# 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.[4]

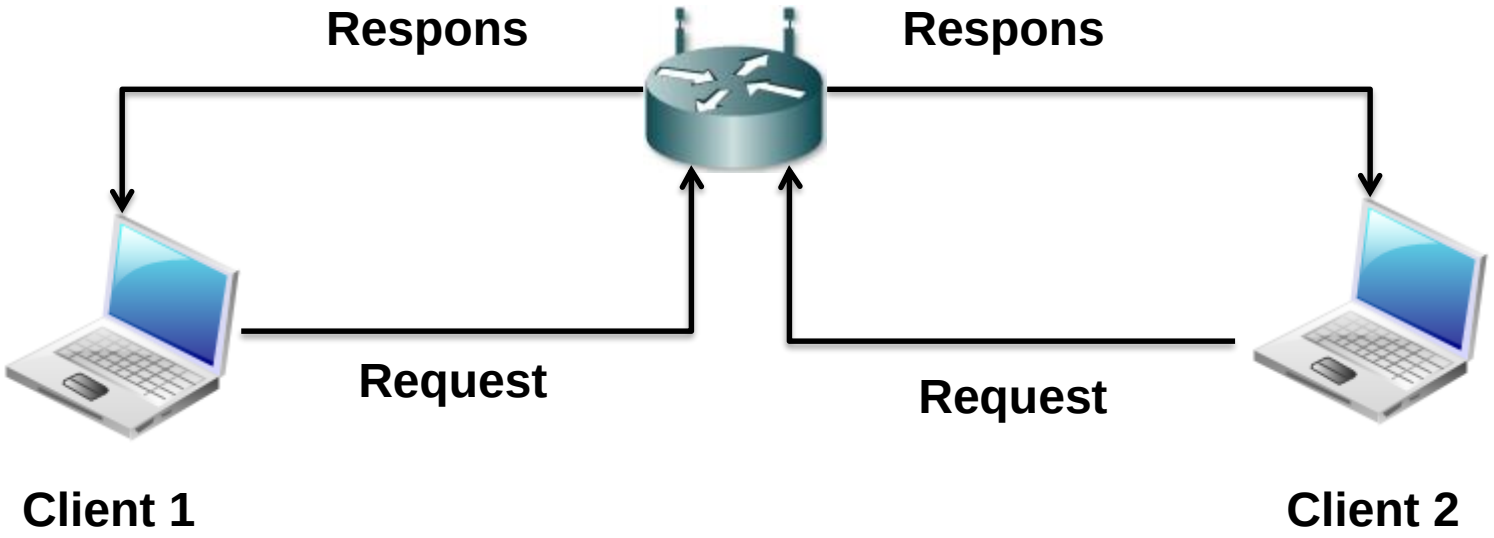
# Definisi

*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

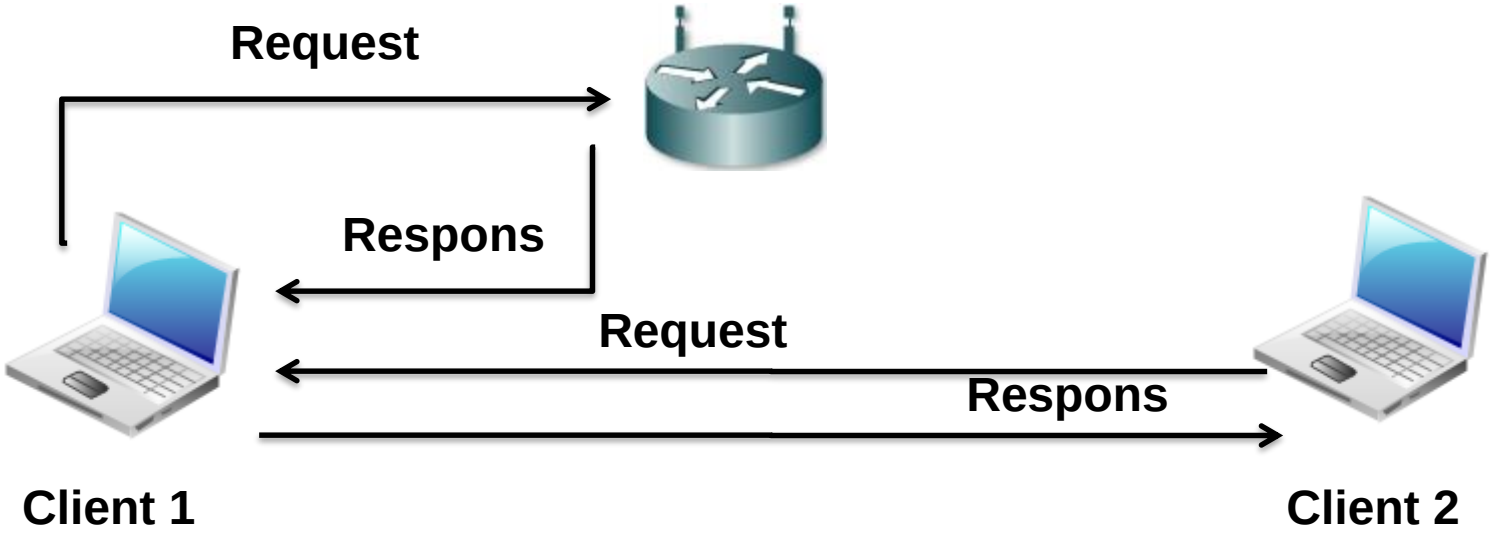
***Output***

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 berlandasan 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 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

