Introduction

“Attacktive Directory" is an advanced training simulation designed for learning network penetration testing in Windows Active Directory environments. It offers a practical approach to understanding network vulnerabilities, focusing on tools like Impacket, Bloodhound, and Kerbrute for enumeration and exploitation. This room is ideal for both beginners and experienced professionals looking to enhance their skills in Active Directory. security.
https://tryhackme.com/room/attacktivedirectory
https://tryhackme.com/p/Damiano254

Task 1: Intro: Deploy The Machine

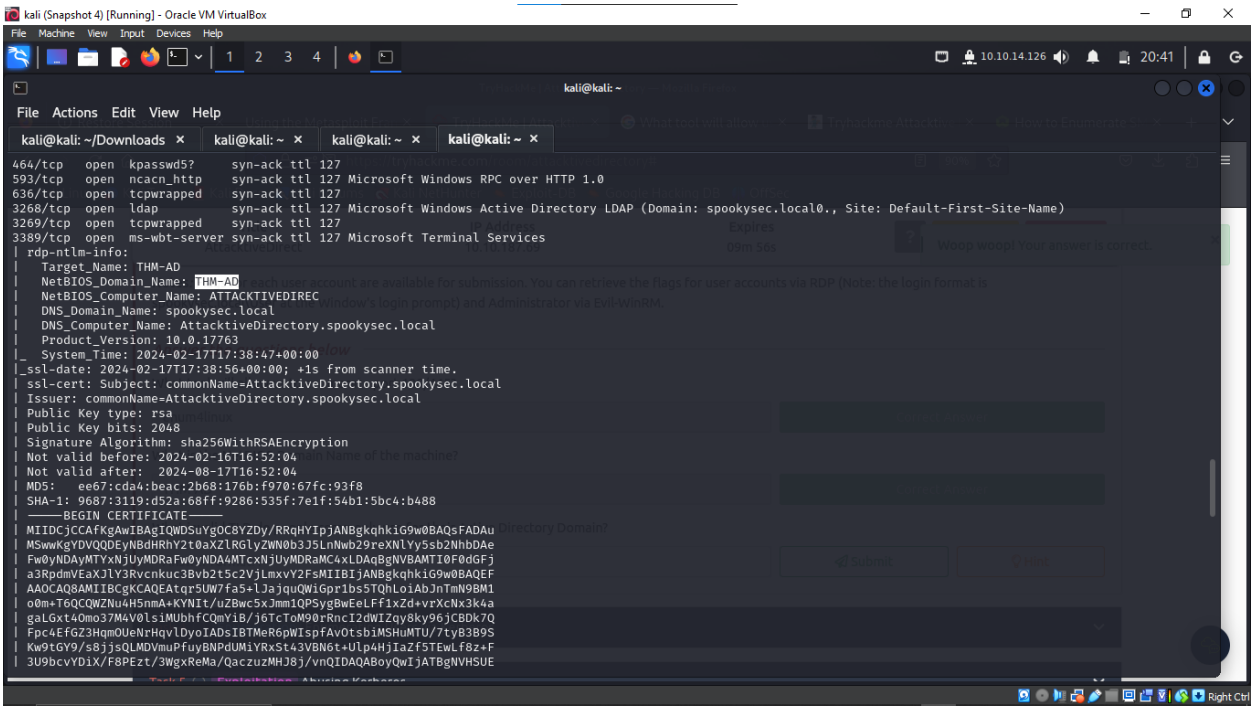
- **Accessing Attactive Directory**:
  Machines Utilized for the Exercise: THM (TryHackMe) Attack Box and Kali Linux Attack Box

Task 2: Intro Setup

- **Installing Impacket**: Detailed steps for installing Impacket on either Kali 2019.3 or Kali 2021.1, including cloning the Impacket GitHub repo and installing Python requirements.
- **Installing Bloodhound and Neo4j**: Instructions to install these tools using the **apt install** command. Troubleshooting tips include updating and upgrading packages if issues arise.

Task 3: Enumeration Welcome to Attactive Directory

- **Introduction by Spooks**: A welcome message and background about the room's creation and its evolution.
- **Enumeration with Nmap**: Guidance on using Nmap for basic enumeration, followed by the use of other utilities for further service enumeration.
- First, we will scan our target machine using Nmap



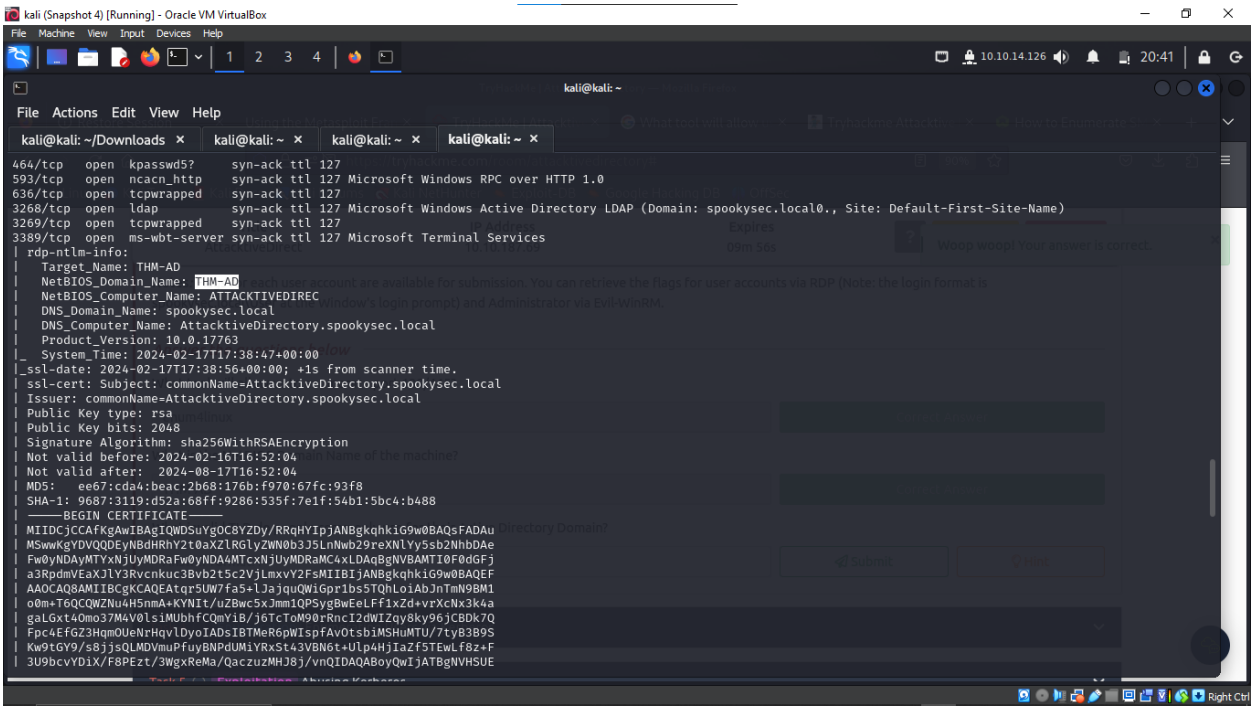
- **Questions and Answers**:
  - **Tool for enumerating port 139/445**: enum4linux

It looks like SMB is open, so we're in business.

