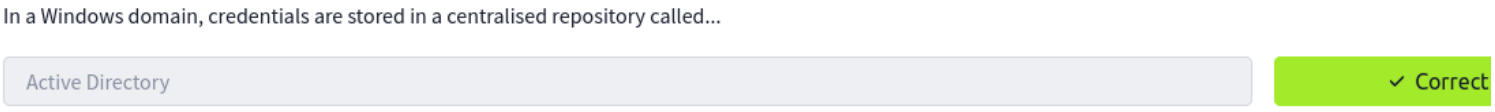
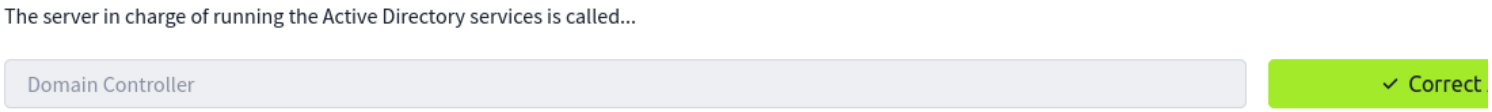
ACTIVE DIRECTORY BASICS

Introduction

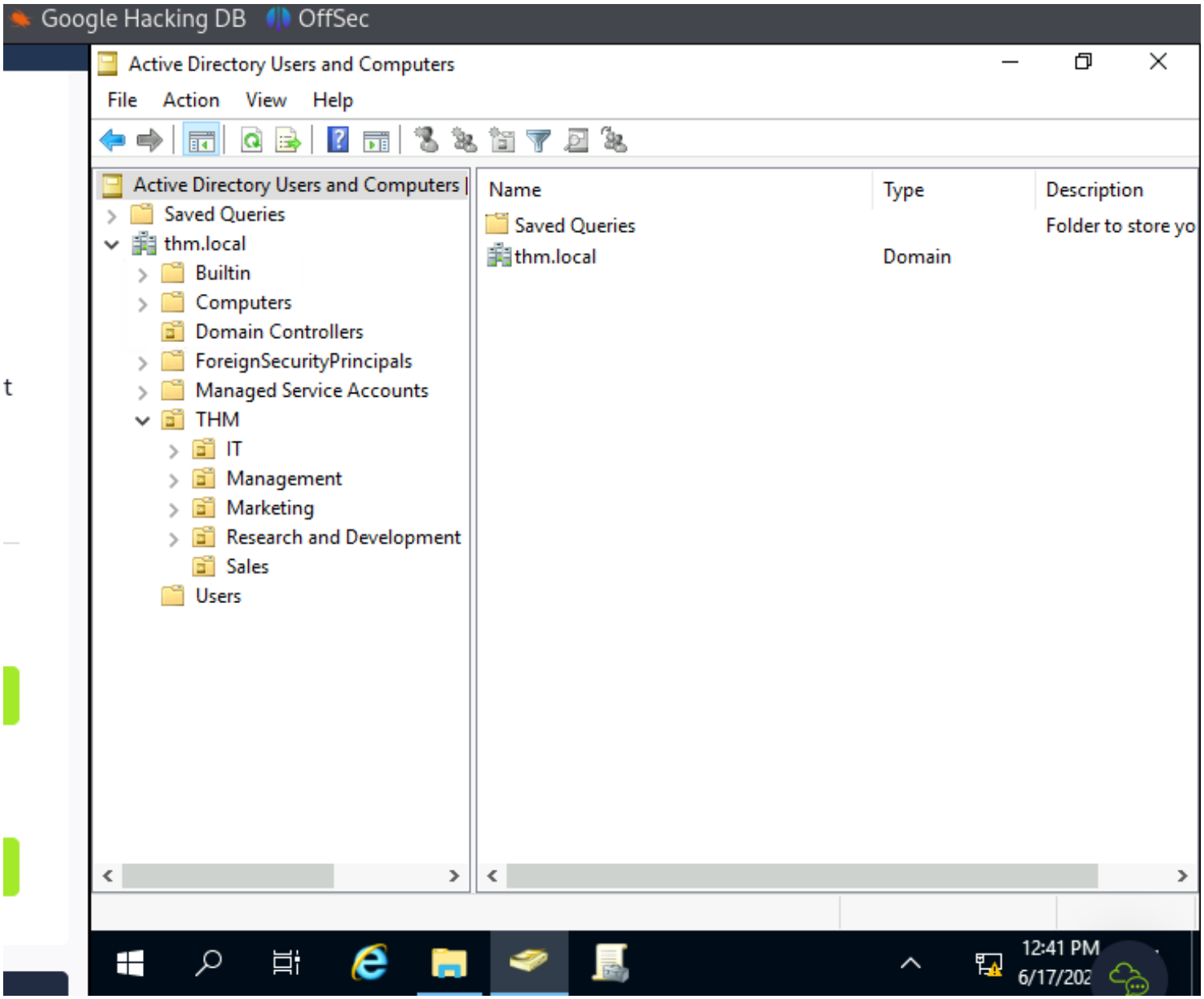
Active Directory (AD) is a critical component in the realm of enterprise IT infrastructure, providing a comprehensive directory service developed by Microsoft for Windows domain networks. AD facilitates the management of network resources by storing information about objects on the network and making this information easy for administrators and users to find and use. This report delves into the functionalities, benefits, and implementation of Active Directory, highlighting its role in enhancing security, simplifying administrative tasks, and ensuring seamless network management within an organization.

Q & A





A domain controller is **the server responsible for managing network and identity security requests**. It acts as a gatekeeper and authenticates whether the user is authorized to access the IT resources in the domain.

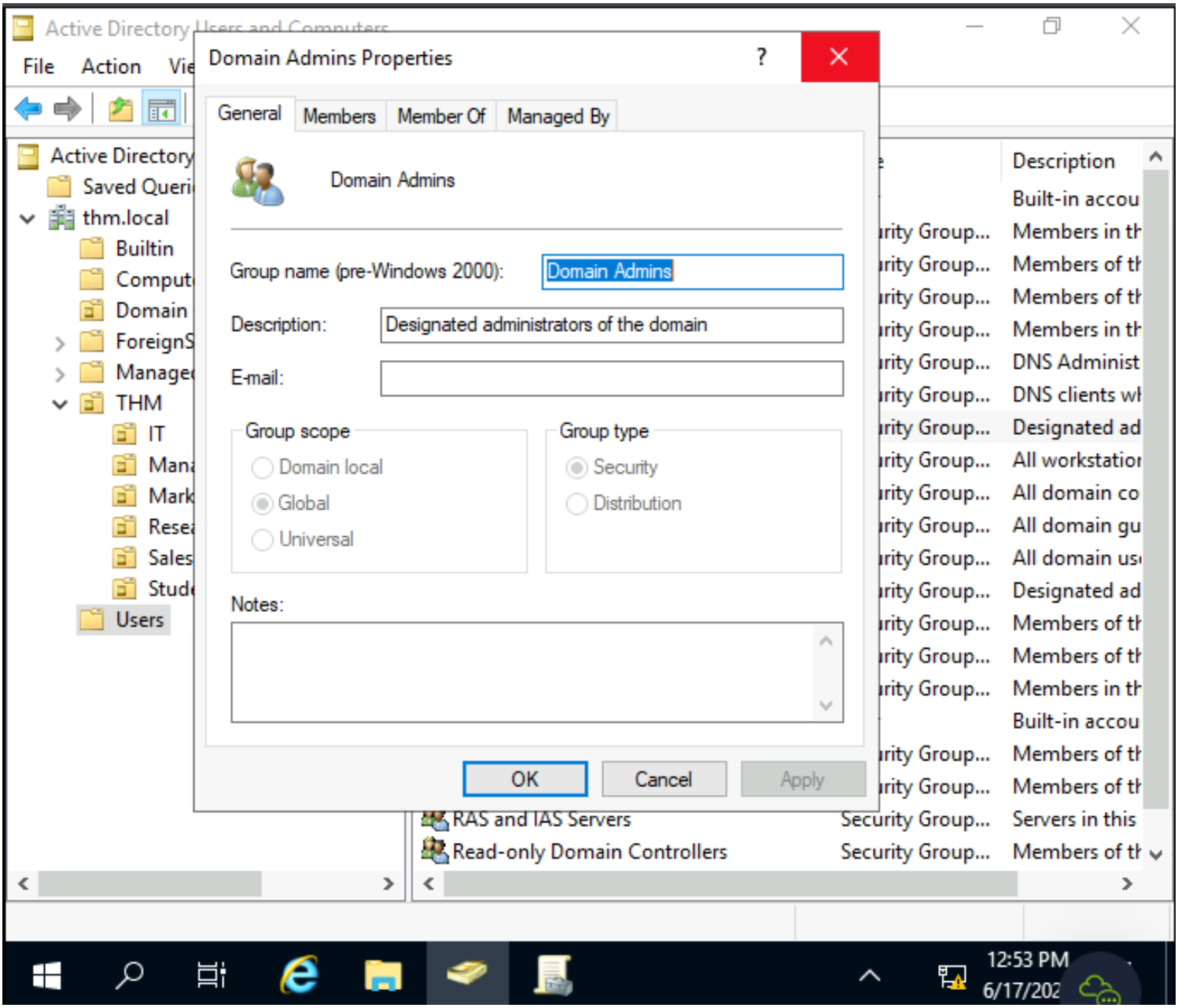


Which group normally administrates all computers and resources in a domain?

Domain Admins

✓ Correct Answer

As shown below, Domain Admins is the group that administrates all the computers and resources within a domain.