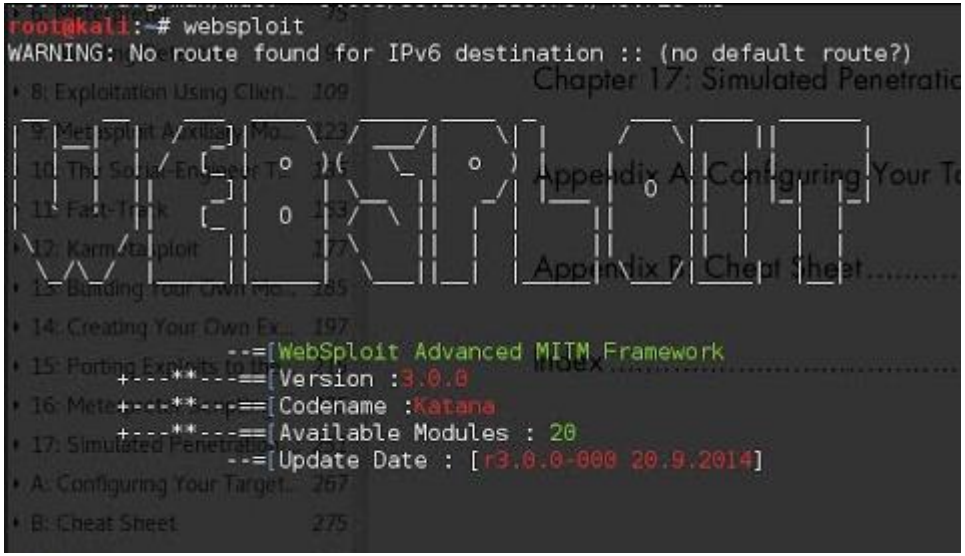
# Kali Linux

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.

# Kali Linux


**Gambar Sistem Operasi Kali Linux**

# WEBSPLOIT

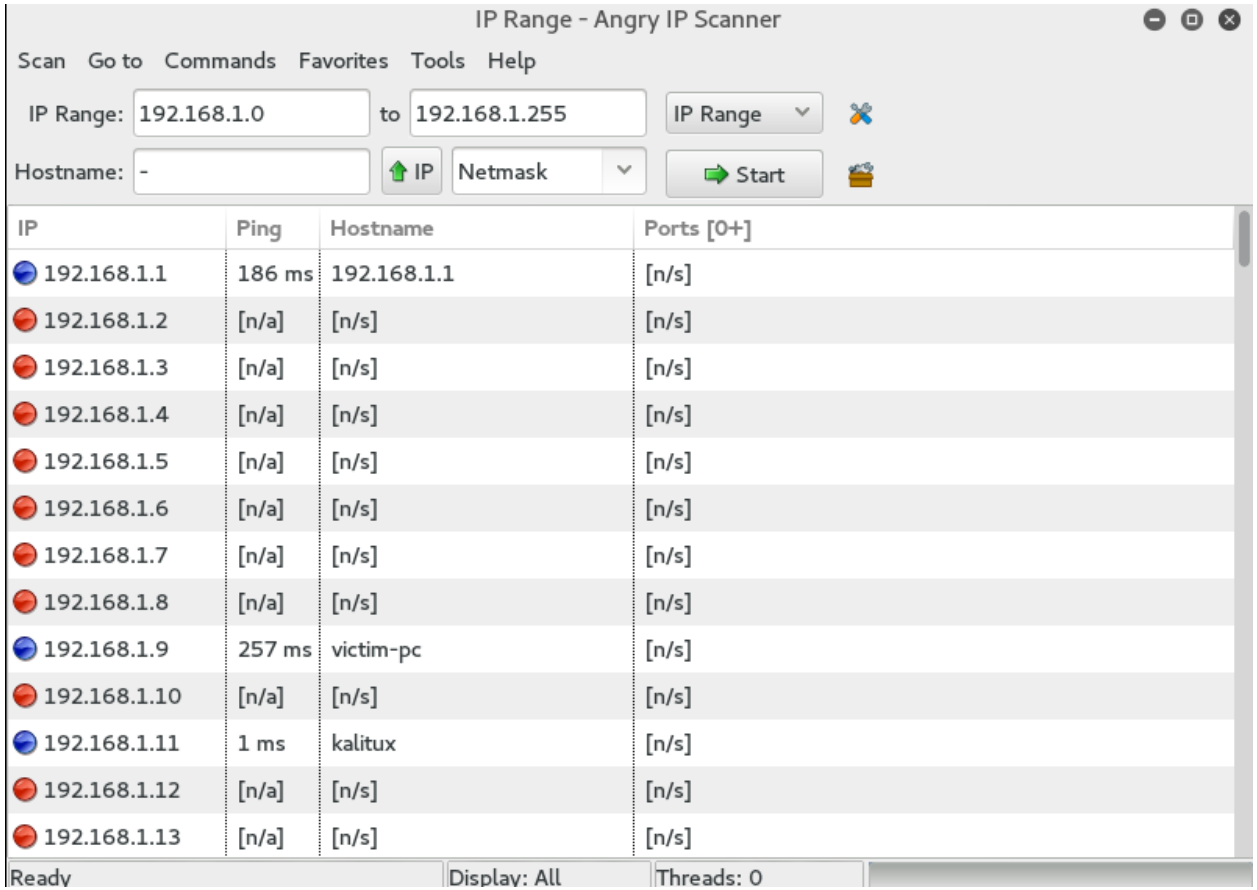



Websploit adalah software yang mempunyai fungsi untuk menganalisa suatu sistem untuk menemukan berbagai jenis kerentanan. Salah satu modul di dalam websploit adalah modul MITM.