Enum4linux is a tool used to enumerate SMB shares on both Windows and Linux systems. It is basically a wrapper around the tools in the Samba package and makes it easy to quickly extract information from the target pertaining to SMB.

Enter **enum4linux** in the terminal by itself to view the help and usage information:

- **NetBIOS-Domain Name**: THM-AD



- **Common invalid TLD for Active Directory Domain**: .local

Popular Domain Naming Mistakes

Before we discuss current best practices, there are a couple of popular practices that are *no* longer recommended.

The first is using a generic top-level domain. Generic TLDs like `.local`, `.lan`, `.corp`, etc, are now being sold by ICANN, so the domain you're using internally today – `company.local` could potentially become another company's property tomorrow. If you're still not convinced, here are some more reasons why you shouldn't use `.local` in your Active Directory domain name

Secondly, if you use an external public domain name like `company.com`, you should avoid using the same domain as your internal Active Directory name because you'll end up with a split DNS. Split DNS is when you have two separate DNS servers managing the exact same DNS Forward Lookup Zone, increasing the administrative burden.

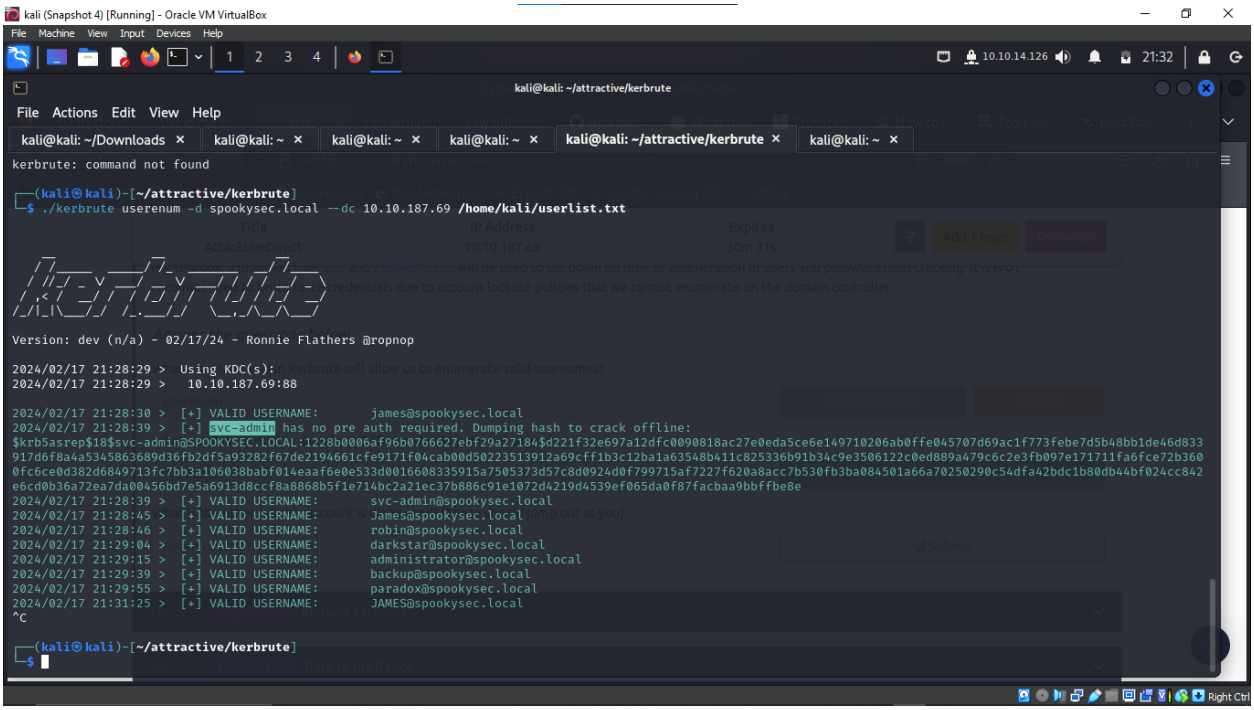
Task 4: Enumeration Enumerating Users via Kerberos

- **Introduction to Kerberos**: Overview of Kerberos and its role in Active Directory.
- **Enumeration with Ker brute**: Using Ker brute for brute force discovery of users and passwords. Downloaded the Kerbrute from the following link: https://github.com/ropnop/kerbrute/releases
  Downloaded the Password List and the Username List:
- `wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/userlist.txt`

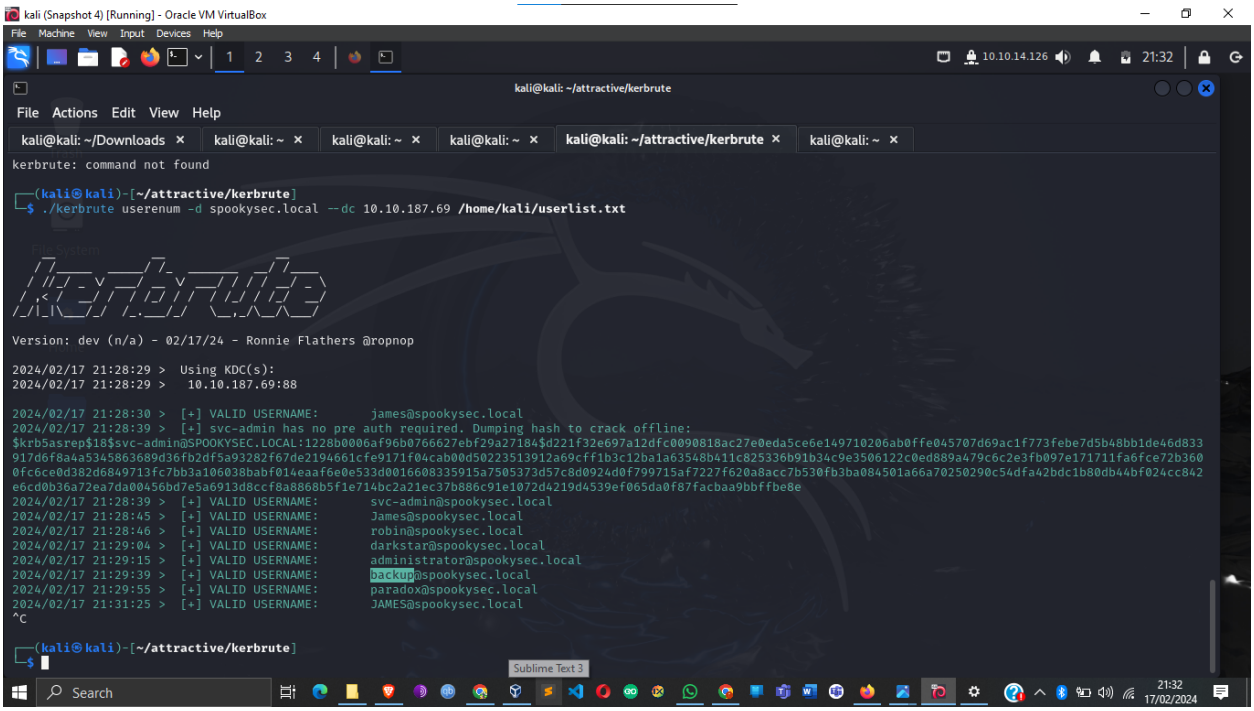
```
wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt
```

