Active Directory Basics — TryHackMe

kawsar uddin · Follow

17 min read · Jun 9, 2023

Listen Share More

This room will introduce the basic concepts and functionality provided by Active Directory.

Answer: active directory

The server in charge of running the Active Directory services is called…

Answer: Domain Controller

Note:

What is AD?

*=> **Active directory** is a **directory database /server** that stores **users' information** such as **usernames, phone numbers, emails, and many other credentials. The same network User's things can be managed from an active directory. Privileges of the users are also controlled from the active directory.***

The server that runs the Active Directory services is known as a ***Domain Controller (DC).***

To overcome some ***limitations like manually creating users by visiting each computer separately, and fixing problems in any computer manually, creating a specific boundary for each user manually,*** *we can use a* ***Windows domain.*** *Simply put a* ***Windows domain*** *for a* ***group of users and computers under the administration of a given business.*** *The main idea behind a domain is to* ***centralize the administration of common components of a Windows computer network in a single repository called Active Directory (AD).*** *The server that runs the Active Directory services is known as a* ***Domain Controller (DC).***

The main advantages of having a configured Windows domain are:

- ***Centralized identity management: All users across the network*** *can be* ***configured from Active Directory*** *with* ***minimum*** *effort.*
- ***Managing security policies:*** *You can c****onfigure security policies directly*** *from* ***Active Directory*** *and apply them to* ***users and computers*** *across the* ***network*** *as needed.*

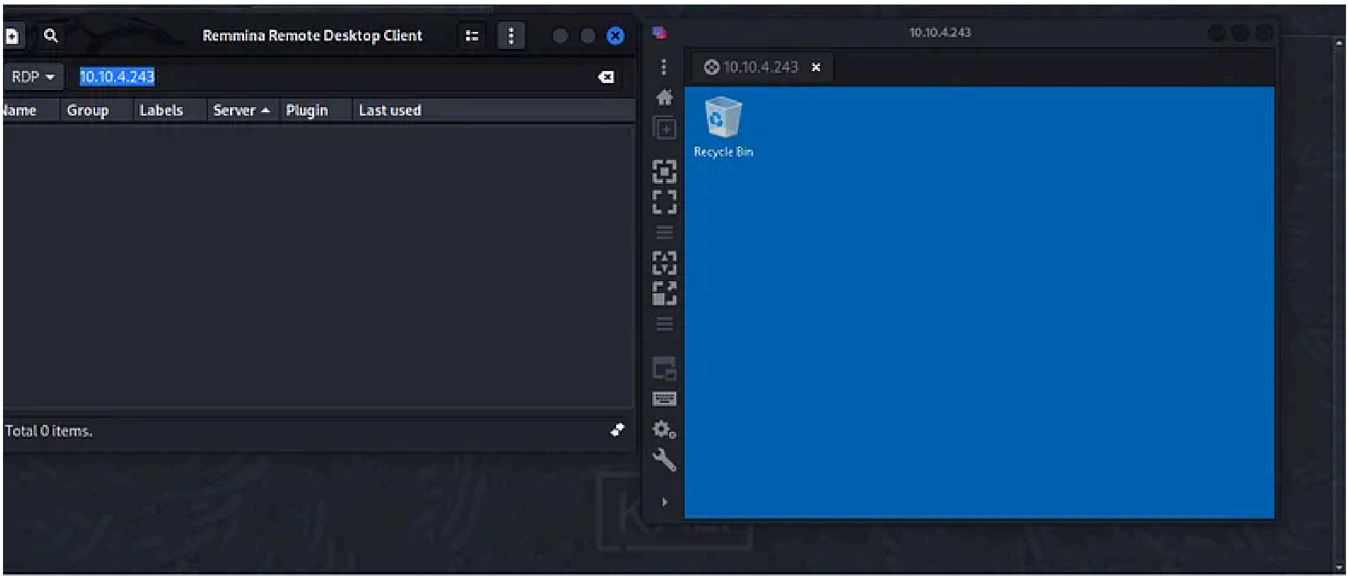
A Real-World Example

If this sounds a bit confusing, chances are that you have already interacted with a Windows domain at some point in your school, university, or work.

In school/university networks, you will often be provided with a username and password that you can use on any of the computers available on campus. Your credentials are valid for all machines because whenever you input them on a machine, it will forward the authentication process back to the Active Directory, where your credentials will be checked. Thanks to Active Directory, your credentials don't need to exist in each machine and are available throughout the network.

Active Directory is also the component that allows your school/university to restrict you from accessing the control panel on your school/university machines. Policies will usually be deployed throughout the network so that you don't have administrative privileges over those computers.

I have used ***Remmina*** *a Kali tool to enter the* ***THM.local*** *using the* ***RDP*** *port.* ***Username:*** *Administrator* ***Password:*** *Password321*



The RDP server

Task 3: Active Directory:

Which group normally administrates all computers and resources in a domain?

Answer: *Domain Admin*

What would be the name of the machine account associated with a machine named TOM-PC?

Answer: *TOM-PC$*

Suppose our company creates a new department for Quality Assurance. What type of containers should we use to group all Quality Assurance users so that policies can be applied consistently to them?

Answer: *Organizational unit*

Note:

The ***core*** *of any* ***Windows Domain*** *is the* ***Active Directory Domain Service (AD DS)****. This* ***service acts as a catalog*** *that holds the* ***information of all of the "objects" that exist on your network.*** *Amongst the many objects supported by AD, we have* ***users, groups, machines, printers, shares, and many others.*** *Let's look at some of them:*

Users

Users are one of the most common object types in Active Directory*. Users are one of the* ***objects*** *known as* ***security principals****, meaning that they can be* ***authenticated*** *by the* ***domain and can be assigned privileges over resources like files or printer****s. You could say that a* ***security principal is an object*** *that can* ***act upon resources in the network.***

Users can be used to represent two types of entities:

- ***People: users will generally represent persons** in your **organization** that need to access the network, like **employees.***
- ***Services:** you can also **define users to be used by services like IIS or MSSQL**. Every single service requires a **user to run,** but **service users** are different from **regular users** as they will only have the **privileges needed to run their specific service. (Here the users are not like normal users meaning this type of user account is created for running a particular service or application on the Windows operating system. This kind of account is by default account already created in the operating system. But any person can create a service account if needed. Example: allows accounts to start network services or services that run continuously on a computer, even when no one is logged on to the console)***

Machines (**A computer account represents your desktop or laptop to the active directory. There is an account name and an account ID associated with your computer account**)

*Machines are another type of **object** within **Active Directory**; for **every computer that joins** the Active Directory domain, a **machine object will be created**. Machines are also considered "**security principals**" and are assigned an account just as any regular user. This account has **somewhat limited rights within the domain itself.***

*The machine accounts themselves are **local administrators o**n the assigned computer, they are generally not supposed to be accessed by anyone except the **computer itself**, but **as with any other account**, if you have the password, you can use it to log in.*

***Note: Machine Account passwords** are **automatically rotated** out and are generally **comprised of 120 random characters**.*

*Identifying machine accounts is **relatively easy**. They follow a **specific naming scheme**. The machine account name is the computer's name followed by a dollar sign. **For example, a machine named `DC01` will have a machine account called `DC01$` .***

Security Groups

*If you are familiar with **Windows,** you probably know that you can define user **groups to assign access rights to files or other resources to entire groups instead of single users**. This allows for better manageability as you can add users to an existing group, and they* *will automatically inherit all of the group's privileges. Security groups are also considered security principals and, therefore, can have privileges over resources on the network.*

Groups can have both users and machines as members. If needed, groups can include other groups as well.

Several groups are created by default in a domain that can be used to grant specific privileges to users. As an example, here are some of the most important groups in a domain:

Domain Admins: *Users of this group have* ***administrative privileges*** *over the* ***entire domain****. By default, they can* ***administer any computer on the domain, including the DCs****.*

Server Operators: *Users in this group can* ***administer Domain Controllers. They cannot change any administrative group memberships.***

Backup Operators: *Users in this group* ***are allowed to access any file, ignoring their permissions****. They are* ***used to perform backups of data on computers****.*

Account Operators: Users in this group can create or modify other accounts in the domain.

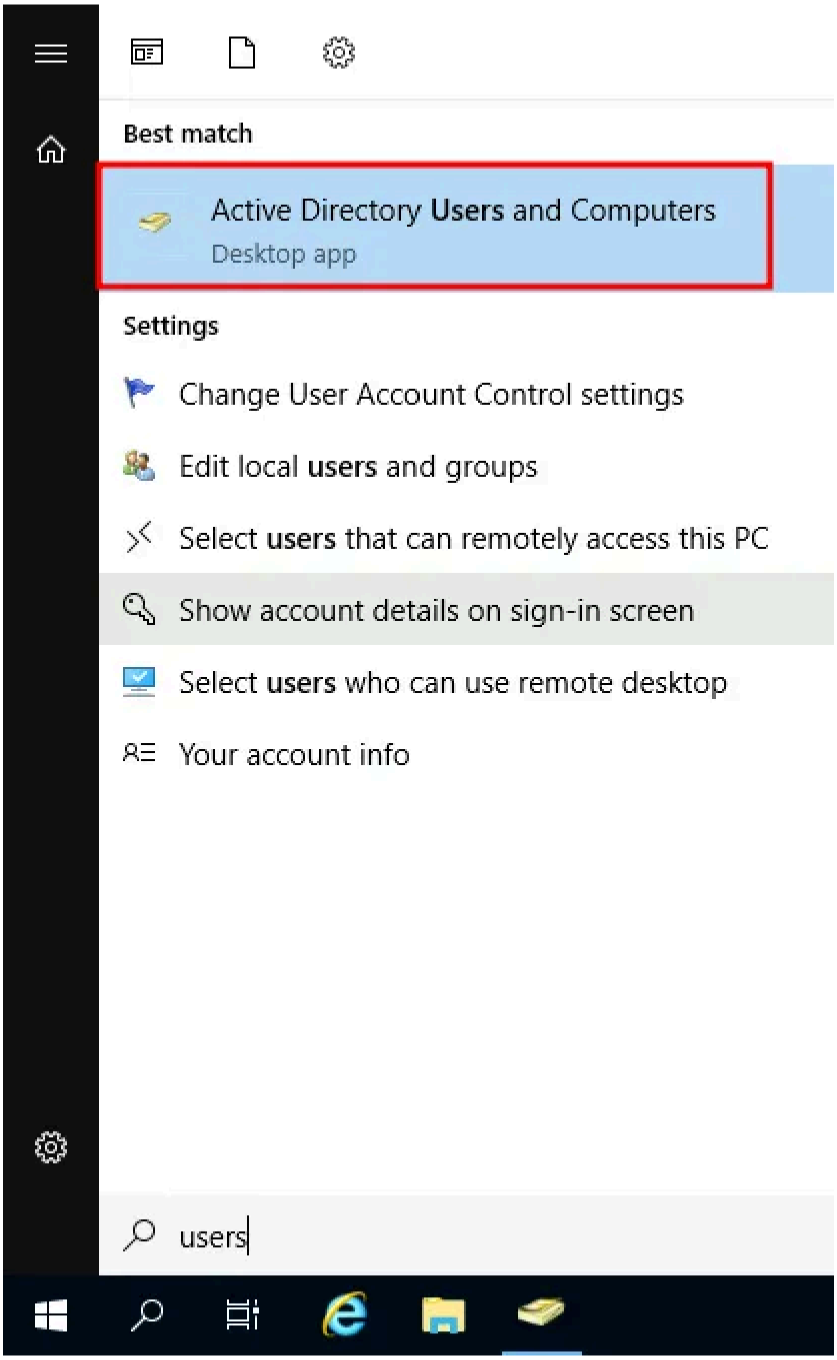
Domain Users: *Includes* ***all existing user accounts in the domain****.*

