indonesian backtrack team

"The quieter you become, the more you are able to hear"

E-book id-backtrack
#2 Edition - Beta Edition
"Get Up From Beginner"

author

THJC

./Index Of Pages

./Opening

Setelah berhasil membuat e-book *#1 Beginner Section*, ternyata niat untuk menulis lagi tumbuh. Seiring banyaknya tutorial dan informasi yang bermanfaat di dunia maya ini.

Nah untuk e-book *#2 Get Up from Beginner* membahas beberapa isu – isu yang baru – baru ini. Dan sedikit melakukan kenakalan dengan metasploit.

Dan kita membahas mengenai Backtrack 5 R1 yang beberapa hari yang lalu telah rilis.

Semoga dapat bermanfaat informasi yang ada di e-book ini :)

Segala kritik dan saran bisa dikirim ke :
doomsday1009@gmail.com

./Backtrack 5 R1

Setelah tanggal 10 mengalami penundaan, akhirnya tanggal 19.8.2011

Backtrack 5 R1 diluncurkan

File iso yang cukup besar, membuat user backtrack Indonesia berfikir 2 kali untuk mendownload file iso tersebut.

Namun, ternyata ada cara praktisnya. Yaitu dengan melakukan dist-upgrade...
Mari kita jabarkan langkahnya

root@bt:~/# apt-get update
root@bt:~/# apt-get dist-upgrade

Nah silakan melakukan update :)

Namun ternyata ada juga dengan cara menggunakan python :)

root@bt:~/# wget http://bl4ck5w4n.tk/wpcontent/uploads/2011/08/bt5migrate.tar

root@bt:~/# tar -xvf bt5migrate.tar

root@bt:~/# cd bt5migrate

root@bt:~/# python bt5migrate.py

Silakan memilih KDE/GNOME...
Untuk cara menggunakan python, BT5 harus **32BIT!**

./VideoDownloader

Mungkin disini banyak yang menyukai menonton video di Youtube ataupun di Vimeo

Download video di **Youtube** :

```
id-backtrack@bt:~$ apt-get update
id-backtrack@bt:~$ apt-get install youtube-dl
```

Namun, diperlukan update agar bisa mendownload videonya..

```
id-backtrack@bt:~$ sudo youtube-dl -U
id-backtrack@bt:~$ sudo youtube-dl -U
```

Setelah selesai di update 2x, barulah Youtube downloader dapat digunakan :)

```
id-backtrack@bt:~$ youtube-dl [LINKYOUTUBE]
```

Download video di **Vimeo** :

```
id-backtrack@bt:~$ wget
http://ossguy.com/video_hosts/vimeo_downloader.sh

id-backtrack@bt:~$ chmod +x vimeo_downloader.sh
```

Lalu siap di gunakan,
Gunakan dengan cara berikut

```
id-backtrack@bt:~$ ./vimeo_downloader.sh [LINKVIMEO]
```

Semoga berguna :)

Video Downloader

Vimeo
Author : ***ParkourCrew***
Link : **http://forum.id-backtrack.com/showthread.php?tid=611**

Youtube
Author : ***gtx150***
Link : **http://forum.id-backtrack.com/showthread.php?tid=501**

./Percantik tampilan GRUB

Mau tampilan grub kalian seperti ini?

Mau tahu caranya? Gampang . . .
Ikuti saja cara berikut :)

Copy file gambar [.png / .tga] ke /usr/share/images/desktop-base
Bisa dengan user ROOT

Atau Command : cp /home/IBT/IBT.png /usr/share/images/desktop-base

Catatan : Ganti /home/IBT/IBT.png dengan direktori anda dan nama file anda :)

id-backtrack@bt:~$ sudo gedit /etc/grub.d/05_debian_theme

Lalu cari :
WALLPAPER="/usr/share/images/desktop-base/moreblue-orbit-grub.png"

Ganti dengan
WALLPAPER="/usr/share/images/desktop-base/[NAMA FILE ANDA.PNG]"

Catatan : **BACKUP FILE ASLINYA!**

Lalu
id-backtrack@bt:~$ sudo update-grub
Dan reboot deh, cek GRUBnya :)

Percantik tampilan GRUB
Author : *Kenzie*
Link : http://forum.id-backtrack.com/showthread.php?tid=563

./Mengganti MOTD

```
#!/bin/sh
TERM=linux
export TERM
clear
echo
"#################################################################"
echo "[*] Welcome to the BackTrack 5 Distribution,
Codename \"Revolution\""
echo " "
echo "[*] Official Indonesian Backtrack Team web : http://id-
backtrack.com"
echo " "
echo
"#################################################################"
echo " "
echo -e "[*] To start a graphical interface,
type \"\e[0;33mstartx\e[0m\"."
echo -e "[*] The default root password is \"\e[0;33mtoor\e[0m\"."
echo ""
```

Mau menjadi seperti itu?
Caranya mudah...

id-backtrack@bt:~$ gedit /etc/update-motd.d/10-help-text

Tinggal edit deh, pesan apa yang mau ditampilkan :)

Mengganti MOTD
Author : *Aquaman86*
Link : http://forum.id-backtrack.com/showthread.php?tid=511

./Instalasi VirtualBox

Pasti disini tau semua yang namanya **VirtualBox**, ya?
Nah terkadang sedikit membingungkan, ketika kita ingin melakukan exploit atau mencoba sesuatu di lingkungan Backtrack kita.

