Journal of Internet and Software Engineering Vol: 1, No 3, 2024, Page: 1-12

Optimalisasi Pengujian Penetrasi: Penerapan Serangan MITM (*Man in the Middle Attack*) menggunakan Websploit

Desita Auliafitri*, Erry RizkiSuro, Muhamad Rangga Maulana Malik, Aep Setiawan

Program Studi Teknologi Rekayasa Komputer, Sekolah Vokasi, IPB University

Abstract: Kemajuan di era digital telah memberikan berbagai kemudahan melalui internet, termasuk dalam pengelolaan sistem informasi. Sistem informasi memerlukan proses autentikasi untuk memvalidasi pengguna sebelum mengakses suatu informasi. Namun, proses autentikasi rentan terhadap serangan siber, salah satunya adalah serangan MITM (*Man in the Middle*). Serangan MITM dapat dilakukan menggunakan websploit. Websploit merupakan alat keamanan siber yang dapat digunakan untuk memantau dan mencatat aktivitas jaringan. Hasil penelitian menunjukkan bahwa Websploit menggunakan modul http_sniffer mampu mengidentifikasi dan mengumpulkan data sensitif secara efektif dari pengguna yang terhubung ke jaringan publik. Penelitian ini mengindikasikan adanya potensi risiko keamanan yang signifikan dalam lingkungan jaringan yang tidak aman.

Kata kunci: Internet, Kali Linux, Man-in-the-Middle, Websploit

DOI: https://doi.org/10.47134/pjise.v1i3.2620
*Correspondence: Desita Auliafitri
Email: auliafitridesita@apps.ipb.ac.id

Received: 15-05-2024
Accepted: 30-06-2024
Published: 31-07-2024

Abstract: *Advancements in the digital era have provided various conveniences through the internet, including in the management of information systems. Information systems require an authentication process to validate users before accessing information. However, the authentication process is vulnerable to cyberattacks, one of which is the MITM (Man in the Middle) attack. MITM attacks can be carried out using Websploit. Websploit is a cybersecurity tool that can be used to monitor and record network activities. The research results show that Websploit, using the http_sniffer module, can effectively identify and collect sensitive data from users connected to a public network. This study indicates the potential for significant security risks in unsecured network environments.*

Keywords: *Internet, Kali Linux, Man-in-the-Middle, Websploit*

Pendahuluan

Dalam kemajuan era digital, keamanan siber menjadi isu penting seiring dengan meningkatnya ketergantungan masyarakat dan berbagai sektor industri pada teknologi informasi dan komunikasi. Ketergantungan pada teknologi informasi dan komunikasi menandakan bahwa tingginya angka pengguna aktif internet. Internet adalah jaringan komunikasi yang menghubungkan media elektronik dengan cepat melalui transmisi sinyal protokol TCP/IP dengan frekuensi yang disesuaikan oleh jaringan komunikasi (Fahmi dkk., 2020; Maharani dkk., 2021). Tingginya penggunaan internet juga menimbulkan tindakan anti-sosial dan berbagai kejahatan yang dilakukan melalui jaringan internet yang akan merugikan orang bahkan negara (Vimy dkk., 2022; Wahib dkk., 2022). Oleh karena itu, perkembangan internet seharusnya diikuti dengan keamanan siber yang terjamin, untuk memastikan bahwa lalu lintas informasi dan aktivitas masyarakat yang dilakukan melalui internet aman dan rahasia (Makbull Rizki, 2022). Keamanan siber bertujuan untuk menemukan, memperbaiki, dan mengurangi ancaman serta serangan siber yang dapat mengancam infrastruktur, data, perangkat keras, dan perangkat lunak sistem siber (Ramadhani & Pratama, 2022). Aktivitas ini melindungi sistem dan jaringan komputer dari ancaman, gangguan, serangan, dan akses ilegal yang dapat mengganggu keamanan data serta informasi jaringan. Selain itu, keamanan siber juga digunakan untuk melindungi jaringan komputer dari pengawasan yang tidak diinginkan, seperti aktivitas intelijen (Aji, 2022; Wahib dkk., 2022). Salah satu ancaman yang paling berbahaya dan umum terjadi dalam bidang keamanan siber adalah serangan *Man in the Middle* (MITM).

