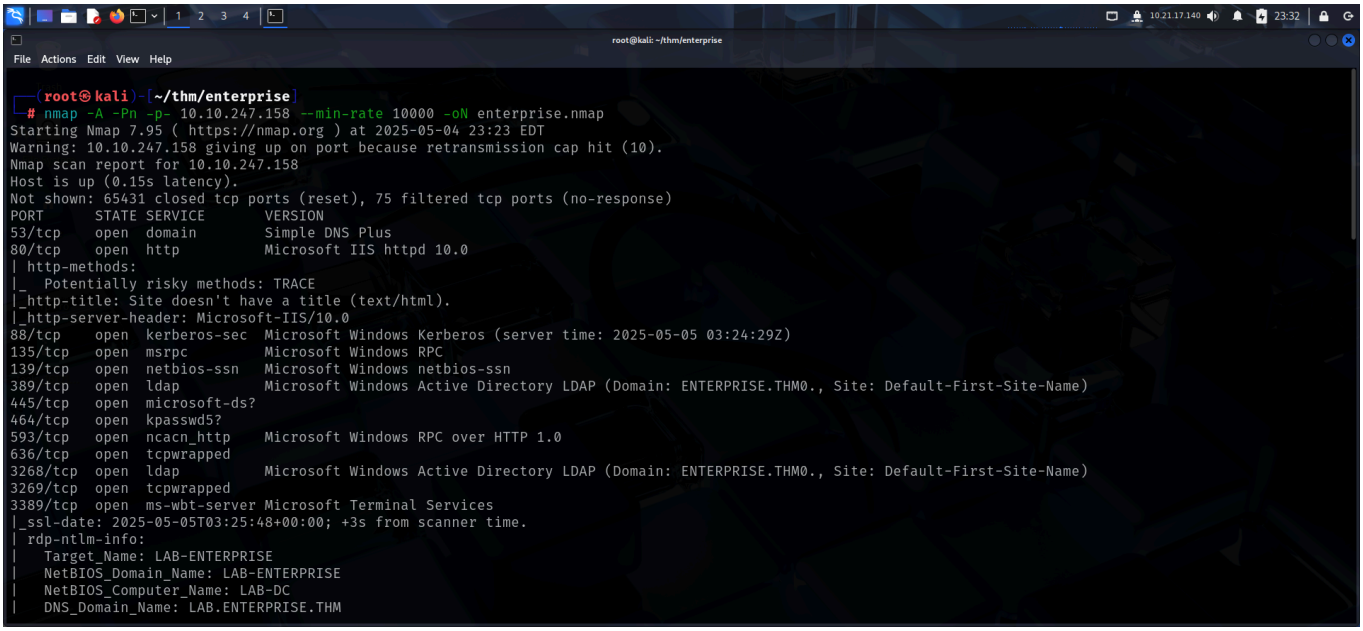
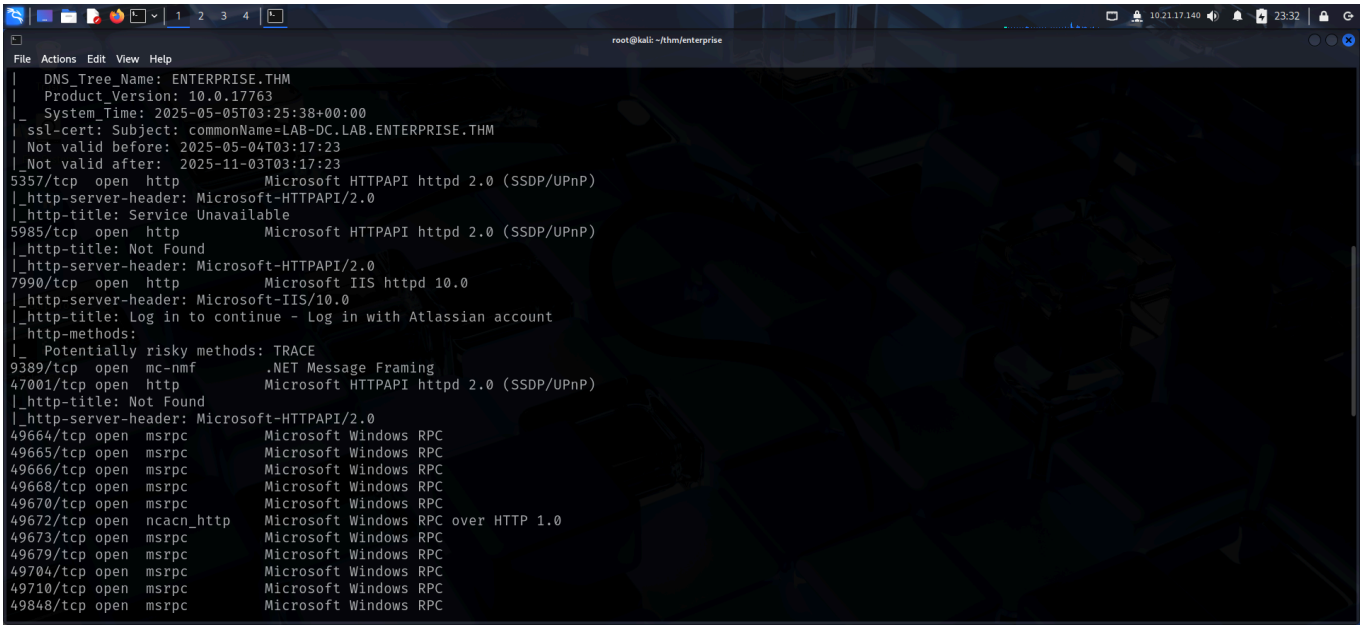
ENTERPRISE

To access the machine, click on the link given below:
https://tryhackme.com/room/enterprise

SCANNING

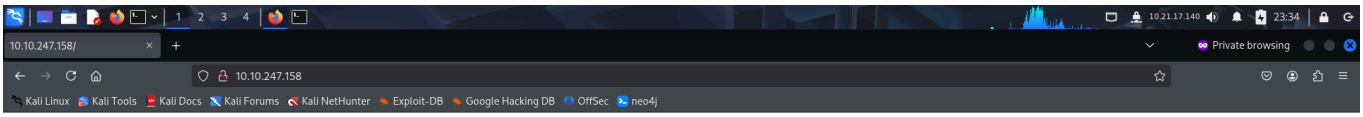
I performed an **nmap** aggressive scan on the target to find open ports and the services running on them.



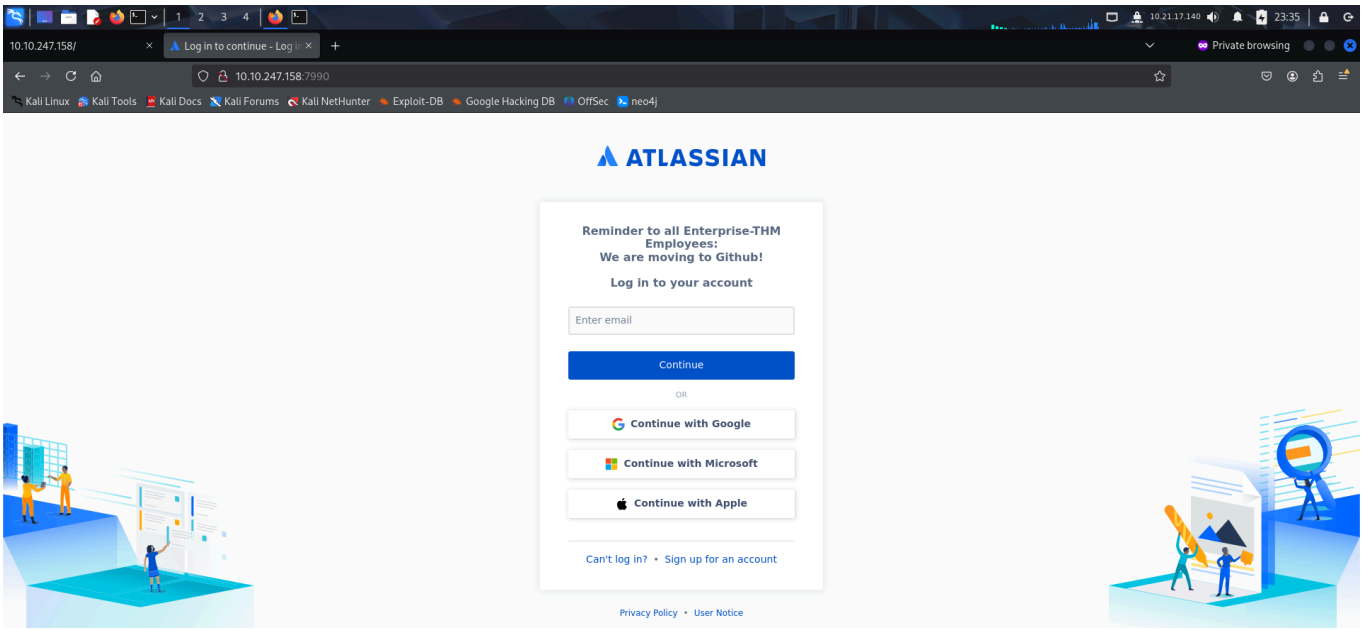


FOOTHOLD

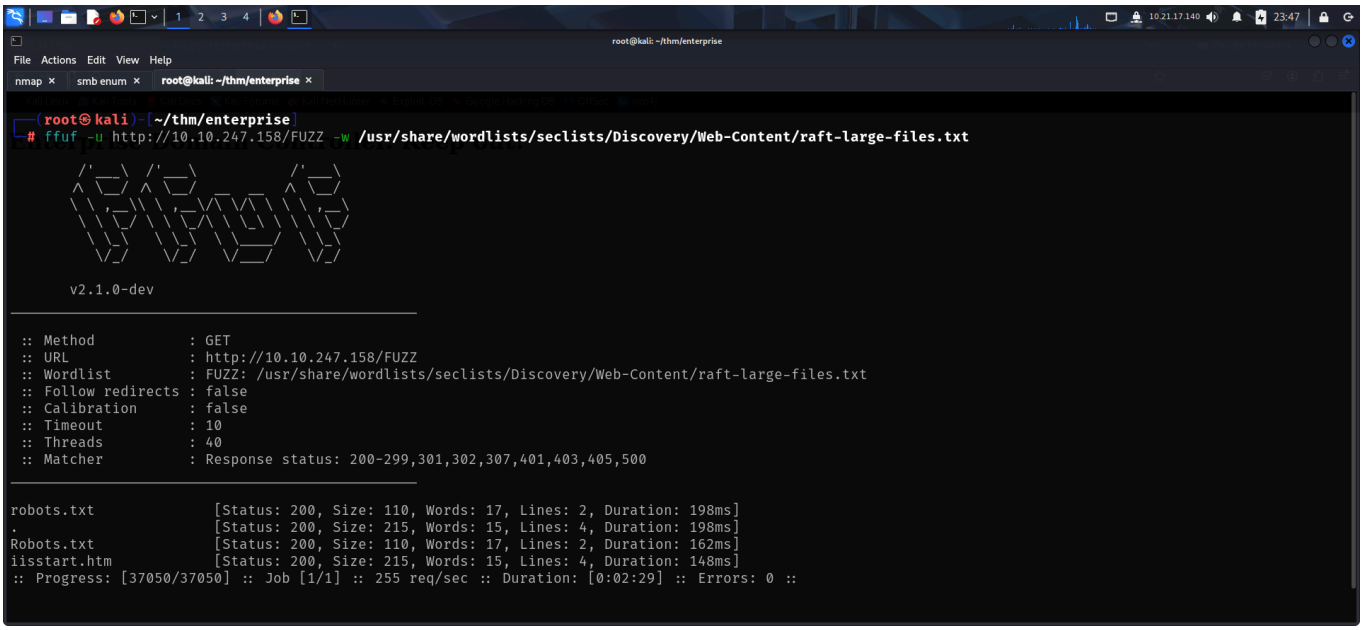
I accessed the web application running on port 80 and 7990.



