**Attacktive Directory**

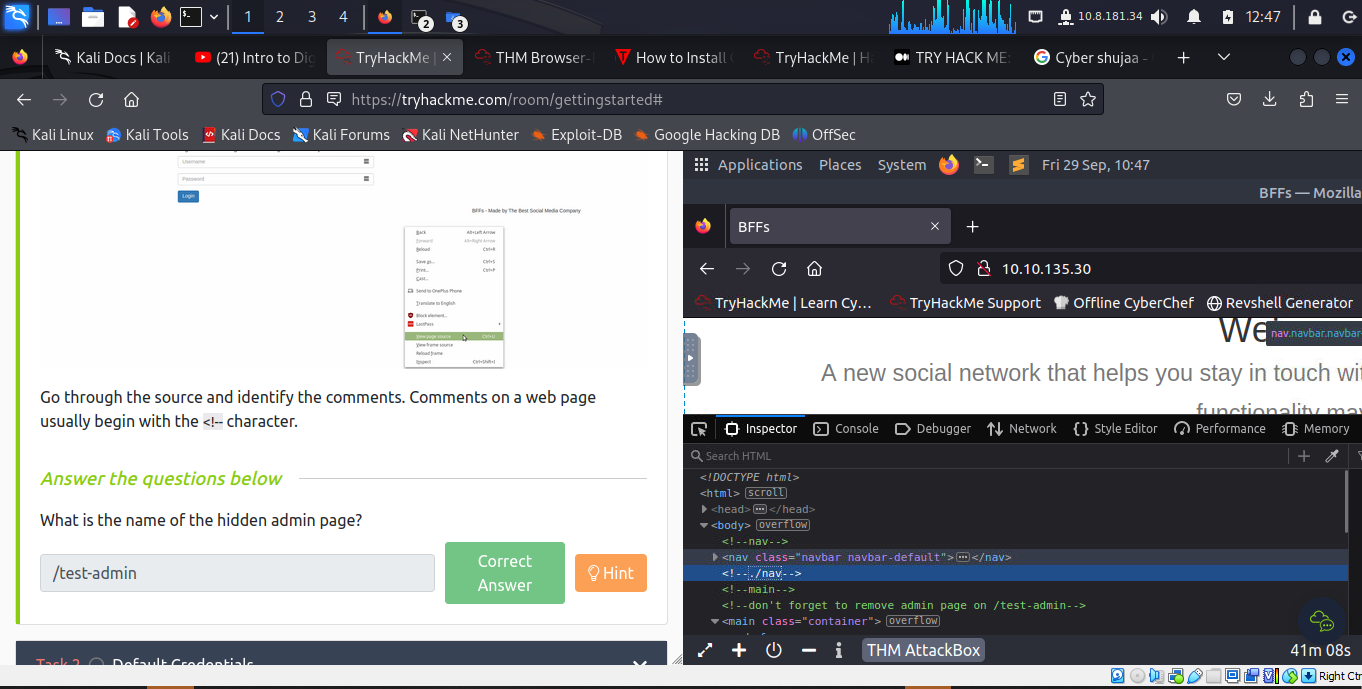
**Introduction**

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>.**

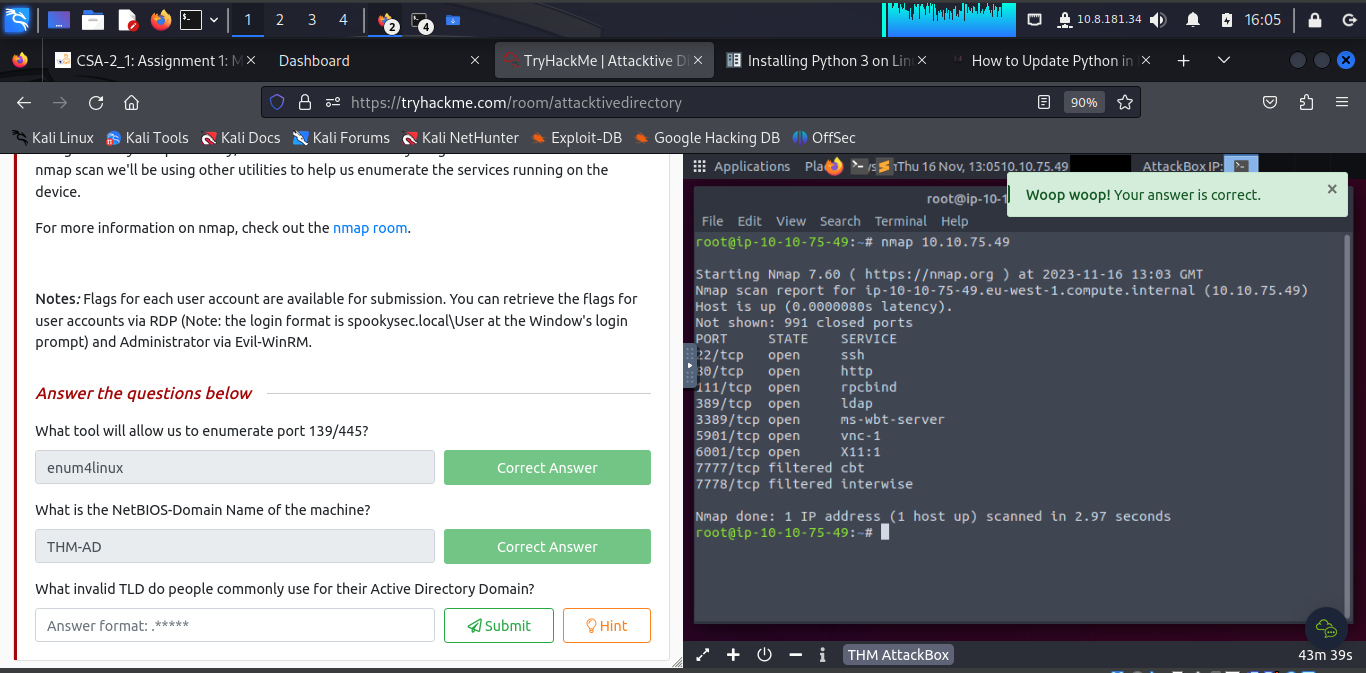
First, the learner will need to clone the Impacket Github repo onto your box. The following command will clone Impacket into /opt/impacket:

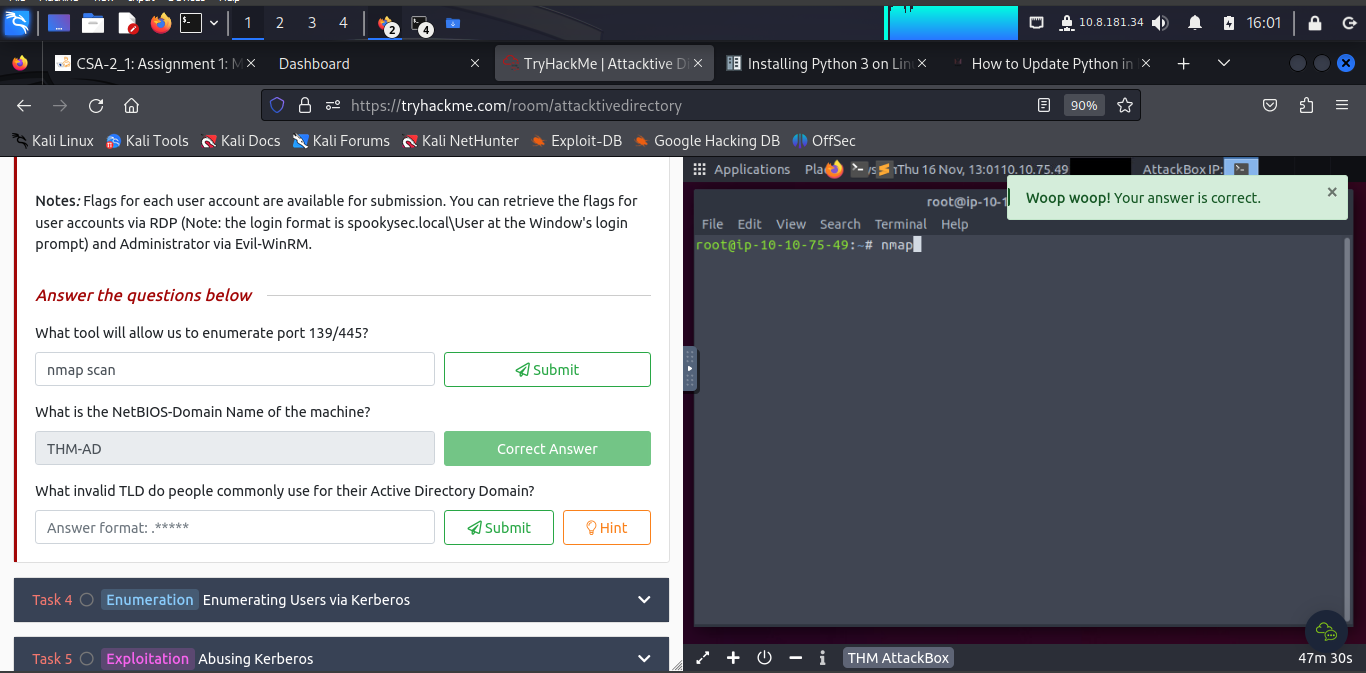
**git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket**