Berbagai kelemahan pada protokol dapat memungkinkan terjadinya serangan *Man in the Middle* (MITM) melalui jaringan pada metode kriptografi publik dan proses kerja *interlock protocol* (Awalsyah dkk., 2023; Rusdi & Prasti, 2019). Serangan *Man in the Middle* (MITM) adalah bentuk serangan dimana penyerang menyusup ke dalam komunikasi antara dua pihak yang sedang berinteraksi, dengan tujuan untuk menguping, menyadap, atau memodifikasi data yang sedang ditransmisikan (Riadi dkk., 2020). Serangan ini dimulai dengan penyerang menyadap atau mencuri paket data, seperti video, audio, gambar, dan dokumen, kemudian diubah dan dikembalikan ke komputer tujuan, yang kemudian diterima oleh komputer tujuan (Ajharie & Sulistiyono, 2022). Serangan ini dapat dilakukan dalam berbagai bentuk, seperti pengalihan lalu lintas jaringan, pemalsuan identitas, atau pengubahan pesan. Dampak dari serangan MITM dapat sangat merugikan, termasuk kebocoran data sensitif, kehilangan privasi, pencurian identitas, dan kerugian finansial yang signifikan.

Untuk menguji dan memahami proses serangan MITM dibutuhkan alat-alat khusus untuk menjalankan serangan tersebut. Salah satu alat yang sering digunakan adalah Websploit. Websploit adalah rangkaian alat keamanan siber yang dirancang untuk melakukan pengujian penetrasi dan mengevaluasi kerentanan jaringan (Setiyadi, 2017). Dengan modul http_sniffer, Websploit dapat memantau dan mencatat aktivitas jaringan secara efektif, memungkinkan penyerang untuk mengumpulkan data sensitif dari pengguna yang terhubung ke jaringan.

Penelitian ini menggunakan Kali Linux dalam penerapannya. Kali Linux merupakan platform pengujian penetrasi yang paling populer di dunia dan digunakan oleh para profesional keamanan dalam berbagai bidang (Asaad, 2021). Penetration adalah metode proaktif untuk mengevaluasi keamanan aset digital dengan mencari dan mengeksploitasi kerentanan, meniru cara operasional peretas dalam serangan siber (Ghanem & Chen, 2020). Kali Linux menyediakan platform yang ideal untuk menggunakan alat-alat seperti Websploit dalam melakukan serangan siber. Dengan Kali Linux simulasi serangan dalam lingkungan yang terkendali dapat dilakukan untuk membantu memahami mekanisme serangan dan mengembangkan strategi mitigasi yang efektif.

Pada penelitian yang berjudul "Analisis Serangan *Man in the Middle* (MITM) Menggunakan *Firmware Hacking Glinet Router* 6416a di Jaringan Wireless" serangan *Man in the Middle* (MitM) "sniffing" dapat terjadi pada server yang menggunakan protokol HTTPS, dengan catatan server HTTPS tersebut memperbolehkan *client* untuk melakukan *request* HTTP ke server, sedangkan server yang hanya menerima HTTPS only, tidak berhasil dikarenakan pertukaran informasi hanya berjalan jika terjadi koneksi HTTPS antara *client* dan server tersebut (Wiharjo & Widiasari, 2019).

Pada penelitian yang dilakukan oleh (Rizaldi Setiadi dkk., 2021), Serangan MITM dengan teknik ARP Spoofing menggunakan MITM proxy dapat merekam seluruh komunikasi dan melihat informasi sensitif pengguna ketika mengakses *website*. Hasil deteksi menggunakan algoritma K-NN dapat mengelompokkan jenis serangan atau bukan serangan dengan tingkat akurasi di atas 90% yaitu 95.1% dengan tingkat *error rate* di bawah 10% yaitu 4.9%.

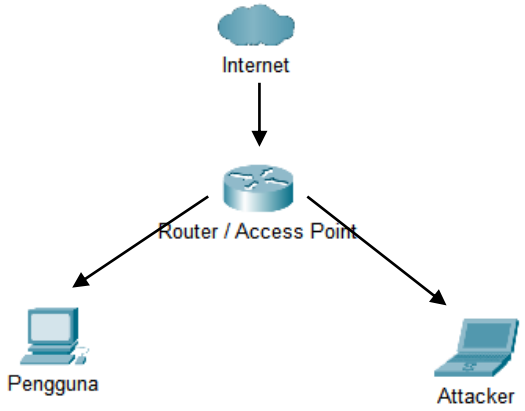
Pada penelitian yang dilakukan oleh (Wahanani dkk., 2020), serangan MITM dengan teknik sniffing menggunakan tools wireshark, smartsniff ettercap pada HTTPS sangat sulit untuk mengetahui *username* dan *password*. Sehingga penggunaan SSL dapat meningkatkan keamanan HTTP dan aktivitas komunikasi antar pengguna ataupun admin dengan *webserver* terjaga dengan baik melalui enkripsi data.