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

TOM-PC$

✓ Correct Answer

The machine account name is the computer's name followed by a dollar sign. This can be seen from the infomation displayed in the image below.

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$`.

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?

Organizational Units

✓ Correct Answer

Organisational units are container objects that allow us to classify users and machines.

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 organised in **Organizational Units (OUs)** which are container objects that allow you to classify users and machines. OUs are mainly used to define sets of users with similar policing requirements. The people in the Sales department of your organisation 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.

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

delegation

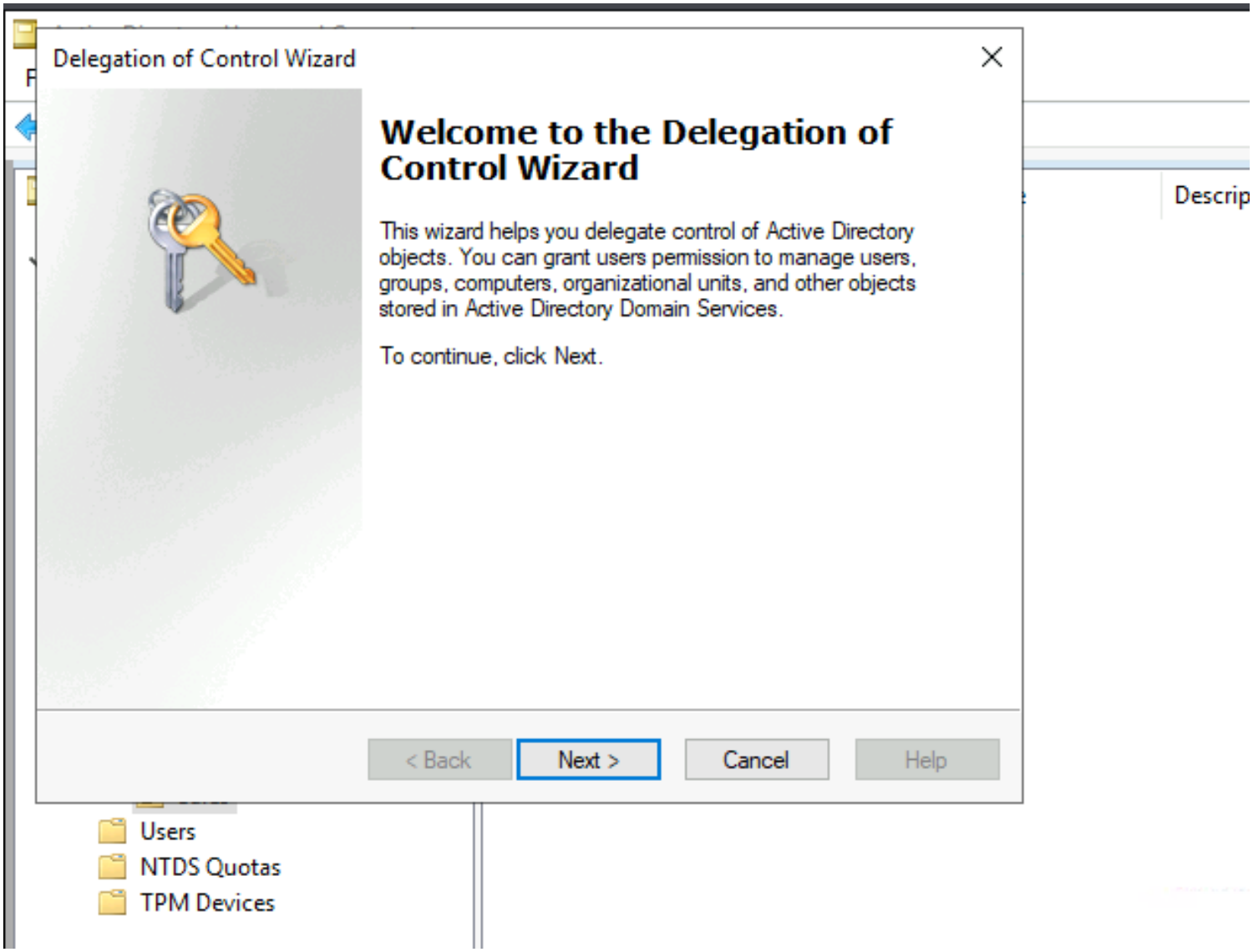
✓ Correct

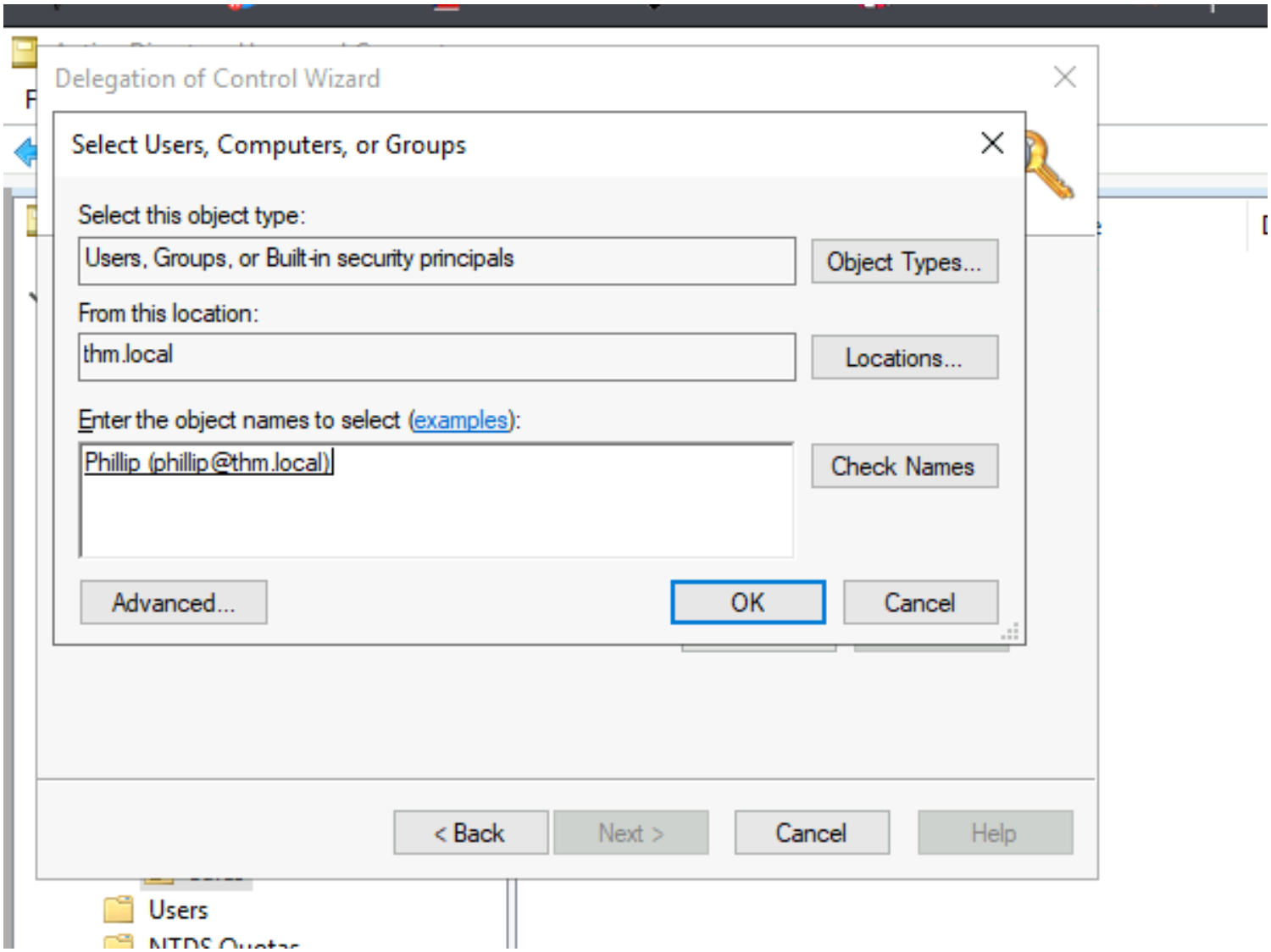
As it can be seen from the images below, Delegation involves granting privileges to a user over some OU or other AD objects.

