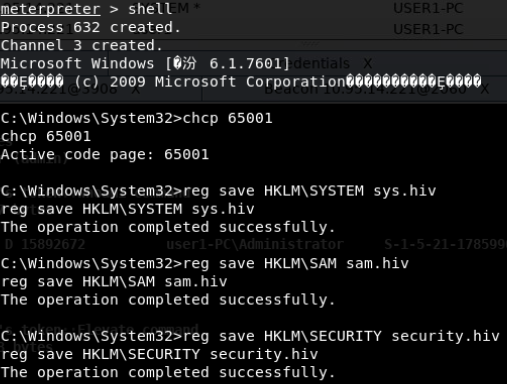
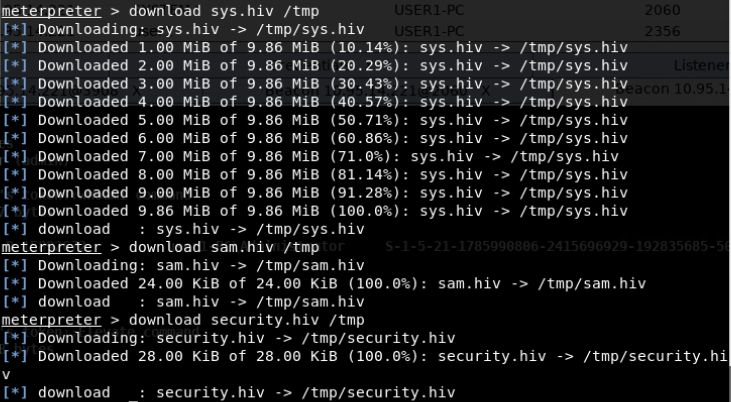
**离线提取目标机hash：**

离线提取目标机hash

当mimikatz不允许使用时，离线提取hash值



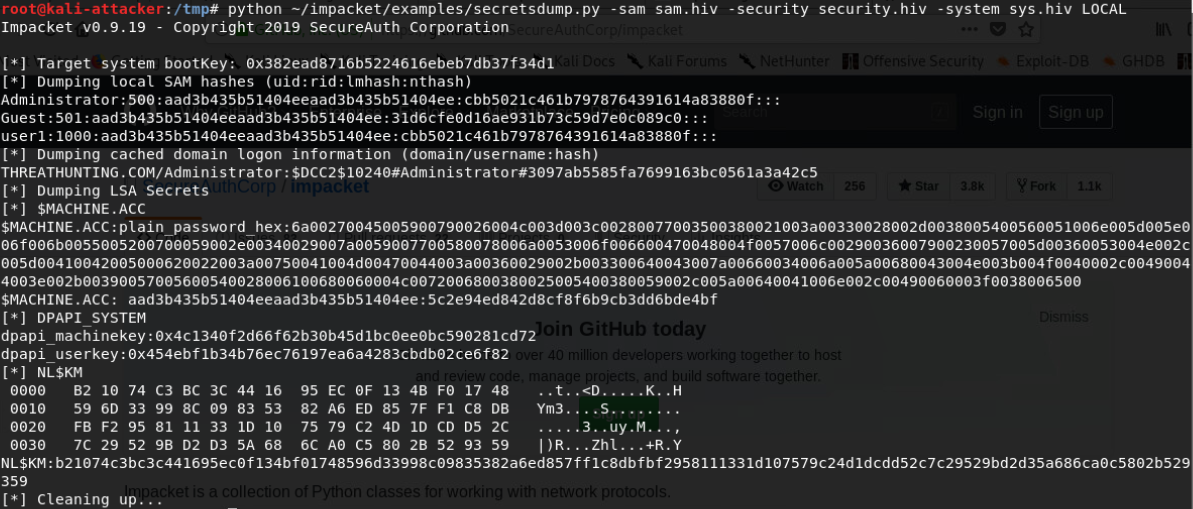






离线提取目标机hash:

https://github.com/SecureAuthCorp/impacket



**NTDS.dit中提取域内用户密码hash：**

获取NTDS.dit

当拥有域管权限后，可提取ntds.dit文件

Ntds.dit是主要的AD数据库，包括有关域用户，组和组成员身份的信息。它还包括域中所有用户的密码哈希值。为了进一步保护密码哈希值，使用存储在SYSTEM注册表配置单元中的密钥对这些哈希值进行加密。