Pada penelitian "Penerapan Teknologi Blockchain untuk Mengatasi Serangan Man In The Middle (Firmansyah, 2023), didapatkan hasil bahwa teknologi *blockchain* efektif dalam meningkatkan keamanan komunikasi, mencegah serangan *spoofing*, serta menjaga integritas data yang dikirimkan antara pihak yang berkomunikasi. Identitas pengguna dapat diverifikasi dengan akurat, dan data yang terekam dalam *blockchain* tidak dapat dimanipulasi oleh serangan MITM. Dengan demikian, penerapan teknologi *blockchain* dapat menjadi solusi yang efektif untuk melindungi jaringan komputer dari serangan *Man in the Middle*.

Penelitian ini bertujuan untuk mengeksplorasi mekanisme serangan MITM menggunakan Websploit pada platform Kali Linux, serta menilai dampak dan risiko yang ditimbulkan oleh serangan tersebut. Selain itu, penelitian ini juga akan membahas langkah-langkah keamanan yang dapat diterapkan untuk mencegah serangan MITM, termasuk penggunaan enkripsi *end-to-end*, sertifikat digital, dan kesadaran pengguna akan pentingnya keamanan sistem informasi.

Metode

Dalam penelitian ini untuk mengumpulkan data penulis menggunakan teknik pengumpulan data studi literatur. Studi literatur adalah metode penelitian yang melibatkan pencarian, analisis, dan publikasi yang relevan dengan sistem yang dikembangkan. Studi literatur dilakukan dengan tujuan mengumpulkan data yang berkaitan dengan serangan *Man in the Middle Attack* (MITM) serta penggunaan Websploit tools. Kami telah mengumpulkan referensi literatur dari sumber-sumber terpercaya, termasuk artikel ilmiah, publikasi daring, jurnal ilmiah, tutorial video, serta situs web yang relevan. Hal ini dilakukan dengan tujuan untuk memperoleh pemahaman yang mendalam mengenai teknik *Man in the Middle Attack* menggunakan Websploit tools.



Gambar 1. Skema Jaringan

Dalam skema jaringan, *hacker* akan memanfaatkan posisinya di antara pengguna dan Internet untuk melakukan serangan MITM. Dengan menggunakan alat Websploit Tools untuk menyadap atau memodifikasi lalu lintas data antara pengguna dan internet, sehingga dapat memantau log aktivitas dan mengakses data privasi pengguna tanpa sepengetahuan mereka.

1. Internet: Sumber lalu lintas data yang mencakup semua informasi yang dikirim dan diterima oleh pengguna.
2. *Router / Access Point*: Pusat jaringan yang menghubungkan pengguna dengan Internet. Pengguna akan menghubungkan perangkat mereka *ke router* atau *access point* untuk mengakses Internet.
3. Pengguna: Pengguna yang mengira mereka berada dalam jaringan yang aman. Mereka mungkin terhubung ke jaringan rumah, kantor, atau *hotspot* umum.
4. *Attacker:* Penyerang yang telah berhasil mengintai jaringan yang digunakan oleh Pengguna. *Attacker* menggunakan MITM untuk mencuri informasi sensitif atau memantau aktivitas pengguna tanpa sepengetahuan mereka.

Hasil dan Pembahasan

Serangan *Man in the Middle* (MITM) adalah salah satu bentuk serangan siber dengan posisi penyerang berada di tengah-tengah komunikasi yang terjadi antara dua pihak tanpa sepengetahuan mereka. Penyerang secara diam-diam menyusup dan mengintersepsi komunikasi serta pengganggguan transmisi data dengan tujuan mengakses informasi rahasia, seperti kredensial login, data pribadi, atau informasi finansial. Penyerang, yang berada di antara kedua pihak, dapat memantau, memanipulasi, atau menyisipkan data dalam proses komunikasi, tanpa diketahui oleh pihak yang terlibat.