- **Questions and Answers**:
  - **Kerbrute command for valid usernames**: userenum

  - **What notable account is discovered? (These should jump out at you)**: svc-admin

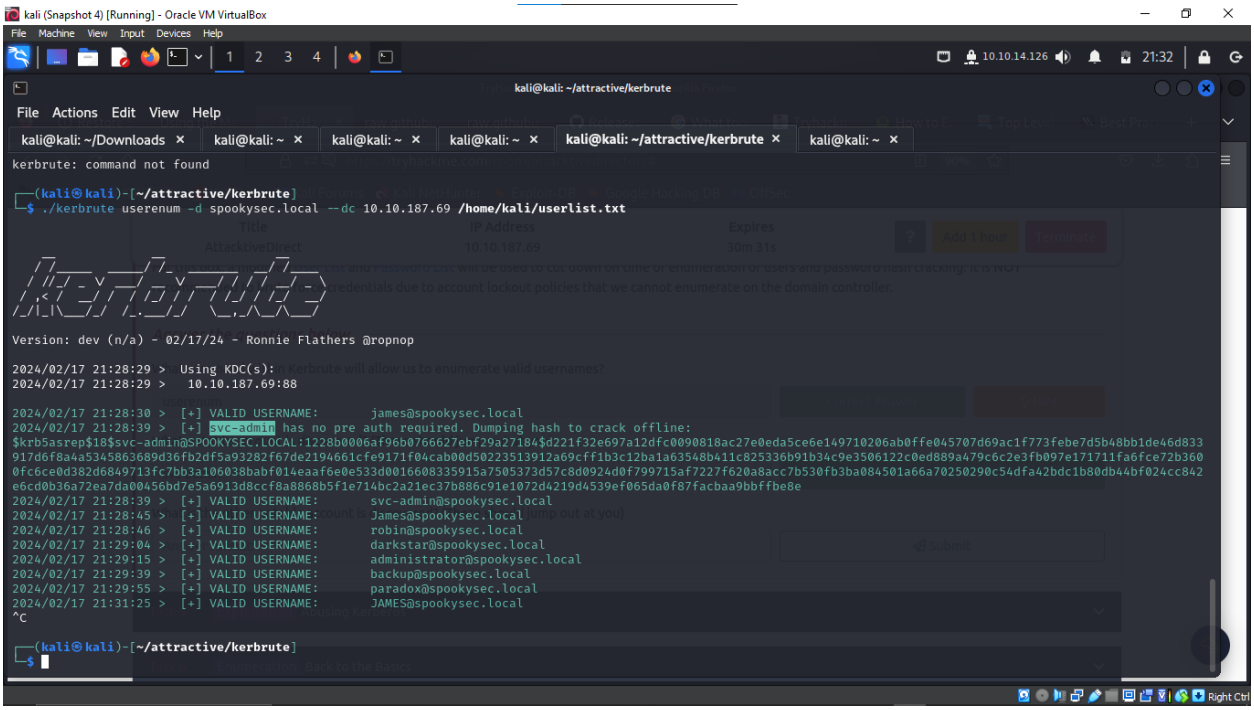


  - **What notable account is discovered? (These should jump out at you)**: backup

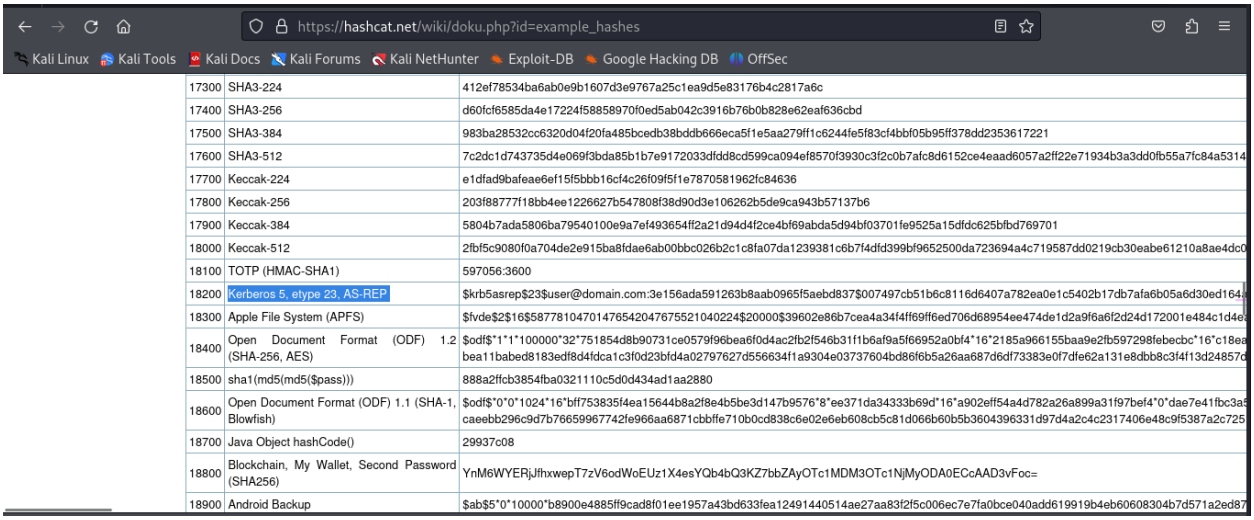


Task 5: Exploitation Abusing Kerberos

- **ASREPRoasting**: Explanation of ASREPRoasting in Kerberos and how to exploit it using Impacket's "GetNPUsers.py".
    - **Questions and Answers**:
        - **We have two user accounts that we could potentially query a ticket from. Which user account can you query a ticket from with no password?** svc-admin



- **Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)**
  : Kerberos 5 AS-REP etype 23