# - Studi Kasus -

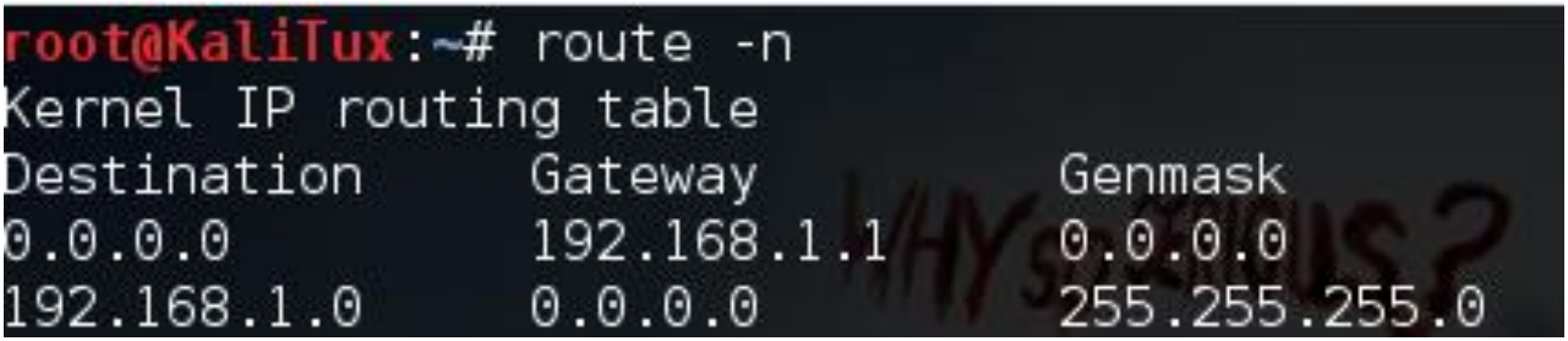
# Studi Kasus

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



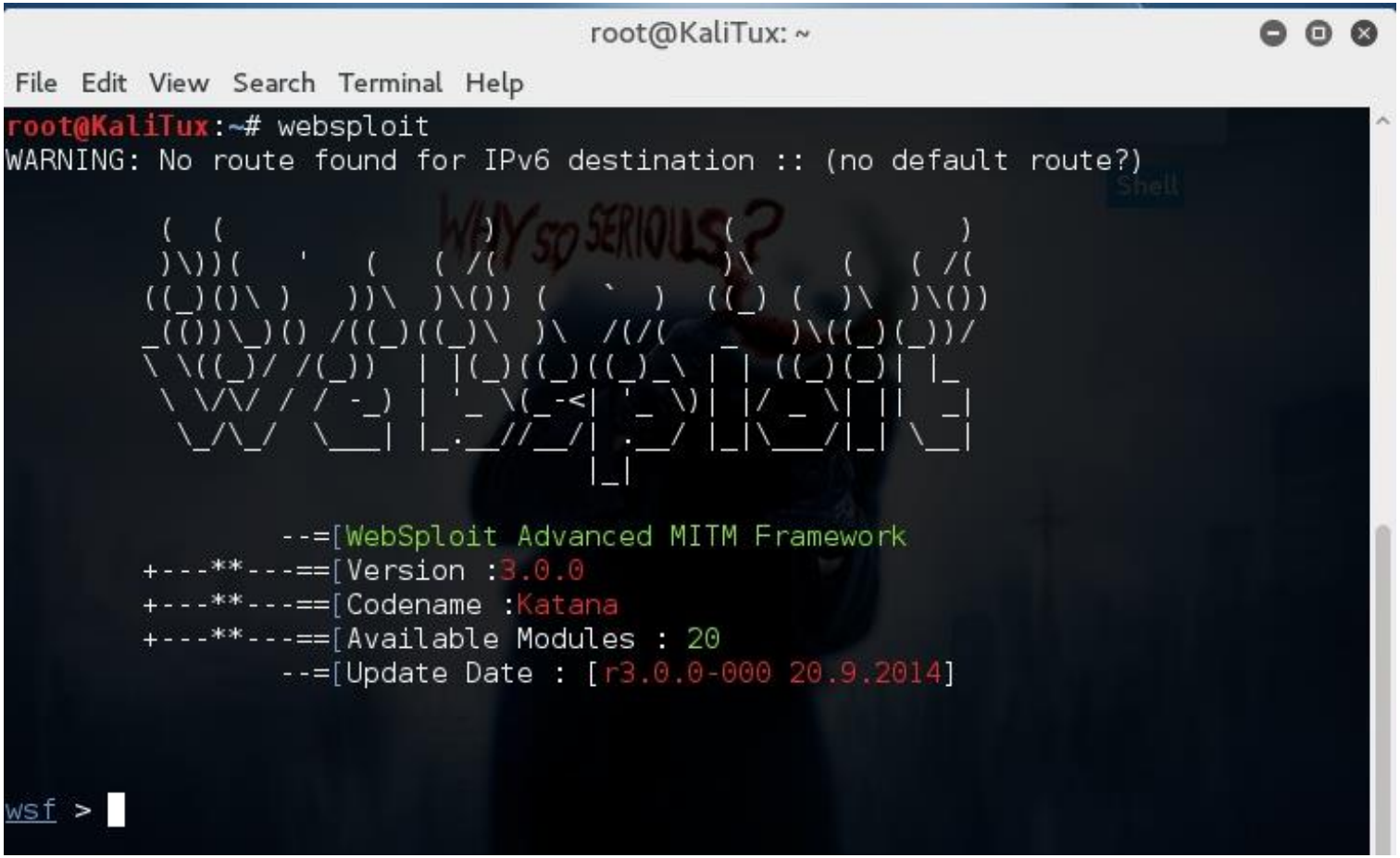
# Studi Kasus

2. Pencarian