Websploit, sebagai alat pengujian penetrasi, memungkinkan pengguna untuk memantau dan mencatat aktivitas jaringan secara efektif, sehingga memungkinkan pengumpulan data sensitif dari perangkat yang terhubung ke jaringan. Dalam penggunaan Websploit, fitur http_sniffer sangat berguna untuk pelaksanaan serangan *Man-in-the-Middle* (MITM) dengan cara memantau lalu lintas HTTP yang tidak terenkripsi antara perangkat target dan server.

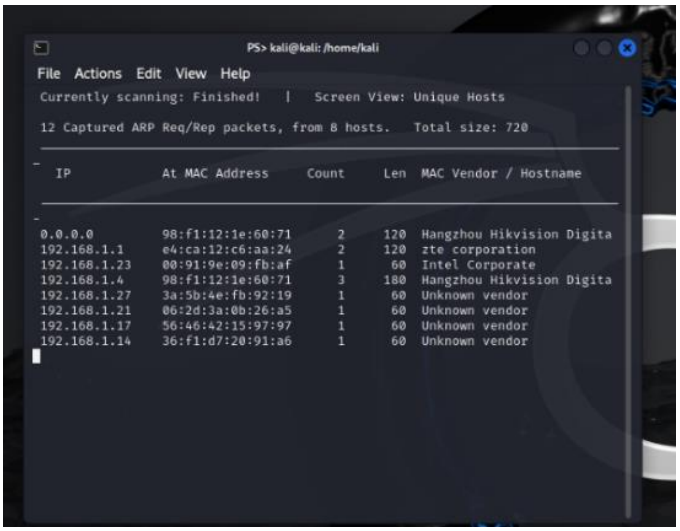
Proses ini dimulai dengan identifikasi IP perangkat yang terhubung dan jaringan yang digunakan melalui perintah **ifconfig** dan **sudo netdiscover -i eth0 -r [IP]**. Selanjutnya, dilakukan identifikasi terhadap target dan *gateway* yang relevan. Setelah target dan *gateway* diidentifikasi, fitur http_sniffer yang tersedia dalam Websploit digunakan untuk memonitor lalu lintas jaringan yang sedang berlangsung. Wireshark, sebagai alat pendukung, membantu memvisualisasikan dan memantau paket data yang dikirim dan diterima oleh perangkat dalam jaringan. Dengan menggunakan situs uji seperti **testphp.vulnweb.com** serangan MITM yang dilakukan dapat divalidasi dengan memantau kredensial login yang dimasukkan. Hasil pengujian menunjukkan bahwa Websploit efektif dalam menangkap data sensitif, yang menunjukkan potensi risiko keamanan yang signifikan dalam lingkungan jaringan yang tidak aman.

Langkah-langkah yang dilakukan peneliti secara rinci adalah sebagai berikut.

1. Identifikasi Target dan Gateway

Gambar 2. Informasi IP yang Terhubung.

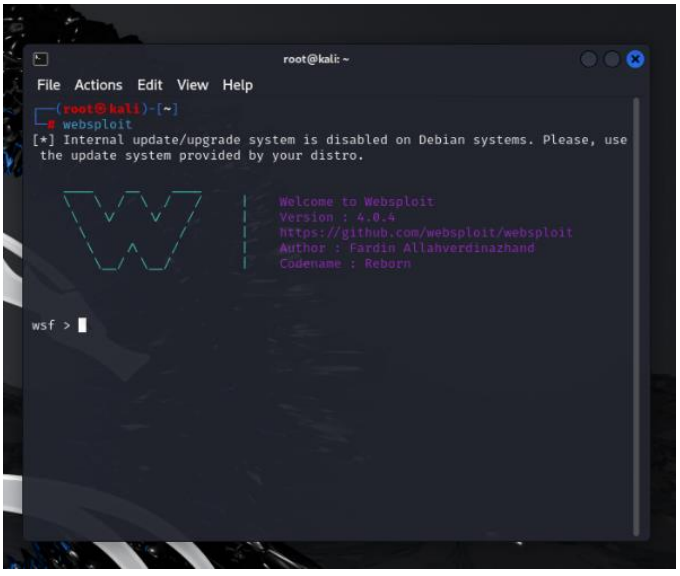
Langkah pertama dalam serangan MITM adalah mengidentifikasi IP perangkat target dan *gateway* jaringan. Buka terminal di Kali Linux, ketik perintah **ifconfig** untuk mengetahui IP dari jaringan yang terhubung. IP **192.168.1.29** merupakan IP yang terhubung dari perangkat yang digunakan.



