Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan Vol. 7 No. 1. Juni 2022 | P-ISSN: 2527-9858
E-ISSN: 2548-1180

Implementasi Framework Mitm *(Man In The Middle Attack)* Untuk Memantau Aktifitas Pengguna Dalam Satu Jaringan

Mohamad Arie Ajharie[1], Mulia Sulistiyono[2]

[1,2] *Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta*

[1]mohamad.ajharie@students.amikom.ac.id,

[2*]muliasulistiyono@amikom.ac.id (penulis korespondensi)

Abstrak— Kemajuan teknologi informasi yang semakin kencang harus diimbangi dengan kemampuan untuk melakukan pengamanan terhadap informasi. Berbagai masalah penyerangan jaringan yang bertujuan merugikan pengguna perlu kita pahami bagaimana konsep penyerangan tersebut. Serangan MITM *(Man In The Middle*) membelokan traffic paket data melewati perangkat penyerang. Perangkat penyerang mengaku sebagai router ketika berkomunikasi dengan client dan mengaku client ketika berkomunikasi dengan router. *Tools* MITMF mampu menjalankan program sslstrip dimana website yang menggunakan teknologi SSL (HTTPS) akan dipaksa menjadi HTTP. Penyerang harus berada dalam satu jaringan dan pada saat tools MITMF diaktifkan secara otomatis akan melakukan serangan sekaligus melakukan paket sniffing dan menampilkan secara langsung pada terminal. Website yang tidak menggunakan teknologi SSL akan menampilkan informasi tanpa enkripsi. Dalam penelitian ini akan dibahas tentang bagaimana serangan MITM bekerja terutama dari sisi klien dan menggunakan metode sniffing serta akan memberikan hasil berupa data proses MITM yang akurat dan dapat dibuktikan menggunakan framework MITM. Hasil pengujian menunjukan website yang dapat di bypass username dan passwordnya adalah website dengan protokol keamanan HTTP. Sedangkan terhadap protokol keamanan HTTPS tidak mampu untuk mendeteksi aktivitas browser. Akses terhadap website dengan protokol keamanan HTTPS bisa dialihkan ke protokol keamanan HTTP.
Kata kunci— ***Man in the middle, MITM, Sniffing, MITMF***

Abstract— **I**nformation technology that are getting faster must be balanced with the ability to secure information. Various problems of network attacks that aim to harm users, we need to understand how the concept of the attack is. MITM (Man In The Middle) attacks bend data packet traffic through the attacker's device. The attacker's device pretends to be a router when communicating with a client and pretends to be a client when it communicates with a router. The MITMF tool is able to run the SSLStrip program where websites that use SSL technology (HTTPS) will be forced to become HTTP. Attackers must be in the same network and when the MITMF tool is activated it will automatically carry out attacks while simultaneously carrying out packet sniffing and displaying it directly on the terminal. Websites that do not use SSL technology will display information without encryption. In this study, we will discuss how MITM attacks work, especially from the client side and using the sniffing method and will provide results in the form of accurate and provable MITM process data using the MITM framework. The test results show that the website that can be bypassed the username and password is a website with the HTTP security protocol. Meanwhile, the HTTPS security protocol is unable to detect browser activity. Access to websites with the HTTPS security protocol can be redirected to the HTTP security protocol.
Keywords— Man in the middle, MITM, Sniffing, MITMF

I. PENDAHULUAN

Indonesia diakui masih banyak mempunyai PR di sisi keamanan siber. Dalam dokumen Global Cybersecurity Index 2017 yang diterbitkan oleh ITU-D, Indonesia mendapatkan nilai 0.424 dan berada di posisi nomor 69 dari 164 negara dengan status *Maturing* (sedang menuju kesiapan) [1], selain itu Indonesia merupakan salah satu negara dengan penggunaan internet yang relatif tinggi.[2]. Kondisi seperti ini menuntut tenaga profesional jaringan untuk memberikan keamanan terhadap penggunaan internet dengan mencari tahu banyak hal yang membuatnya mengerti betul cara kerja dan teknologi keamanan jaringan. Banyak sekali informasi berharga yang perlu dilindungi untuk mencegah suatu tindak kejahatan dalam dunia maya. Pencurian informasi dapat dilakukan dengan beberapa cara salah satunya adalah dengan memantau jaringan menggunakan software dan mencatat informasi tersebut dalam bentuk teks yang jelas. Dalam beberapa kasus bisa juga memanfaatkan *cookies* yang tersimpan dalam web browser. Alangkah berbahayanya ketika ketidaktahuan pengguna internet menggunakan jaringan tersebut untuk mengakses transaksi perbankan.

