Kali MSF

The Metasploit Framework（简称metasploit），它是一款开源的安全漏洞利用和测试工具，也是目前最流行、最强大、最具扩展性的渗透测试框架之一。集成了各种平台上常见的漏洞和流行的shellcode，并持续保持更新。拥有世界上最大的渗透测试攻击数据库，可以利用其现有的payload进行一系列的渗透测试。

如何使用 MSF

MSFconsole是使用Metasploit框架（MSF）的最常用的接口，通过该接口可以实现对MSF的控制和使用。它提供了一个“一体式”集中式控制台，并允许访问 MSF 中几乎所有可用的选项。

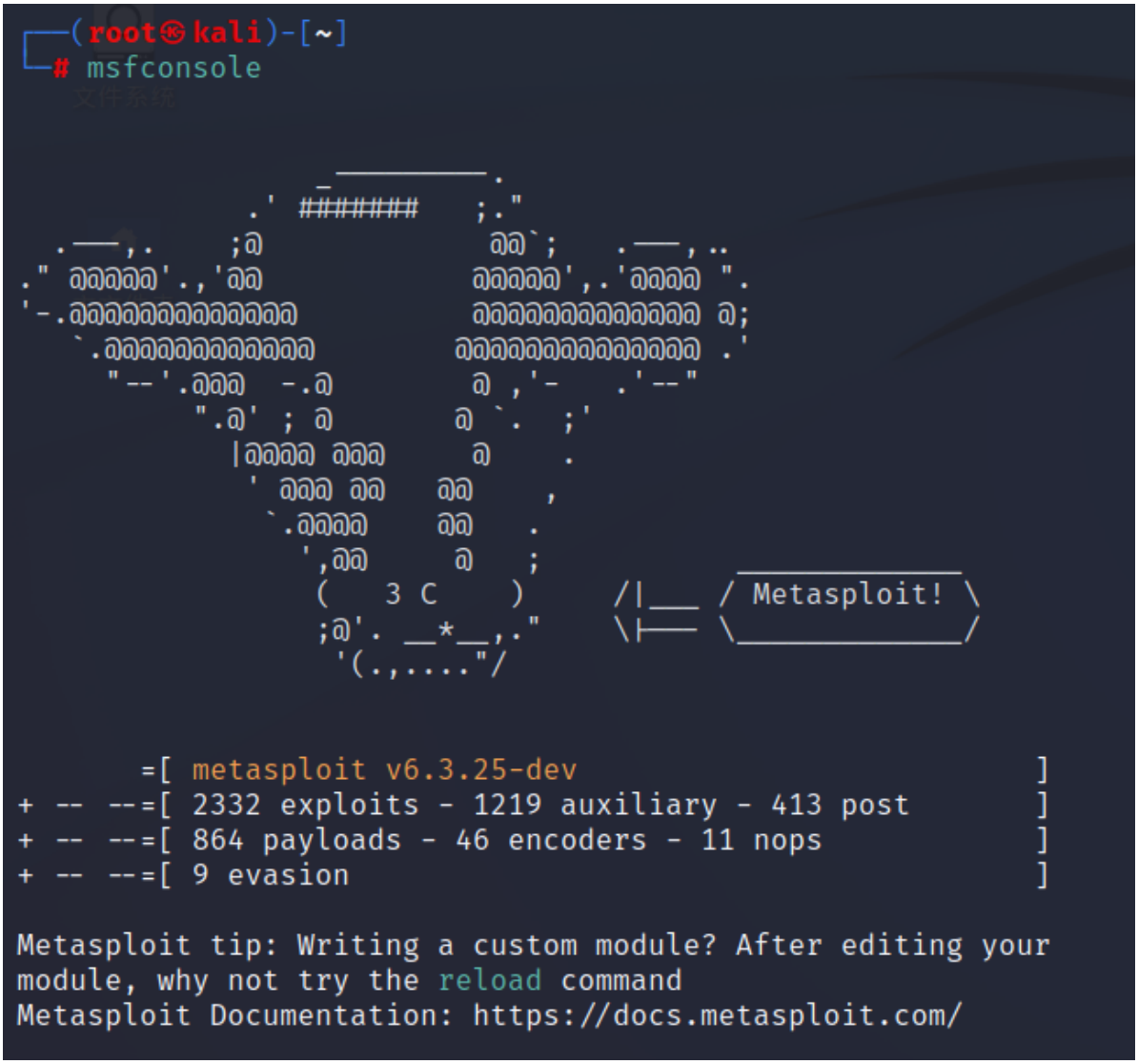
启动 MSFconsole

在Kali系统的命令行中输入 **msfconsole** 即可启动。MSFconsole 位于 **/usr/share/metasploit-framework/msfconsole** 目录中。

加 **-q** 选项删除开始的图形，是 **msfconsole** 的安静启动模式。

```
root@kali:# msfconsole -q
msf >
```

使用 MSFconsole 界面



如何使用命令提示符

可以传递 **-h** 给 **msfconsole** 以查看其他可用的使用选项。

```
root@kali:~# msfconsole -h
Usage: msfconsole [options]

Common options
    -E, --environment ENVIRONMENT    The Rails environment. Will use RAIL_ENV
environment variable if that is set.  Defaults to production if neither option
not RAILS_ENV environment variable is set.

Database options
    -M, --migration-path DIRECTORY   Specify a directory containing additional
DB migrations
    -n, --no-database                Disable database support
    -y, --yaml PATH                  Specify a YAML file containing database
settings

Framework options
    -c FILE                          Load the specified configuration file
    -v, --version                    Show version

Module options
```

```
        --defer-module-loads         Defer module loading unless explicitly
asked.
    -m, --module-path DIRECTORY      An additional module path


Console options:
    -a, --ask                        Ask before exiting Metasploit or accept
'exit -y'
    -d, --defanged                   Execute the console as defanged
    -L, --real-readline              Use the system Readline library instead of
RbReadline
    -o, --output FILE                Output to the specified file
    -p, --plugin PLUGIN              Load a plugin on startup
    -q, --quiet                      Do not print the banner on startup
    -r, --resource FILE              Execute the specified resource file (- for
stdin)
    -x, --execute-command COMMAND    Execute the specified string as console
commands (use ; for multiples)
    -h, --help                       Show this message