Domain Computers: *Includes all existing* ***computers in the domain****.*

Domain Controllers: *Includes all* ***existing DCs on the domain****.*

Active Directory Users and Computers

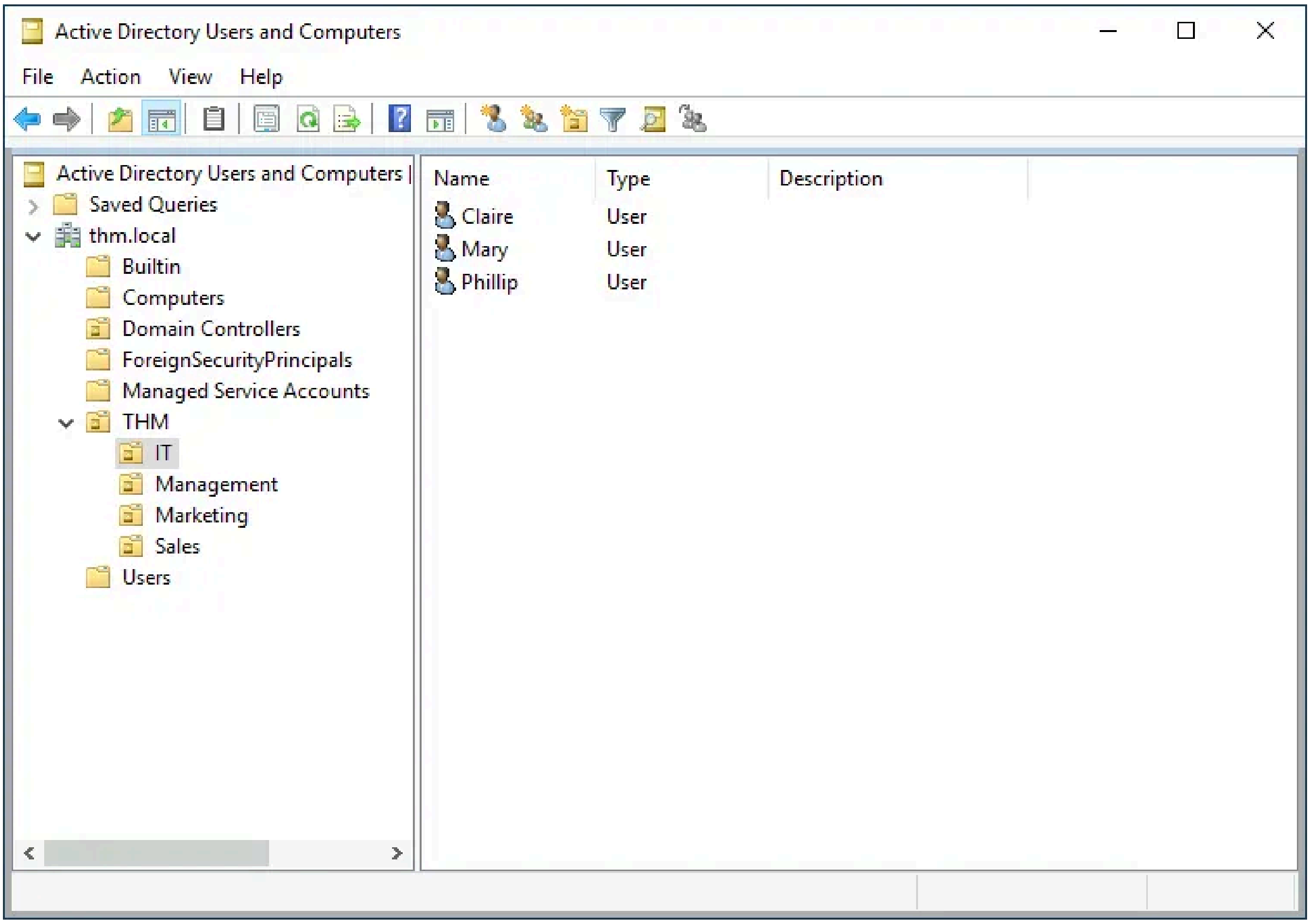
To configure users, groups, or machines in Active Directory, we need to log in to the ***Domain Controller and run "Active Directory Users and Computers" from the start menu:***


Best match
Active Directory Users and Computers
Desktop app
Settings
Change User Account Control settings
Edit local users and groups
Select users that can remotely access this PC
Show account details on sign-in screen
Select users who can use remote desktop
Your account info
users

This will open up a window where you can see the ***hierarchy of users, computers, and groups that exist in the domain.*** *These objects are organized in* ***Organizational Units*** *(OUs) which are* ***container objects that allow you to classify users and machines(OUs are a group where all different groups are kept separately inside which means all groups are the child of the OU group, but each group is also called OU separately).*** *OUs are mainly used to define* ***sets of users with similar policing requirements.*** *The people in the Sales department of your organization are likely to have a different set of policies applied than the people in IT, for example. Keep in mind that a user can only be a part of a single OU at a time.*

Checking our machine, we can see that there is already an ***OU called `THM` with four child OUs for the IT, Management, Marketing, and Sales departments.*** *It is very typical to see* *the OUs mimic the business' structure, as it allows for efficiently deploying baseline policies that apply to entire departments. Remember that while this would be the expected model most of the time, you can define OUs arbitrarily. Feel free to right-click the* `THM` *OU and create a new OU under it called* `Students` *just for the fun of it.*

If you open any OUs, you can see the users they contain and perform simple tasks like creating, deleting, or modifying them as needed. You can also reset passwords if needed (pretty useful for the helpdesk):



Name	Type	Description
Claire	User	
Mary	User	
Phillip	User	

You probably noticed already that there are other default containers apart from the THM OU. These containers are created by Windows automatically and contain the following:

- ***Builtin: Contains default groups available to any Windows host.***
- ***Computers:*** *Any* ***machine joining the network will be put here by default****. You can move them if needed.*
- ***Domain Controllers: Default OU that contains the DCs in your network.***
- ***Users:*** *Default users and groups that apply to a domain-wide context.*

- ***Managed Service Accounts:** Holds accounts used by services in your Windows domain.*

Security Groups vs OUs

You are probably wondering why we have both groups and OUs. While both are used to classify users and computers, their purposes are entirely different:

- ***OUs** are handy for **applying policies** to **users and computers**, which include **specific configurations** that pertain to sets of users depending on their particular role in the enterprise. Remember, **a user can only be a member of a single OU at a time**, as it wouldn't make sense to try to apply two different sets of policies to a single user.*
- ***Security Groups**, on the other hand, are used to **grant permissions over resources.** For example, you will use groups if you want to allow some users to access a shared folder or network printer. A **user can be a part of many groups, which is needed to grant access to multiple resources.***

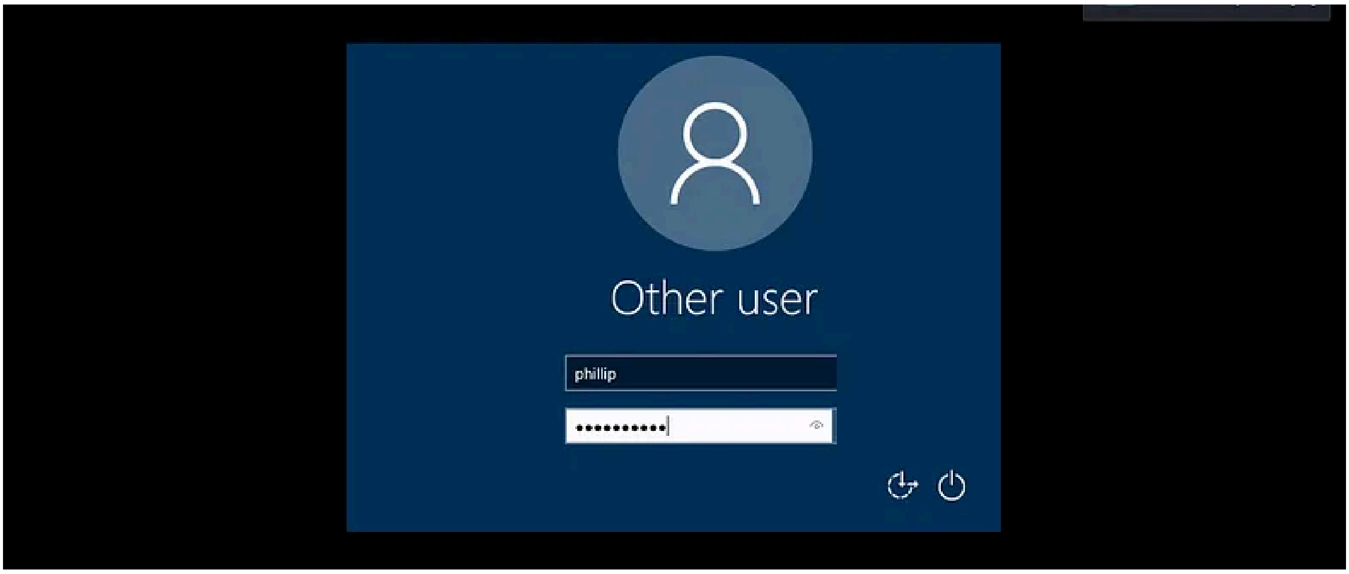
Task 4: Managing Users in AD:

What was the flag found on Sophie's desktop?