Serangan MITM (*Man In The Middle*) *Attack* adalah serangan terhadap jaringan akses terbuka [3]. MITM merupakan bentuk serangan di dalam jaringan komputer, dimana (*attacker*) berada di tengah-tengah (middle) antara korban dengan tujuan korban[4]. Bentuk serangan dari MITM dapat berupa adanya penyadap komunikasi suara dan teks, perusakan privasi, dan hilangnya jaminan keaslian suatu data akibat diubah oleh pelaku (*attacker*) [5] serta termasuk pembajakan sesi, pencurian data sensitif, pencurian login, dan pencurian informasi pribadi [4].

Sejumlah aplikasi dan layanan pada Application layer yang rentan terhadap jenis serangan MITM) antara lain pada jenis layanan surat elektronik (*e-mail*), layanan komunikasi teks berbasis web, *Domain Name System* (DNS), dan telepon berbasis Internet Protocol (*Voice Internet Protocol/VOIP).* Bentuk penyerangan dimulai dari bagaimana seorang pelaku (*Attacker*) melakukan proses pembelokkan (penyadapan, pencurian) paket data (audio, video, gambar, dokumen), untuk kemudian diubah (modifikasi) lalu dikembalikan ke komputer tujuan, untuk kemudian diterima oleh komputer tujuan tersebut. Pelaku berada ditengah-tengah antara si korban dengan tujuan si korban, pada jaringan komputer (baik intranet maupun internet).[4]

Dampak dari serangan ini signifikan karena penyerang dapat mencegat, menyisipkan, atau mengubah aliran lalu

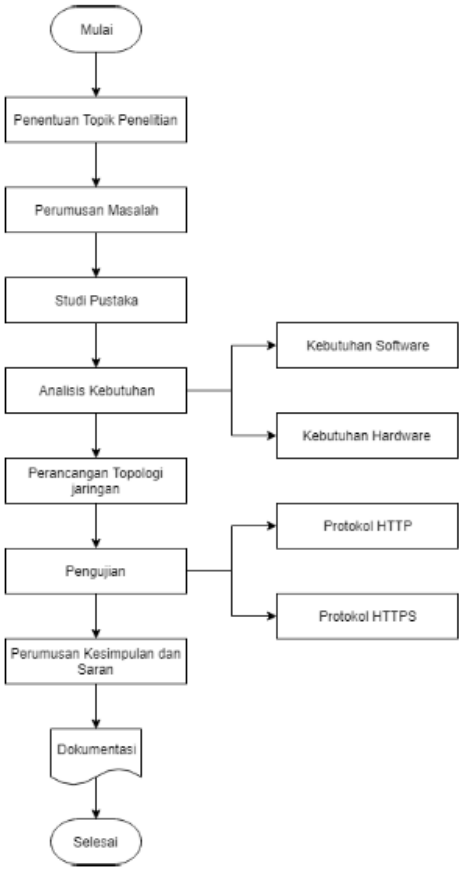
lintas jaringan tanpa terdeteksi. Oleh karena itu, penyerang mengetahui kedua rahasia tersebut dan dapat dengan mudah menjalankan dua sesi terenkripsi secara bersamaan. Dengan koneksi, sangat mudah untuk memantau dan memanipulasi data yang disediakan antara server dan browser [6].

*Man In The Middle framework (*MITMF) bertujuan untuk menyediakan paket lengkap serangan MITM sebagai upaya meningkatkan serangan dan meningkatkan teknik yang ada. Awalnya dibangun untuk mengatasi kekurangan yang signifikan dari alat lain. MITMF hampir sepenuhnya ditulis ulang dari awal untuk menyediakan kerangka kerja modular dan dapat digunakan siapa saja untuk menerapkan serangan MITM [7]

