TryHackMe Intro to Windows

Saikat Karmakar | AUG 19 : 2021

Windows file system and permissions explained

What is the file system?

It is the method and data structure that an operating system uses to keep track of files on a disk or partition. Without a file system, the information saved in a storage media would be one large body of data with no way to tell where the information begins and ends.

Windows file system structure is:

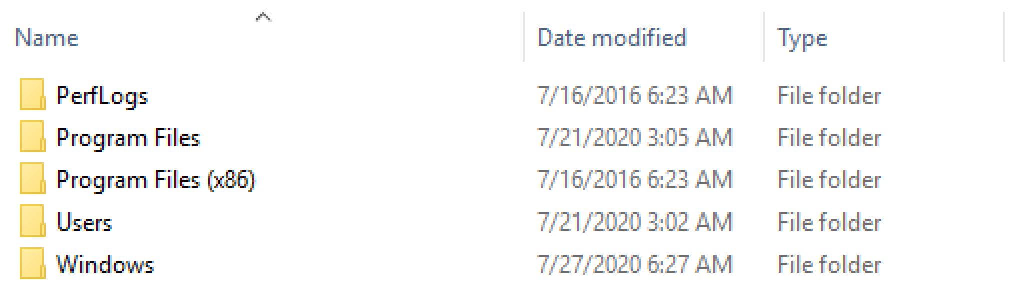
- Logical drives (Ex: Local Disk C)
- Folders (these are the folders that come by default. Ex: Documents, Downloads, Music)
- Files

Something that might also interest you would be the folders located on the C drive and their role. These folders are:

- PerfLogs
- Program Files
- Program Files (x86)
- Users
- Windows

Let me break them down and explain each of them:

1. PerfLogs - Stores the system issues and other reports regarding performance
2. Program Files and Program Files (x86) - Is the location where programs install unless you change their path (Ex: Choosing to install software on D drive)
3. Users - In this folder are stored the users created. It also stores users generated data (Ex: Saving a file on your Desktop)
4. Windows - It's the folder which basically contains the code to run the operating system and some utility tools (we'll talk about them later)



Name	Date modified	Type
PerfLogs	7/16/2016 6:23 AM	File folder
Program Files	7/21/2020 3:05 AM	File folder
Program Files (x86)	7/16/2016 6:23 AM	File folder
Users	7/21/2020 3:02 AM	File folder
Windows	7/27/2020 6:27 AM	File folder

File permissions

FIles permissions can be set by an administrator or a privileged account. These permissions can be applied to:

- Users
- Groups

Permissions that can be set are:

- Full control
- Modify
- Read & execute
- List folders content
- Read
- Write
- Special permissions

Full control - allows the user/users/group/groups to set the ownership of the folder, set permission for others, modify, read, write, and execute files.

Modify - allows the user/users/group/groups to modify, read, write, and execute files.

Read & execute - allows the user/users/group/groups to read and execute files.

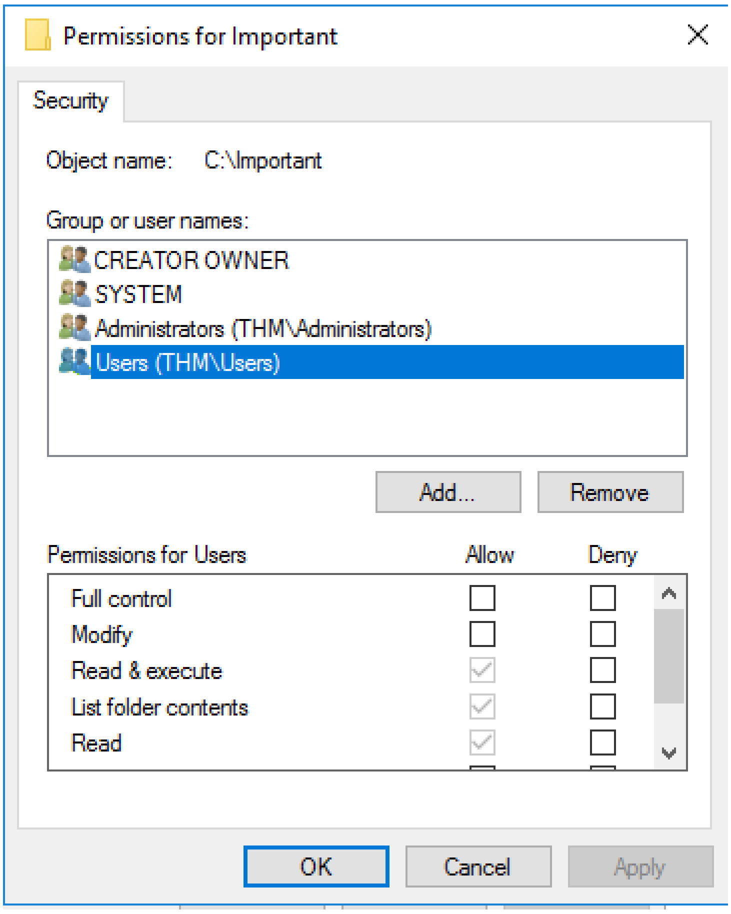
List folder contents - allows the user/users/group/groups to list the contents (files, subfolders, etc) of a folder.

Read - only allows the user/users/group/groups to read files.

Write - allows the user/users/group/groups to write data to the specified folder (automatically set when "Modify" right is checked).

Note: You can allow or deny permissions for users or groups.

To set permissions for a file or folder right click on the file and select "Properties". Go to the "Security" tab and click on the "Edit" button.



Permissions for Important

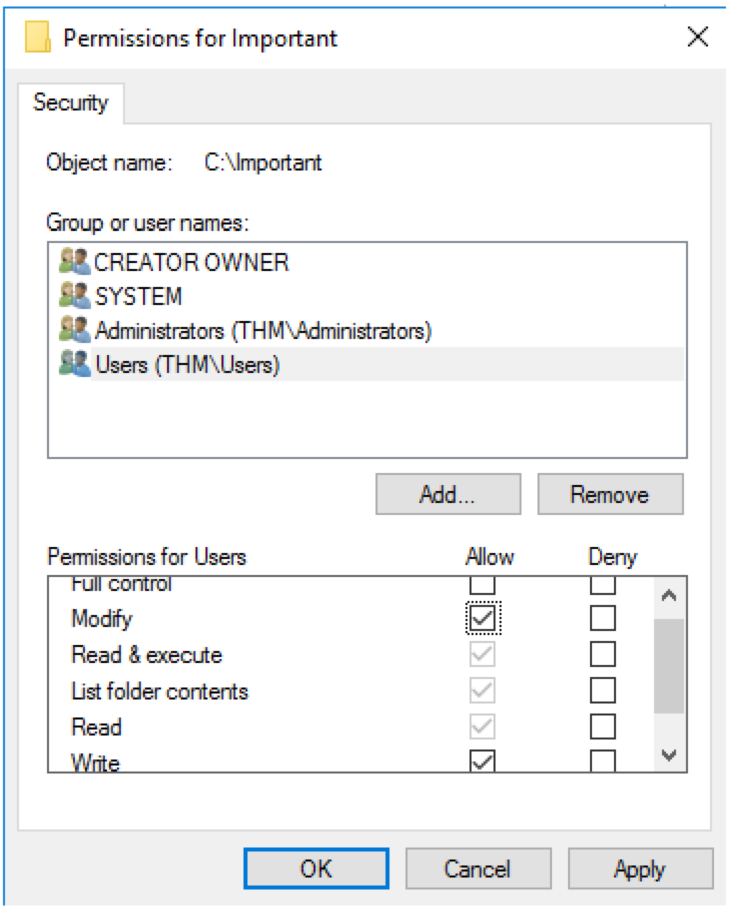
Object name: C:\Important

Group or user names:

CREATOR OWNER
SYSTEM
Administrators (THM\Administrators)
Users (THM\Users)

Permissions for Users	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

As you can see Users can only read, execute, and list the folder contents. However, we want to allow them to be able to store, edit, or delete files inside that folder. To do that, check the "Modify" box (you will see that by checking the Modify box the Write box will be automatically checked too).



