Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet

Angga Setiyadi
Jurusan Teknik Informatika FTIK UNIKOM
Jl. Dipati Ukur No. 112-118 Bandung 40132
Email : angga.setiyadi@email.unikom.ac.id

Abstrak – Monitoring jaringan merupakan salah satu bagian dalam manajemen jaringan dimana monitoring berfungsi untuk mengevaluasi performa dan melihat efisiensi serta stabilitas operasional. Analisa dan monitoring trafik diperlukan untuk meningkatkan kualitas layanan jaringan karena adanya keragaman kebutuhan bandwidth oleh arus trafik yang dihasilkan dari aplikasi berbeda. Websploit adalah software yang dikembangkan oleh team offensife security yang mempunyai fungsi untuk menganalisis sistem dimana sebuah kelemahan atau bug akan dicari. Salah satu modul yang ada pada websploit adalah module network/MITM atau Man In The Middle Attack. Man In The Middle Attack adalah salah satu teknik kemanan jaringan dimana penyadap menempatkan dirinya berada di tengah-tengah perangkat yang saling berkomunikasi. IP yang di monitor adalah 192.168.1.9, yang mengakses halaman web http://www.unikom.ac.id dan http://www.kompas.com.

Kata kunci *:* Monitoring aktifitas pengguna, WEBSPLOIT, MITM, Akses Internet

I. PENDAHULUAN

Jaringan komputer merupakan suatu sistem yang menghubungkan berbagai komputer untuk dapat berbagi sumber daya, komunikasi dan akses informasi. Jaringan komputer telah menjadi suatu hal yang sangat penting untuk mendukung berbagai aktifitas.

Monitoring terhadap lalu lintas data di jaringan merupakan hal yang paling utama dan penting yang harus dilakukan oleh seorang administrator. Dengan melakukan monitoring aktifitas pengguna internet didalam jaringan hasilnya dapat digunakan untuk keperluan pemantauan keamanan jaringan.

A. Latar Belakang

Monitoring jaringan merupakan salah satu bagian dalam manajemen jaringan dimana monitoring berfungsi untuk mengevaluasi performa dan melihat efisiensi serta stabilitas operasional. Analisa dan monitoring trafik diperlukan untuk meningkatkan kualitas layanan jaringan karena adanya keragaman kebutuhan bandwidth oleh arus trafik yang dihasilkan dari aplikasi berbeda.

Websploit adalah software yang dikembangkan oleh team offensife security yang mempunyai fungsi untuk menganalisis sistem dimana sebuah kelemahan atau bug akan dicari. Salah satu modul yang ada pada websploit adalah module network/MITM atau *Man In The Middle Attack. Man In The Middle Attack* adalah salah satu teknik kemanan jaringan dimana penyadap menempatkan dirinya berada di tengah-tengah perangkat yang saling berkomunikasi.

B. Tujuan

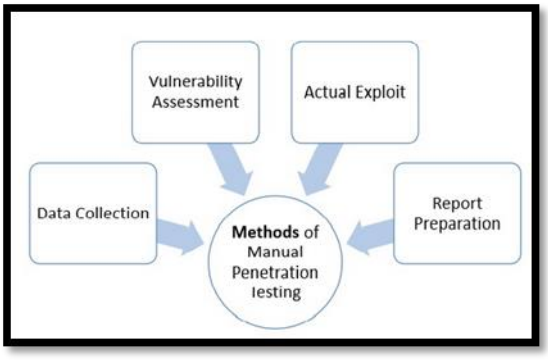
Tujuan penelitian ini adalah untuk mengimplementasikan modul network MITM pada websploit sebagai monitoring aktifitas pengguna dalam mengakses internet.

C. Rumusan Masalah

Berdasarkan uraian latar belakang permasalahan yang telah diuraikan, maka rumusan masalah yang akan dikaji dalam penelitian ini adalah *"Bagaimana mengimplementasikan modul network MITM pada websploit sebagai monitoring aktifitas pengguna dalam mengakses internet"*

D. Tahap Penelitian

Adapun tahapan penelitian yang dilakukan untuk Implementasi modul network/MITM Pada websploit untuk memonitoring aktifitas pengguna dalam mengakses internet dapat dilihat pada gambar 1 [3].