Gambar 3. IP yang Terhubung pada Jaringan Wi-Fi

Ketik perintah **sudo netdiscover -i eth0 -r 192.168.1.0/24** untuk melihat seluruh IP yang terhubung ke jaringan WiFi beserta perangkat didalamnya.

2. Konfigurasi Websploit



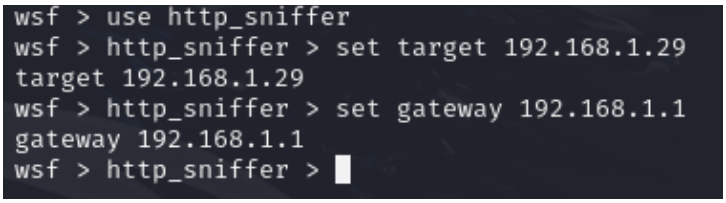
Gambar 4. Tampilan Websploit

Melacak dan memantau IP yang telah ditemukan dengan menggunakan alat bernama Websploit. Buka Websploit di terminal dengan hak akses *root*, karena memerlukan izin untuk menjalankan program.

Gambar 5. Tampilan Fitur pada Websploit

Gunakan perintah **show** untuk menampilkan semua fitur yang tersedia pada Websploit. Dalam kasus *Man In The Middle Attack* ini, digunakan fitur **http_sniffer**. Fitur ini dipilih karena memungkinkan kita untuk melacak atau memantau aktivitas yang dilakukan oleh perangkat tersebut.

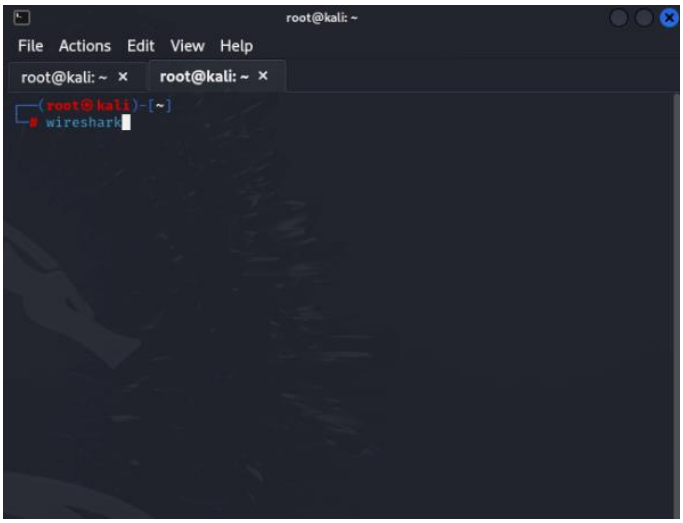
3. Menentukan Target dan Gateway



Gambar 6. Menentukan Target dan Gateway

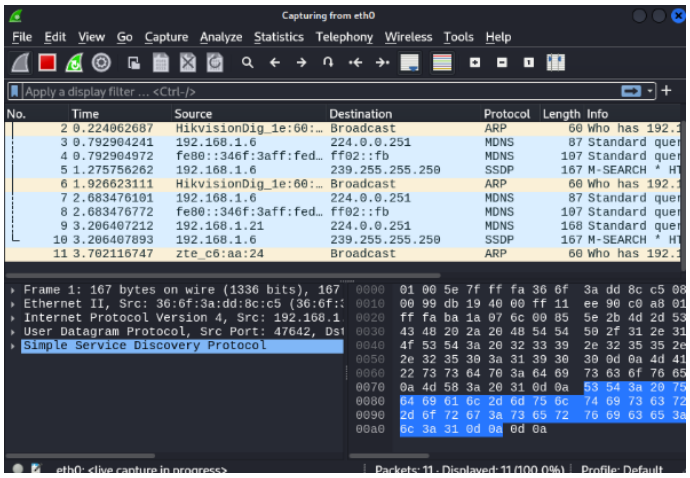
Menentukan perangkat target dan *gateway* jaringan dengan perintah **set target [IP_target]** dan **set gateway [IP_gateway]** untuk melihat lalu lintas pertukaran data dari perangkat tersebut. Pada gambar, **set target 192.168.1.29** dan **set gateway 192.168.1.1**.

4. Penggunaan Wireshark untuk Analisis Lalu Lintas



Gambar 7. Tampilan Wireshark

Sebelum menjalankan perintah di Websploit, buka Wireshark di tab terminal baru. Ketik **wireshark** untuk menjalankan Wireshark.



