COMP 357: ADVANCED PENTESTING

MEGA HACKING - THE FINAL PROJECT: KERBEROASTING (GROUP 02)

COMPLETED BY: TWINKALJIT SINGH

PROFESSOR: ADAM ABERNETHY

(Biggs, 2025)

1. Introduction

This document explains step-by-step how the Active Directory lab was created for Kerberoasting attack testing. The goal is to configure a reproducible Windows AD environment, containing a domain controller, workstation, user accounts, and a vulnerable service account with SPN so that Kerberoasting can be executed and later mitigated.

---

2. Lab Environment Details

Virtual Machines Used

Machine	OS Version	Purpose	Role
DC01	Windows Server 2022	Domain Controller	AD DS + DNS
WIN10-01	Windows 10	Workstation	Attacker machine

System Specs

VM	RAM	CPU	Storage
DC01	4 GB	2 cores	40 GB
WIN10-01	4 GB	2 cores	40 GB

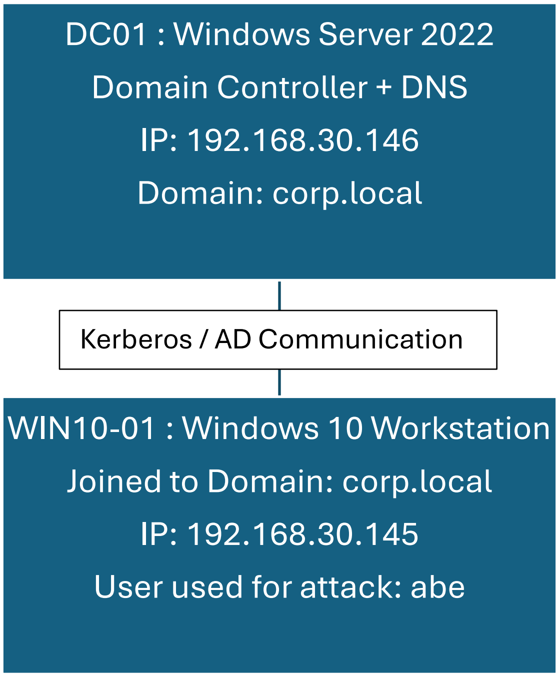
Network Configuration

Both systems are on **VMware Host-Only Network: 192.168.30.0/24**

Host	IP	DNS	Notes
DC01	192.168.30.146	192.168.30.146	Static
WIN10-01	192.168.30.145	192.168.30.146	Static

---

3. Network Diagram



DC01 : Windows Server 2022
Domain Controller + DNS
IP: 192.168.30.146
Domain: corp.local

Kerberos / AD Communication

WIN10-01 : Windows 10 Workstation
Joined to Domain: corp.local
IP: 192.168.30.145
User used for attack: abe