Gambar 1. Metoda *Penetration Testing*

II. TINJAUAN PUSTAKA

A. Jaringan Komputer

Jaringan komputer adalah himpunan "Interkoneksi" antara 2 komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (wireless). Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data/informasi, berbagi resource yang dimiliki, seperti file, printer, media penyimpanan (hardisk, floppy disk, cd-rom, flash disk,dll) [1].

Manfaat jaringan komputer bagi pengguna adalah sebagai berikut :

1. Mengakses informasi yang berada di lingkungan yang berbeda.
2. Komunikasi antar pengguna
3. Hiburan interaktif

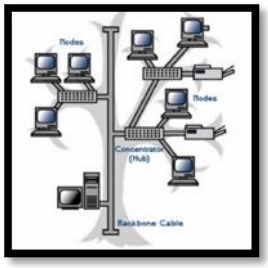
B. Topologi Jaringan

Topologi menggambarkan struktur jaringan, atau bagaimana sebuah jaringan didesain. macam-macam topologi jaringan diantaranya adalah sebagai berikut [2] :

1. Topologi Pohon

   Topologi pohon merupakan topologi yang bisa digunakan pada jaringan didalam ruangan kantor yang bertingkat. Pada jaringan pohon, terdapat beberapa tingkatan simpul (node). Keunggulan jaringan model pohon adalah dapat membentuk suatu kelompok yang dibutuhkan pada setiap saat.

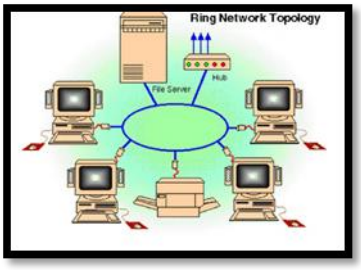
   Berikut ini adalah gambar dari topologi pohon dapat dilihat pada gambar 2.



Gambar 2. Topologi Pohon

2. Topologi Cincin

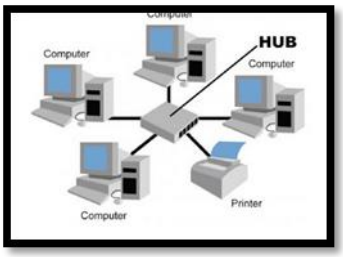
   Topologi cincin adalah topologi jaringan disetiap komputer yang terhubung akan membuat lingkaran. Adapun kelebihan dari topologi ini adalah kabel yang digunakan bisa lebih dihemat. Berikut ini adalah gambar dari topologi cincin dapat dilihat pada gambar 3.



Gambar 3. Topologi Cincin

3. Topologi Bintang (*Star*)

   Topologi bintang atau yang lebih sering disebut dengan star topology sudah menggunakan bantuan alat lain untuk mengkoneksikan jaringan komputer. Alat yang dipakai disini adalah hub atau switch. Keuntungan dari topologi ini dapat memudahkan admin dalam mengelola jaringan, dapat memudahkan dalam penambahan komputer atau terminal serta memudahkan mendeteksi kerusakan dan kesalahan jaringan. Berikut ini adalah gambar dari topologi star dapat dilihat pada gambar 4.

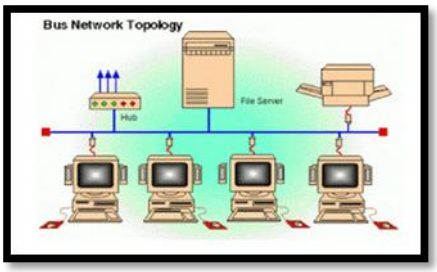


Gambar 4. Topologi Bintang (*Star*)

4. Topologi Bus

   Topologi ini adalah topologi awal yang digunakan untuk menghubungkan komputer. Dalam topologi ini, masing-masing komputer akan terhubung ke satu kebel panjang dengan beberapa terminal dan pada akhir dari kabel harus diakhiri dengan satu terminator. Keuntungan dari topologi bus adalah pengembangan jaringan atau penambahan workstation baru dapat dilakukan dengan mudah tanpa mengganggu workstation lain.