Beberapa penelitian yang terkait diantaranya ”Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet”. Penelitian tersebut bertujuan untuk menghasilkan pedoman bagi administrator jaringan dalam memonitoring lalu lintas data untuk keamanan jaringan. Dalam penelitian tersebut juga di jelaskan perintah-perintah untuk menjalankan modul secara detail. Diawali dengan pengumpulan data untuk memperoleh informasi yang diperlukan berupa IP address. Pada tahap implementasi modul di paparkan gambar tools websploit beserta perintah-perintah yang harus diketikkan untuk menggunakan modul mitm. Pengujian menggunakan metode sniffing dilakukan dengan mengakses alamat website dari perangkat target hingga didapatkanlah hasil laporan monitoring [8]. Selain itu implementasi MITM juga dapat digunakan pada device smarthpone sebagai media penyerangan. Proses eksploitasi tersebut menggunakan metode sniffing. proses implementasi dilakukan unlock dan rooting pada perangkat smartphone menggunakan aplikasi Nexus Root Toolkit, instalasi Busybox dan Kali NetHunter pada smartphone serta instalasi VNC server untuk me-remote perangkat smartphone. Pengujian dilakukan menggunakan metode sniffing dengan mengaktifkan tools Badusb MITM Attack dan mengakses alamat web yang menggunakan protokol HTTP melalui perangkat target. Sedangkan, untuk menguji alamat web yang menggunakan protokol HTTPS menggunakan tools tambahan SLStrips [9]. Pencegahan MITM juga dapat dilakukan dengan menggunakan teknologi SSL serta mendeteksi serangan man in the middle dengan algoritma Blowfish dan algoritma Diffie-Hellman (D-H) [10]. Berbeda dengan penelitian yang sudah dilakukan diatas, dalam penelitian ini akan membahas tentang bagaimana serangan MITM bekerja terutama dari sisi klien dan menggunakan metode sniffing serta akan memberikan hasil berupa data proses MITM yang akurat dan dapat dibuktikan menggunakan framework MITM.

II. METODOLOGI PENELITIAN

Langkah penelitian yang dilakukan dalam penelitian ini seperti terdapat pada gambar 1 dibawah ini.



Gambar 1. Langkah penelitian yang dilakukan

Data dan informasi yang dihimpun didasarkan pada materi penelitian yang akan digunakan yaitu terkait penerapan metode-metode MITM. Materi-materi tersebut meliputi jaringan komputer, topologi jaringan, jenis jaringan komputer, internet, WLAN (Wireless Local Area Network), HTTP (Hypertext Transfer Protocol), HTTPS (Hypertext Transfer Protocol Secure), Kali Linux, MITM (Man In The Middle), MITMF (Man In The Middle framework), ARP Attack (ARP Spoofing / ARP Poisoning).

Alat dan bahan yang digunakan dalam penelitian ini terdiri dari perangkat keras (hardware) dan perangkat lunak (software). Adapun perangkat keras (hardware) yang digunakan dalam penelitian ini dijabarkan dalam Tabel 1.

TABEL I
SPESIFIKASI PERANGKAT KERAS

No	Hardware	Spesifikasi
1	Huawei E5830	Wireless Standar: 802.11 b/g Wireless Frekuensi: 2.4 ~ 2.4835GHz
2	TP-LINK TL-WN727N	Wireless Standar: 802.11 b/g Wireless Frekuensi: 2.4 ~ 2.4835GHz
3	HP Laptop 14CM0014AX	Processor : AMD A9-9425 RADEON R5, 5 COMPUTE CORES 2C+3G (2CPUs), 3.1GHz RAM: 4 GB ,Hardisk: 1 TB,VGA: AMD Radeon(TM) 520 Wireless Standar: 802.11 b/g/n Wireless Frekuensi: 2.4 ~ 2.4835GHz
4	Lenovo Ideapad 320-14AST	Processors: AMD A9-9420 RADEON R5, 5 COMPUTE CORES 2C+3G (2 CPUs), ~3.0GHz RAM: 4 GB Hardisk: 1 TB VGA: AMD Radeon R5 Wireless Standar: 802.11 b/g/n Wireless Frekuensi: 2.4 ~ 2.4835GHz
5	Xiaomi Redmi 5A	Processors: Quad-core 1.4 GHz Cortex-A53 RAM: 2 GB Storage: 16 GB Wireless Standar: 802.11 b/g/n Wireless Frekuensi:

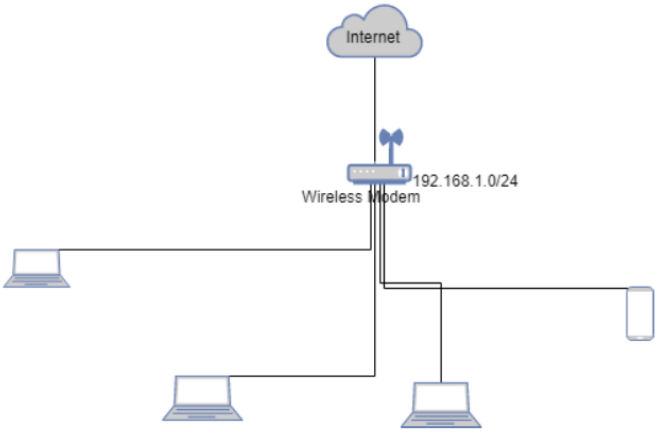
		2.4 ~ 2.4835GHz
6	Lenovo G450	Processor: Pentium(R) Dual-Core CPU T4500 @2.30GHz (2CPUs) RAM: 1 GB Harddisk: 465 GB Wireless Standar: 802.11 b/g/n Wireless Frekuensi: 2.4 ~ 2.4835GHz

Penulis juga membutuhkan perangkat lunak (software) untuk melakukan penelitian. Berikut perangkat lunak (software) yang digunakan dalam penelitian ini dapat dilihat dalam Tabel 2.

TABEL 2
SPESIFIKASI PERANGKAT LUNAK

No	Software	Spesifikasi
1	Kali Linux 2019.2 64-bit	Sistem operasi Kali Linux digunakan sebagai attacker/penyerang
2	Windows 10 64-bit	Sistem operasi Windows 10 digunakan sebagai target penyerangan
3	VM VirtualBox	Vitualbox digunakan untuk menjalankan sistem operasi linux secara virtual
4	Opera Browser v6.2	Opera browser digunakan untuk menguji penyerangan terhadap aktifitas browser
5	Chrome Mobile Browser v75.0	Chrome mobile browser digunakan untuk menguji penyerangan terhadap aktifitas browser pada perangkat smartphone.
6	Windows 7 32-bit	Sistem operasi Windows 7 digunakan sebagai target penyerangan.

Pada tahap perancangan, peneliti melakukan perancangan sesuai kebutuhan perangkat yang telah dipaparkan pada tahap sebelumnya. Rancangan yang dibuat adalah topologi jaringan yang akan digunakan. Peneliti menggunakan 1 modem sebagai sumber internet, 3 Laptop dengan salah satu dari perangkat tersebut digunakan sebagai penyerang dan target monitoring, serta 1 smarphone yang akan digunakan sebagai target monitoring. Media transmisi yang digunakan dalam topologi untuk penelitian ini tidak menggunakan kabel (wireless). Berikut ini adalah topologi jaringan yang digunakan dapat dilihat pada gambar 2.



Gambar 2. Topologi Jaringan yang digunakan.

Pada tahapan testing peneliti melakukan implementasi dan pengujian terhadap aktifitas web browser pengguna dalam satu jaringan. Metode yang digunakan peneliti adalah Metode Manual Penetration Testing. Kegiatan yang dilakukan peneliti dalam penelitian ini adalah sebagai berikut :

a. Data Collection & Vulnerability Assessment
Pada tahap ini dilakukan pengumpulan data serta analisa keamanan secara menyeluruh terhadap bebagai dokumen terkait keamanan informasi dan hasil scanning jaringan untuk keberlangsungan penelitian. Data yang dikumpulkan berupa :

- Pencarian Informasi IP Gateway

Gateway merupakan sebuah perangkat untuk menghubungkan dari satu jaringan kompuetr dengan jaringan komputer yang lainnya yang menggunakan berbagai protokol komunikasi yang berbeda. Informasi IP gateway menjadi hal yang penting dalam penelitian ini karena proses eksploitasi akan memanipulasi IP gateway jaringan yang digunakan.

- Pencarian Data IP Address

Data IP address yang aktif diperlukan untuk menentukan IP address yang akan dijadikan sebagai target eksploitasi. Penelitian ini akan menyeleksi target secara spesifik dengan tujuan lalu lintas data yang tertangkap hanya berasal dari satu IP address.

- Pencarian Informasi Berdasarkan IP Address

Tahap ini peneliti akan menggali informasi mengenai sistem operasi yang digunakan dan scanning port berdasarkan IP address yang sudah ditemukan.