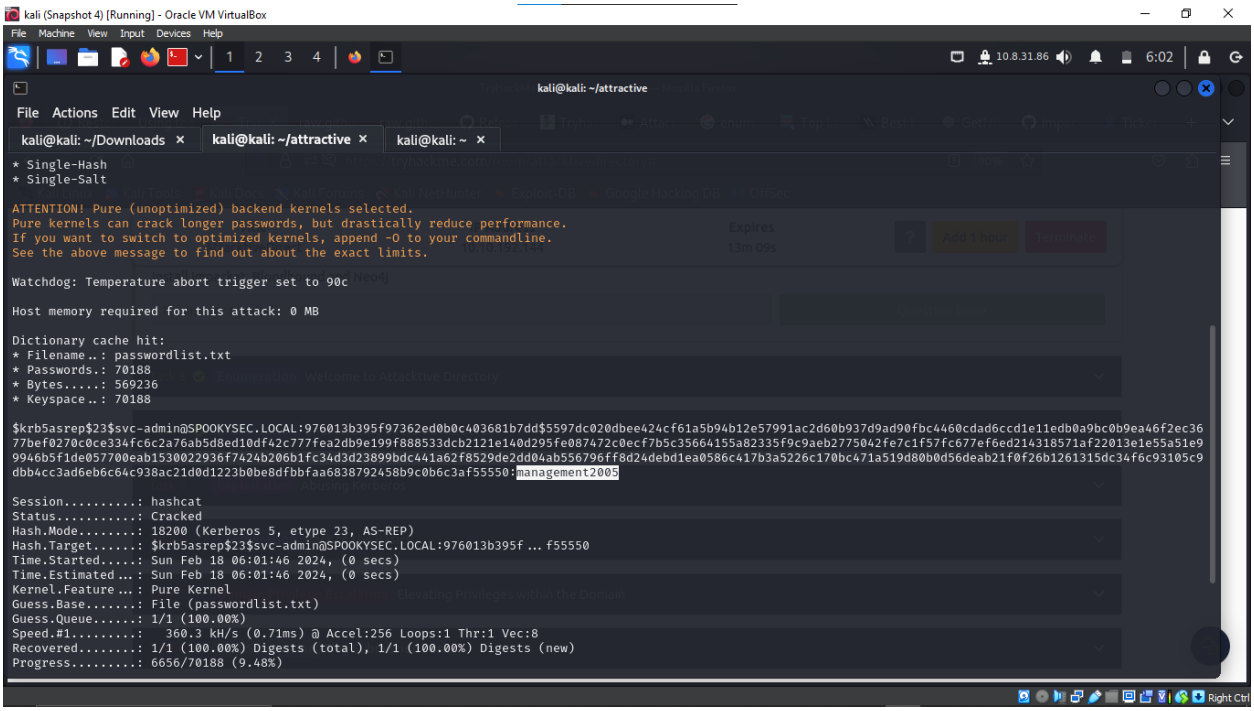
17300	SHA3-224	412ef78534ba6ab0e9b1607d3e9767a25c1ea9d5e83176b4c2817a6c
17400	SHA3-256	d60fcf6585da4e17224f58858970f0ed5ab042c3916b76b0b828e62eaf636cbd
17500	SHA3-384	983ba28532cc6320d04f20fa485bcedb38bddb666eca5f1e5aa279ff1c6244fe5f83cf4bbf05b95ff378dd2353617221
17600	SHA3-512	7c2dc1d743735d4e069f3bda85b1b7e9172033dfdd8cd599ca094ef8570f3930c3f2c0b7afc8d6152ce4eaad6057a2ff22e71934b3a3dd0fb55a7fc84a5314
17700	Keccak-224	e1dfad9bafeae6ef15f5bbb16cf4c26f09f5f1e7870581962fc84636
17800	Keccak-256	203f88777f18bb4ee1226627b547808f38d90d3e106262b5de9ca943b57137b6
17900	Keccak-384	5804b7ada5806ba79540100e9a7ef493654ff2a21d94d4f2ce4bf69abda5d94bf03701fe9525a15dfdc625bfbd769701
18000	Keccak-512	2fbf5c9080f0a704de2e915ba8fdae6ab00bbc026b2c1c8fa07da1239381c6b7f4dfd399bf9652500da723694a4c719587dd0219cb30eabe61210a8ae4dc0
18100	TOTP (HMAC-SHA1)	597056:3600
18200	Kerberos 5, etype 23, AS-REP	$krb5asrep$23$user@domain.com:3e156ada591263b8aab0965f5aebd837$007497cb51b6c8116d6407a782ea0e1c5402b17db7afa6b05a6d30ed164
18300	Apple File System (APFS)	$fvde$2$16$58778104701476542047675521040224$20000$39602e86b7cea4a34f4ff69ff6ed706d68954ee474de1d2a9f6a6f2d24d172001e484c1d4e
18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	odf*1*1*100000*32*751854d8b90731ce0579f96bea6f0d4ac2fb2f546b31f1b6af9a5f66952a0bf4*16*2185a966155baa9e2fb597298febecbc*16*c18ea bea11babed8183edf8d4fdca1c3f0d23bfd4a02797627d556634f1a9304e03737604bd86f6b5a26aa687d6df73383e0f7dfe62a131e8dbb8c3f4f13d24857d
18500	sha1(md5(md5($pass)))	888a2ffcb3854fba0321110c5d0d434ad1aa2880
18600	Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	odf*0*0*1024*16*bff753835f4ea15644b8a2f8e4b5be3d147b9576*8*ee371da34333b69d*16*a902eff54a4d782a26a899a31f97bef4*0*dae7e41fbc3a5 caeebb296c9d7b76659967742fe966aa6871cbbffe710b0cd838c6e02e6eb608cb5c81d066b60b5b3604396331d97d4a2c4c2317406e48c9f5387a2c725
18700	Java Object hashCode()	29937c08
18800	Blockchain, My Wallet, Second Password (SHA256)	YnM6WYERjJfhxwepT7zV6odWoEUz1X4esYQb4bQ3KZ7bbZAyOTc1MDM3OTc1NjMyODA0ECcAAD3vFoc=
18900	Android Backup	ab5*0*10000*b8900e4885ff9cad8f01ee1957a43bd633fea12491440514ae27aa83f2f5c006ec7e7fa0bce040add619919b4eb60608304b7d571a2ed87

- **Hashcat mode for the hash**: 18200

18200	Kerberos 5, etype 23, AS-REP	$krb5asrep$23$user@domain.com:3e156ada591263b8aab0965f5aebd837$007497cb51b6c8116d6407a782ea0e1c5402b17db7afa6b05a6d30ed164a