   Berikut ini adalah gambar dari topologi star dapat dilihat pada gambar 5.



Gambar 5. Topologi Bus

C. Internet

Internet (*Interconnection-Networking*) adalah seluruh jaringan komputer yang saling terhubung menggunakan standar sistem global transmission control protocol/internet protocol suite (TCP/IP) sebagai protokol pertukaran paket *(packet switching communication protocol*) untuk melayani miliaran pengguna di seluruh dunia.

Pada dasarnya internet bekerja dengan adanya alamat IP (*Internet Protocol*) yang akan menjadi penghubung dari server-server lain yang tersebar didunia. Kerja internet sangat cepat, karena didukung oleh satelit yang dengan mudah memancarkan gelombang internet ke bagian lain di penjuru bumi. Satu server terbesar memegang kendali akses situs seluruh dunia, dan server itu disebarkan satu-persatu di tiap negara atau daerah lainnya. Server di berbagai belahan dunia saling terhubung dan terpusat. Setiap server ditandai dengan alamat yang disebut IP (*Internet Protocol*). IP ini yang akan membedakan koneksi internet pada server satu dengan yang lain. Client komputer yang dipasang internet nantinya akan berhubungan langsung dengan server terdekat untuk terus terhubung dengan *client* lainnya di penjuru dunia.

D. KALI Linux

Kali Linux adalah distribusi berlandasan distribusi Debian GNU/Linux untuk tujuan forensik digital dan digunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh *Offensive Security*. Kali linux dikembangkan oleh pengembang Backtrack sebelumnya yaitu Mati Aharoni bersama pengembang baru bernama Devon Kearns dari Offensive Security.

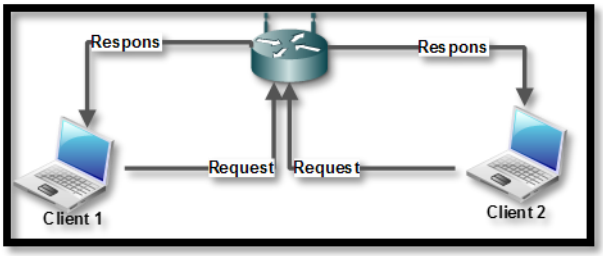
Secara umum kali linux memiliki berbagai macam tools yang dapat dibagi ke dalam beberapa kasifikasi berdasarkan fungsi utamanya yaitu :

1. *Information Gathering* digunakan untuk mengumpulkan informasi dari suatu sistem
2. *Reverse Enginerring* digunakan untuk menganalisa suatu sistem melalui identifikasi komponen=komponennya dan keterkaitan antar komponen tersebut lalu membuat abstraksi dan informasi perancangan dari sistem yang dianalisa
3. *Exploitation Tools* digunakan untuk mengekspoitasi celah yang terdapat pada suatu sistem.
4. *Vulnerability Assessement* digunakan untuk melakukan pencarian, identifikasi, perhitungan terhadap celah keamanan suatu sistem
5. *Privilege Escalation* digunakan untuk melakukan serangan yang bertujuan untuk menaikkan tingkat akses didalam suatu sistem.

E. Man In The Middle

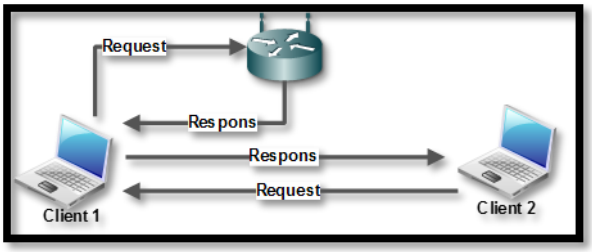
Man In The Middle Attack adalah salah satu teknik dalam keamanan jaringan dimana penyusup menempatkan dirinya berada di tengah-tengah dua perangkat atau lebih yang saling berkomunikasi. Hasil dari teknik *Man In The Middle Attack* ini adalah penyadapan informasi.