Delegation

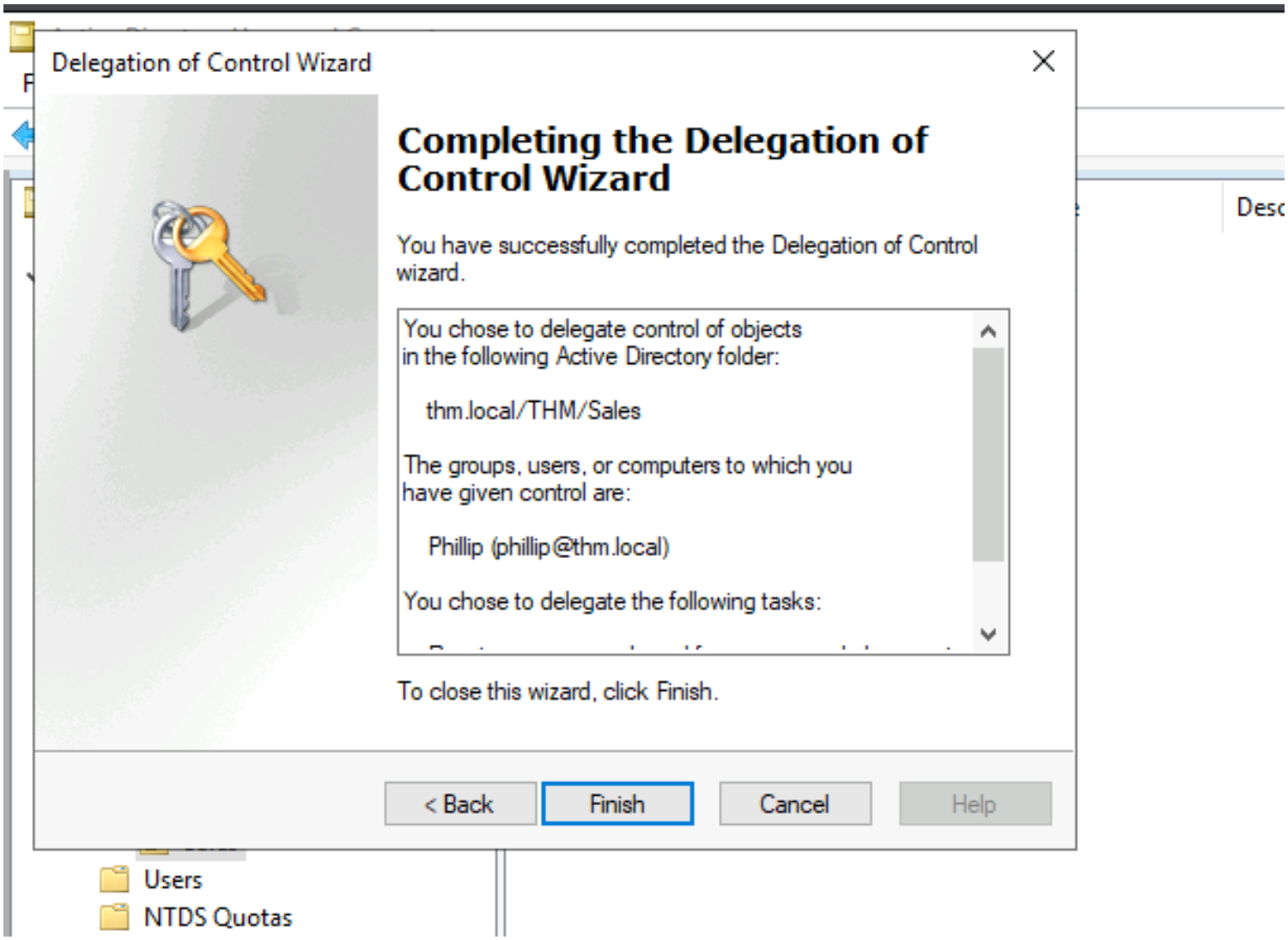
One of the nice things you can do in AD is to give specific users some control over some OUs. This process is known as **delegation** and allows you to grant users specific privileges to perform advanced tasks on OUs without needing a Domain Administrator to step in.

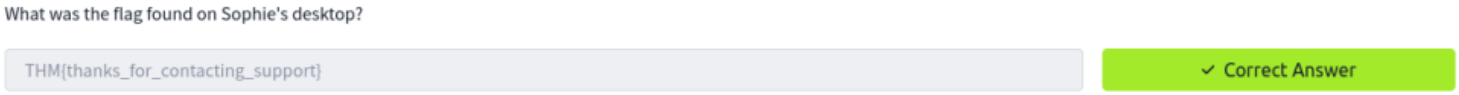
The images below shows how I was performing delegation to user phillip.


Delegation of Control Wizard
Welcome to the Delegation of Control Wizard
This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.
To continue, click Next.
< Back
Next >
Cancel
Help
Users
NTDS Quotas
TPM Devices

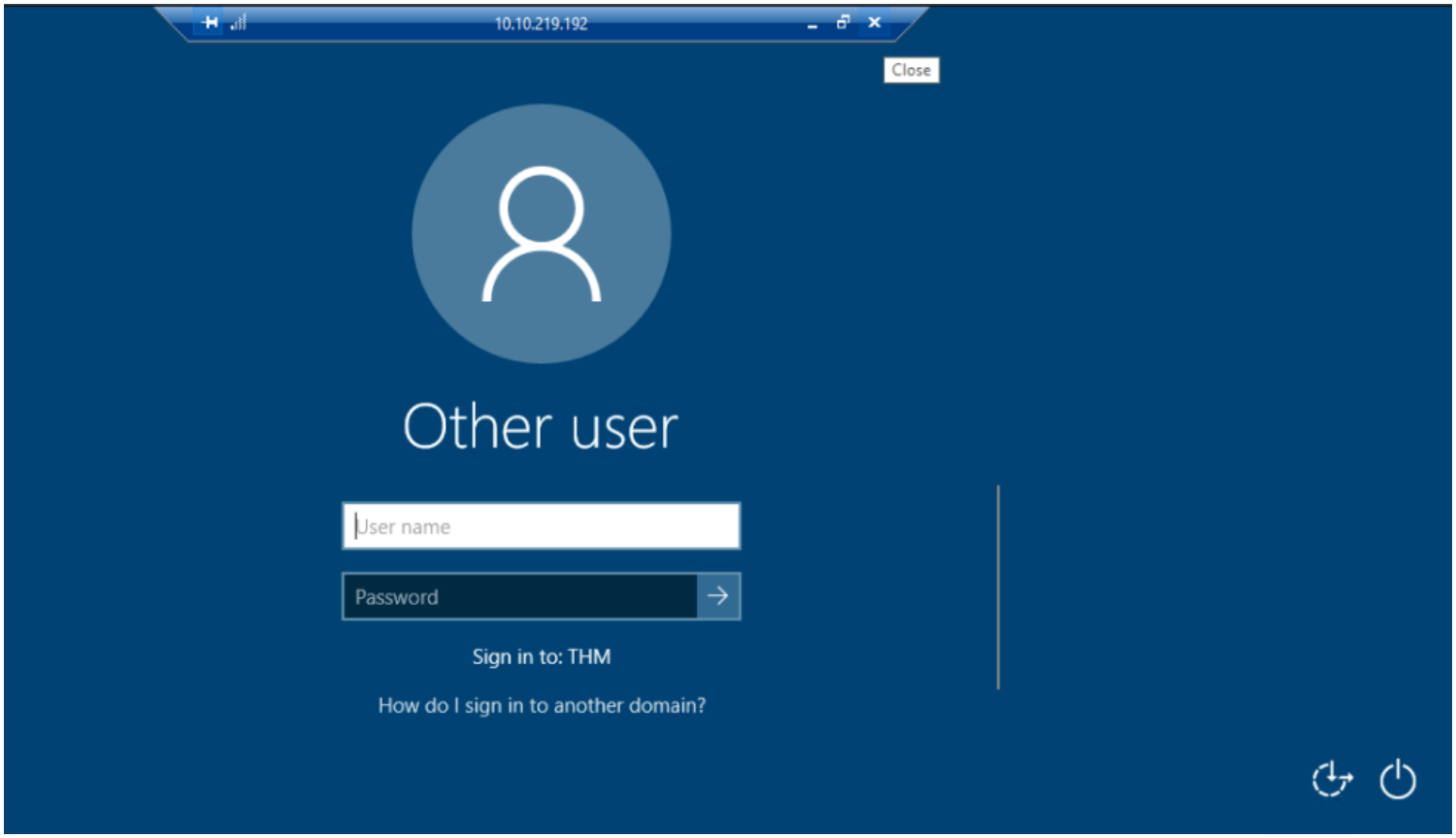


After completing the delegation of control wizard, I clicked on finish to complete the process.
From the images above, I was delegating control to user Phillip over other users' from the management, marketing and sales group.