Permissions for Important

Object name: C:\Important

Group or user names:

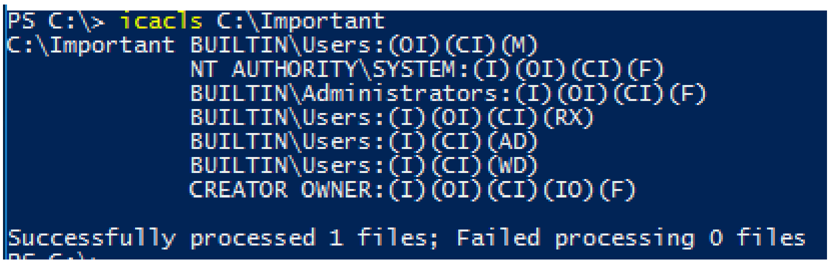
CREATOR OWNER
SYSTEM
Administrators (THM\Administrators)
Users (THM\Users)

Permissions for Users	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	☑	□

To apply the changes click on the "Apply" button.

The reason we do not set the full control permission on the folder is that users could set permissions and take ownership of the folder themselves (without the action of an administrator/privileged user).

A tool you can use to check the files or folder permissions is "**icacls**".



```
PS C:\> icacls C:\Important
C:\Important BUILTIN\Users:(OI)(CI)(M)
             NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
             BUILTIN\Administrators:(I)(OI)(CI)(F)
             BUILTIN\Users:(I)(OI)(CI)(RX)
             BUILTIN\Users:(I)(CI)(AD)
             BUILTIN\Users:(I)(CI)(WD)
             CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
```

Let's explain what those letters in parentheses mean as right now you might be confused.

I - permission inherited from the parent container

F - full access (full control)

M - Modify right/access

OI - object inherit

IO - inherit only

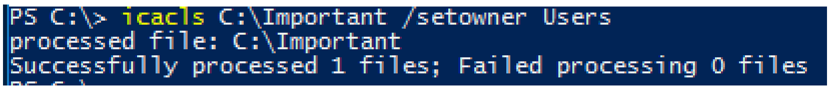
CI - container inherit

RX - read and execute

AD - append data (add subdirectories)

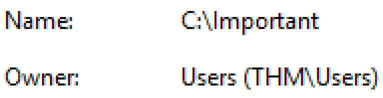
WD - write data and add files

You can use icacls to check permissions, set ownership of the folder, set, remove or deny permissions. An example would be setting the ownership of the folder to Users.



```
PS C:\> icacls C:\Important /setowner Users
processed file: C:\Important
Successfully processed 1 files; Failed processing 0 files
```

To check if that applied you can right-click on the folder and select "Properties", go to the "Security" tab, and click on "Advanced". There you should be able to see that the owner is "Users".



Name: C:\Important

Owner: Users (THM\Users)

What is authentication?

Authentication is a process for verifying the identity of a person (or an object or a service). When you authenticate a person, the goal is to verify that the person is not an imposter.

Local authentication

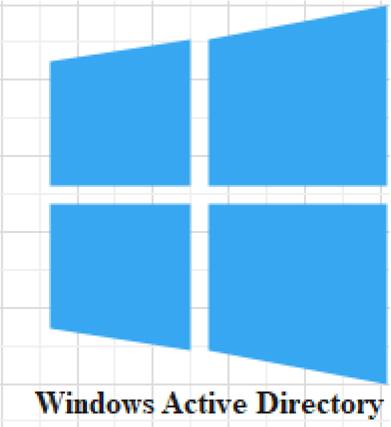
Local authentication is done using the Local Security Authority (LSA). LSA is a protected subsystem that keeps track of the security policies and the accounts that are on a computer system. It also maintains information about all aspects of local security on a computer.

Types of Active Directory

There are two types of Active Directory:

- On-Premise Active Directory (AD)
- Azure Active Directory (AAD)

Authentication on On-Premise Active Directory



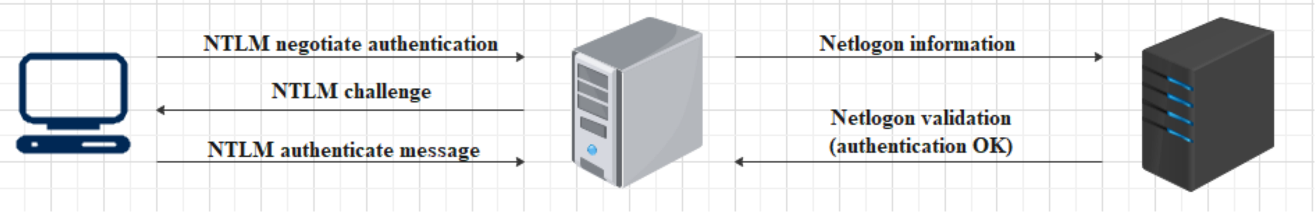
On-premise Active Directory has a record of all users, PCs and Servers and authenticates the users signing in (the network logon). Once signed in, Active Directory also governs what the users are, and are not, allowed to do or access (authorization).

In an on-premise Active Directory environment the authentication can be made by using the following protocols:

- NTLM
- LDAP / LDAPS
- KERBEROS

NTLM / NTLM 2

NTLM uses a challenge-response sequence of messages between a client and a server system. NTLM provides authentication based on a challenge-response authentication scheme. It does not provide data integrity or data confidentiality protection for the authenticated network connection.

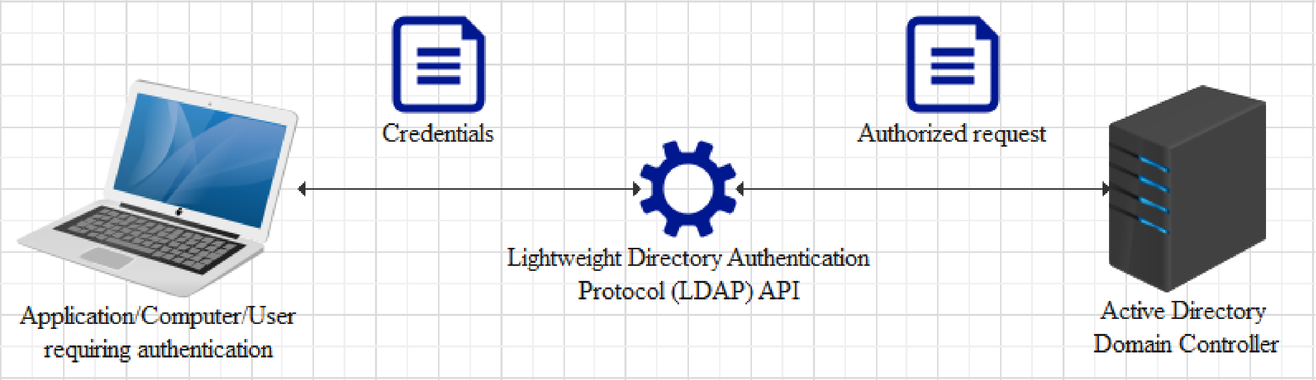

NTLM negotiate authentication
NTLM challenge
NTLM authenticate message
Netlogon information
Netlogon validation (authentication OK)

LDAP / LDAPS

The main difference between LDAP and LDAPS is that LDAPS support encryption and therefore the credentials are not sent in plain text across the network.

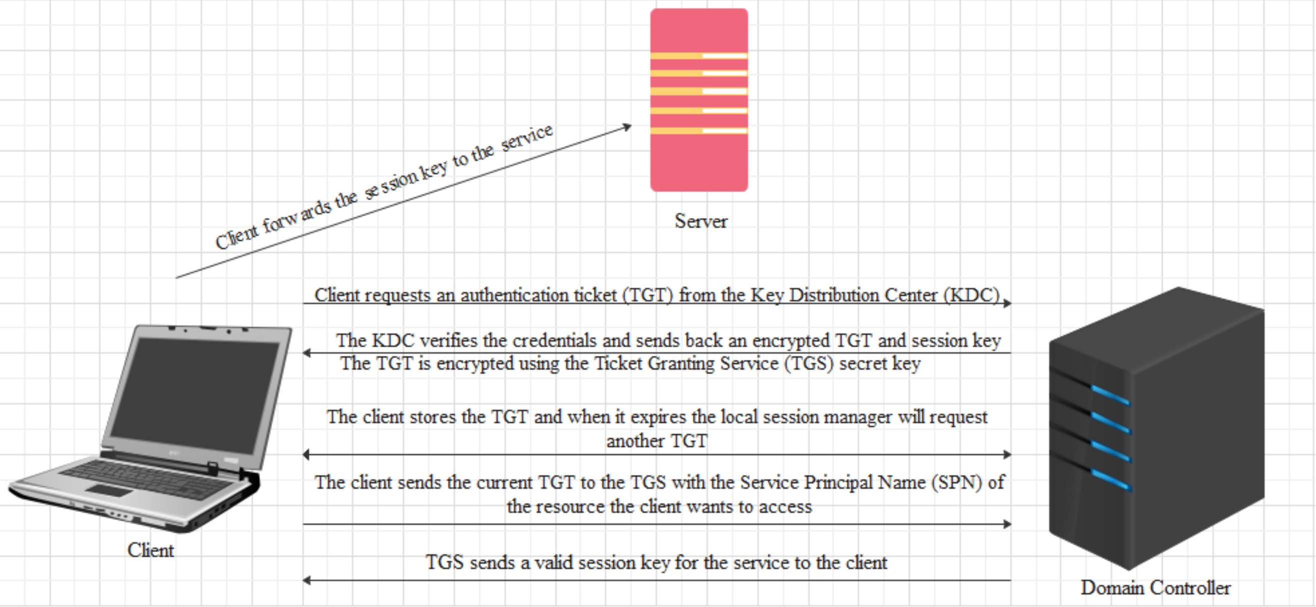
Another thing to keep in mind is that the Domain Controller (DC) can be considered a database of users, groups, computers and so on (contains information about objects). Using LDAP/LDAPS the user's workstation sends the credentials using an API to the Domain Controller in order to validate them and be able to log in.