Man In The Middle Attack bekerja dengan mengeksploitas ARP (*Address Resolution Protocol*). Protokol ARP merupakan sebuah protokol yang bertanggung jawab mencari tahu MAC Address atau alamat hardware dari suatu host yang tergabung dalam sebuah jaringan LAN dengan memanfaatkan atau berdasarkan IP Address yang terkonfigurasi pada host yang bersangkutan. Berikut ini adalah gambar pengiriman data sebelum dilakukan serangan *Man In The Middle Attack* dapat dilihat pada gambar 6



Gambar 6. Pengiriman Data Sebelum Dilakukan Serangan Man In The Middle Attack

Berikut ini adalah gambar pengiriman data setelah dilakukan serangan *Man In The Middle Attack* dapat dilihat pada gambar 7



Gambar 7. Pengiriman data setelah dilakukan serangan Man In The Middle Attack

F. WEBSPLOIT

Websploit adalah software yang mempunyai fungsi untuk menganalisa suatu sistem untuk menemukan berbagai jenis kerentanan. Webspoit adalah proyek open source yang dikembangkan oleh team Offensife Security. Beberapa module didalam webspoit diantaranya adalah sebagai berikut :

1. Autopwn digunakan dari metaspoit untuk scan dan ekspoitasi sasaran layanan
2. WMAP digunakan untuk memindai metaspoit wmap plugin
3. Format Infector digunakan untuk Menyuntikan payload ke dalam format file
4. Phpmyadmin digunakan untuk mencari target halaman login di phpmyadmin
5. LFI digunakan untuk memindai, mengambil alih website.
6. Apache user digunakan untuk mencari nama direktori server

7. Dir Bruter digunakan untuk mencari direktori target dengan wordlist
8. Admin Finder digunakan untuk mencari halaman login admin
9. MLITM Attack digunakan untuk serangan XSS Phising
10. MITM digunakan untuk mengeksploitasi ARP
11. Java Applet Attack digunakan untuk menyerang applet java
12. *USB Infection Attack* digunakan untuk membuat backdoor executable untuk menginfeksi USB pada operating sistem windows
13. *WEB Killer Attack* digunakan untuk membuat tidak berfungsinya suatu website.

Perintah-perintah yang digunakan pada module MITM adalah sebagai berikut ini :

1. Perintah untuk menggunakan module MITM

```
use network/mitm
```

2. Perintah untuk melihat opsi pada module MITM

```
show options
```

3. Perintah untuk menggunakan interface dari ethernet

```
set Interface eth0
```

4. Perintah untuk menset alamat gateway

```
set ROUTER alamatgateway
```

5. Perintah untuk menset alamat target

```
set TARGET alamattarget
```

6. Perintah untuk memindai alamat url yang dikunjungi target

```
set SNIFFER urlsnarf
```

7. I MITM pada webspoit

```
run
```

G. NMAP

Nmap digunakan untuk menemukan *hosts* serta services yang aktif di dalam jaringan komputer. NMAP adalah security scanner/network scanner yang ditemukan oleh Gordon Lyon. Berikut ini adalah perintah-perintah yang sering digunakan pada NMAP diantaranya :

1. Perintah untuk *Host Discovery*

```
nmap –sP [targetIP]
```

2. Perintah untuk Multi IP Scanning

```
nmap [targetIP] [targetIP]
```

3. Perintah untuk Mendeteksi sistem operasi

```
nmap -O [targetIP]
```

4. Perintah untuk mengetahui Multi IP Scanning

```
nmap -O [targetIP]
```

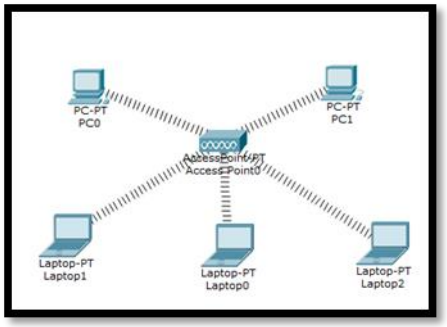
5. Perintah untuk melakukan scanning dengan menampilkan informasi dari service tertentu

```
Nmap –sV [targetIP]
```

III. IMPLEMENTASI

A. Skema Jaringan

Skema jaringan untuk implementasi modul network MITM pada websploit sebagai monitoring aktifitas pengguna dalam mengakses internet dapat dilihat pada gambar 8.