informasi untuk alamat IP Gateway



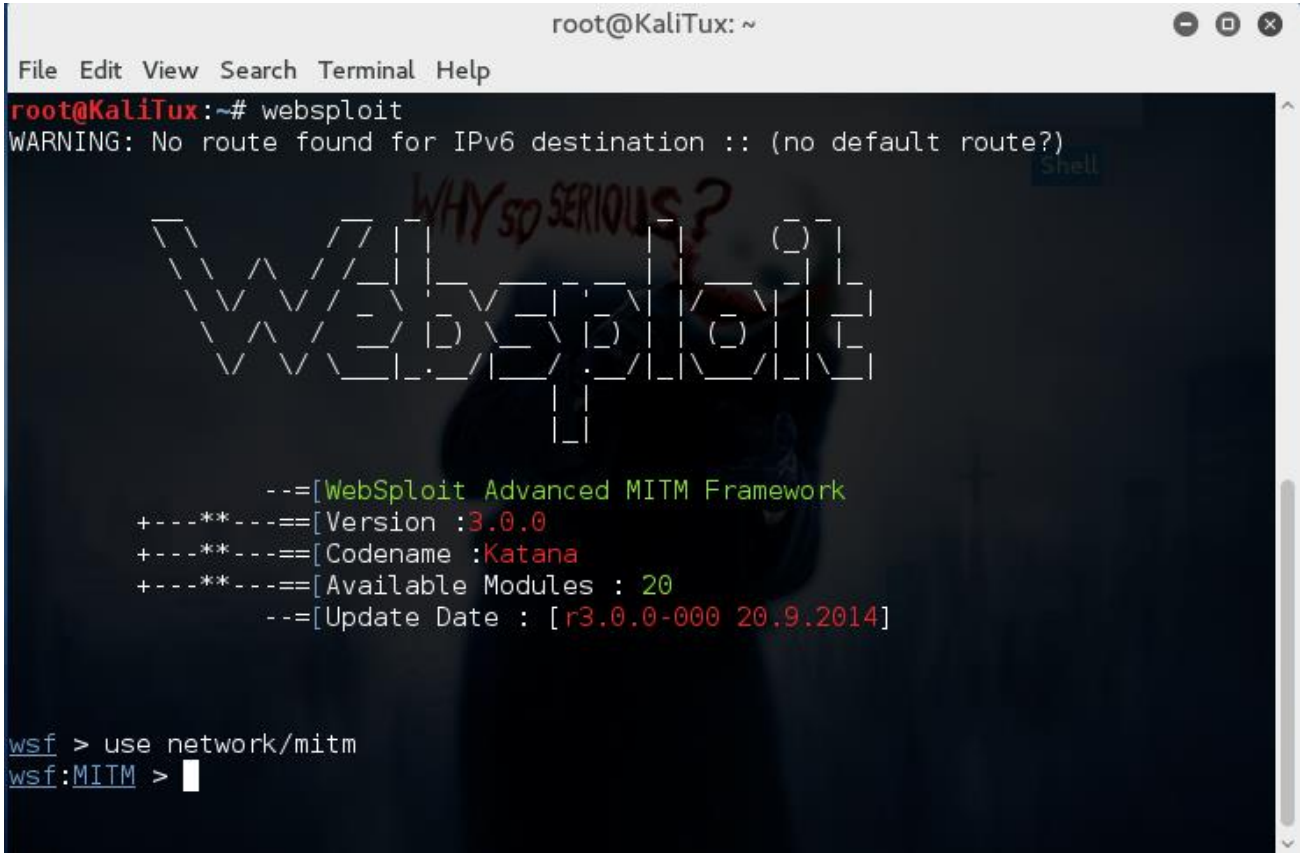
# Studi Kasus

3. Perintah untuk masuk ke dalam websploit



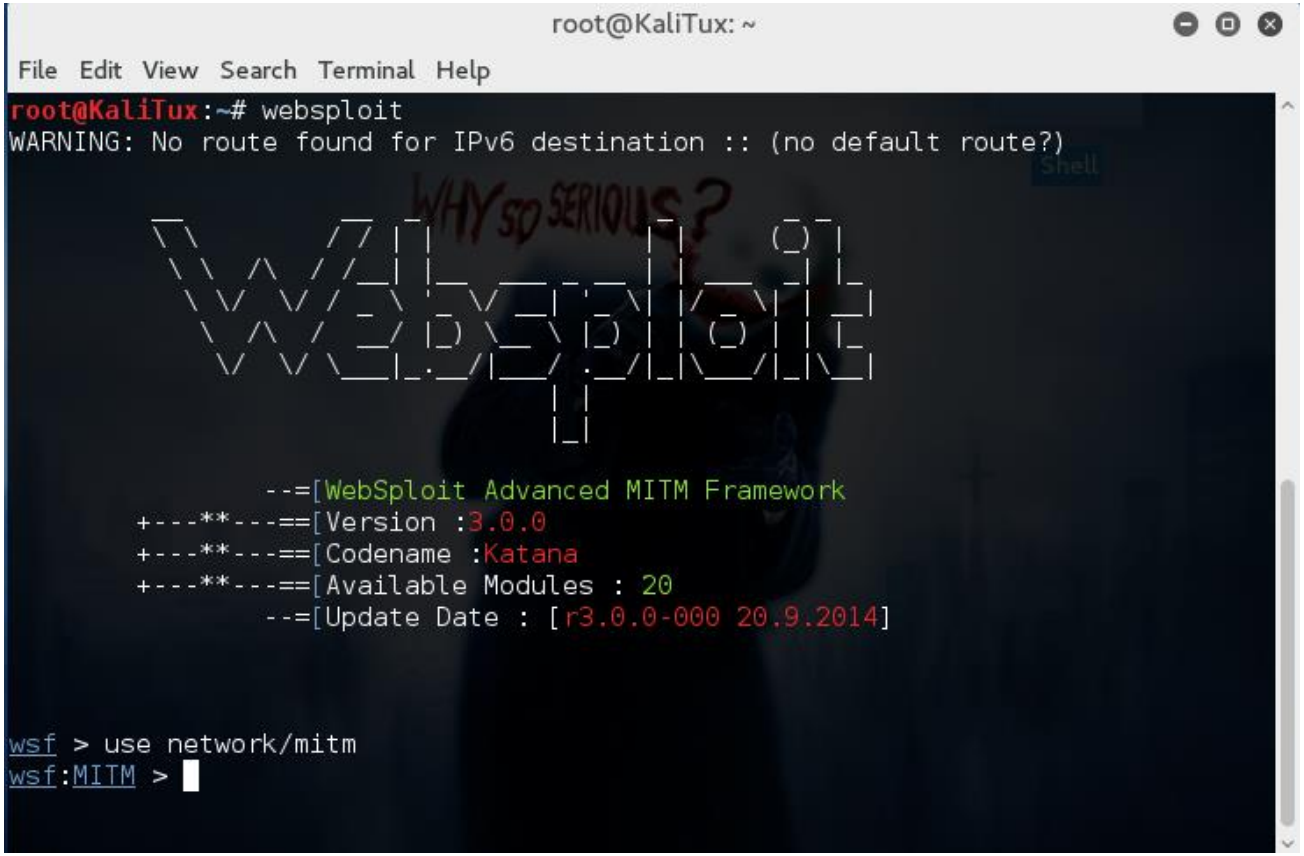