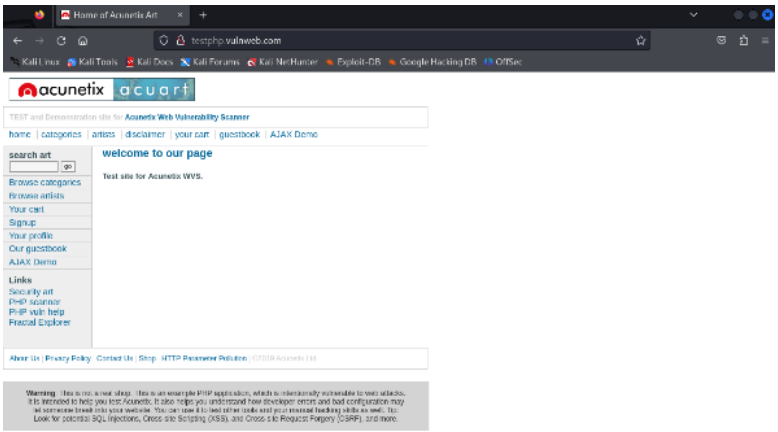
Gambar 8. Tampilan Pemantauan Lalu Lintas melalui Wireshark

Jalankan Wireshark dan pilih *interface* jaringan yang sesuai untuk mulai memantau lalu lintas jaringan. Wireshark akan memberikan tampilan grafis dari semua paket data yang ditransmisikan, sehingga analisis lalu lintas jaringan dapat dilakukan dengan lebih jelas.

5. Mengaktifkan Program http_sniffer

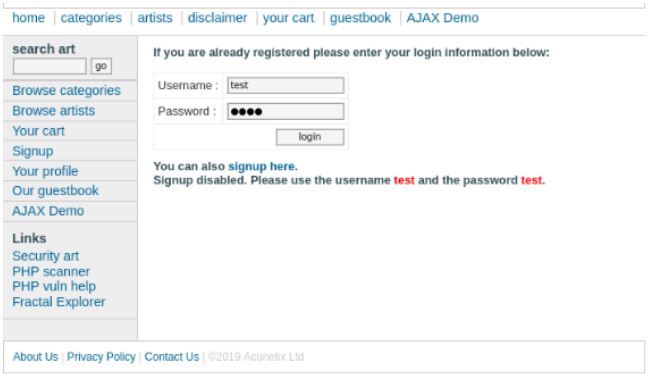
Setelah Wireshark berjalan, kembali ke terminal Websploit. Jalankan program http_sniffer dengan mengetik **execute**. semua lalu lintas HTTP yang tidak terenkripsi dapat ditangkap oleh Websploit. Informasi sensitif seperti *username, password, cookie*, dan data lain yang dikirim dalam bentuk teks biasa dapat dengan mudah diidentifikasi dan disimpan oleh penyerang.

6. Validasi Serangan



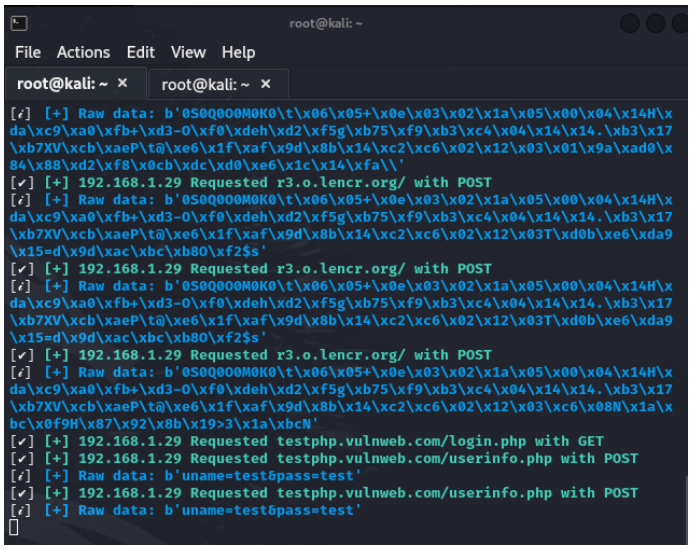
Gambar 9. Tampilan Situs testphp.vulnweb.com

Untuk memvalidasi keberhasilan efektivitas serangan, dapat dilakukan dengan mengakses situs uji seperti **testphp.vulnweb.com**. Situs ini diakses untuk menguji apakah data dapat dipantau atau tidak.