***Answer:** THM{thanks_for_contacting_support}*

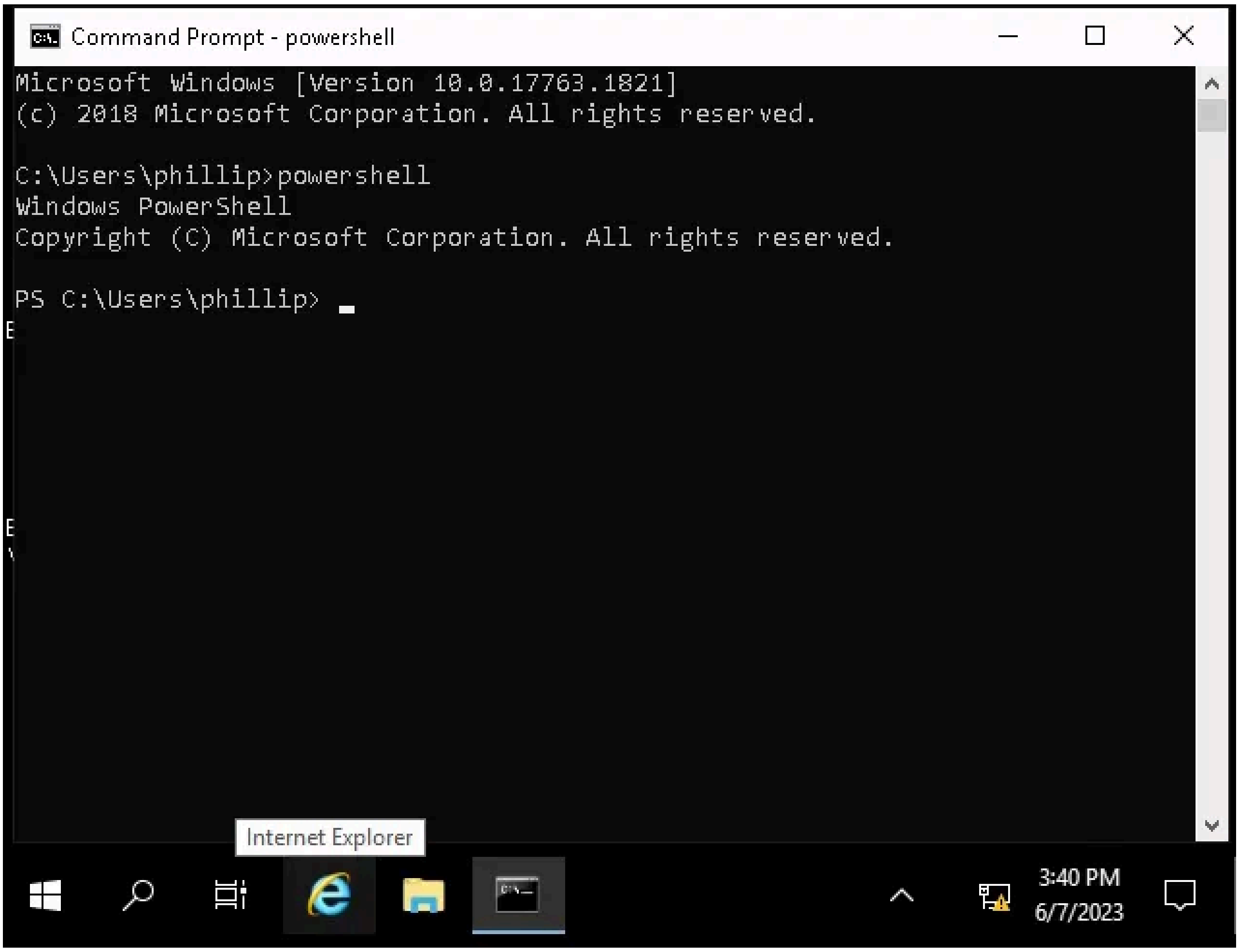
Note:

*After the **delegation** enter the **Phillips** account by using remmina using the RDP port. Username and password: **phillip: Claire2008***



The RDP screen

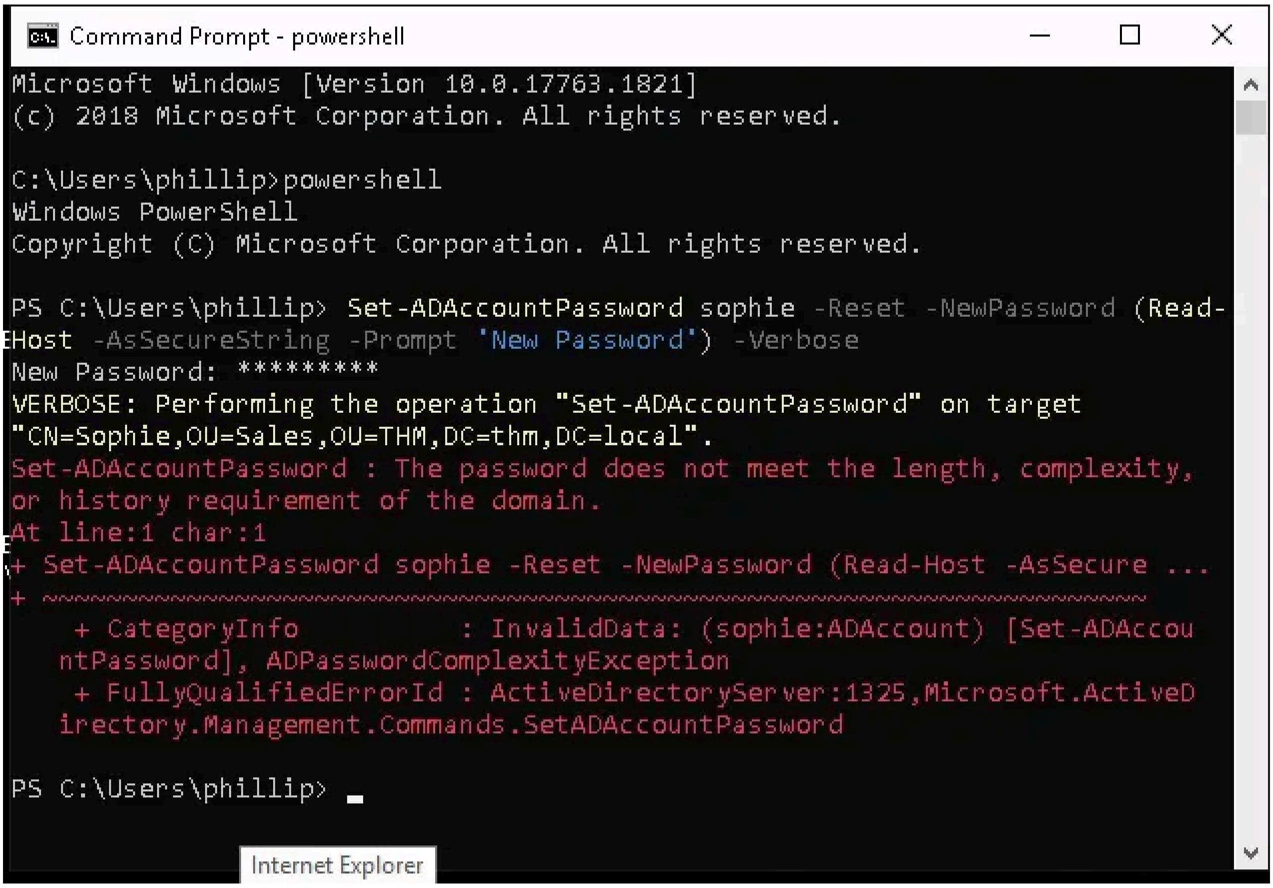
Inside the Phillip, account open the ***Command prompt*** *and transfer it to PowerShell using* ***Command:*** *powershell in* ***cmd.***



```
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\phillip>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\phillip> _
```

The cmd to PowerShell

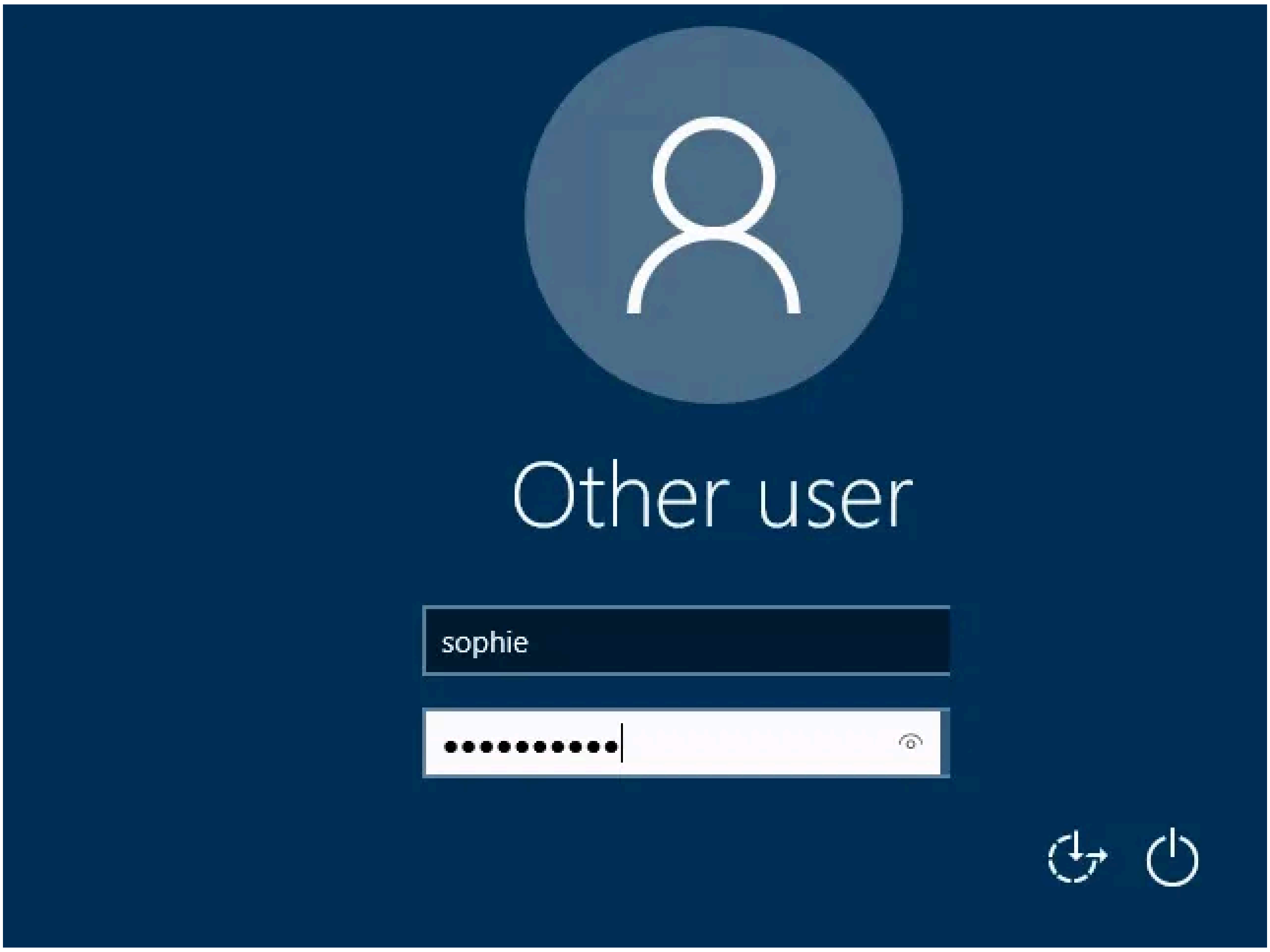
Now to set the password type this command: ***Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password') -Verbose***