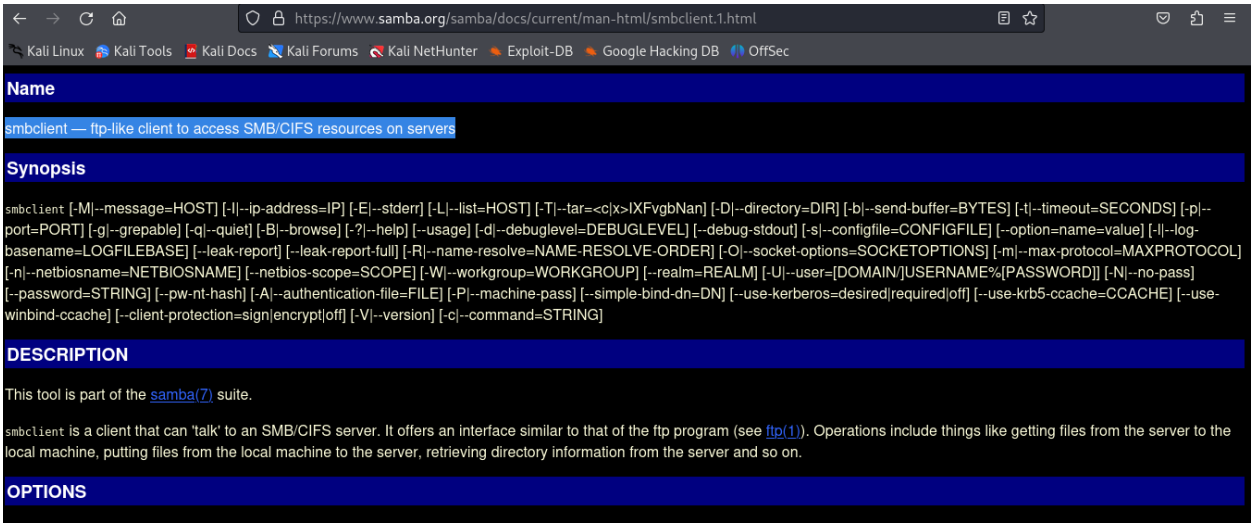
- **Password of user account after cracking the hash**: management2005

Hashcat -a 0 -m 18200 hash.txt passwordlist.txt --force

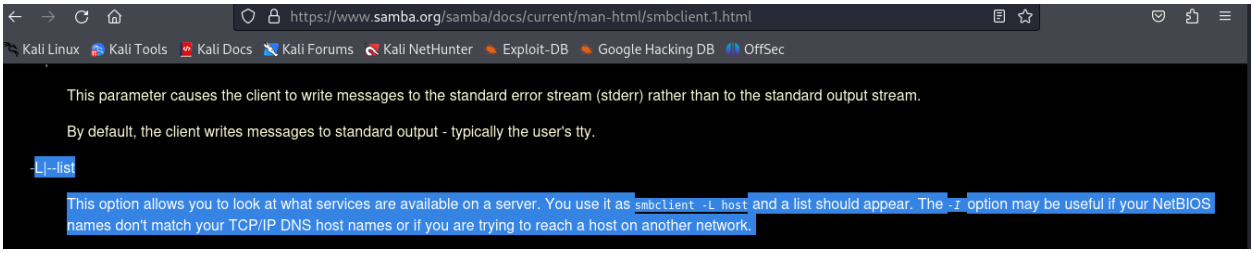


Task 6: Enumeration Back to the Basics

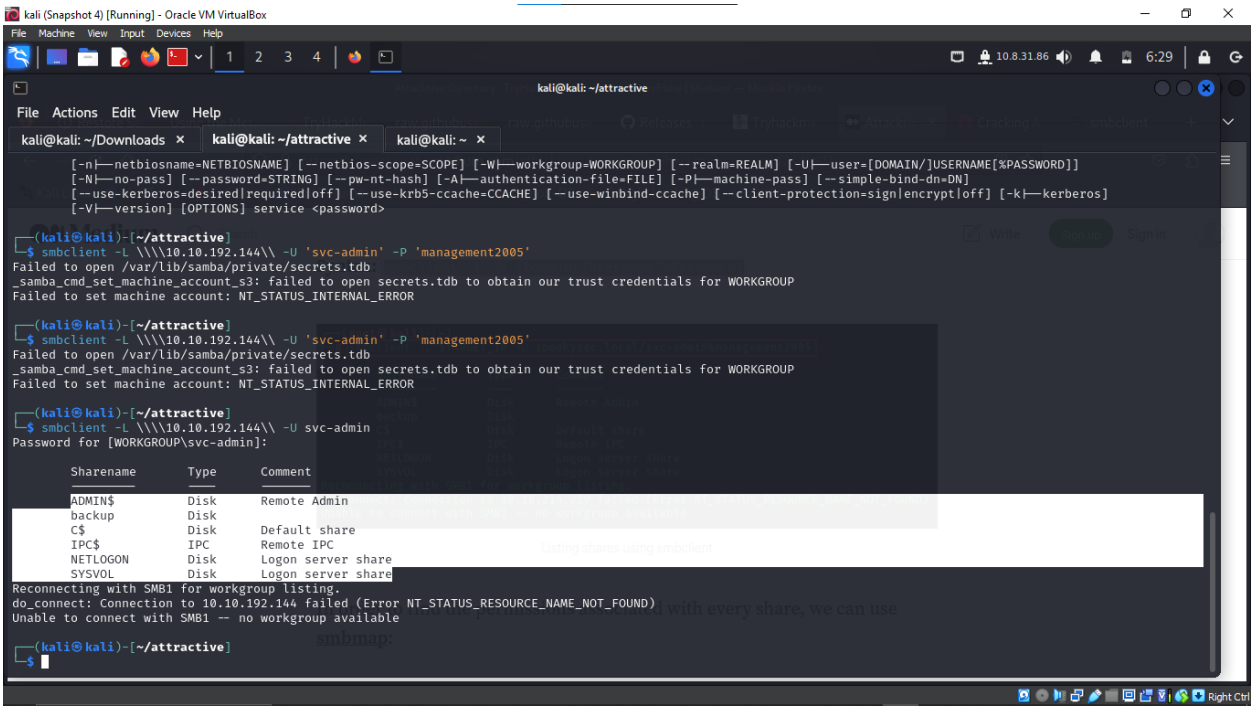
- **Enumerating SMB Shares**: Instructions on using smbclient to map remote SMB shares and locate specific files.
    - **Questions and Answers**:
        - **Utility for mapping SMB shares**: smbclient