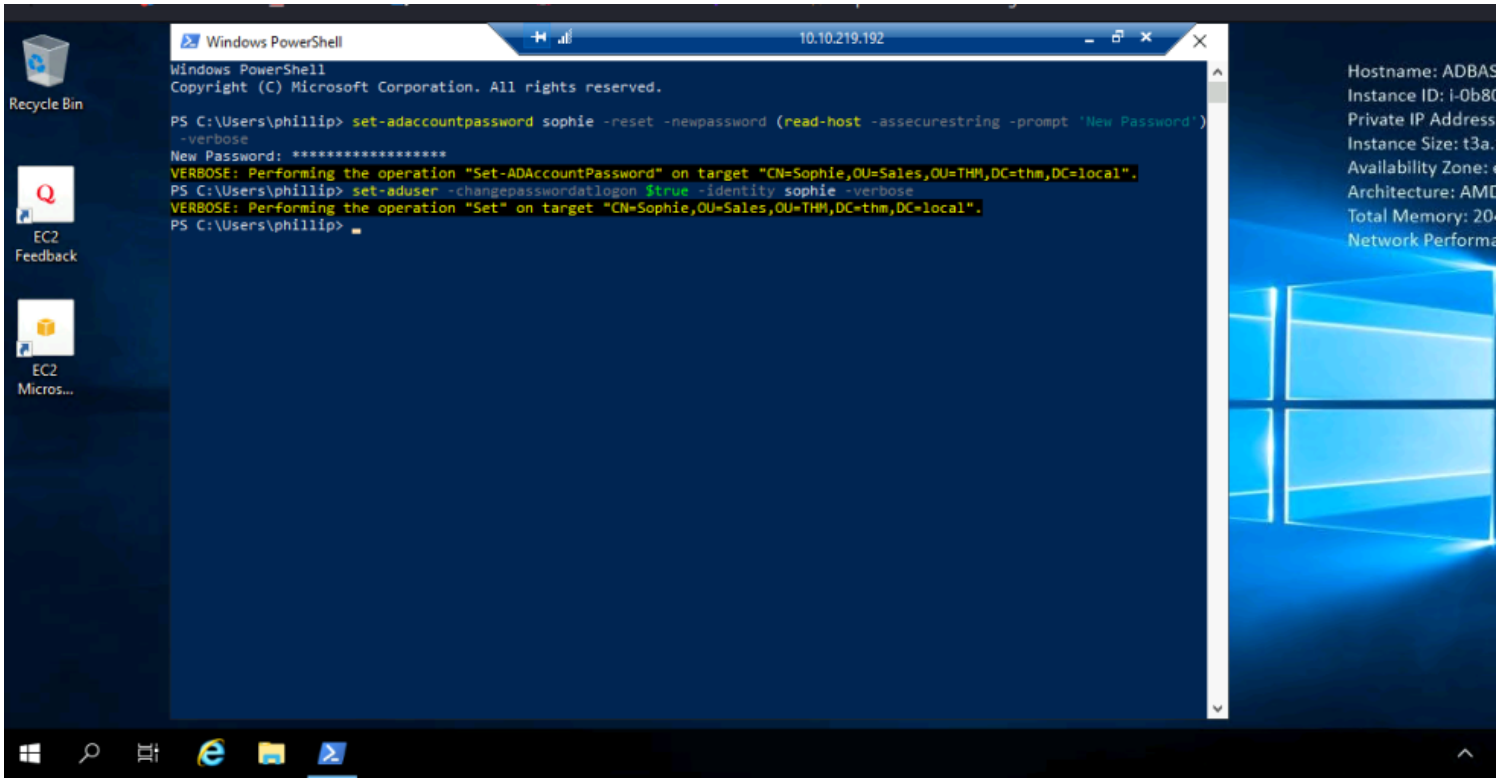




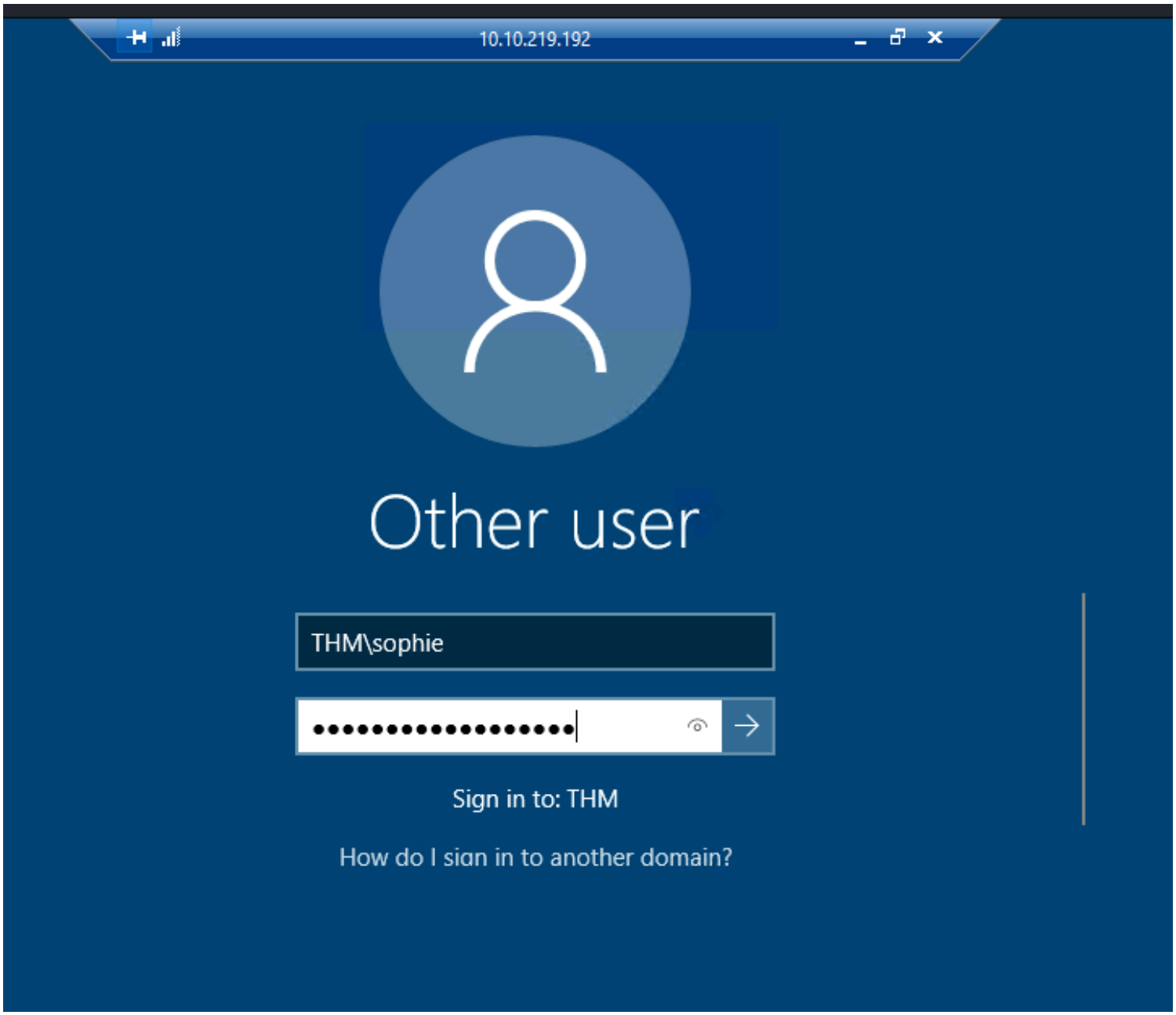
After successfully completing the delegation of control wizard, connected to user phillip via rdp as shown in image below.
And here is how I retrieved the flag.



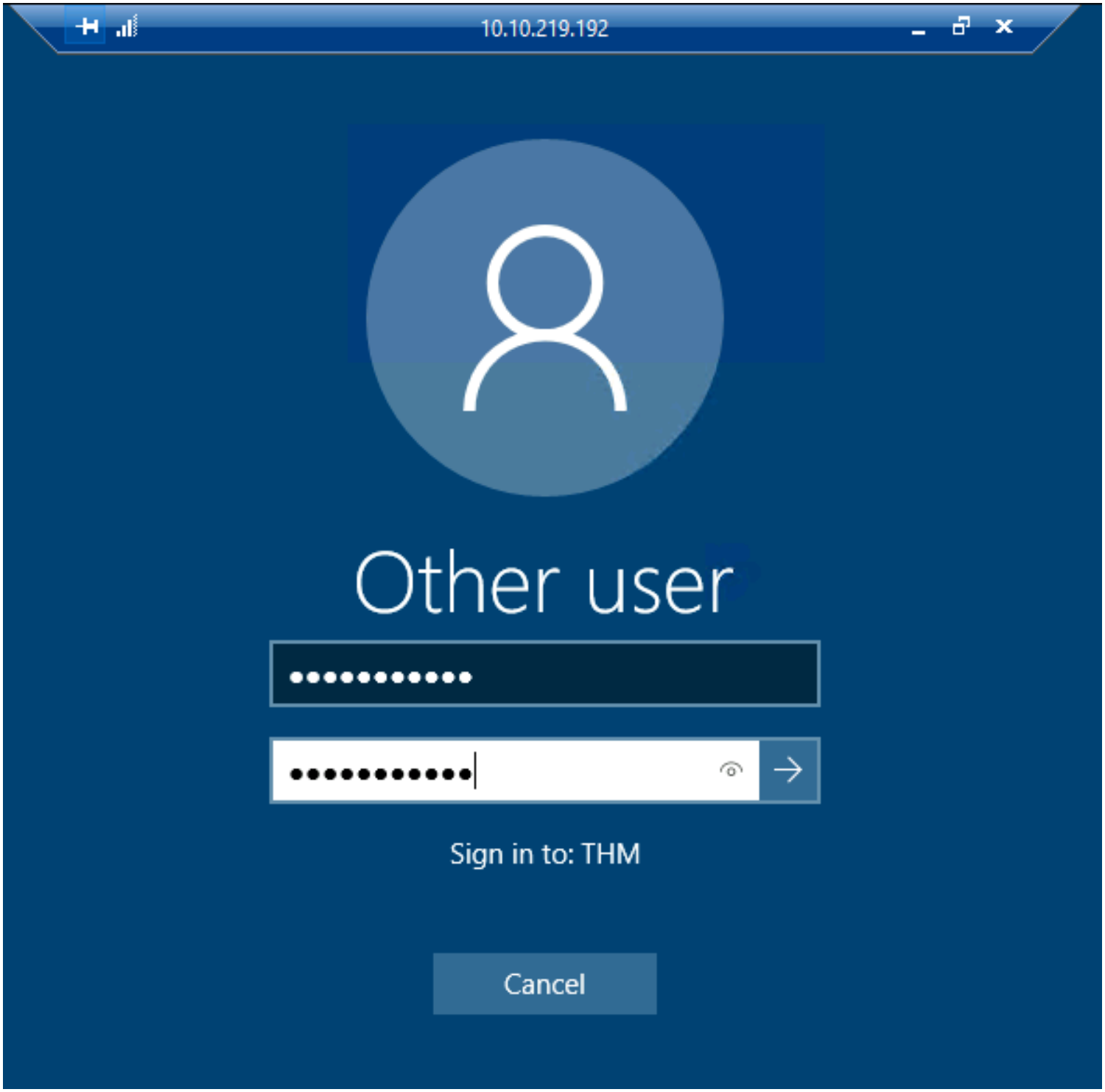
Just to confirm User Phillip had controll over other users from other groups, I tried changing the password of the user sophie as shown below