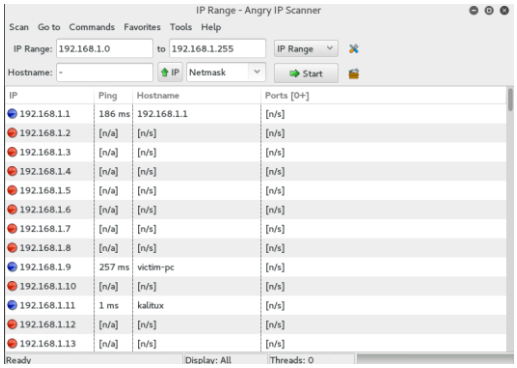
Gambar 8. Analisis Jaringan implementasi modul network MITM pada websploit sebagai monitoring aktifitas pengguna dalam mengakses internet

B. Data Collection & Vulnerability Assesement

Data collection/pengumpulan data dilakukan untuk memperoleh informasi yang dibutuhkan dalam rangka mencapai tujuan penelitian. Sedangkan vulnerability assessment adalah analisa keamanan yang menyeluruh serta mendalam terhadap berbagai dokumen terkait keamanan informasi, hasil scanning jaringan, konfigurasi pada sistem untuk mengetahui seluruh potensi kelemahan kritis yang ada. Data yang dikumpulkan dalam penelitian ini diantaranya adalah sebagai berikut :

1. Data IP Address yang sedang aktif

Pencarian IP Address yang sedang aktif menggunakan aplikasi *angry ip scanner*. Berikut ini adalah gambar dari hasil pencarian data atau scanning IP Address yang aktif dapat dilihat pada gambar 9.



Gambar 9. *Scanning IP Address* Menggunakan *Angry IP Scanner*

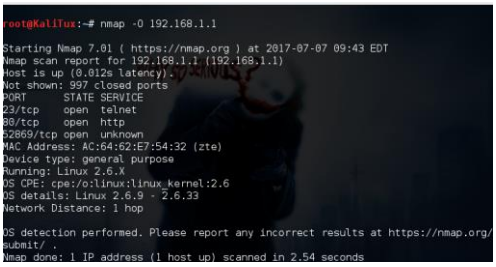
Berdasarkan gambar 9 terdapat 3 IP Address yang aktif diantaranya adalah alamat IP 192.168.1.1, 192.168.1.9 dan 192.168.1.11

2. Data Informasi Berdasarkan IP Address

Penggalian data informasi dilakukan untuk mencari data operating sistem yang digunakan. Pencarian data operating sistem yang digunakan menggunakan software NMAP. Berikut ini adalah hasil penggalian data informasi untuk setiap IP Address.

a. IP Address 192.168.1.1

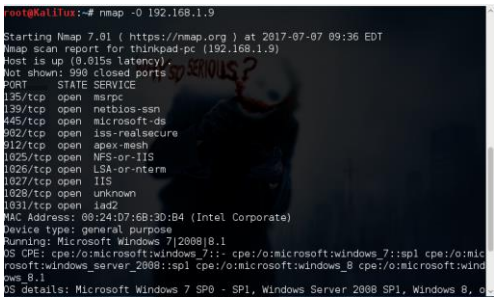
Sistem operasi yang digunakan oleh IP Address 192.168.1.1 yaitu sistem operasi Linux dengan computer name 192.168.1.1. Berikut ini adalah gambar dari penggalian data informasi IP Address 192.168.1.1 dapat dilihat pada gambar 10.