```

也可以进入 msf 环境中，使用`help`命令的列出帮助信息。

```
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


Database Backend Commands
=========================

    Command           Description
    -------           -----------
    creds             List all credentials in the database
    db_connect        Connect to an existing database
    db_disconnect     Disconnect from the current database instance
    db_export         Export a file containing the contents of the database
    db_import         Import a scan result file (filetype will be auto-detected)
    db_nmap           Executes nmap and records the output automatically
    db_rebuild_cache  Rebuilds the database-stored module cache
    db_status         Show the current database status
    hosts             List all hosts in the database
    loot              List all loot in the database
    notes             List all notes in the database
    services          List all services in the database
    vulns             List all vulnerabilities in the database
    workspace         Switch between database workspaces
```

补全标签

MSFconsole 旨在快速使用MSF，由于可用的模块种类繁多，因此可能很难记住我们希望使用的特定模块的确切名称和路径。

与大多数其他 shell 一样，输入我们知道的内容并按“Tab”键将显示可用选项列表，如果只有一个选项，则自动补全字符串。

Tab 补全取决于 ruby readline 扩展，并且控制台中的几乎每个命令都支持 Tab 补全。

```
use exploit/windows/dcerpc
```

```
msf > use exploit/windows/smb/ms
use exploit/windows/smb/ms03_049_netapi
use exploit/windows/smb/ms04_007_killbill
```

```
use exploit/windows/smb/ms04_011_lsass
use exploit/windows/smb/ms04_031_netdde
use exploit/windows/smb/ms05_039_pnp
use exploit/windows/smb/ms06_025_rasmans_reg
use exploit/windows/smb/ms06_025_rras
use exploit/windows/smb/ms06_040_netapi
use exploit/windows/smb/ms06_066_nwapi
use exploit/windows/smb/ms06_066_nwwks
use exploit/windows/smb/ms06_070_wkssvc
use exploit/windows/smb/ms07_029_msdns_zonename
use exploit/windows/smb/ms08_067_netapi
use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
use exploit/windows/smb/ms10_046_shortcut_icon_dllloader
use exploit/windows/smb/ms10_061_spoolss
use exploit/windows/smb/ms15_020_shortcut_icon_dllloader
msf > use exploit/windows/smb/ms08_067_netapi
```