---

4. Domain Controller Setup (Windows Server 2022)

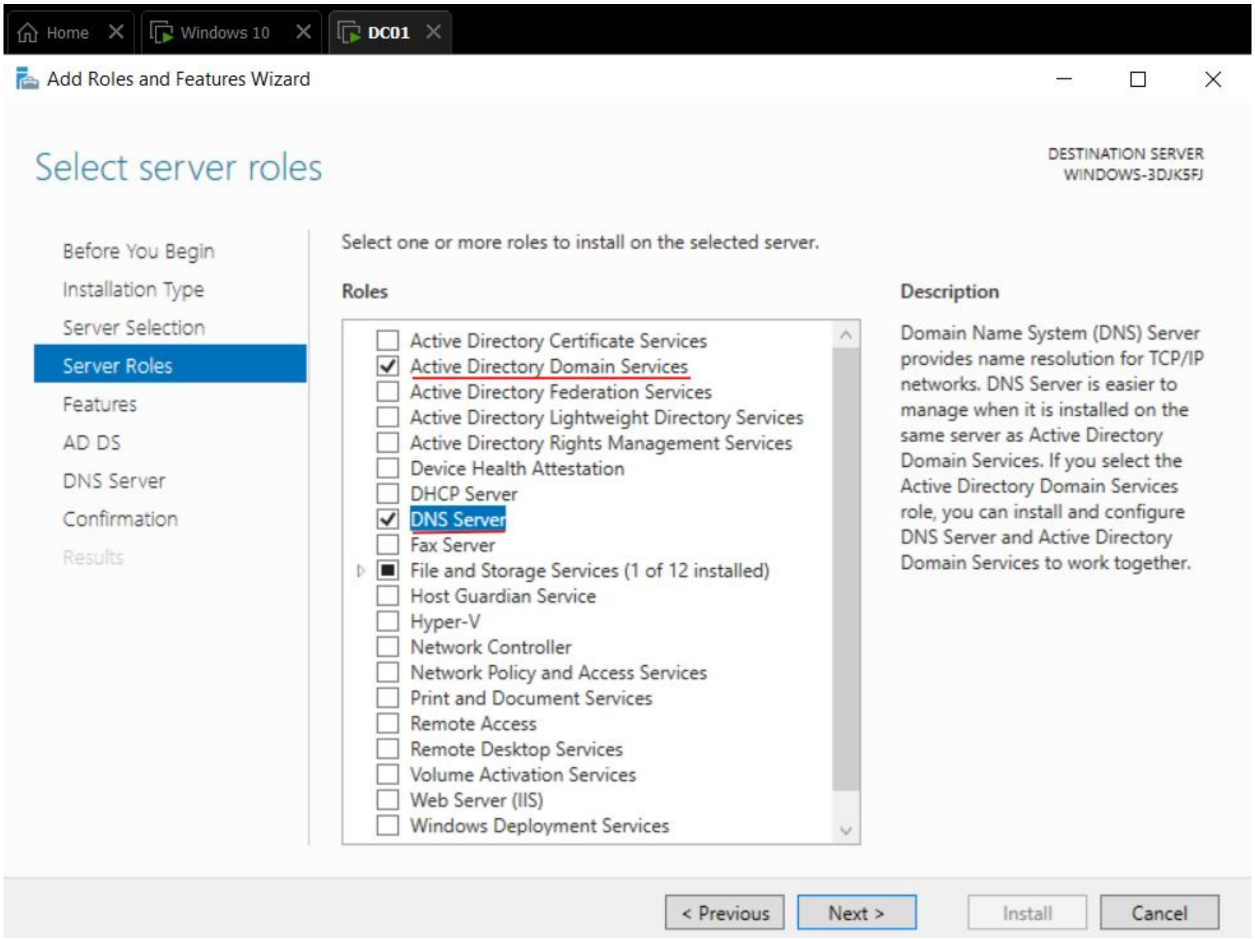
1. Configure static IP
   IPv4: 192.168.30.146
   DNS: 192.168.30.146

2. Rename computer: **DC01**

3. Open *Server Manager: Add Roles and Features*

   - Select **Active Directory Domain Services**

   - Select **DNS Server**



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WINDOWS-3DJK5FJ

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD DS
- DNS Server
- Confirmation
- Results

Select one or more roles to install on the selected server.