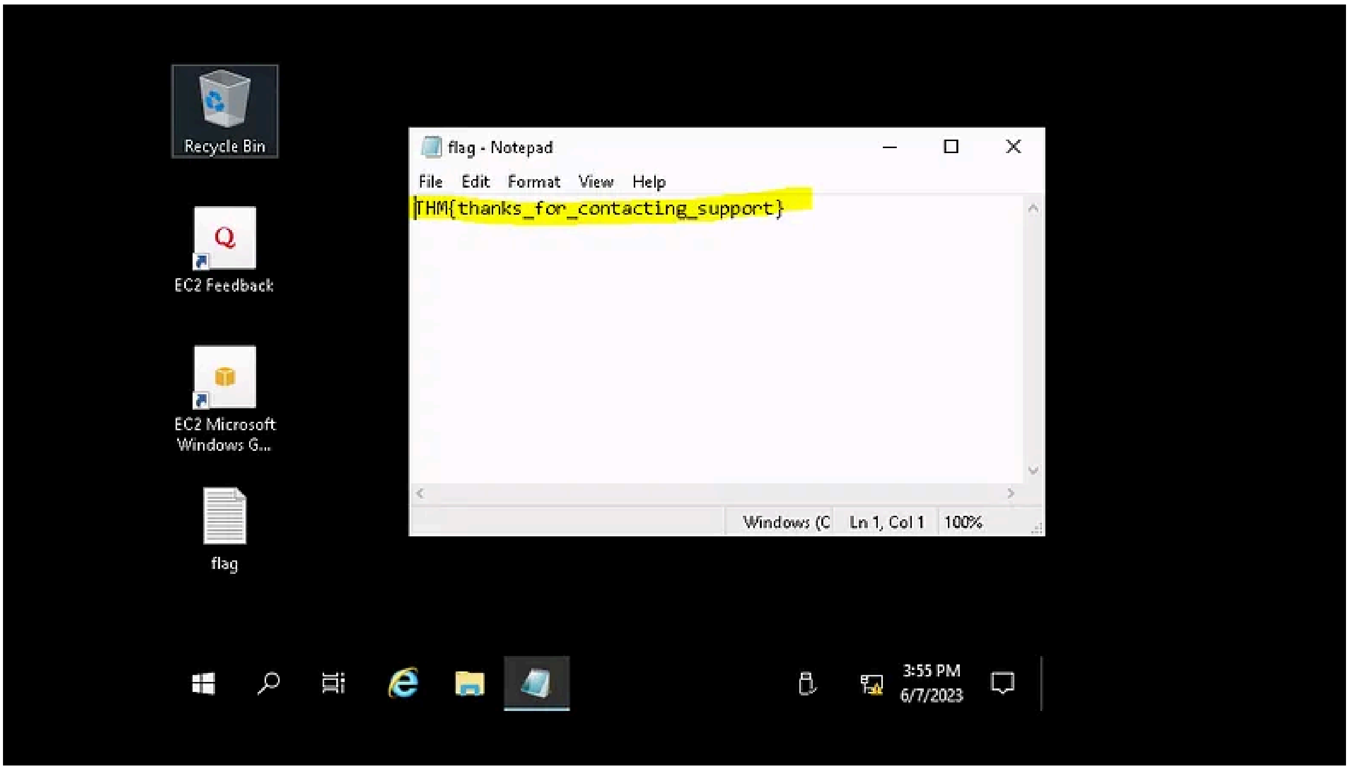
```
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\phillip>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\phillip> Set-ADAccountPassword sophie -Reset -NewPassword (Read-
Host -AsSecureString -Prompt 'New Password') -Verbose
New Password: *********
VERBOSE: Performing the operation "Set-ADAccountPassword" on target
"CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
Set-ADAccountPassword : The password does not meet the length, complexity,
or history requirement of the domain.
At line:1 char:1
+ Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecure ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidData: (sophie:ADAccount) [Set-ADAccou
   ntPassword], ADPasswordComplexityException
    + FullyQualifiedErrorId : ActiveDirectoryServer:1325,Microsoft.ActiveD
   irectory.Management.Commands.SetADAccountPassword

PS C:\Users\phillip> _
```

The password set

Here I have set the password: ***abcD12345****



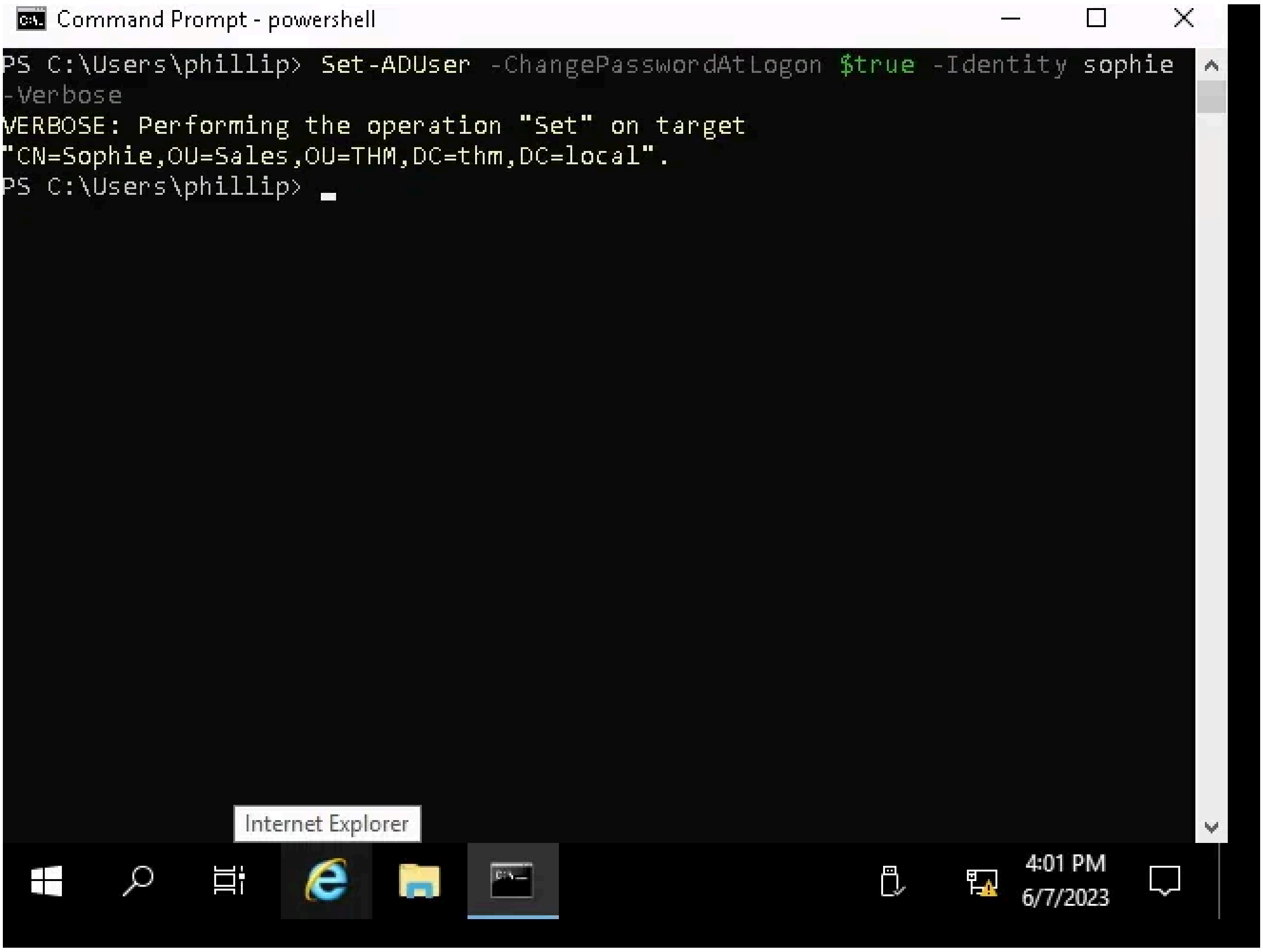
Entering the account


Recycle Bin
EC2 Feedback
EC2 Microsoft Windows G...
flag
flag - Notepad
File Edit Format View Help
Windows (C Ln 1, Col 1 100%
3:55 PM
6/7/2023

THM{thanks_for_contacting_support}

The flag

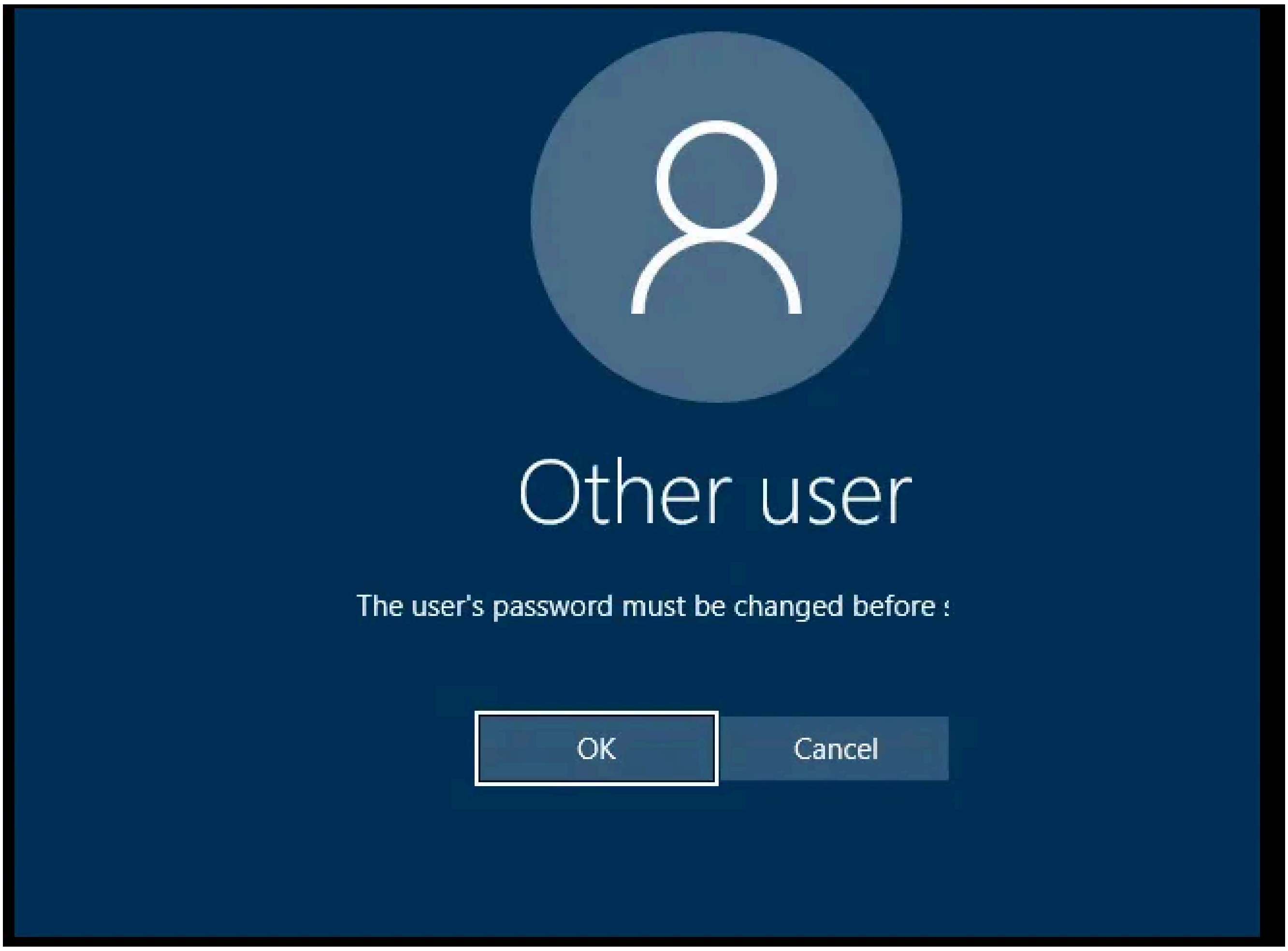
Now we have taken the flag. So we do not want Sophie to use our given password. We will force Sophie's account to ***show a reset option when Sophie will log into her account. The reset option showing process will be done from the Phillips account using this*** *command:* ***Set-ADUser -ChangePasswordAtLogon $true -Identity sophie -Verbose***



```
PS C:\Users\phillip> Set-ADUser -ChangePasswordAtLogon $true -Identity sophie
-Verbose
VERBOSE: Performing the operation "Set" on target
"CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
PS C:\Users\phillip> _
```