# Studi Kasus

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



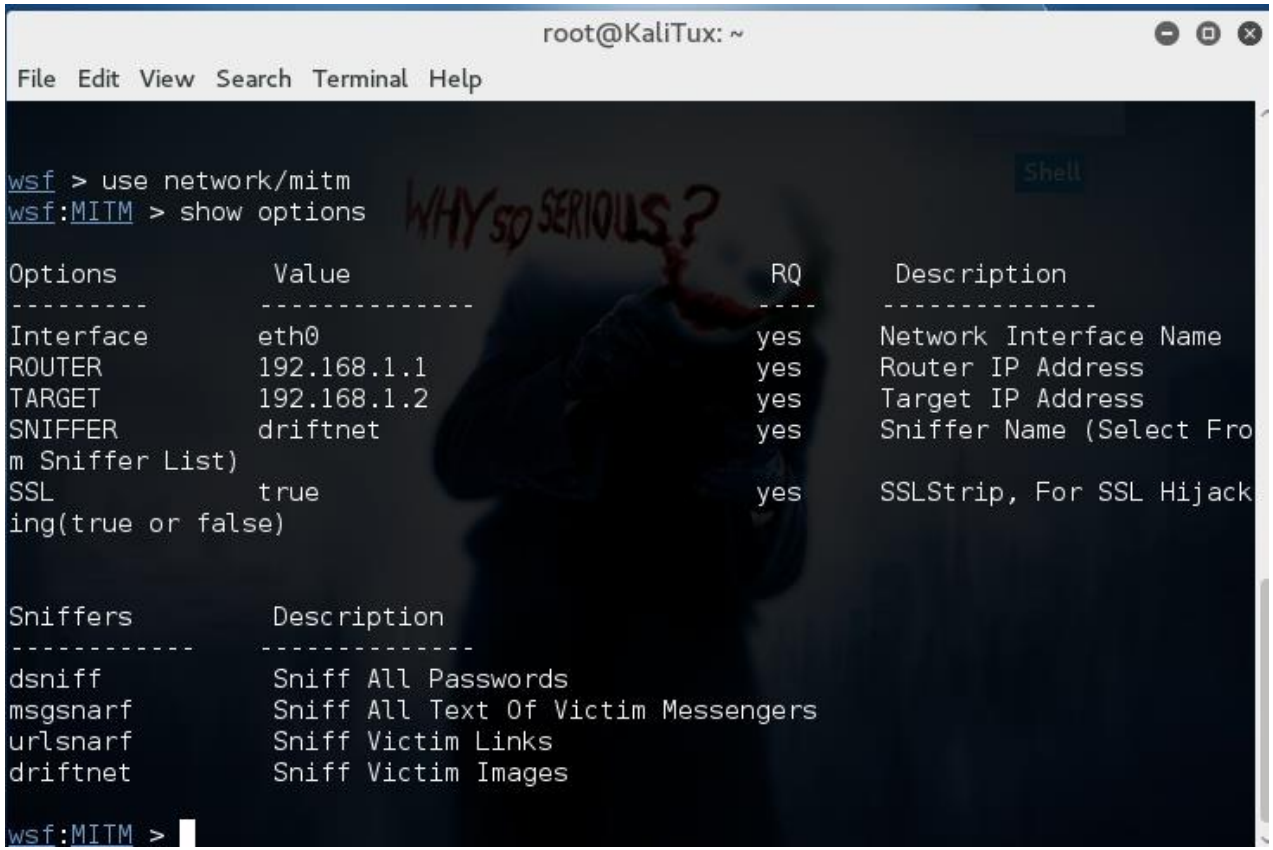
# Studi Kasus

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



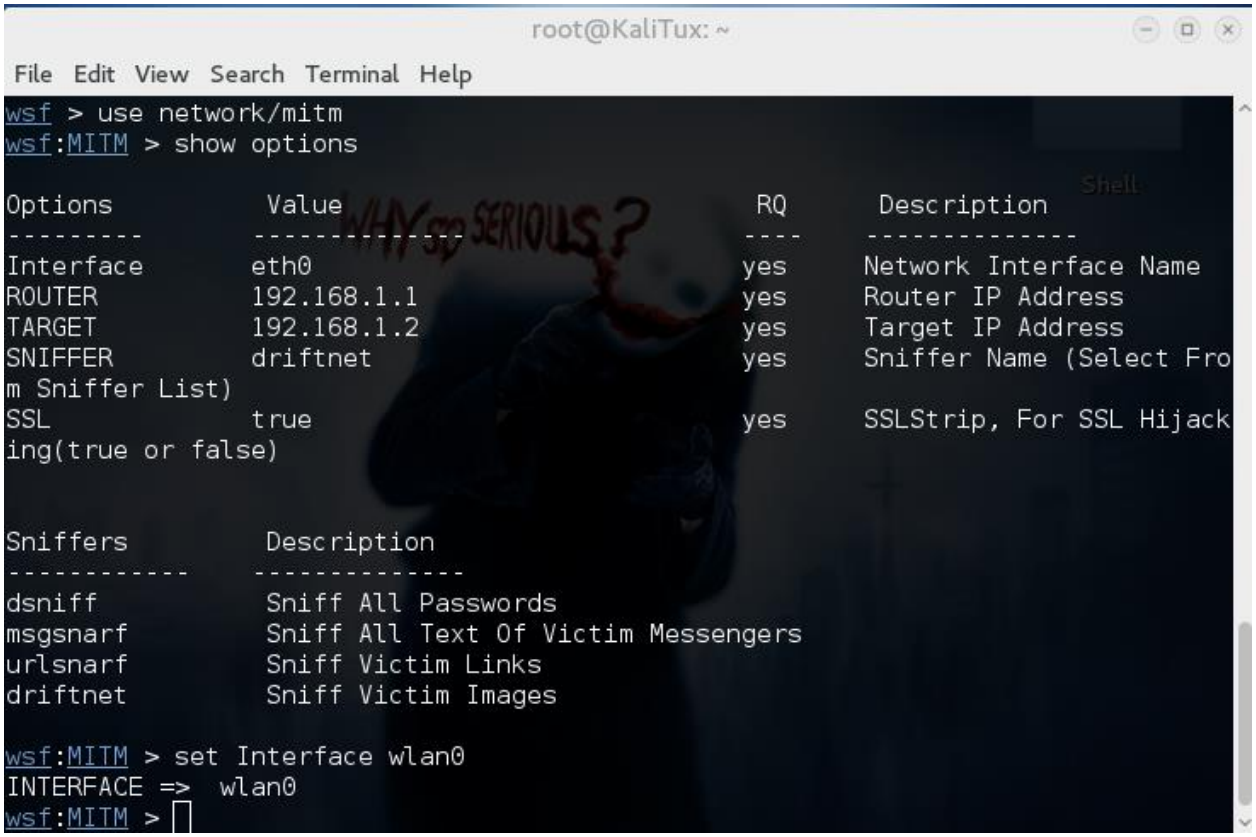