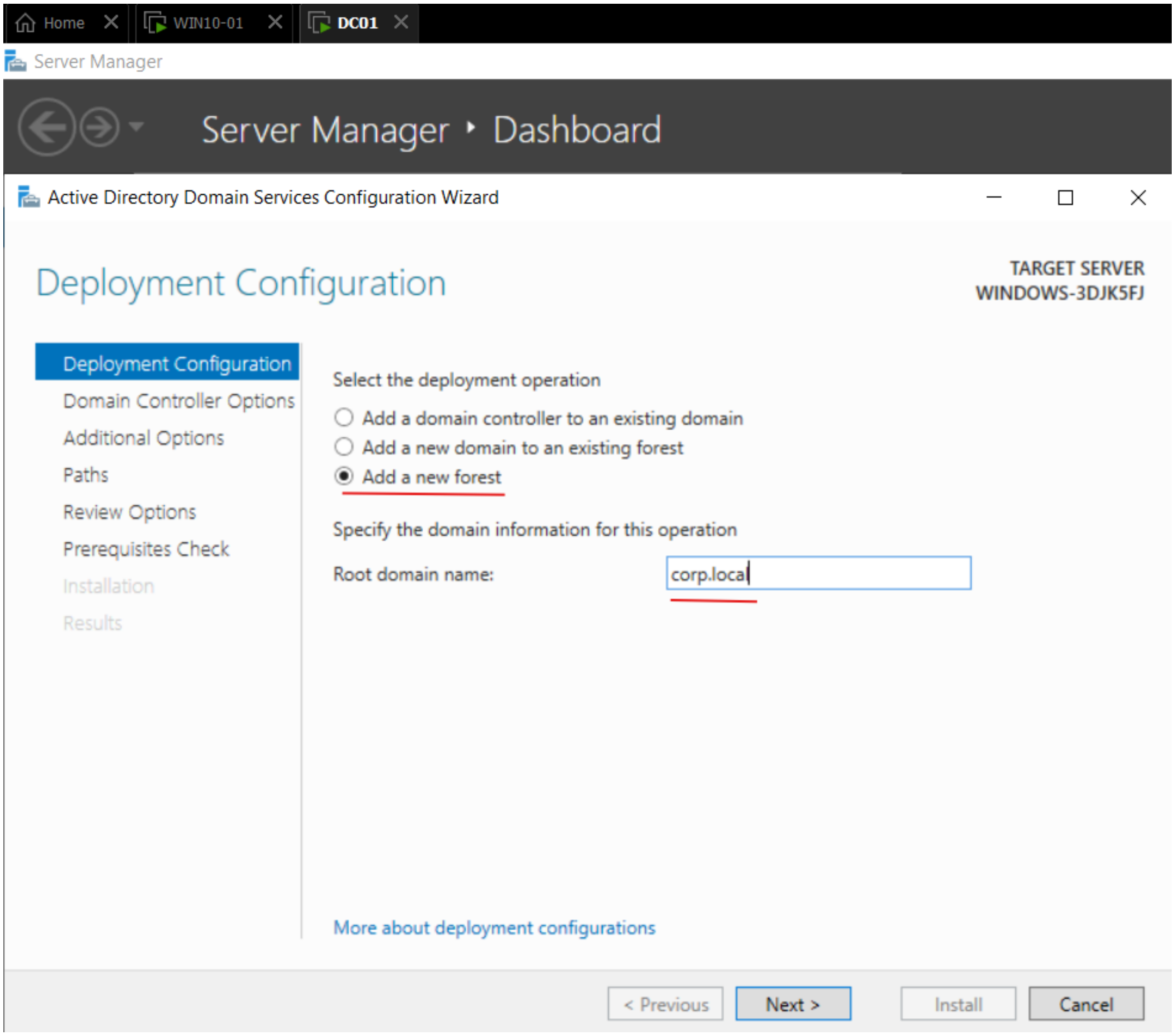
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Controller
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

4. Promote to Domain Controller
   - Select **Add new forest**