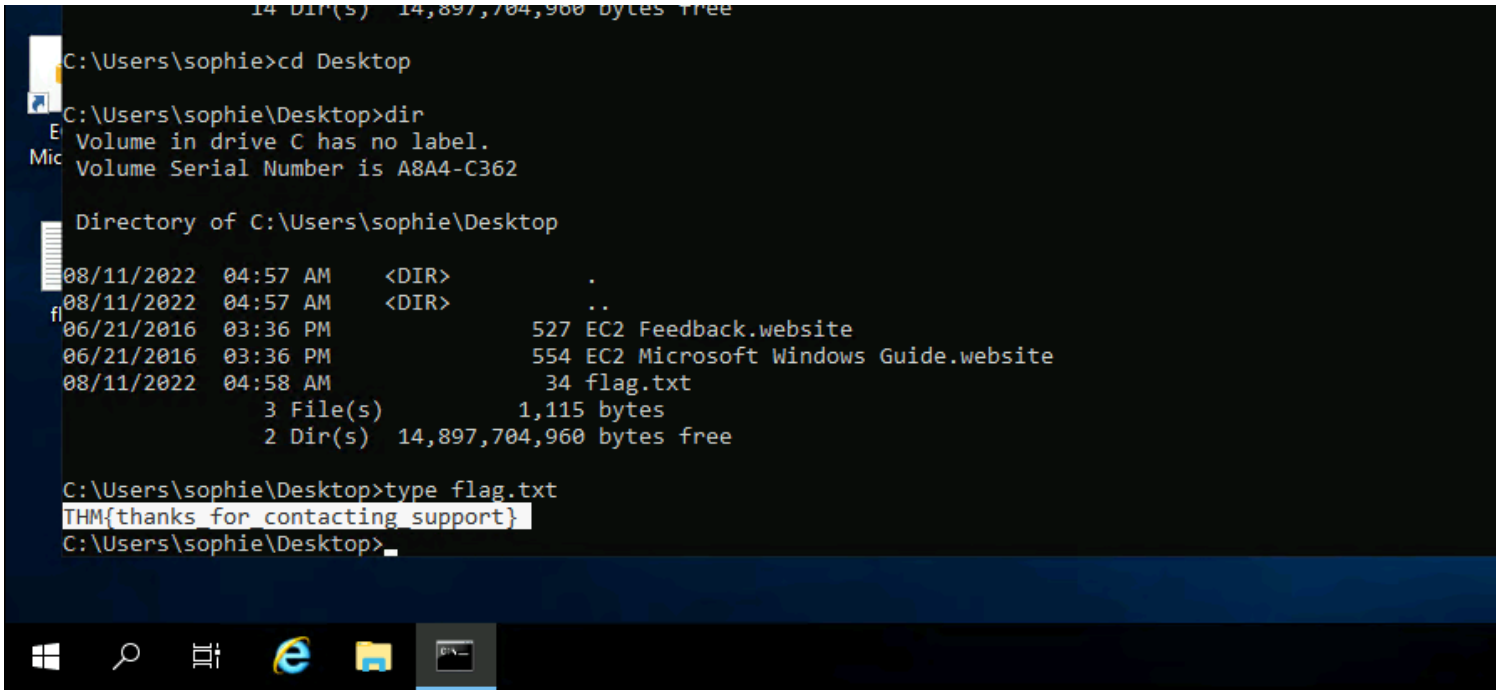
To confirm that the changes occured, I tried to use user sophie's creds to connecto to her account via rdp.



Right here I was asked to type in and confirm the new password.



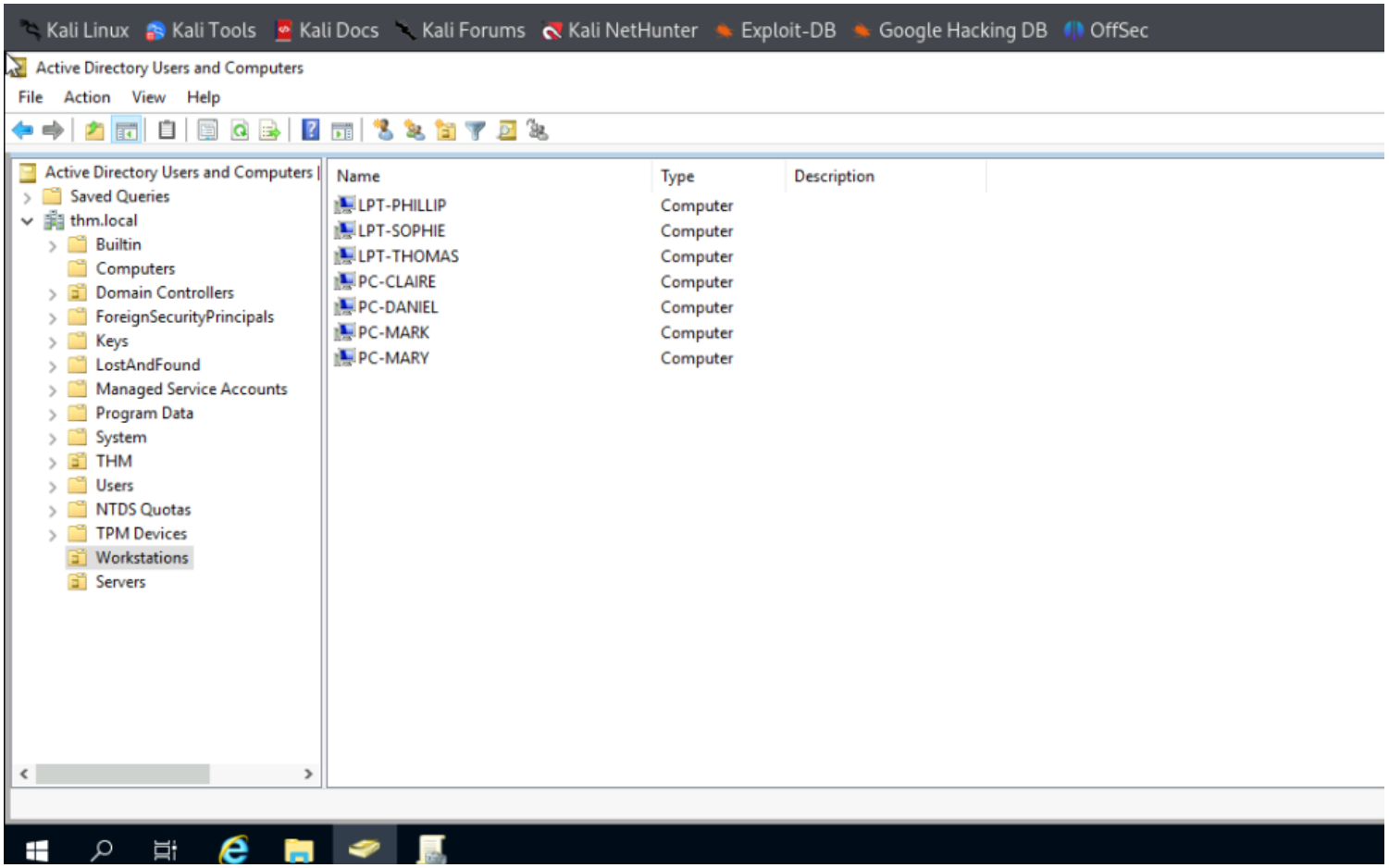
Once I successfully logged in, In the desktop directory, I read the content of flag.txt using the type command as shown in the image below.



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

7 ✓ Correct

As it can be seen from the image below, 7 computers ended up in the workstation OU.