Gambar 10. Tampilan Login Situs testphp.vulnweb.com

Klik bagian *signup* atau halaman *login* pada situs uji. Masukkan ***username test*** dan ***password test*** untuk melakukan pengujian keberhasilan program dari websploit tersebut.



Gambar 11. Pemantauan Lalu Lintas Berhasil

Jika berhasil, *username* dan *password* yang dimasukkan akan terlihat dan dipantau melalui Websploit seperti gambar.

Untuk mengurangi risiko serangan MITM dan meningkatkan keamanan jaringan, beberapa strategi mitigasi dapat diterapkan dalam menjaga integritas dan kerahasiaan data di era digital yang terus berkembang. Strategi-strategi mitigasi serangan MITM dapat dilakukan dengan beberapa cara. Pertama, menggunakan enkripsi *end-to-end* memastikan bahwa data yang dikirim antara pengirim dan penerima tidak dapat dibaca oleh pihak ketiga. Protokol seperti HTTPS, SSL/TLS harus diimplementasikan untuk semua komunikasi yang sensitif. Kedua, menggunakan sertifikat digital untuk mengautentikasi server kepada klien yang akan mencegah penyerang menampilkan dirinya sebagai server yang sah. Ketiga, menggunakan VPN untuk mengenkripsi seluruh lalu lintas jaringan. VPN adalah metode untuk membuat jaringan *private* dan aman dengan menggunakan jaringan publik, seperti internet (Sjafrina dkk., 2019). Hal ini penting dilakukan terutama ketika

menggunakan jaringan WiFi publik yang rentan terhadap serangan MITM. Keempat, selalu menghubungkan perangkat ke jaringan yang aman dan terpercaya. Hindari menggunakan jaringan WiFi publik tanpa enkripsi. Kelima, mengimplementasikan autentikasi dua faktor untuk menambah lapisan keamanan ekstra. Hal ini akan membuat penyerang sulit untuk mendapatkan akses hanya dengan mencuri kredensial *login*. Keenam, melakukan pemantauan jaringan secara aktif untuk mendeteksi aktivitas yang mencurigakan. Alat seperti *Intrusion Detection Systems* (IDS) dapat membantu mendeteksi serangan MITM. *Intrusion Detection Systems* (IDS) akan memantau lalu lintas jaringan untuk mendeteksi aktivitas yang mencurigakan dan tidak biasa dan memberikan peringatan (Tallane & Chandra, 2022). Terakhir, melakukan pelatihan kepada pengguna tentang risiko serangan MITM dan cara menghindarinya, seperti tidak membuka tautan mencurigakan atau mengabaikan peringatan keamanan dari browser.

Simpulan

Penerapan serangan *Man in the Middle* (MITM) menggunakan Websploit pada platform Kali Linux memberikan pemahaman lebih tentang metode dan dampak dari serangan ini terhadap keamanan jaringan. Websploit, dengan fitur http_sniffer, terbukti efektif dalam memantau dan menangkap data sensitif yang dikirim melalui jaringan yang tidak terenkripsi. Proses ini melibatkan identifikasi perangkat target dan *gateway*, konfigurasi Websploit, dan pemantauan lalu lintas jaringan dengan Wireshark untuk validasi dan analisis lebih mendalam. Hasil pengujian menunjukkan bahwa data *login* dan informasi sensitif lainnya dapat dengan mudah dicuri melalui serangan MITM jika tidak ada langkah keamanan yang memadai.

Dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi, penting bagi individu dan organisasi untuk memahami ancaman yang ditimbulkan oleh serangan MITM dan mengambil langkah-langkah yang diperlukan untuk melindungi jaringan dan data mereka. Kesadaran akan risiko ini dan penerapan strategi mitigasi yang tepat sangat penting dalam menjaga integritas dan kerahasiaan informasi di era digital yang terus berkembang.

Daftar Pustaka

Ajharie, M. A., & Sulistiyono, M. (2022). Implementasi Framework Mitm (Man In The Middle Attack) Untuk Memantau Aktifitas Pengguna Dalam Satu Jaringan. *Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan*, *7*(1), 45–49.

Aji, M. P. (2022). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). *Jurnal Politica*

Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Asaad, R. R. (2021). Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. *Academic Journal of Nawroz University (AJNU)*, *10*(1), 7–12. https://doi.org/10.25007/ajnu.v10n1a998

Awalsyah, R. M. S., Harahap, P. S., & Dono, M. (2023). Implementasi Caesar Cipher Dalam Mengenkripsikan Pesan Pada Serangan Man in. *Jurnal JOCOTIS - Journal Science Informatica and Robotics*, *1*(1), 64–72.