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

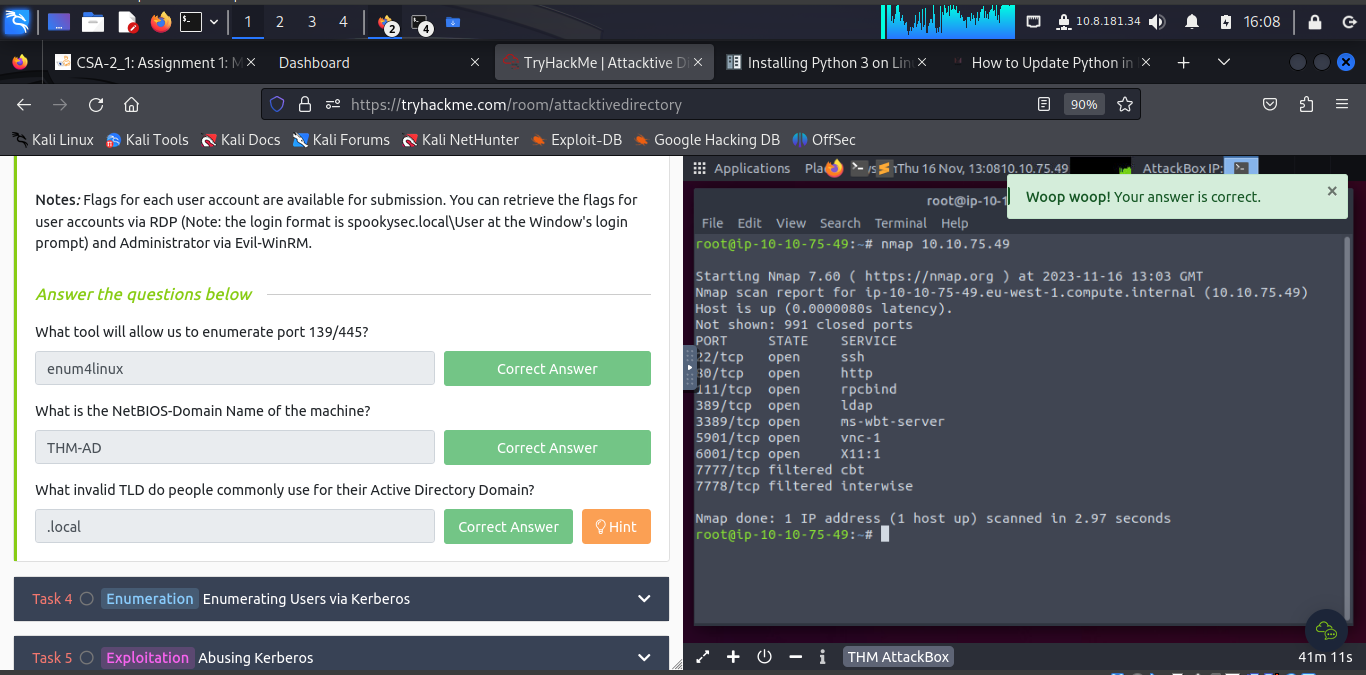
**Enumeration** Basic enumeration starts out with an **nmap scan**. Nmap is a relatively complex utility that has been refined over the years to detect what ports are open on a device, what services are running, and even detect what operating system is running. It's important to note that not all services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





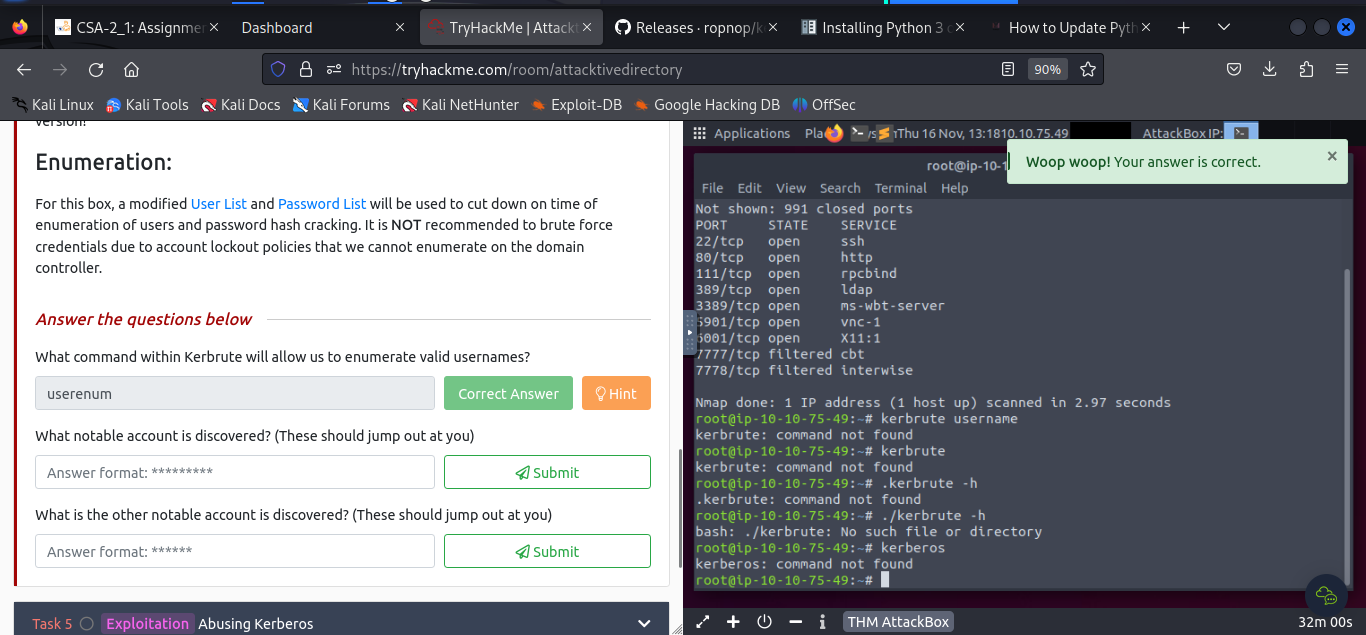
The invalid TLD people commonly use for their Active Directory Domain is **.local**.



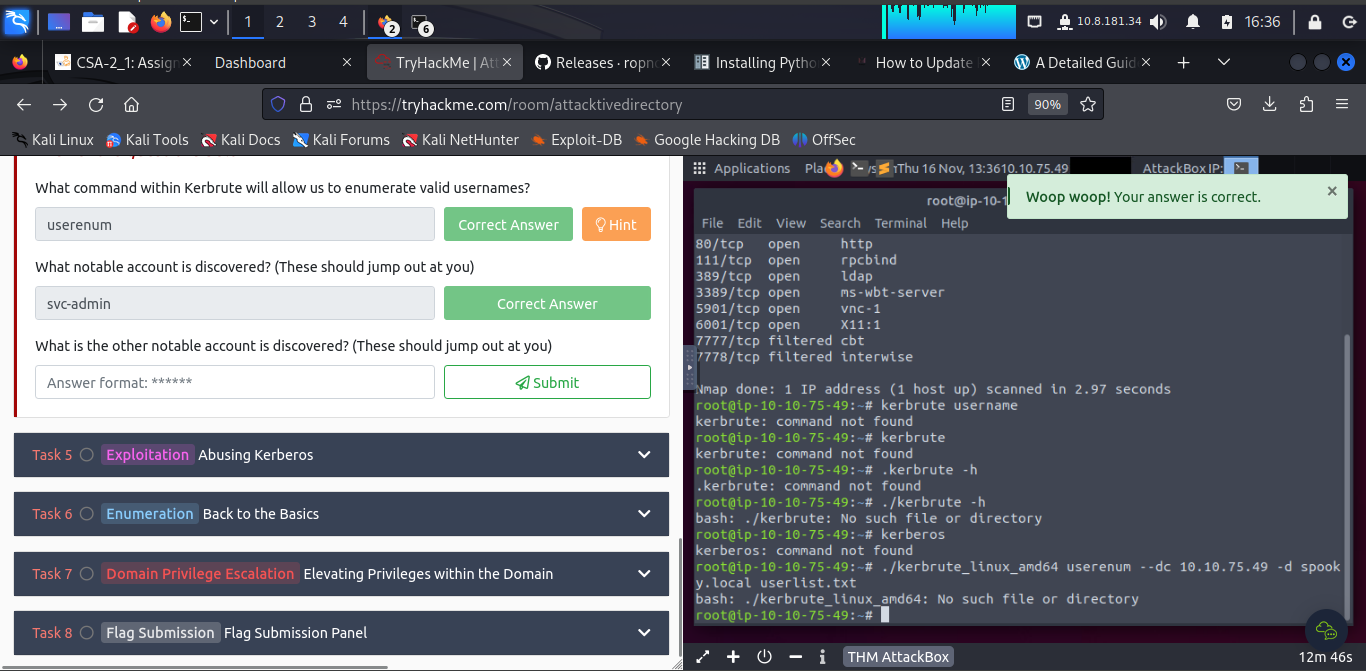
***Task 4: Enumerating Users via Kerberos***