   - Domain Name: corp.local
   - Set DSRM password



Deployment Configuration

Select the deployment operation

○ Add a domain controller to an existing domain

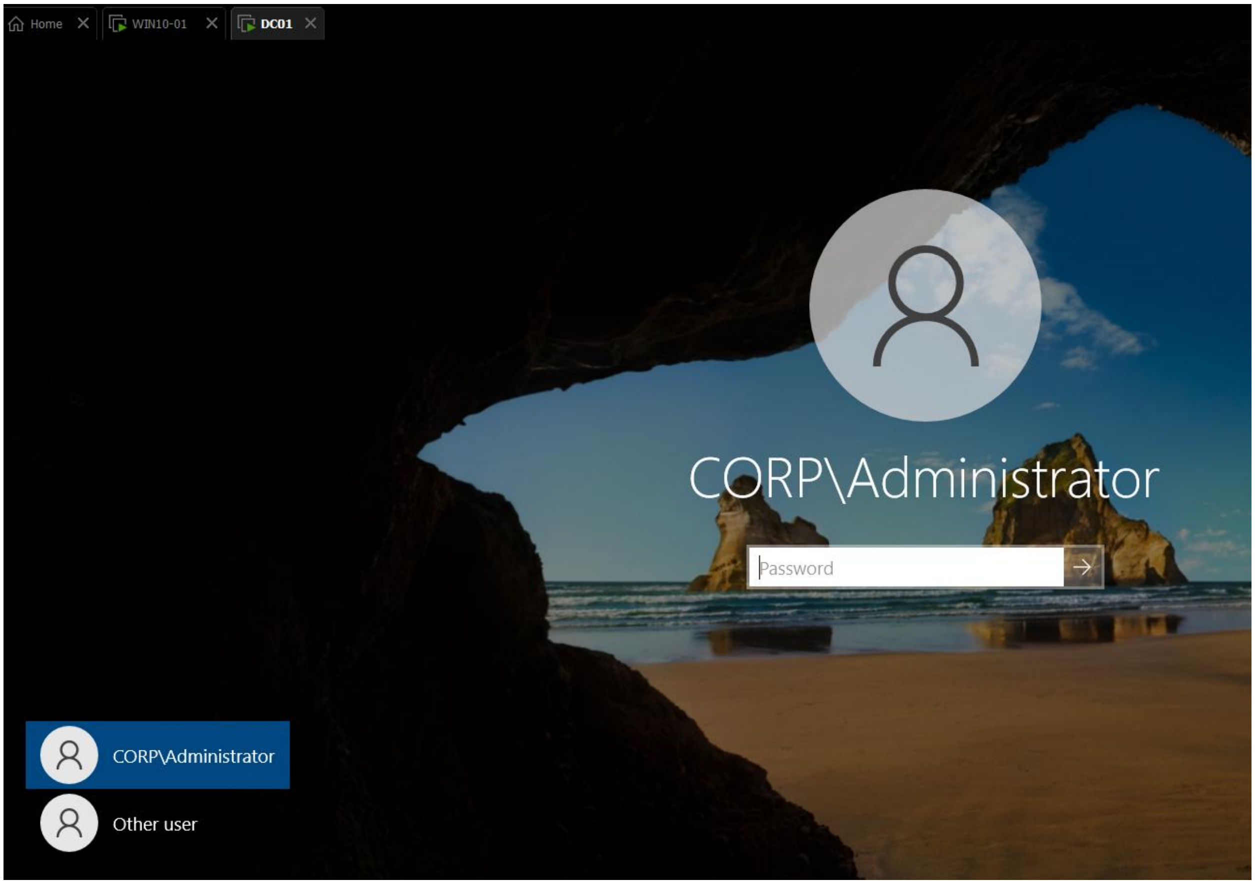
○ Add a new domain to an existing forest