The procedure is similar to the image below:

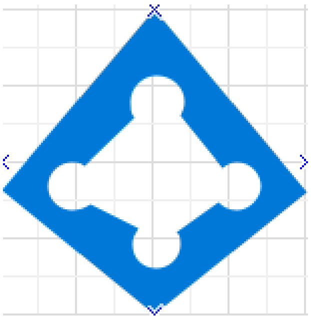

Credentials
Authorized request
Lightweight Directory Authentication Protocol (LDAP) API
Application/Computer/User requiring authentication
Active Directory Domain Controller

KERBEROS

Another way to authenticate is using Kerberos. Kerberos uses W symmetric-key cryptography and requires trusted third-party authorization to verify user identities. The authentication process is similar to the one below:


Client forwards the session key to the service
Server
Client requests an authentication ticket (TGT) from the Key Distribution Center (KDC)
The KDC verifies the credentials and sends back an encrypted TGT and session key
The TGT is encrypted using the Ticket Granting Service (TGS) secret key
The client stores the TGT and when it expires the local session manager will request another TGT
The client sends the current TGT to the TGS with the Service Principal Name (SPN) of the resource the client wants to access
TGS sends a valid session key for the service to the client
Client
Domain Controller

Authentication on Azure Active Directory



Azure Active Directory is a secure online authentication store, which can contain users and groups. Users have a username and a password which are used when you sign in to an application that uses Azure Active Directory for authentication. So, for example, all of the Microsoft Cloud services use Azure Active Directory for authentication: Office 365, Dynamics 365 and Azure.

Azure Active Directory supports the following authentication methods:

- SAML (Security Assertion Markup Language)
- OAUTH 2.0

- OpenID Connect

SAML (Security Assertion Markup Language)

Security Assertion Markup Language (SAML) is a type of Single Sign-On (SSO) standard. It defines a set of rules/protocols that allow users to access web applications with a single login. This is possible because those applications (referred to as “Service Providers”) all trust the systems that verify users’ identities (referred to as “Identity Providers”).

Service Providers - These are the systems and applications that users access throughout the day.

Identity Providers - This would be the system that performs user authentication.

OAUTH 2.0

OAuth 2.0 is a standard that apps use to provide client applications with access.

OAuth 2.0 spec has four important roles:

- The authorization server, which is the server that issues the access token.
- The resource owner, normally your application's end-user, that grants permission to access the resource server with an access token.
- The client, which is the application that requests the access token, and then passes it to the resource server.
- The resource server, which accepts the access token and must verify that it is valid. In this case, this is your application.

OpenID Connect

OpenID Connect is an authentication standard built on top of OAuth 2.0. It adds an additional token called an ID token.

For that, it uses simple JSON Web Tokens (JWT). While OAuth 2.0 is about resource access and sharing, OIDC is all about user authentication

Built-in utility tools

Windows comes with a variety of utility tools. Some of them are:

- Computer Management
- Local Security Policy
- Disk Cleanup
- Registry Editor
- Command-line tools
- Registry Editor (Regedit)

Let's break each of them down and see their usage and why they are important.

Computer Management

Computer Management contains more tools such as:

- Task Scheduler
- Event Viewer
- Shared Folders
- Local users & computers
- Performance Monitor
- Disk Management
- Services & Applications

Task Scheduler - This is a tool that allows predefined actions to be automatically executed whenever a certain set of conditions is met(Ex: You can set up a date and time for a piece of software to be installed, or a script to run).

Event Viewer - Probably one of the most important tools that come with Windows. The Event Viewer logs events that happen across the device (Ex: Successful & Failed login attempts, System Errors, etc). The reason Event Viewer is important is because it can be used to forward the events to a SIEM (Security Information and Event Manager) which helps the IT team of a company determine possible malicious activities.

Shared Folders - Is a directory or a folder that can be shared across the network and can be accessed by multiple users.

Local users and computers - Using local users and computers we can create users, add them to different built-in groups, and they can be given different levels of access (Ex: User A can connect through RDP to a machine but user B can't).

Performance Monitor -Performance Monitor monitors the different activities across the device such as CPU usage, memory usage, etc.

Disk Management - Using Disk Management you can shrink, expand, create new partitions (drives) and format the partitions.

Services & Applications - It is possible to check the running services on the system and you have the ability to start, stop or restart them.

Local Security Policy

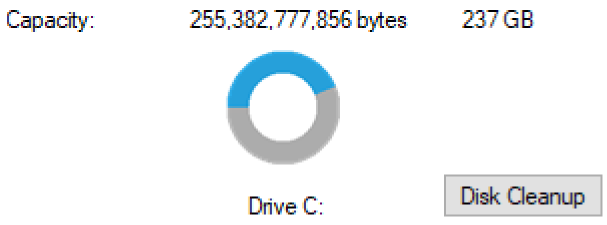
Local Security Policy is a group of settings you can configure to strengthen the computer's security. Even though
most policy settings in Windows are fine, there are a few that need adjusting for enhanced security. You can set the minimum password length, the password complexity level, you can disable guest & local administrator accounts, and many more.

Note: If the computer is not integrated into an Active Directory environment disabling local administrator account is a bad idea.

Disk Cleanup

Another useful utility is Disk Cleanup. Using Disk Cleanup we can delete files that are no longer needed by the system and are just adding up to the computer disk space. Running Disk Cleanup as administrator we can also clean system files (Ex: sometimes, after getting updates some files remain on disk, but these are no longer needed).

To access Disk Cleanup right-click on Local Disk C and click Properties. You should see a button in the General tab named "Disk Cleanup".



You just need to tick the box/files you want to clean and press OK.

Registry Editor

The Windows registry database stores many important operating system settings. For example, it contains entries with information about what should happen when double-clicking a particular file type or how wide the taskbar should be. Built-in and inserted hardware also stores information in the registry when the driver is installed; this driver is called up every time the system is booted up.

To access the Registry Editor you can either search it or use Windows Key + R and type RegEdit.

Command-line tools

Windows comes equipped with two command-line tools (and one can be installed):

- CMD
- Powershell
- Windows Terminal

CMD is the command-line interpreter for Microsoft Windows operating systems used to automate various system-related tasks using scripts and batch files. Users can interact with the OS directly using text-based commands. It emulates most of the command line abilities available in MS-DOS through a command-line interface.

Powershell is mainly used by sysadmins to manage the network and domain they handle, as well as the computers and other devices that are part of it. PowerShell is a scripting language. The PowerShell can interpret batch commands and Powershell commands, but the command prompt can only interpret batch commands.

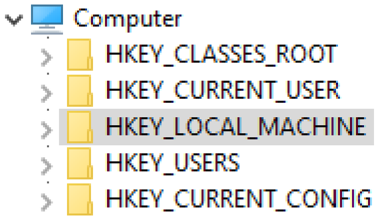
Both CMD and Powershell are powerful command-line tools used to automate system administration tasks by writing a script/batch file. However, CMD has limited administration capabilities as compared to Powershell, which, on the other hand, is a more advanced and modern shell implementation with additional features and enhancements (Ex: cmdlets).

Windows Terminal can be used instead of Powershell and CMD and can be installed from the Microsoft Store. The application includes multiple tab support, alongside themes and customization for developers who want to tweak the Terminal.

