Secure Active Directory Deployment and Hardening in a Virtualized Environment

PROJECT 2

Systems and Virtualization Security

ISSM505(D)

Instructor: Benoit Desforges, MISSM, CISSP

Shovo Ghosh	ID: 155294
Kingsley Adjei-Antwi	ID: 152278
Md Mostafizur Rahman	ID: 154059
Anik Siddique	ID: 151884

CONCORDIA UNIVERSITY OF EDMONTON

Table of Contents

Introduction

This report documents the setup and hardening of a virtualized domain environment consisting of two Windows Server 2022 systems. One server is configured as the Domain Controller (DC), while the other serves as the File Server. A Windows 10 client is used for testing permissions and Group Policy configurations. Kali Linux was used for Nessus vulnerability scans. The goal of the project was to implement Active Directory (AD), configure Group Policies, set up permissions, and use security tools to evaluate and harden the environment**.**

Lab Setup

Virtualization Environment:

- VMware Workstation was used to create and manage the virtual machines.

System Details:

- **Windows Server 2022 (Domain Controller)**: Configured as a Domain Controller for the mydomain.local domain.
- **Windows Server 2022 (File Server)**: Configured as a file server and joined to the domain.
- **Windows 10 Client**: Joined to the domain to test permissions and Group Policy.
- **Kali Linux**: Used for Nessus vulnerability scans to assess security risks in the environment.

Network Configuration:

- Subnet: 192.168.56.x
- Domain Controller IP: 192.168.56.101
- File Server IP: 192.168.56.102
- Windows 10 Client IP: 192.168.56.103
- Kali Linux IP: 192.168.56.104 (for Nessus only).
- Gateway: 192.168.56.1

Setup Process:

- Installed and configured **Windows Server 2022** as a Domain Controller and **File Server**.
- Joined the Windows 10 client to the domain.

- Configured shared folder structure on the **File Server** (C:\TestData\Users, Jobs, and Accounts) with appropriate permissions.

Install Active Directory Domain Services (AD DS)

1. Log in to your primary VM running Windows Server 2022.
2. Open Server Manager (it should open automatically at login; if not, find it in the Start menu).
3. In Server Manager, click on Add Roles and Features from the Dashboard.
4. In the Add Roles and Features Wizard:
    - Before You Begin: Click Next.
    - Installation Type: Choose Role-based or feature-based installation and click Next.
    - Server Selection: Select your server from the server pool and click Next.
    - Server Roles:
        - Scroll down and select Active Directory Domain Services.
        - A pop-up window will appear, asking if you want to add features required for AD DS. Click Add Features.
        - Click Next.
5. Features:
    - Leave the default selection (no additional features are necessary for AD DS).
    - Click Next.
6. AD DS Overview:
    - This page gives an overview of AD DS. Click Next.
7. Confirmation:
    - Review your selections and click Install.
8. Installation Progress:
    - Wait for the installation to complete (this may take a few minutes).