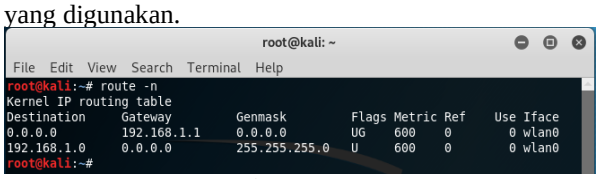
b. Actual Exploit
Pada tahap Actual Exploit penulis menjelaskan implementasi dari framework MITM serta melakukan pengujian terhadap pengguna yang berada dalam satu jaringan. Peneliti menggunakan kode untuk melakukan eksploitasi terhadap keamanan komputer. Actual Exploit untuk memantau aktifitas pengguna lain dalam satu jaringan dapat menggunakan tools MITMF.

c. Report Preparation
Pada tahapan ini penulis memaparkan hasil dari pengujian yang dilakukan. Hasil yang didapatkan akan di paparkan menggunakan table yang meliputi informasi IP address, sistem operasi yang digunakan, waktu akses website, alamat website yang di akses, serta username dan password

III. HASIL DAN PEMBAHASAN

a. Data Collection and Vulnerability Assesment
Pengumpulan informasi mengenai IP address menggunakan tools nmap yang sudah ada di dalam sistem operasi Kali Linux. Data yang didapatkan pada tahap ini akan digunakan pada proses pengujian. Pada tahap ini juga akan mengamati informasi sistem operasi, nama perangkat, dan port yang terbuka berdasarkan IP address.

- Pencarian Informasi IP Gateway
Berikut ini adalah informasi alamat gateway jaringan yang digunakan.

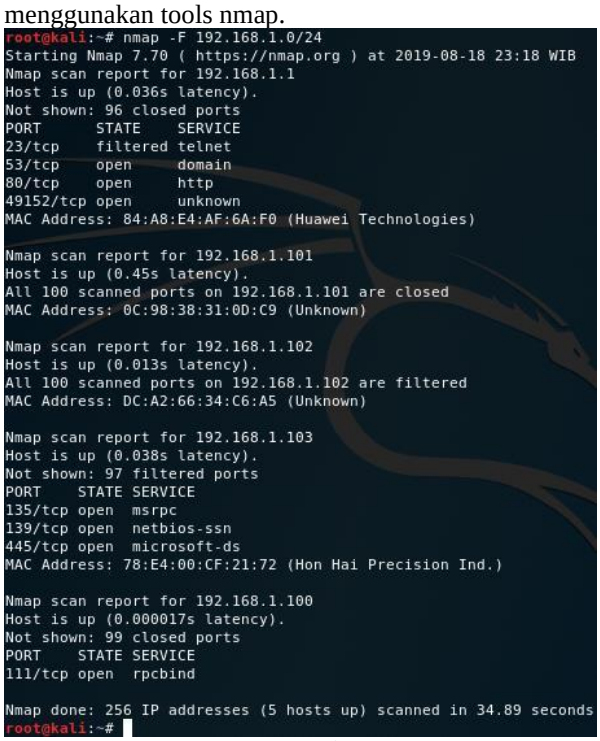


Gambar 3. Informasi Gateway.

Berdasarkan gambar 3 diatas informasi gateway jaringan yang digunakan telah didapatkan yaitu 192.168.1.1.

- Pencarian Data IP Address
Mengetikkan perintah nmap –F 192.168.1.0/24 pada terminal Kali Linux. Dengan perintah tersebut nmap akan berjalan dan parameter –F akan melakukan

pencarian terhadap IP address pada range 192.168.1.0/24. Berikut ini adalah hasil dari pencarian data IP address yang aktif dalam satu jaringan menggunakan tools nmap.



Gambar 4. Pencarian IP address aktif menggunakan nmap.

Berdasarkan hasil pencarian IP address yang aktif menggunakan nmap pada gambar 4 diatas penulis paparkan hasil pencarian tersebut dalam bentuk tabel sebagai berikut.

TABEL 3
DATA IP ADDRESS AKTIF

No	IP ADDRESS	STATUS
1	192.168.1.1	UP
2	192.168.1.100	UP
3	192.168.1.101	UP
4	192.168.1.102	UP
5	192.168.1.103	UP

- Pencarian Informasi Berdasarkan IP Address

Tahap berikutnya yaitu melakukan penggalian informasi dari setiap data IP address. Berikut ini hasil pencarian informasi berdasarkan IP address yang telah ditemukan pada tahap sebelumnya:

Dengan menggunakan tools nmap didapatkan informasi mengenai sistem operasi yang digunakan. Berdasarkan penggalian informasi diatas, berikut informasi tersebut dalam bentuk tabel sebagai berikut.