Registry Editor

Registry Editor can be considered a database that contains low-level settings for Microsoft Windows settings and applications. The registries are structured as follows:

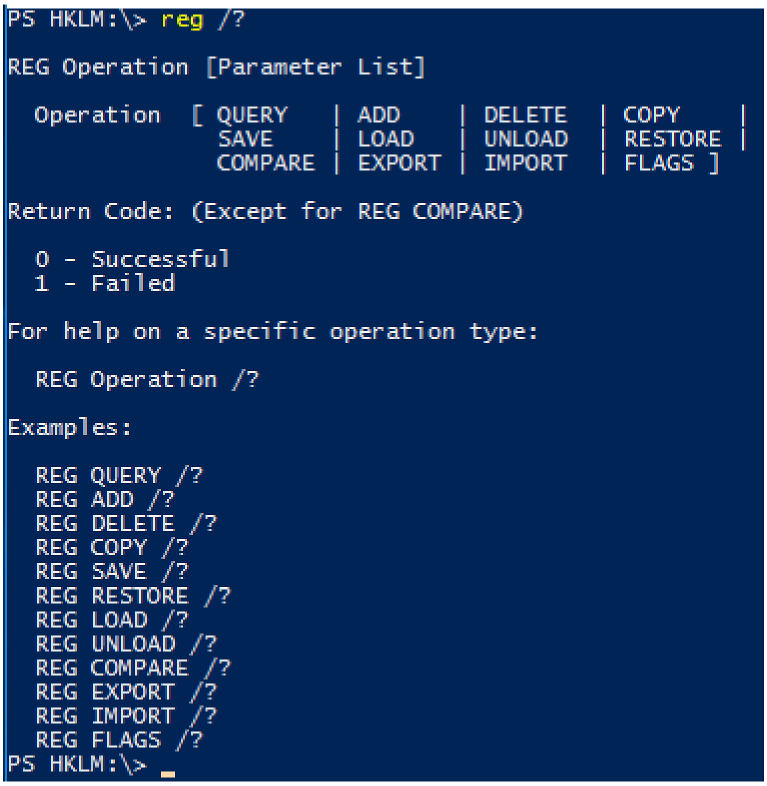
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG



Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG

A feature of Powershell is that you can browse the registries. You can do that by typing: "**cd <REG DB>**" (Example: **cd HKLM:**).

Windows also has a builtin tool named "reg" which can be used from the command line to add, remove, query, import, export, etc registry keys.



```
PS HKLM:\> reg /?

REG Operation [Parameter List]

  Operation  [ QUERY   | ADD    | DELETE  | COPY    |
               SAVE    | LOAD   | UNLOAD  | RESTORE |
               COMPARE | EXPORT | IMPORT  | FLAGS ]

Return Code: (Except for REG COMPARE)

  0 - Successful
  1 - Failed

For help on a specific operation type:

  REG Operation /?

Examples:

  REG QUERY /?
  REG ADD /?
  REG DELETE /?
  REG COPY /?
  REG SAVE /?
  REG RESTORE /?
  REG LOAD /?
  REG UNLOAD /?
  REG COMPARE /?
  REG EXPORT /?
  REG IMPORT /?
  REG FLAGS /?
PS HKLM:\> _
```

There is also available a GUI that can be used. You can search for "**Regedit**" or type it in the command line.

There is no point to remember the paths for some settings that are located in the registry editor. You can look up for the settings on the internet.

Types of servers

What is a server?

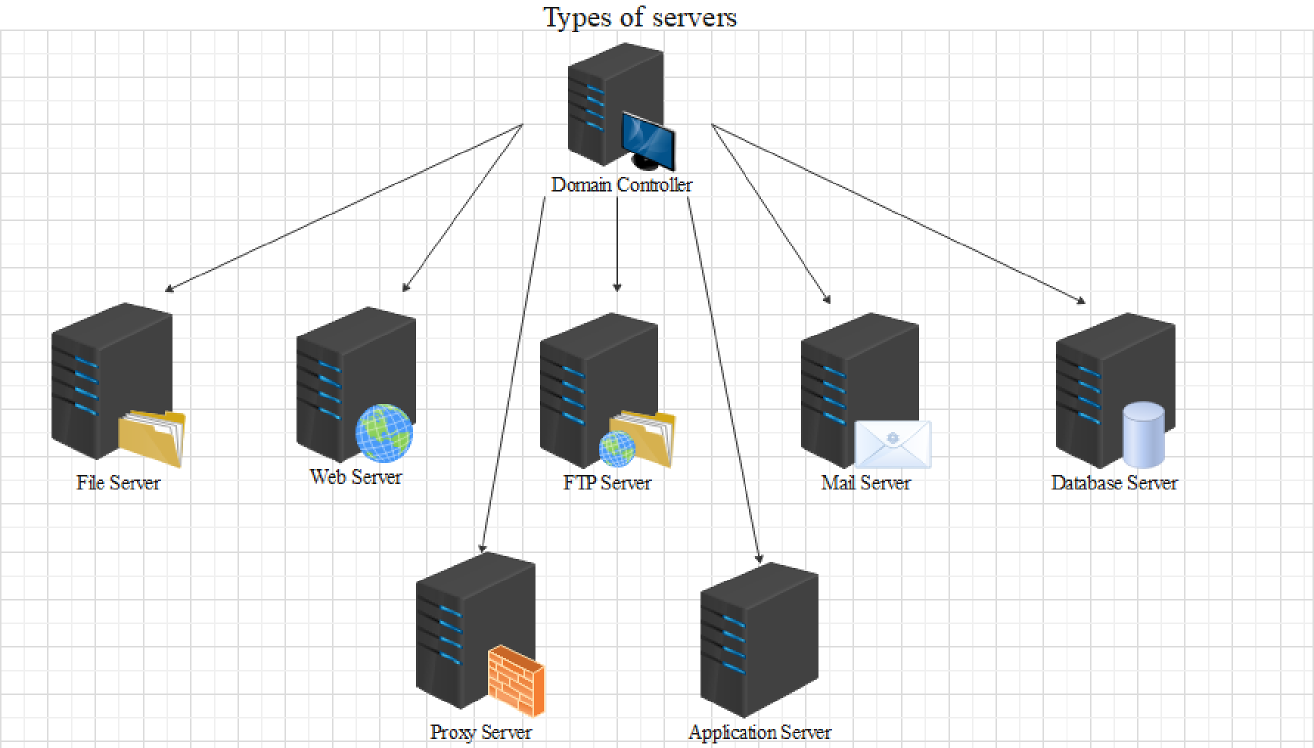
A server is a piece of hardware or software equipment that provides functionality for other softwares or devices.

Types of servers

Servers can be used for a variety of actions or things. The most common ones are:

- Domain Controller
- File server
- Web server

- FTP Server
- Mail Server
- Database Server
- Proxy Server
- Application Server



Domain Controller - Might be one of the most important servers because in an AD or AAD infrastructure we can control users, groups, restrict actions, improve security, and many more of other computers and servers.

File Server - File servers provide a great way to share files across devices on a network.

Web Server- It serves static or dynamic content to a Web browser by loading a file from a disk and serving it across the network to a user’s Web browser.

FTP Server - Makes possible moving one or more files securely between computers while providing file security and organization as well as transfer control.

Mail Server - Mail servers move and store mail over corporate networks (via LANs and WANs) and across the Internet.

Database Server - A database server is a computer system that provides other computers with services related to accessing and retrieving data from one or multiple databases.

Proxy Server - This server usually sits between a client program and an external server to filter requests, improve performance, and share connections.

Application Server - They're usually used to connect the database servers and the users.