Nah jangan khawatir, VirtualBox sudah bisa di-install di lingkungan linux. Mau tahu?
Ikuti saja caranya!

Backtrack 5 tidak disertai dengan kernel headers yang sudah terinstall. So, kita perlu untuk mendonlotnya dan dilanjutkan dengan menginstall VirtualBox. Perintah-perintahnya adalah seperti berikut ini:

```
id-backtrack@bt:~$ prepare-kernel-sources
id-backtrack@bt:~$ cd /usr/src/linux
id-backtrack@bt:~$ cp -rf include/generated/* include/linux/
```

Setelah yang diatas tersebut selesai, edit-lah /etc/apt/sources.list sebagaimana tertulis dibawah ini :

```
id-backtrack@bt:~$ echo deb
http://download.virtualbox.org/virtualbox/debian lucid contrib non-
free >> /etc/apt/sources.list
```

dan donlot virtualbox-nya :

```
id-backtrack@bt:~$ wget -q http://
download.virtualbox.org/virtualbox/debian/oracle_vbox.asc -O- | sudo
apt-key add -

id-backtrack@bt:~$ apt-get update

id-backtrack@bt:~$ apt-cache search virtualbox

id-backtrack@bt:~$ apt-get install virtualbox-4.0
```

Instalasi VirtualBox
Link : http://netsecuritystuff.wordpress.com/2011/05/23/virtualbox-on-backtrack-5/

./Wget Tricks

Tau **Wget** kan?
Wget adalah aplikasi download via terminal.
Nah, biasanya kan kita hanya menggunakan Wget dengan perintah

id-backtrack@bt:~$ wget [LINKDOWNLOAD]

Nah untuk kali ini, kita akan membahas cheatsheet dari Wget-nya :)
Banyak hal yang Wget lakukan ternyata.

Menyambung Download File Yang Terputus :
id-backtrack@bt:~$ wget -c <url>

Rename hasil download
id-backtrack@bt:~$ wget -O <nama file> <url>

Download banyak url. buat listnya dalam sebuah file, misal listdownload.txt
id-backtrack@bt:~$ wget -i listdownload.txt

Limit kecepatan [10k = 10Kb]
id-backtrack@bt:~$ wget --limit-rate=10k <url>

Kalau mau download dibalik proxy
id-backtrack@bt:~$ export http_proxy="http://proxyanda:port"
Lalu download!

Kalau butuh username+password untuk autentifikasi
id-backtrack@bt:~$ export http_proxy="http://username:password@proxyanda:port"

Nah, ternyata cheatsheetnya banyak juga kan ya?
Silakan melakukan eksperimen :)

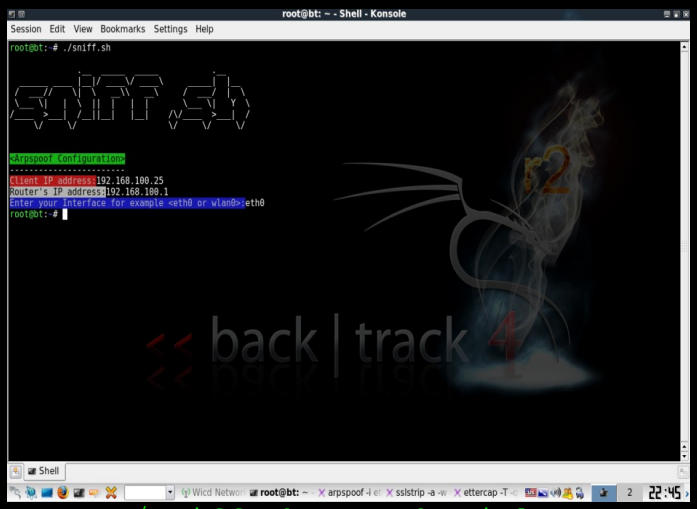
Wget Tricks
Author : ***RR12***
Link : **http://forum.id-backtrack.com/showthread.php?tid=619**