Volume Shadow Copy Service 是微软从 Windows XP 开始提供的用于创建一致性的时间点副本（也就是快照）的服务框架

用于数据备份

支持Windows Server 2003 及以上操作系统

系统默认在特定条件下自动创建数据备份，如补丁安装后。在Win7系统大概每隔一周自动创建备份，该时间无法确定

禁用VSS会影响系统正常使用，如 System Restore和 Windows Server Backup

hash数量：所有用户

免杀：不需要

优点：

获得信息全面

简单高效

无需下载ntds.dit，隐蔽性高

通过Volume Shadow Copy获得域控服务器NTDS.dit文件

调用Volume Shadow Copy服务会产生日志文件，位于System下，Event ID为7036

执行ntdsutil snapshot "activate instance ntds" create quit quit会额外产生Event ID为98的日志文件

ntdsutil 域环境默认安装

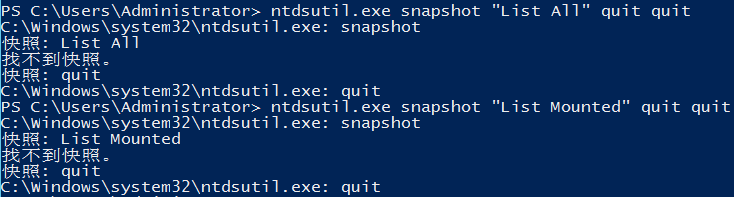
支持系统：

Server 2003

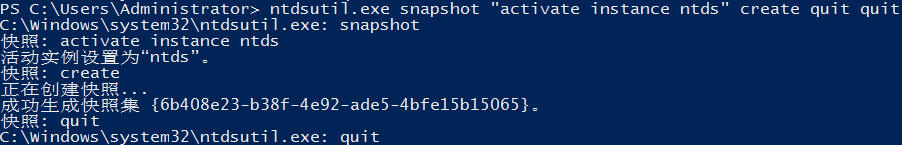
Server 2008

Server 2012

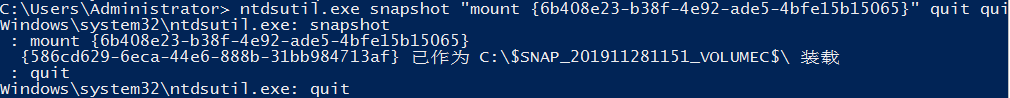
1.查询当前系统的快照