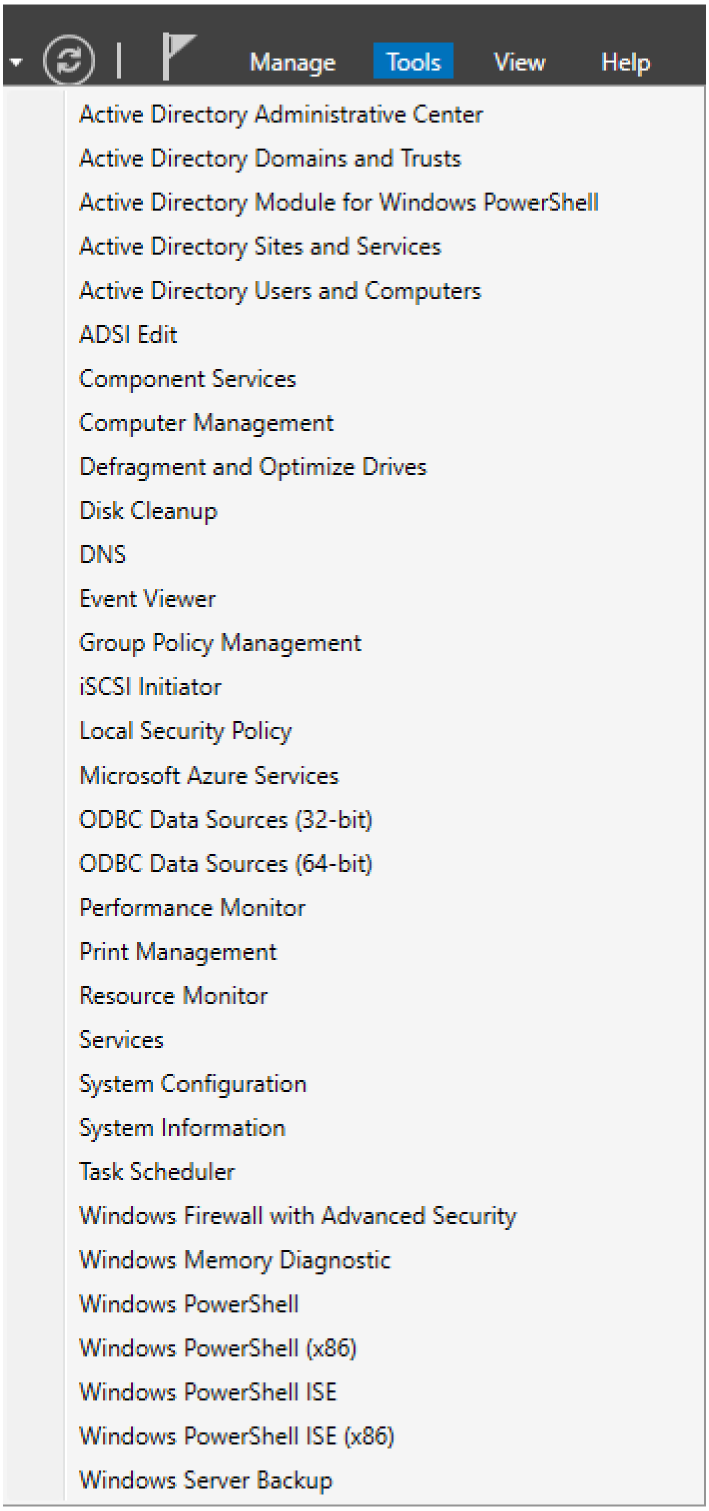
Users and Groups Management

Users and Groups Management in Active Directory

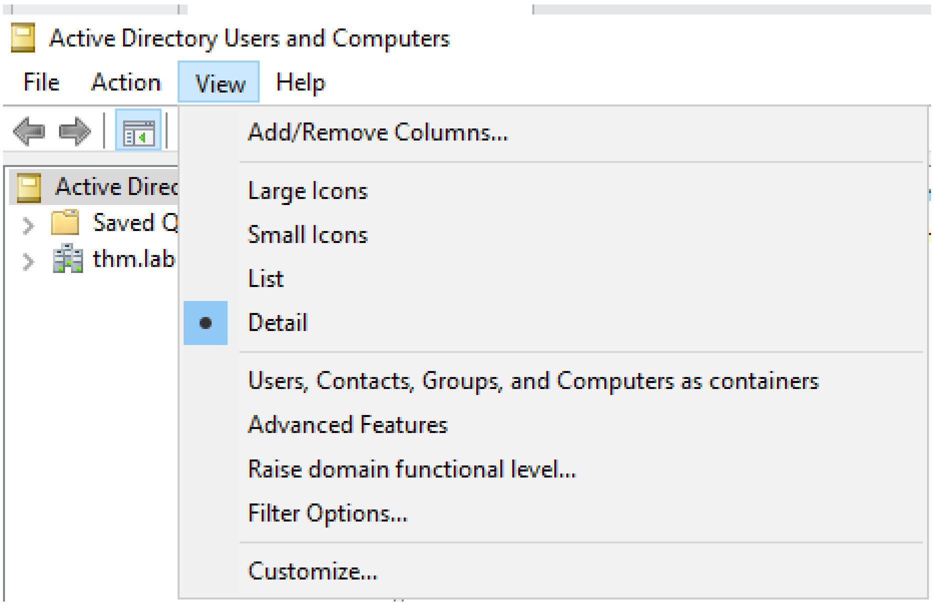
Deploy the machine and authenticate using RDP (on Windows) or Remmina/Xfreerdp (on Linux) with the user:

Administrator:T ryhackme123!

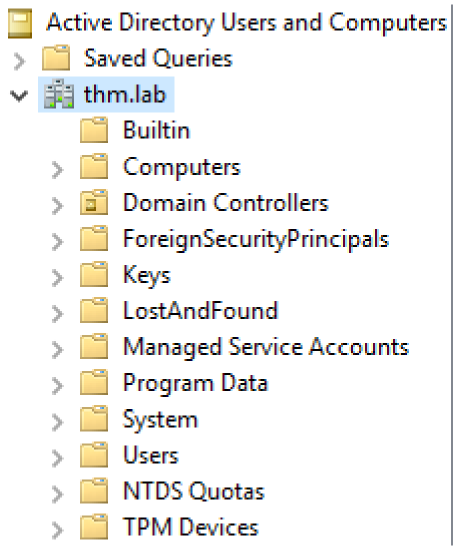
In Active Directory user management is done using the Active Directory Users and Computers. To access it go to Tools > Active Directory Users and Computers.



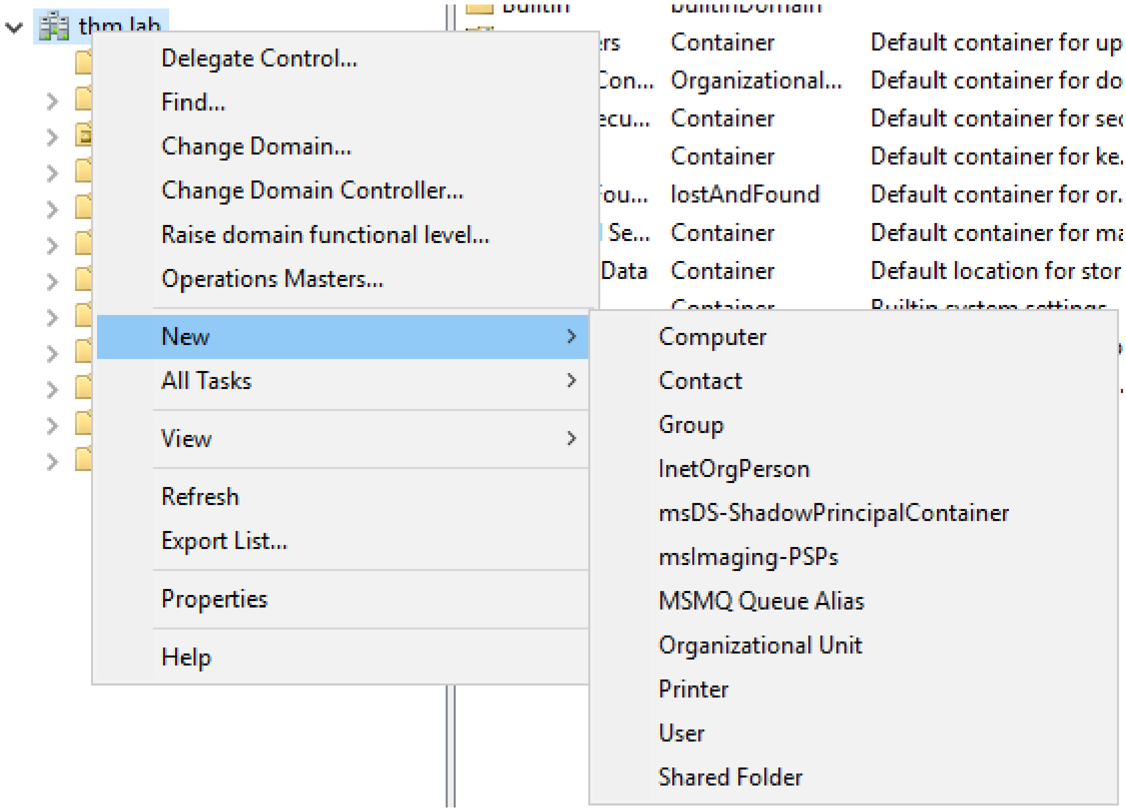
Before any other action let's enable Advanced Features which adds additional features when looking at an object properties. That is doable by going to View > Advanced Features.



By double-clicking on thm.lab we are presented with the Active Directory tree.