./Sniffing

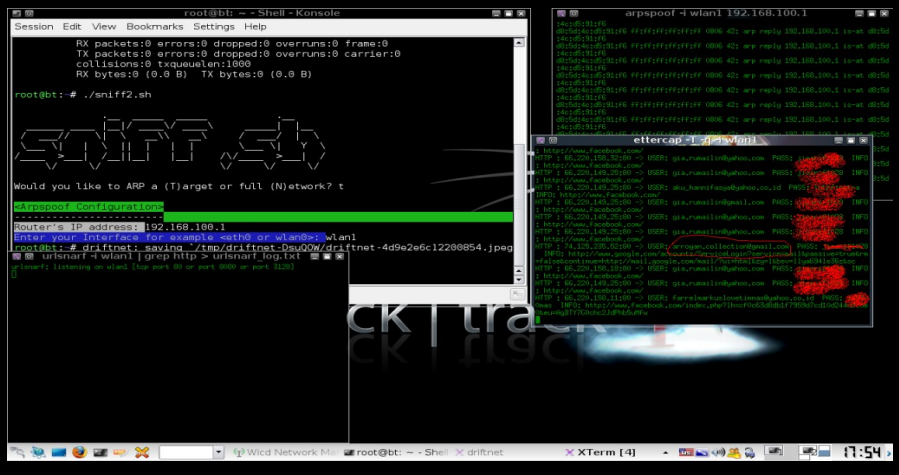
Mau sniffing di jaringan?
Mari kita melakukan!

Pertama, salin scriptnya!
http://pastie.org/pastes/2414050/text?key=era7tx3zm3hqtzubr7l6g

Lalu simpan dengan nama terserah, sebagai contoh "sniff.sh"
Simpan!
Setelah itu, ubah permissionsnya
id-backtrack@bt:~$ chmod +x sniff.sh
Lalu jalankan dengan perintah :
id-backtrack@bt:~$ ./sniff.sh



./sniff.sh saat berjalan



Sniffing
Author : *gtx150*
Link : http://forum.id-backtrack.com/showthread.php?tid=310

./Nessus Scanner

Buka konsol, dan jalankan

```
id-backtrack@bt:~$ /opt/nessus/sbin/nessus-adduser
Login : IBTeam
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload
plugins, etc…) (y/n) [n]: y

User rules
----
nessusd has a rules system which allows you to restrict the hosts
that backtrack has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are
done :
(the user can have an empty rules set)
```

Pada Tahap berikut ente bisa memasukan rulles pada user baru tersebut, misalnya kita hanya membatasi dia mengakses ip-address ato host serta subneting tertentu. Maka kita dapat mensetingnya secara manual..

Syntaknya seperti ini
accept|deny ip/mask

contoh:
accept 192.168.1.3/24

ya kalo ente mau dia hanya mengakses hanya dari network dia berada .. maka masukan syntak ini

accept client_ip
default deny

Kalo gw sih enter2 aja dulu .. anggap aja no rules

Langkah selanjutnya adalah menverifikasi user yang telah di buat. Nessus akan memastikan apakah anda telah yakin dengan user yang telah anda ciptakan

Login : backtrack
Password : ***********
This user will have 'admin' privileges within the Nessus server
Rules :
Is that ok ? (y/n) [y] y
User added

2. **Register Your Nessus**

Nah pembuatan user selesai.. sekarang ane coba jalankan

id-backtrack@bt:~$ /etc/init.d/nessusd start
Starting Nessus : .
id-backtrack@bt:~$ Missing plugins. Attempting a plugin update…
Your installation is missing plugins. Please register and try again.
To register, please visit http://www.nessus.org/register/

Jiahh ada error missing plugin. ya itu karena kita di haruskan meregister nessus terlebih dahulu ..ok deh kita coba ya..
buka browser anda terus go to url
http://www.nessus.org/products/nessus/ne...tion-codes
Nah terus pilih yang using nessus ad home.. karena memang ada nessus yang di gunakan bagi mereka yang pro alias berbayar. Sangat di sayangkan pada versi gratisan ini, kita hanya di pernankan melakukan scanning 16 IP address dalam waktu bersamaan dan memiliki kecepatan yang sama.

Sebelum registrasi .. mending mattin dulu proses nessus nya

id-backtrack@bt:~$ /etc/init.d/nessusd stop
Shutting down Nessus : /etc/init.d/nessusd: line 34: kill: (3535) - No such process

Nah pada proses registrasi nantinya akan di hadapkan dengan TOS
Terus nanti anda di haruskan mengisi user name yang terdiri dari nama depan dan nama belakang
Serta alamat email, nah setelah sukses. Nessus akan mengirimkan kode aktivasi tersebut pada email yang anda daftarkan tadi.