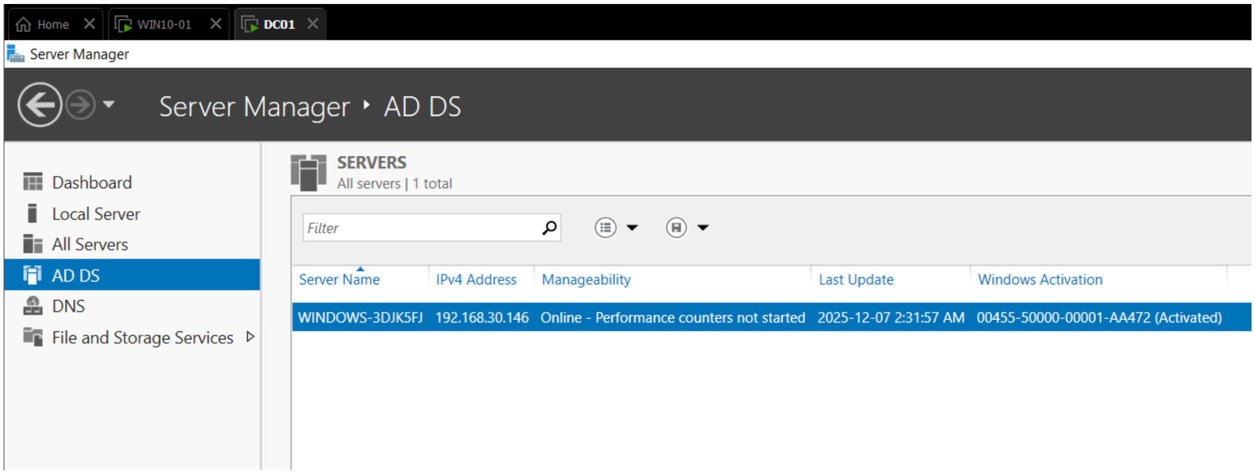
● Add a new forest

Specify the domain information for this operation

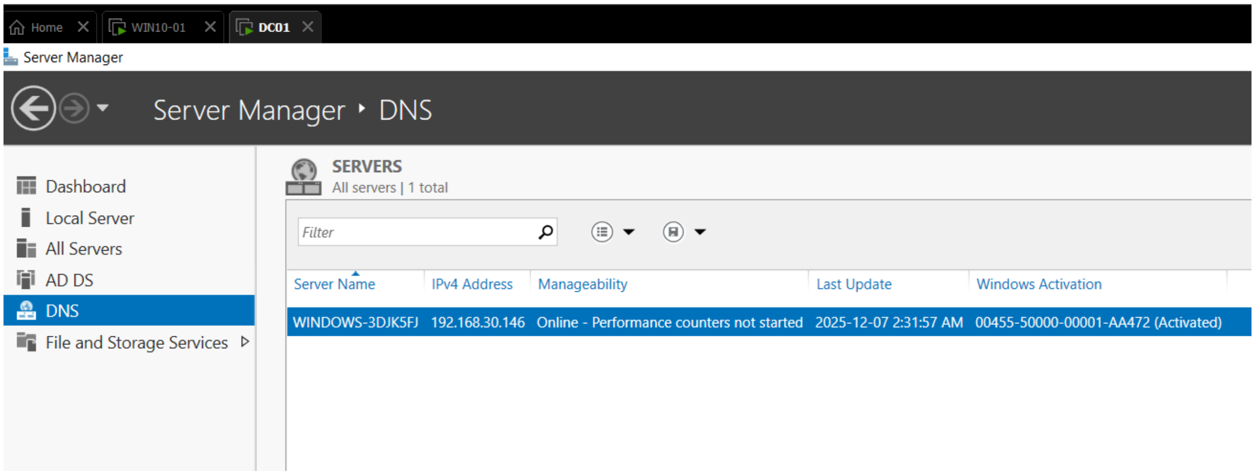
Root domain name: corp.local

5. Restart





Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WINDOWS-3DJK5FJ	192.168.30.146	Online - Performance counters not started	2025-12-07 2:31:57 AM	00455-50000-00001-AA472 (Activated)



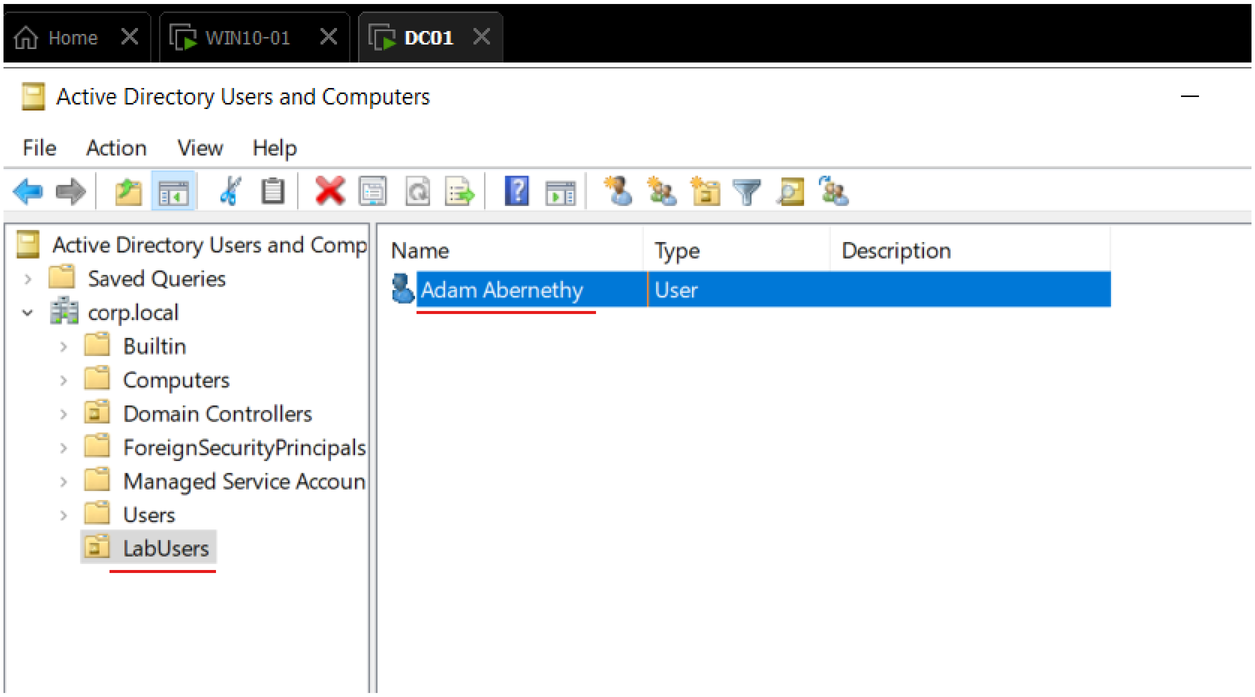
SERVERS
All servers | 1 total

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WINDOWS-3DJK5FJ	192.168.30.146	Online - Performance counters not started	2025-12-07 2:31:57 AM	00455-50000-00001-AA472 (Activated)