# Studi Kasus

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



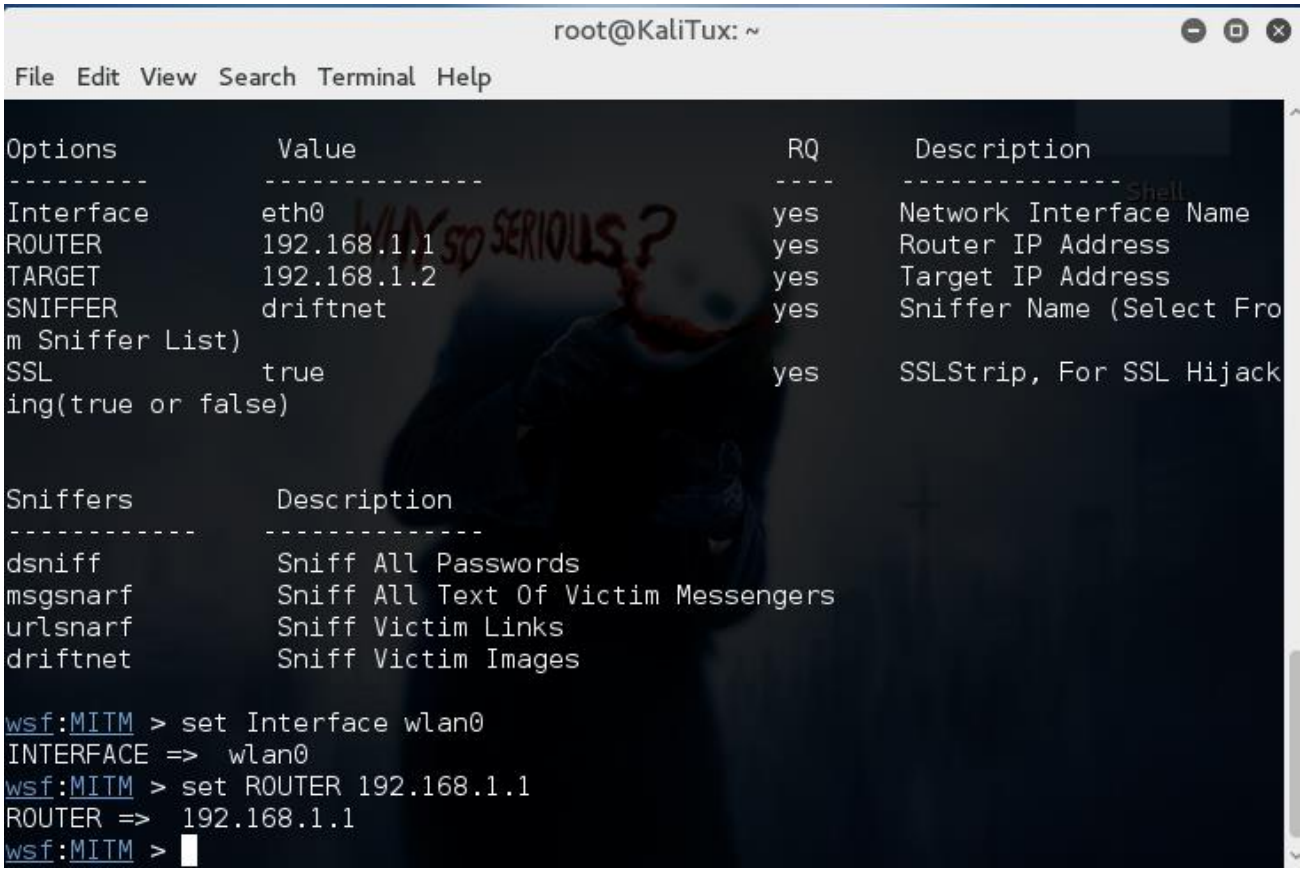
# Studi Kasus

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



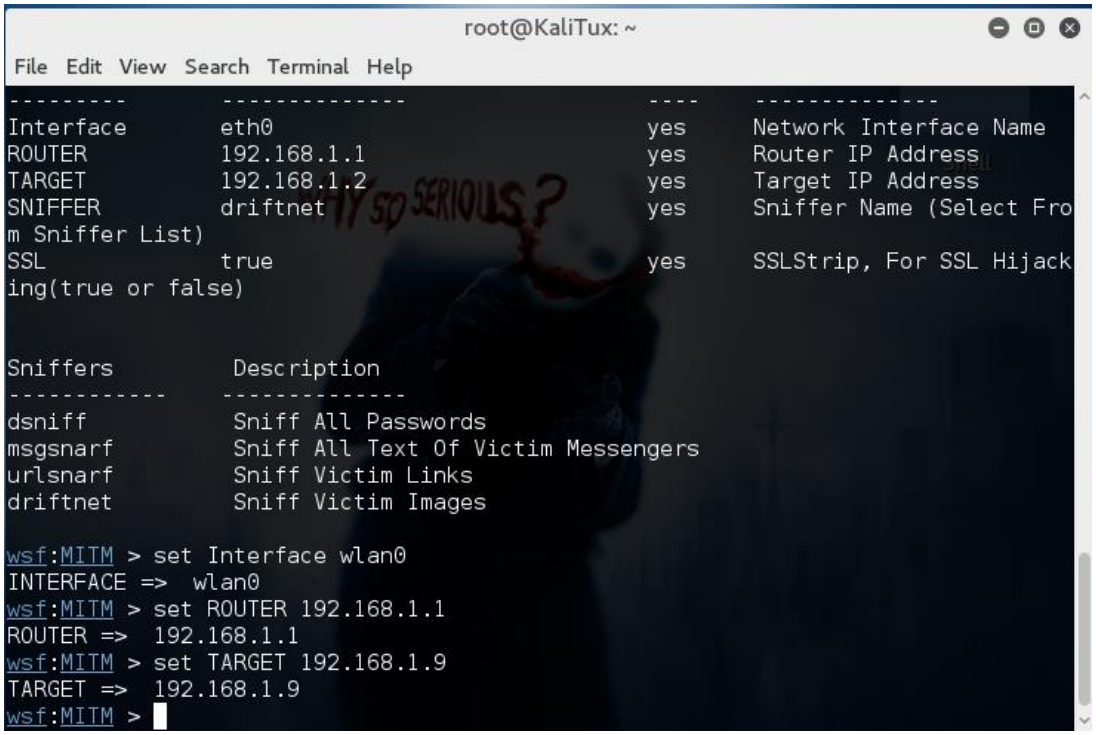