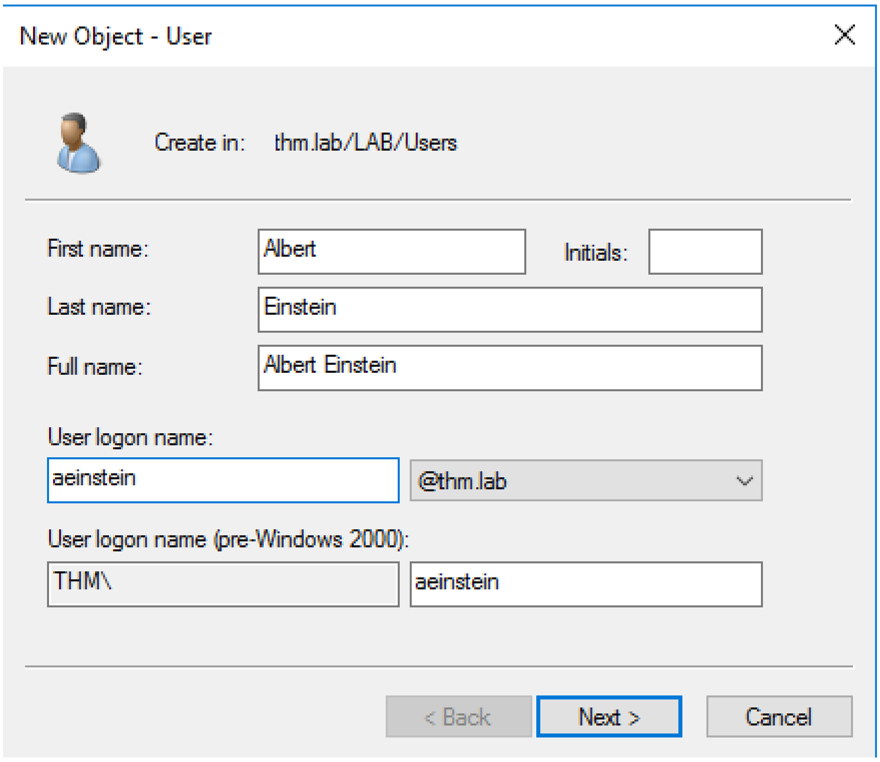


Let's create an Organizational Unit (OU) where to store the users. To do that right-click on the domain name (thm.lab) and go to New > Organizational Unit. I named it LAB and clicked OK to create it.



Let's create two more OUs inside the newly created OU (it will look nested). In one OU we'll store users and in the second one, we'll store Groups. To create the OU's we can repeat the steps above (Right-click on LAB OU > New > Organizational Unit).

Time to create some users and groups! To do so right-click on the Users OU and go to New > User and fill in the information required.


New Object - User

Create in: thm.lab/LAB/Users

First name: Albert

Initials:

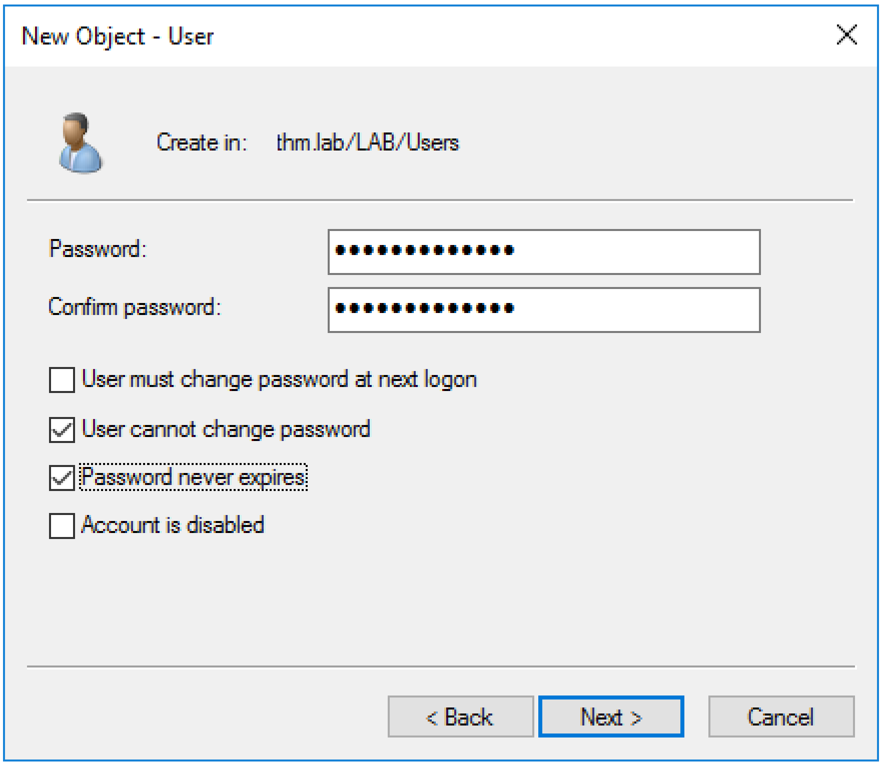
Last name: Einstein

Full name: Albert Einstein

User logon name: aeinstein @thm.lab

User logon name (pre-Windows 2000): THM\ aeinstein

Click Next and set a password for the user.



New Object - User

Create in: thm.lab/LAB/Users

Password: •••••••••••••

Confirm password: •••••••••••••

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

The reason I checked only "Password never expires" is because I do not want the password to expire after a period of time (the default period of time in AD is 42 days). In a production environment, you would probably check "User must change password at next logon" so the user can set a password he desires after you created his AD account.

Since the password can be set to expire after a period of time it would be a bad idea to check the "User cannot change password" because he won't be able to reset the password and you will have to manually intervene.

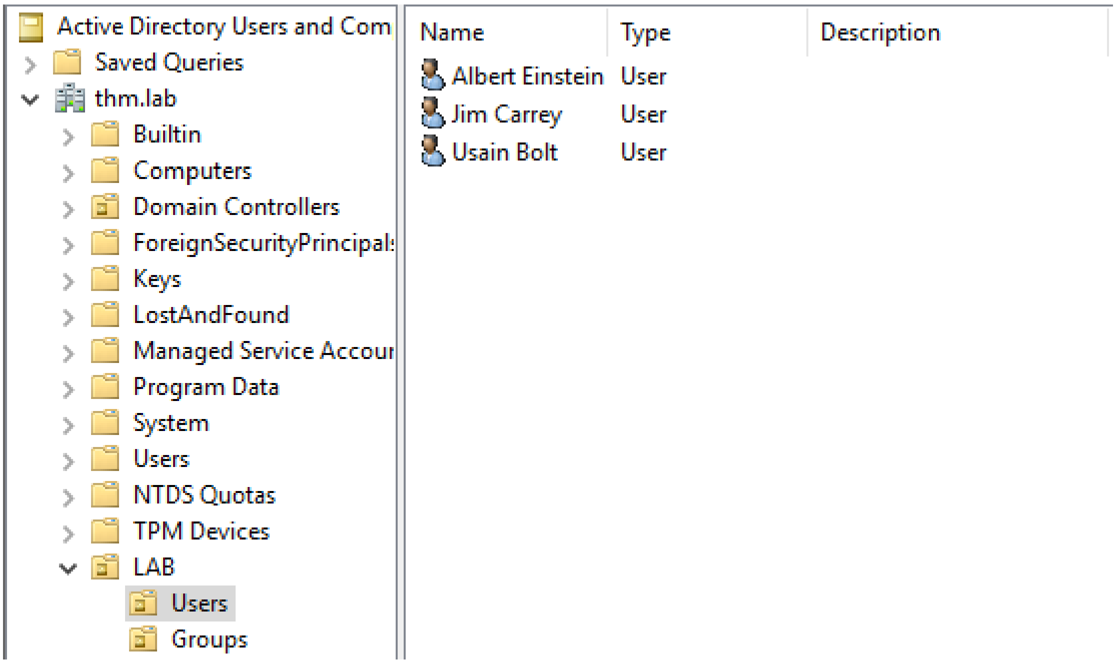
As for the last box "Disable account" it's obvious the action that will take place. It will disable the user account. You might want to disable a user account in case he has a leave (let's say 6 months leave) and you do not want him or any other colleague or malicious entity to use his account.

Click on Next and you will be shown the account information and click Finish to finish the account creation.

Note: The username that is going to be used by the user in order to authenticate is the one you set in the User Logon Name.

You've successfully created your first AD user. Now, create two more users and name them as you wish.