Sekarang kita mengaktifkan saja dengan kode aktivasinya

id-backtrack@bt:~$ /opt/nessus/bin/nessus-fetch --register 3IC3-B310-4C9T-CE37-5D2E
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org…

Nah aktivasi codenya berhasil dan langsung di cek update pluginsnya .

4. Mencoba Nessus Pertama Kalinya

Setelah berhasil di update kita tinggal menjalankan nessus

```
id-backtrack@bt:~$ /etc/init.d/nessusd start
Starting Nessus : .
```

sekarang buka browser aja terus masukin alamat ini..ingat jgn lupa pake https

https://localhost:8834/

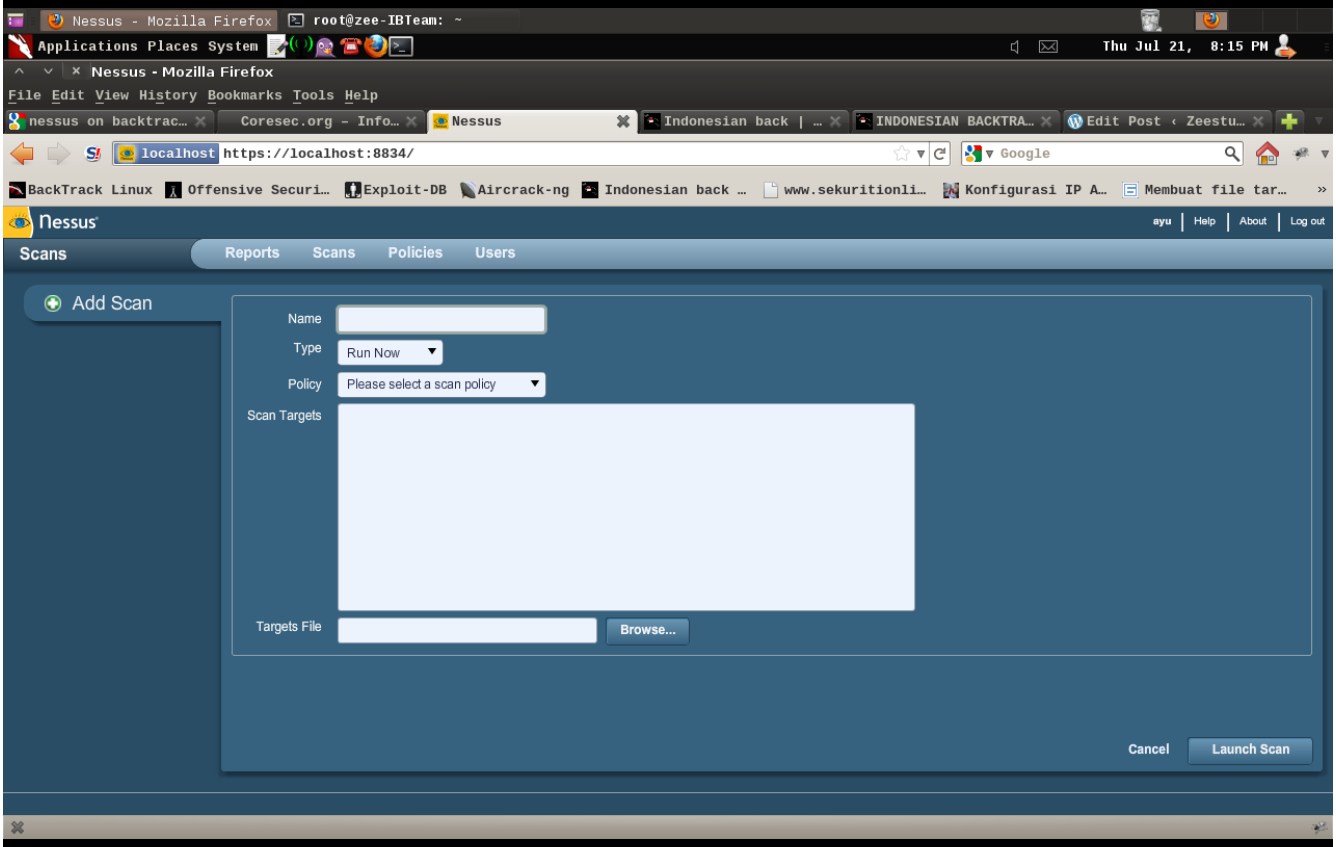
Nah klo udah login kita tinggal memulai scann.. klik tombol scann kemudian add new scan.. nantinya ente harus mengisi form. Masukan nama untuk proses scann, terus pilih type nya ..