Gambar 10. Penggalian Data Informasi IP Address 192.168.1.1

b. IP Address 192.168.1.9

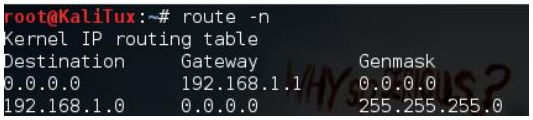
Sistem operasi yang digunakan oleh IP Address 192.168.1.9 yaitu sistem operasi windows 7 dengan *computer name* THINKPAD-PC. Berikut ini adalah gambar dari penggalian data informasi IP Address 192.168.1.9 dapat dilihat pada gambar 10.



Gambar 10. Penggalian Data Informasi IP Address 192.168.1.9

3. Data Informasi IP Gateway

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda. Alamat gateway pada implementasi modul network mitm pada websploit untuk memonitoring aktifitas pengguna dalam mengakses internet adalah 192.168.1.1 Berikut ini adalah data informasi IP Gateway dapat dilihat pada gambar 12.



Gambar 12. Informasi IP Gateway

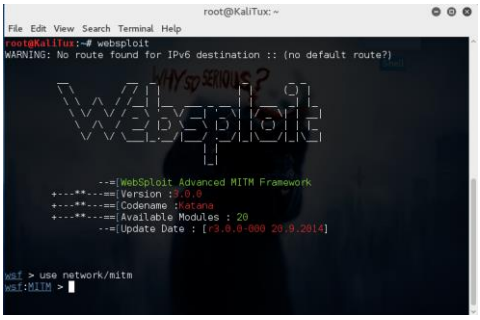
C. Actual Exploit

Actual Exploit adalah sebuah teknik atau metoda menggunakan atau memanfaatkan sebuah kode untuk menyerang keamanan komputer atau sistem secara spesifik. *Actual Exploit* untuk memonitoring aktifitas pengguna dalam mengakses internet menggunakan software websploit dan modul yang digunakan adalah network/MITM. Langkah implementasi modul network/MITM untuk memonitoring aktifitas pengguna dalam mengakses internet adalah sebagai berikut :

1. Perintah websploit pada console digunakan untuk memberikan masuk kedalam aplikasi websploit. Berikut ini adalah layar keluaran dari mengetikan perintah websploit dapat dilihat pada gambar 13

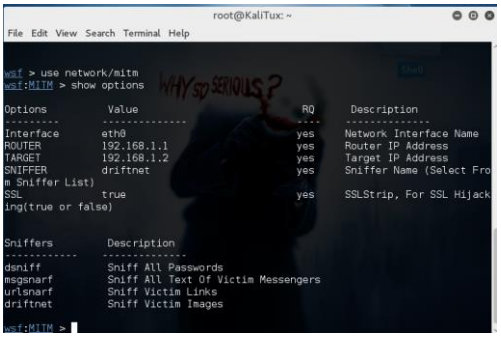
Gambar 13. Layar utama websploit

2. Perintah use network/mitm digunakan untuk menggunakan module network/mitm pada websploit. Berikut ini adalah layar keluaran menggunakan module network/mitm pada websploit dapat dilihat pada gambar 14.



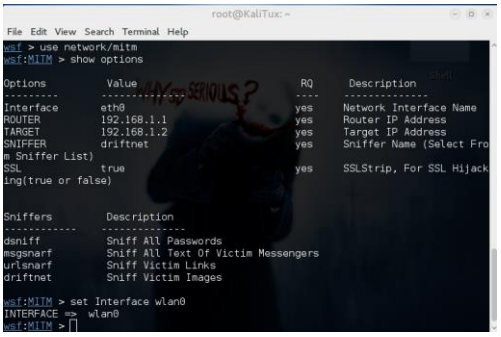
Gambar 14. Perintah network/mitm

3. Perintah *show options* digunakan untuk melihat opsi yang ada pada modul MITM. Berikut ini adalah layar keluaran mengetikan perintah *show options* pada module network/mitm dapat dilihat pada gambar 15.