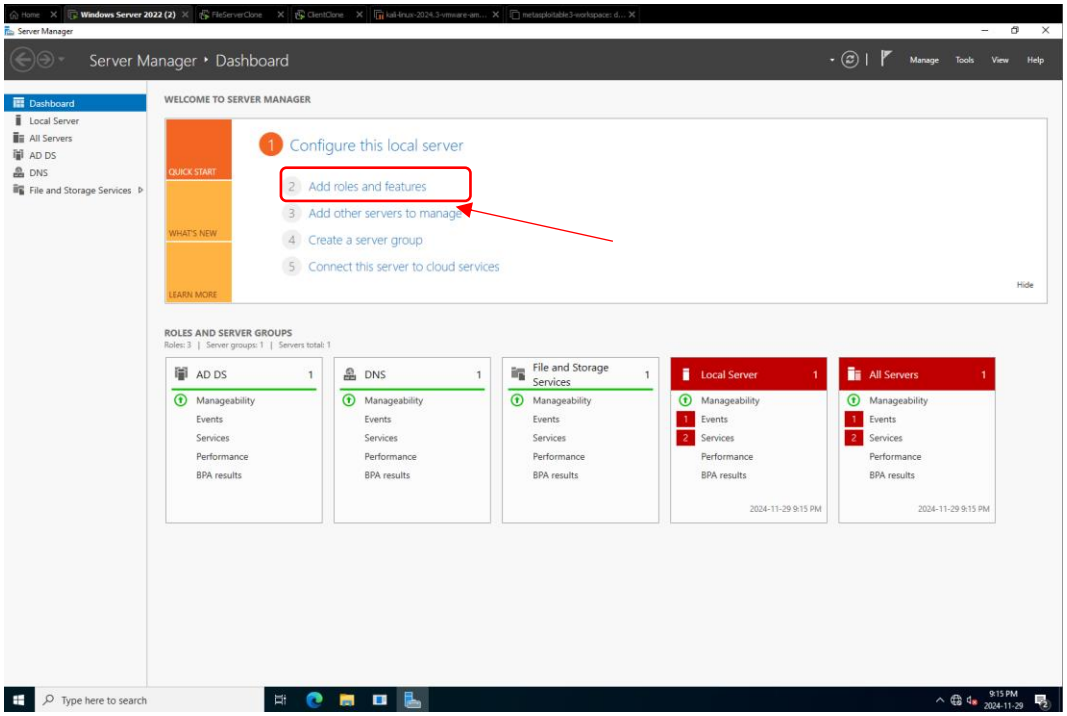


Figure 1 Select add roles and features

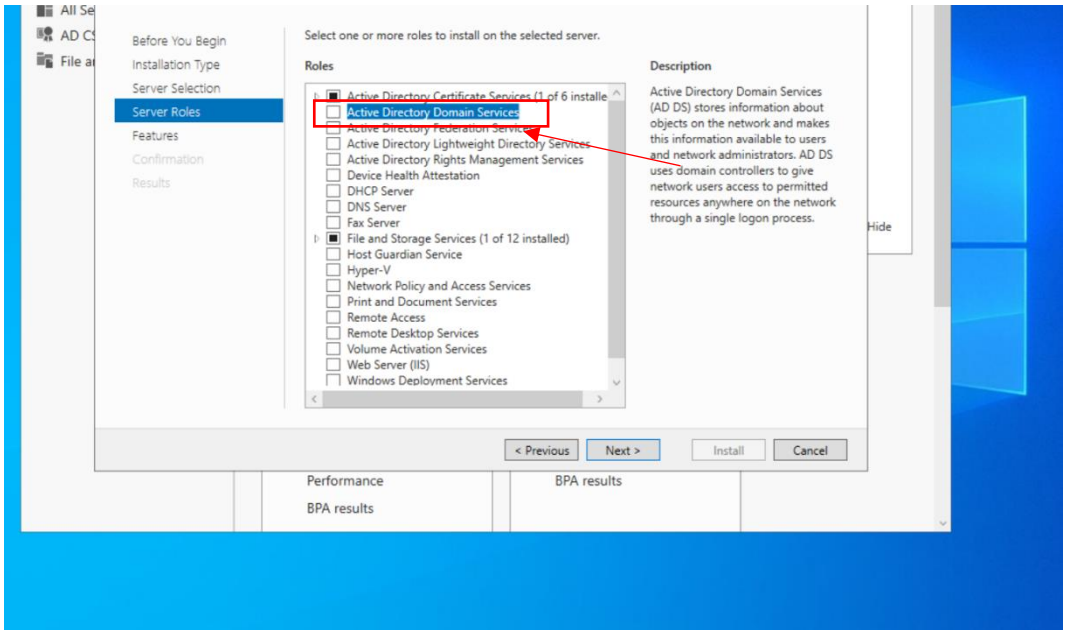


Figure 2 check ADMS

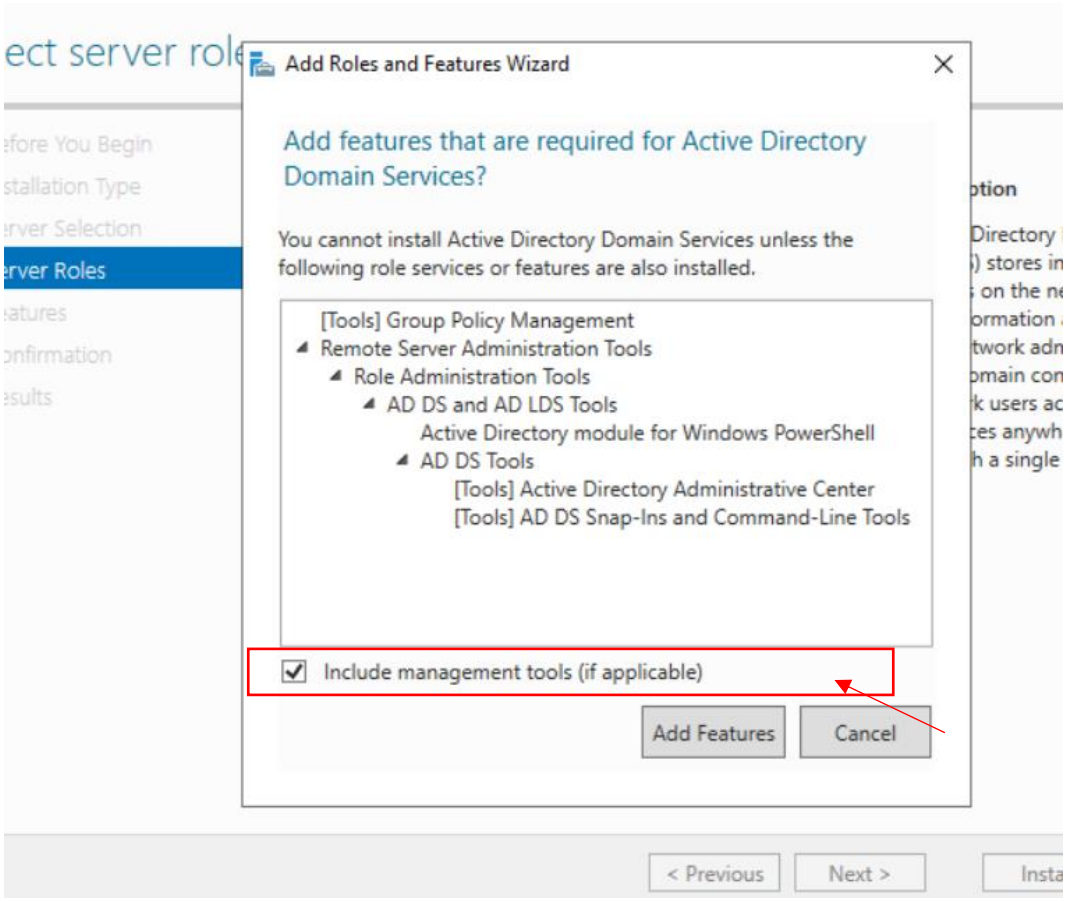


Figure 3 check include management tools and click add features

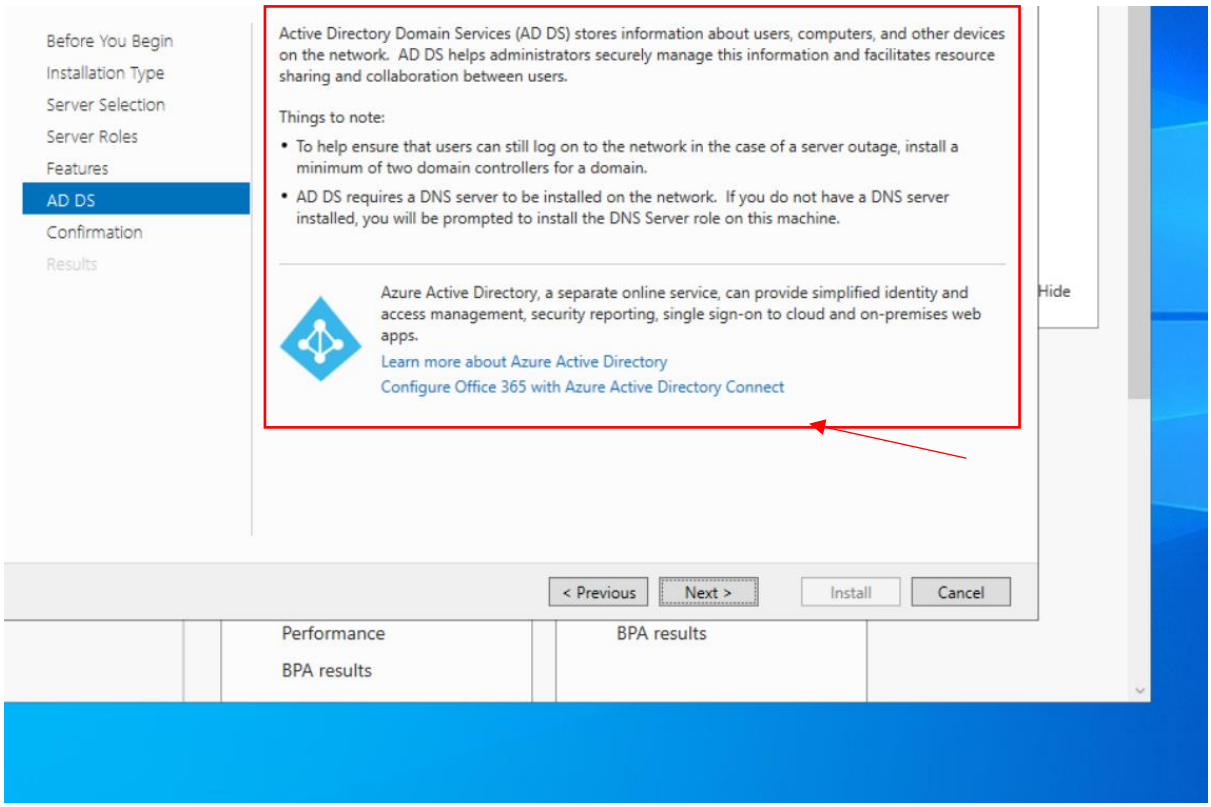


Figure 4 read this information on AD DS and click next

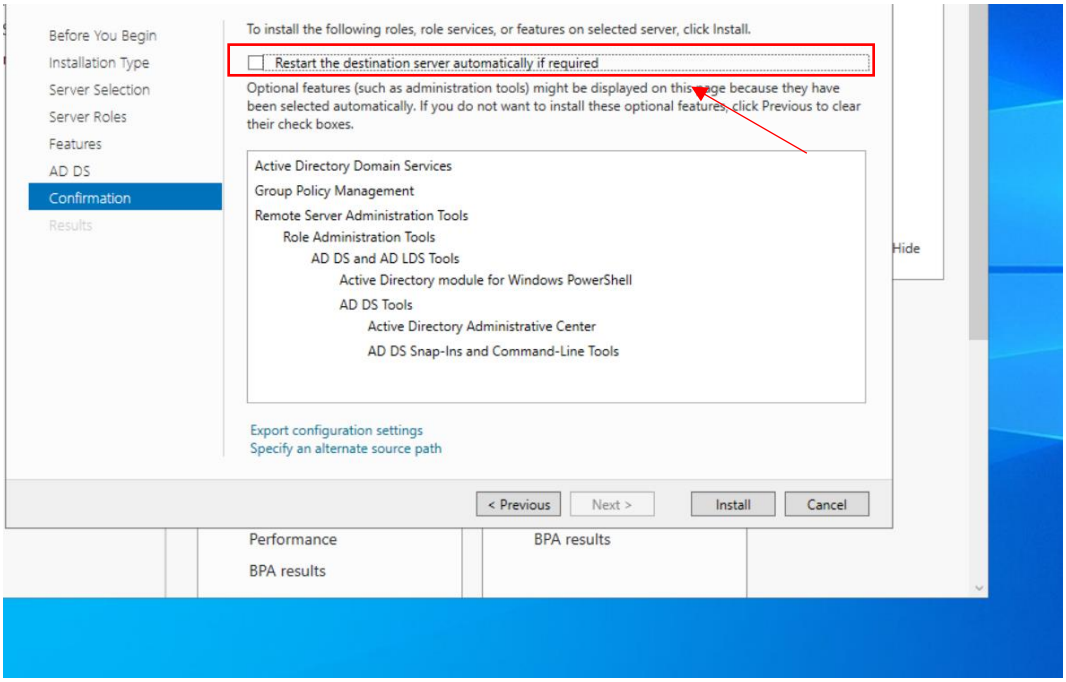


Figure 5 check restart the destination and click next

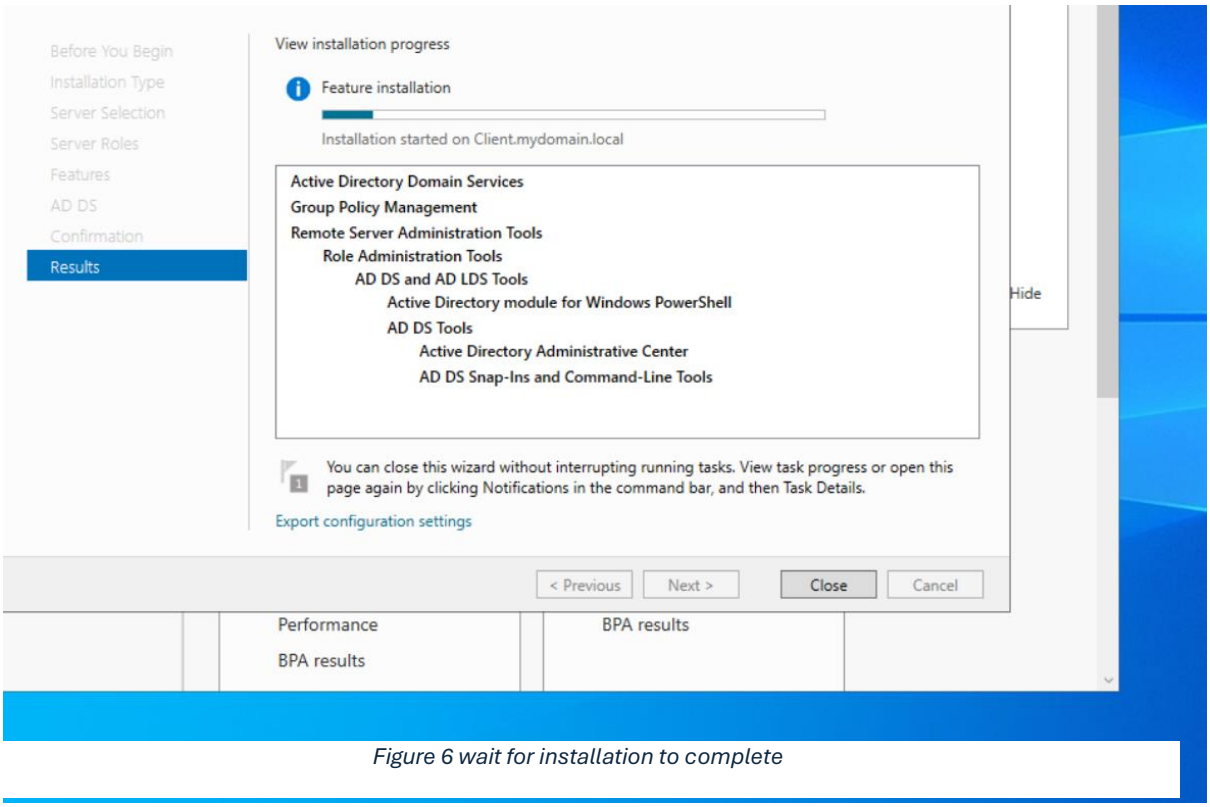


Figure 6 wait for installation to complete

- Once installation is complete, you will see a notification in Server Manager with an option to Promote this server to a domain controller. Click this link.

Promote Server to Domain Controller

1. In the Active Directory Domain Services Configuration Wizard:
    - Deployment Configuration:
        - Select Add a new forest.
        - In the Root domain name field, enter your desired domain name (mydomain.local).
        - Click Next.

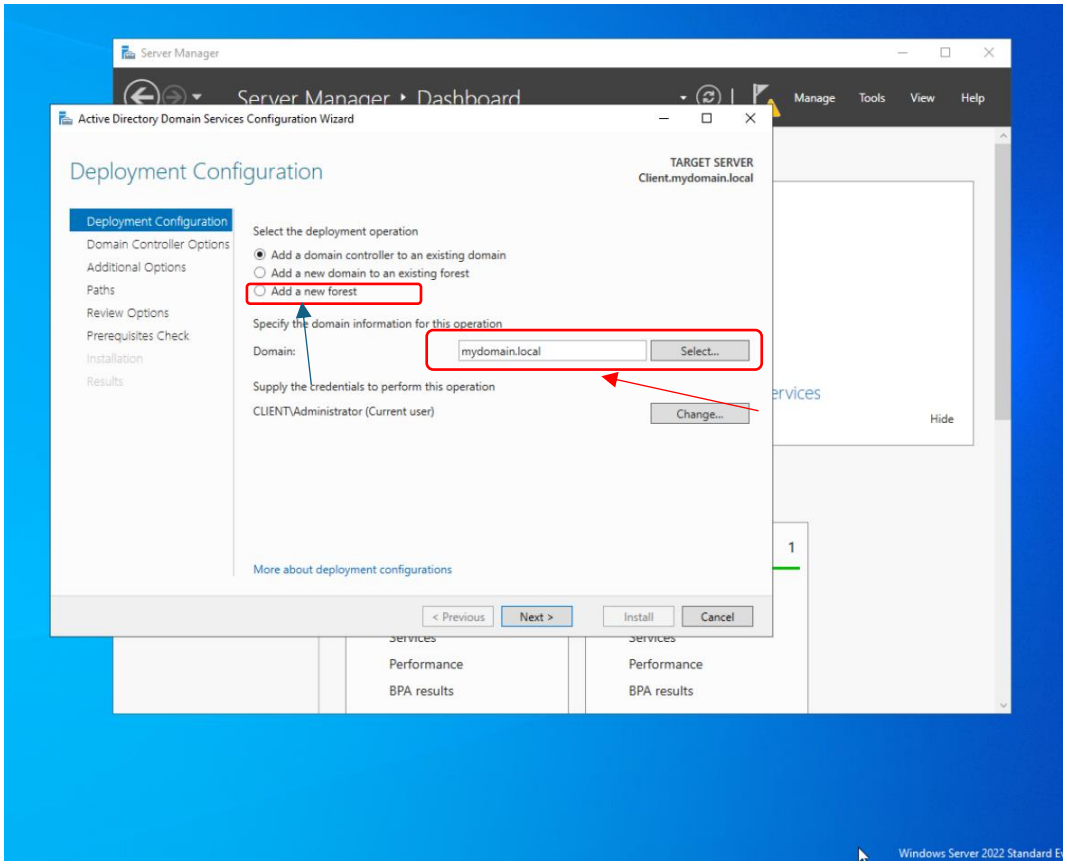


Figure 7 Select Add a new forest. enter a domain name and click next

Domain Controller Options:

- Set the Forest functional level and Domain functional level to Windows Server 2022 (recommended) or Windows Server 2016 if compatibility with older systems is required.
- Check Domain Name System (DNS) server (this will configure DNS on the DC).

- Ensure Global Catalog (GC) is checked by default.
- Leave Read-only domain controller (RODC) unchecked.
- Set a Directory Services Restore Mode (DSRM) password (used for recovery purposes). Make sure to record this password securely.
- Click Next.

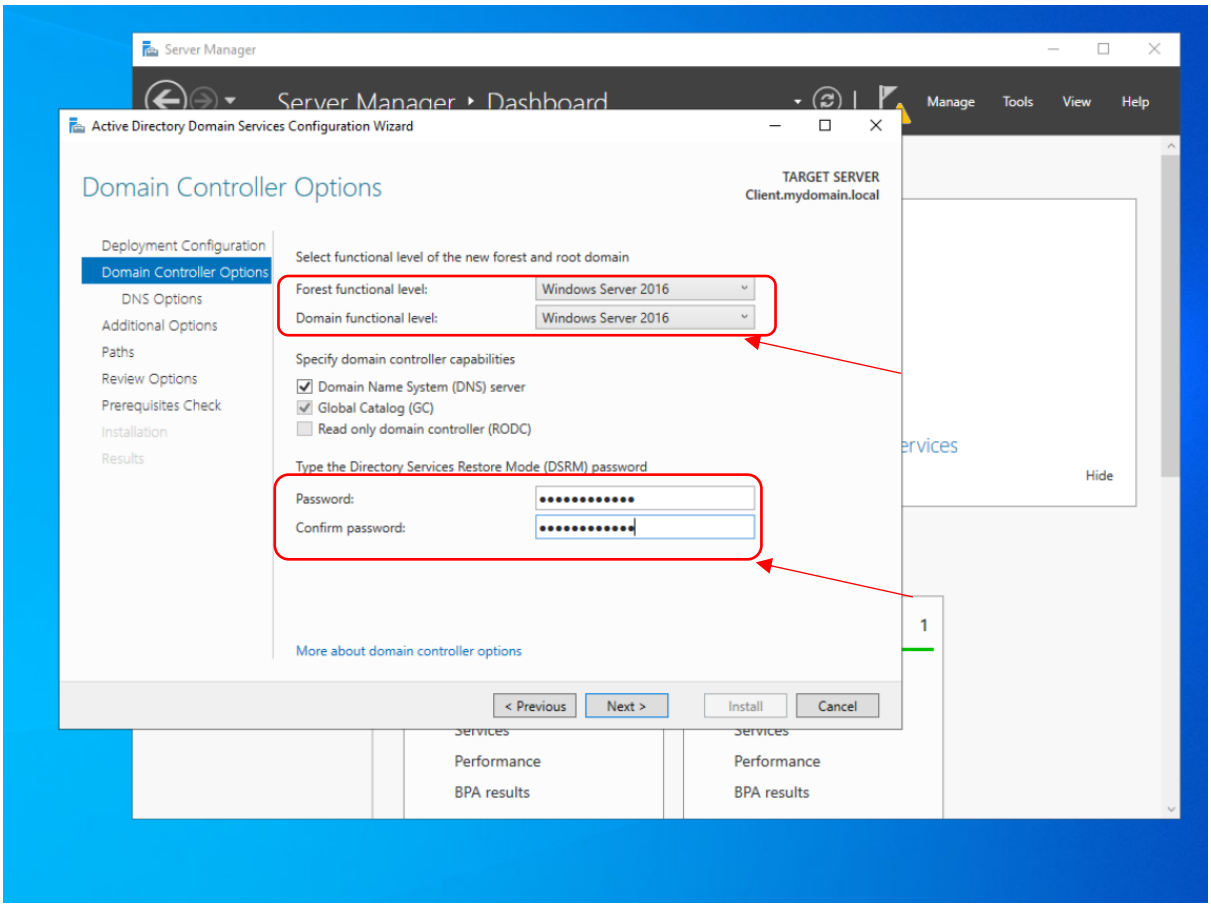


Figure 8 set the password and functional levels

2. **DNS Options:**
   - A warning about a delegation for DNS may appear. This is normal for a new forest setup. Click Next.

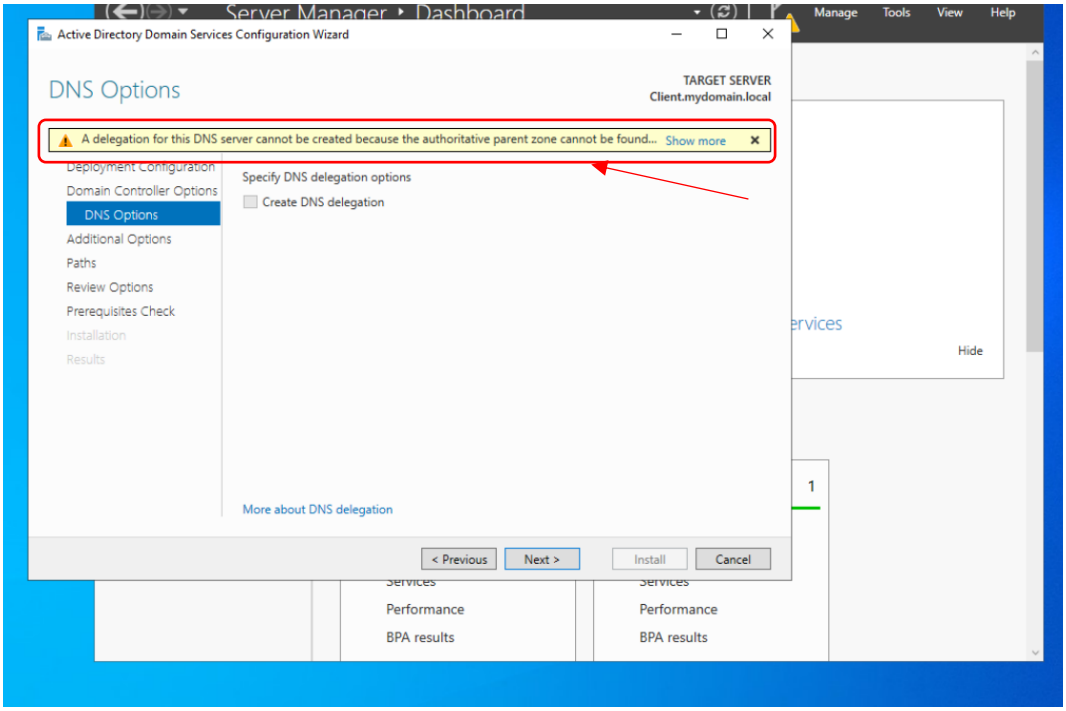


Figure 9 A warning about a delegation for DNS may appear. This is normal for a new forest setup. Click Next.

3. Additional Options:

- Verify that the NetBIOS domain name is correct (it should match the root domain name you set up earlier).

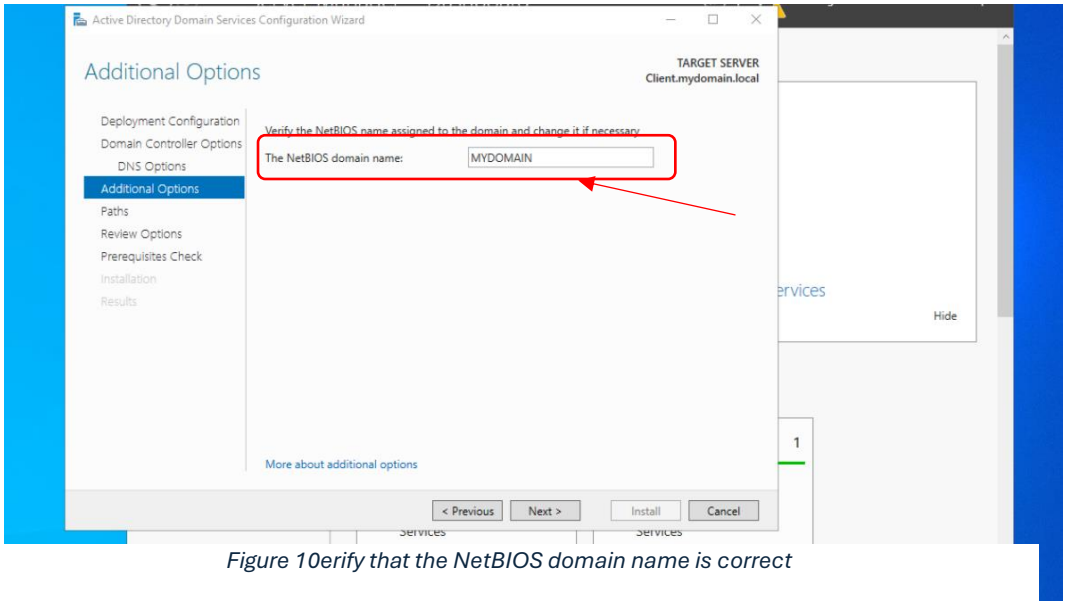


Figure 10erify that the NetBIOS domain name is correct

- Click Next.

4. Paths:

- Specify the folders for the Database, Log files, and SYSVOL.

- The default paths are generally fine, so you can click Next.

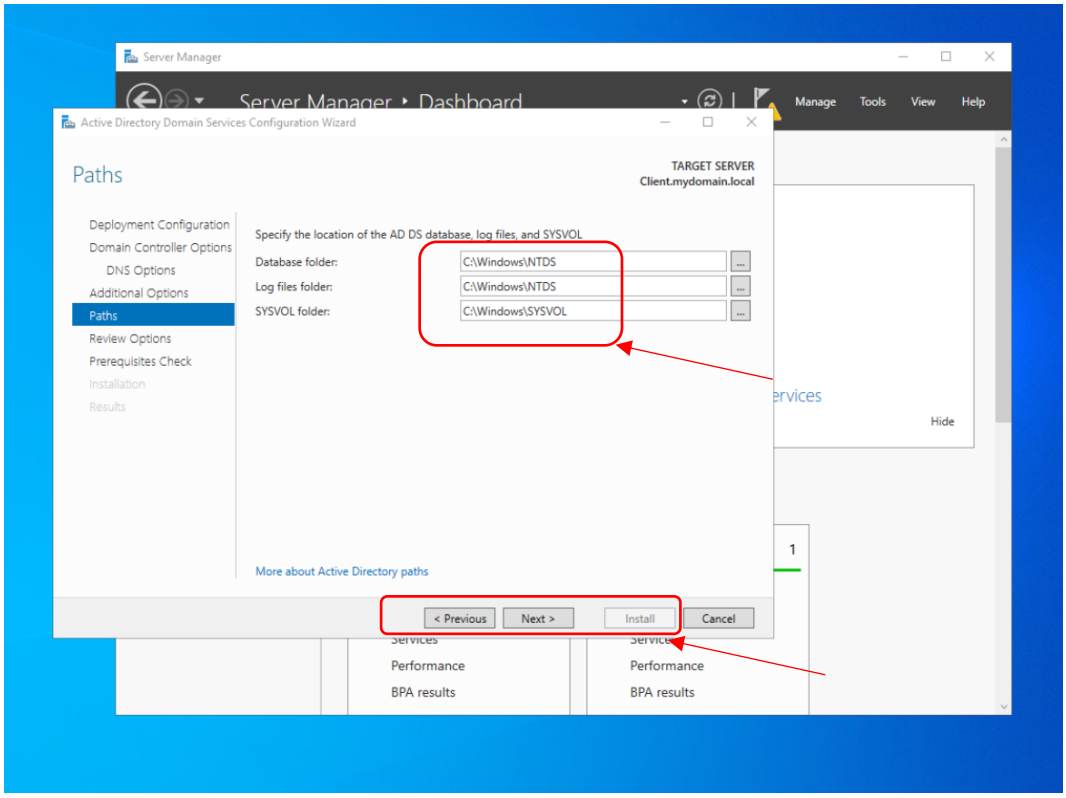


Figure 11 review paths and install

5. **Review Options:**
    - Review your configuration. If everything looks correct, click Next.
6. **Prerequisites Check:**
    - The wizard will check to ensure all prerequisites are met.
    - If there are warnings, review them (you can ignore minor warnings related to DNS delegation in a new forest).
    - Click Install to begin the promotion process.

Step 3: Complete the Promotion and Restart

1. After the installation completes, the server will automatically restart to apply the changes.
2. Log back in after the restart using your domain credentials if prompted (mydomain\Administrator).

Step 4: Verify AD DS and DNS Installation

1. Open Server Manager:

- Check that Active Directory Domain Services and DNS are listed and running in the left panel.

2. **Open Active Directory Users and Computers:**
   - Press Windows + R, type dsa.msc, and press Enter.
   - Confirm that your domain (mydomain.local) is listed.
3. **Test the Configuration:**
   - Create a test user in Active Directory Users and Computers.
   - Join a client computer (e.g., another Windows machine) to the domain.

Create user accounts and groups in Active Directory (AD).

Step 1: Open Active Directory Users and Computers (ADUC)

1. **Log in** to the Domain Controller with domain administrator privileges.
2. Open **Server Manager**.
3. In Server Manager, go to **Tools** → **Active Directory Users and Computers**.

Step 2: Create Groups

1. In ADUC, expand your **domain** (e.g., mydomain.local).
2. Select the **Users** container (this is one of the default organizational units).
3. **Right-click** the **Users** container, select **New** → **Group**.
4. **Create the First Group**:
   - In the **Group name** field, enter Test1.
   - Keep **Global** as the **Group scope** and **Security** as the **Group type**.
   - Click **OK** to create the group.
5. **Create the Second Group**:
   - Repeat the steps above to create the second group, named Test2.

Step 3: Create User Accounts

1. **Right-click** the **Users** container again, select **New** → **User**.

2. **Create User April**:
    - **First name**: April
    - **User logon name**: April
    - Click **Next**.
    - Set a **password** for April, and configure any password options (like requiring a password change at the next login if desired).
    - Click **Next** → **Finish**.
3. **Create Remaining Users**:
    - Repeat the steps to create users **May**, **June**, **July**, and **August** with similar configurations.

Step 4: Add Users to Groups

1. In ADUC, find and **right-click** the user **April** → Select **Add to a group**.
2. In the **Select Group** window, type Test1, then click **Check Names**. This should underline the group name if it exists.

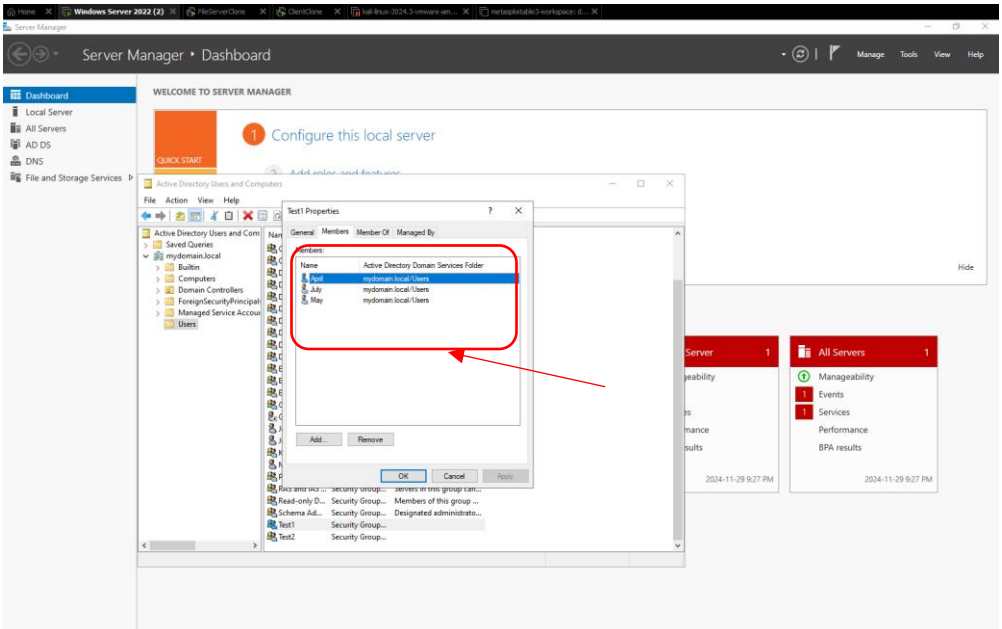


Figure 12 Test 1 Showing members April, July and May

3. Click **OK** to add April to the Test1 group.
4. Repeat these steps to add the following users to the respective groups
    - **May** and **June** to Test1
    - **July** to Test2

- **August** does not need to be added to any group.

Step 5: Verify Group Memberships

1. In ADUC, **double-click** each group (Test1 and Test2) to open its properties.
2. Go to the **Members** tab to confirm that the correct users are in each group:
    - **Test1** should contain **April**, **May**, and **June**.
    - **Test2** should contain **July**.
    - **August** should not appear in either group.

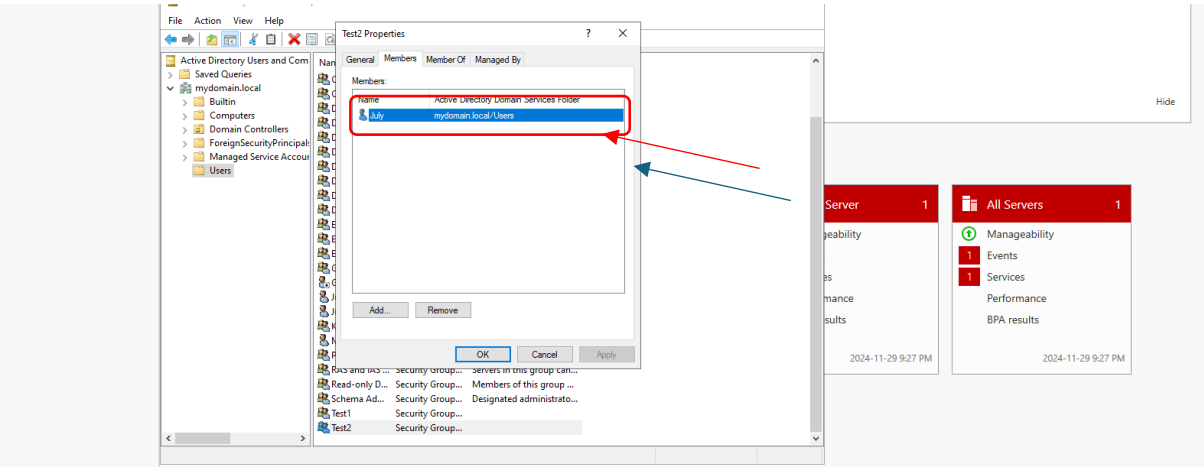


Figure 13 Test 2 Showing only July as a member

Add the File Server Role

1. **Log in** to the server that will act as your file server.
2. Open **Server Manager**.
3. Click **Add Roles and Features** in the **Dashboard**.
4. In the **Add Roles and Features Wizard**:
    - **Before You Begin**: Click **Next**.
    - **Installation Type**: Select **Role-based or feature-based installation** and click **Next**.
    - **Server Selection**: Choose your server from the list and click **Next**.
    - **Server Roles**: Scroll down and select **File and Storage Services** if not already selected.
    - Expand **File and iSCSI Services**, then check **File Server**.

- Click **Next** and then **Install** to add the role.

5. **Complete Installation**:
    - Wait for the installation to complete, then click **Close**.

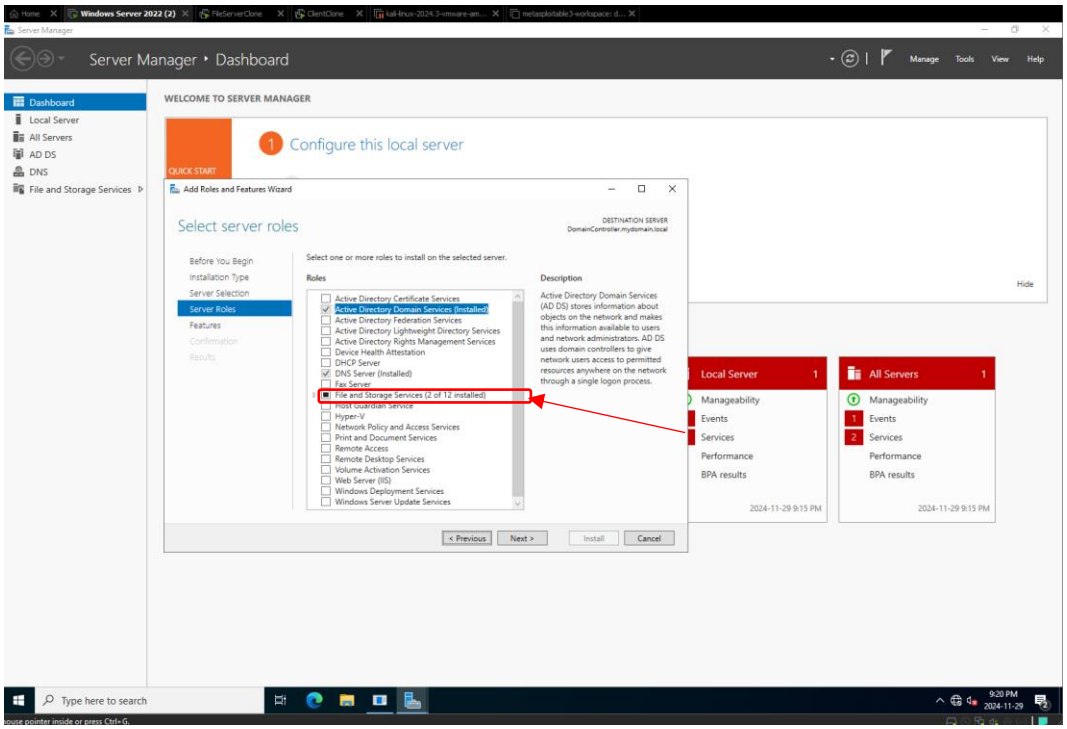


Figure 14 Scroll down and select File and Storage Services if not already selected.

Disable Automatic Updates

1. Open **Settings** (use **Windows + I** shortcut).
2. Go to **Update & Security** → **Windows Update**.
3. Select **Advanced options**.
4. Under **Pause updates**, choose the maximum pause period if you just want to delay updates temporarily.
5. To fully disable updates:
    - Type **Services** in the Start menu to open the Services Manager.
    - Locate **Windows Update** in the list of services.
    - Right-click **Windows Update** → **Properties**.
    - Set **Startup type** to **Disabled**.

- Click **Stop** (if it's running), then **OK**.

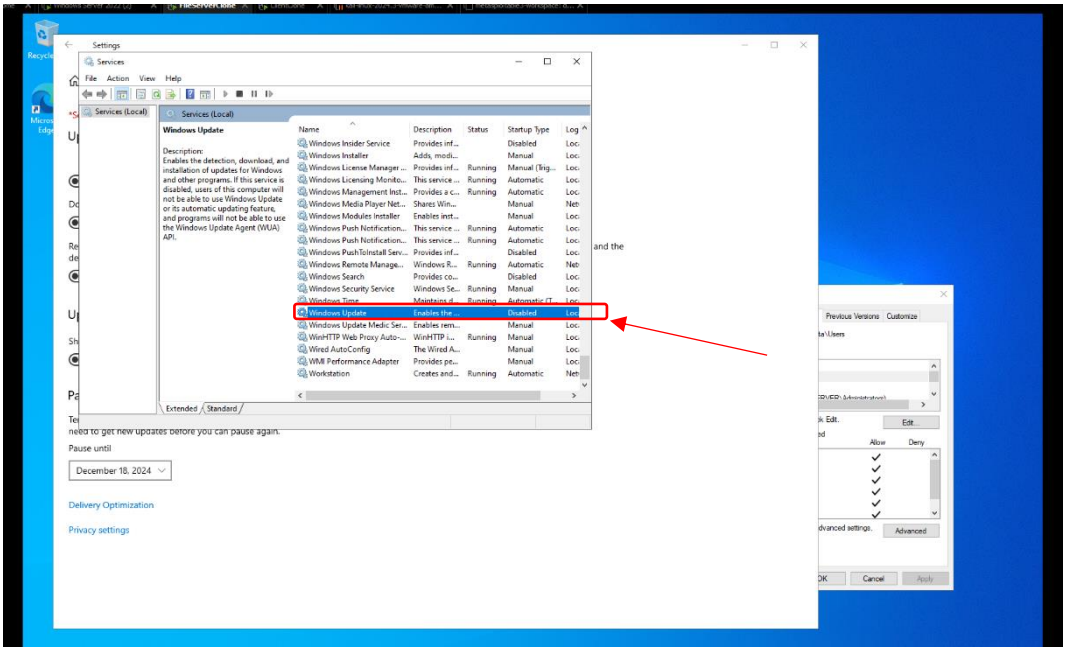


Figure 16 Disabling automatic updates

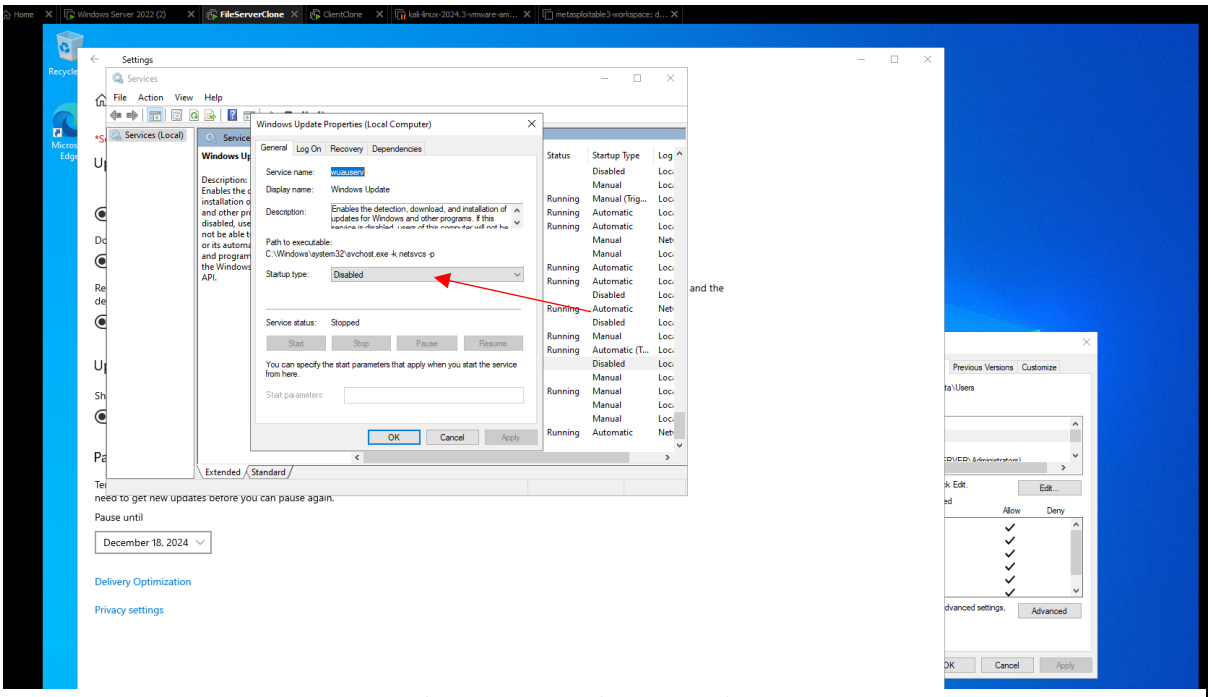


Figure 15 Automatic updates disabled

Create the Directory Structure

1. Open **File Explorer**.
2. Navigate to the root of the **C:** drive.

3. **Create the Main Folder**:
    - Right-click on an empty area, select **New** → **Folder**.
    - Name the new folder TestData.
4. **Create Subfolders**:
    - Open TestData, then create three subfolders inside it:
        - Right-click → **New** → **Folder** → Name the folder **Users**.
        - Repeat to create **Jobs** and **Accounts**.

After completing these steps, your file server is set up with the File Server role, automatic updates are disabled, and the folder structure C:\TestData\Users, C:\TestData\Jobs, and C:\TestData\Accounts is created

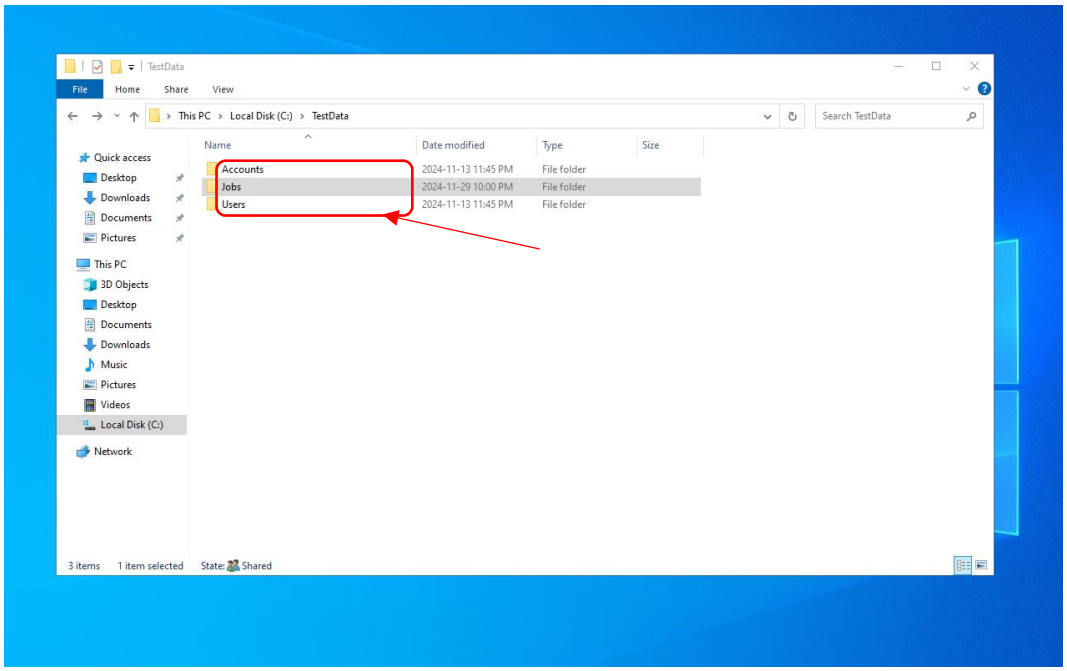


Figure 17 Creation of Directory (folders Accounts, Jobs and Users)

Step 1: Open File Explorer and Navigate to the TestData Folder

1. Log in to the file server.
2. Open **File Explorer** and navigate to **C:\TestData**.

Step 2: Set Permissions for Data\Users

1. Right-click on the **Users** folder inside **C:\TestData** and select **Properties**.
2. Go to the **Security** tab and click **Edit**.

3. In the **Permissions for Users** window, click **Add**.
4. In the **Select Users or Groups** dialog:
    - Type **Authenticated Users** (or **Domain Users** if you only want domain users to access this).
    - Click **Check Names** to verify the name, then **OK**.
5. In the **Permissions** section, select **Allow** for **Full Control** (or **Modify** if you don't want full control).
6. Click **OK** to apply the permissions.

Step 3: Set Permissions for Data\Jobs

1. Right-click on the **Jobs** folder in **C:\TestData** and select **Properties**.
2. Go to the **Security** tab and click **Edit**.
3. Click **Add** and type **Test1** to add the **Test1** group.
    - Click **Check Names** to verify, then **OK**.
4. In the **Permissions** section, select **Allow** for **Modify**.
5. To add permissions for **August**:
    - Click **Add** again, type **August**, and click **Check Names** to verify.
    - Click **OK**.
6. For **August**, select **Allow** for **Read & Execute** only.
7. Click **OK** to apply these permissions.

Step 4: Set Permissions for Data\Accounts

1. Right-click on the **Accounts** folder in **C:\TestData** and select **Properties**.
2. Go to the **Security** tab and click **Edit**.
3. Click **Add** and type **Test2** to add the **Test2** group.
    - Click **Check Names** to verify, then **OK**.
4. In the **Permissions** section for **Test2**, check **Allow** for both **Read & Execute** and **Write**.
5. Click **OK** to apply these permissions.

Step 5: Verify Permissions

1. To ensure permissions are set correctly, you can:
    - Right-click each folder, go to **Properties** → **Security** tab, and review the **Group or usernames** and associated permissions.
2. Test by logging in as different users or by using the **Effective Access** tab in each folder's **Advanced Security Settings** to simulate access for each user or group.

After completing these steps, your permissions should be configured as follows:

- All users can access **C:\TestData\Users**.
- **Test1** group has **Modify** permissions for **C:\TestData\Jobs**.
- **August** has **Read** permissions for **C:\TestData\Jobs**.
- **Test2** group has **Read and Write** permissions for **C:\TestData\Accounts**.

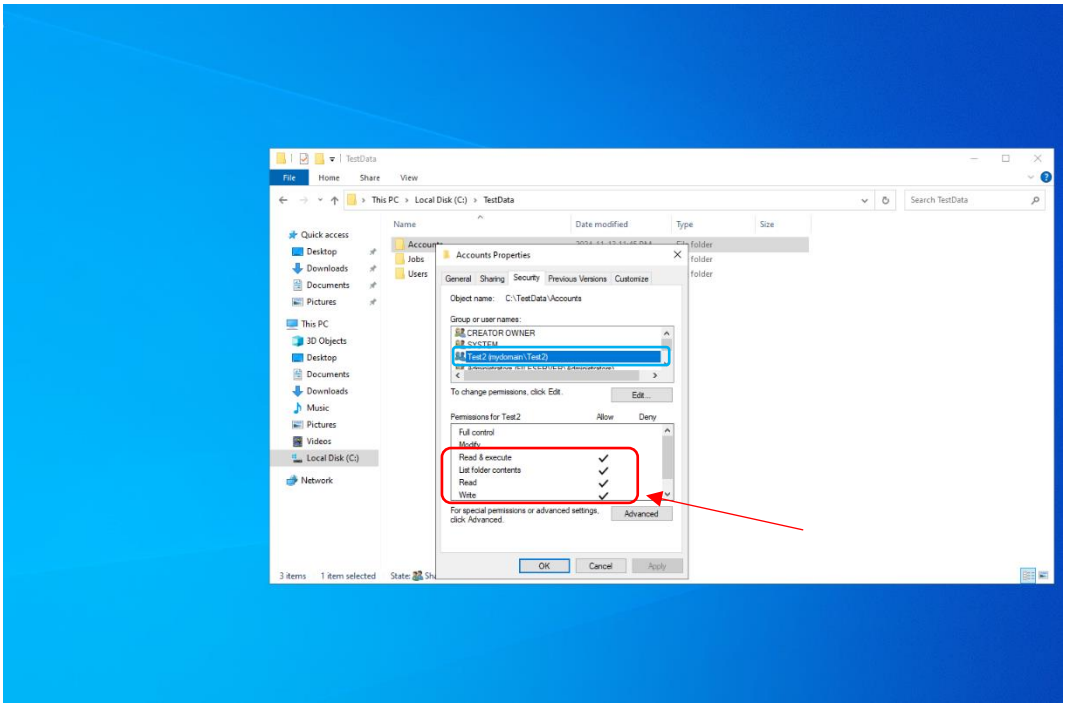


Figure 18 Test2 group with Read and Write Permissions for Accounts folder

Permissions Setup

- **Users Folder**: All domain users granted access.
- **Jobs Folder**:
    - **Test1** group: Modify permissions.
    - **August**: Initially read-only access, later updated to include create permissions.

- **Accounts Folder**: **Test2** group: Read and write permissions.

August Permissions Change:

- **Initial Setup**: **August** was granted **read-only** access to the Jobs folder.
- **Permission Update**: After testing, it was required that **August** have the ability to **create folders** in the Jobs folder. The permissions for **August** were updated to include **Write** permissions, allowing folder creation but preventing modification of existing files. This was done to ensure that **August** could create subfolders but not alter the existing contents in the directory.