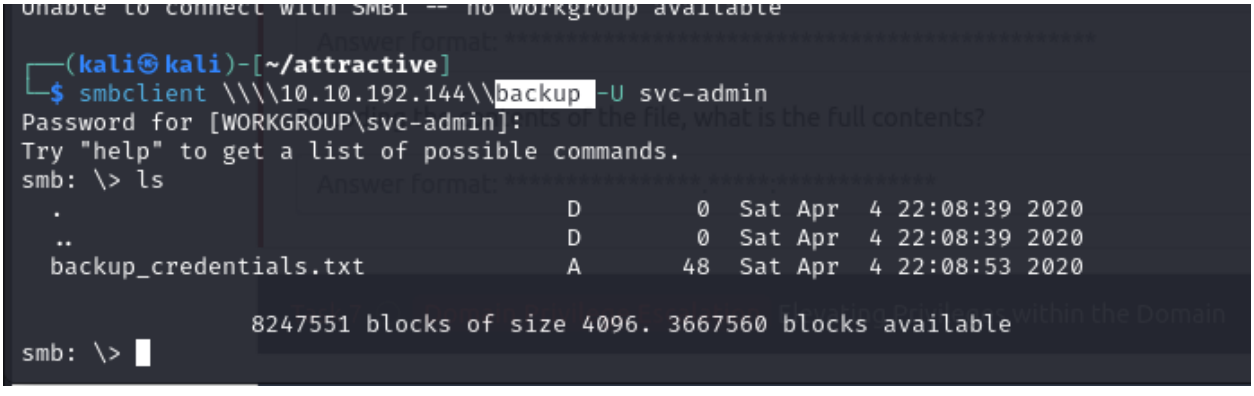
- **Option to list shares**: -L



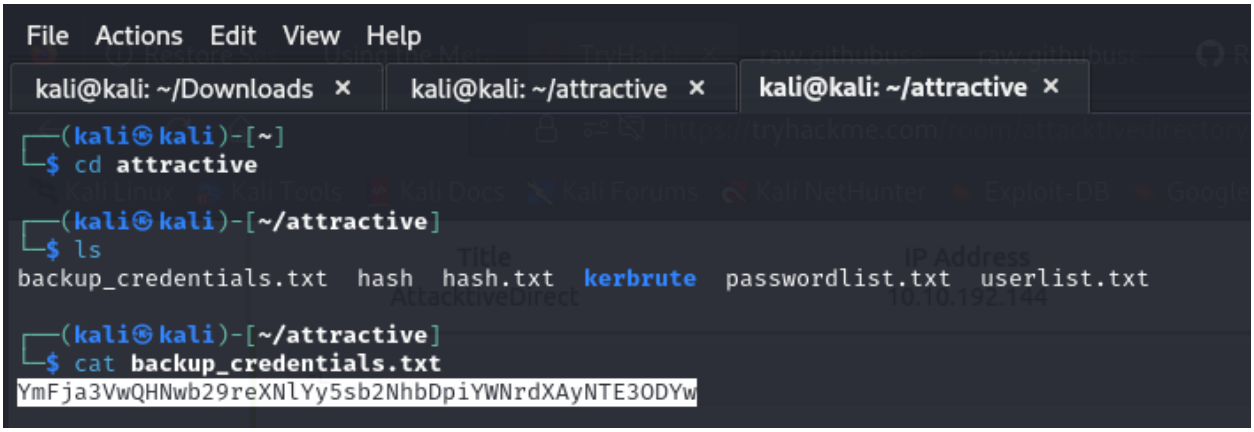
- **Number of shares listed**: 6



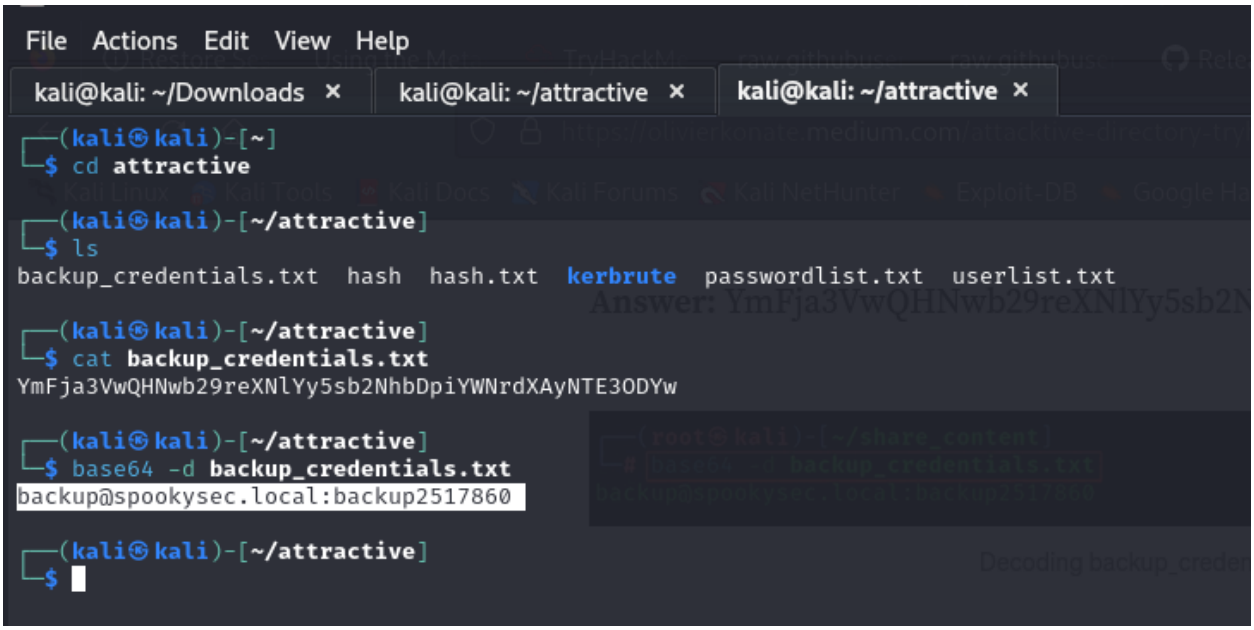
- **Share containing a specific text file**: backup



- **Content of the file**: YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