exploit 是 Metasploit 最常用的接口。课堂时间有限，不可能展示exploit下的所有漏洞利用模块，所以会挑一些典型的漏洞进行讲解。学会了典型漏洞的利用方式之后，其他的漏洞利用模块都可以按照同样的步骤去学习使用，大同小异。

MSF console Commands

MSFconsole 有许多不同的命令选项可供选择，以下是参考其输出的一组核心 Metasploit 命令。

```
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
go_pro        Launch Metasploit web GUI
grep          Grep the output of another command
help          Help menu
info          Displays information about one or more module
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
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
```

back

一旦完成了特定模块的工作，或者如果无意中选择了错误的模块，可以发出 **back** 命令返回前一个命令行。

```
msf auxiliary(ms09_001_write) > back
msf >
```

banner

显示 banner 信息

```
msf > banner
 _                                                  _
/     /         __                          _   __  /_/ __
| |  / | _____               ___   _____ | | /   _
| | /| | | ___ |- -|   /    / __ | -__/ | || | || | |- -|
|_|   | | | _|__  | |_  / - __    | |    | | __/| |  | |_
      |/  |____/  ___/ / \___/   /     __|    |_  ___


       =[ metasploit v6.2.2-dev                         ]
+ -- --=[ 2227 exploits - 1171 auxiliary - 398 post    ]
+ -- --=[ 864 payloads - 45 encoders - 11 nops         ]
```

check

漏洞检查 选项，可以检查目标是否容易受到特定漏洞的攻击，而不是实际利用它。需要注意的是，支持check的漏洞利用模块并不多。

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    172.16.194.134   yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
```

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf exploit(ms08_067_netapi) > check

[*] Verifying vulnerable status... (path: 0x0000005a)
[*] System is not vulnerable (status: 0x00000000)
[*] The target is not exploitable.
msf  exploit(ms08_067_netapi) >
```

color

命令行字符设置是否展示颜色，可以搭配banner进行尝试。

```
msf > color
Usage: color >'true'|'false'|'auto'>

Enable or disable color output.
```

connect

msfconsole 中内置了一个微型 Netcat，支持 SSL、代理和文件传输。通过发出的 **connect** 带有 IP 地址和端口号命令，可以从 msfconsole 中连接到远程主机，就像使用 Netcat 或 Telnet 一样。

```
msf > connect 192.168.1.1 23
[*] Connected to 192.168.1.1:23
DD-WRT v24 std (c) 2008 NewMedia-NET GmbH
Release: 07/27/08 (SVN revision: 10011)
DD-WRT login:
```

可以通过`-h`来查看所有附加选项参数。

```
msf > connect -h
Usage: connect [options]

Communicate with a host, similar to interacting via netcat, taking advantage of
any configured session pivoting.

OPTIONS:

    -C        Try to use CRLF for EOL sequence.
    -P <opt>  Specify source port.
    -S <opt>  Specify source address.
    -c <opt>  Specify which Comm to use.
    -h        Help banner.
    -i <opt>  Send the contents of a file.
    -p <opt>  List of proxies to use.
    -s        Connect with SSL.
    -u        Switch to a UDP socket.
```

```
    -w <opt>  Specify connect timeout.
    -z        Just try to connect, then return.
```