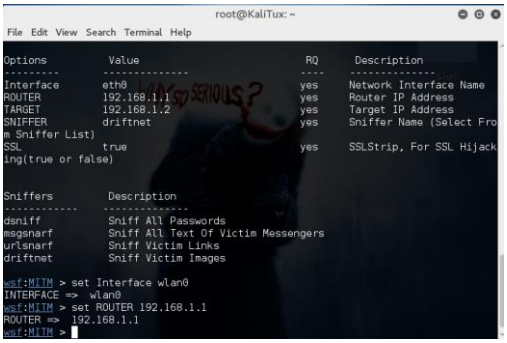
Gambar 15. Perintah *show options*

4. Perintah *set interface* wlan0 digunakan untuk menggunakan komponen *wireless*. Berikut ini adalah layar keluaran mengetikan perintah *set interface* wlan0 pada module network/mitm dapat dilihat pada gambar 16.



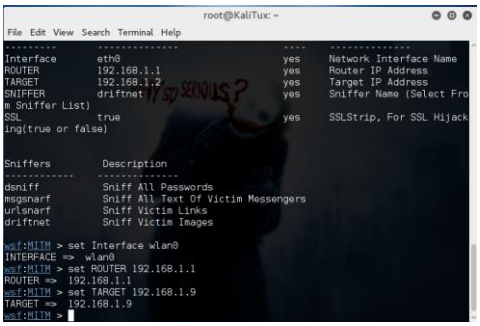
Gambar 16. Perintah *show interface wlan0*

5. Perintah *set ROUTER* 192.168.1.1 digunakan untuk menset alamat IP router/gateway yang digunakan didalam jaringan. Berikut ini adalah layar keluaran mengetikan perintah *set ROUTER* 192.168.1.1 pada module network/mitm dapat dilihat pada gambar 17.



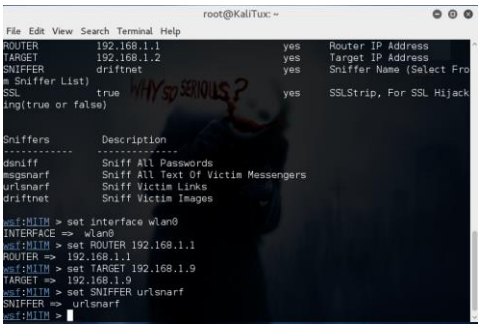
Gambar 17. Perintah set ROUTER 192.168.1.1

6. Perintah *set target 192.168.1.9* digunakan untuk menset alamat IP target. Alamat IP yang akan dimonitoring aktifitas pengguna dalam mengakses internet adalah IP 192.168.1.9. Berikut ini adalah layar keluaran mengetikan perintah *set target 192.168.1.9* pada module network/mitm dapat dilihat pada gambar 18.



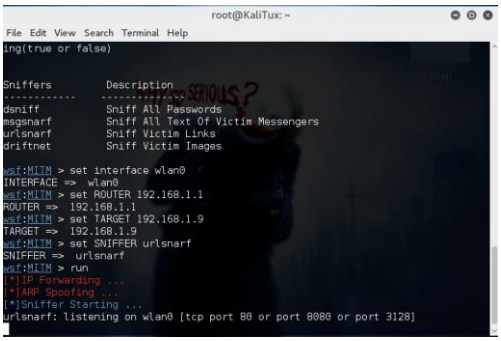
Gambar 18. Perintah set TARGET 192.168.1.9

7. Perintah set *SNIFFER urlsnarf* digunakan untuk memindai alamat url yang dikunjungi oleh target. Berikut ini adalah layar keluaran mengetikan perintah *SNIFFER urlsnarf* pada module network/mitm dapat dilihat pada gambar 19.



Gambar 19. Perintah set *SNIFFER urlsnarf*

8. Perintah RUN digunakan untuk menjalankan konfigurasi-konfigurasi perintah yang telah diset sebelumnya. Berikut ini adalah layar keluaran mengetikan perintah *run* pada module network/mitm dapat dilihat pada gambar 20.