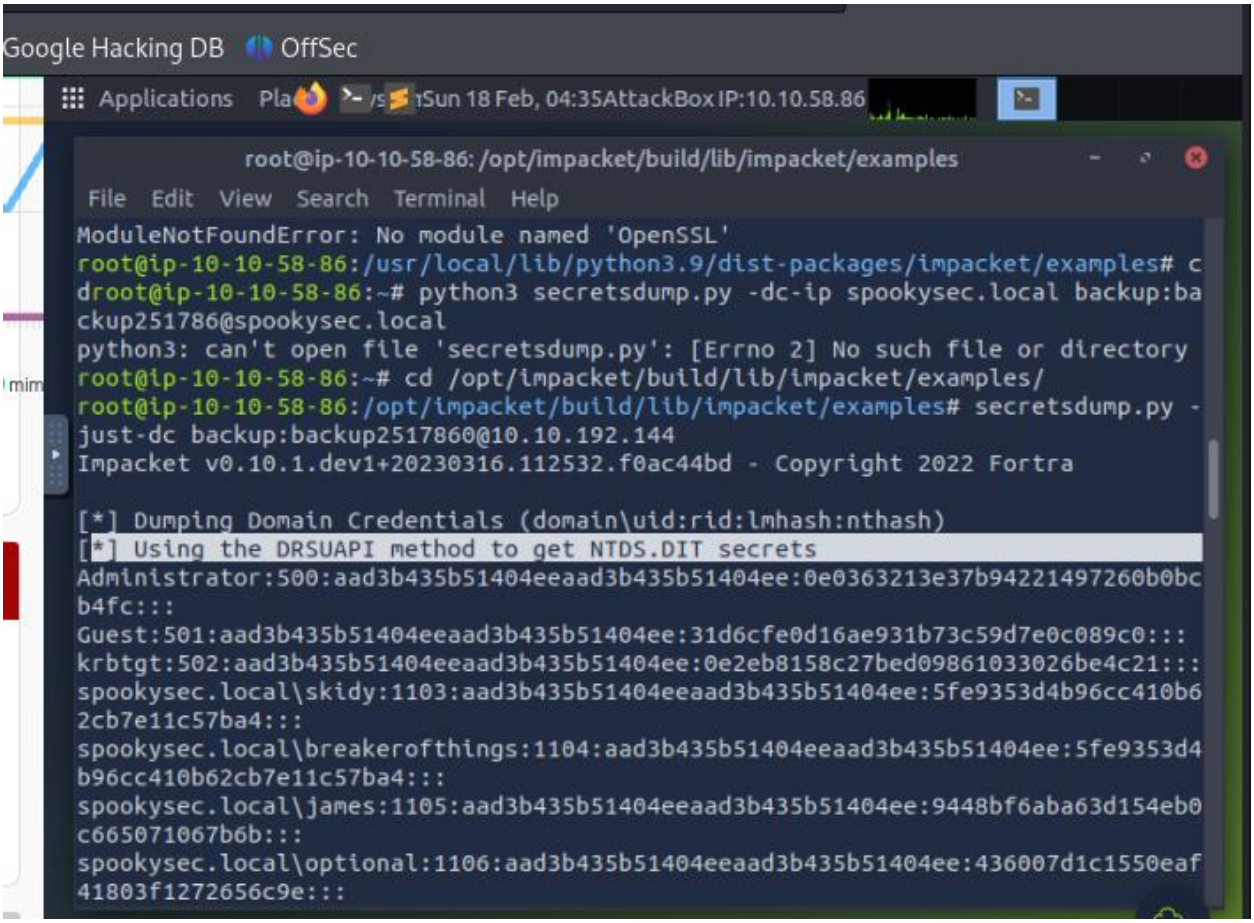


- **Decoded contents of the file**: backup@spookysec.local: backup2517860

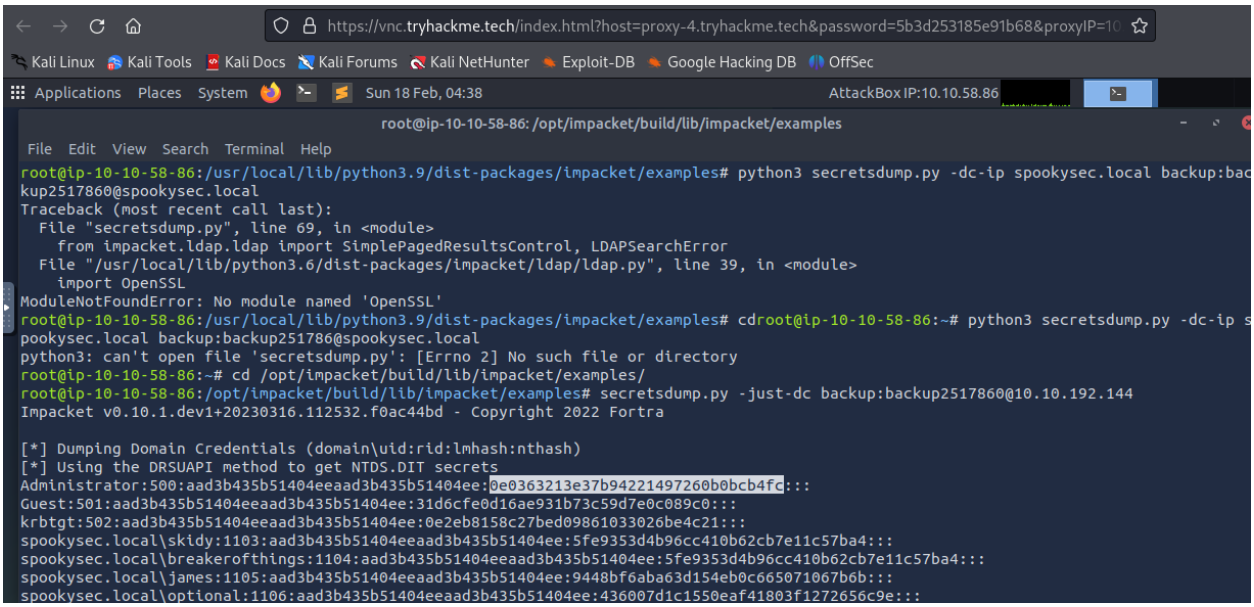


Task 7: Exploitation Let's Sync Up!

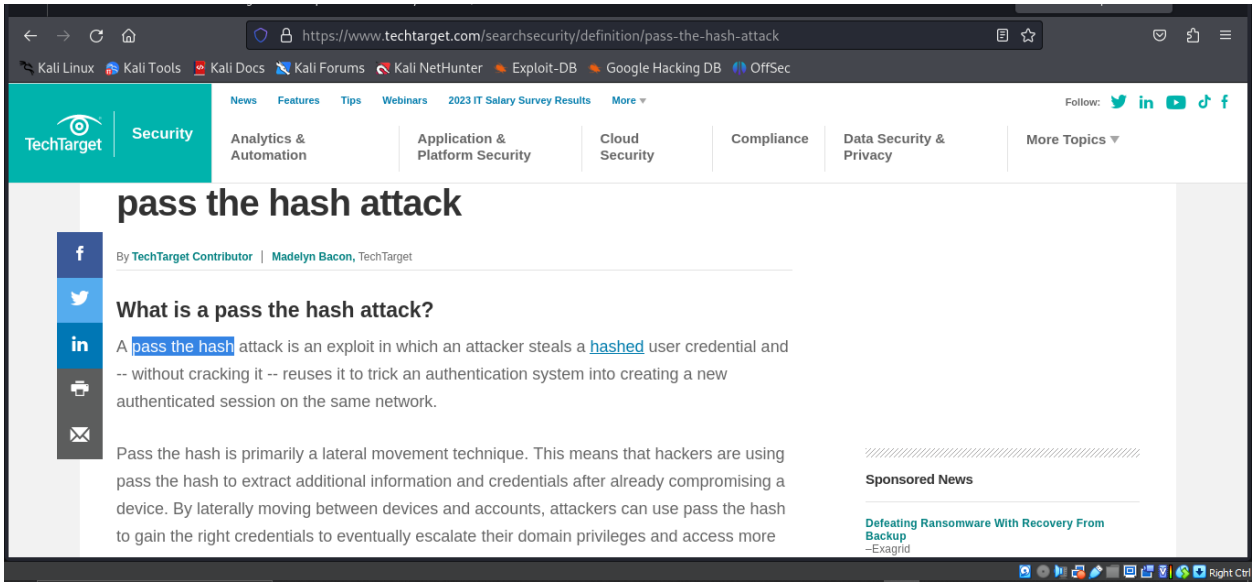
- **Exploiting the Backup Account**: Using the backup account's permissions to sync with the Domain Controller and retrieve password hashes.
    - **Questions and Answers**:
        - **Method to dump NTDS.DIT**: DRSUAPI