exit

退出 msfconsole.

```
msf exploit(ms10_061_spoolss) > exit
root@kali:~#
```

grep

该 **grep** 的命令类似的Linux的grep。它匹配来自另一个 msfconsole 命令的输出内容。

以下是使用的示例， **grep** 匹配包含字符串“http”的输出，该输出来自 **搜索** 包含字符串“oracle”的模块。

```
msf > grep
Usage: grep [options] pattern cmd

Grep the results of a console command (similar to Linux grep command)

OPTIONS:

    -A <opt&>  Show arg lines of output After a match.
    -B   Show arg lines of output Before a match.
    -c        Only print a count of matching lines.
    -h        Help banner.
    -i        Ignore case.
    -k   Keep (include) arg lines at start of output.
    -m   Stop after arg matches.
    -s   Skip arg lines of output before attempting match.
    -v        Invert match.
msf >
msf > grep http search oracle
   auxiliary/scanner/http/oracle_demantra_database_credentials_leak      2014-
02-28       normal     Oracle Demantra Database Credentials Leak
   auxiliary/scanner/http/oracle_demantra_file_retrieval                 2014-
02-28       normal     Oracle Demantra Arbitrary File Retrieval with
Authentication Bypass
   auxiliary/scanner/http/oracle_ilom_login
         normal     Oracle ILO Manager Login Brute Force Utility
   exploit/multi/http/glassfish_deployer                                 2011-
08-04       excellent  Sun/Oracle GlassFish Server Authenticated Code Execution
   exploit/multi/http/oracle_ats_file_upload                             2016-
01-20       excellent  Oracle ATS Arbitrary File Upload
   exploit/multi/http/oracle_reports_rce                                 2014-
01-15       great      Oracle Forms and Reports Remote Code Execution
   exploit/windows/http/apache_chunked                                   2002-
06-19       good       Apache Win32 Chunked Encoding
   exploit/windows/http/bea_weblogic_post_bof                            2008-
07-17       great      Oracle Weblogic Apache Connector POST Request Buffer
Overflow
```

```
   exploit/windows/http/oracle9i_xdb_pass                                2003-
08-18       great      Oracle 9i XDB HTTP PASS Overflow (win32)
   exploit/windows/http/oracle_beehive_evaluation                        2010-
06-09       excellent  Oracle BeeHive 2 voice-servlet processEvaluation()
Vulnerability
   exploit/windows/http/oracle_beehive_prepareaudiotoplay                2015-
11-10       excellent  Oracle BeeHive 2 voice-servlet prepareAudioToPlay()
Arbitrary File Upload
   exploit/windows/http/oracle_btm_writetofile                           2012-
08-07       excellent  Oracle Business Transaction Management FlashTunnelService
Remote Code Execution
   exploit/windows/http/oracle_endeca_exec                               2013-
07-16       excellent  Oracle Endeca Server Remote Command Execution
   exploit/windows/http/oracle_event_processing_upload                   2014-
04-21       excellent  Oracle Event Processing FileUploadServlet Arbitrary File
Upload
   exploit/windows/http/osb_uname_jlist                                  2010-
07-13       excellent  Oracle Secure Backup Authentication Bypass/Command
Injection Vulnerability
```

help

列出帮助list和所有可用的命令.

```
msf > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
...snip...

Database Backend Commands
=========================

    Command           Description
    -------           -----------
    db_connect        Connect to an existing database
    db_disconnect     Disconnect from the current database instance
    db_export         Export a file containing the contents of the database
    db_import         Import a scan result file (filetype will be auto-detected)
...snip...
```

info

信息 命令会提供包括所有选项、目标和其它信息的特定漏洞利用模块的详细信息。

info 命令还提供以下信息：

作者和许可信息
漏洞参考（即：CVE、BID 等）
模块可能具有的任何有效载荷限制

```
msf  exploit(ms09_050_smb2_negotiate_func_index) > info

       Name: MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table
Dereference
     Module: exploit/windows/smb/ms09_050_smb2_negotiate_func_index
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-09-07

Provided by:
  Laurent Gaffie <laurent.gaffie@gmail.com>
  hdm <x@hdm.io>
  sf <stephen_fewer@harmonysecurity.com>

Available targets:
  Id  Name
  --  ----
  0   Windows Vista SP1/SP2 and Server 2008 (x86)

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see
https://github.com/rapid7/meta
                                     sploit-framework/wiki/Using-Metasploit
  RPORT   445              yes       The target port (TCP)
  WAIT    180              yes       The number of seconds to wait for the
attack to comple
                                     te.

Payload information:
  Space: 1024

Description:
  This module exploits an out of bounds function table dereference in
  the SMB request validation code of the SRV2.SYS driver included with
  Windows Vista, Windows 7 release candidates (not RTM), and Windows
  2008 Server prior to R2. Windows Vista without SP1 does not seem
  affected by this flaw.

References:
  https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2009/MS09-
050
  https://nvd.nist.gov/vuln/detail/CVE-2009-3103
```

```
  http://www.securityfocus.com/bid/36299
  OSVDB (57799)
  https://seclists.org/fulldisclosure/2009/Sep/0039.html
```