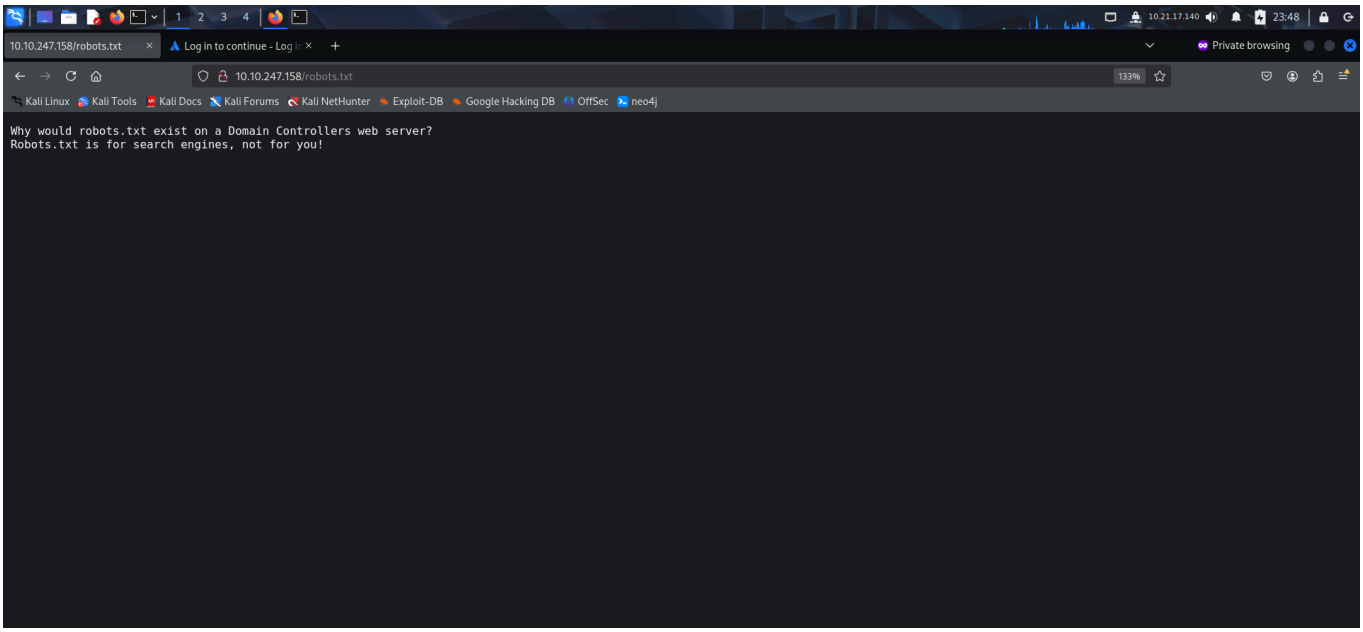
Enterprise Domain Controller. Keep out!



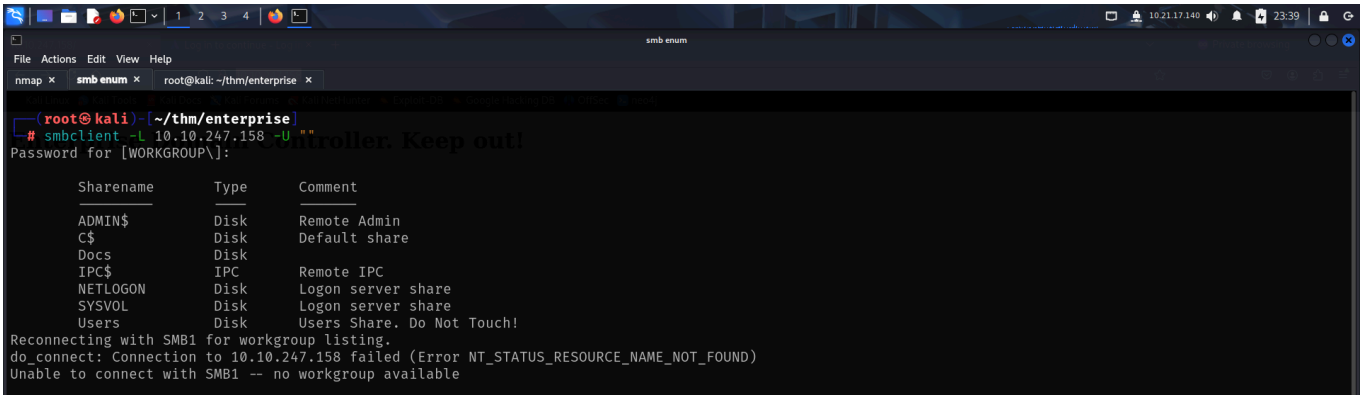
I fuzzed hidden files and found a *robots.txt* file on the domain controllers web app. This seemed wierd so I accessed it through my browser.



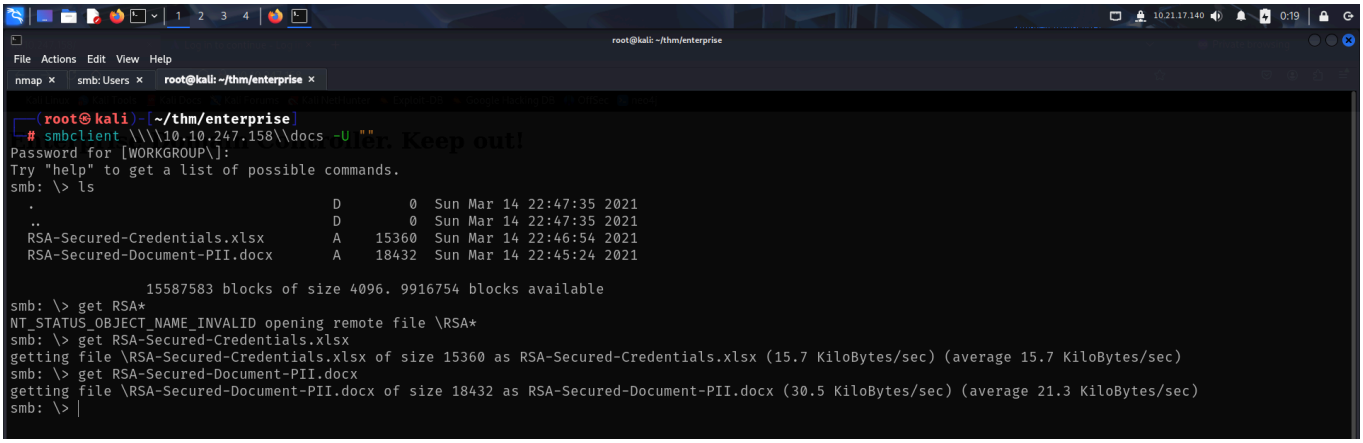
However, I did not get any useful information.



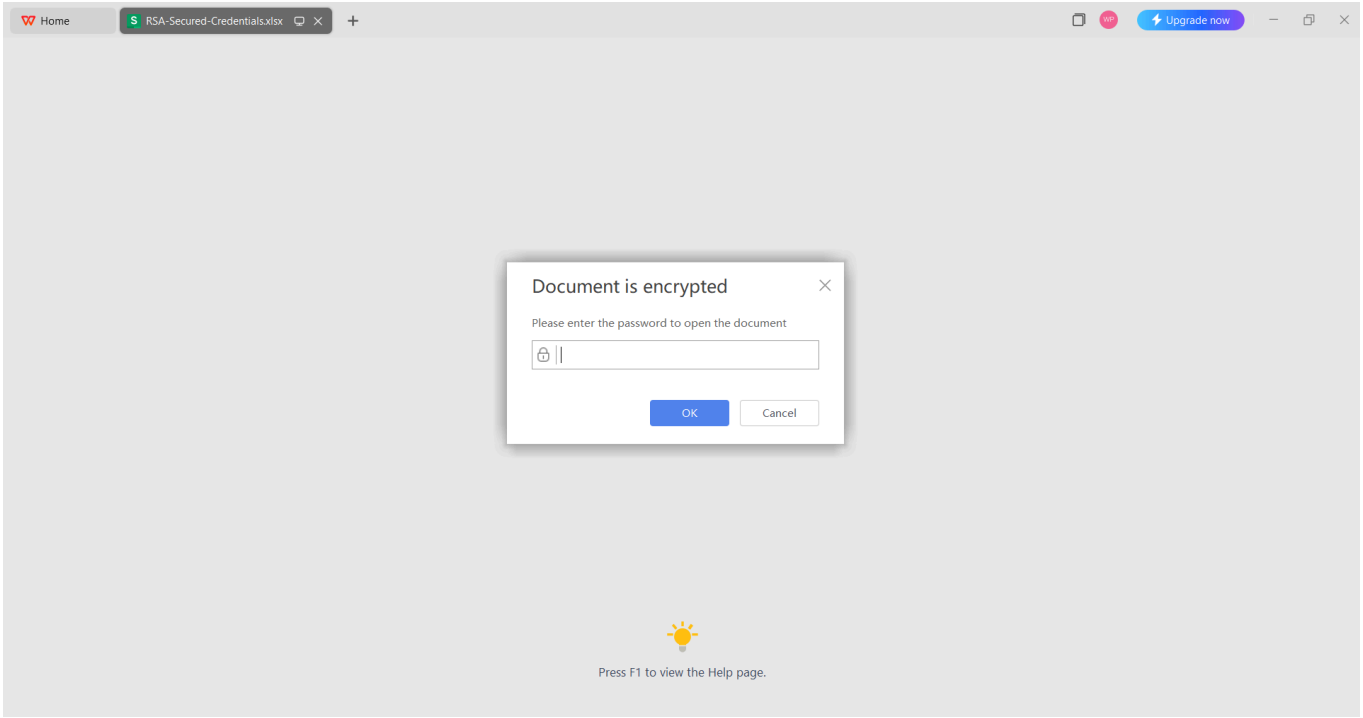
I then looked for smb shares using **smbclient**.

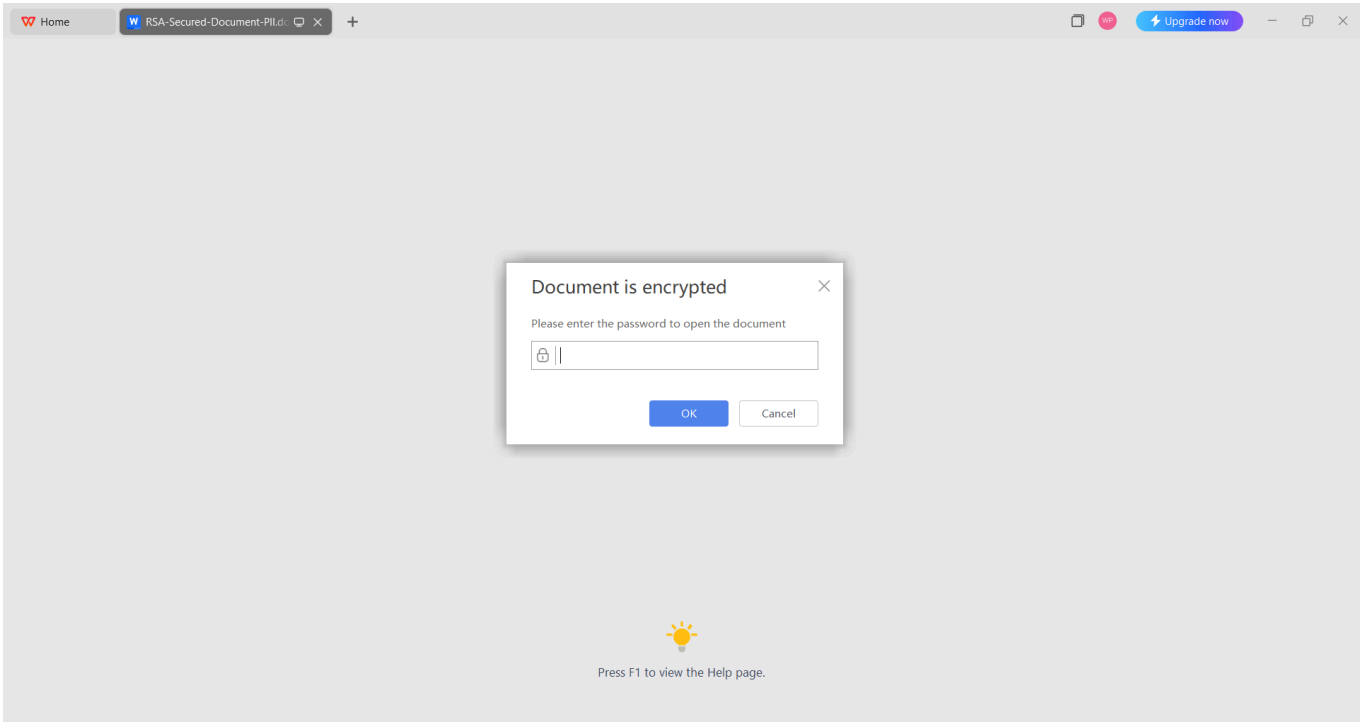


There were 2 interesting shares. So I first accessed the *docs* share and downloaded the files present in it.



Both the documents were password protected, so I couldn't open it.





I then accessed the *Users* share.

```
┌──(root㉿kali)-[~/thm/enterprise]
└─# smbclient \\\\10.10.247.158\\Users -U ""
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Thu Mar 11 21:11:49 2021
  ..                                  DR        0  Thu Mar 11 21:11:49 2021
  Administrator                        D        0  Thu Mar 11 16:55:48 2021
  All Users                        DHSrn        0  Sat Sep 15 03:28:48 2018
  atlbitbucket                         D        0  Thu Mar 11 17:53:06 2021
  bitbucket                            D        0  Thu Mar 11 21:11:51 2021
  Default                            DHR        0  Thu Mar 11 19:18:03 2021
  Default User                     DHSrn        0  Sat Sep 15 03:28:48 2018
  desktop.ini                        AHS      174  Sat Sep 15 03:16:48 2018
  LAB-ADMIN                            D        0  Thu Mar 11 19:28:14 2021
  Public                              DR        0  Thu Mar 11 16:27:02 2021

                15587583 blocks of size 4096. 9927105 blocks available
smb: \>
```

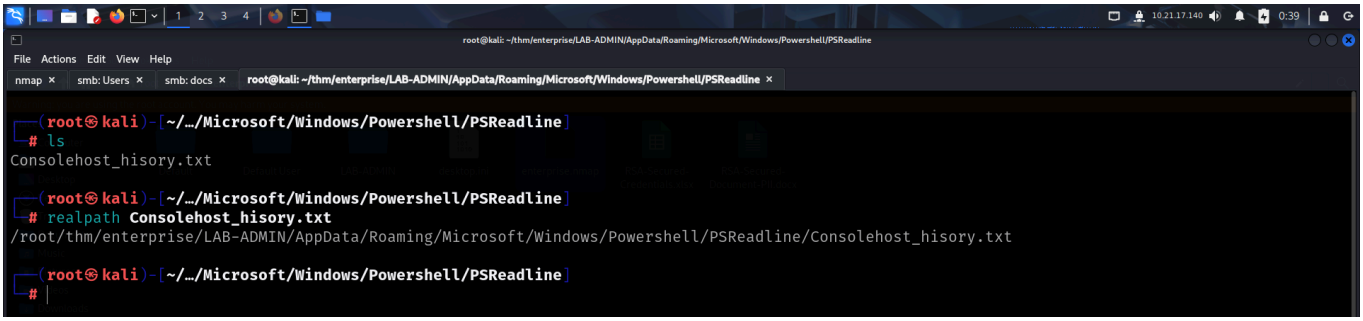
It had a bunch of files so I downloaded everything.

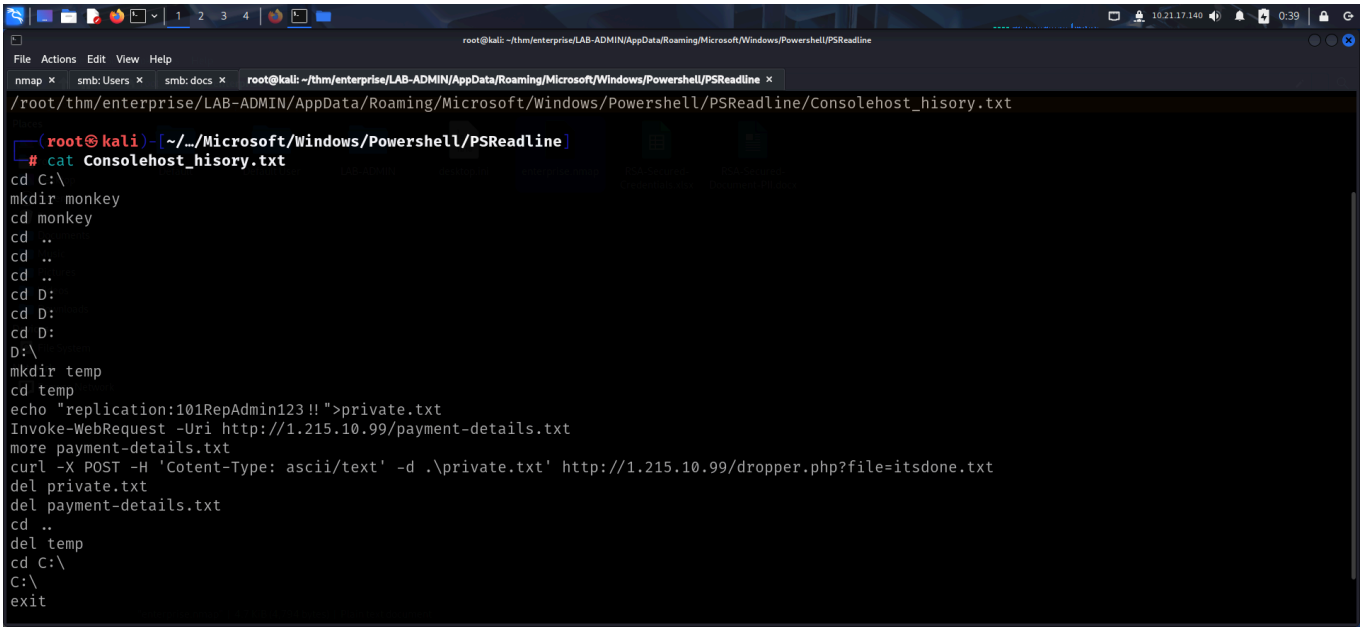
```
┌──(root㉿kali)-[~/thm/enterprise]
└─# smbclient \\\\10.10.247.158\\Users -U ""
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \desktop.ini of size 174 as desktop.ini (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
NT_STATUS_ACCESS_DENIED listing \Administrator\*
NT_STATUS_STOPPED_ON_SYMLINK listing \All Users\*
NT_STATUS_ACCESS_DENIED listing \atlbitbucket\*
NT_STATUS_ACCESS_DENIED listing \bitbucket\*
NT_STATUS_ACCESS_DENIED opening remote file \Default\NTUSER.DAT
NT_STATUS_ACCESS_DENIED opening remote file \Default\NTUSER.DAT.LOG1
NT_STATUS_ACCESS_DENIED opening remote file \Default\NTUSER.DAT.LOG2
NT_STATUS_ACCESS_DENIED opening remote file \Default\NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TM.blf
NT_STATUS_ACCESS_DENIED opening remote file \Default\NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer00000000000000000001.regtrans-ms
NT_STATUS_ACCESS_DENIED opening remote file \Default\NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer00000000000000000002.regtrans-ms
NT_STATUS_ACCESS_DENIED listing \Default User\*
NT_STATUS_ACCESS_DENIED listing \Public\*
NT_STATUS_ACCESS_DENIED listing \Default\Application Data\*
NT_STATUS_ACCESS_DENIED listing \Default\Cookies\*
NT_STATUS_ACCESS_DENIED listing \Default\Local Settings\*
NT_STATUS_ACCESS_DENIED listing \Default\My Documents\*
NT_STATUS_ACCESS_DENIED listing \Default\NetHood\*
NT_STATUS_ACCESS_DENIED listing \Default\PrintHood\*
NT_STATUS_ACCESS_DENIED listing \Default\Recent\*
NT_STATUS_ACCESS_DENIED listing \Default\SendTo\*
NT_STATUS_ACCESS_DENIED listing \Default\Start Menu\*
```

I used the `find` command to look for files containing words like `history` or `secret` or something similar in their name and examined them.

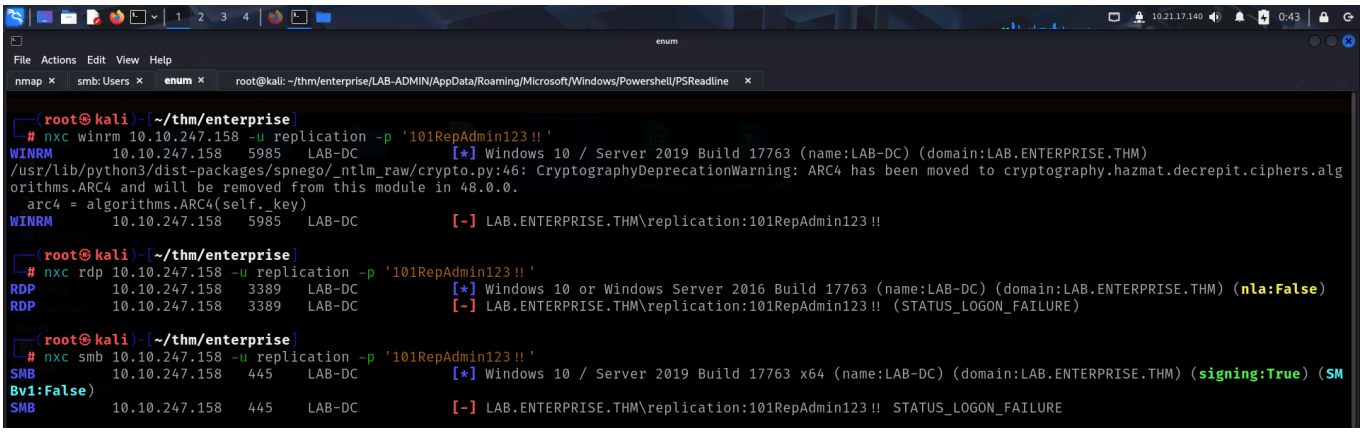
```
find /root/thm/enterprise/APPADMIN/ -type f -name "*history*"
```

I found a credential inside a file called `Consolehost_history.txt`.

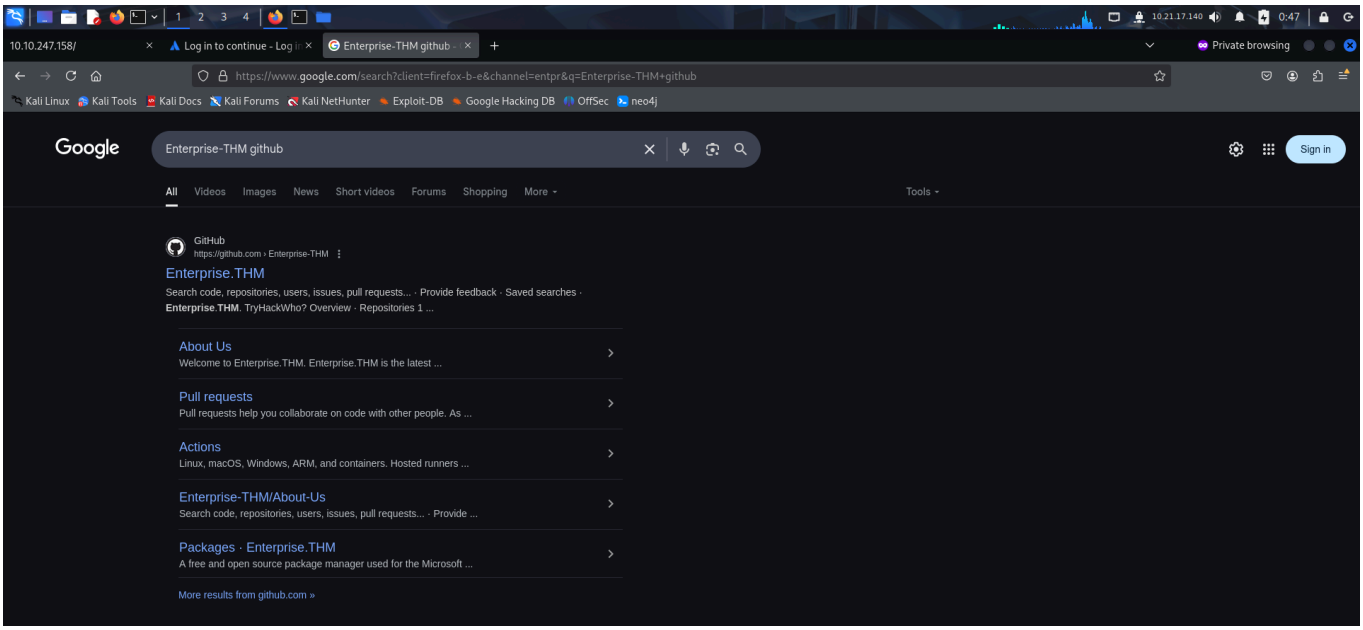




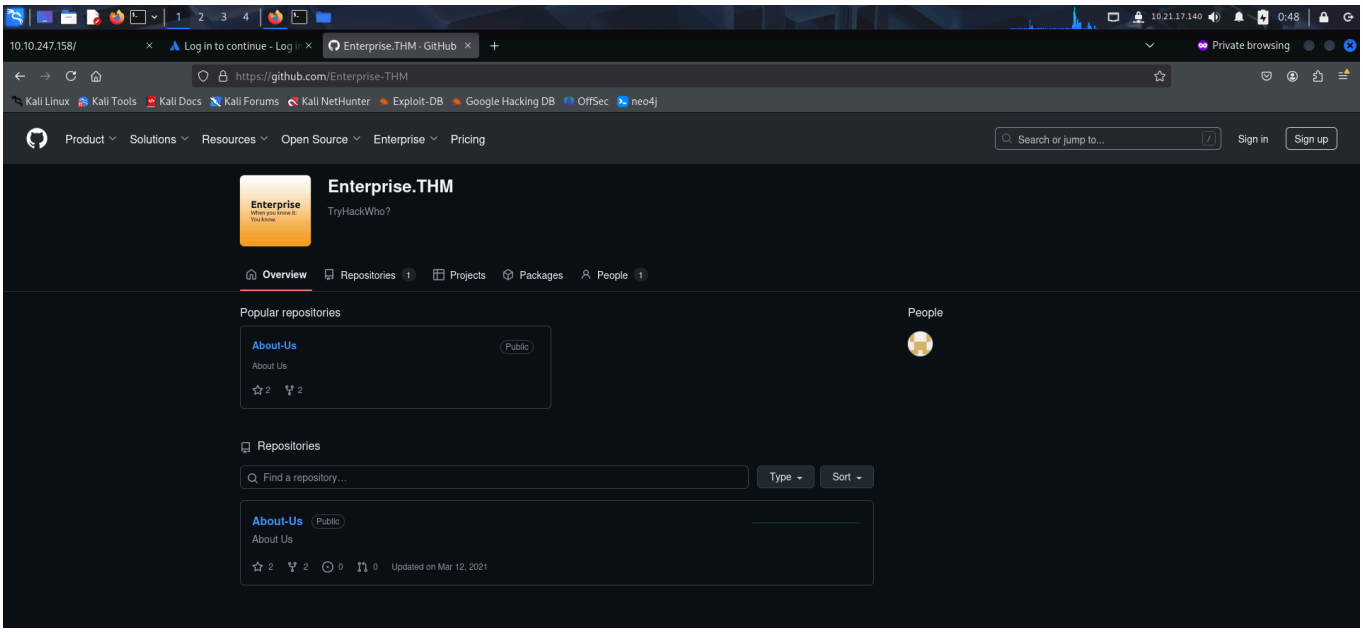
I tested the credential to see if I could use it for command execution but failed.

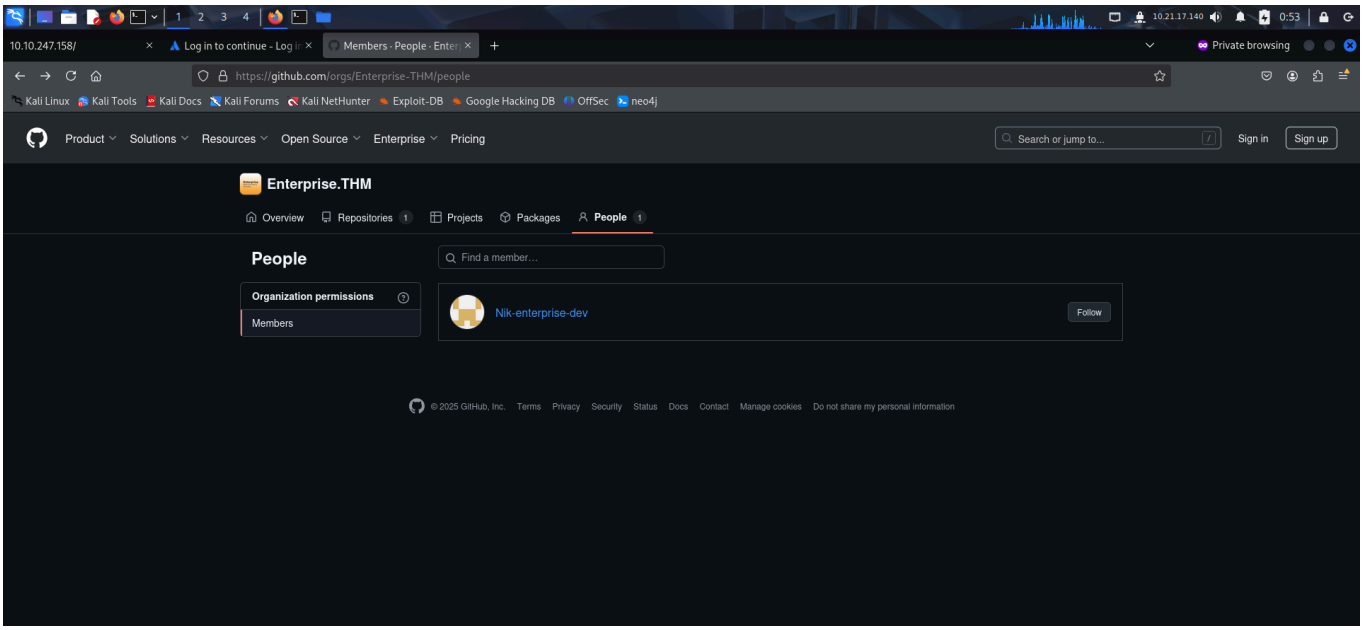


The atlasian login page said they were shifting to github, so i looked for its github.

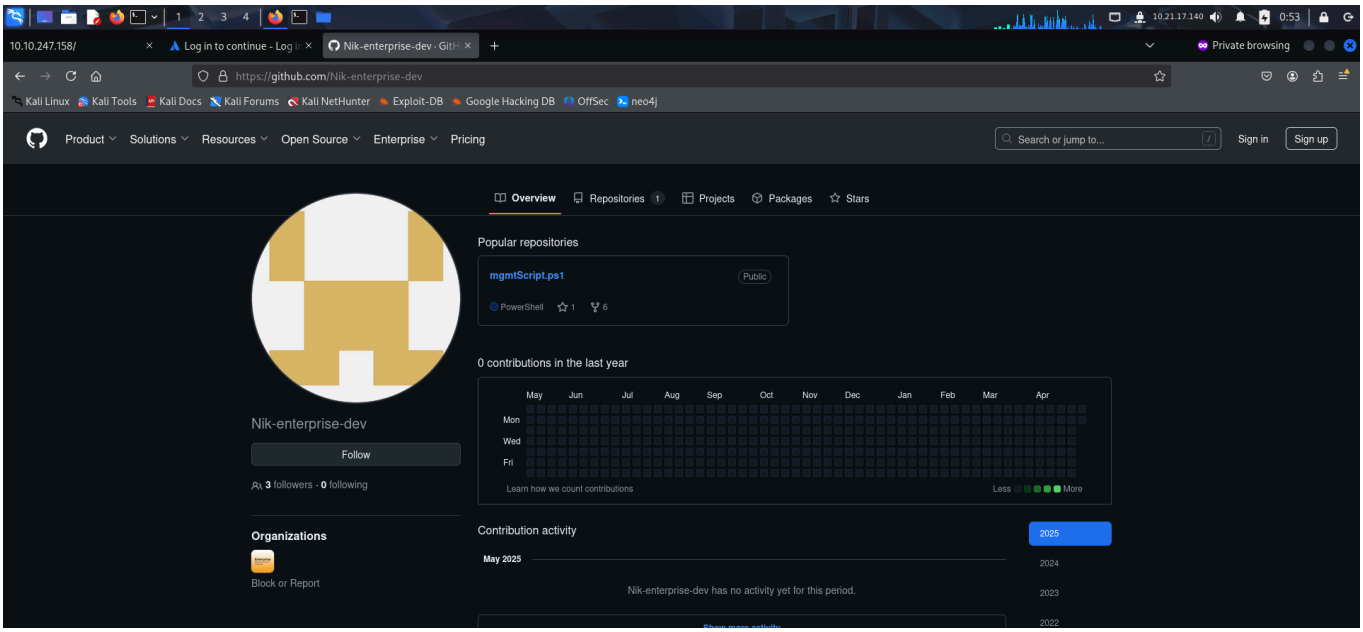


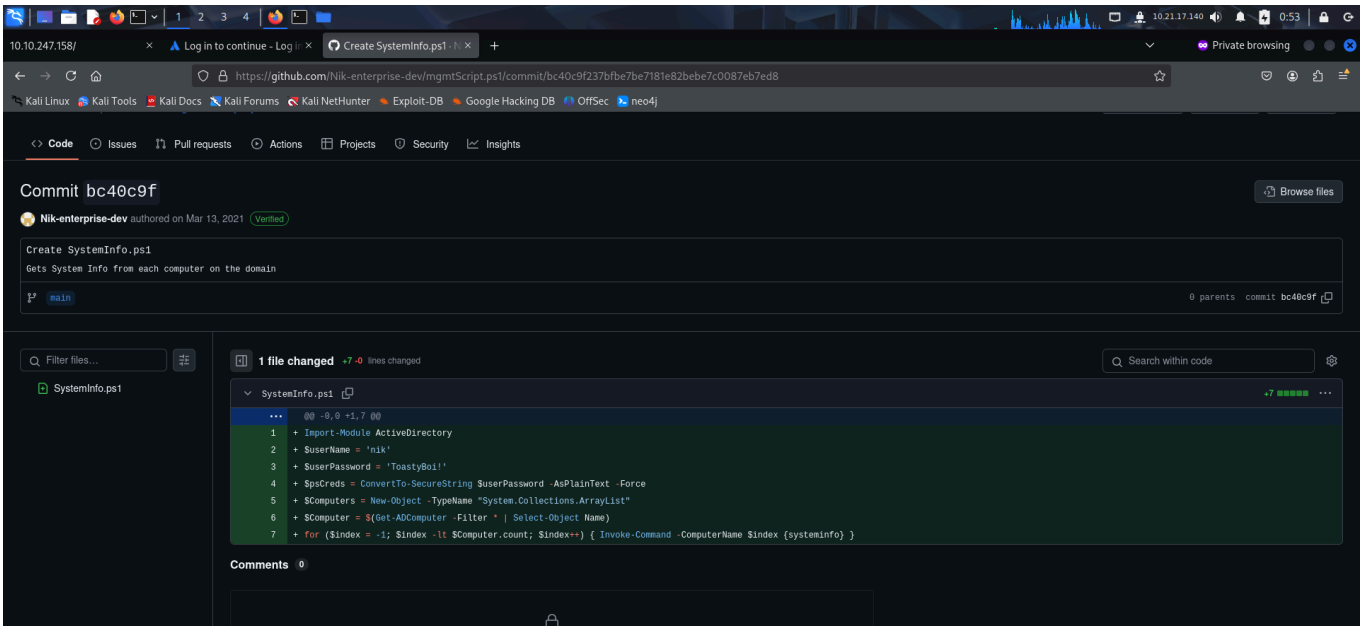
I found the organization on github and viewed its peoples.



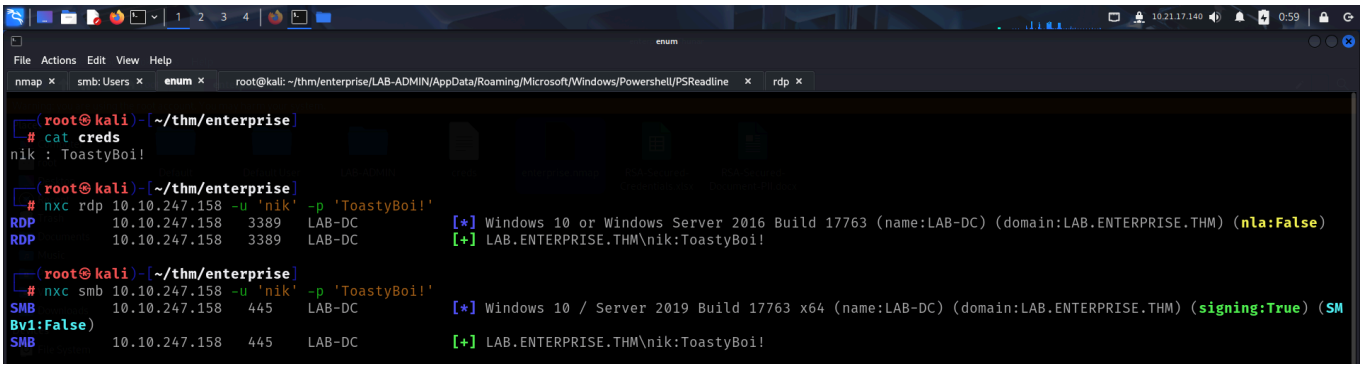


I accessed the user profile and viewed the uploaded script and found a new set of credentials.

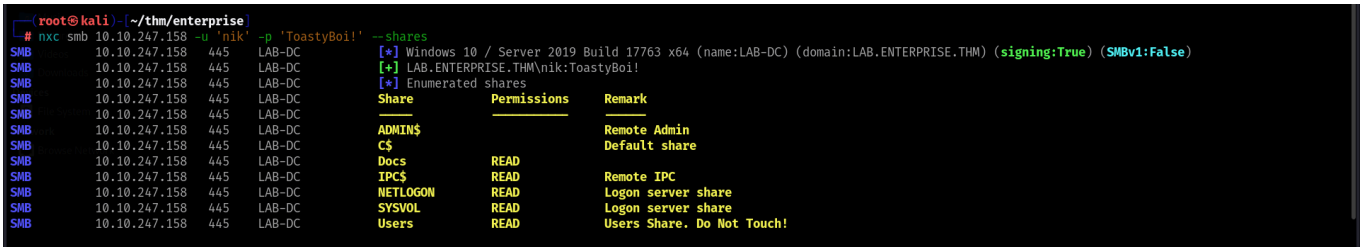




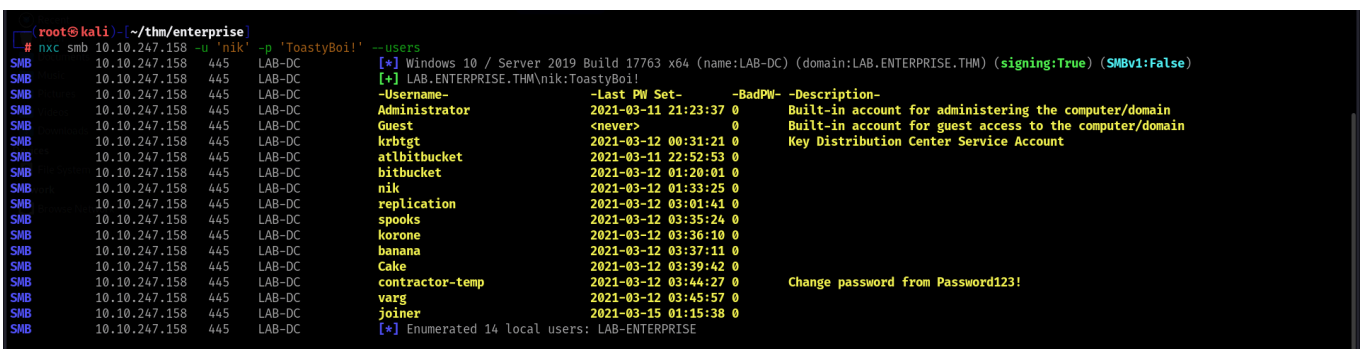
These were valid credentials but it didn't allow us to execute commands.



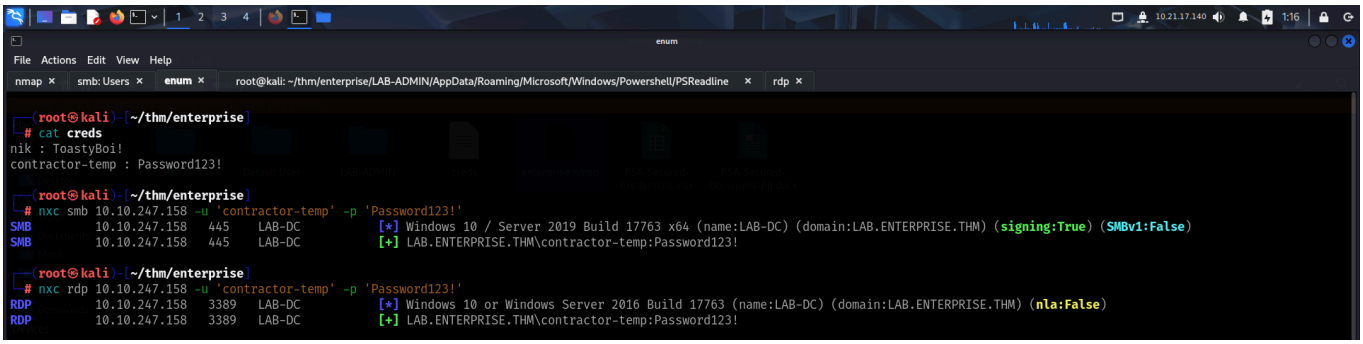
I used these credentials to look for any other share that might be reserved for the user.



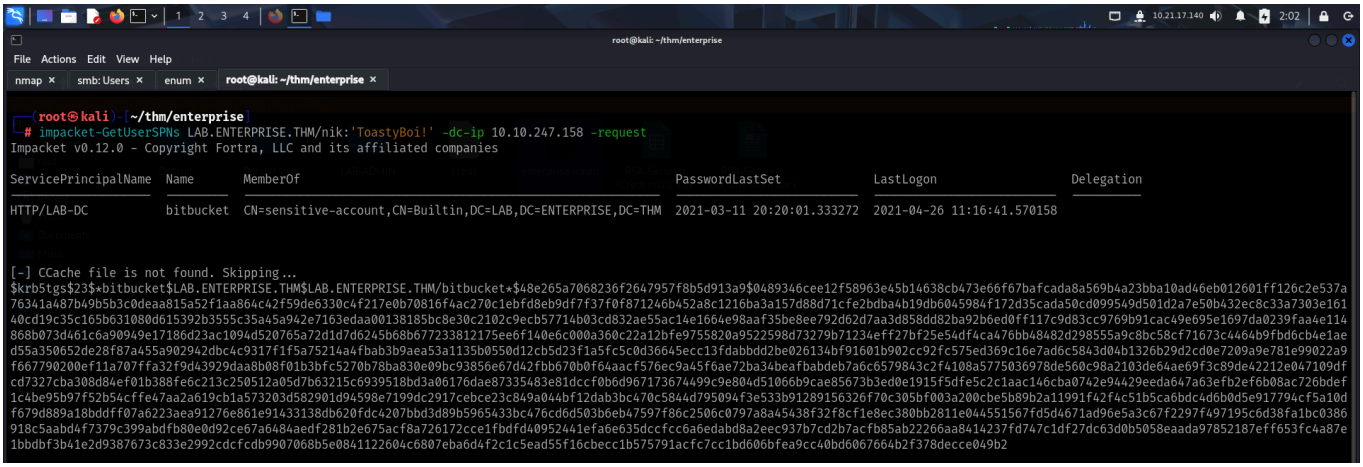
I then enumerated the users and found the credential of another user in its description.



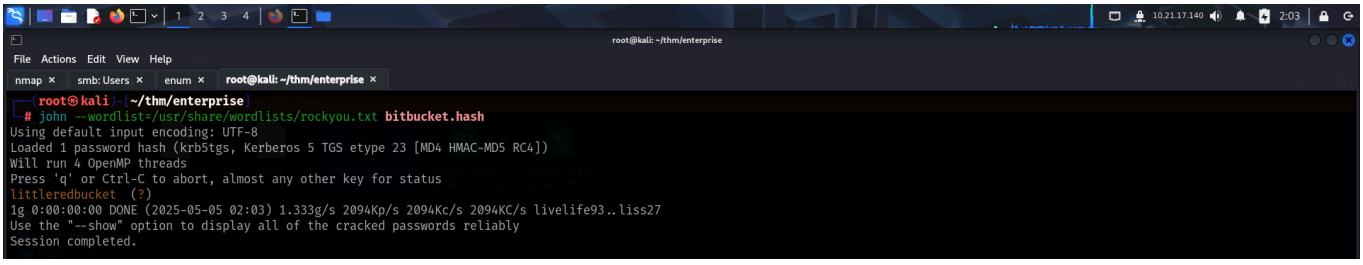
I tested these creds aswell but it didnt provide access to the system.



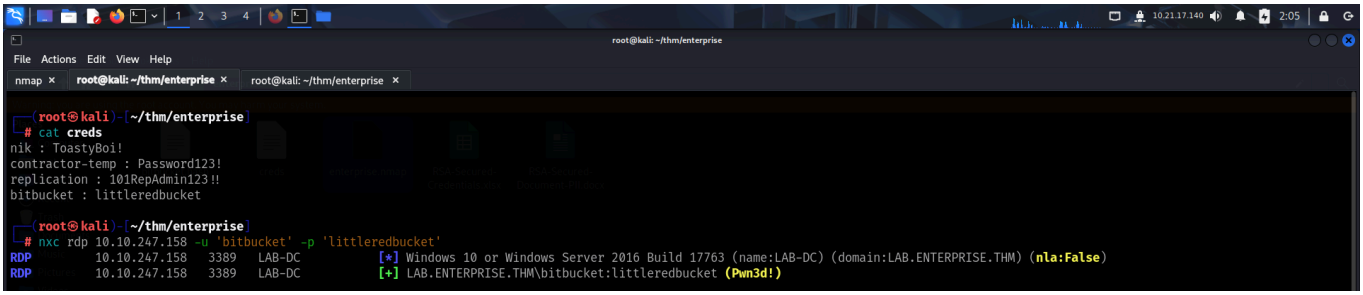
I then looked for kerberoastable accounts and got the kerberoast hash for the user `bitbucket`.

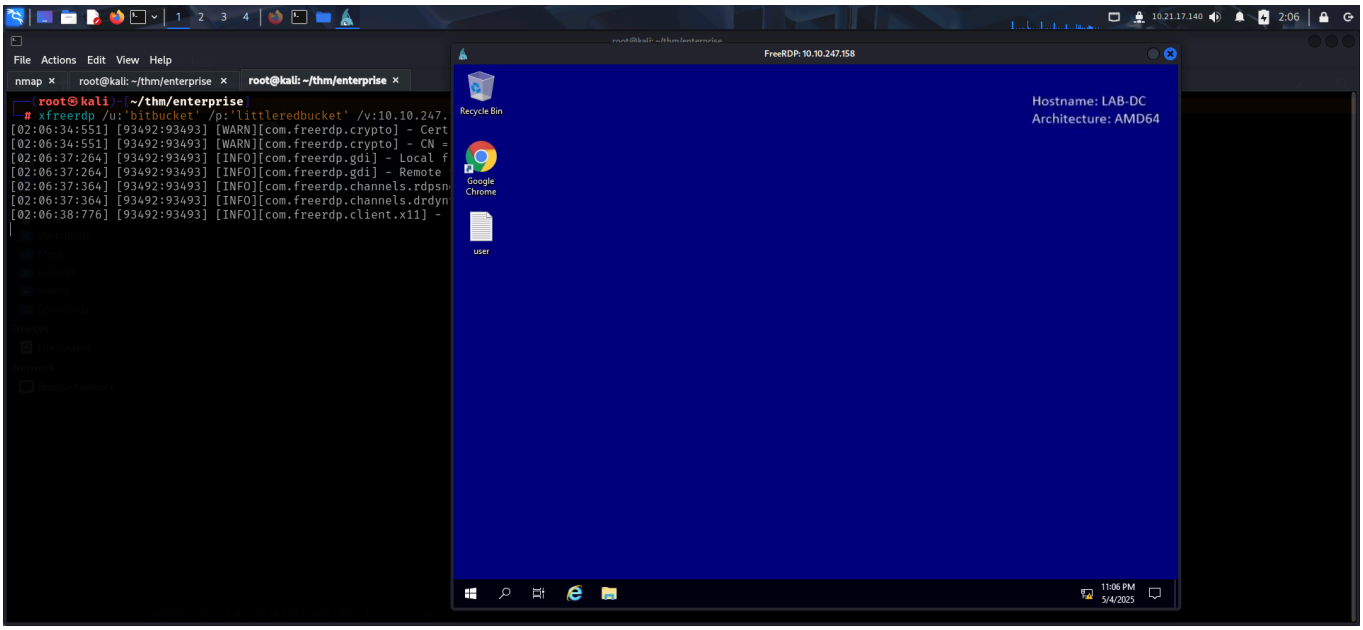


I then cracked the hash using **john**

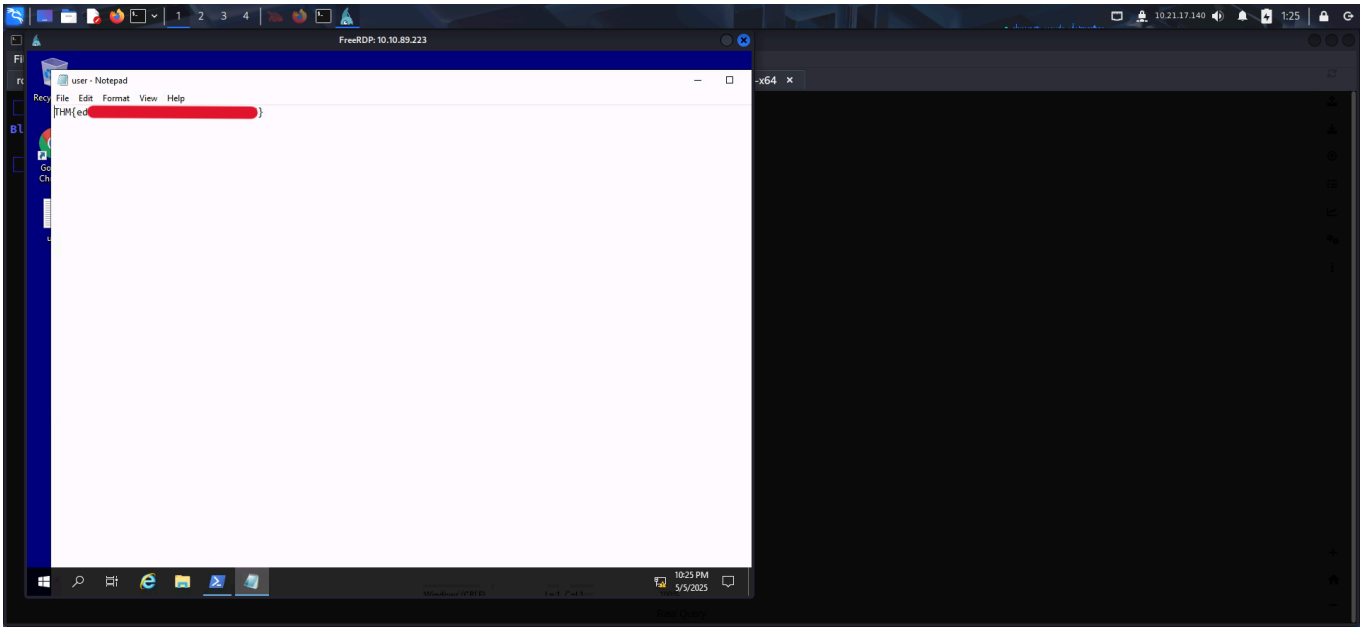


Finally, I accessed the machine using this credential. Through **rdp**.





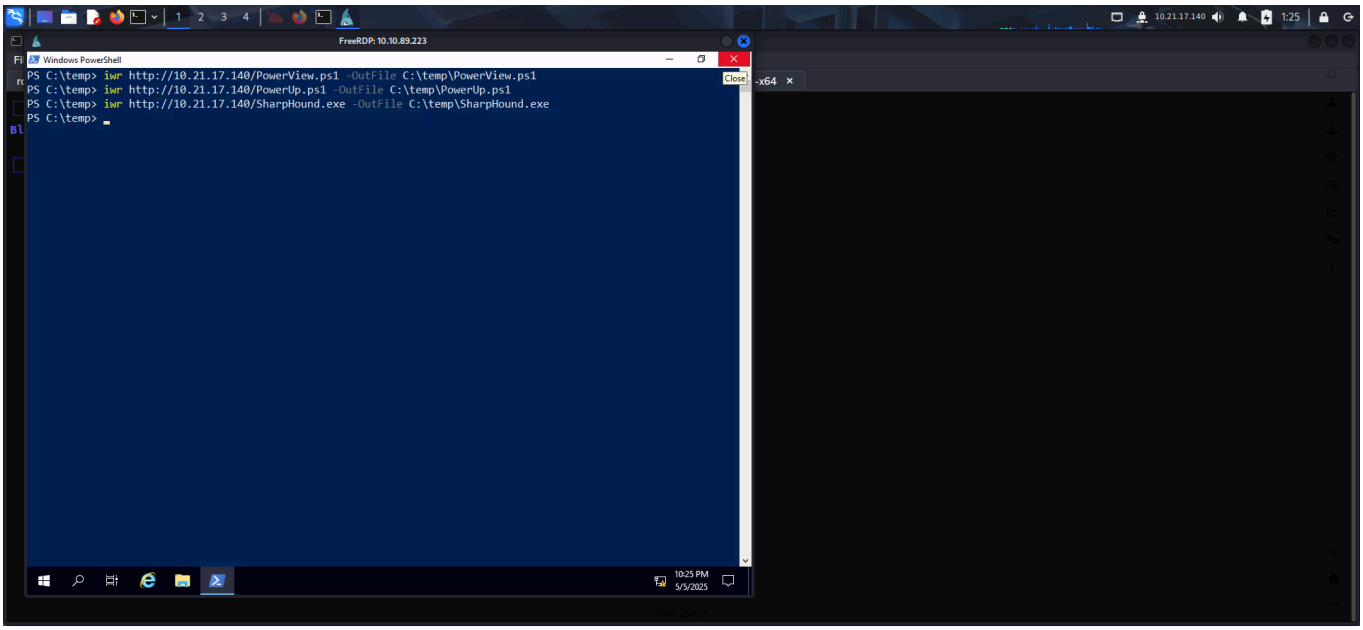
I then accessed the user flag from the Desktop.



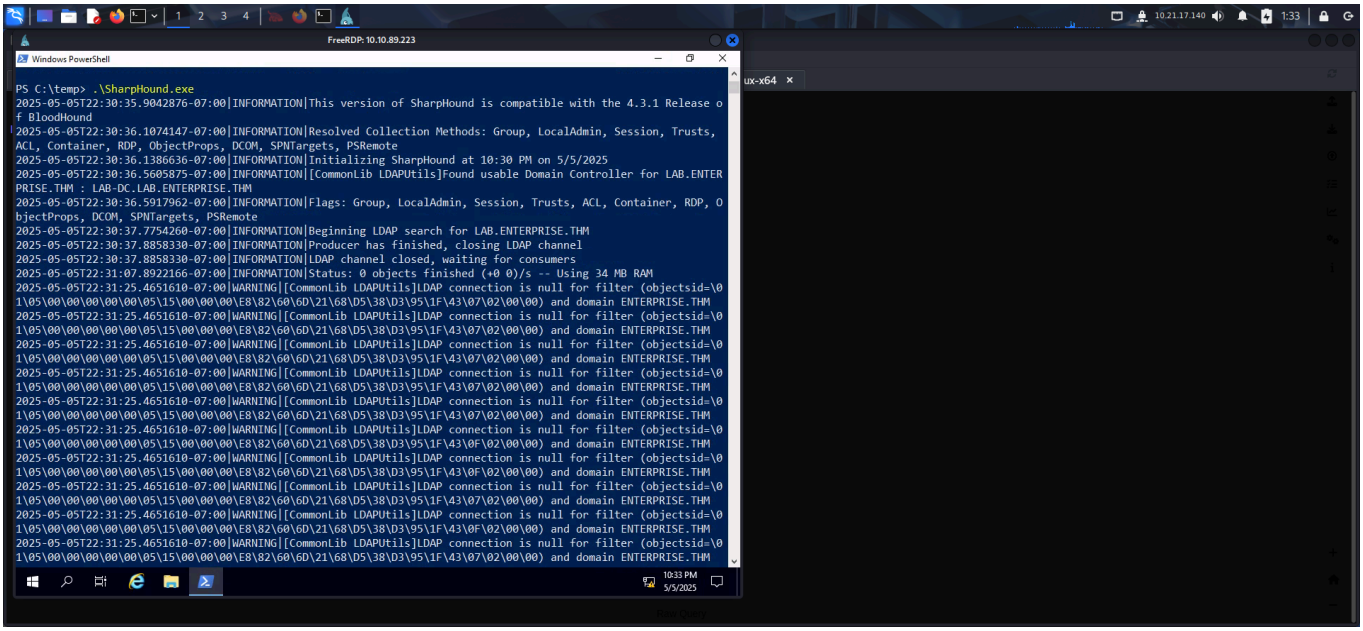
PRIVILEGE ESCALATION

I downloaded few tools for enumerating privilege escalation vectors.