Fahmi, M. I., Kifti, W. M., & Marpaung, N. (2020). Pemanfaatan Teknologi Informasi Dalam Penggunaan Website Sebagai Media Informasi Pada Polsek Porsea Kabupaten Toba Samosir. *Jurdimas (Jurnal Pengabdian Kepada Masyarakat) Royal*, *3*(1), 51–54. https://doi.org/10.33330/jurdimas.v3i1.494

Firmansyah, D. (2023). Penerapan Teknologi Blockchain Untuk. *Jurnal JOCOTIS - Journal Science Informatica and Robotics*, *1*(1), 73–80. https://jurnal.ittc.web.id/index.php/jct/

Ghanem, M. C., & Chen, T. M. (2020). Reinforcement Learning for Efficient Network Penetration Testing. *Information*, *11*(6), 1–23. https://doi.org/10.3390/info11010006

Maharani, D., Helmiah, F., & Rahmadani, N. (2021). Penyuluhan Manfaat Menggunakan Internet dan Website Pada Masa Pandemi Covid-19. *Abdiformatika: Jurnal Pengabdian Masyarakat Informatika*, *1*(1), 1–7. https://doi.org/10.25008/abdiformatika.v1i1.130

Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Ramadhani, M. R., & Pratama, A. R. (2022). Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia. *Automata*, *1*(2), 1164. https://doi.org/10.46930/ojsuda.v30i1.3167

Riadi, I., Umar, R., & Busthomi, I. (2020). Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain. *Journal of Information Engineering and Educational Technology*, *4*(1), 15–19. https://doi.org/10.26740/jieet.v4n1.p15-19

Rizaldi Setiadi, R., Suryani, V., & Agus Triawan, M. (2021). Implementasi dan Deteksi Serangan Man-In-The-Middle Berbasis MITM Proxy Terhadap Protokol HTTPS Menggunakan Metode K-NN. *e-Proceeding of Engineering*, *8*(5), 10486.

Rusdi, M. I., & Prasti, D. (2019). Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux. *PROSIDING SEMANTIK*, *2*(1), 260–269.

Setiyadi, A. (2017). Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet Seminar Nasional Komputer dan Informatika. *Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet Seminar Nasional Komputer dan Informatika*, 113–120. https://ojs.unikom.ac.id/index.php/senaski/article/view/934

Sjafrina, F., Arnesia, P. D., & Aqim, A. (2019). Rancang Bangun Jaringan VPN Berbasis IPSEC Menggunakan Mikrotik Routerboard Pada PT. Zahir Internasional. *Seminar*

Nasional Teknologi Informasi dan Komunikasi STI&K SeNTIK, *3*(1), 2581–2327. https://ejournal.jak-stik.ac.id/index.php/sentik/article/download/267/117

Tallane, R. B., & Chandra, D. W. (2022). Implementation of Intrusion Detection System (Ids) Using Security Onion. *Syntax Literate: Jurnal Ilmiah Indonesia*, *7*(10), 685–704.

Vimy, T., Wiranto, S., Rudiyanto, Widodo, P., & Suwarno, Panji. . . (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal Kewarganegaraan*, *6*(1), 2319–2327. http://journal.upy.ac.id/index.php/pkn/article/view/2989

Wahanani, H. E., Aditiawan, F. P., & Mumpuni, R. (2020). Uji Coba Serangan Man In The Middle Pada Keamanan SSL Protokol Http. Dalam *Jurnal Sistem Informasi Dan Bisnis Cerdas (SIBC)* (Vol. 13, Nomor 1).

Wahib, P., Narotama, A. T., Rijki, N., Sahrudin, Permana, F., Sagara, D., Azkhal, D. I., Anwar, M., & Juniawan, M. R. (2022). Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital. *Abdi Jurnal Publikasi*, *1*(2), 64–68. https://jurnal.portalpublikasi.id/index.php/AJP/index

Wiharjo, D., & Widiasari, I. R. (2019). Analisis Serangan Man in the Middle (MitM) Menggunakan Firmware Hacking Glinet Router 6416a di Jaringan Wireless. *Artikel Ilmiah*, *672018705*. https://repository.uksw.edu/handle/123456789/20247