jobs

对工作在后台的进程进行操作。

```
msf > jobs -h
Usage: jobs [options]

Active job manipulation and interaction.

OPTIONS:

    -K      Terminate all running jobs.
    -h      Help banner.
    -i      Lists detailed information about a running job.
    -k      Terminate the specified job name.
    -l      List all running jobs.
    -v      Print more detailed info.  Use with -i and -l
```

kill

杀死正在运行的进程。

```
msf exploit(ms10_002_aurora) > kill 0
Stopping job: 0...

[*] Server stopped.
```

search

msfconsole包含广泛的基于正则表达式的搜索功能。如果对所要查找的内容有大致了解，可以通过**search**进行搜索。

```
msf6 > search usermap_script

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check
Description
   -  ----                                ---------------  ----       -----  ---
--------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No
Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use
exploit/multi/samba/usermap_script
```

name

要使用描述性名称进行搜索，需要使用**name**关键字。

```
msf > search name:mysql

Matching Modules
================

   Name                                              Disclosure Date  Rank
Description
   ----                                              ---------------  ----
  -----------
   auxiliary/admin/mysql/mysql_enum                                   normal
MySQL Enumeration Module
   auxiliary/admin/mysql/mysql_sql                                    normal
MySQL SQL Generic Query
   auxiliary/analyze/jtr_mysql_fast                                   normal
John the Ripper MySQL Password Cracker (Fast Mode)
   auxiliary/scanner/mysql/mysql_authbypass_hashdump  2012-06-09       normal
  MySQL Authentication Bypass Password Dump
   auxiliary/scanner/mysql/mysql_hashdump                             normal
MYSQL Password Hashdump
   auxiliary/scanner/mysql/mysql_login                                normal
MySQL Login Utility
   auxiliary/scanner/mysql/mysql_schemadump                           normal
MYSQL Schema Dump
   auxiliary/scanner/mysql/mysql_version                              normal
MySQL Server Version Enumeration
   exploit/linux/mysql/mysql_yassl_getname            2010-01-25      good
  MySQL yaSSL CertDecoder::GetName Buffer Overflow
   exploit/linux/mysql/mysql_yassl_hello              2008-01-04      good
  MySQL yaSSL SSL Hello Message Buffer Overflow
   exploit/windows/mysql/mysql_payload                2009-01-16      excellent
Oracle MySQL for Microsoft Windows Payload Execution
   exploit/windows/mysql/mysql_yassl_hello            2008-01-04      average
MySQL yaSSL SSL Hello Message Buffer Overflow
msf >
```

platform

可以使用**platform**将搜索范围缩小到影响特定平台的模块。

```
msf > search platform:aix

Matching Modules
================

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   payload/aix/ppc/shell_bind_tcp                         normal  AIX Command
Shell, Bind TCP Inline
   payload/aix/ppc/shell_find_port                        normal  AIX Command
Shell, Find Port Inline
   payload/aix/ppc/shell_interact                         normal  AIX execve
shell for inetd
...snip...
```

type

使用**type**可以按模块类型进行过滤，如辅助、发布、利用等。

```
msf > search type:post

Matching Modules
================

   Name                                              Disclosure Date  Rank
Description
   ----                                              ---------------  ----
 -----------
   post/linux/gather/checkvm                                          normal
Linux Gather Virtual Environment Detection
   post/linux/gather/enum_cron                                        normal
Linux Cron Job Enumeration
   post/linux/gather/enum_linux                                       normal
Linux Gather System Information
...snip...
```