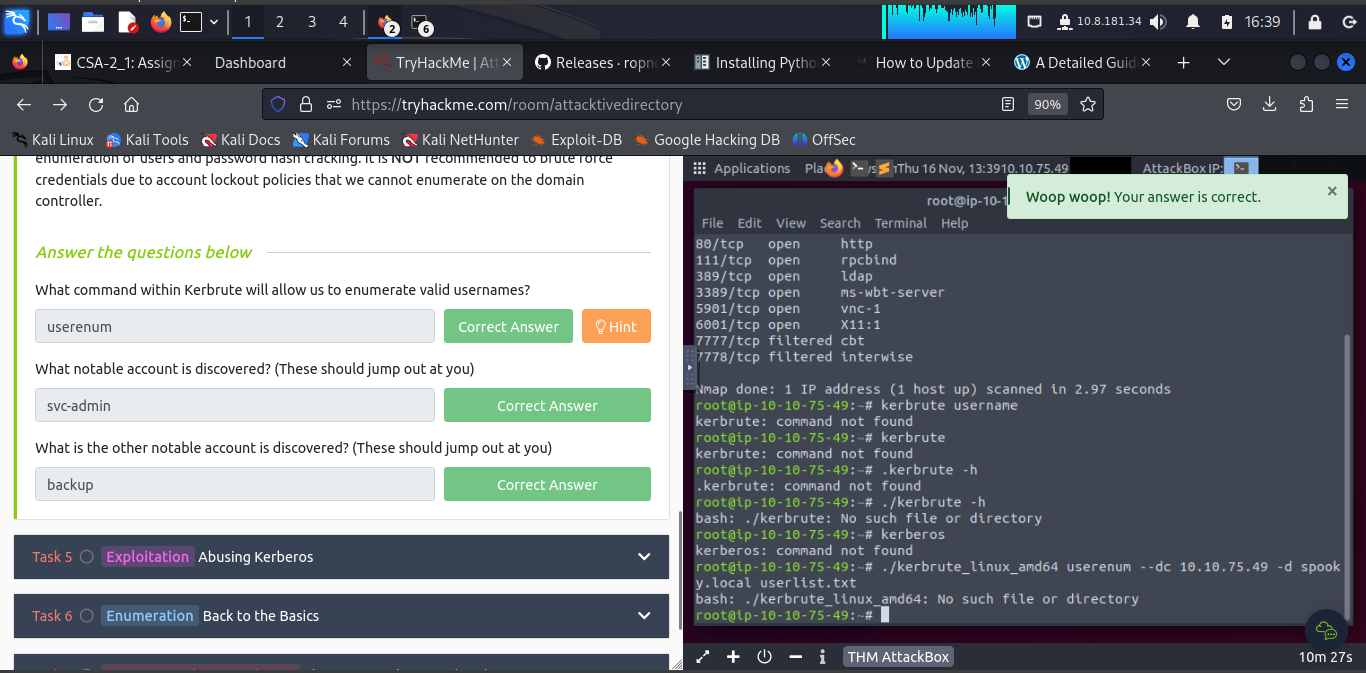
Kerberos is a key authentication service within Active Directory. With this port open, the learner can use a tool called **Kerbrute** (by Ronnie Flathers @ropnop) to brute force discovery of users, passwords and even password spray.

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

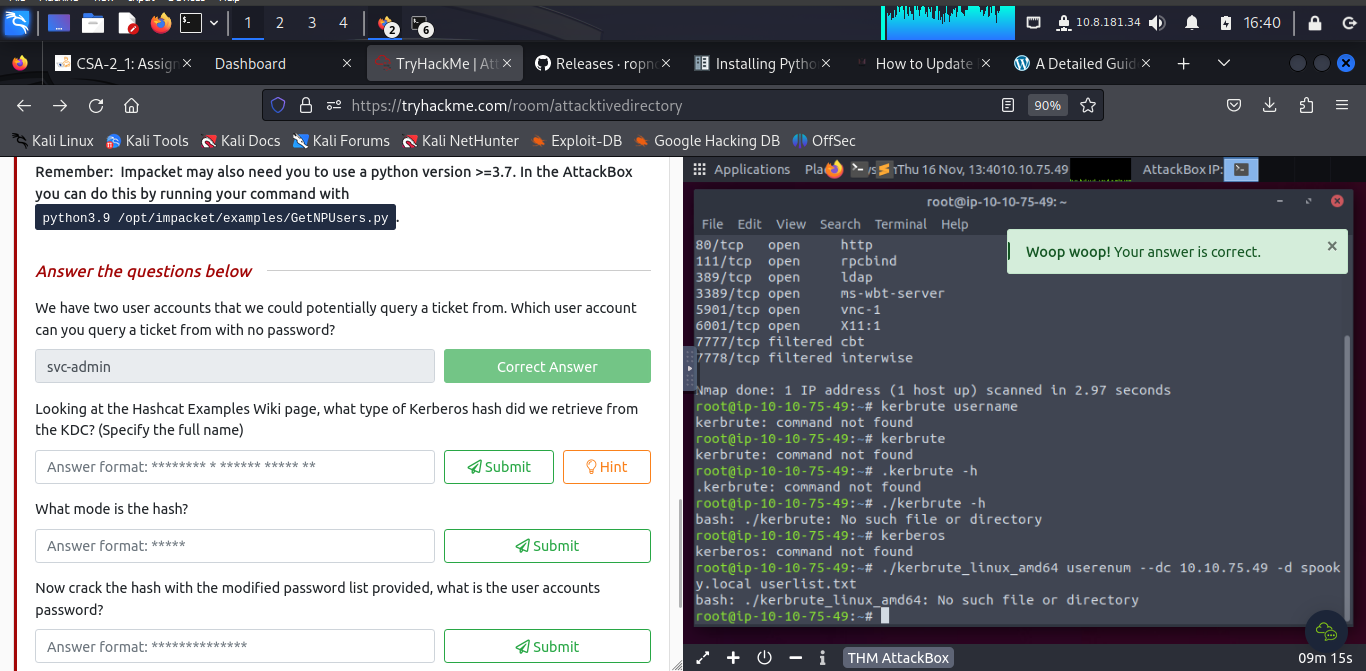


The learner downloaded **kerbrute\_linux\_amd64** and run the command **/kerbrute\_linux\_amd64 userenum --dc 10.10.75.49 -d spookysec.local userlist.txt**

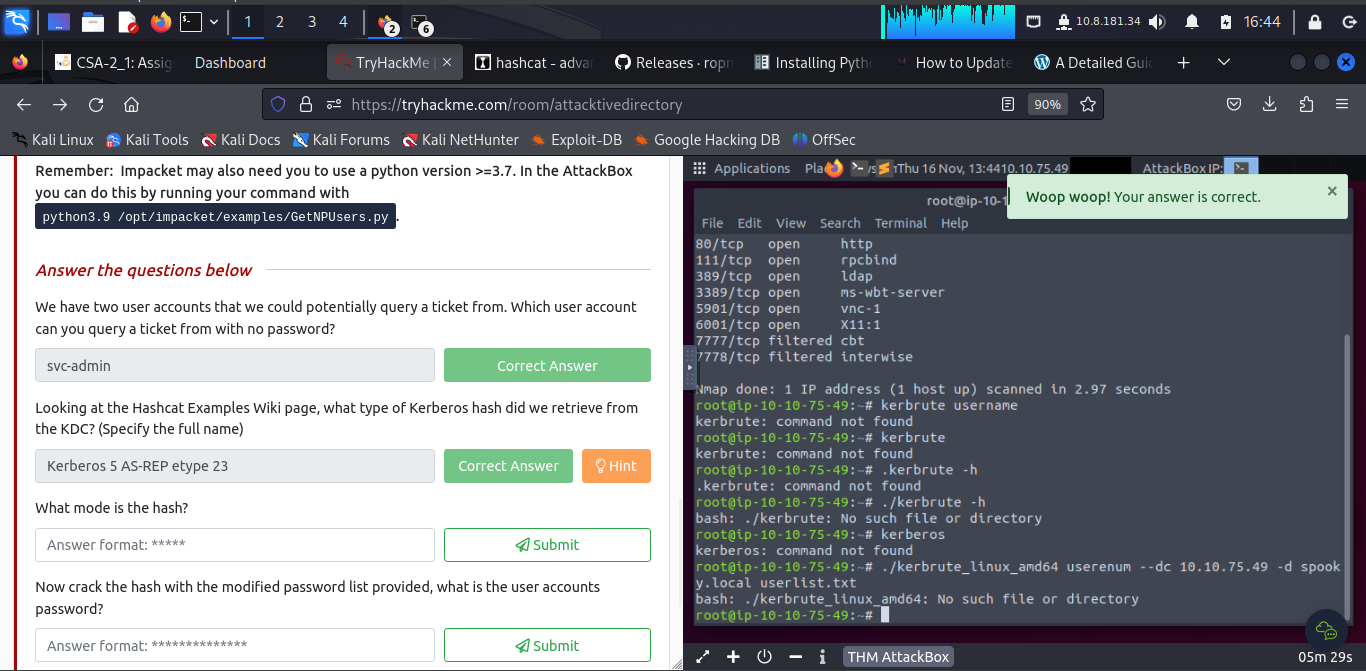


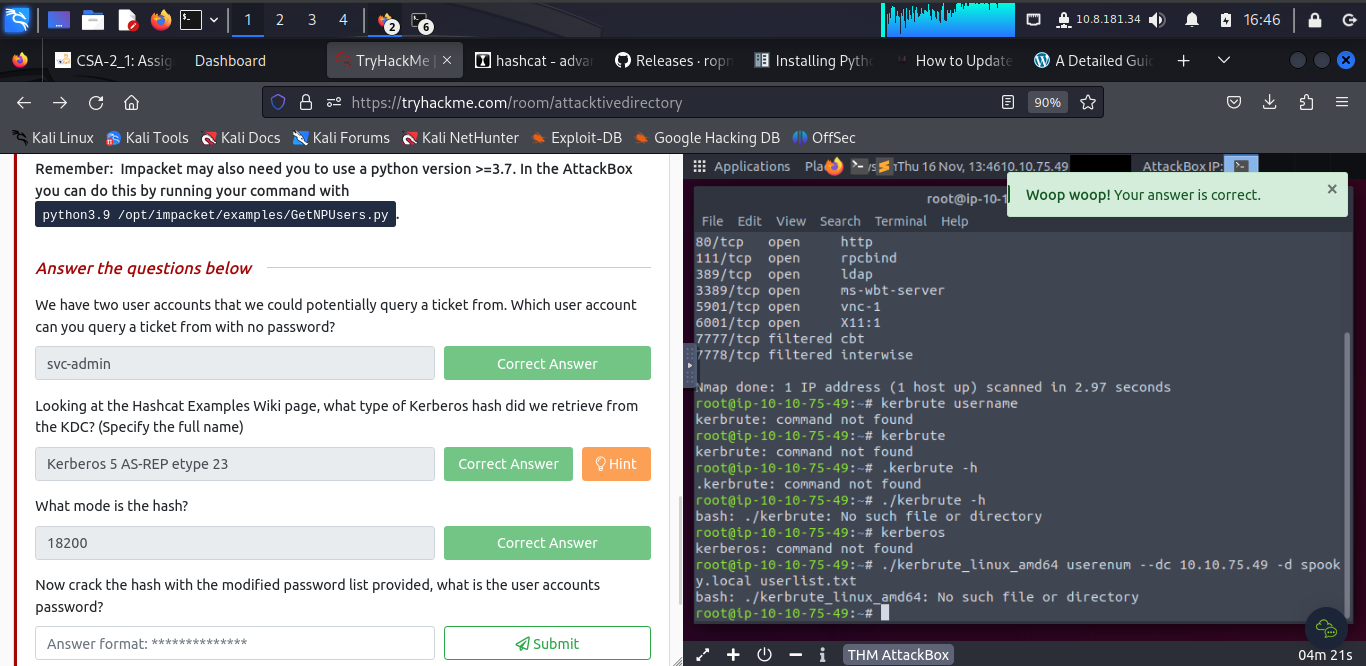


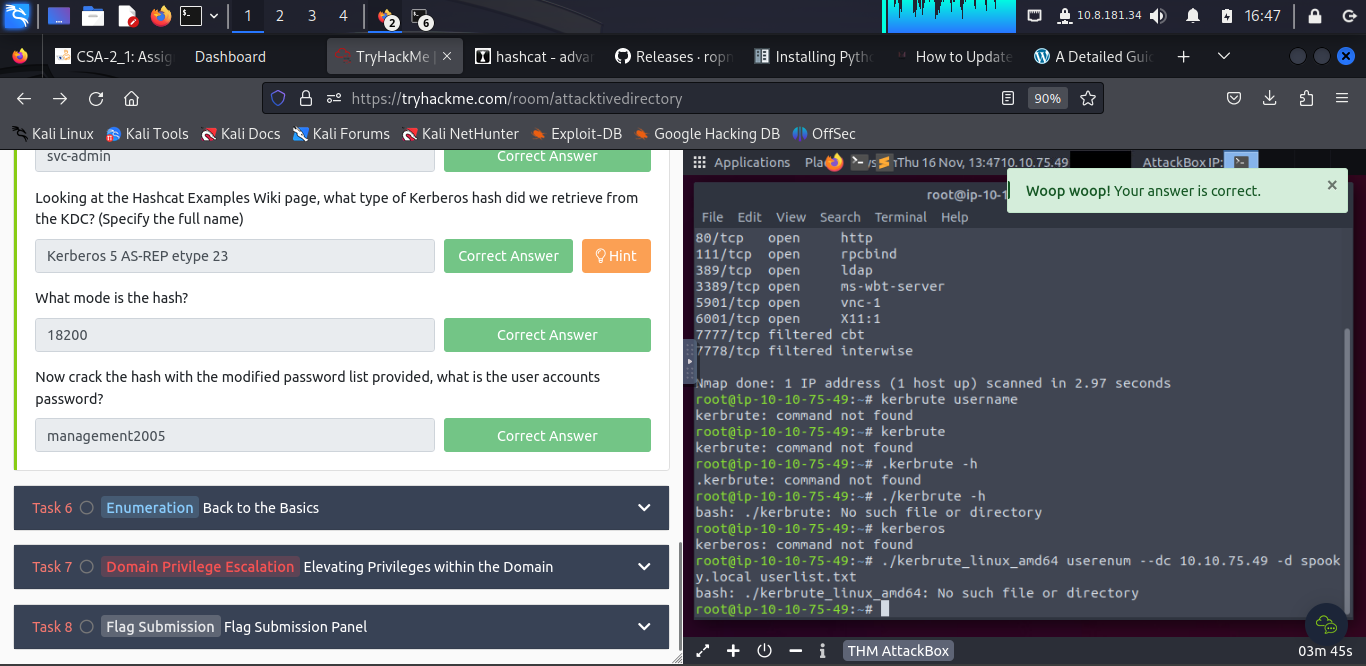
***Task 5: Abusing Kerberos***



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.



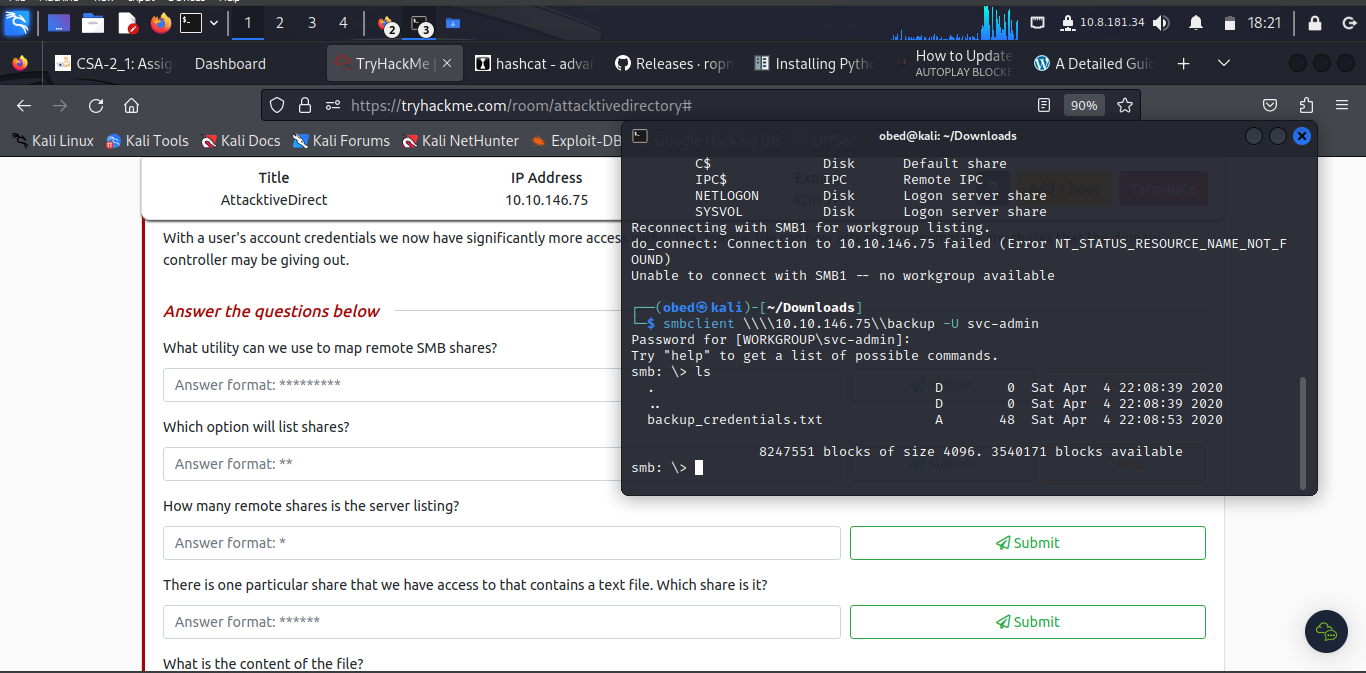


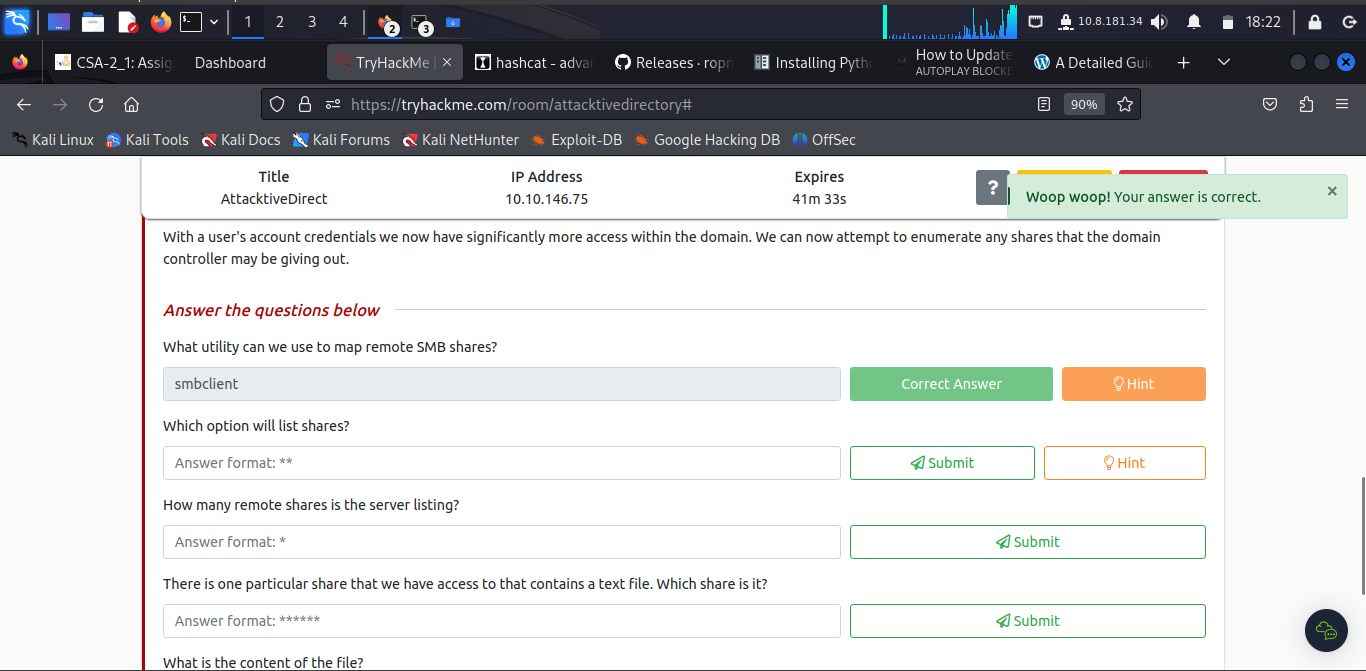


The learner run the following command **hashcat -m 18200 hash.txt passwordlist.txt**

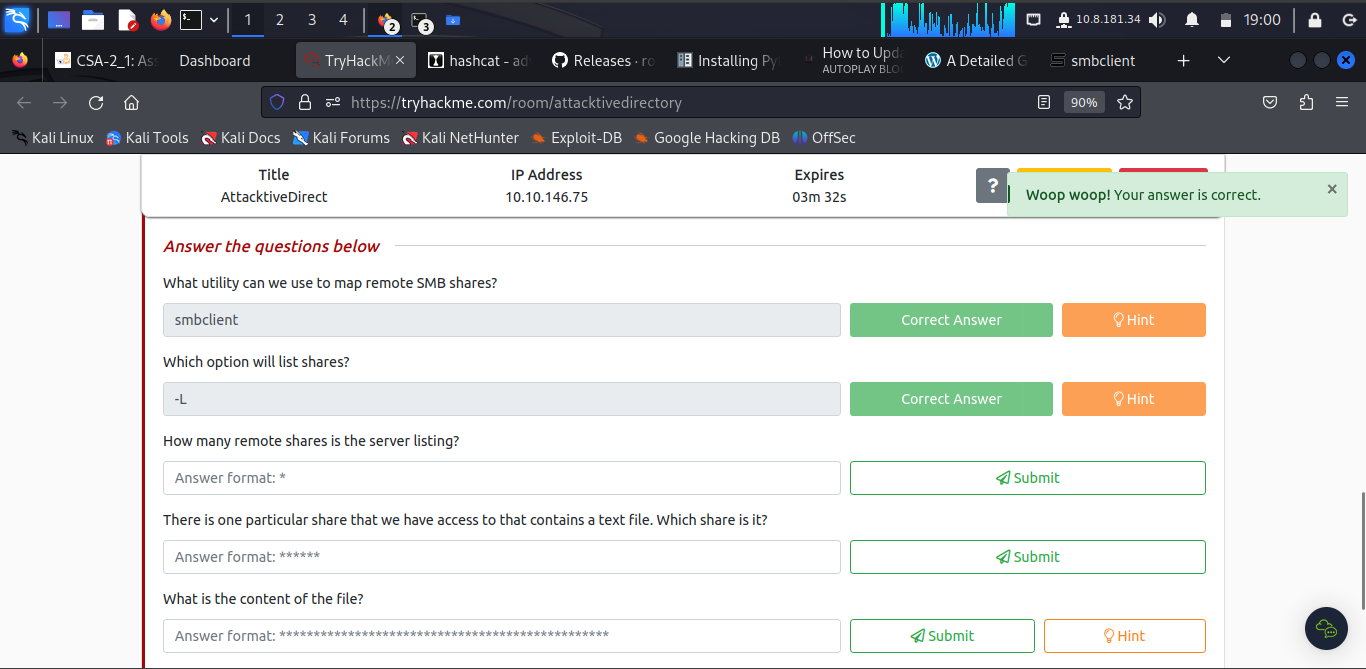
***Task 6: Back to the Basics***

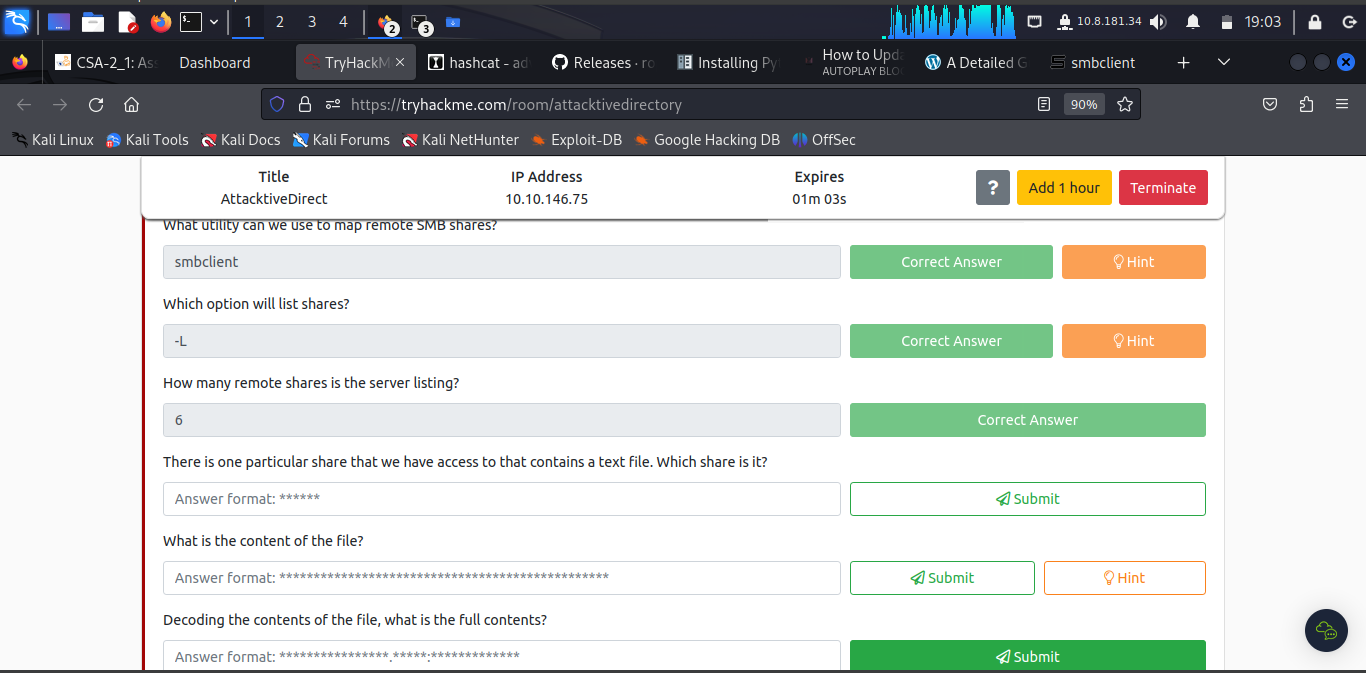
Connecting to the **smbclient**





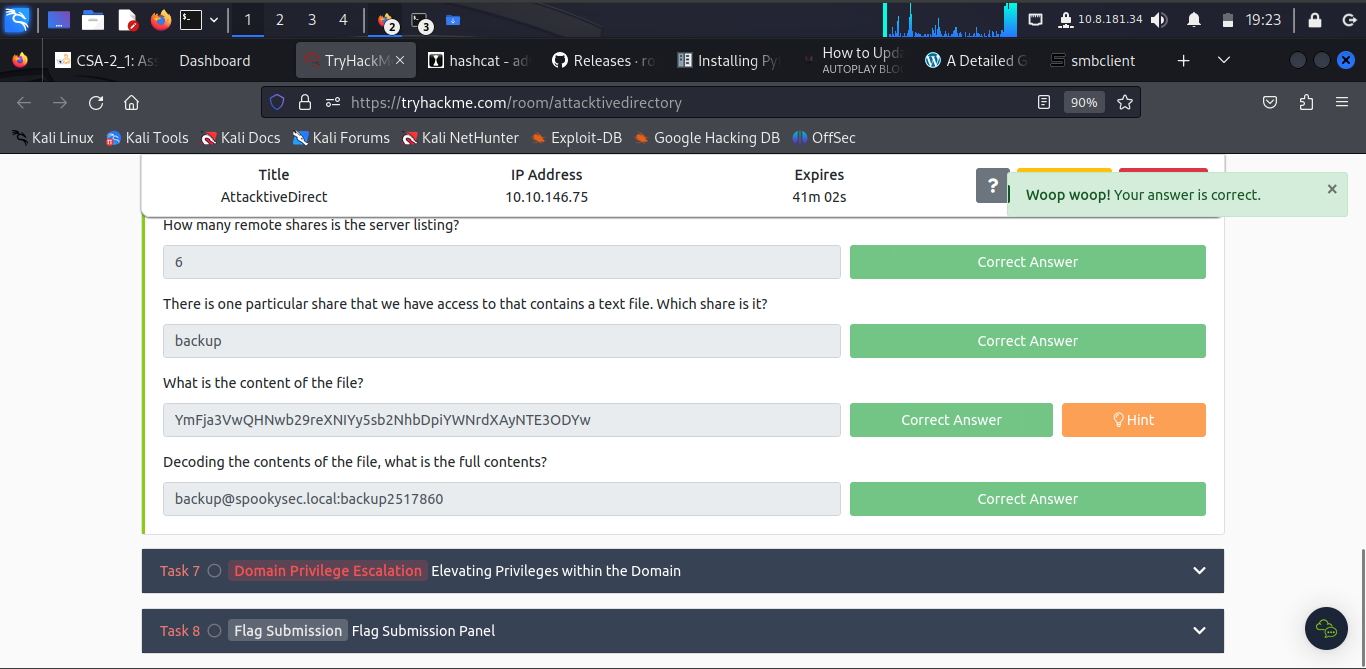
To get the option of list shares the learner has to use **-L**





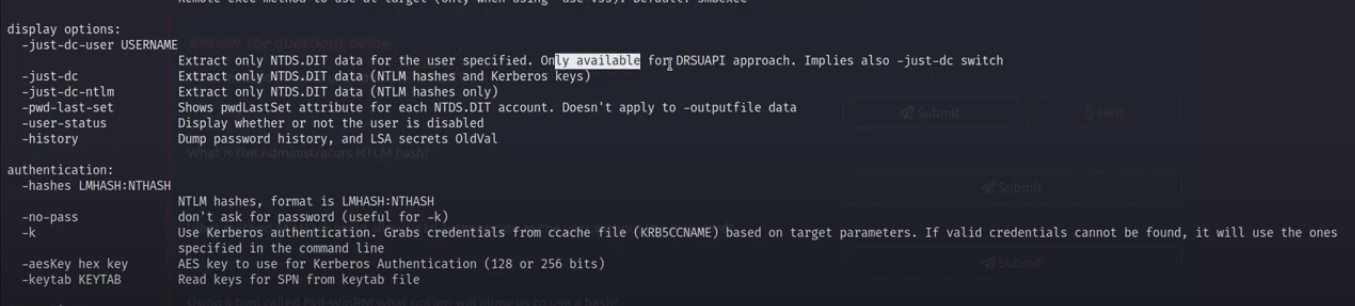


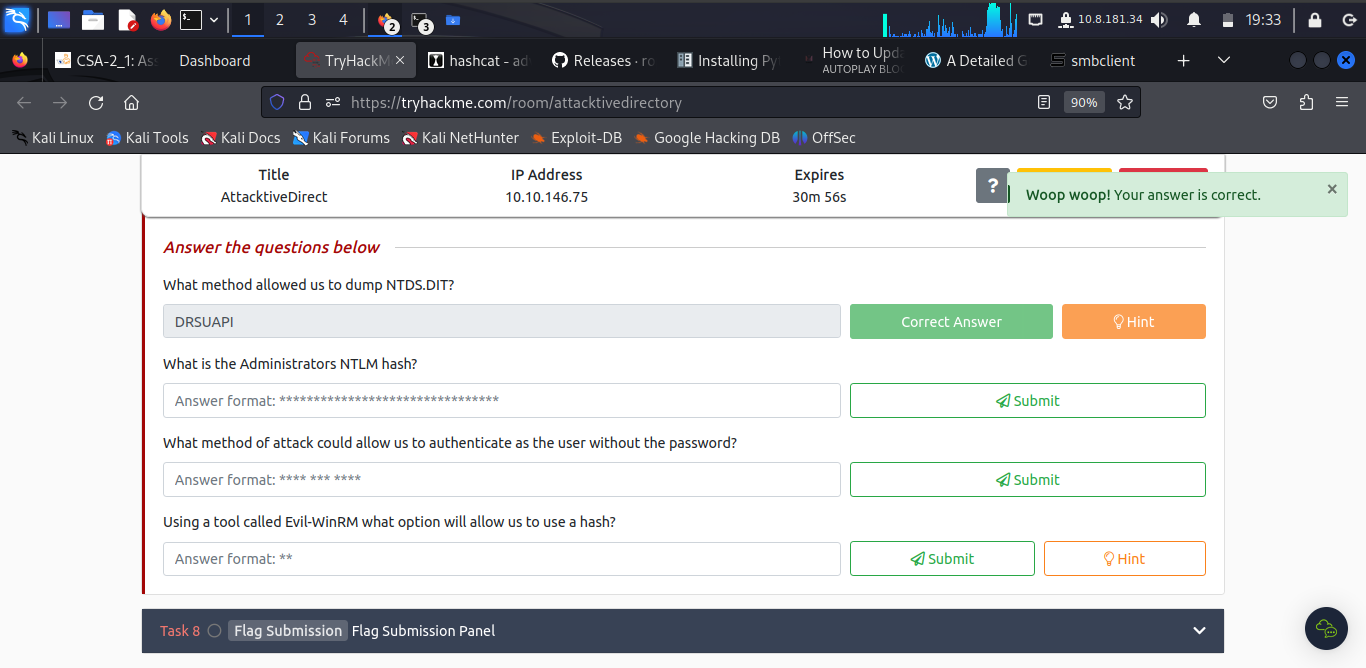
The learner ran the command **cat backup\_credentials.txt | xclip –sel clip**

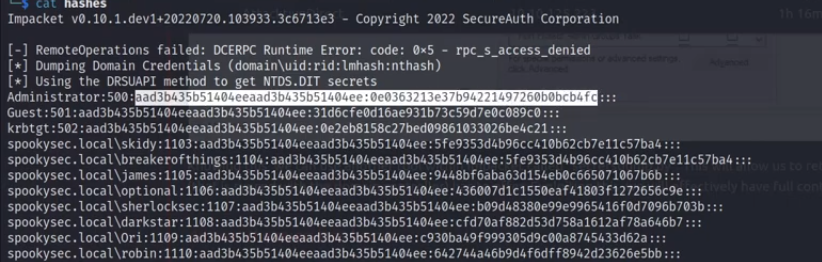


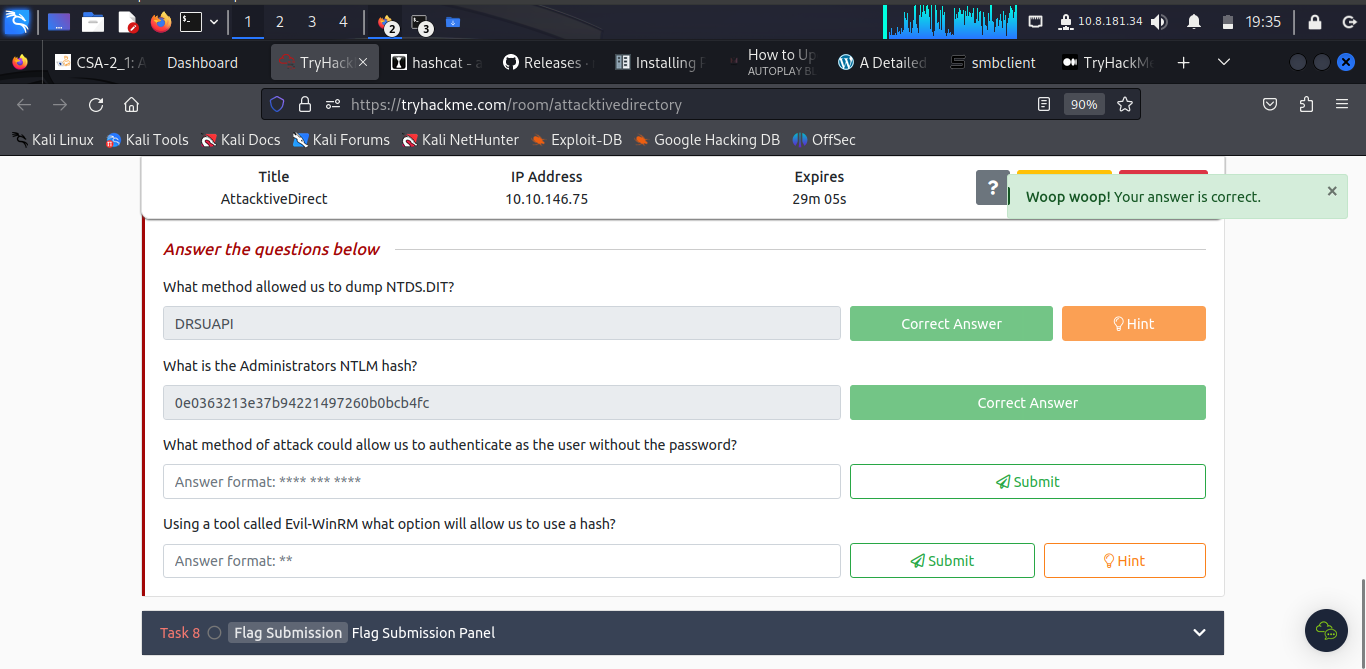
The learner ran the command **cat backup\_credentials.txt | base64 –d | xclip –sel clip**