2.创建快照

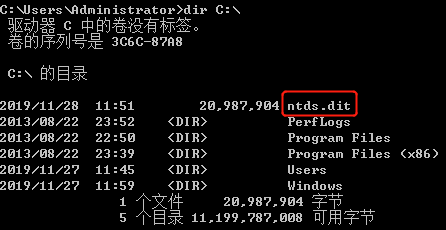


3.挂载快照

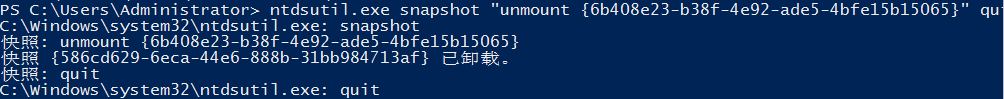


4.复制ntds.dit





5.卸载快照



6.删除快照



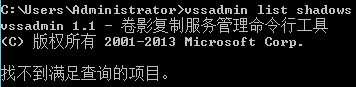
vssadmin 域环境默认安装

支持系统：

Server 2008

Server 2012

1.查询当前系统的快照

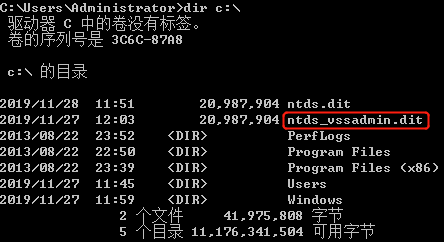


2.创建快照



3.复制ntds.dit





4.删除快照



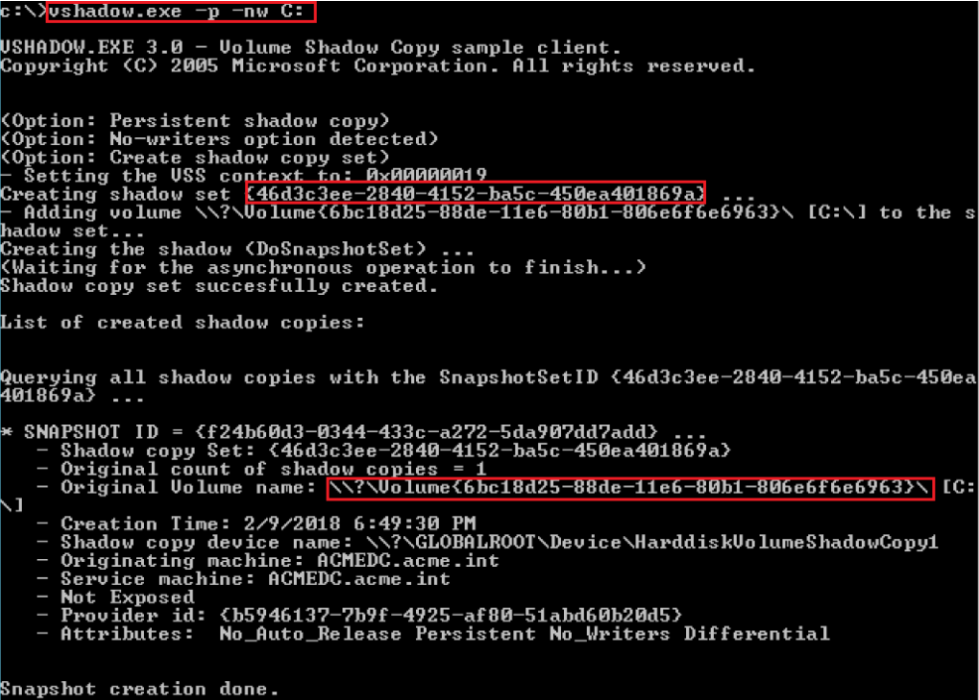
vshadow.exe 系统默认不支持

1.查询当前系统快照

vshadow.exe -q

2.创建快照

vshadow.exe -p -nw c:

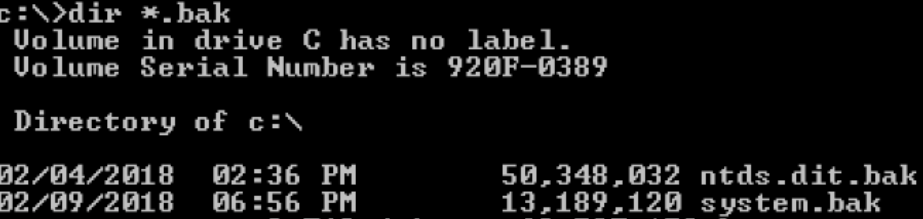


3.复制ntds.dit

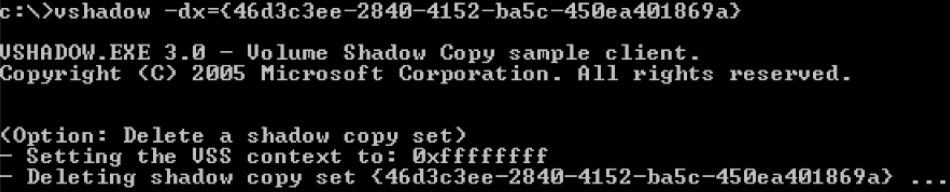


4.提取SYSTEM hive





5.删除快照



vshadow.exe执行命令

vshadow.exe -nw -exec=c:\windows\system32\notepad.exe c:

执行后，后台存在进程VSSVC.exe，同时显示服务Volume Shadow Copy正在运行，需要手动关闭进程VSSVC.exe，但会产生日志7034。

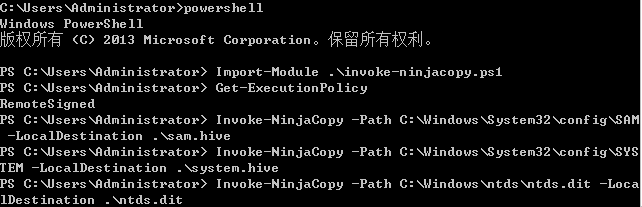
利用思路：

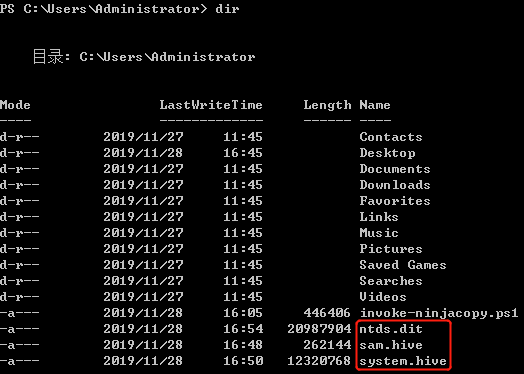
vshadow.exe包含微软签名，能绕过某些白名单的限制。如果作为启动项，Autoruns的默认启动列表不显示。

通过NinjaCopy获得域控服务器NTDS.dit文件

https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1

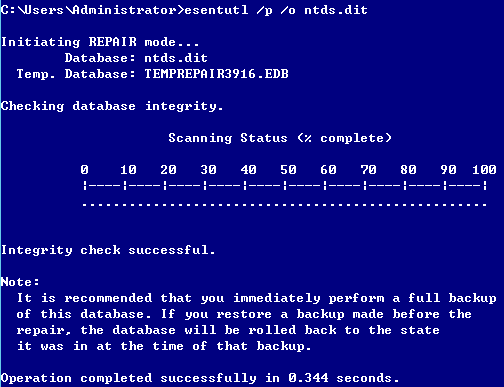
没有调用Volume Shadow Copy服务，所以不会产生日志文件7036





读取ntds.dit中密码哈希:

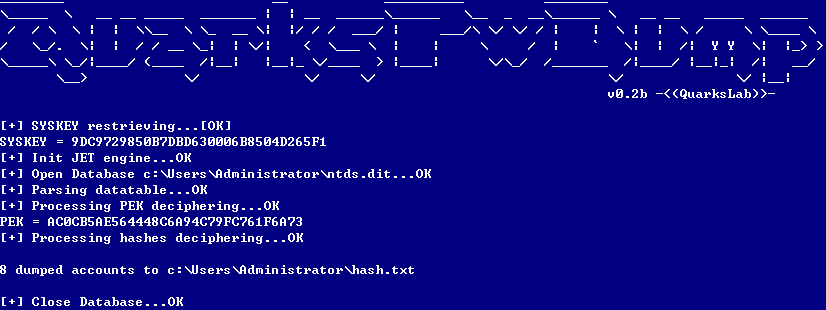
1.Quarks PwDump 一款开放源代码的Windows用户凭据提取工具，它可以抓取windows平台下多种类型的用户凭据，包括：本地帐户、域帐户、缓存的域帐户和Bitlocker。



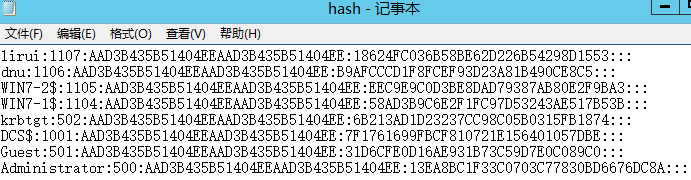


需输入文件的绝对路径:









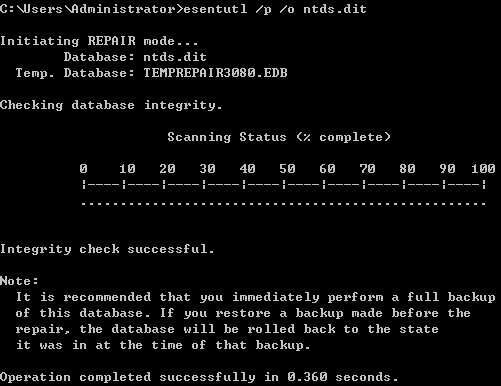
2. secretsdump.py

https://github.com/SecureAuthCorp/impacket/blob/master/examples/secretsdump.py

secretsdump.py -ntds ntds.dit.bak -system system.bak LOCAL

https://github.com/maaaaz/impacket-examples-windows/blob/master/secretsdump.exe

secretsdump.exe -system system.hive -ntds ntds.dit LOCAL



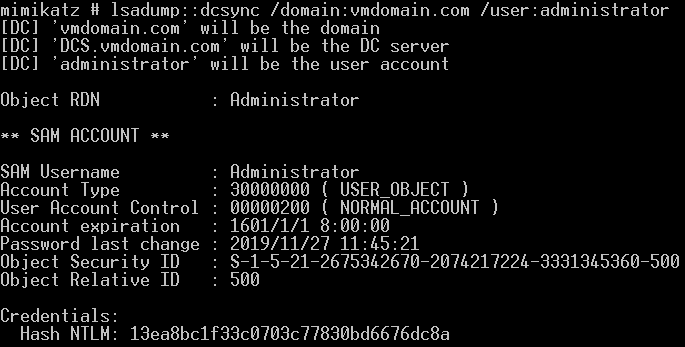


**DCsync获取所有域用户密码hash:**

它模拟域控制器来请求该域中用户的所有哈希，只要有权限(具有从域控制器中提取哈希的权限)，就不需要运行任何域控制器上的命令，也不必删除 DC 上的任何文件。

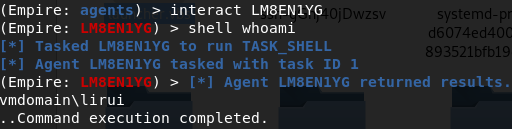
通常是限于域管理员、企业管理员、域控制器用户组以及将复制更改权限设置为允许（即复制所有更改和复制目录更改）的任何人

mimikatz:

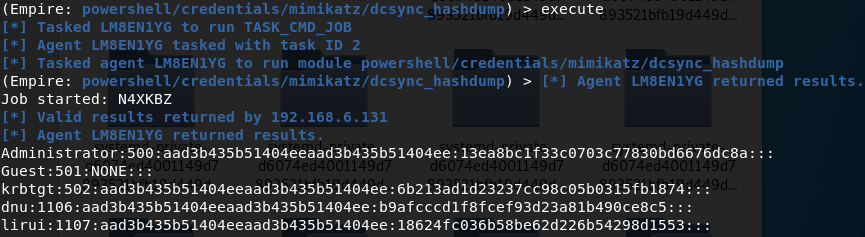


empire dcsync\_hashdump:

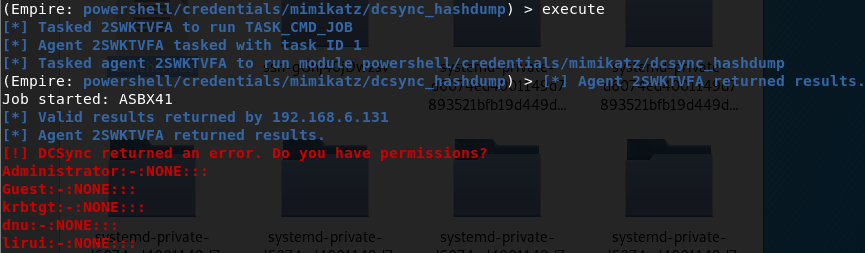
域管权限:







普通域用户:



本地管理员:

