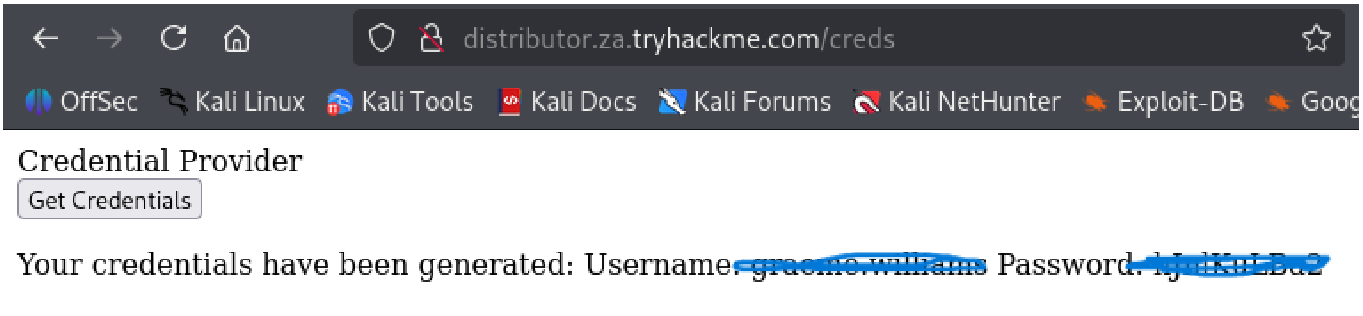
Enumerating Active Directory

Firstly stage request credentials:

we can simply do that by navigating to http://distributor.za.tryhackme.com/creds



Credential Provider

Your credentials have been generated: Username: [redacted] Password: [redacted]

now we can connect to the lab using our creds using this command `ssh za.tryhackme.com\\<AD Username>@thmjmp1.za.tryhackme.com`
and by this we can log into our target user we should mimic as compromised

Secondly Stage Credential Injection:

if one day we can get a username and password for active directory but we don't know how to use them we can use runas.exe which is a legitimate Windows binary to inject creds into memory and usual command looks like this `runas.exe /netonly /user:<domain>\<username> cmd.exe` Let's look at the parameters:

- **/netonly** - Since we are not domain-joined, we want to load the credentials for network authentication but not authenticate against a domain controller. So commands executed locally on the computer will run in the context of your standard Windows account, but any network connections will occur using the account specified here.
- **/user** - Here, we provide the details of the domain and the username. It is always a safe bet to use the Fully Qualified Domain Name (FQDN) instead of just the NetBIOS name of the domain since this will help with resolution.
- **cmd.exe** - This is the program we want to execute once the credentials are injected. This can be changed to anything, but the safest bet is cmd.exe since you can then use that to launch whatever you want, with the credentials injected.

second thing we can try to red the `SYSVOL` in the domain controller which is a shared folder that can be read by any user of the domain and it contains data about group polices and any other domain related scripts It is an essential component for Active Directory since it delivers these

GPOs to all computers on the domain. Domain-joined computers can then read these GPOs and apply the applicable ones, making domain-wide configuration changes from a central location

IP vs Hostnames

Question: *Is there a difference between* `dir \\za.tryhackme.com\SYSVOL` *and* `dir \\<DC IP>\SYSVOL` *and why the big fuss about DNS?*

There is quite a difference, and it boils down to the authentication method being used. When we provide the hostname, network authentication will attempt first to perform Kerberos authentication. Since Kerberos authentication uses hostnames embedded in the tickets, if we provide the IP instead, we can force the authentication type to be NTLM. While on the surface, this does not matter to us right now, it is good to understand these slight differences since they can allow you to remain more stealthy during a Red team assessment. In some instances, organisations will be monitoring for OverPass- and Pass-The-Hash Attacks. Forcing NTLM authentication is a good trick to have in the book to avoid detection in these cases.

Using Injected Credentials

Now that we have injected our AD credentials into memory, this is where the fun begins. With the /netonly option, all network communication will use these injected credentials for authentication. This includes all network communications of applications executed from that command prompt window.

This is where it becomes potent. Have you ever had a case where an MS SQL database used Windows Authentication, and you were not domain-joined? Start MS SQL Studio from that command prompt; even though it shows your local username, click Log In, and it will use the AD credentials in the background to authenticate! We can even use this to authenticate to web applications that use NTLM Authentication.

Q1: What native Windows binary allows us to inject credentials legitimately into memory?
A1: runas.exe

Q2: What parameter option of the runas binary will ensure that the injected credentials are used for all network connections?
A2: /netonly

Q3: What network folder on a domain controller is accessible by any authenticated AD account and stores GPO information?
A3: SYSVOL

Q4: When performing dir \za.tryhackme.com\SYSVOL, what type of authentication is performed by default?
A4: Kerberos Authentication

Third stage Enumeration through Microsoft Management Console:

now we need to connect to `THMJMP1` using rdp we can do that through kali or any distributions of Linux using #xfreerdp3 by using this command `xfreerdp3 /u:<username> /p:<password> /cert:ignore /v:<target_ip_adress>`
after connection we can load mmc using `WIN+R` to open run and then type mmc then we can add domains by clicking on file > Add/Remove Snap-in > we will add all 3 active directory > we will change the forest for the first two and the domain for the third one to `za.tryhackme.com` then we can get into active directory users and computers and see the data we need

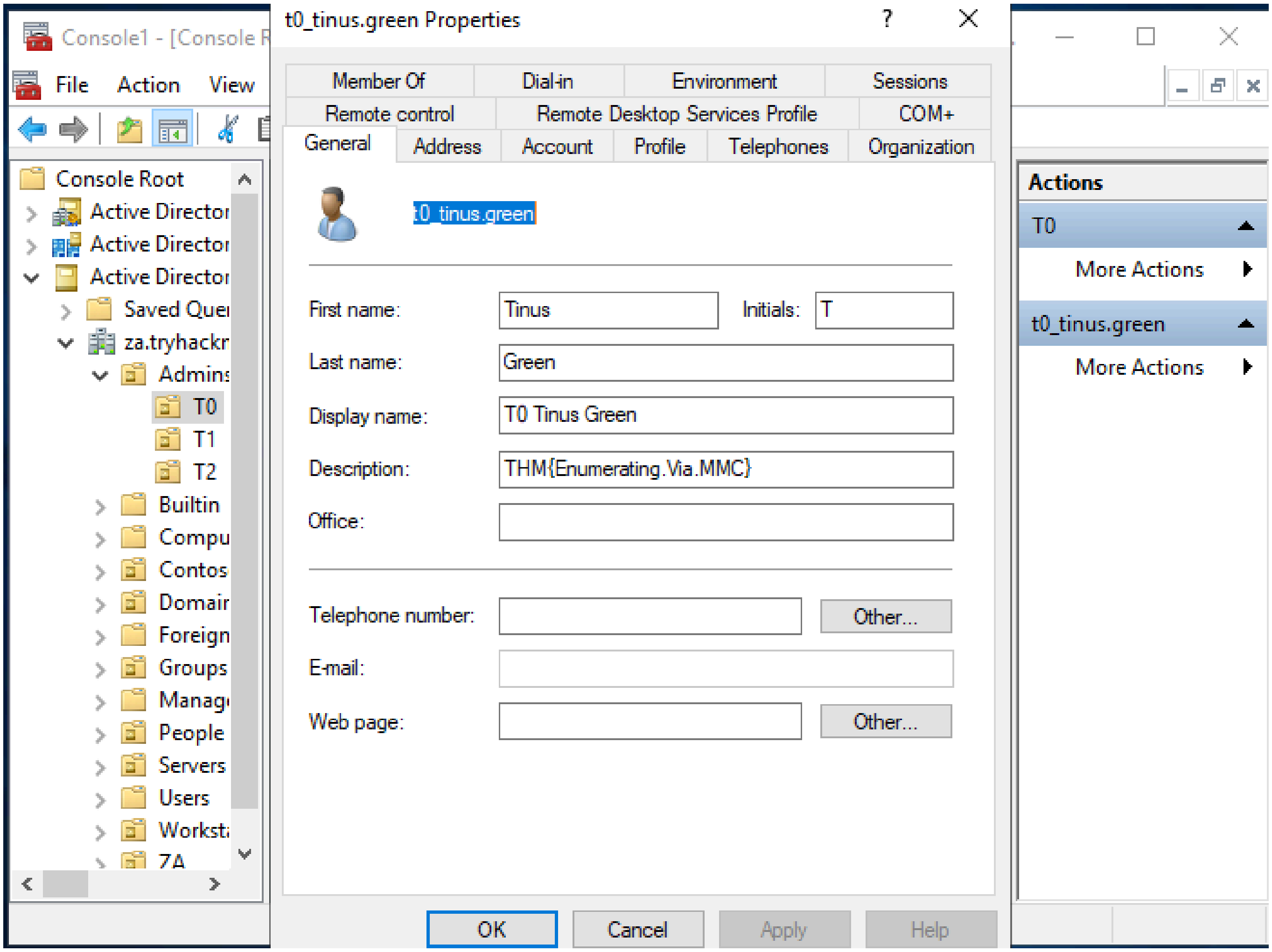
Q1: How many Computer objects are part of the Servers OU?
A1: 2

Q2: How many Computer objects are part of the Workstations OU?
A2: 1

Q3: How many departments (Organisational Units) does this organisation consist of?
A3: 7

Q4: How many Admin tiers does this organisation have?
A4: 3

Q5: What is the value of the flag stored in the description attribute of the t0_tinus.green account?
A5: THM{Enumerating.Via.MMC}



t0_tinus.green Properties

t0_tinus.green

First name: Tinus

Initials: T

Last name: Green

Display name: T0 Tinus Green

Description: THM{Enumerating.Via.MMC}

Office:

Telephone number:

E-mail:

Web page:

Enumeration through Command Prompt:

There are times when you just need to perform a quick and dirty AD lookup, and Command Prompt has your back. Good ol' reliable CMD is handy when you perhaps don't have RDP access to a system, defenders are monitoring for PowerShell use, and you need to perform your AD Enumeration through a Remote Access Trojan (RAT). It can even be helpful to embed a couple of simple AD enumeration commands in your phishing payload to help you gain the vital information that can help you stage the final attack.

CMD has a built-in command that we can use to enumerate information about AD, namely `net`. The `net` command is a handy tool to enumerate information about the local system and AD. We will look at a couple of interesting things we can enumerate from this position, but this is not an exhaustive list.

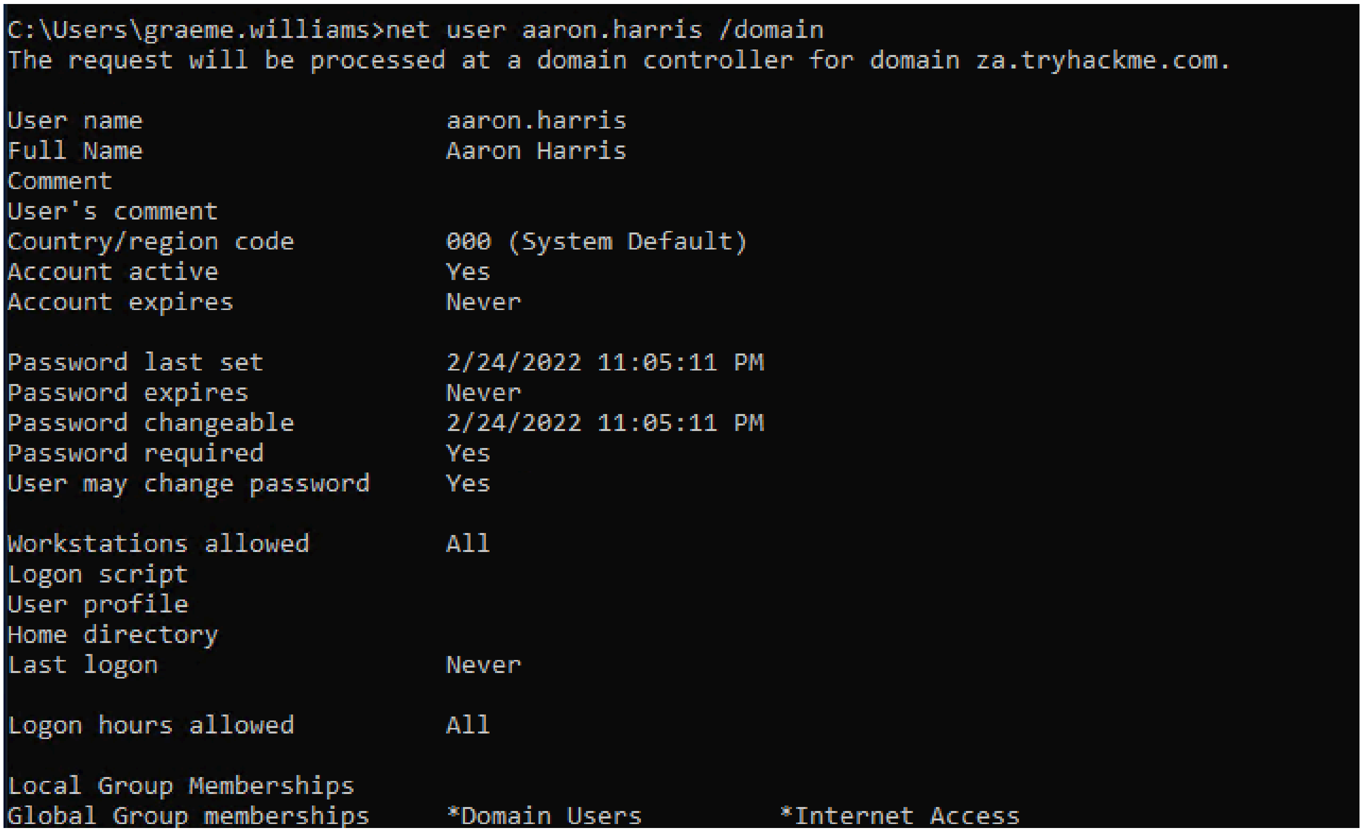
Note: For this task you will have to use THMJMP1 and won't be able to use your own Windows VM. This will be explained in the drawbacks.

we can enumerate all the users using #net by doing `net user /domain` and we can quarry all the data about a certain user using `net user <username> /domain` and we can use it again to list all the groups using `net group /domain` and again we can query all the data about a certain group using the command `net group <groupname> /domain`

We can use the `net` command to enumerate the password policy of the domain by using the `accounts` sub-option `net accounts /domain`

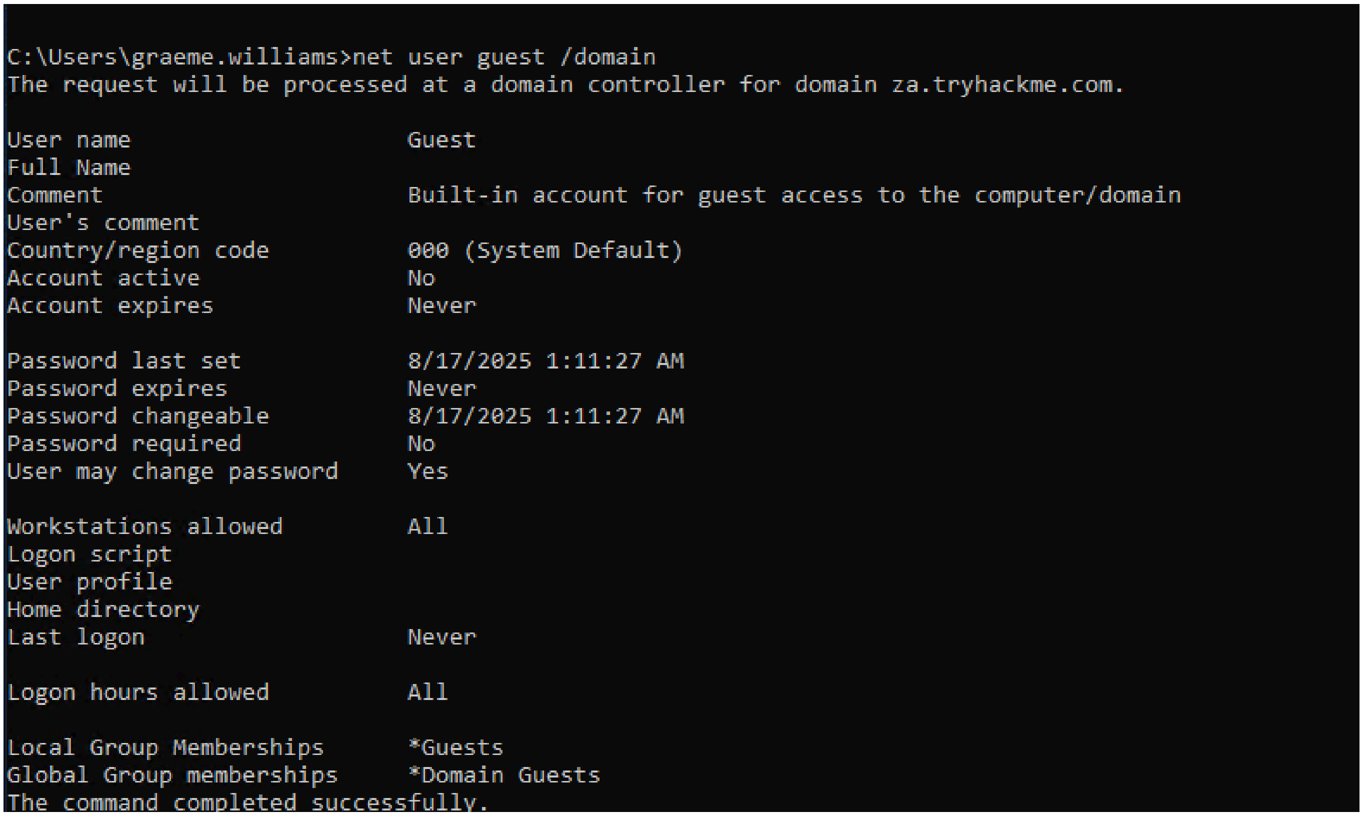
and this will provide us with helpful information

Q1: Apart from the Domain Users group, what other group is the aaron.harris account a member of?
A1: Internet Access



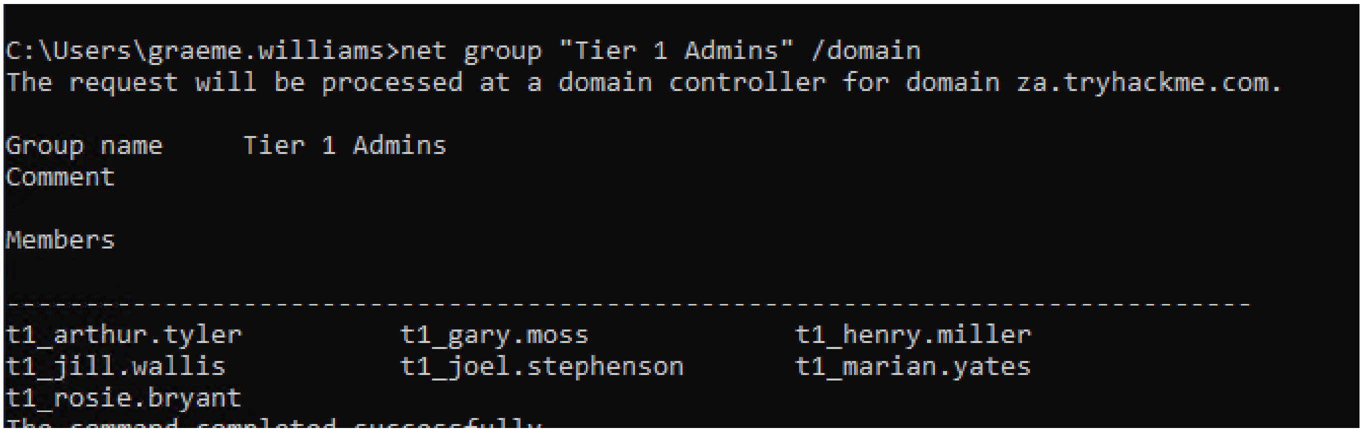
```
C:\Users\graeme.williams>net user aaron.harris /domain
The request will be processed at a domain controller for domain za.tryhackme.com.

User name                    aaron.harris
Full Name                    Aaron Harris
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/24/2022 11:05:11 PM
Password expires             Never
Password changeable          2/24/2022 11:05:11 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     *Domain Users         *Internet Access
```

Q2: Is the Guest account active? (Yay,Nay)
A2: Nay



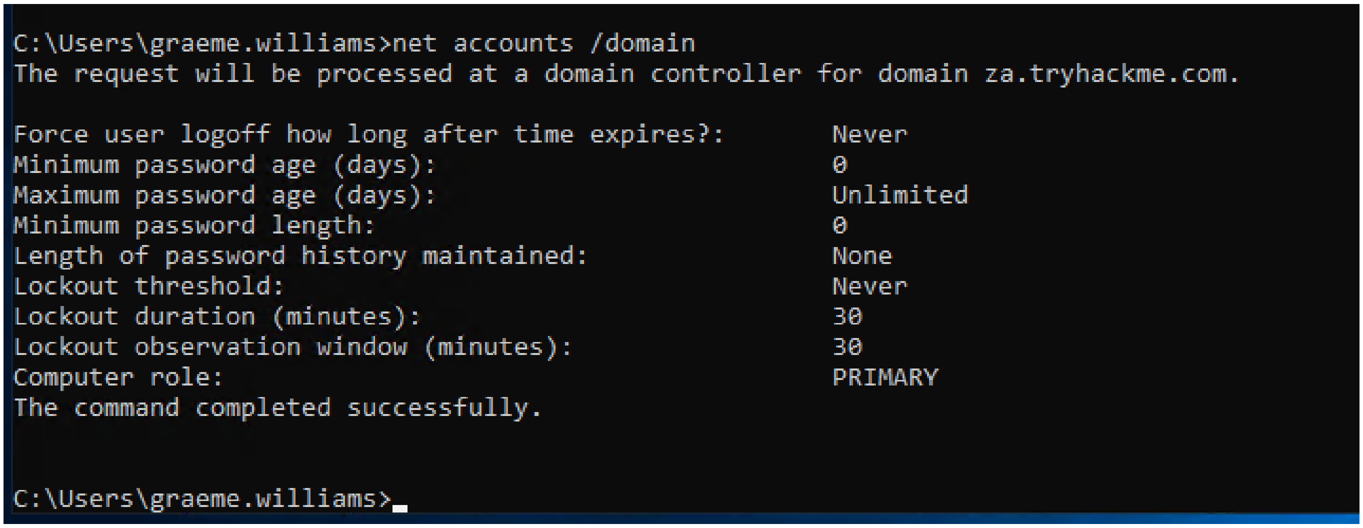
```
C:\Users\graeme.williams>net user guest /domain
The request will be processed at a domain controller for domain za.tryhackme.com.

User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never

Password last set            8/17/2025 1:11:27 AM
Password expires             Never
Password changeable          8/17/2025 1:11:27 AM
Password required            No
User may change password     Yes

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

Logon hours allowed          All

Local Group Memberships      *Guests
Global Group memberships     *Domain Guests
The command completed successfully.
```

Q3: How many accounts are a member of the Tier 1 Admins group?
A3: 7



```
C:\Users\graeme.williams>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.
```

Q4: What is the account lockout duration of the current password policy in minutes?
A4: 30



```
C:\Users\graeme.williams>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.


C:\Users\graeme.williams>_
```

Enumeration through PowerShell

PowerShell

PowerShell is the upgrade of Command Prompt. Microsoft first released it in 2006.
While PowerShell has all the standard functionality Command Prompt provides, it also provides access to cmdlets (pronounced command-lets), which are .NET classes to perform specific functions. While we can write our own cmdlets, like the creators of PowerView did, we can already get very far using the built-in ones.

Since we installed the AD-RSAT tooling in Task 3, it automatically installed the associated cmdlets for us. There are 50+ cmdlets installed. We will be looking at some of these, but refer to this list for the complete list of cmdlets.

Using our SSH terminal, we can upgrade it to a PowerShell terminal using the following command: `powershell`

we can enumerate users using `Get-ADUser` like `Get-ADUser -Identity gordon.stevens -Server za.tryhackme.com -Properties *`

The parameters are used for the following:

- -Identity - The account name that we are enumerating
- -Properties - Which properties associated with the account will be shown, * will show all properties
- -Server - Since we are not domain-joined, we have to use this parameter to point it to our domain controller

For most of these cmdlets, 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

We can use the `Get-ADGroup` cmdlet to enumerate AD groups: like `Get-ADGroup -Identity Administrators -Server za.tryhackme.com`

A more generic search for any AD objects can be performed using the `Get-ADObject` cmdlet. For example, if we are looking for all AD objects that were changed after a specific date `$ChangeDate = New-Object DateTime(2022, 02, 28, 12, 00, 00)` `Get-ADObject -Filter 'whenChanged -gt $ChangeDate' -includeDeletedObjects -Server za.tryhackme.com`

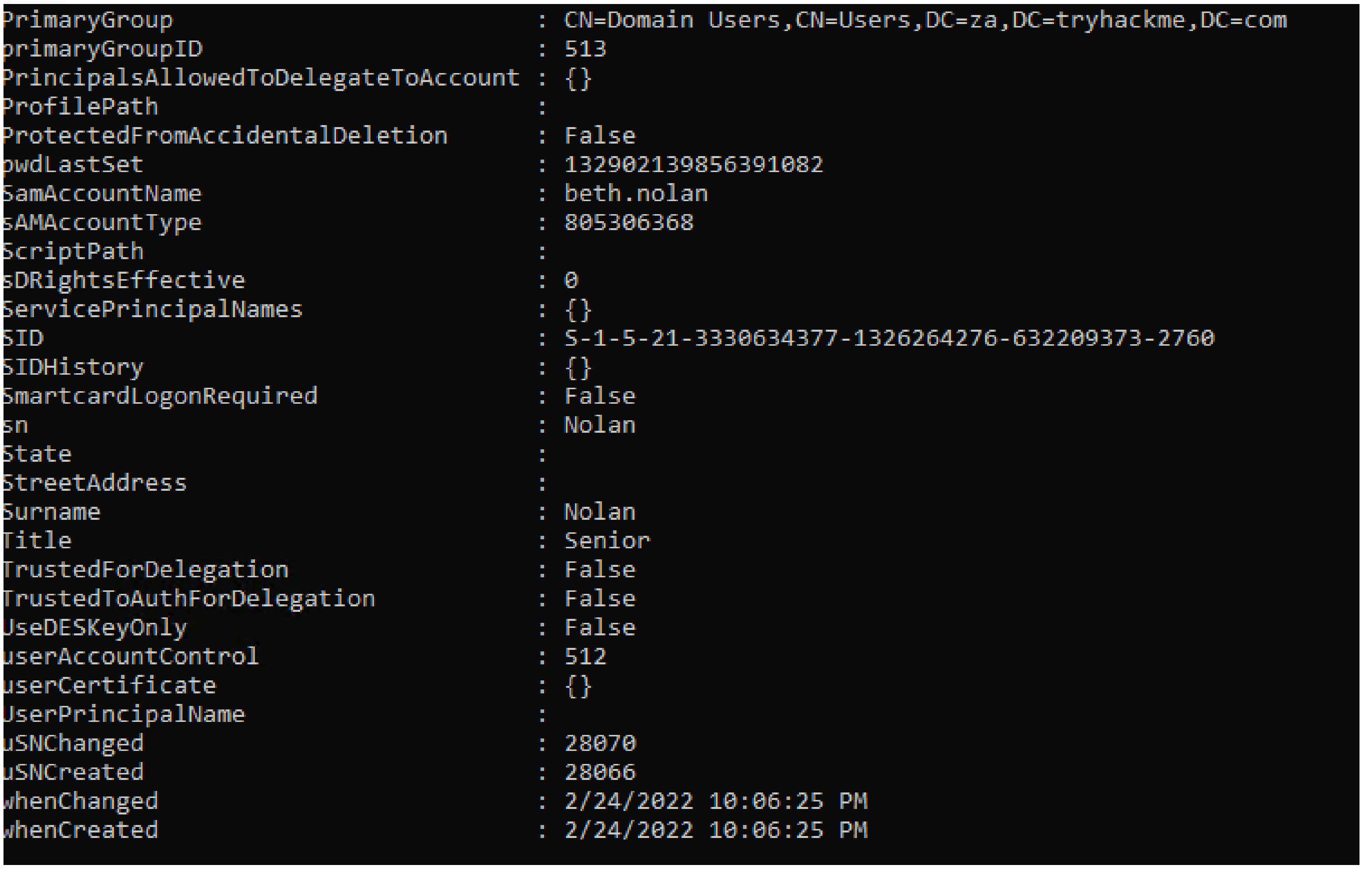
We can use `Get-ADDomain` to retrieve additional information about the specific domain `Get-ADDomain -Server za.tryhackme.com`

The great thing about the AD-RSAT cmdlets is that some even allow you to create new or alter existing AD objects. However, our focus for this network is on enumeration. Creating new objects or altering existing ones would be considered AD exploitation, which is covered later in the AD module.

However, we will show an example of this by force changing the password of our AD user by using the `Set-ADAccountPassword` cmdlet

```
Set-ADAccountPassword -Identity gordon.stevens -Server za.tryhackme.com -OldPassword (ConvertTo-SecureString -AsPlaintext "old" -force) -NewPassword (ConvertTo-SecureString -AsPlainText "new" -Force)
```

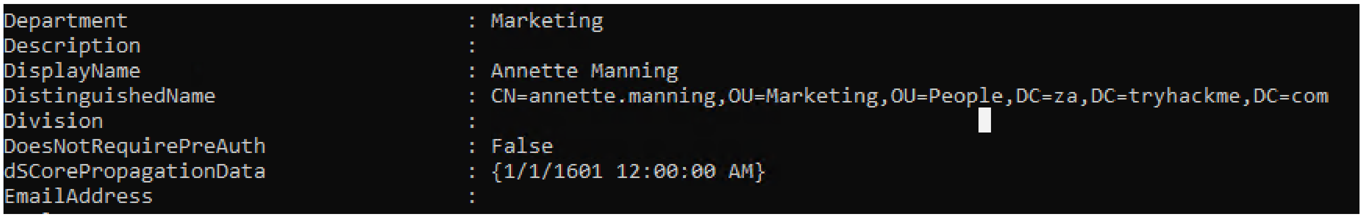
Q1: What is the value of the Title attribute of Beth Nolan (beth.nolan)?
A1: senior



```
PrimaryGroup                         : CN=Domain Users,CN=Users,DC=za,DC=tryhackme,DC=com
primaryGroupID                       : 513
PrincipalsAllowedToDelegateToAccount : {}
ProfilePath                          :
ProtectedFromAccidentalDeletion      : False
pwdLastSet                           : 132902139856391082
SamAccountName                       : beth.nolan
sAMAccountType                       : 805306368
ScriptPath                           :
sDRightsEffective                    : 0
ServicePrincipalNames                : {}
SID                                  : S-1-5-21-3330634377-1326264276-632209373-2760
SIDHistory                           : {}
SmartcardLogonRequired               : False
sn                                   : Nolan
State                                :
StreetAddress                        :
Surname                              : Nolan
Title                                : Senior
TrustedForDelegation                 : False
TrustedToAuthForDelegation           : False
UseDESKeyOnly                        : False
userAccountControl                   : 512
userCertificate                      : {}
UserPrincipalName                    :
uSNChanged                           : 28070
uSNCreated                           : 28066
whenChanged                          : 2/24/2022 10:06:25 PM
whenCreated                          : 2/24/2022 10:06:25 PM
```

Q2: What is the value of the DistinguishedName attribute of Annette Manning (annette.manning)?

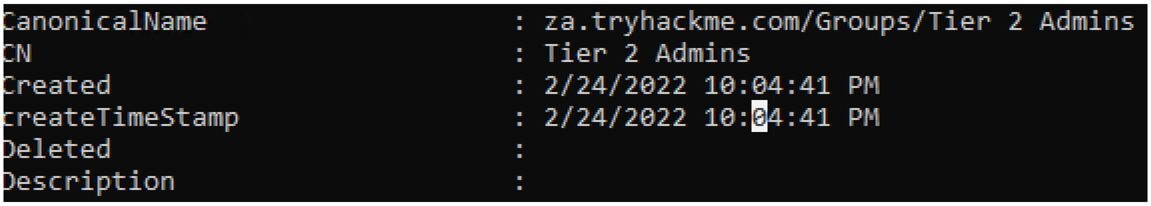
A2: CN=annette.manning,OU=Marketing,OU=People,DC=za,DC=tryhackme,DC=com



```
Department                           : Marketing
Description                          :
DisplayName                          : Annette Manning
DistinguishedName                    : CN=annette.manning,OU=Marketing,OU=People,DC=za,DC=tryhackme,DC=com
Division                             :
DoesNotRequirePreAuth                : False
dSCorePropagationData                : {1/1/1601 12:00:00 AM}
EmailAddress                         :
```

Q3: When was the Tier 2 Admins group created?

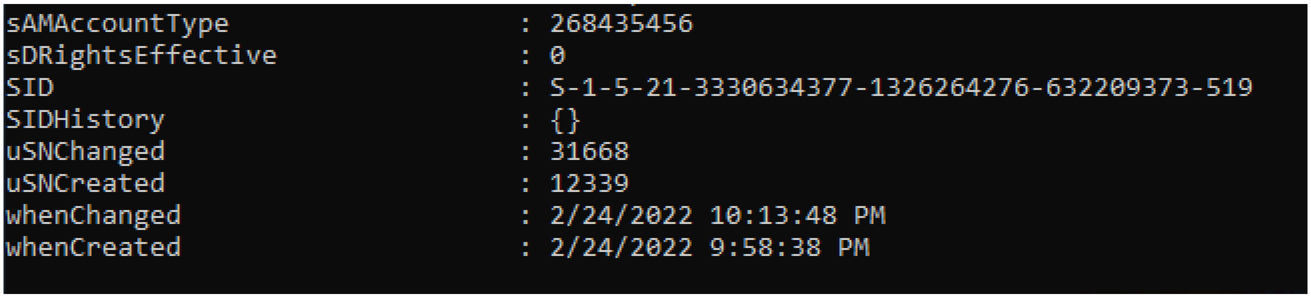
A3: 2/24/2022 10:04:41 PM



```
CanonicalName                        : za.tryhackme.com/Groups/Tier 2 Admins
CN                                   : Tier 2 Admins
Created                              : 2/24/2022 10:04:41 PM
createTimeStamp                      : 2/24/2022 10:04:41 PM
Deleted                              :
Description                          :
```

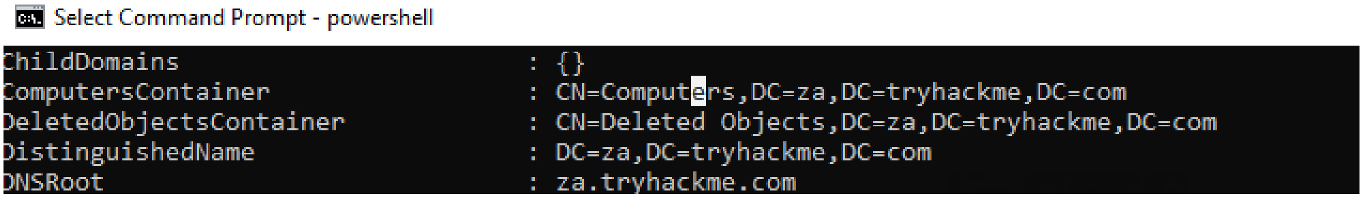
Q4: What is the value of the SID attribute of the Enterprise Admins group?

A4: S-1-5-21-3330634377-1326264276-632209373-519



```
sAMAccountType                : 268435456
sDRightsEffective             : 0
SID                           : S-1-5-21-3330634377-1326264276-632209373-519
SIDHistory                    : {}
uSNChanged                    : 31668
uSNCreated                    : 12339
whenChanged                   : 2/24/2022 10:13:48 PM
whenCreated                   : 2/24/2022 9:58:38 PM
```

Q5: Which container is used to store deleted AD objects?
A5: CN=Deleted Objects,DC=za,DC=tryhackme,DC=com



```
ChildDomains                         : {}
ComputersContainer                   : CN=Computers,DC=za,DC=tryhackme,DC=com
DeletedObjectsContainer              : CN=Deleted Objects,DC=za,DC=tryhackme,DC=com
DistinguishedName                    : DC=za,DC=tryhackme,DC=com
DNSRoot                              : za.tryhackme.com
```

Enumeration through Bloodhound:

Lastly, we will look at performing AD enumeration using Bloodhound. Bloodhound is the most powerful AD enumeration tool to date, and when it was released in 2016, it changed the AD enumeration landscape forever.

Bloodhound History

For a significant amount of time, red teamers (and, unfortunately, attackers) had the upper hand. So much so that Microsoft integrated their own version of Bloodhound in its Advanced Threat Protection solution. It all came down to the following phrase:

"Defenders think in lists, Attackers think in graphs." - Unknown

Bloodhound allowed attackers (and by now defenders too) to visualise the AD environment in a graph format with interconnected nodes. Each connection is a possible path that could be exploited to reach a goal. In contrast, the defenders used lists, like a list of Domain Admins or a list of all the hosts in the environment.

This graph-based thinking opened up a world to attackers. It allowed for a two-stage attack. In the first stage, the attackers would perform phishing attacks to get an initial entry to enumerate AD information. This initial payload was usually incredibly noisy and would be detected and contained by the blue team before the attackers could perform any actions apart from exfiltrating the enumerated data. However, the attackers could now use this data offline to create an attack path in graph format, showing precisely the steps and hops required. Using this information during the second phishing campaign, the attackers could often reach their goal in minutes once a breach was achieved. It is often even faster than it would take the blue team to receive their first alert. This is the power of thinking in graphs, which is why so many blue teams have also started to use these types of tools to understand their security posture better.

Sharphound

You will often hear users refer to Sharphound and Bloodhound interchangeably. However, they are not the same. Sharphound is the enumeration tool of Bloodhound. It is used to enumerate the AD information that can then be visually displayed in Bloodhound. Bloodhound is the actual GUI used to display the AD attack graphs. Therefore, we first need to learn how to use Sharphound to enumerate AD before we can look at the results visually using Bloodhound.

There are three different Sharphound collectors:

- **Sharphound.ps1** - PowerShell script for running Sharphound. However, the latest release of Sharphound has stopped releasing the Powershell script version. This version is good to use with RATs since the script can be loaded directly into memory, evading on-disk AV scans.
- **Sharphound.exe** - A Windows executable version for running Sharphound.
- **AzureHound.ps1** - PowerShell script for running Sharphound for Azure (Microsoft Cloud Computing Services) instances. Bloodhound can ingest data enumerated from Azure to find attack paths related to the configuration of Azure Identity and Access Management.

Note: Your Bloodhound and Sharphound versions must match for the best results. Usually there are updates made to Bloodhound which means old Sharphound results cannot be ingested. This network was created using Bloodhound v4.1.0. Please make sure to use this version with the Sharphound results.

When using these collector scripts on an assessment, there is a high likelihood that these files will be detected as malware and raise an alert to the blue team. This is again where our Windows machine that is non-domain-joined can assist. We can use the `runas` command to inject the AD credentials and point Sharphound to a Domain Controller. Since we control this Windows machine, we can either disable the AV or create exceptions for specific files or folders, which has already been performed for you on the THMJMP1 machine. You can find the Sharphound binaries on this host in the `C:\Tools\` directory. We will use the SharpHound.exe version for our enumeration, but feel free to play around with the other two. We will execute Sharphound as follows:

```
Sharphound.exe --CollectionMethods <Methods> --Domain za.tryhackme.com --ExcludeDCs
```

Parameters explained:

- CollectionMethods - Determines what kind of data Sharphound would collect. The most common options are Default or All. Also, since Sharphound caches information, once the first run has been completed, you can only use the Session collection method to retrieve new user sessions to speed up the process.
- Domain - Here, we specify the domain we want to enumerate. In some instances, you may want to enumerate a parent or other domain that has trust with your existing domain. You can tell Sharphound which domain should be enumerated by altering this parameter.
- ExcludeDCs -This will instruct Sharphound not to touch domain controllers, which reduces the likelihood that the Sharphound run will raise an alert.

You can find all the various Sharphound parameters here. It is good to overview the other parameters since they may be required depending on your red team assessment circumstances.

Using your SSH PowerShell session from the previous task, copy the Sharphound binary to your AD user's Documents directory `copy C:\Tools\Sharphound.exe ~\Documents\` we will run sharp hound using all and session collection method `SharpHound.exe --CollectionMethods All --Domain za.tryhackme.com --ExcludeDCs` then we need to start blood hound too wee the results we start with running #neo4j with `neo4j console start` then on another tab `bloodhound --no-sandbox` to visualize the result

Q1: What command can be used to execute Sharphound.exe and request that it recovers Session information only from the za.tryhackme.com domain without touching domain controllers?
A1: Sharphound.exe --CollectionMethods Session --Domain za.tryhackme.com --ExcludeDCs

Q2: Apart from the krbtgt account, how many other accounts are potentially kerberoastable?
A2: 4

Q3: How many machines do members of the Tier 1 Admins group have administrative access to?
A3: 2

Q4: How many users are members of the Tier 2 Admins group?
A4: 15