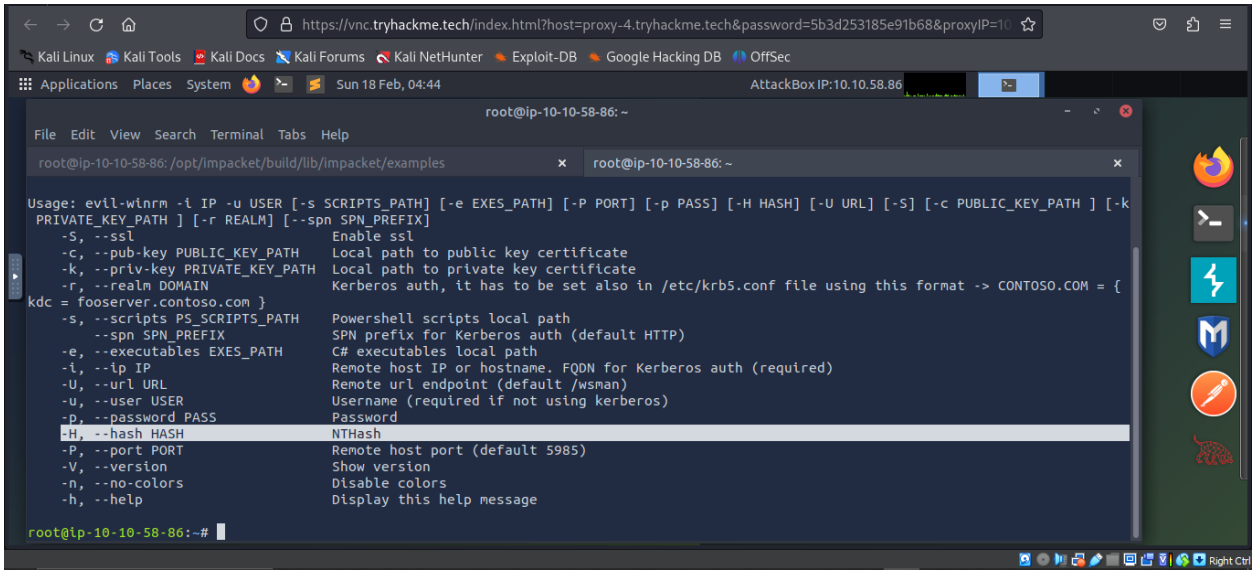
- **Administrator's NTLM hash**: 0e0363213e37b94221497260b0bcb4fc



- **Attack method for authentication without the password**: Pass the Hash

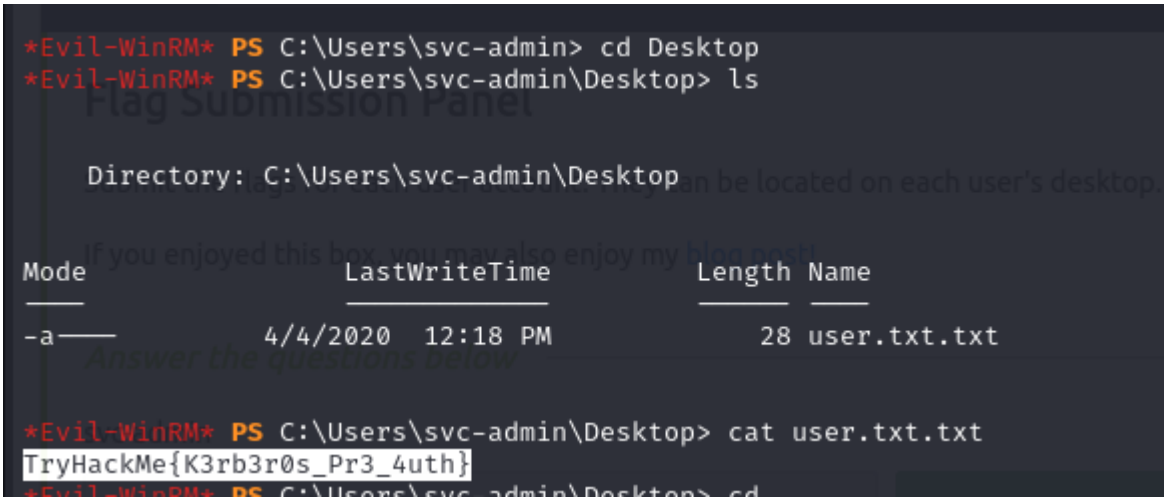


- **Evil-WinRM option for using a hash**: -H



Task 8: Flag Submission Flag Submission Panel

- **Flag Submission**: Instructions for submitting flags for each user account.
  - **Questions and Answers**:
    - **svc-admin Flag**: TryHackMe{K3rb3r0s_Pr3_4uth}



- **backup Flag**: TryHackMe{B4ckM3UpSc0tty!}

```
    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> cat priEsc.txt
Cannot find path 'C:\Users\backup\Desktop\priEsc.txt' because it does not exist.
At line:1 char:1
+ cat priEsc.txt
+ ~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\backup\Desktop\priEsc.txt:String) [Get-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Users\backup\Desktop> cat privEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
*Evil-WinRM* PS C:\Users\backup\Desktop>
```

- **Administrator Flag**: TryHackMe{4ctiveD1rectoryM4st3r}

```
Path
----
C:\Users\Administrator\Documents


*Evil-WinRM* PS C:\Users\Administrator\Documents> Dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    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> cat root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
```

Conclusion

Completing the "Attacktive Directory" course signifies a significant advancement in understanding Active Directory security. I have gained practical experience in identifying and exploiting network vulnerabilities using various tools and techniques. This foundational knowledge is crucial for further growth in cybersecurity, emphasizing the importance of continuous learning and adaptation in this ever-evolving field.

Damiano254 [0x5]

Get Profile Badge ID | Share Room Badges

Rooms Complete | Badges | Created Rooms | Yearly Activity | Tickets