5. Creating Users & Service Account

Open **Active Directory Users and Computers**

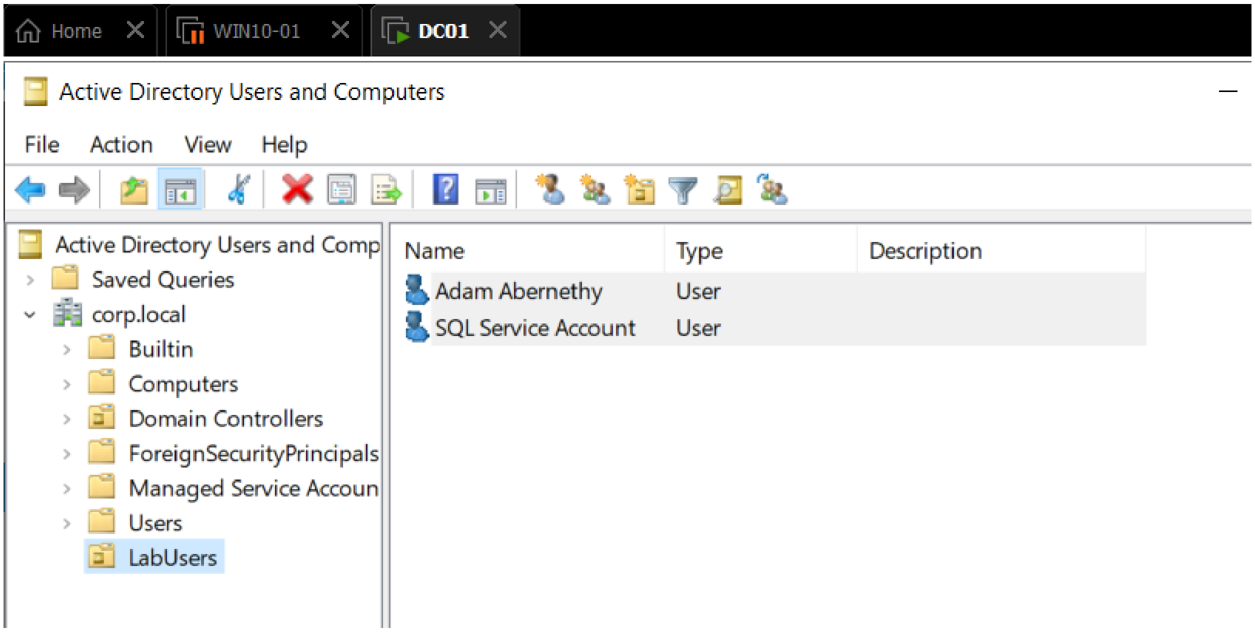
1. Create OU: **LabUsers**
2. Create normal low-priv user:
3. Name: Abe
4. User Login: abe@corp.local
5. Password: Secure but known for lab
6. Create **Service Account for Kerberoasting**
7. Name: svc-sql
8. Weak password (for lab purpose)
9. Password never expires
10. Added to Domain Admins for escalation impact



Active Directory Users and Computers

- Active Directory Users and Comp
  - Saved Queries
  - corp.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accoun
    - Users
    - LabUsers