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

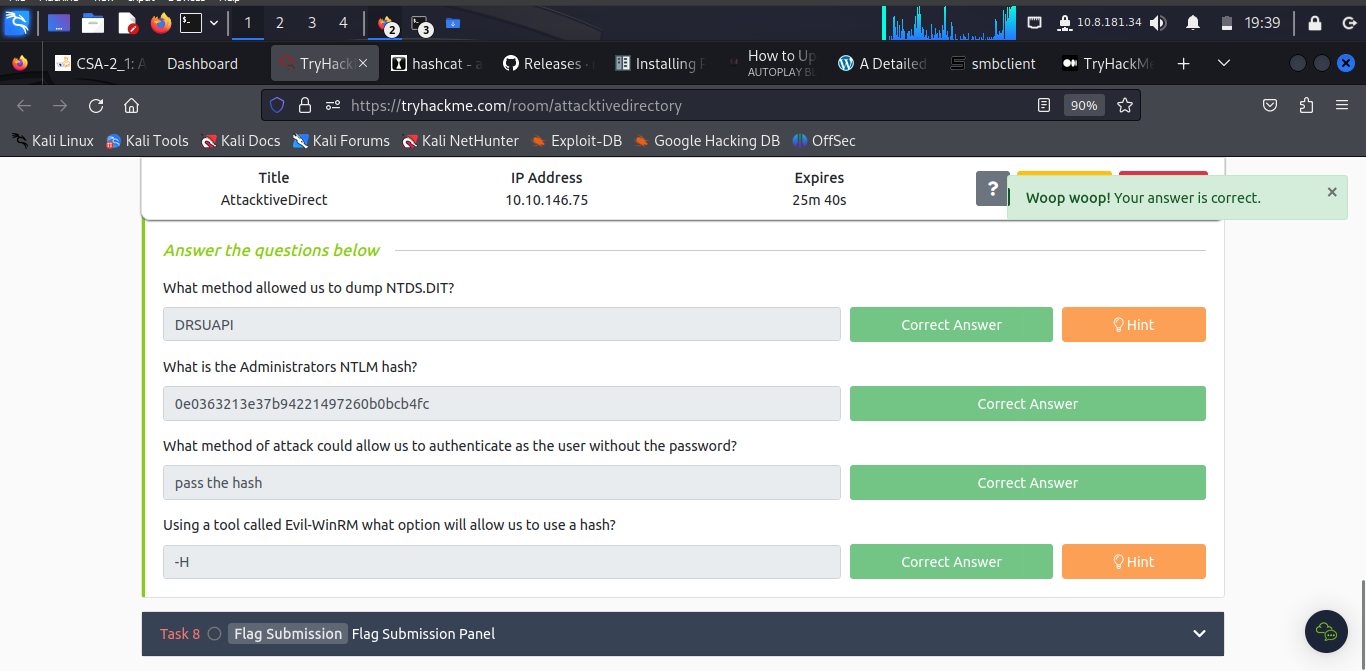






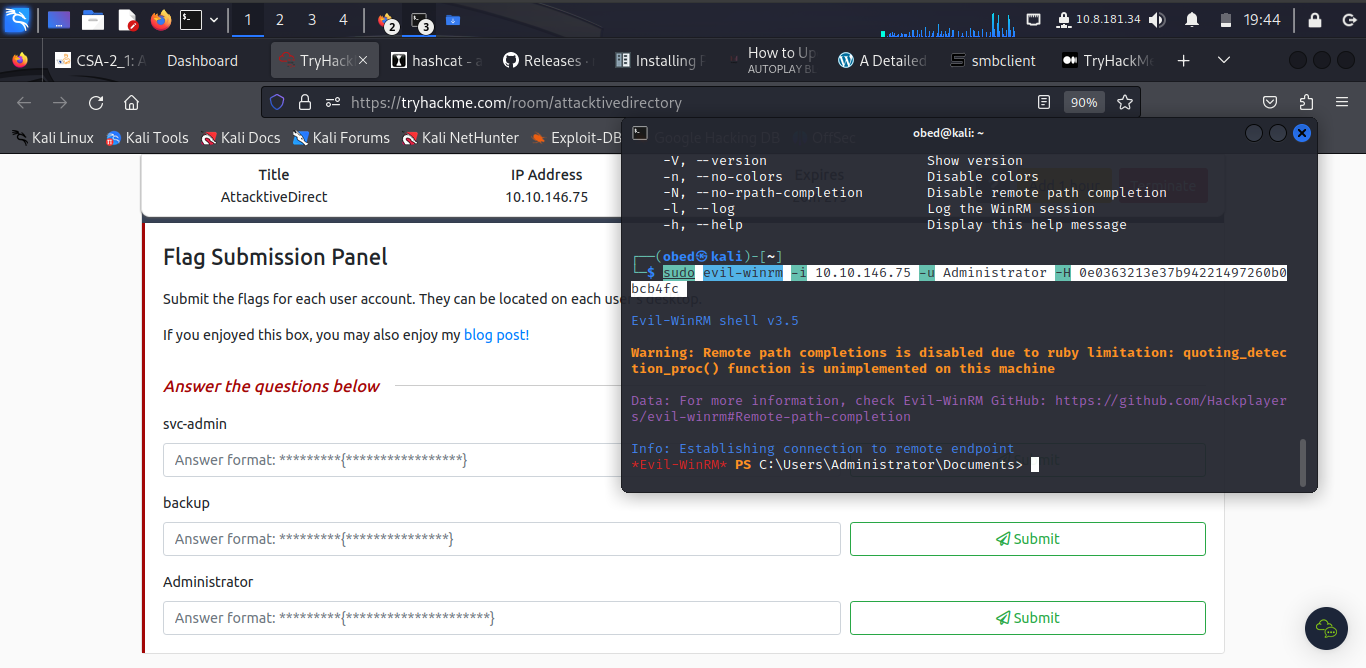




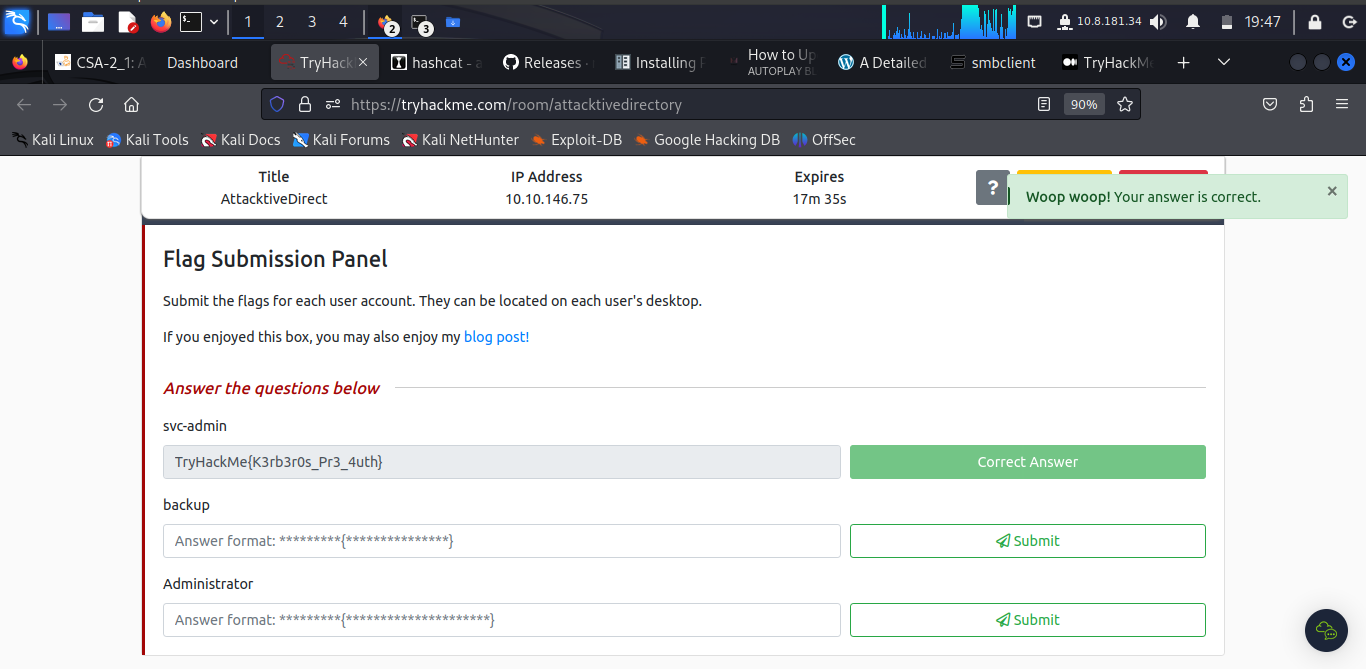


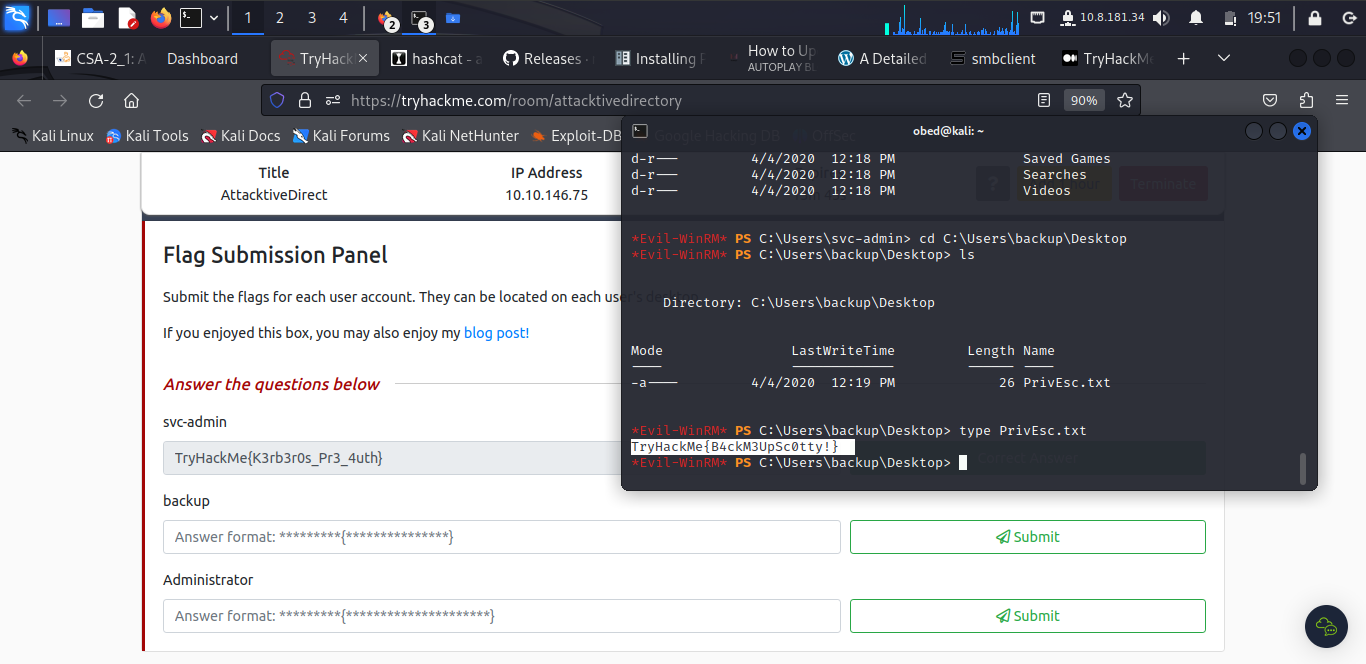
***Task 8: Flag Submission Panel***

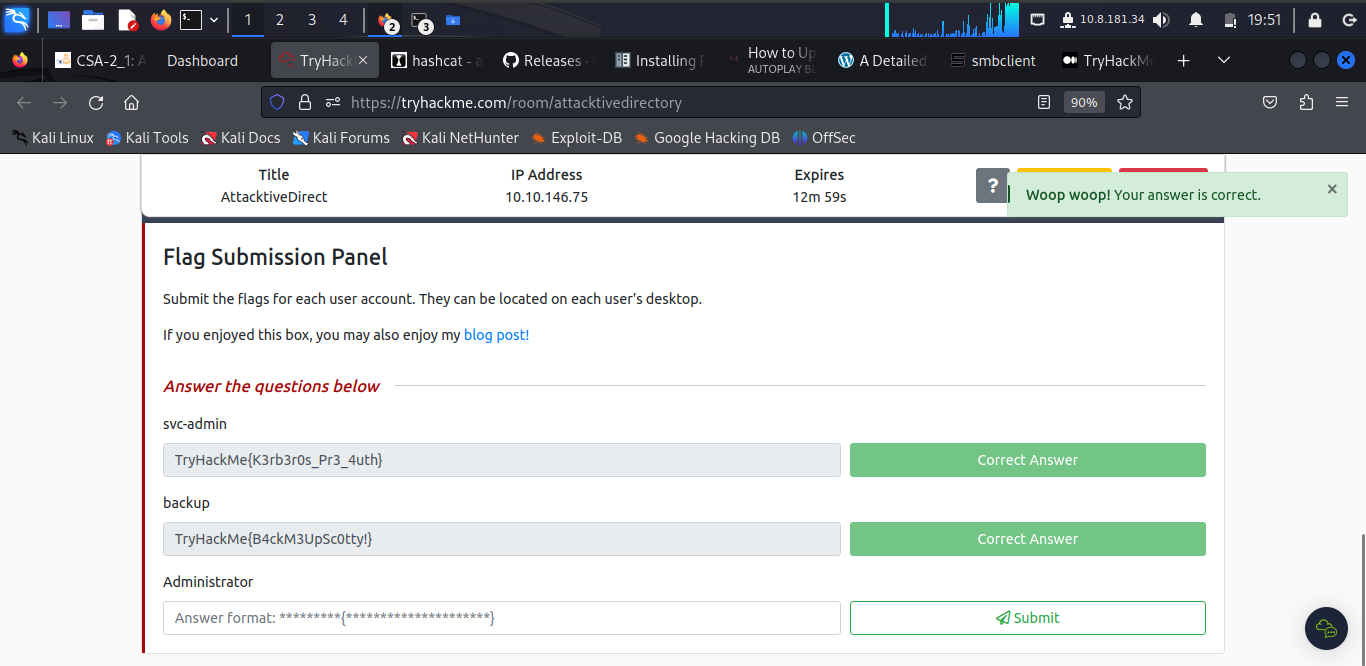