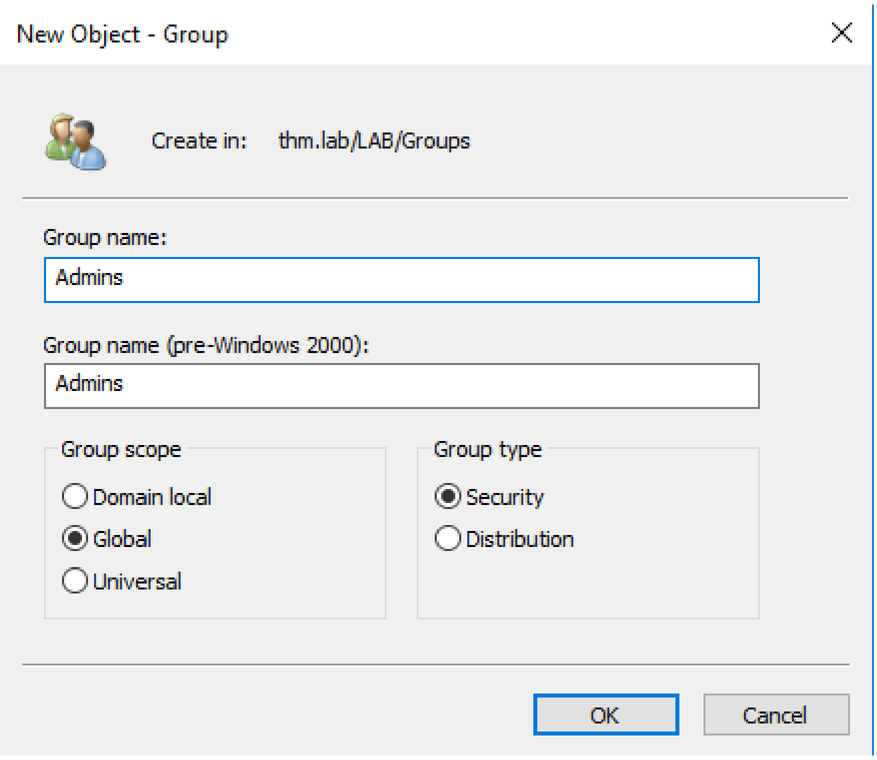
We should have three users in the AD:



Name	Type	Description
Albert Einstein	User	
Jim Carrey	User	
Usain Bolt	User	

Let's move to the Groups OU. Right click on the OU > New > Group.

I named the group Admins and clicked OK to create it.


New Object - Group

Create in: thm.lab/LAB/Groups

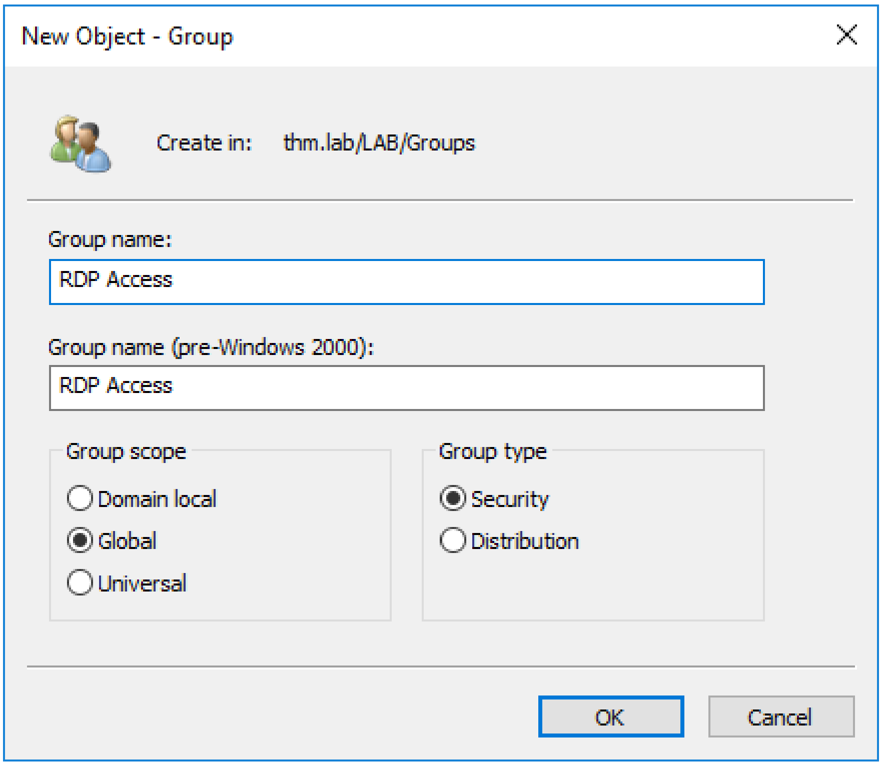
Group name: Admins

Group name (pre-Windows 2000): Admins

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Then I created another group named RDP Access.



New Object - Group

Create in: thm.lab/LAB/Groups

Group name:
RDP Access

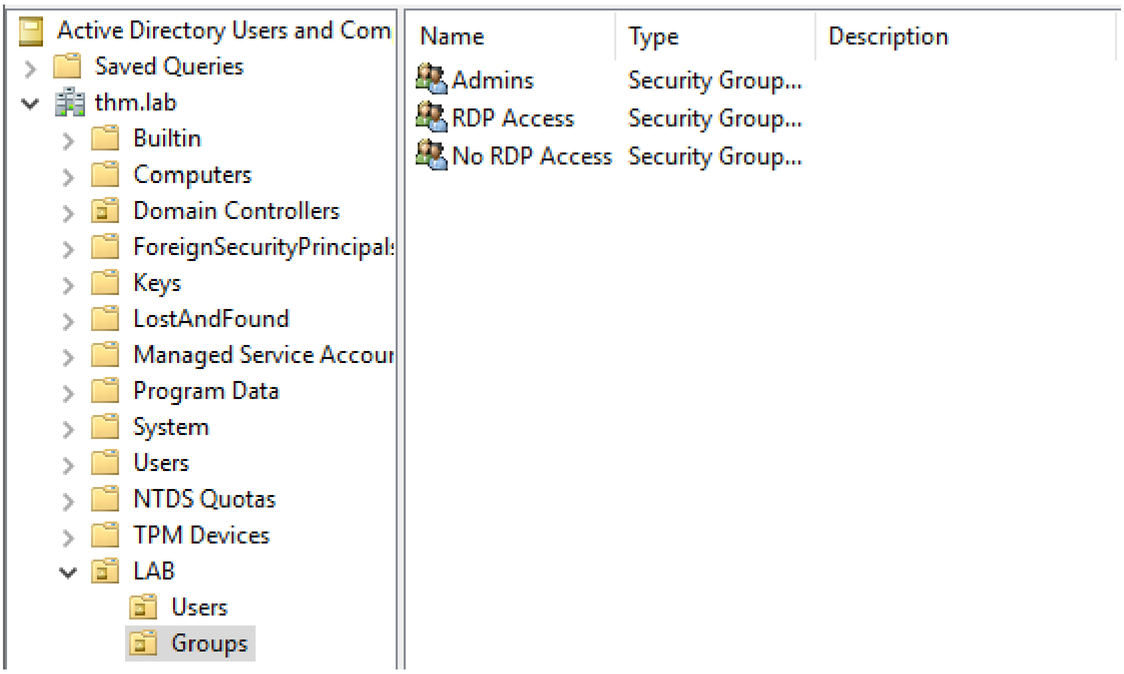
Group name (pre-Windows 2000):
RDP Access

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

And finally using the same method create one more group named No RDP Access.

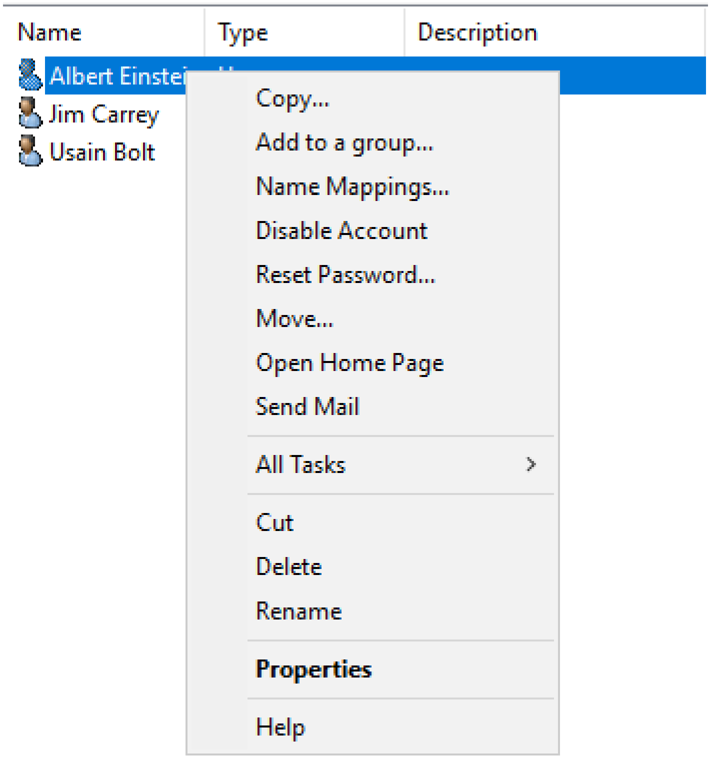
We should have the following groups in AD:



Name	Type	Description
Admins	Security Group...	
RDP Access	Security Group...	
No RDP Access	Security Group...	