1. run now
agar langung running proses scan yang telah kita namai tadi

2. scheduled
nnti diisikan jadwal sehingga proses akan berjalan sesuai dengan

skedul yang ditentukan
3. template
proses scan yang sudah di atur baik secara default

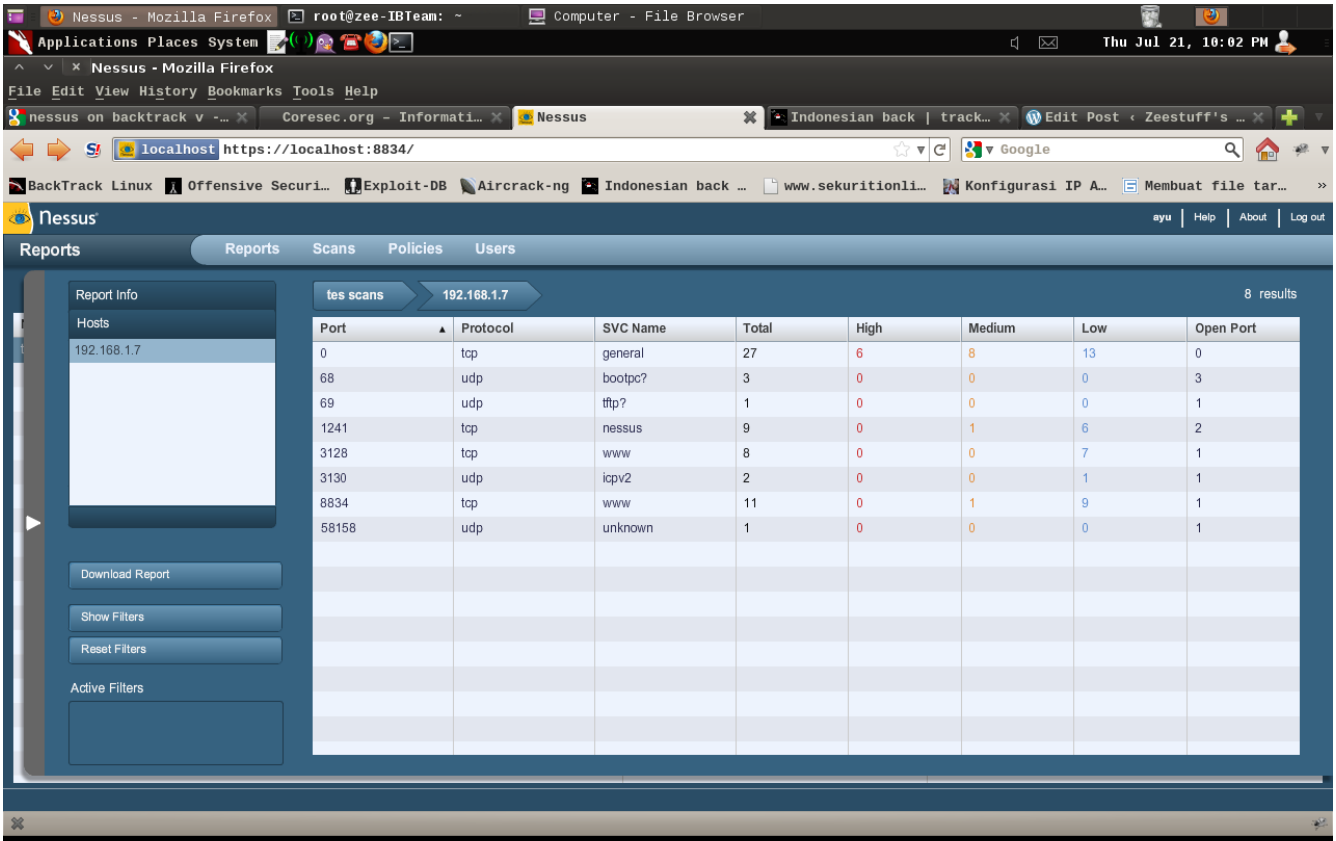
Kemudian kita harus memilih policies. misalnya kita hanya menyecann jaringan kita sendiri maka kita sudah seharusnya memilih internal scann network. kalo untuk ke web maka bisa menggunakan Web Apps test



Pada scans targets isikan target ip yang hendak kita scan.
Bisa 6 sekaligus.
Atau jika anda ada file daftar target bisa menggunakan fiture upload.

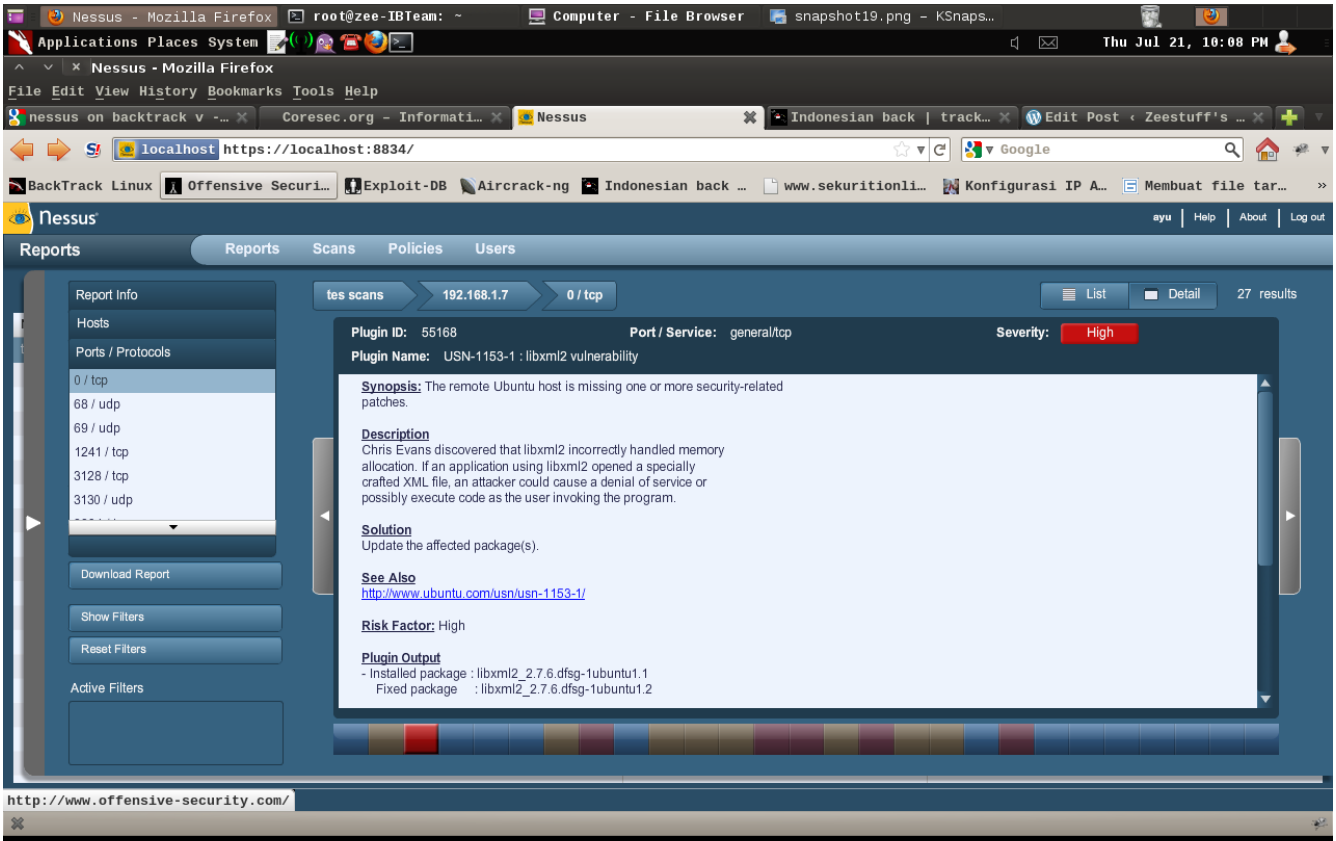
salah satu kekurangan dalam tools ini adalah begitu banyaknya cpu memory yang di pakai sehingga pada proses scan psti pc ato laptop akan terasa berat.

Ok anggap aja scann ente sudah selesai ..
Untuk melihat reports ente tnggal menekan button reports, kemudian akan terlihat table yang berisi nama operasi scann. Untuk melihat secara detail ente tinggal mengklik nama operasi scannnya



Memang lumayan akurat serta lengkap informasi hasil scann dari tools ini. Hasil scann dari tools ini di bedakan dari tingkat bahaya vurln tersebut. Di mulai dari high, medium serta low. Bahkan port yang di exploitasi juga terlihat dengan jelas.

Nah salah satu fiture yang paling gw demen sebenarnya adalah, bahwa nessus akan memberikan informasi mendetail terhadap jenis vurln serta memberikan link exploit bahkan memberikan solusi dan cara untuk menangkalnya