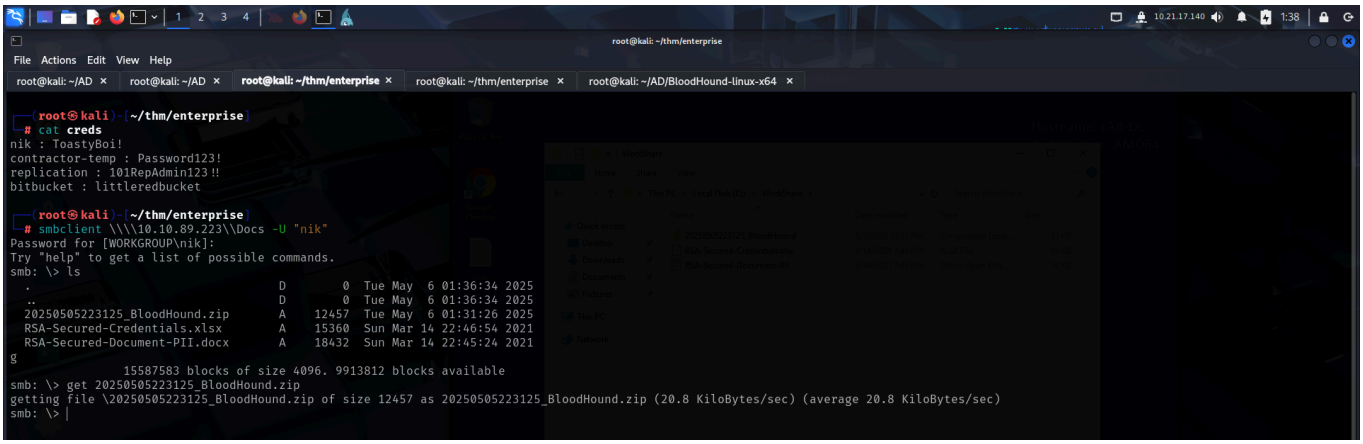
- PowerView
- PowerUp
- Sharphound



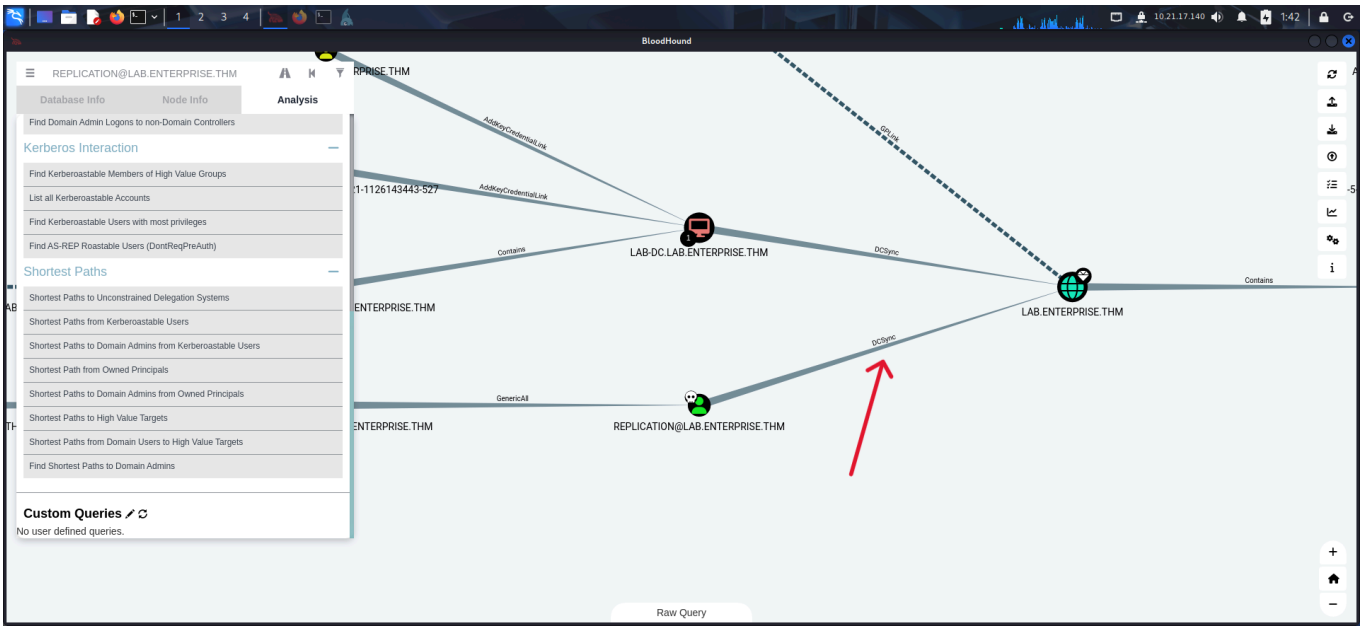
I first ran **sharphound** for comprehensive enumeration.



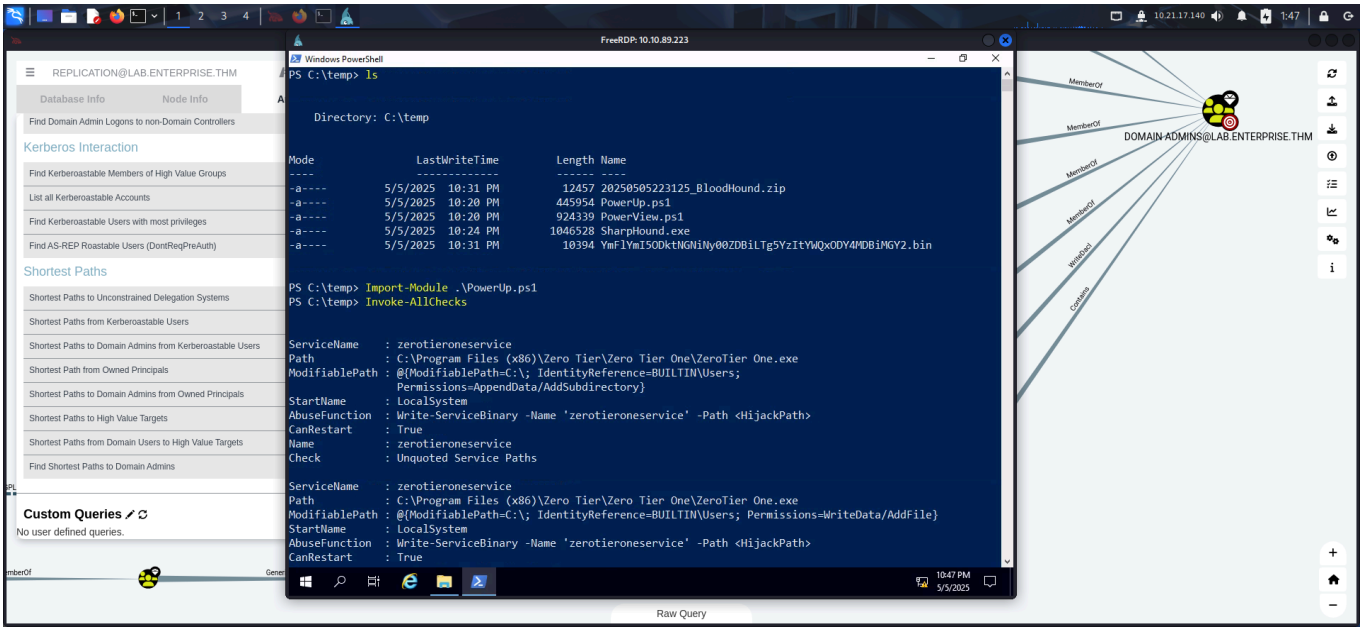
I downloaded the zip created by sharphound through smb share and uploaded it on **bloodhound**.



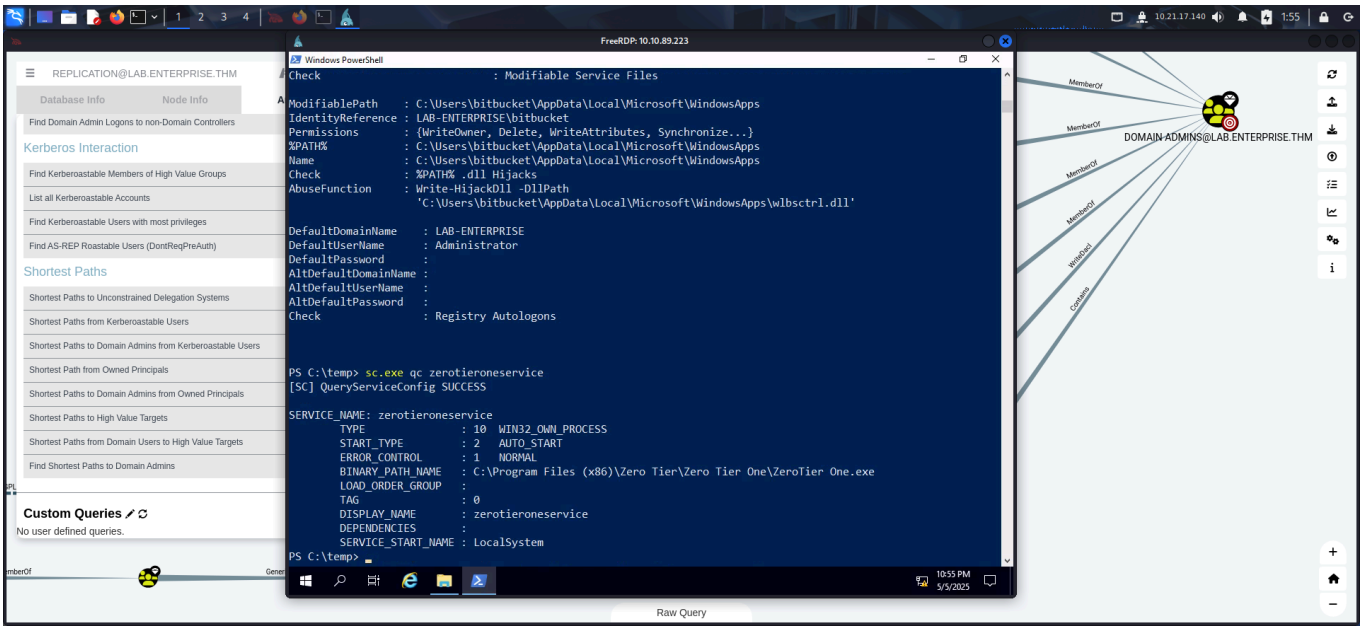
I found an interesting permission. The *Replication* user was allowed to perform **dc-sync**.



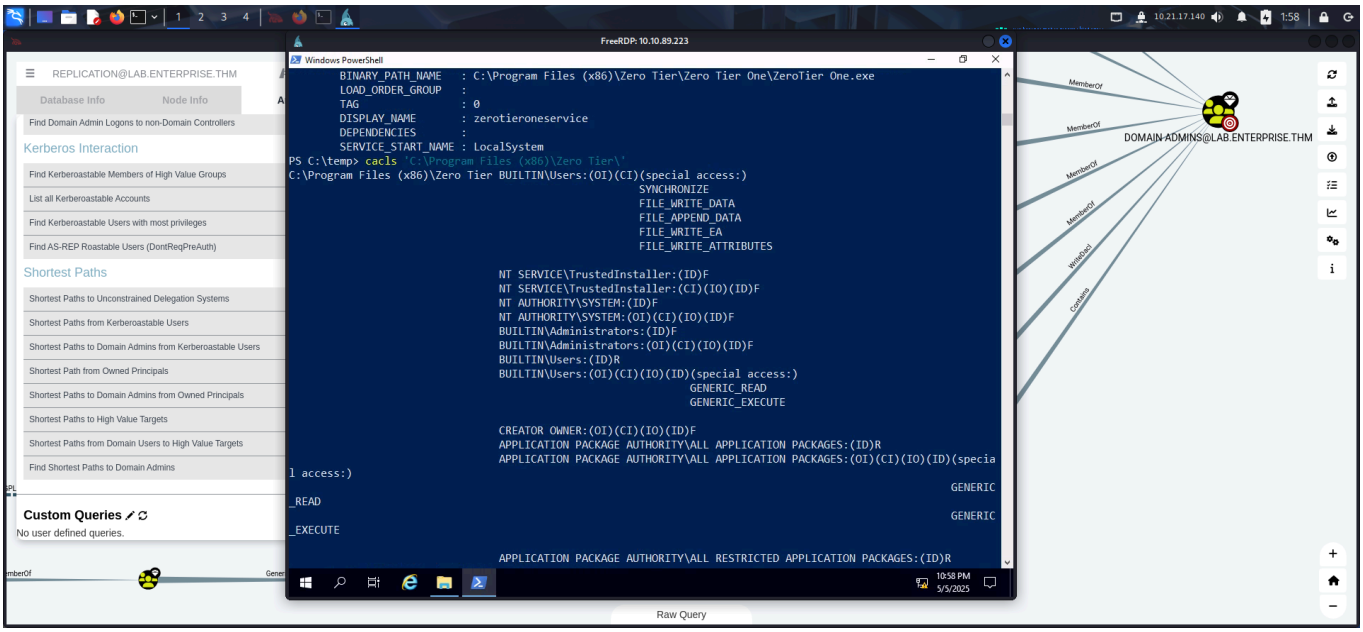
I then ran **PowerUp** to look for misconfigurations in the local system.