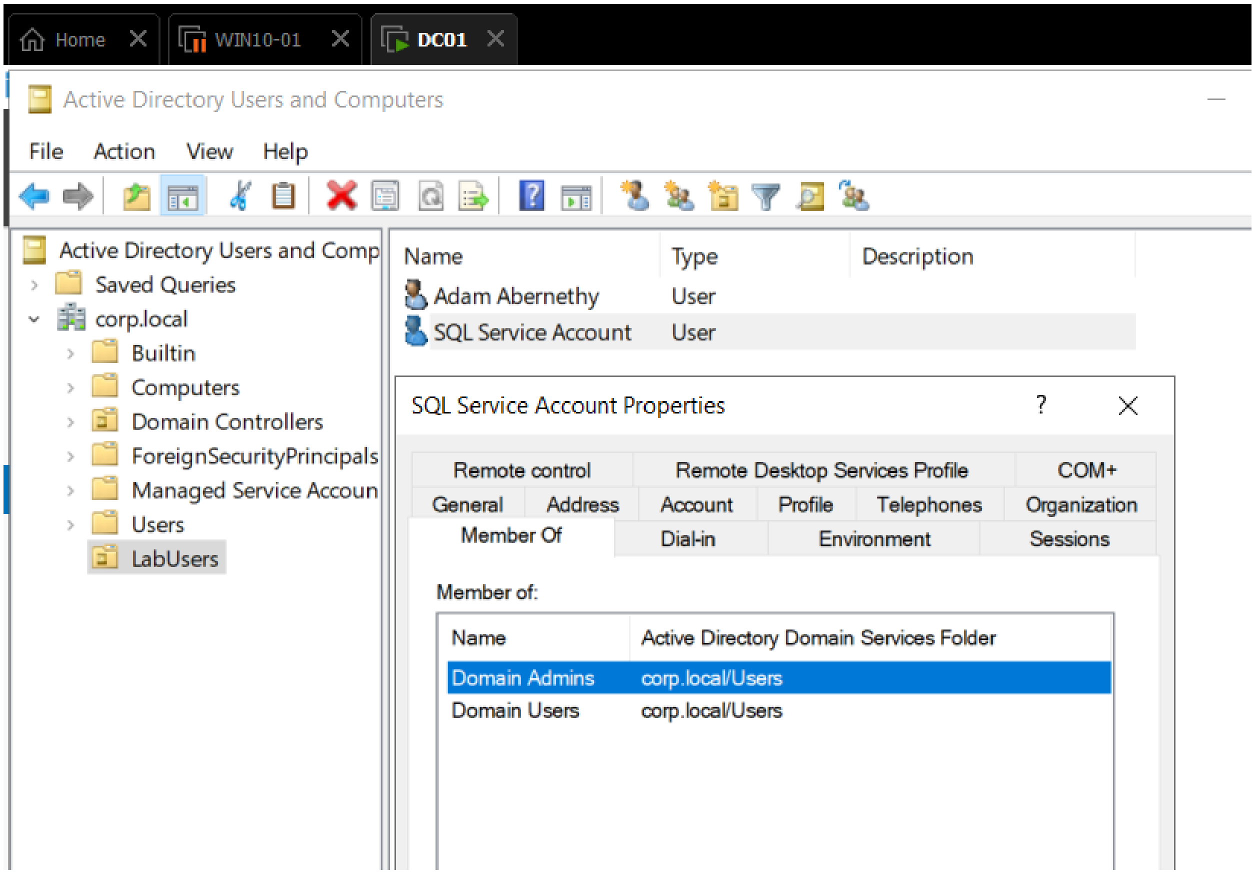
Name	Type	Description
Adam Abernethy	User	



Active Directory Users and Computers

- Active Directory Users and Comp
  - Saved Queries
  - corp.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accoun
    - Users
    - LabUsers

Name	Type	Description
Adam Abernethy	User	
SQL Service Account	User	



Name	Type	Description
Adam Abernethy	User	
SQL Service Account	User	

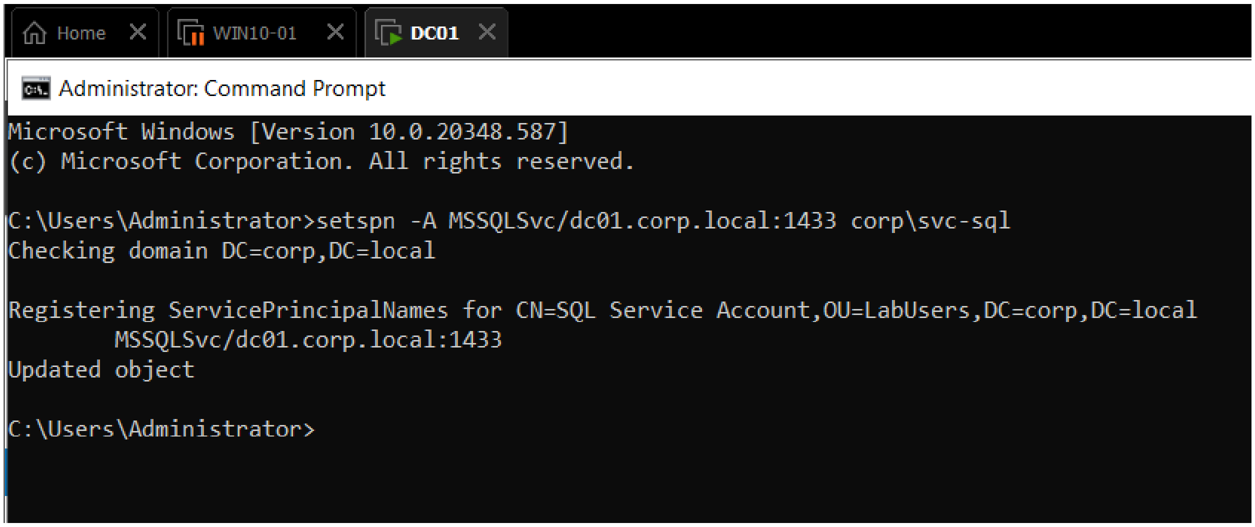
Member of:

Name	Active Directory Domain Services Folder
Domain Admins	corp.local/Users
Domain Users	corp.local/Users

6. Create SPN (Required for Kerberoasting)

On DC:

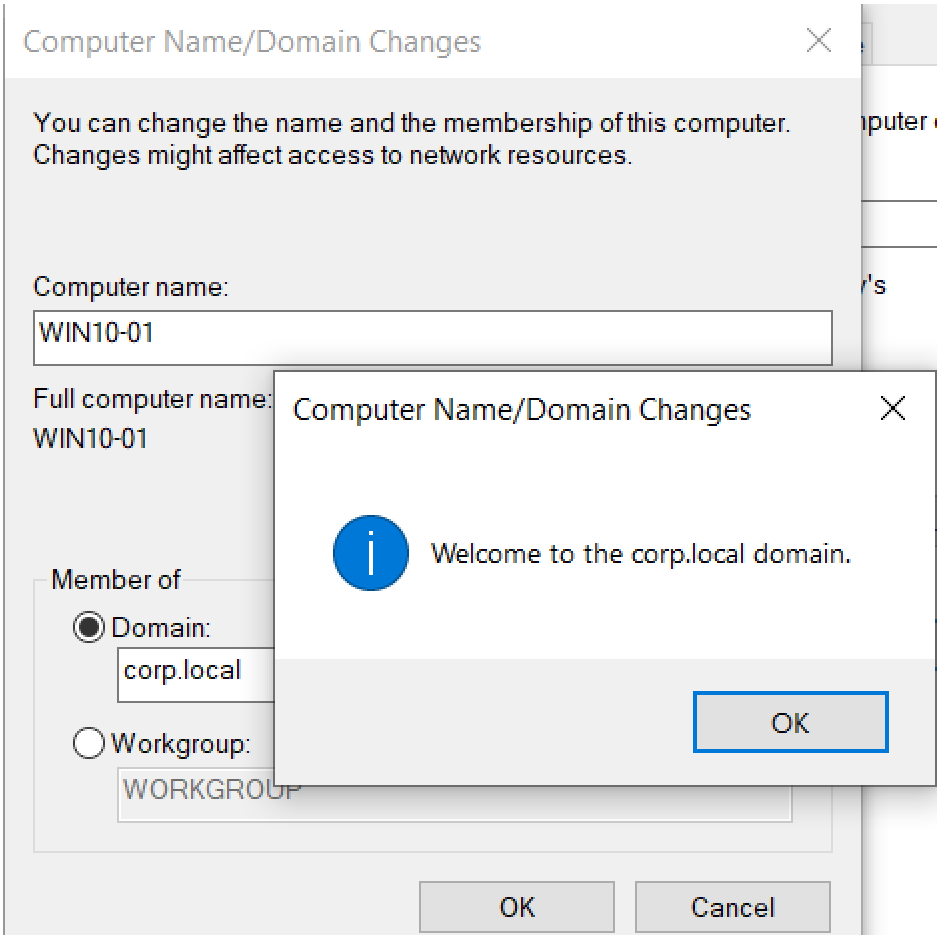
```
setspn -A MSSQLSvc/dc01.corp.local:1433 corp\svc-sql
```



```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -A MSSQLSvc/dc01.corp.local:1433 corp\svc-sql
Checking domain DC=corp,DC=local

Registering ServicePrincipalNames for CN=SQL Service Account,OU=LabUsers,DC=corp,DC=local
        MSSQLSvc/dc01.corp.local:1433
Updated object

C:\Users\Administrator>
```

7. Join Workstation to Domain (Windows 10)

1. Set static IP: 192.168.30.145, DNS 192.168.30.146
2. Rename PC: **WIN10-01**
3. Join domain
   Settings > System > About > Domain > corp.local
4. Login as corp\abe



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
WIN10-01

Full computer name:
WIN10-01

Member of
● Domain:
corp.local
○ Workgroup:
WORKGROUP

Computer Name/Domain Changes

Welcome to the corp.local domain.

---

8. Lab Environment Completed

We now have:

- **DC01.corp.local**: Domain Controller
- **WIN10-01.corp.local:** Domain Workstation
- Users:
  - **corp\abe**: attacker (low privilege)

- **svc-sql**: privileged service account with SPN