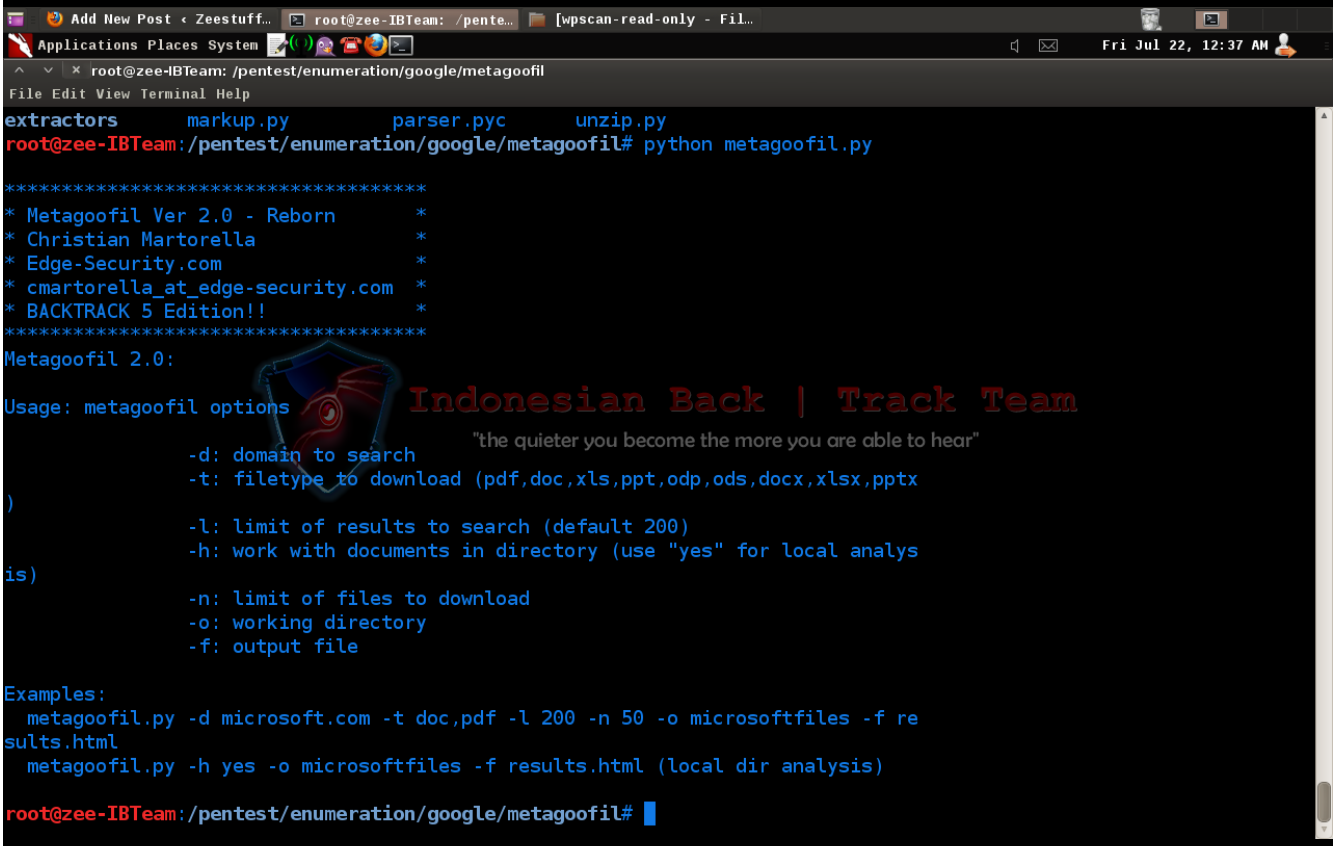

```
NessusScanner
Author     : Zee Eichel
Link       : http://forum.id-backtrack.com/showthread.php?tid=470
```