The learner ran the command to access ***sudo evil-winrm -i 10.10.146.75 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc***

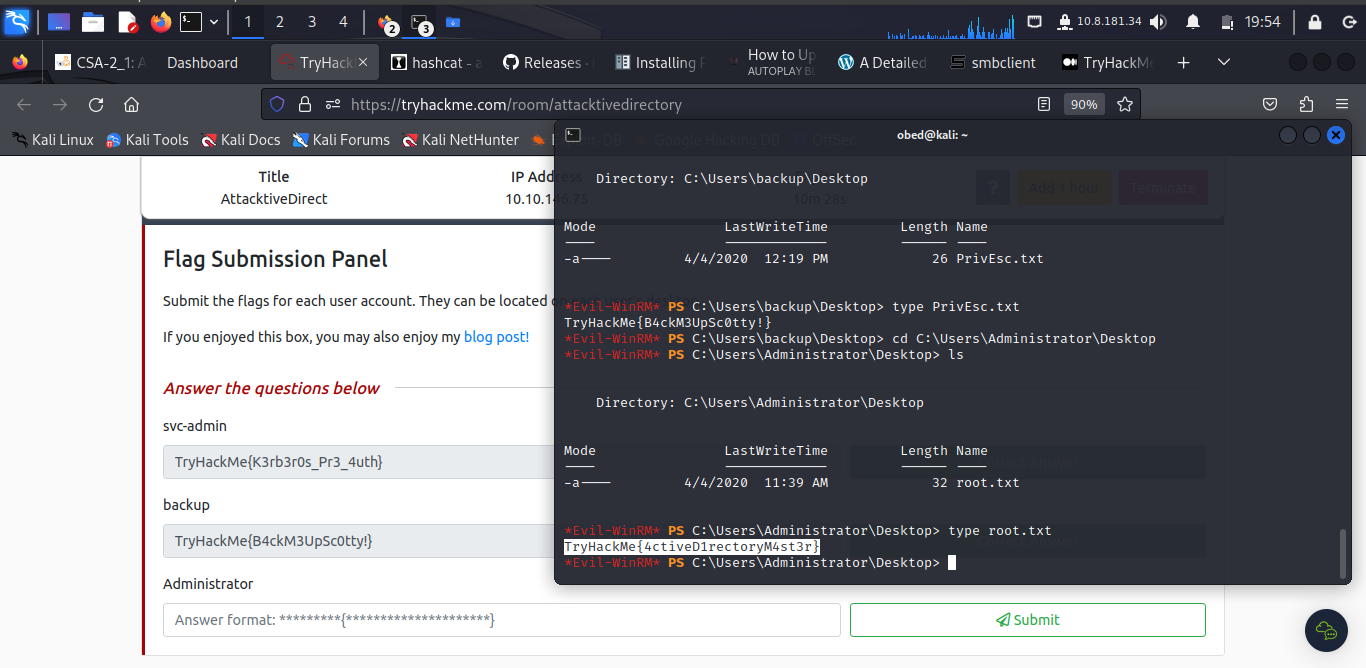


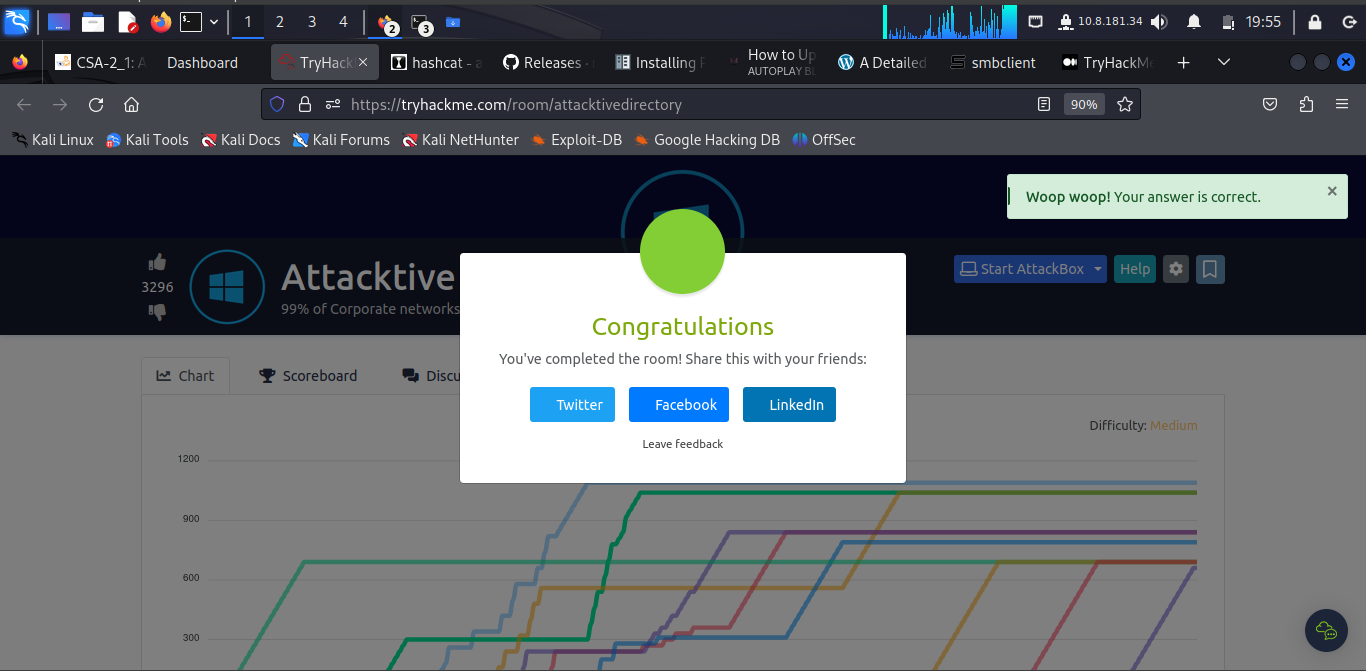












**Conclusion**

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