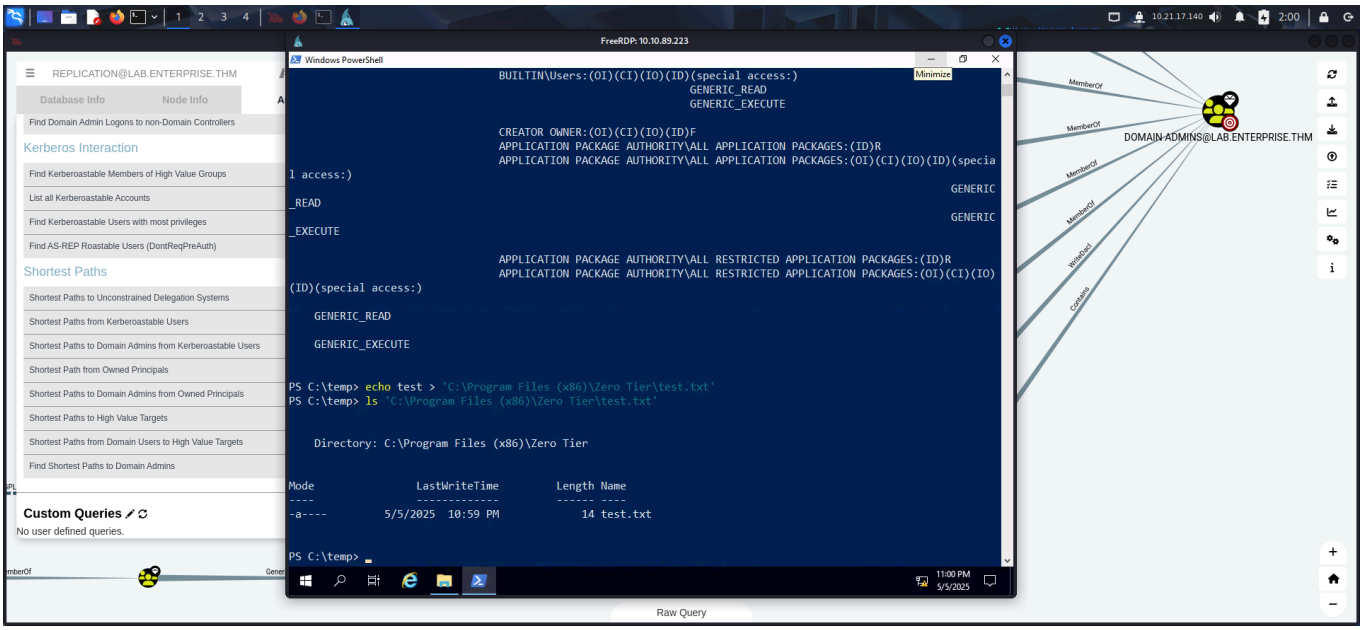


It discovered an **unquoted service path** vulnerability.

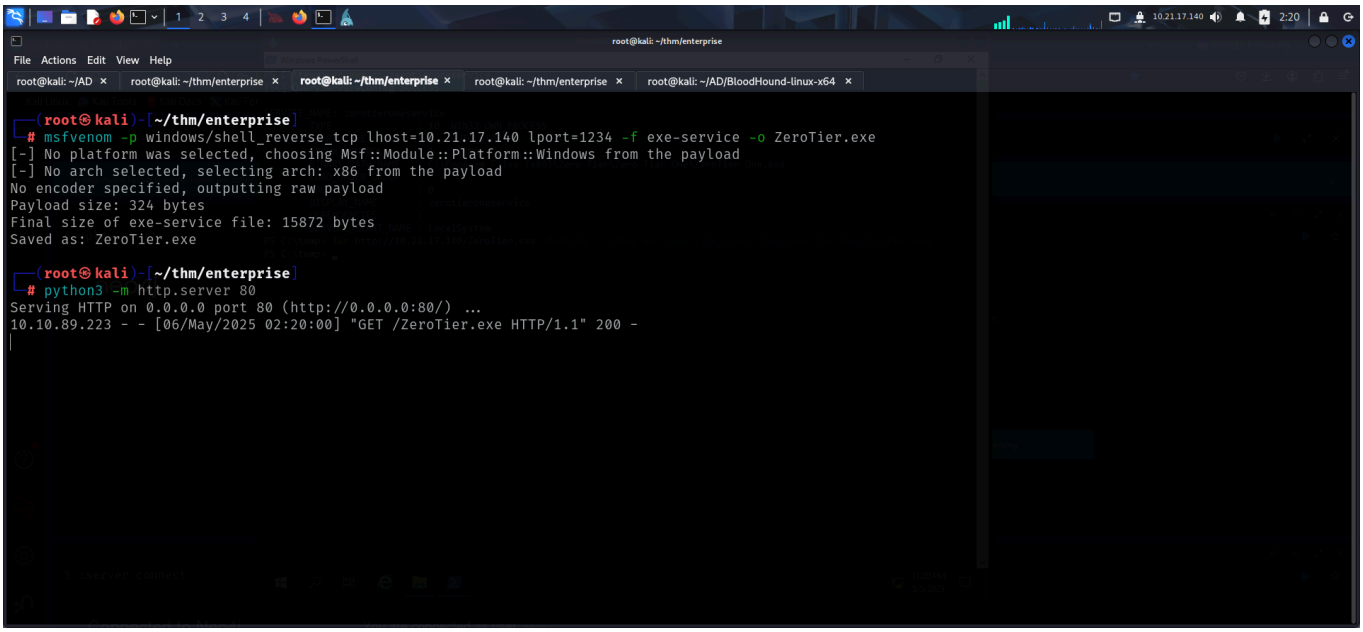


I then verified my access on the path of the exe.

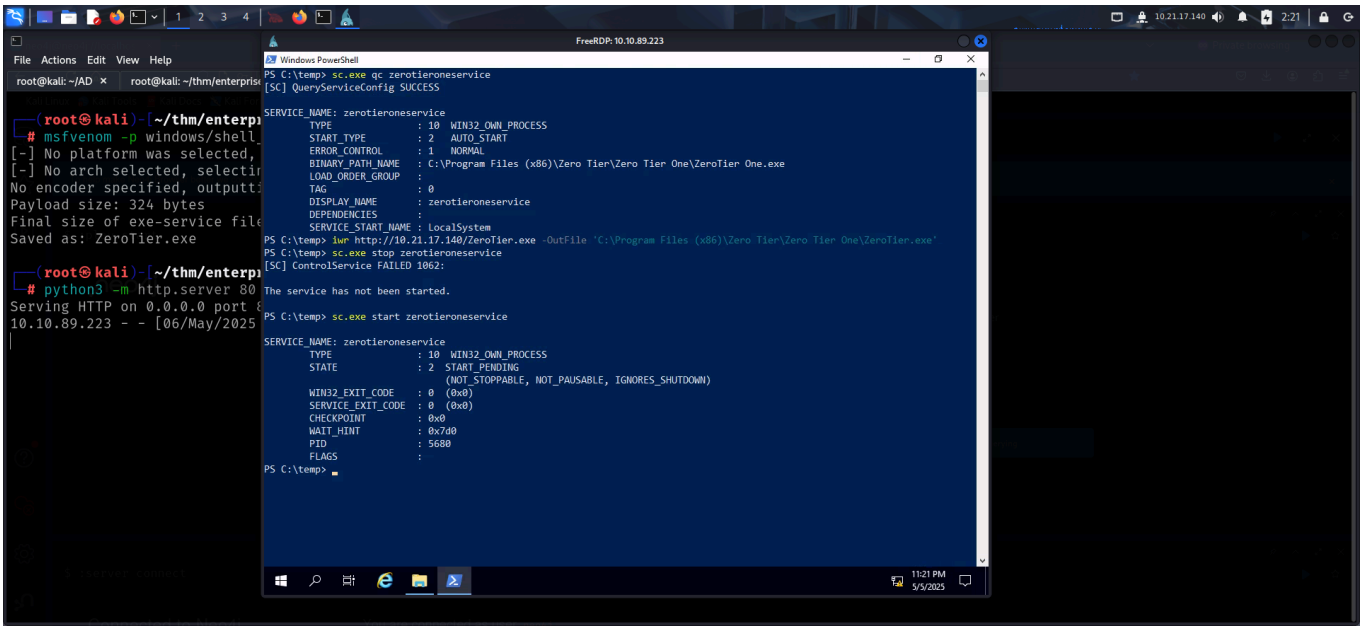




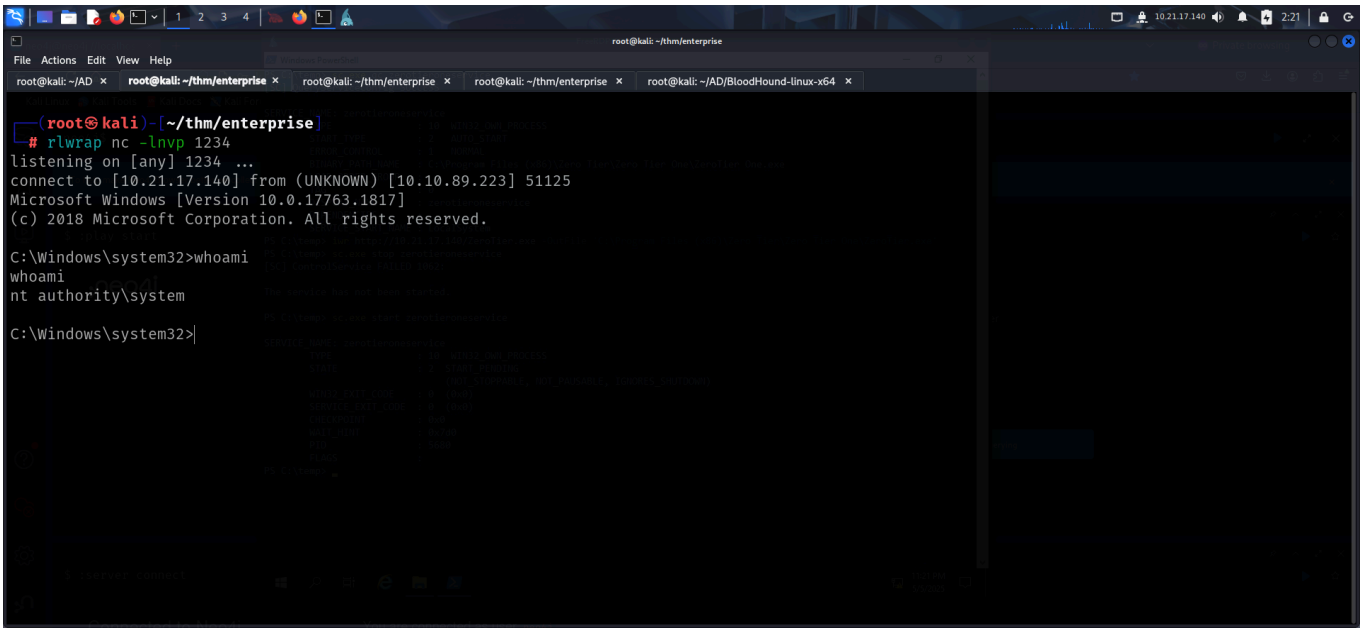
Since I had access, I created a payload using **msfvenom** and upload it on the vulnerable path.



Finally, I started a listener on my local machine and restarted the service.



Finally, I got a reverse shell as **nt authority\system**.



I then captured the root flag from **Administrator's** desktop.