# Studi Kasus

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



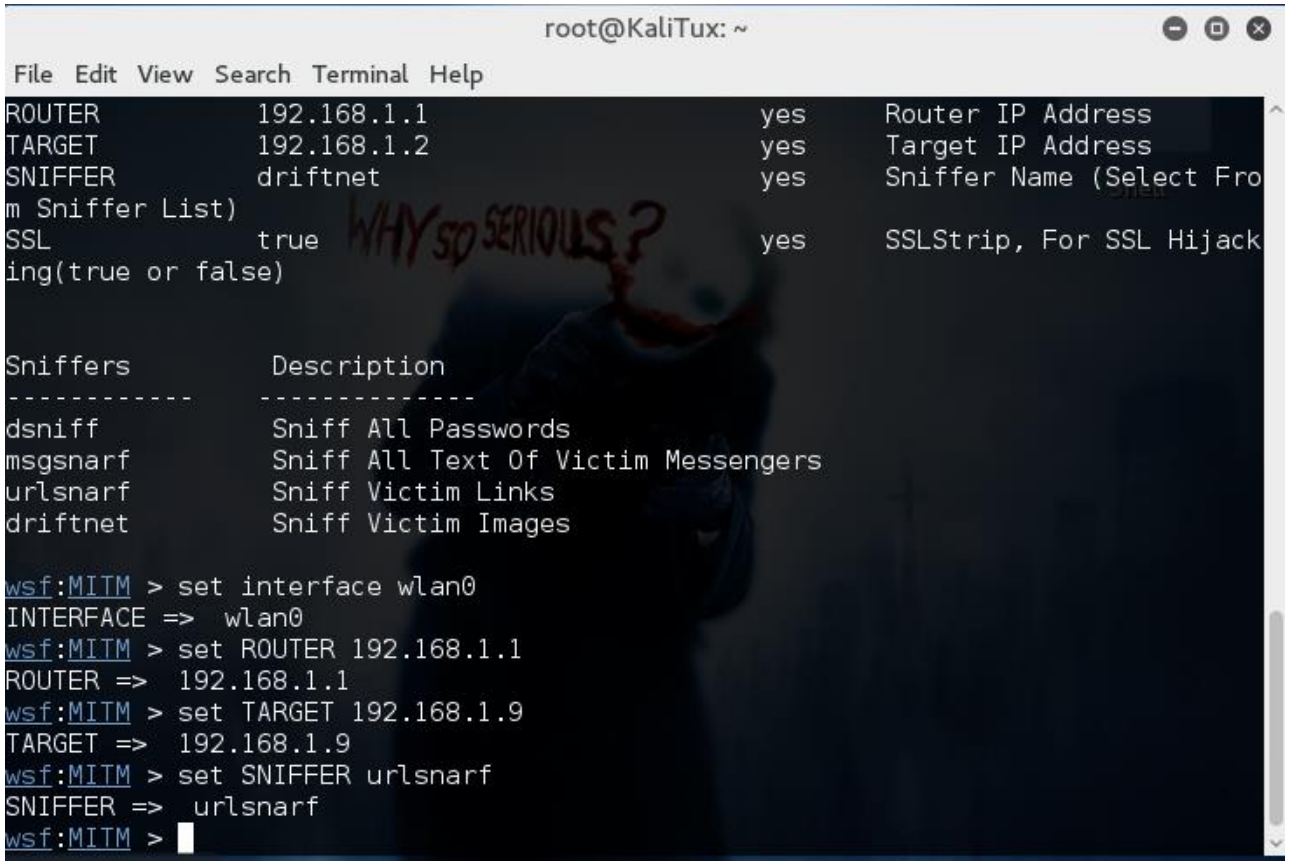
# Studi Kasus

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.