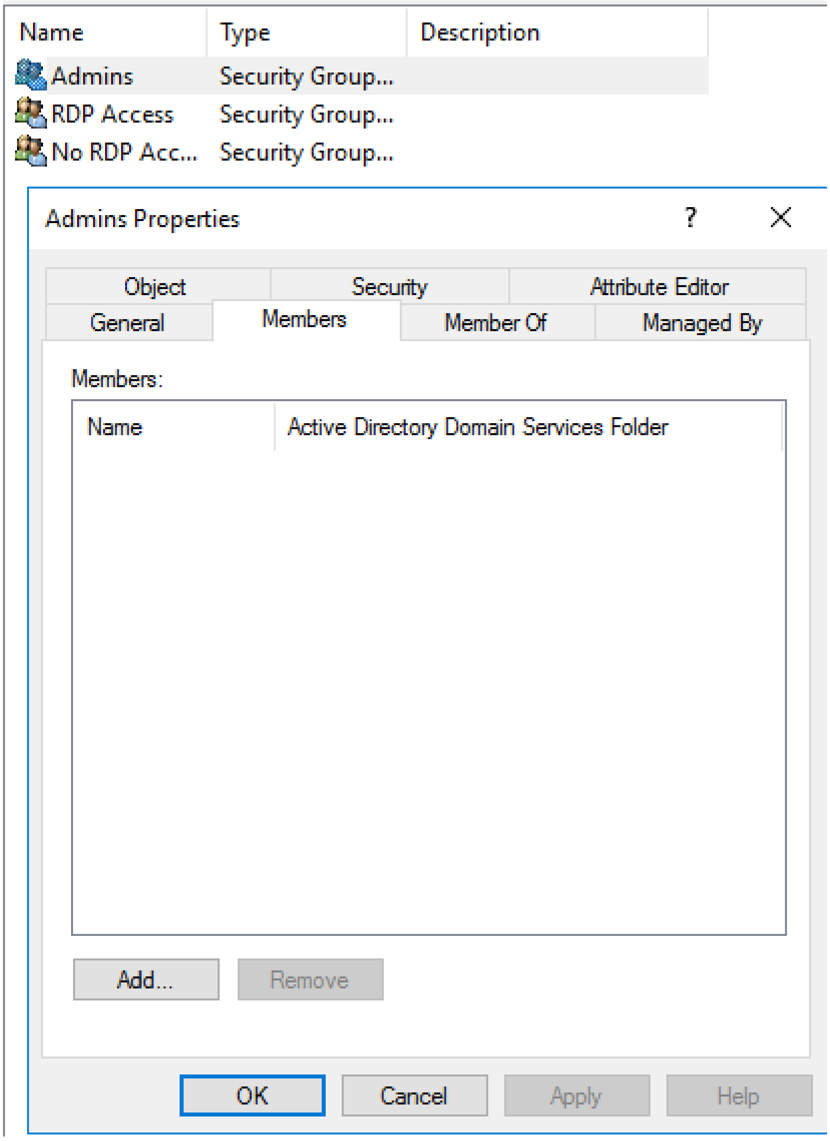
To assign a user to a group you can do that in two ways:

1. Right-clicking a user > Add to a group



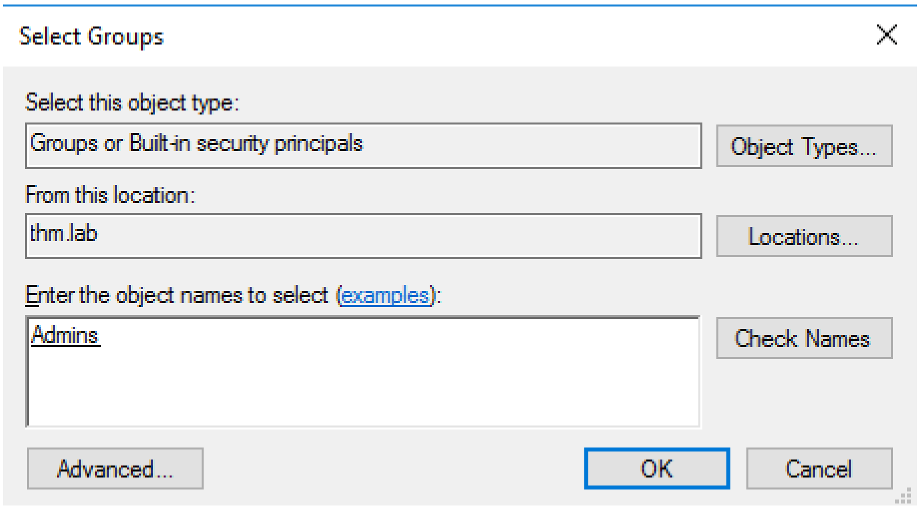
Name	Type	Description
Albert Einstei	U	
Jim Carrey		
Usain Bolt		

```
2. Double-clicking a group > click on Members tab > Add
```



Name	Type	Description
Admins	Security Group...	
RDP Access	Security Group...	
No RDP Acc...	Security Group...	

Using the first method let's add Albert Einstein to the Admins group. A window will be prompted to search for an object in the AD. You can type in the Enter object name to select field the name of the group created (in my case Admins), click Check Names, and OK to add the user to the specified group.



Select Groups

Select this object type:
Groups or Built-in security principals

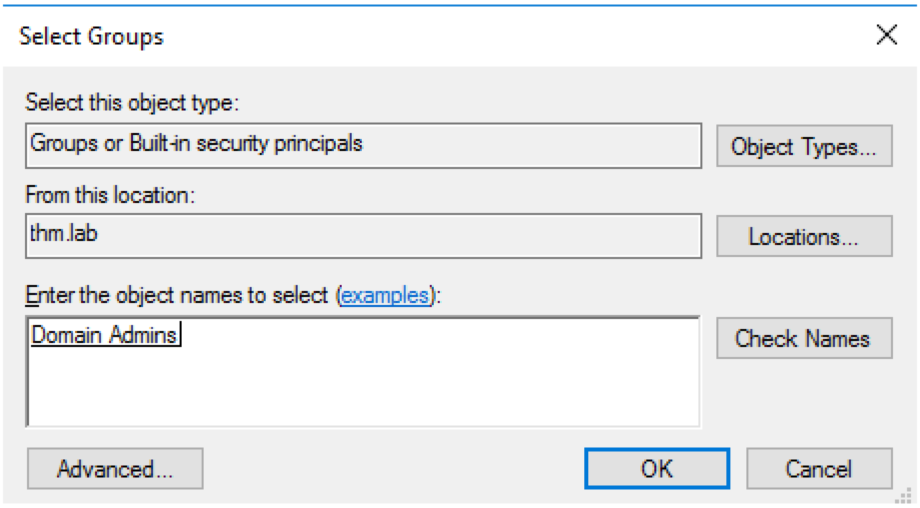
From this location:
thm.lab

Enter the object names to select (examples):
Admins

Proceed to add one of the created users to the RDP Access group and the other to the No RDP Access group.

Another thing to keep in mind is that an object can be a member of another object (Ex: A group can be a member of another group).

We added Albert Einstein to a group named Admins. Let's add the Admins group to the Domain Admins group. To do that we can right-click on Admins group > Add to a group and search for Domain Admins and press OK.



Select Groups

Select this object type:
Groups or Built-in security principals

From this location:
thm.lab

Enter the object names to select (examples):
Domain Admins

As we've done with Albert Einstein's account, add both **RDP Access** and **No RDP Access** groups to the **Remote Desktop Users** group

Note: Even though adding the **No RDP Access** group to the **RDP Users** group the **No RDP Access** group can be blocked using GPO. This will be done in the next task (Creating your first GPO).