Reseting the password

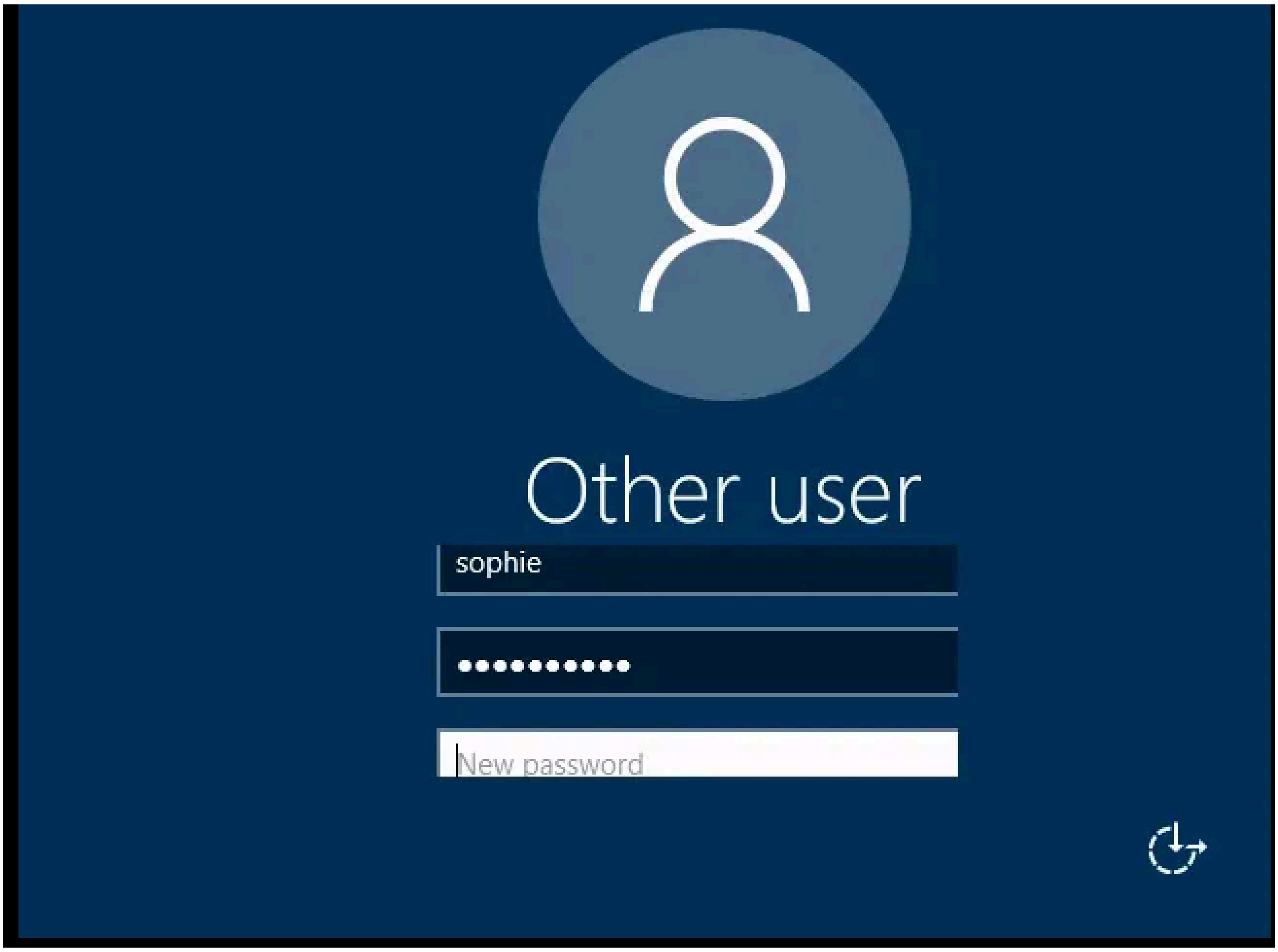
Now see that you cannot enter Sophie's account using the password you provided to get the flag. See that the password reset option has been shown.



Other user

The user's password must be changed before s

Click ok



Other user

sophie

●●●●●●●●●●

The new password option

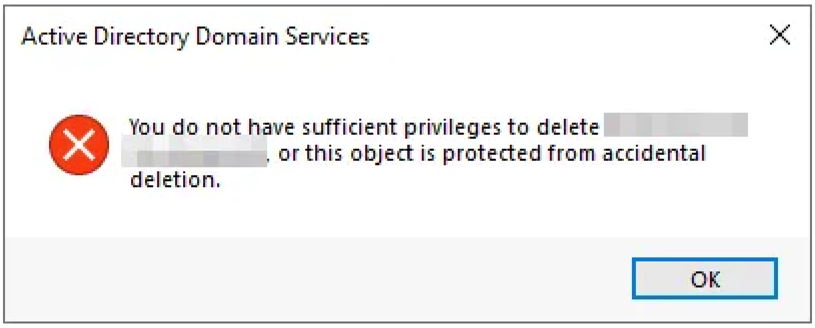
The process of granting privileges to a user over some OU or other AD Object is called…

Answer: *delegation*

Note:
Your first task as the new domain administrator is to check the existing AD OUs and users, as some recent changes have happened to the business. You have been given the following organizational chart and are expected to make changes to the AD to match it:

Deleting extra OUs and users

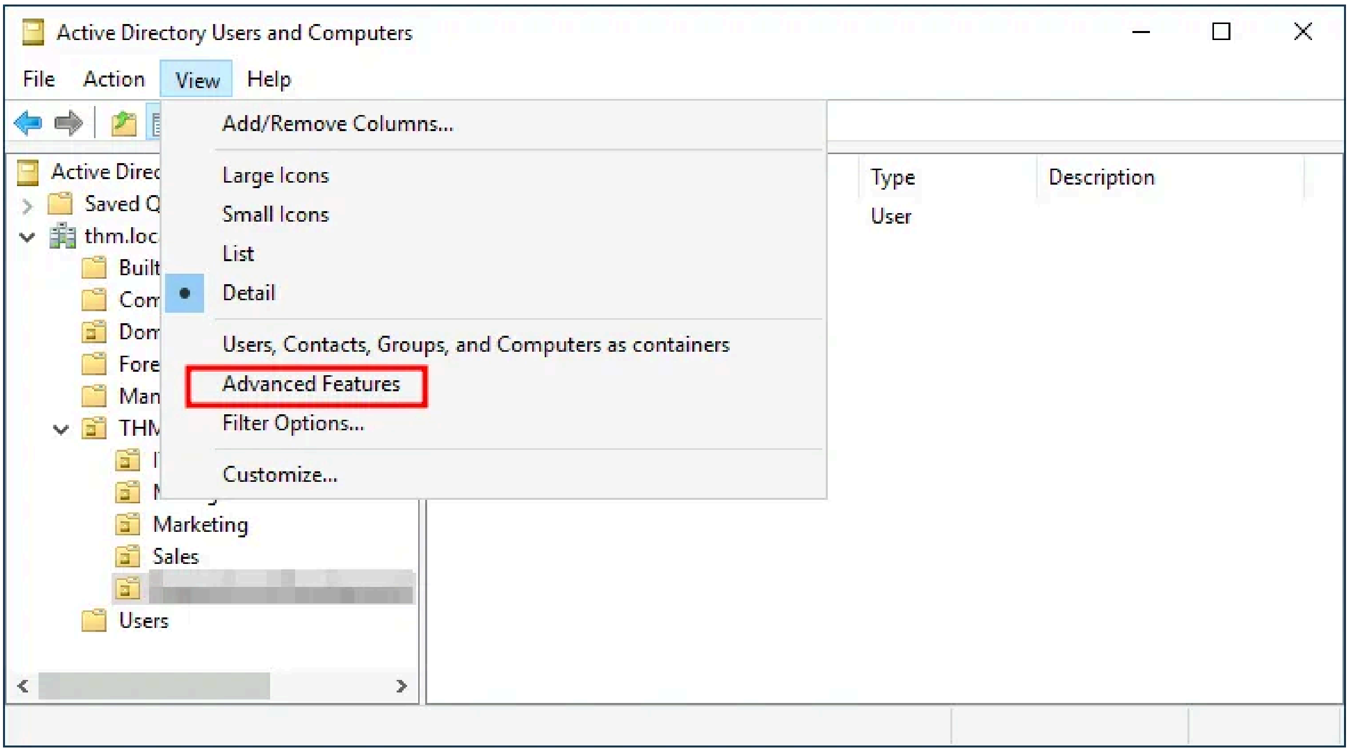
The first thing you should notice is that there is an additional department OU in your current AD configuration that doesn't appear in the chart. We've been told it was closed due to budget cuts and should be removed from the domain. If you try to right-click and delete the OU, you will get the following error:



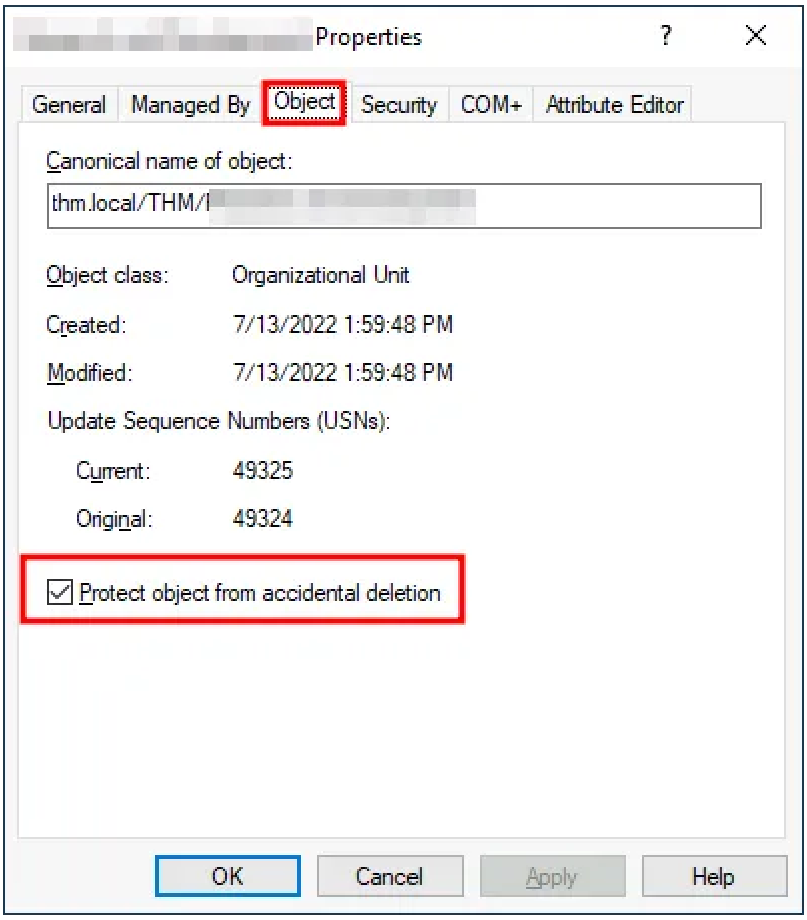
Active Directory Domain Services

You do not have sufficient privileges to delete [redacted] [redacted], or this object is protected from accidental deletion.

By default, OUs are protected against accidental deletion. To delete the OU, we need to enable the ***Advanced Features*** *in the View menu:*



This will show you some additional containers and enable you to disable the accidental deletion protection. To do so, right-click the OU and go to Properties. You will find a checkbox in the Object tab to disable the protection:



Canonical name of object: thm.local/THM/[redacted]

Object class: Organizational Unit

Created: 7/13/2022 1:59:48 PM

Modified: 7/13/2022 1:59:48 PM

Update Sequence Numbers (USNs):

Current: 49325

Original: 49324

☑ Protect object from accidental deletion

Be sure to uncheck the box and try deleting the OU again. You will be prompted to confirm that you want to delete the OU, and as a result, any users, groups, or OUs under it will also be deleted.