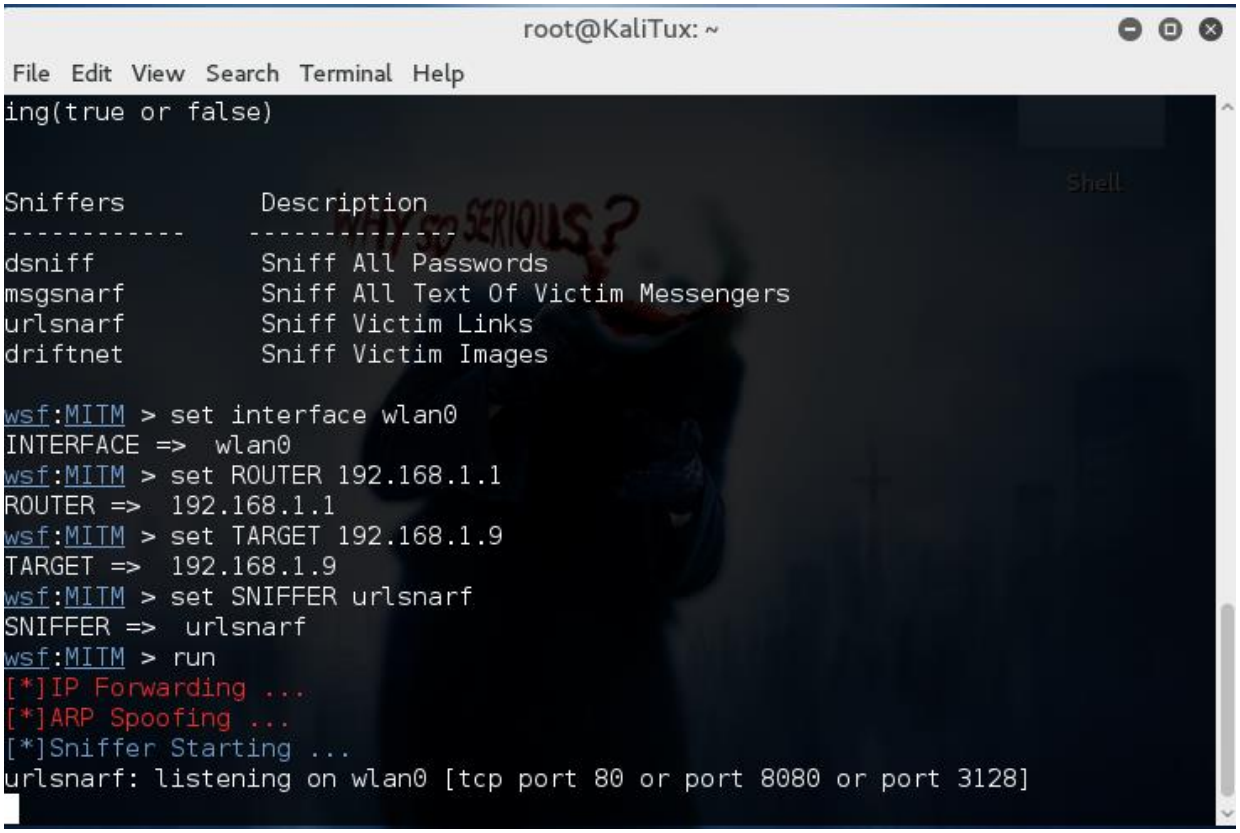
# Studi Kasus

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



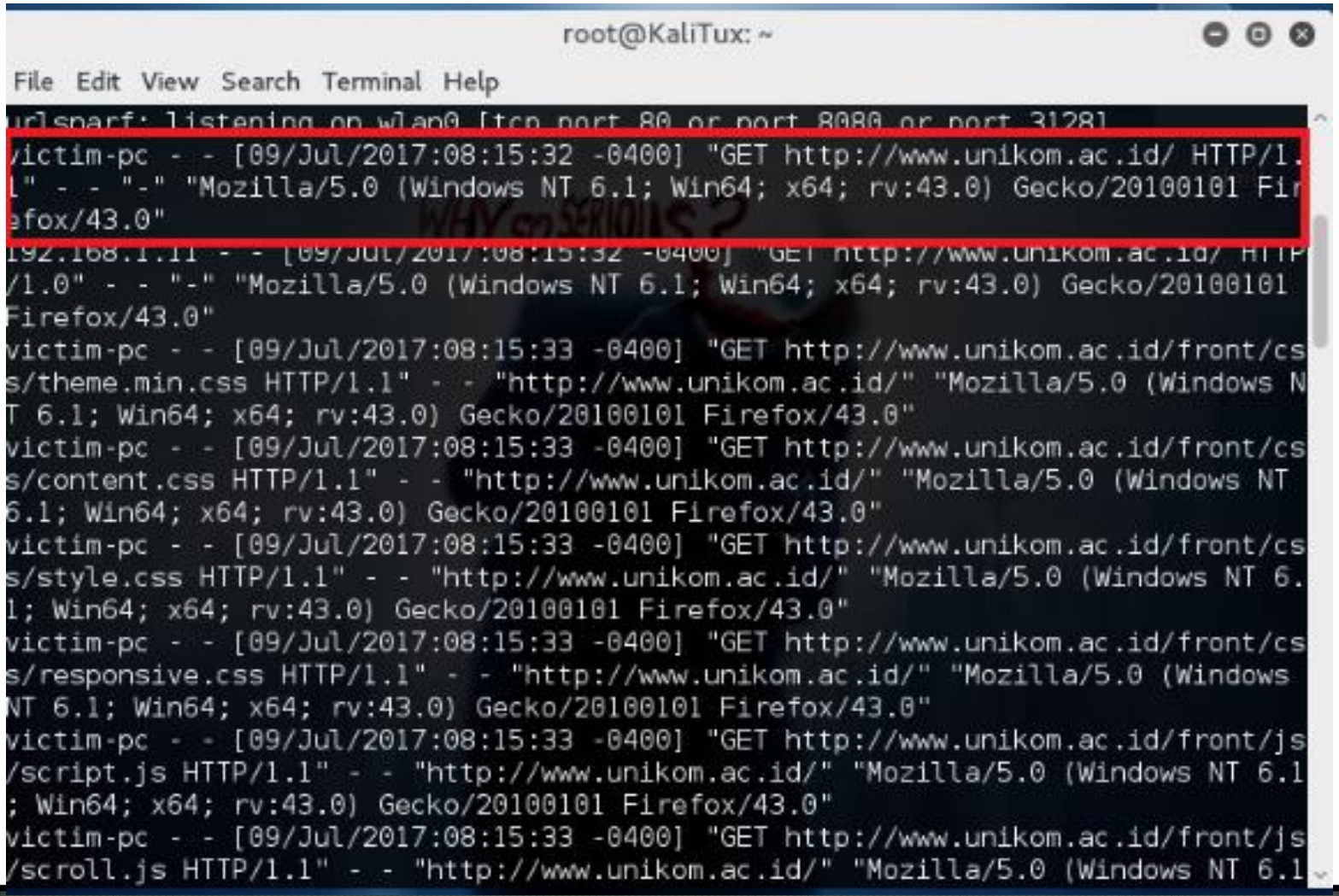
# Studi Kasus

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



# Studi Kasus

OUTPUT



# - SELESAI -