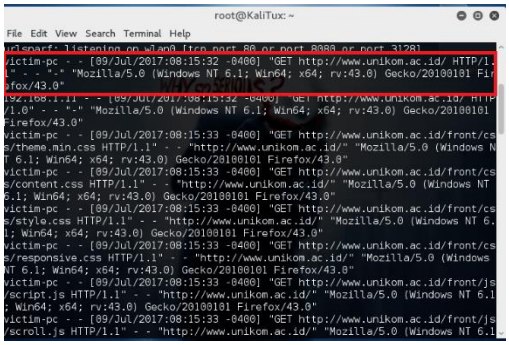


Gambar 20. Perintah *run*

D. Report Preparition

Report prepartion adalah penguraian secara detail laporan hasil dari *actual exploit* dengan bukti-bukti yang sudah diproses secara mendalam dan dapat dipertanggungjawabkan secara ilmiah. Berikut ini adalah hasil pengujian monitoring aktifitas alamat IP 192.168.1.9 dalam mengakses internet Berdasarkan tahapan yang telah dilakukan pada langkah *actual exploit* :

1. Pengujian dengan mengakses halaman web http://www.unikom.ac.id. Berikut ini adalah Hasil pengujian dari alamat IP 192.168.1.9 dengan mengakses http://www.unikom.ac.id dapat dilihat pada gambar 21.



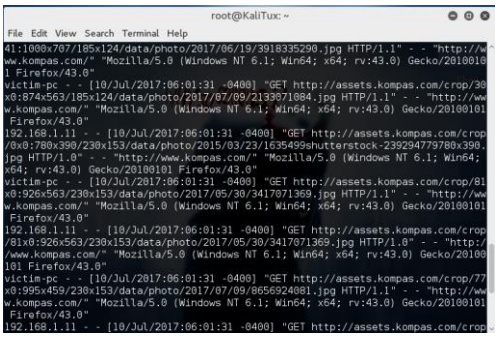
Gambar 21. Pengujian 1 dengan mengakses halaman WEB www.unikom.ac.id

Hasil laporan dari alamat IP 192.168.1.9 dengan mengakses halaman WEB www.unikom.ac.id dapat dilihat pada tabel 1.

Tabel 1. Hasil Laporan Pengujian 1

Computer Name	Victim-pc
Tanggal Akses	9 Juli 2017
Jam Akses	08:15:32
Alamat URL yang diakses	http://www.unikom.ac.id
Browser yang digunakan	Mozilla
Sistem Operasi yang digunakan	Windows NT

2. Pengujian dengan mengakses halaman web http://www.kompas.com. Hasil pengujian dari alamat IP 192.168.1.9 dengan mengakses http://www.kompas.com dapat dilihat pada gambar 22.



Gambar 22. Pengujian 2 dengan mengakses halaman WEB www.kompas.com

Hasil laporan dari alamat IP 192.168.1.9 dengan mengakses halaman WEB www.kompas.com dapat dilihat pada tabel 2.

Tabel 2. Hasil Laporan Pengujian 1

Computer Name	Victim-pc
Tanggal Akses	10 Juli 2017
Jam Akses	06:01:32
Alamat URL yang diakses	http://www.kompas.com/
Browser yang digunakan	Mozilla
Sistem Operasi yang digunakan	Windows NT

IV. KESIMPULAN

Berdasarkan uraian pembahasan implementasi dan pengujian yang telah dilakukan, maka dapat diambil kesimpulan bahwa penelitian ini sudah dapat mengimplementasikan modul network mitm pada websploit untuk memonitoring aktifitas pengguna dalam mengakses internet.

REFERENSI

[1] M. Syafrizal, Pengantar Jaringan Komputer, Yogyakarta, C.V. Andi Offset, 2005

[2] E.V.Haryanto, Jaringan Komputer, Yogyakarta, C.V. Andi Offset, 2012

[3] tutorialspoint (2017, Jul.8) Penetration Testing - Manual & Automated [online]. Available : https://www.tutorialspoint.com/penetration_testing/penetration_testing_manual_automated.htm