After deleting the extra OU, you should notice that for some of the departments, the users in the AD don't match the ones in our organizational chart. Create and delete users as needed to match them.

Delegation (Example: A member of an IT support group can change the username and password of the other group's low-privilege members from his account because this power is given to him by the organization using the delegate control option of the target OU in the Active directory)

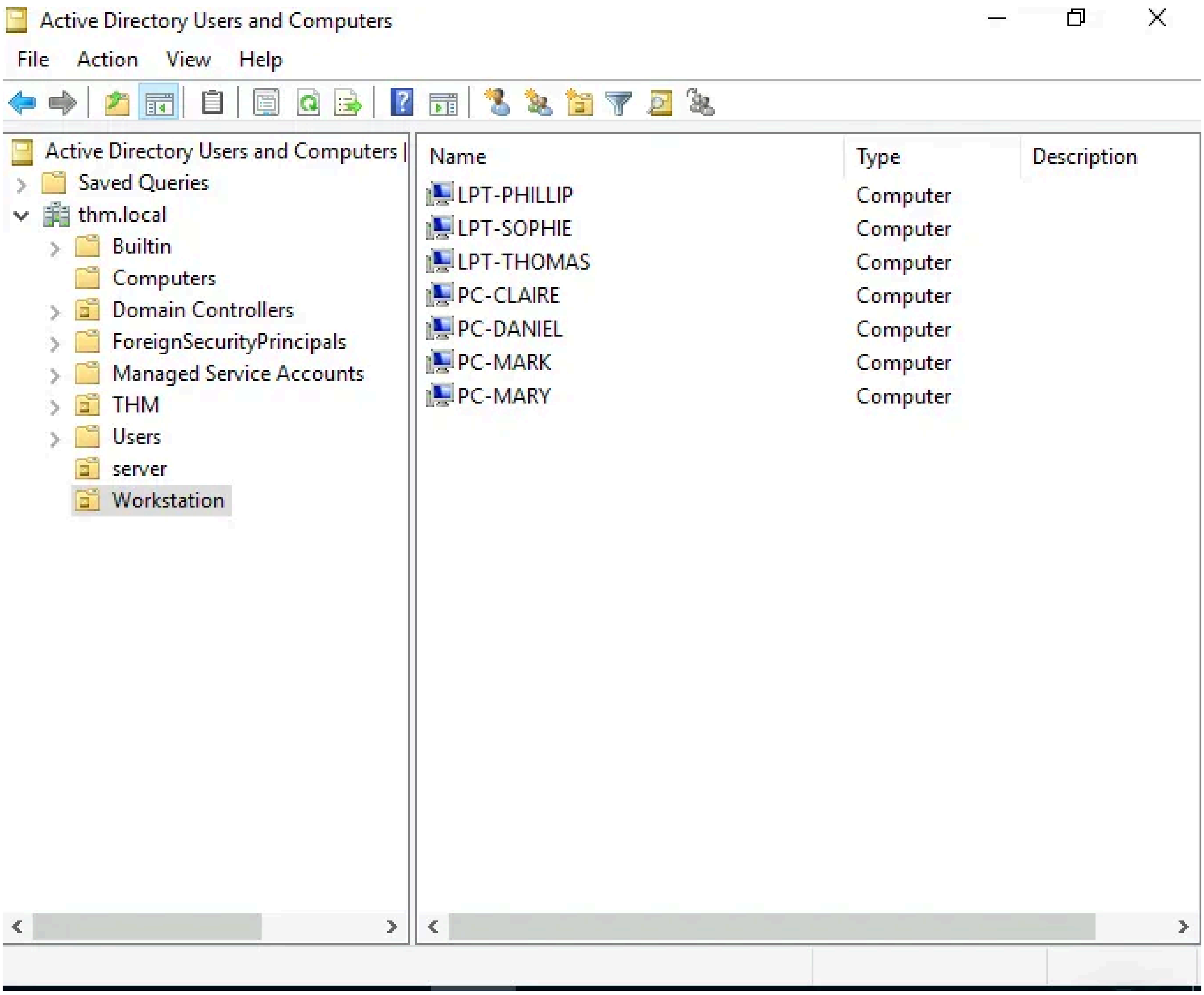
One of the nice things you can do in ***AD*** *is to give* ***specific users some control over some OUs****. This process is known as* ***delegation*** *and allows you to grant users* ***specific privileges*** *to perform* ***advanced*** *tasks on OUs without needing a* ***Domain Administrator*** *to step in.*

One of the most common use cases for this is granting `IT support` *the privilege to reset other low-privilege users' passwords. According to our organizational chart, Phillip is in charge of IT support, so we'd probably want to delegate the control of resetting passwords over the Sales, Marketing, and Management OUs to him.*

Task 5: Managing Computers in AD:

After organizing the available computers, how many ended up in the Workstations OU?

Answer: *7*



Active Directory Users and Computers
- Saved Queries
- thm.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - THM
  - Users
  - server
  - Workstation

Name	Type	Description
LPT-PHILLIP	Computer	
LPT-SOPHIE	Computer	
LPT-THOMAS	Computer	
PC-CLAIRE	Computer	
PC-DANIEL	Computer	
PC-MARK	Computer	
PC-MARY	Computer	

The workstation

Is it recommendable to create separate OUs for Servers and Workstations? (yay/nay)

Answer: yay

Task 6: Group Policies:

What is the name of the network share used to distribute GPOs to domain machines?

Answer: SYSVOL

Can a GPO be used to apply settings to users and computers? (yay/nay)

Answer: Yay

Task 7: Authentication Methods:

Will a current version of Windows use NetNTLM as the preferred authentication protocol by default? (yay/nay)

Answer: nay

When referring to Kerberos, what type of ticket allows us to request further tickets known as TGS?

Answer: *Ticket Granting Ticket*

When using NetNTLM, is a user's password transmitted over the network at any point? (yay/nay)

Answer: *nay*

Note:

When using Windows domains, all credentials are stored in the Domain Controllers. Whenever a user tries to authenticate to a service using domain credentials, the service will need to ask the Domain Controller to verify if they are correct. ***Two protocols*** *can be used for network authentication in Windows domains:*

- ***Kerberos:*** *Used by any recent version of Windows. This is the default protocol in any recent domain.*
- ***NetNTLM:*** *Legacy authentication protocol kept for compatibility purposes.*

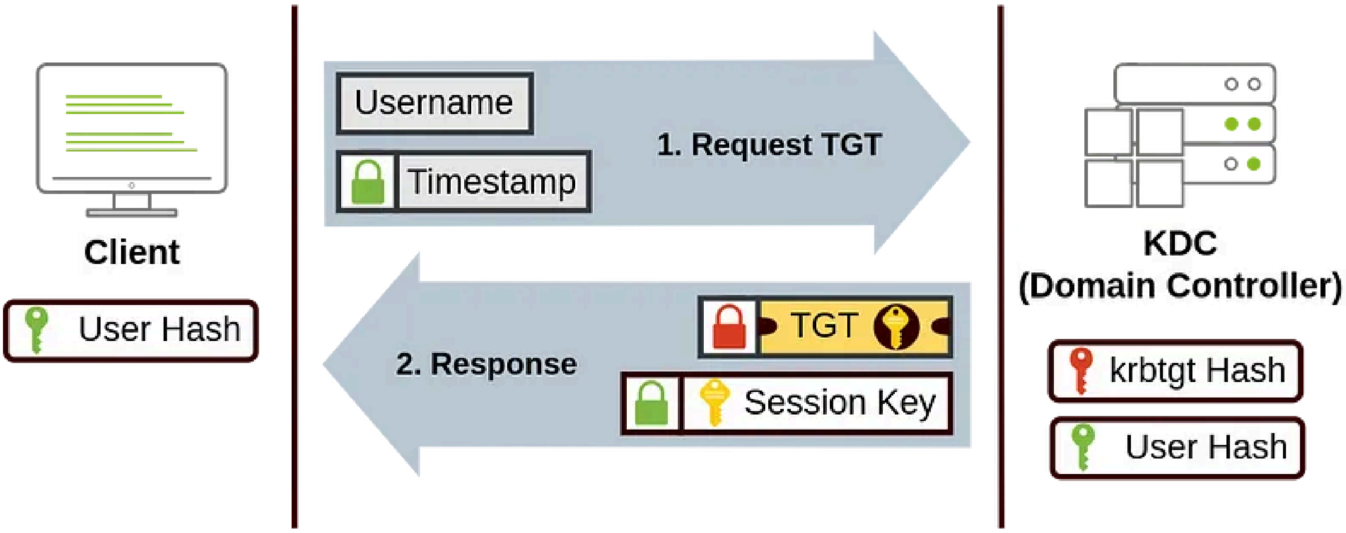
While NetNTLM should be considered obsolete, most networks will have both protocols enabled. Let's take a deeper look at how each of these protocols works.

When Kerberos is used for authentication, the following process happens:

1. *The user sends their* ***username and a timestamp*** *encrypted using a key derived from their password to the* ***Key Distribution Center (KDC)****, a service usually installed on the* ***Domain Controller in charge of creating Kerberos tickets on the network.***

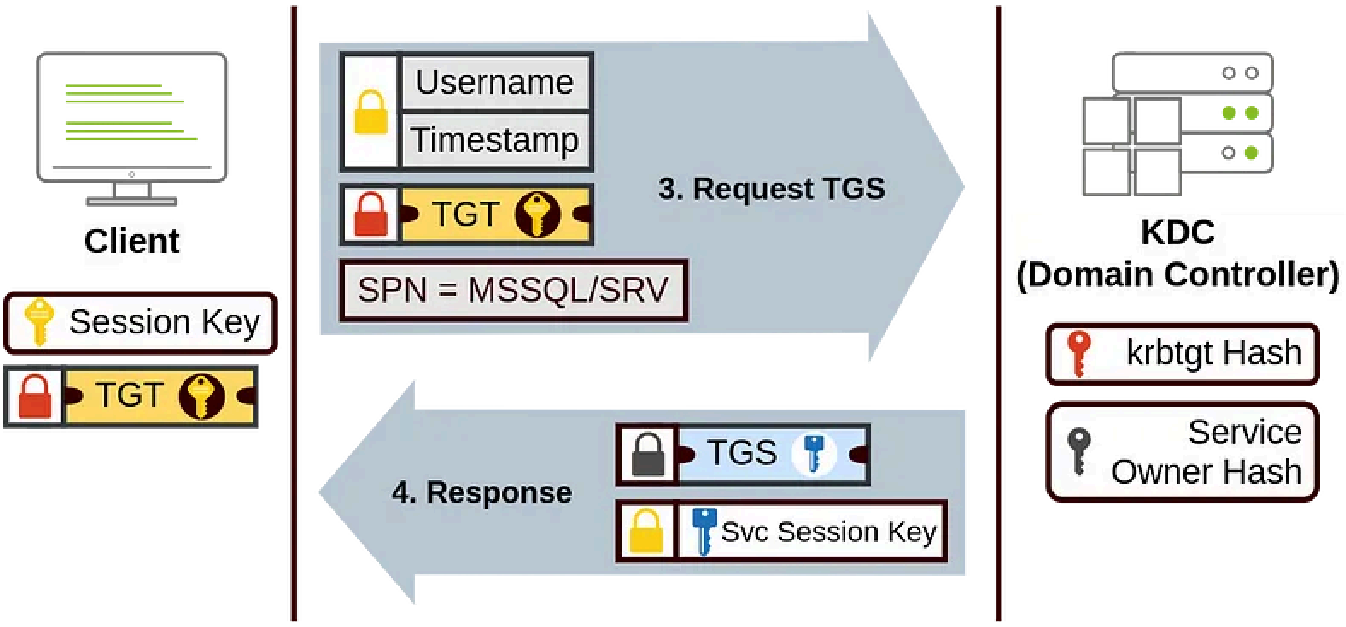
The KDC will ***create and send*** *back a* ***Ticket Granting Ticket (TGT)****, which will allow the* ***user to request additional tickets to access specific services****. The need for a* ***ticket*** *to get more tickets may sound a bit weird, but it allows users to request service tickets without passing their credentials every time they want to connect to a service. Along with the TGT, a* ***Session Key*** *is given to the user, which they will need to generate the following requests.*