TABEL 4
INFORMAASI IP ADDRESS AKTIF

IP ADDRESS	MAC ADDRESS	OS	KERNEL
192.168.1.1	84:A8:E4:AF:6A:F0	Linux	2.6
192.168.1.100	-	Linux	3
192.168.1.101	0C:98:38:31:0D:C9	-	-
192.168.1.102	70:C9:4E:E1:5E:BD	Windows	-
192.168.1.103	78:E4:00:CF:21:72	Windows 7	-

b. Actual Exploit

- Implementasi

Dalam tahap ini dilakukan implementasi framework MITM untuk memonitoring pengguna dalam satu jaringan. Berikut ini langkah-langkah implementasi framework MITM untuk memantau pengguna dalam satu jaringan.

1) Install paket-paket library
2) Download MITMF
3) Download dan update submodule MITMF
4) Install paket requirements
5) Mengaktifkan ip forwarding dengan mengetikkan perintah pada terminal "echo 1 > /proc/sys/net/ipv4/ip_forward". Perintah tersebut bertujuan agar perangkat dapat meneruskan paket data ke jaringan yang berbeda.
6) Menjalankan MITMf dan melihat perintah-perintah yang bisa dijalankan pada MITMF dengan mengetikkan perintah "./mitmf.py" di dalam directory MITMF.

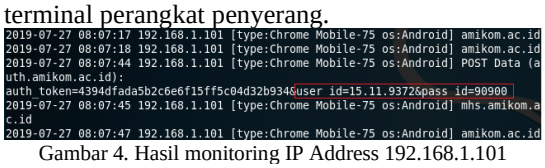
- Pengujian

Pada tahap pengujian ini dilakukan pengujian dengan mengakses website yang menggunakan protokol HTTP dan HTTPS. Dengan melakukan pengujian terhadap protokol yang berbeda tersebut akan ditemukan perbedaan hasil penelitian yang berbeda Berikut adalah langkah-langkah pengujian yang dilakukan:

1) Pengujian protokol HTTP

Pengujian dilakukan dengan menjalankan tools MITMF dan mengakses alamat website auth.amikom.ac.id melalui perangkat pengguna smartphone dan Chrome Mobile web browser. Berikut ini adalah langkah dari pengujian framework MITM pada website yang menggunakan protokol HTTP:

- Menjalankan framework MITM dengan mengetikkan perintah ./MITMF.py pada terminal linux.
- Menentukan interface jaringan yang digunakan dengan menggunakan argument "–i wlan0".
- Menentukan options --arp dan --spoof untuk memanipulasi MAC address
- Memasukkan IP Gateway yang telah didapatkan yaitu 192.168.1.1
- Memasukkan IP address target monitoring 192.168.1.101
- Menjalankan Chrome Mobile browser pada perangkat target monitoring untuk mengakses alamat auth.amikom.ac.id dan melakukan input data login
- Data yang tertangkap akan ditampilkan di dalam terminal perangkat penyerang.



Gambar 4. Hasil monitoring IP Address 192.168.1.101

b) Pengujian protokol HTTPS

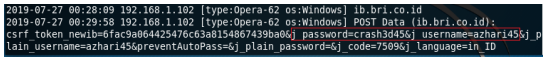
Pengujian dilakukan dengan menjalankan framework MITM dan mengakses alamat website ib.bri.co.id melalui perangkat pengguna laptop dan Opera web browser. Berikut ini adalah

langkah dari pengujian framework MITM pada website yang menggunakan protokol HTTPS:

- Menjalankan tools MITMF dengan perintah ./MITMF.py
- Menentukan options --arp dan --spoof untuk memanipulasi MAC address
- Memasukkan data ip gateway yang telah didapatkan pada tahap sebelumnya yaitu 192.168.1.1
- Memasukan IP address target monitoring 192.168.1.102
- Mengaktifkan SSLStrip dengan perintah --hsts.

Gambar 5. Monitoring IP address 192.168.1.102

- Menjalankan Opera Web browser dan memasukkan alamat ib.bri.co.id pada kotak URL. Akses perangkat ke alamat ib.bri.co.id secara otomatis dialihkan ke alamat webib.bri.co.id. Berikut tampilan gambar ib.bri.co.id setelah dialihkan.
- Data yang tertangkap akan ditampilkan pada terminal linux.