author

使用**author**关键字搜索，可以按自己喜好的作者搜索模块。

```
msf > search author:dookie

Matching Modules
================

   Name                                                  Disclosure Date
Rank     Description
   ----                                                  ---------------  -
---     -----------
   exploit/osx/http/evocam_webserver                     2010-06-01
average  MacOS X EvoCam HTTP GET Buffer Overflow
   exploit/osx/misc/ufo_ai                               2009-10-28
average  UFO: Alien Invasion IRC Client Buffer Overflow Exploit
   exploit/windows/browser/amaya_bdo                     2009-01-28
normal   Amaya Browser v11.0 bdo tag overflow
...snip...
```

multiple

还可以将多个关键字组合在一起，以进一步缩小返回结果的范围。

```
msf > search cve:2011 author:jduck platform:linux

Matching Modules
================

   Name                                          Disclosure Date  Rank
Description
   ----                                          ---------------  ----     ------
-----
   exploit/linux/misc/netsupport_manager_agent  2011-01-08       average
NetSupport Manager Agent Remote Buffer Overflow
```

sessions

sessions命令允许列出、与衍生会话交互和终止衍生会话。

```
msf > sessions -h
Usage: sessions [options] or sessions [id]

Active session manipulation and interaction.

OPTIONS:

    -C   Run a Meterpreter Command on the session given with -i, or all
    -K   Terminate all sessions
    -c   Run a command on the session given with -i, or all
    -h   Help banner
    -i   Interact with the supplied session ID
    -k   Terminate sessions by session ID and/or range
    -l   List all active sessions
    -q   Quiet mode
    -r   Reset the ring buffer for the session given with -i, or all
```

```
    -s   Run a script on the session given with -i, or all
    -t   Set a response timeout (default: 15)
    -u   Upgrade a shell to a meterpreter session on many platforms
    -v   List sessions in verbose mode
    -x   Show extended information in the session table

Many options allow specifying session ranges using commas and dashes.
For example:  sessions -s checkvm -i 1,3-5  or  sessions -k 1-2,5,6
```

要列出所有活动的会话，使用 **-l** 选项传递给**sessions**。

```
msf exploit(3proxy) > sessions -l

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

  Id  Description    Tunnel
  --  -----------    ------
  1   Command shell  192.168.1.101:33191 -> 192.168.1.104:4444
```

要与给定会话交互，只需使用 **-i** ，后面跟会话的id号。

```
msf exploit(3proxy) > sessions -i 1
[*] Starting interaction with 1...

C:\WINDOWS\system32>
```

set

set命令允许为正在使用的当前模块配置框架选项和参数。

```
msf auxiliary(ms09_050_smb2_negotiate_func_index) > set RHOST 172.16.194.134
RHOST => 172.16.194.134
msf auxiliary(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  172.16.194.134   yes       The target address
   RPORT  445              yes       The target port
   WAIT   180              yes       The number of seconds to wait for the
attack to complete.

Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)
```

Metasploit还允许设置在运行时使用的编码器。当不确定哪些有效负载编码方法将与给定的漏洞一起工作时，就需要进行选择。这在漏洞利用开发中特别有用。

```
msf  exploit(ms09_050_smb2_negotiate_func_index) > show encoders

Compatible Encoders
===================

   Name                    Disclosure Date  Rank       Description
   ----                    ---------------  ----       -----------
   generic/none                             normal     The "none" Encoder
   x86/alpha_mixed                          low        Alpha2 Alphanumeric
Mixedcase Encoder
   x86/alpha_upper                          low        Alpha2 Alphanumeric
Uppercase Encoder
   x86/avoid_utf8_tolower                   manual     Avoid UTF8/tolower
   x86/call4_dword_xor                      normal     Call+4 Dword XOR Encoder
   x86/context_cpuid                        manual     CPUID-based Context Keyed
Payload Encoder
   x86/context_stat                         manual     stat(2)-based Context
Keyed Payload Encoder
   x86/context_time                         manual     time(2)-based Context
Keyed Payload Encoder
   x86/countdown                            normal     Single-byte XOR Countdown
Encoder
   x86/fnstenv_mov                          normal     Variable-length
Fnstenv/mov Dword XOR Encoder
   x86/jmp_call_additive                    normal     Jump/Call XOR Additive
Feedback Encoder
   x86/nonalpha                             low        Non-Alpha Encoder
   x86/nonupper                             low        Non-Upper Encoder
   x86/shikata_ga_nai                       excellent  Polymorphic XOR Additive
Feedback Encoder
   x86/single_static_bit                    manual     Single Static Bit
   x86/unicode_mixed                        manual     Alpha2 Alphanumeric
Unicode Mixedcase Encoder
   x86/unicode_upper                        manual     Alpha2 Alphanumeric
Unicode Uppercase Encoder
```