Notice the TGT is encrypted using the ***krbtgt*** *account's password hash, and therefore the user can't access its contents. It is essential to know that the encrypted TGT includes a copy of the Session Key as part of its contents, and the KDC has no need to store the Session Key as it can recover a copy by decrypting the TGT if needed.*

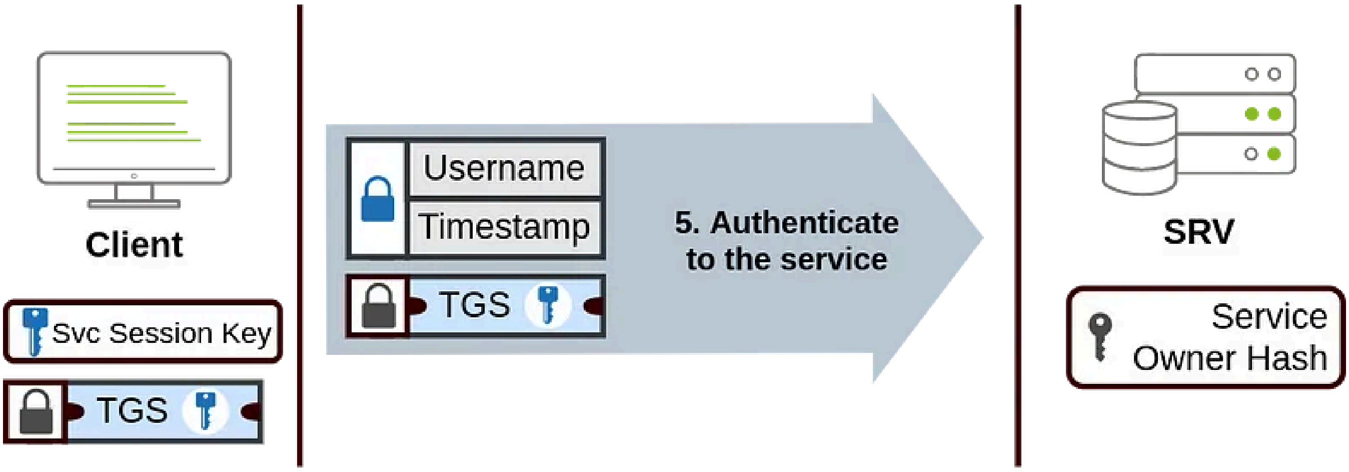


2. When a user wants to connect to a service on the network like a share, website, or database, they will use their TGT to ask the KDC for a ***Ticket Granting Service (TGS)****. TGS are tickets that allow connection only to the specific service they were created for. To request a TGS, the user will send their username and a timestamp encrypted using the Session Key, along with the TGT and a* ***Service Principal Name (SPN),*** *which indicates the service and server name we intend to access.*

As a result, the KDC will send us a TGS along with a ***Service Session Key****, which we will need to authenticate to the service we want to access. The TGS is encrypted using a key derived from the* ***Service Owner Hash****. The Service Owner is the user or machine account that the service runs under. The TGS contains a copy of the Service Session Key on its encrypted contents so that the Service Owner can access it by decrypting the TGS.*

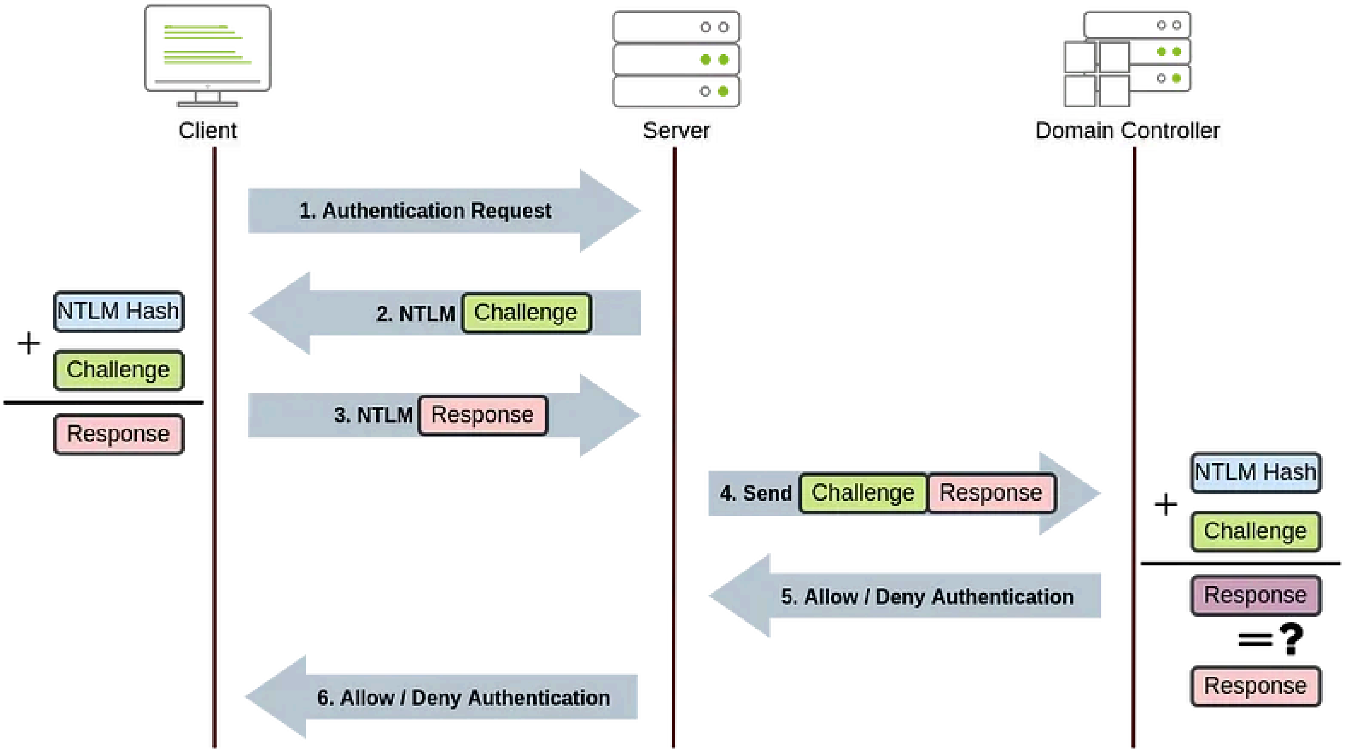


3. The TGS can then be sent to the desired service to authenticate and establish a connection. The service will use its configured account's password hash to decrypt the TGS and validate the Service Session Key.



NetNTLM*(The NTLM hash is the cryptographic format in which user passwords are stored on Windows systems.)* ***Authentication***

NetNTLM works using a challenge-response mechanism. The entire process is as follows:



1. *The client sends an* ***authentication request*** *(the* ***domain name*** *and the* ***username*** *)to the server they want to access.*

2. *The server generates a* ***random number and sends it as a challenge to the client.***

3. *The client combines their* ***NTLM password hash with the challenge (and other known data) to generate a response to the challenge and sends it back to the server for verification.***

4. *The* ***server forwards the challenge and the response to the Domain Controller for verification.***

5. *The domain controller uses the challenge to* ***recalculate*** *the response and* ***compares it to the original response sent by the client****. If they both match, the client is authenticated; otherwise, access is denied. The authentication result is sent back to the server.*

6. ***The server forwards the authentication result to the client.***

Note that the user's password (or hash) is never transmitted through the network for security.

Note: *The described process applies when* ***using a domain account****. If a local* ***account is used, the server can verify the response to the challenge itself without requiring interaction with the domain controller*** *since it has the* ***password hash stored locally on its SAM(security account manager).***

Task 8: Trees, Forests, and Trusts:

What is a group of Windows domains that share the same namespace called?

Answer: *tree*

What should be configured between two domains for a user in Domain A to access a resource in Domain B?

Answer: *2 trust relationship*

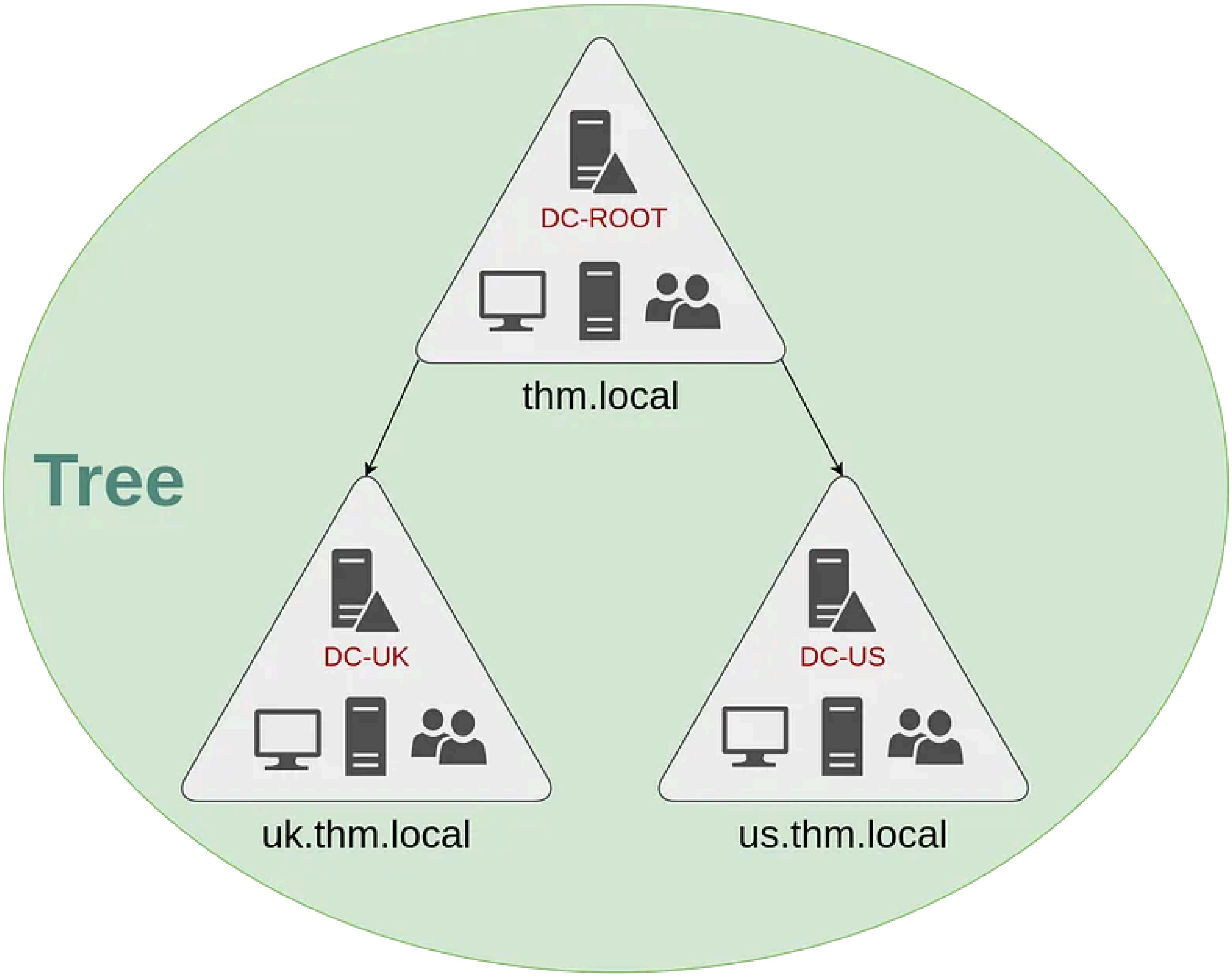
Note:

Trees

Imagine, for example, that suddenly your company ***expands to a new country****. The new country has different laws and regulations that require you to* ***update your GPOs to comply****. In addition,* ***you now have IT people in both countries****, and* ***each IT team needs to manage the resources that correspond to each country without interfering with the other team****. While you could create a* ***complex OU structure and use delegations*** *to* *achieve this, having a huge AD structure might be hard to manage and prone to human errors.*

Luckily for us, Active Directory supports ***integrating multiple*** *domains so that you can partition your network into units that can be managed independently. If you have* ***two domains*** *that share the same namespace (* `thm.local` *in our example), those domains can be joined into a* ***Tree****.*

If our `thm.local` *domain was split into* ***two subdomains for UK and US*** *branches, you could build a tree with* ***a root domain*** *of* `thm.local` *and two subdomains called* `uk.thm.local` *and* `us.thm.local` *, each with its AD, computers, and users:*

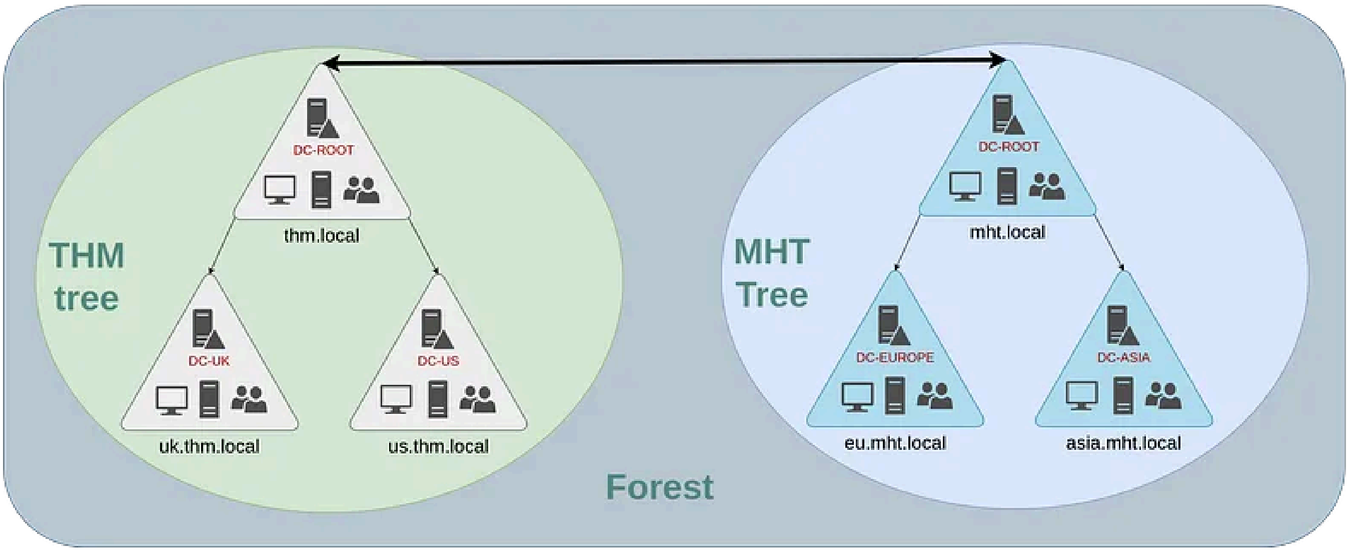


This partitioned structure gives us better control over who can ***access what in the domain.*** *The* ***IT people from the UK will have their own DC that manages the UK resources only****. For example, a UK user would not be able to manage US users. In that way,* ***the Domain Administrators of each branch will have complete control over their respective DCs****, but* *not other branches' DCs.* ***Policies can also be configured independently for each domain in the tree.***

A ***new security group*** *needs to be introduced when talking about* ***trees and forests****. The* ***Enterprise Admins*** *group will* ***grant a user administrative privileges over all of an enterprise's domains****(These enterprise admins can control the both UK and US domain controller). Each domain would still have its* ***Domain Admins with administrator privileges over their single domains*** *and the Enterprise Admins who can control everything in the enterprise.*

Forests

The ***domains you manage can also be configured in different namespaces****. Suppose your company continues* ***growing and eventually acquires another company called `MHT Inc`.*** *When* ***both companies merge, you will probably have different domain trees for each company, each managed by its own IT department. The union of several trees with different namespaces into the same network is known as a forest.***

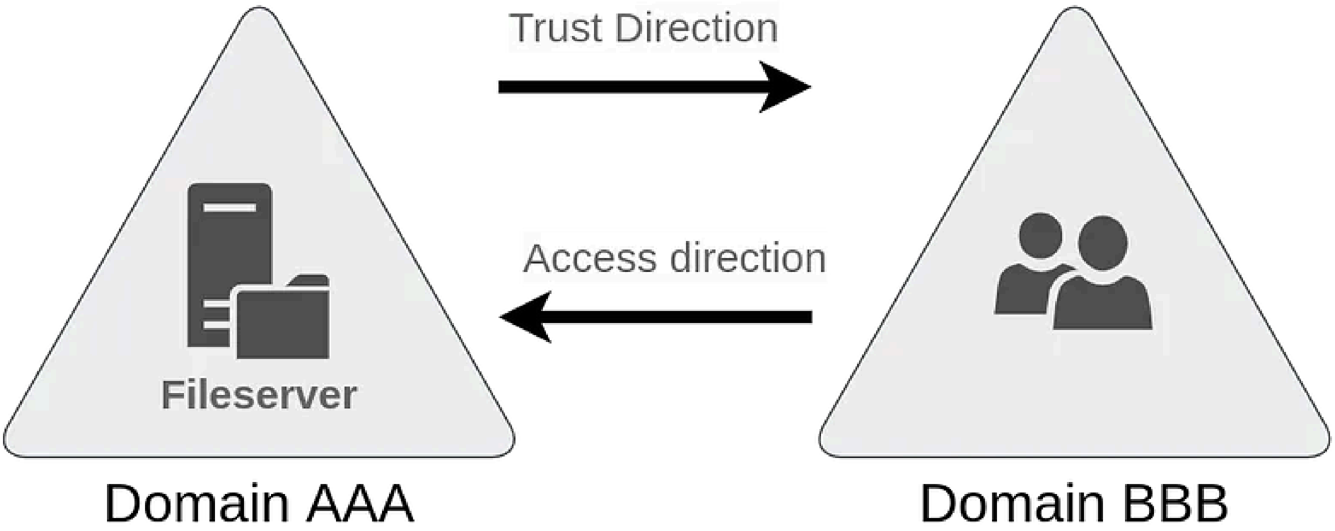


Trust Relationships

Having multiple domains ***organized in trees and forest allows you to have a nice compartmentalized network in terms of management and resources.*** *But* ***at a certain point, a user at THM UK might need to access a shared file in one of MHT ASIA servers.*** *For this to happen, domains arranged in trees and forests are joined together by* ***trust relationships****.*

In simple terms, having a trust relationship between domains allows you to authorize a user from a domain `THM UK` to access resources from the domain `MHT EU`.

The simplest trust relationship that can be established is a ***one-way trust relationship****. In a one-way trust,* ***if*** `Domain AAA` ***trusts*** `Domain BBB` ***, this means that a user on BBB can be authorized to access resources on AAA:***



The direction of the one-way trust relationship is contrary to that of the access direction.

Two-way trust relationships *can also be made* ***to allow both domains to mutually authorize users from the other****. By default,* ***joining several domains under a tree or a forest will form a two-way trust relationship.***

It is important to note that ***having a trust relationship between domains doesn't automatically grant access to all resources on other domains****. Once a trust relationship is established, you have the chance to authorised users across different domains, but it's up to you what is actually authorised or not.****(It means a trust relationship domains have minimum privileges which users can access/see on what kind of data/file.)***

So, Happy learning happy journey.

To get more interesting and detailed articles follow my blog

LinkedIn

Cybersecurity Networking Windows Penetration Testing Pentesting

Follow

Written by kawsar uddin

97 Followers · 18 Following

Completed BSC in Computer Science and Engineering in 2021 September. Passionate in the cyber security field.

No responses yet

What are your thoughts?

Respond

More from kawsar uddin

kawsar uddin

HTTP in detail — TryHackMe

Learn about how you request content from a web server using the HTTP protocol

May 19, 2023 👏 56

kawsar uddin

Vulnversity — TryHackMe Room

In this room, we will learn about active recon, web app attacks, and privilege escalation.

May 2, 2023 👏 53

kawsar uddin

Attacktive Directory — TryHackMe

In this room, we will learn about attacking the directories.

Jun 12, 2023 👏 6

kawsar uddin

Post-Exploitation Basics — TryHackMe

In this room, we will learn the basics of post-exploitation and maintaining access with mimikatz, bloodhound, powerview, and msfvenom

Jun 30, 2023 6 1

See all from kawsar uddin

Recommended from Medium

Infinite_Exploit

Hack The Box | HTB Season -7 | Backfire

We recently tackled the second machine of HackTheBox Season 7: “BackFire.” Although labeled as a medium-level Linux box, I’d rate it closer…

✦ 6d ago 3 1

MatSec

TryhackMe - Windows PowerShell | Cyber Security 101

Windows Powershell TryhackMe

Oct 24, 2024

Lists

Staff picks
804 stories · 1587 saves

Stories to Help You Level-Up at Work
19 stories · 925 saves

Self-Improvement 101
20 stories · 3244 saves

Productivity 101
20 stories · 2740 saves

In Offensive Black Hat Hacking & Security by Harshad Shah

Cybersecurity Roadmap 2025

How to start cybersecurity in 2025?

Dec 14, 2024 112 1

rutbar

TryHackMe—Search Skills | Cyber Security 101 (THM)

Evaluation of Search Results

✦ Oct 26, 2024 1

In System Weakness by Sunny Singh Verma [SuNnY]

Silver Platter TryHackMe Motion Graphics Writeup | Beginner Friendly | Detailed Walkthrough |…

A Detailed motion Graphics writeup for TryHackMe room Silver Platter

✦ Jan 13 50

Jasper Alblas

TryHackMe: Linux Privilege Escalation — Walkthrough

Welcome to this walkthrough on the Linux Privilege Escalation Room on TryHackMe, a Medium level room in which we get to practice privilege...

Nov 25, 2024 7

See more recommendations