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

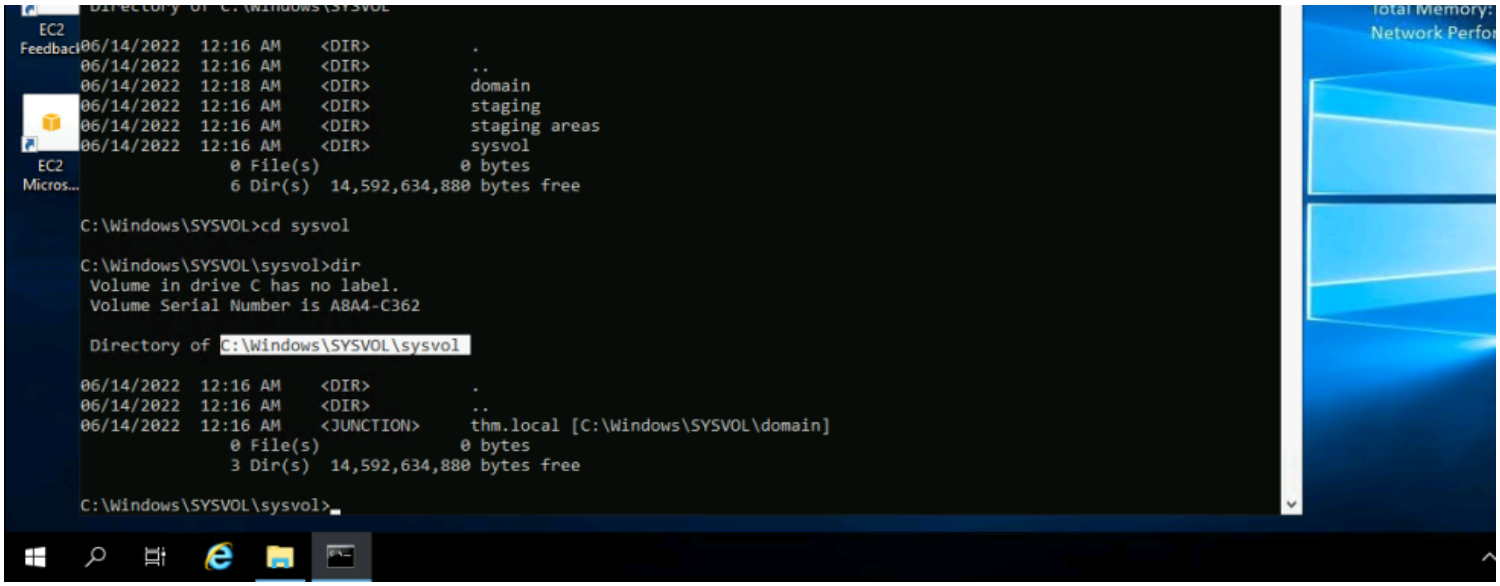
yay ✓ Correct

We can see some servers, some laptops and some PCs corresponding to the users in the AD network. Having all of our devices there is not the best idea since it's very likely that we want different policies for the servers and the machines that regular users use on a daily basis.
Since there is no golden rule on how to organise these machines, an excellent starting point is segregating devices according to their use.

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

sysvol ✓ Correct

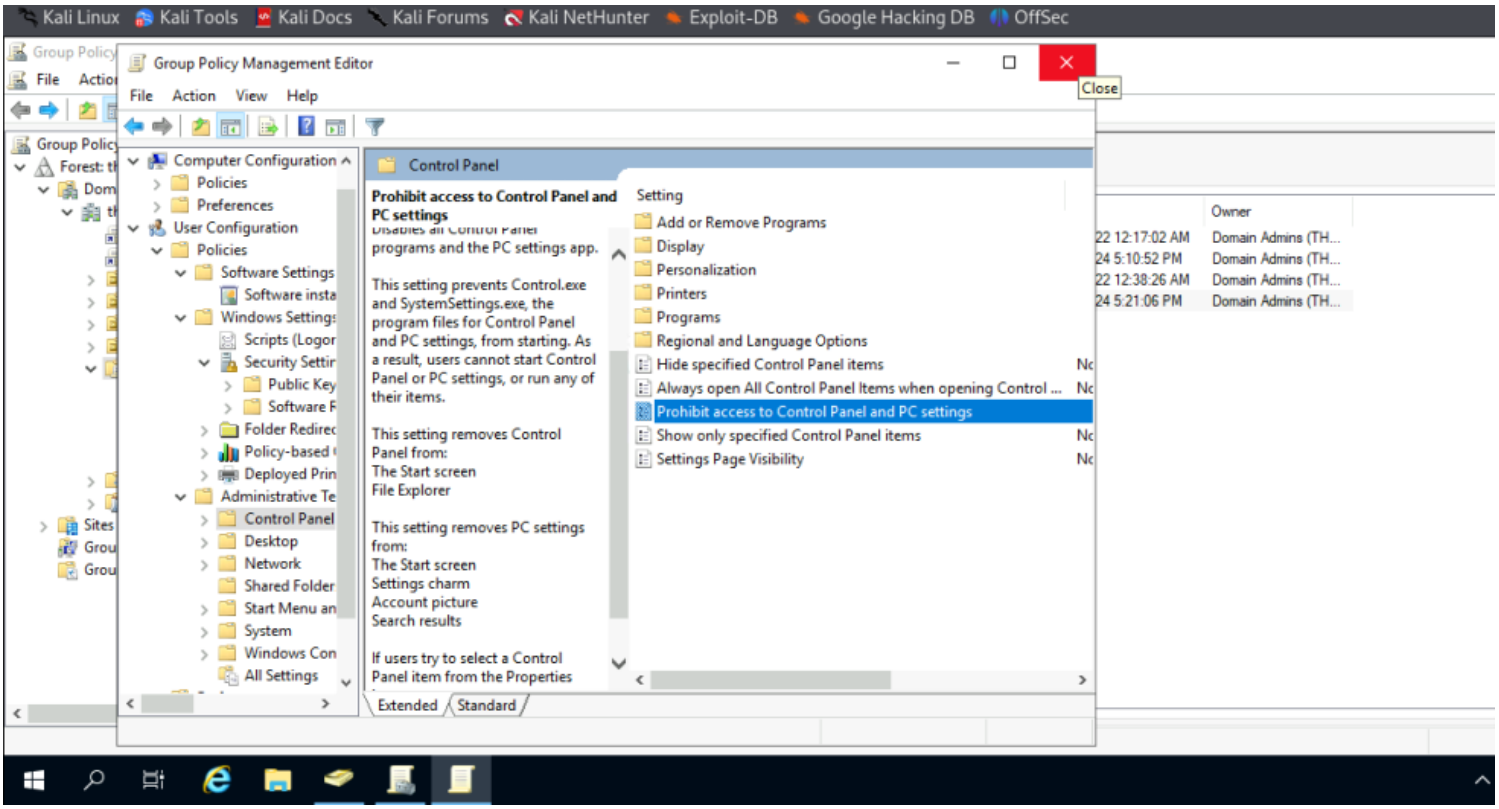
This can be seen from the image below showing the path to sysvol dir.

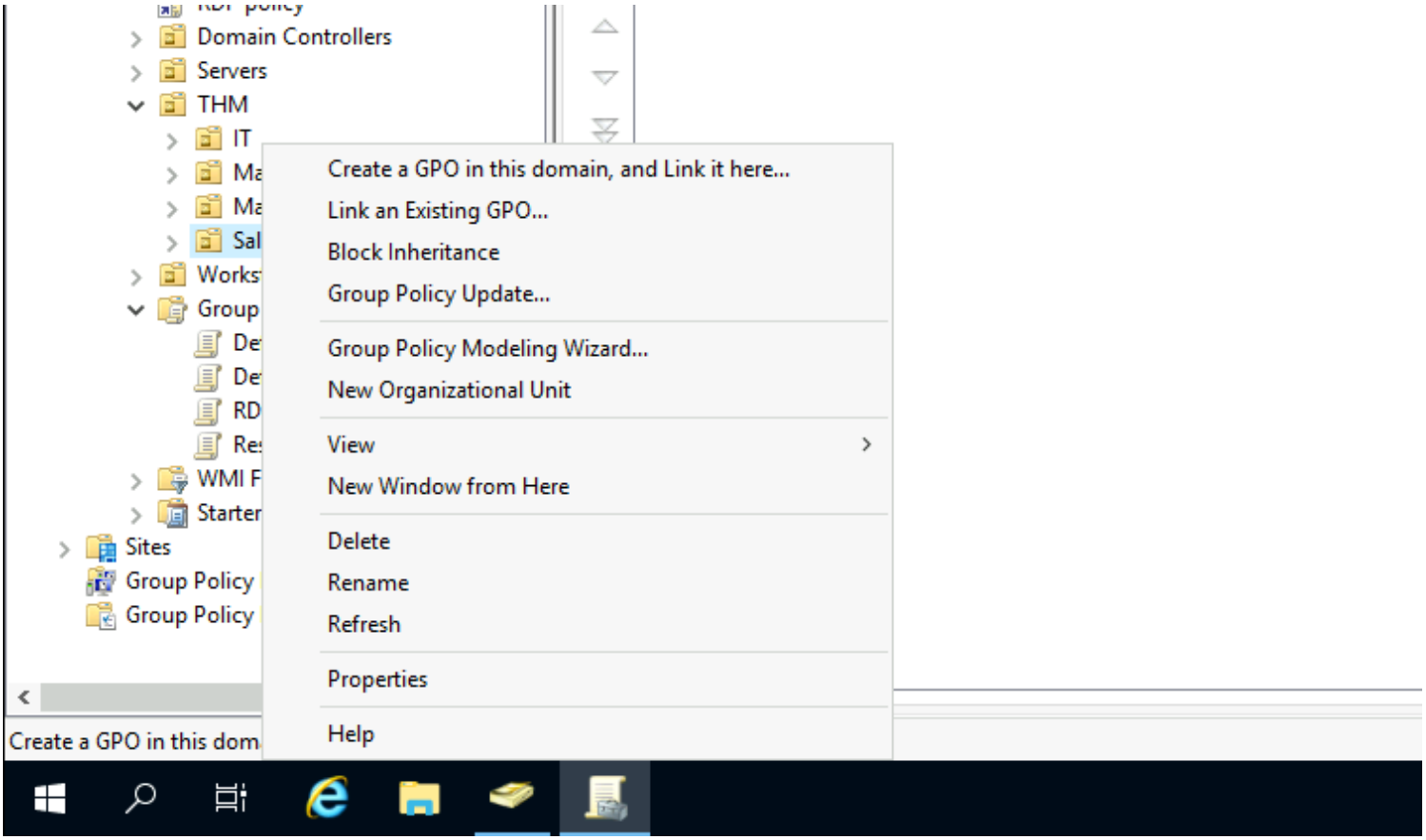


Can a GPO be used to apply settings to users and computers? (yay/nay)