Gambar 5. Hasil Monitoring IP address 192.168.1.102

c. Report Preparation

Hasil pengujian yang dilakukan berupa username dan password proses login pada website yang diakses dari perangkat target pada penelitian. Data yang diperoleh akan dipaparkan dalam bentuk tabel laporan hasil pengujian. Berikut ini adalah hasil dari pengujian implementasi framework MITM untuk memantau aktifitas pengguna dalam satu jaringan dapat dilihat pada table 5.

TABEL 5
LAPORAN HASIL PENGUJIAN

IP ADDRESS	Browser	OS	URL	Hasil
192.168.1.101	Chrome Mobile-75	Android	auth.amikom.ac.id	Berhasil mendapatkan username dan password
192.168.1.102	Opera-62	Windows	ib.bri.co.id	Berhasil mendapatkan username dan password
			https://ib.bri.co.id	Aktivitas browsing tidak terdeteksi
192.168.1.103	Chrome -76	Windows	www.bukalapak.com	Berhasil mendapatkan username dan password
			https://www.bukalapak.com	Aktivitas browsing tidak terdeteksi
192.168.1.103	Internet Explore-11	Windows	sim.unissula.ac.id	Berhasil mendapatkan username dan password
			https://sim.unissula.ac.id	Aktivitas browsing tidak terdeteksi

- Menentukan interface jaringan yang digunakan yaitu wlan0 dengan mengetikkan argument "-i wlan0"

IV. KESIMPULAN

Kesimpulan dari penelitian ini yaitu implementasi framework MITMF untuk memantau aktivitas pengguna dalam satu jaringan berhasil dilakukan. Dibuktikan dengan keberhasilan mengambil paket data yang lewat dan menampilkannya pada *command line*. Hasil pengujian yang telah dilakukan berupa username dan password pada suatu website tanpa diamankan oleh kode enkripsi. Website yang dapat di bypass username dan passwordnya adalah website dengan protokol keamanan HTTP. Sedangkan terhadap protokol keamanan HTTPS tidak mampu untuk mendeteksi aktivitas browser. Akses terhadap website dengan protokol keamanan HTTPS bisa dialihkan ke protokol keamanan HTTP

REFERENSI

[1] S. W, "BSSN dan Peta Keamanan Siber Indonesia" 05 Maret 2018.[Online]. Available: https://inet.detik.com/cyberlife/d-3899799/bssn-dan-peta-keamanan-siber-indonesia. [Diakses 10 Februari 2019]

[2] I. Yuliana., 2019. "Adopsi Social Network Analysis (Sna) Dalam Upaya Membangun Ketangguhan Bencana Di Masyarakat," JIKO (Jurnal Inform. dan Komputer), vol. 2, no. 2, pp. 49–54.

[3] D. Saputra and I. Riadi, "Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method," International Journal of Cyber-Security and Digital Forensics, vol. 8, no. 1, pp. 66–73, 2019, doi: 10.17781/p002558.

[4] Pratama, I Putu AE, S.T., M.T.2015. Handbook Jaringan Komputer Teori dan Praktik Berbasiskan Open Source. Bandung: Informatika.

[5] G. N. Nayak and S. G. Samaddar, 2010. "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions," Proc. - 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010, vol. 5, pp. 491–495, 2010.

[6] Kamajaya, Gede.E.A, Riadi,I., Prayudi.P, Imam Riadi Analisa Investigasi Static Forensics Serangan Man In The Middle Berbasis ARP Poisoning. JIKO (Jurnal Informatika dan Komputer) Akreditasi KEMENRISTEKDIKTI, Vol. 3, No. 1, April 2020, hlm. 6-12 DOI: 10.33387/jiko

[7] Github (2019, Feb.10) Framework for Man-In-The-Middle attacks [Online]. Available: https://github.com/byt3bl33d3r/MITMF

[8] Setiyadi, A. 2017. "Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet".Prosiding Seminar Nasional Komputer dan Informatika (SENASKI).

[9] Muhammad, IZ, Moch Fahru Rizal, S.T., M.T, Mia Rosmiati, S.Si, M.T.2017. "Implementasi BadUSB MITM Attacks Menggunakan Remote Penetrastion Test Pada Kali NetHunter". e-Proceeding of Applied Science.3(3): 1902.

[10] Shubh, T, M.Tech(CE), Shweta Sharma.2016. "Man-In-The-Middle-Attack Prevention Using HTTPS and SSL". International Journal of Computer Science and Mobile Computing.5(6): 569-579.