sockets Layer. *Jurnal Integrasi, 9*(1), 16–23.

Mahtuf, F. R., Hatta, P., & Wihidiyat, E. S. (2019). Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan. *JOINTECS (Journal of Information Technology and Computer Science)*, *4*(1), 17-22.

Mair, Z. R. (2018). *Teori Dan Praktek Sistem Operasi*. Deepublish.

Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V. (2018, May). Decrypting SSL/TLS traffic for hidden threats detection. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 143-146). IEEE.

Sinha, S., & Sinha, S. (2018). Setting Up a Penetration Testing and Network Security Lab. *Beginning Ethical Hacking with Kali Linux: Computational Techniques for Resolving Security Issues*, 19-40.

Watrianthos, R., & Purnama, I. (2018). *Buku Ajar Sistem Operasi*. Uwais Inspirasi Indonesia.

Xie, Y., Feng, D., Tan, Z., & Zhou, J. (2016). Unifying intrusion detection and forensic analysis via provenance awareness. *Future Generation Computer Systems*, *61*, 26-36.