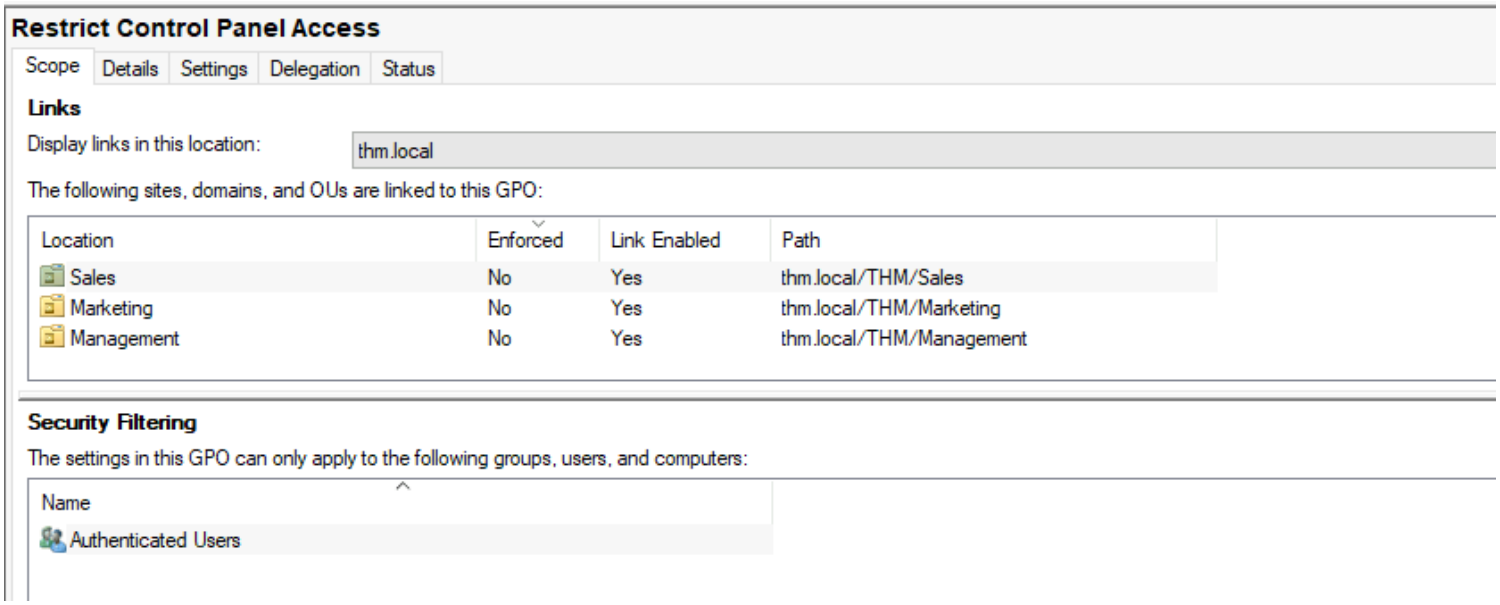
yay ✓ Correct

The images below are a proof of the answer to the question above. So basically I created a new policy that restricts other users from accessing the control panel.

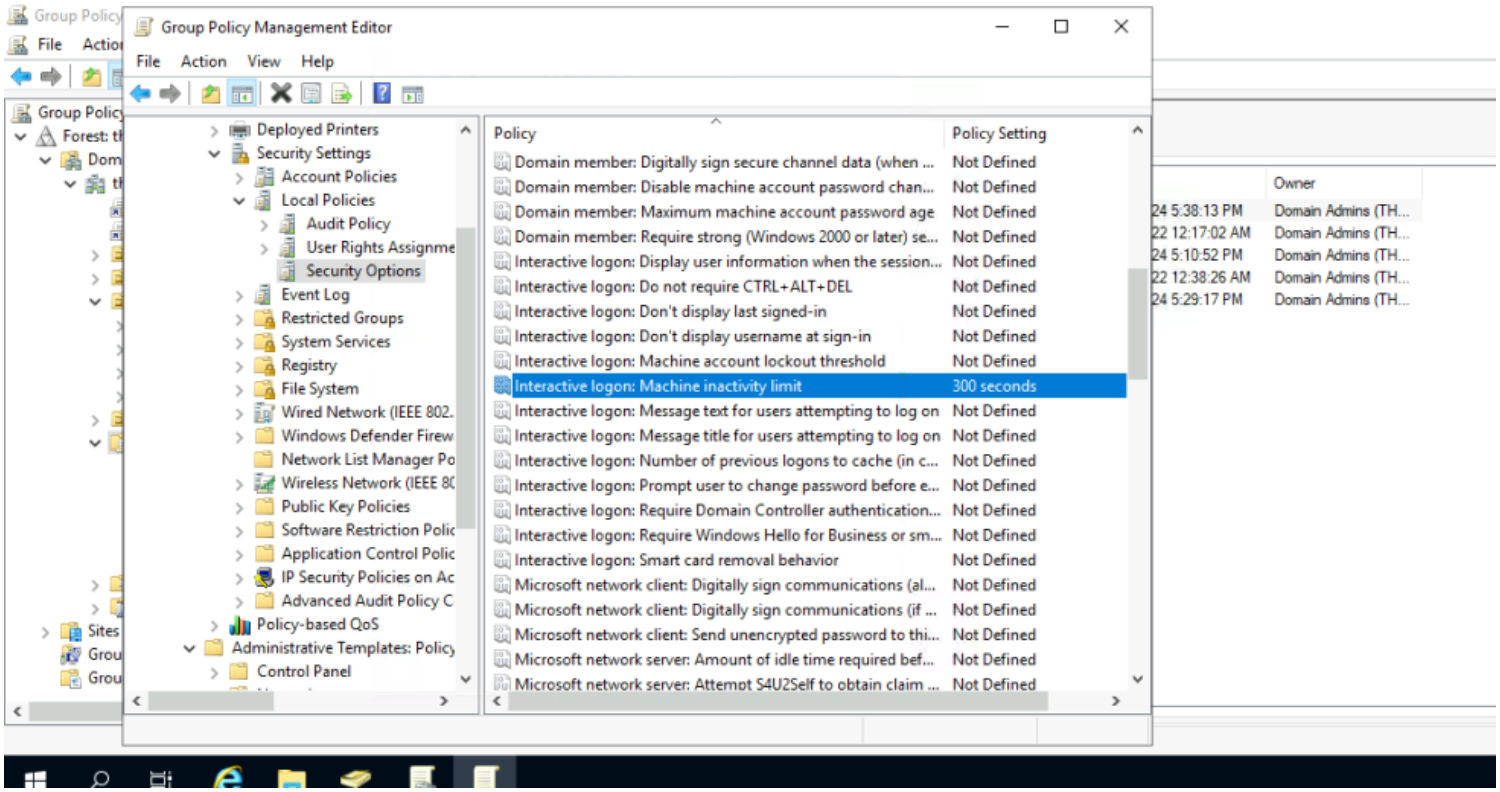


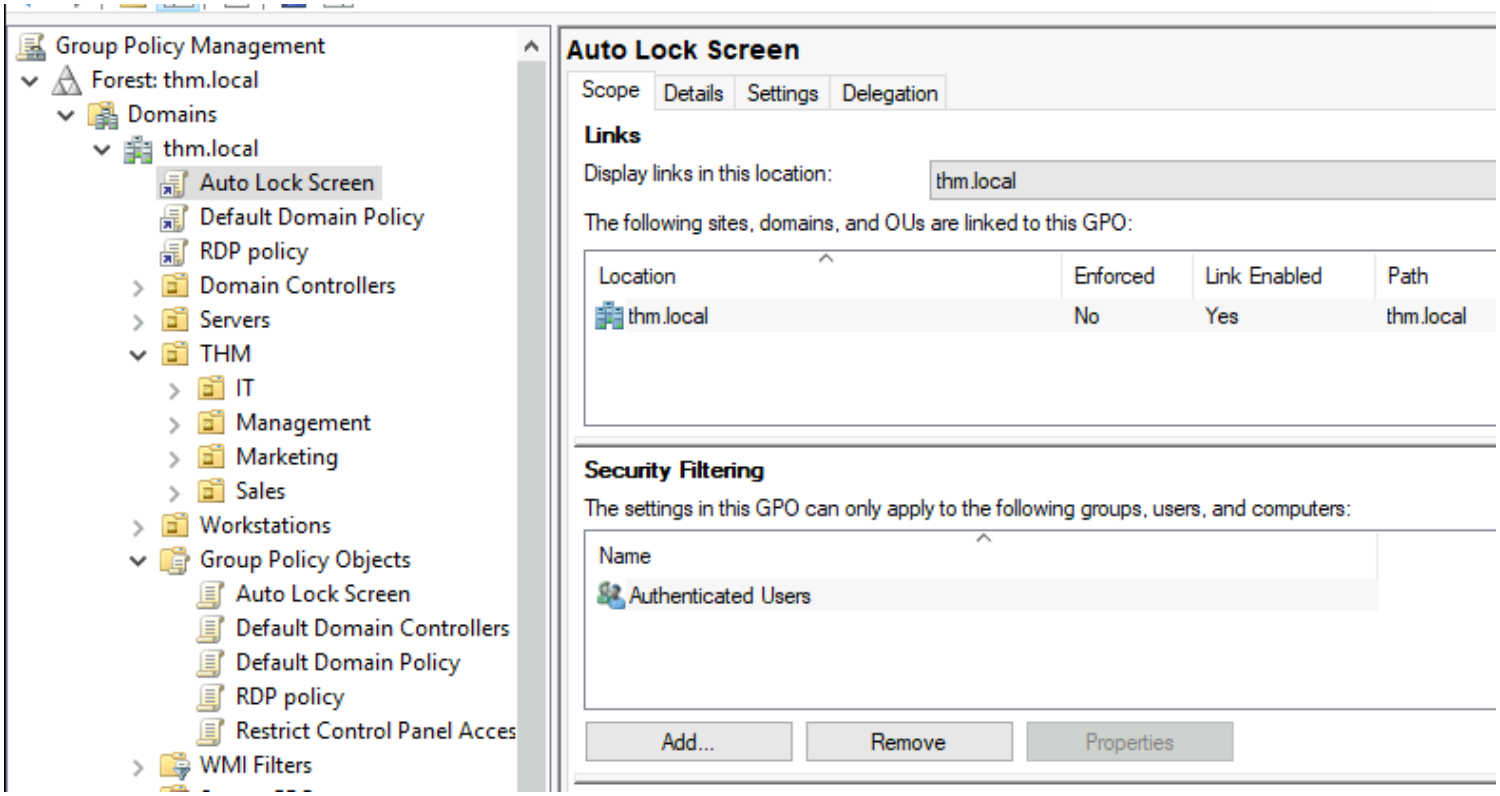


After enabling this policy on the Restrict Control Panel Access GPO, I linked it to the intended groups just as shown below.