unset

与**set**命令相反的是**unset**取消设置，将删除以前使用设置所配置的参数。可以使用**unset all**删除所有分配的变量。

```
msf > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf > set THREADS 50
THREADS => 50
msf > set

Global
======

  Name     Value
  ----     -----
  RHOSTS   192.168.1.0/24
  THREADS  50
```

```
msf > unset THREADS
Unsetting THREADS...
msf > unset all
Flushing datastore...
msf > set

Global
======

No entries in data store.

msf >
```

setg

为了节省渗透期间的大量输入，可以在msfconsole中设置**全局变量**。

可以使用**setg**命令执行此操作。一旦这些设置完成，可以在任意多的漏洞利用和辅助模块中使用它们，还可以保存它们以供下次启动msfconsole时使用。

```
msf > setg LHOST 192.168.1.101
LHOST => 192.168.1.101
msf > setg RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf > setg RHOST 192.168.1.136
RHOST => 192.168.1.136
```

设置不同的变量后，可以运行**save**命令保存当前环境和设置。保存设置后，它们将在启动时自动加载，从而无需再次设置所有内容。

```
msf > save
Saved configuration to: /root/.msf4/config
msf >
```

show

在 msfconsole 提示符下输入 **show** 命令将显示Metasploit中的每个模块，比如常用的命令是**show auxiliary**、**show exploits**、**show payloads**、**show encoders**。

auxiliary

Metasploit的**辅助模块**，主要用于信息搜集阶段，功能包括扫描、口令猜解、敏感信息嗅探、FUZZ测试发掘漏洞、实施网络协议欺骗等。

```
msf > show auxiliary
Auxiliary
=========

   Name                                                Disclosure Date  Rank
Description
   ----                                                ---------------  ----
 -----------
   admin/2wire/xslt_password_reset                     2007-08-15       normal
2Wire Cross-Site Request Forgery Password Reset Vulnerability
   admin/backupexec/dump                                                normal
Veritas Backup Exec Windows Remote File Access
   admin/backupexec/registry                                            normal
Veritas Backup Exec Server Registry Access
...snip...
```

exploits

show exploits是我们最感兴趣的模块，因为Metasploit的核心是利用漏洞。运行**show exploits**以获取 MSF 框架中包含的所有漏洞的列表。

```
msf > show exploits

Exploits
========

   Name                                                    Disclosure Date
Rank       Description
   ----                                                    ---------------
-  ----       -----------
   aix/rpc_cmsd_opcode21                                   2009-10-07
  great      AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer
Overflow
   aix/rpc_ttdbserverd_realpath                            2009-06-17
  great      ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow
(AIX)
   bsdi/softcart/mercantec_softcart                        2004-08-19
  great      Mercantec SoftCart CGI Overflow
...snip...
```

payloads

运行**show payloads**将显示Metasploit中所有可用平台的所有不同有效载荷。

```
msf > show payloads

Payloads
========

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   aix/ppc/shell_bind_tcp                   normal  AIX Command Shell, Bind TCP
Inline
   aix/ppc/shell_find_port                  normal  AIX Command Shell, Find Port
Inline
   aix/ppc/shell_interact                   normal  AIX execve shell for inetd
...snip...
```