./Metagoofil

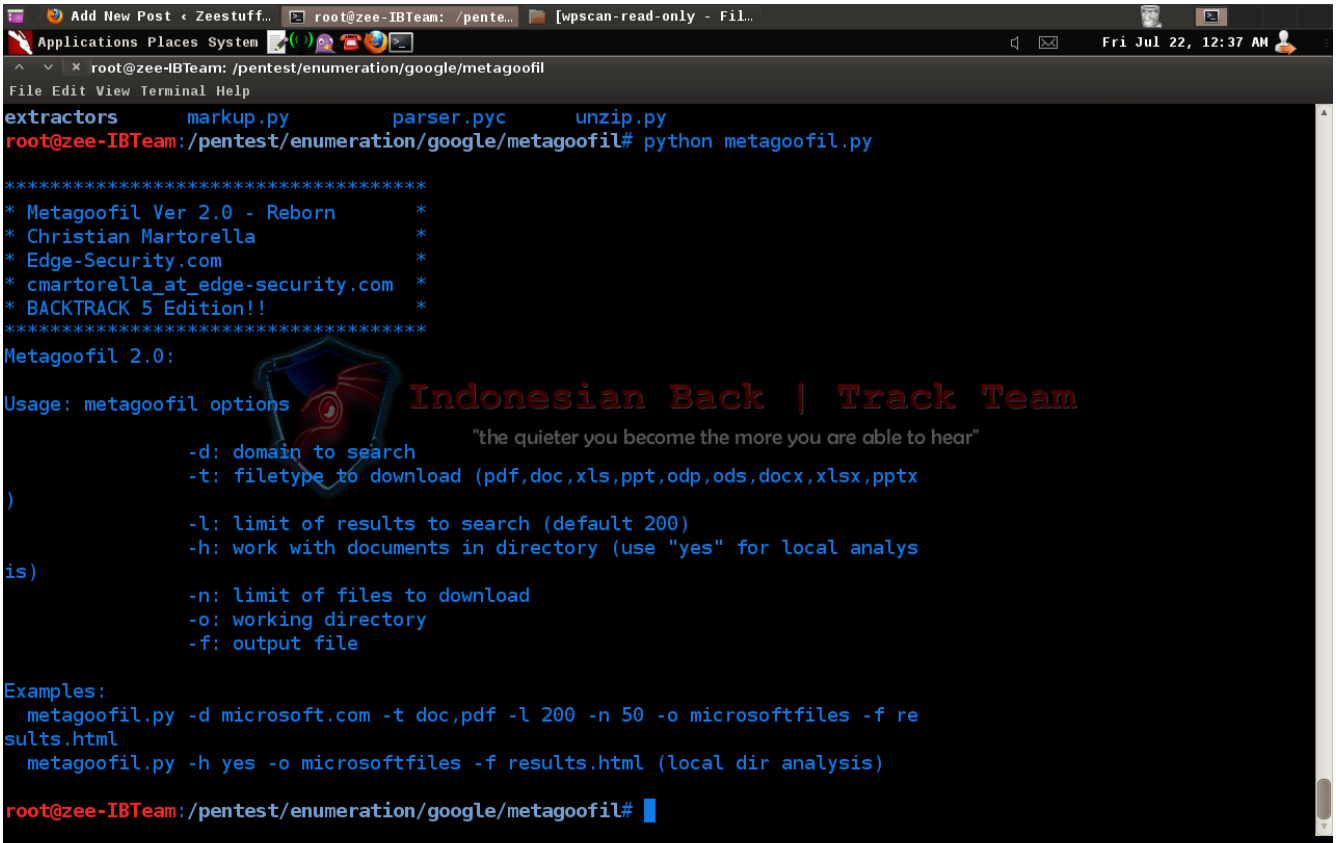
Metagoofil adalah tools yang digunakan untuk mencari atau mengumpulkan informasi berdasarkan tipe dokument dari situs tertentu yang telah di indexing oleh google..

id-backtrack@bt:~$ cd /pentest/enumeration/google/metagoofil
id-backtrack@bt:/pentest/enumeration/google/metagoofil~$

ok coba di mainkan …



ok setelah kita mengetahui semua fungsi perintah maka test



-d (target host) ane isi microsoft.com
-t (tipe file) ane pilih tipe .doc dan .pdf
-l (Batasan Jumlah file) ane isikan 200
-n (Download pada awal esekusi) ane isikan 50
-o (folder di mana hasil esekusi di simpan) ane buat microsoftfiles
-f (laporan hasil yang di buat pada format html) ane masukan results.html

metagoofil.py -h yes -o microsoftfiles -f results.html (local dir analysis)

isikan local dir analysis dengan local directory pada pc kita yang hendak kita ambil dokumentnya ..

Perhatikan pada result pada gambar di atas. Ada 206 file yang di temukan. Dan metagoofil akan mendownload semua file tersebut di mulai dari 50 file pertama dan di simpan pada file microsoftfiles yang telah terbentuk

Metagoofil
Author : *Zee Eichel*
Link : http://forum.id-backtrack.com/showthread.php?tid=472

./InformasiForum

Setelah forum mendapatkan serangan, IBTeam sekarang makin maju.
Banyak fitur – fitur yang telah di masukkan kedalam server IBTeam.

Lalu, yang lebih baru lagi. . .
IBTeam mempunyai domain baru!

http://indonesianbacktrack.or.id/

Dikarenakan masih baru, domain tersebut masih harus disetting di beberapa tempat. Karena masih banyak kekurangannya.
Semoga di kemudian hari pengunjung dapat melakukan login juga di

http://indonesianbacktrack.or.id/

Dan usai sudah e-book #2 "Get Up From Beginner" kali ini, masih terdapat banyak kekurangan di dalam e-book #2 kali ini.

Semoga dapat dibenahi di e-book selanjutnya :)

Dan bagi yang ingin mengirim artikel, silakan mengirim e-mail ke :
doomsday1009@gmail.com

Viva La Backtrack !

Thanks To :

Zee Eichel	james0baster	shendo
90Bl4ck	jurank_dankkal	aip_zenzacky
angga	rightpreneur	Andre_Corleone
jimmyromanticdevil	shadowsmaker	Ares
Liyan Oz	guitariznoizedevilnay	gtx150

Konspirasi.

indonesian backtrack team

"The quieter you become, the more you are able to hear"