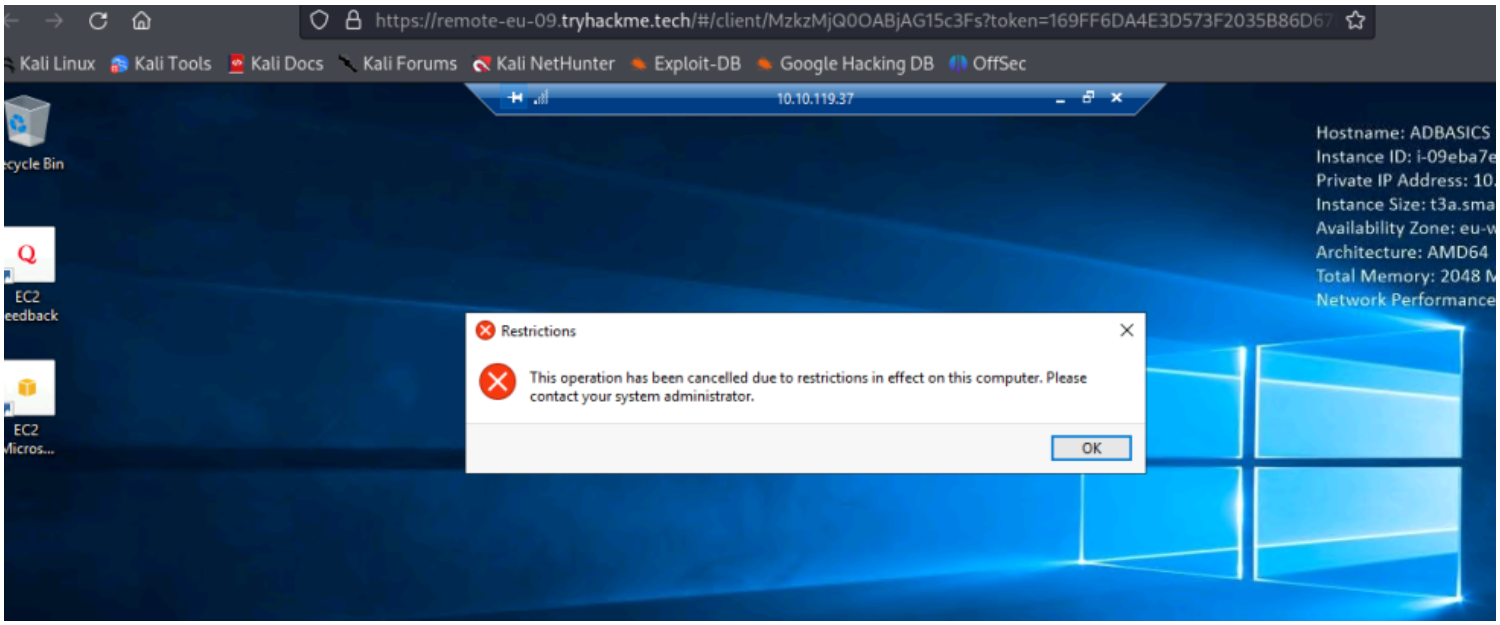


I also configured the interactive logon when the machine is inactive just as shown below.





After successfully enabling this configurations, I logged in as a different user just to confirm if the configurations I made were successfully implemented.
And as it can be seen below, I tried accessing the control panel and here was the error message as in the image below.



As you can see, you can also apply **Security Filtering** to GPOs so that they are only applied to specific users/computers under an OU. By default, they will apply to the **Authenticated Users** group, which includes all users/PCs.

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

nay

✓ Correct

Current versions of windows use kerberos authentication whereas older versions of windows use netNTLM authentication protocol.

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

Ticket Granting Ticket ✓ Correct

Ticket Granting ticket allows us to request further tickets in order to access more services when authenticated within a particular system.

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

nay ✓ Correct

User passwords are not transmitted over the network.

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

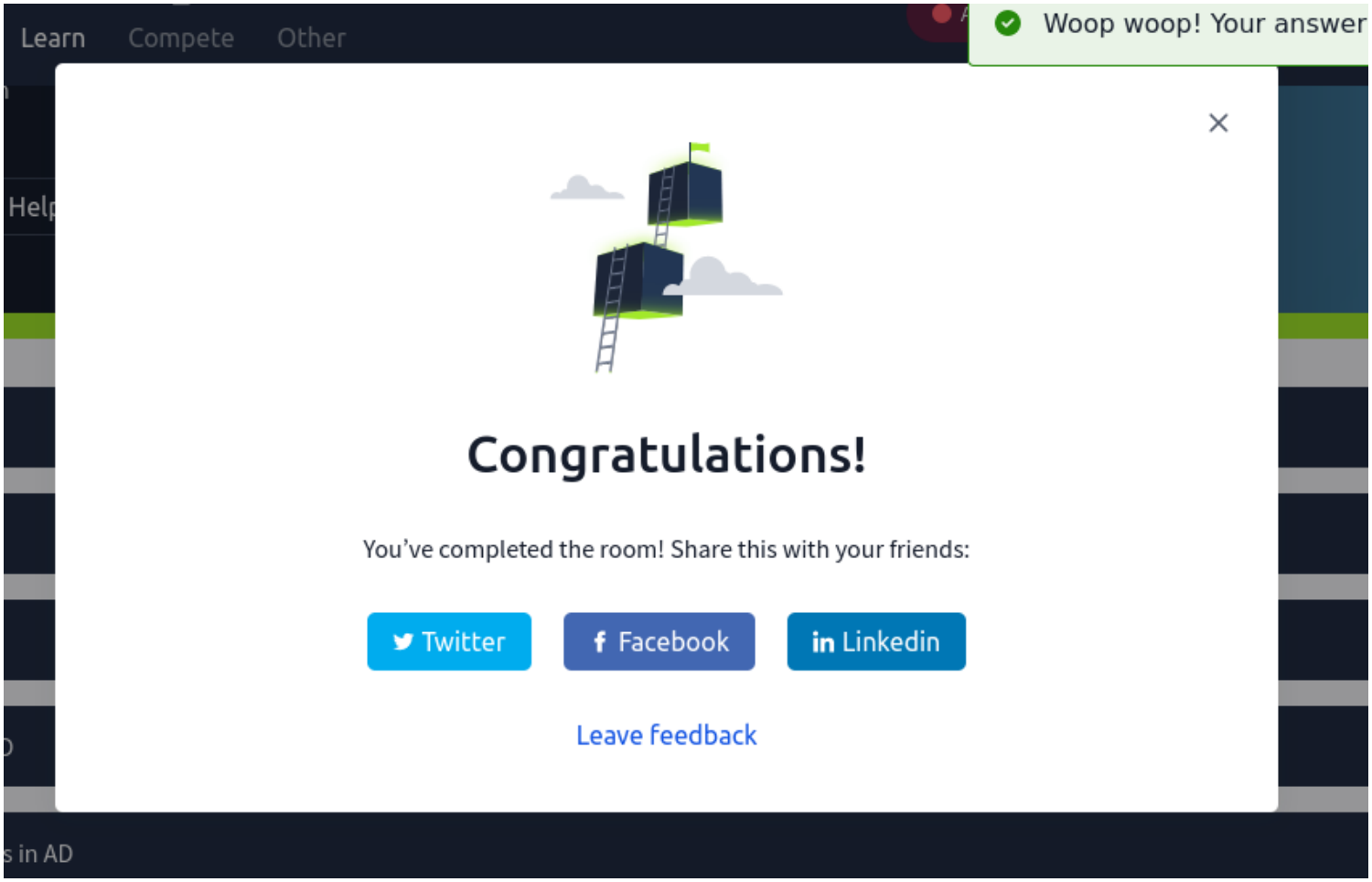
Tree ✓ Correct

Basically tree is comprised of two or more domains.

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

A Trust Relationship ✓ Correct

And this marked the end of the room.



https://tryhackme.com/r/room/winadbasics

Conclusion

In conclusion, Active Directory stands as a cornerstone for robust and efficient network management in modern enterprises. By centralizing authentication, authorization, and directory services, AD not only streamlines administrative processes but also fortifies network security. Its scalability and integration capabilities make it an indispensable tool for organizations of all sizes. Embracing Active Directory not only supports organizational growth but also ensures a secure and well-organized IT environment, paving the way for operational excellence and technological advancement.