当处于某个特定漏洞利用模块下时，运行**show payloads**将只显示与该特定漏洞利用模块兼容的有效负载。例如，如果它是一个Windows漏洞，将不会看到Linux有效负载。

```
msf  exploit(ms08_067_netapi) > show payloads

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   generic/custom                           normal  Custom Payload
   generic/debug_trap                       normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                   normal  Generic Command Shell, Bind
TCP Inline
...snip...
```

options

如果选择了特定模块，则可以发出**show options**命令，显示该特定模块下必要&可选的设置项。

```
msf exploit(ms08_067_netapi) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

targets

如果不确定操作系统是否易受特定攻击，在攻击模块的上下文中运行**show targets**命令，查看支持哪些目标。

```
msf  exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   10  Windows 2003 SP1 Japanese (NO NX)
   11  Windows 2003 SP2 English (NO NX)
   12  Windows 2003 SP2 English (NX)
...snip...
```

advanced

如果希望进一步微调漏洞，可以通过运行**show advanced**查看更多高级选项。

```
msf exploit(ms08_067_netapi) > show advanced

Module advanced options (exploit/windows/smb/ms08_067_netapi):

   Name                  Current Setting    Required  Description
   ----                  ---------------    --------  -----------
   CHOST                                    no        The local client address
   CPORT                                    no        The local client port
   ConnectTimeout        10                 yes       Maximum number of seconds
to establish a
                                                       TCP connection
...snip...
```

encoders

运行**show encoders**将显示MSF中可用的编码器列表。

```
msf > show encoders
Compatible Encoders
===================

   Name                    Disclosure Date  Rank       Description
   ----                    ---------------  ----       -----------
   cmd/generic_sh                           good       Generic Shell Variable
Substitution Command Encoder
   cmd/ifs                                  low        Generic ${IFS}
Substitution Command Encoder
   cmd/printf_php_mq                        manual     printf(1) via PHP
magic_quotes Utility Command Encoder
   generic/none                             normal     The "none" Encoder
   mipsbe/longxor                           normal     XOR Encoder
```

```
   mipsle/longxor                           normal     XOR Encoder
   php/base64                               great      PHP Base64 encoder
   ppc/longxor                              normal     PPC LongXOR Encoder
   ppc/longxor_tag                          normal     PPC LongXOR Encoder
   sparc/longxor_tag                        normal     SPARC DWORD XOR Encoder
   x64/xor                                  normal     XOR Encoder
   x86/alpha_mixed                          low        Alpha2 Alphanumeric
Mixedcase Encoder
   x86/alpha_upper                          low        Alpha2 Alphanumeric
Uppercase Encoder
   x86/avoid_utf8_tolower                   manual     Avoid UTF8/tolower
   x86/call4_dword_xor                      normal     Call+4 Dword XOR Encoder
   x86/context_cpuid                        manual     CPUID-based Context Keyed
Payload Encoder
   x86/context_stat                         manual     stat(2)-based Context
Keyed Payload Encoder
   x86/context_time                         manual     time(2)-based Context
Keyed Payload Encoder
   x86/countdown                            normal     Single-byte XOR Countdown
Encoder
   x86/fnstenv_mov                          normal     Variable-length
Fnstenv/mov Dword XOR Encoder
   x86/jmp_call_additive                    normal     Jump/Call XOR Additive
Feedback Encoder
   x86/nonalpha                             low        Non-Alpha Encoder
   x86/nonupper                             low        Non-Upper Encoder
   x86/shikata_ga_nai                       excellent  Polymorphic XOR Additive
Feedback Encoder
   x86/single_static_bit                    manual     Single Static Bit
   x86/unicode_mixed                        manual     Alpha2 Alphanumeric
Unicode Mixedcase Encoder
   x86/unicode_upper                        manual     Alpha2 Alphanumeric
Unicode Uppercase Encoder
```

use

当决定使用某个特定模块时，使用**use**命令来选择它。**use**命令将上下文更改为特定模块。

```
msf > use dos/windows/smb/ms09_001_write
msf auxiliary(ms09_001_write) > show options

Module options:

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  445              yes       Set the SMB service port

msf auxiliary(ms09_001_write) >
```