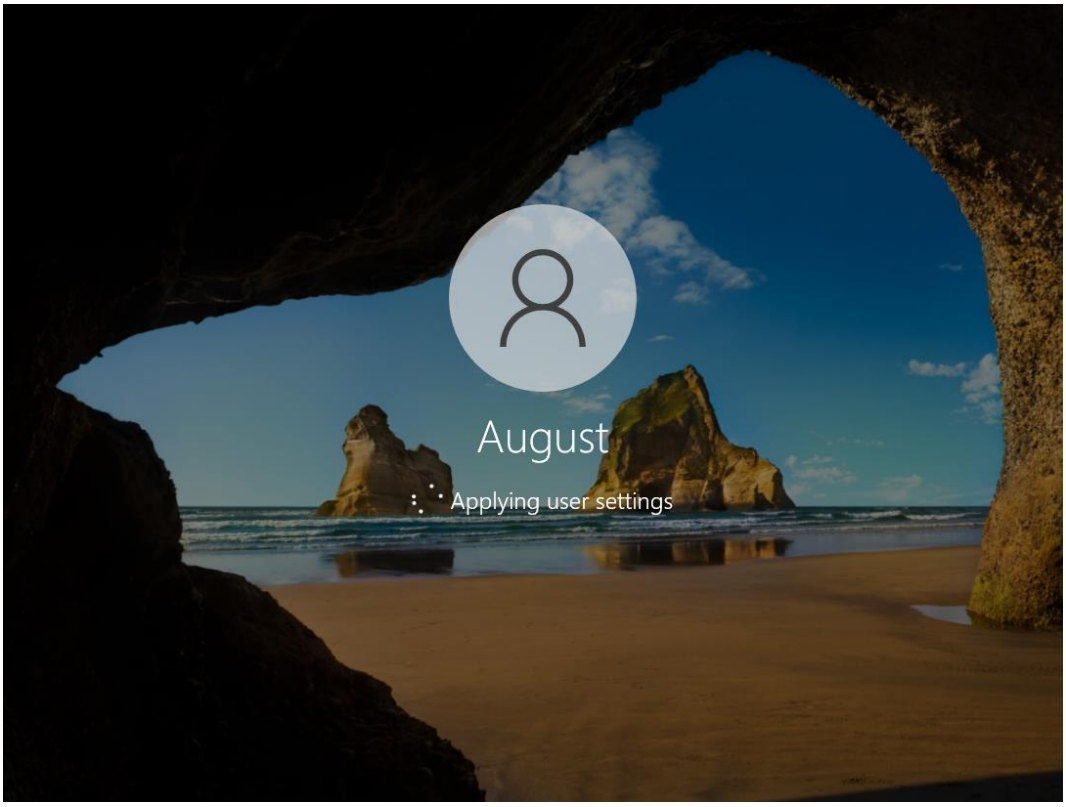


Figure 19 Logging as August on Client Machine

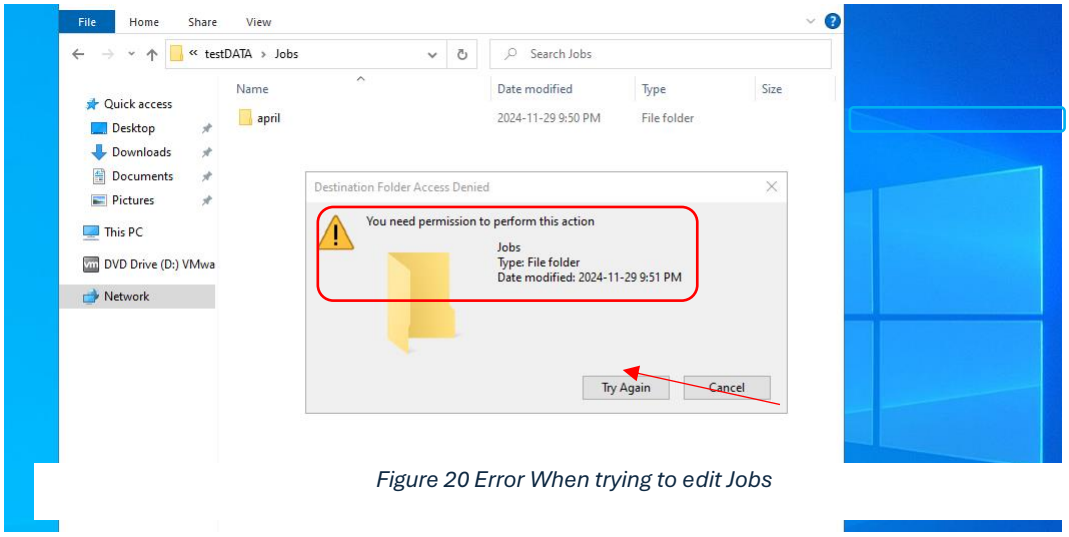


Figure 20 Error When trying to edit Jobs

Configuration Evaluation and Research

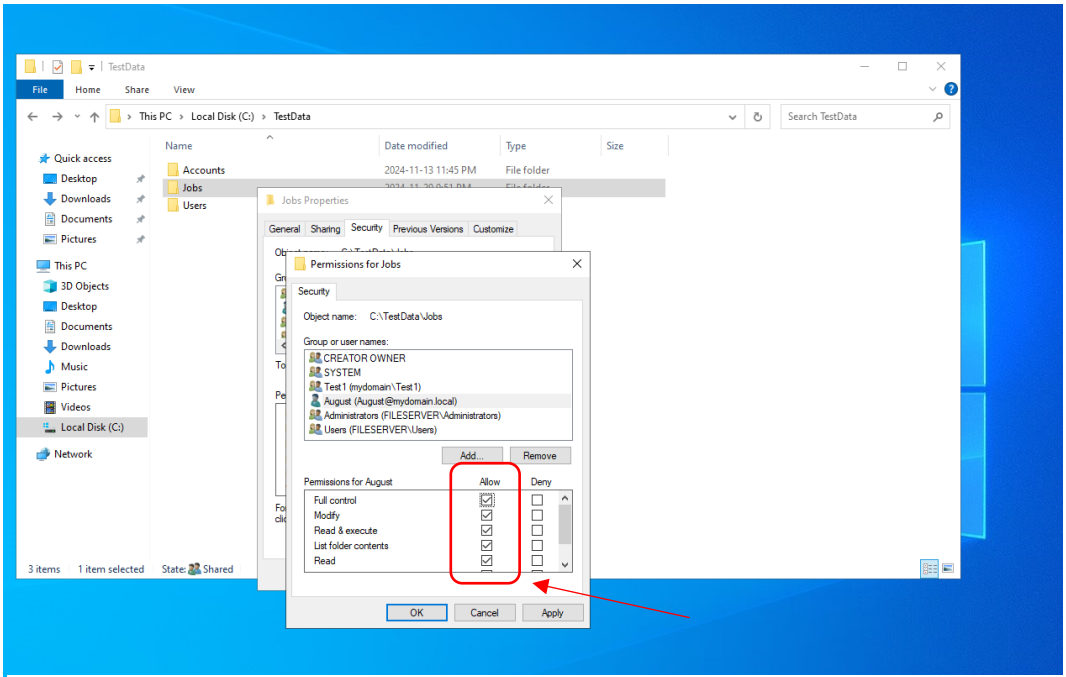


Figure 21 Giving August Full control in Jobs to test access, in file sever

Tools Used:

- **Ping Castle**: Used for Active Directory configuration and security assessments.
- **Nessus**: Performed vulnerability scans using Kali Linux.
- **BloodHound**: Used for detailed graph-based analysis of privilege escalation paths and delegation issues within the Active Directory.

Key Findings:

1. **Short Password Length Policy**: The default password length was less than 8 characters.
    - **Action**: Updated policy to enforce a 12-character minimum.
2. **Delegation Risks**: Some privileged accounts lacked the "Sensitive and cannot be delegated" flag.
    - **Action**: Enabled the flag for all privileged accounts.
3. **Computer Registration by Basic Users**: Default ms-DS-MachineAccountQuota allowed basic users to register up to 10 computers.

- **Action**: Reduced quota to 0 and restricted SeMachineAccountPrivilege to Domain Admins.

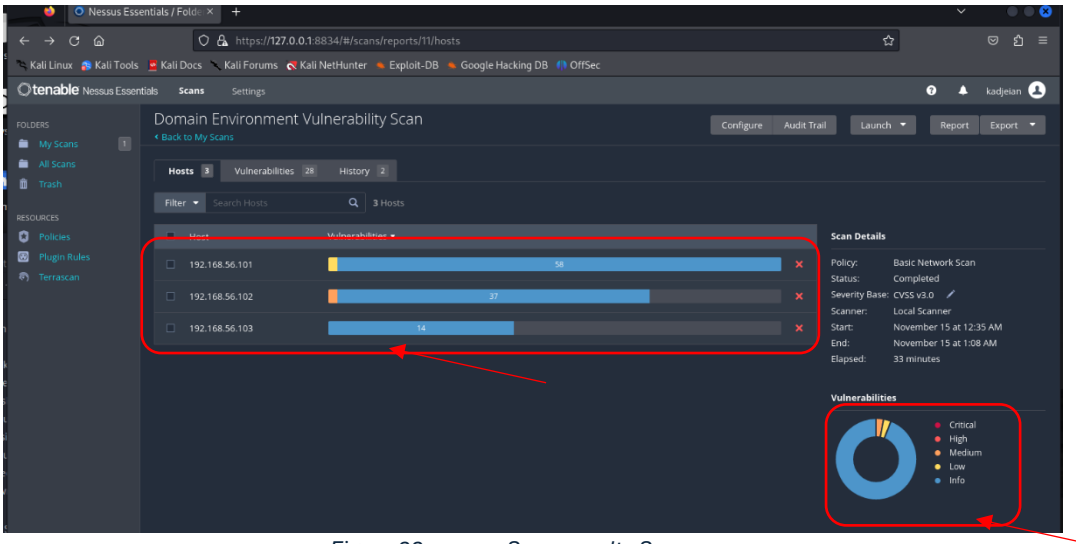
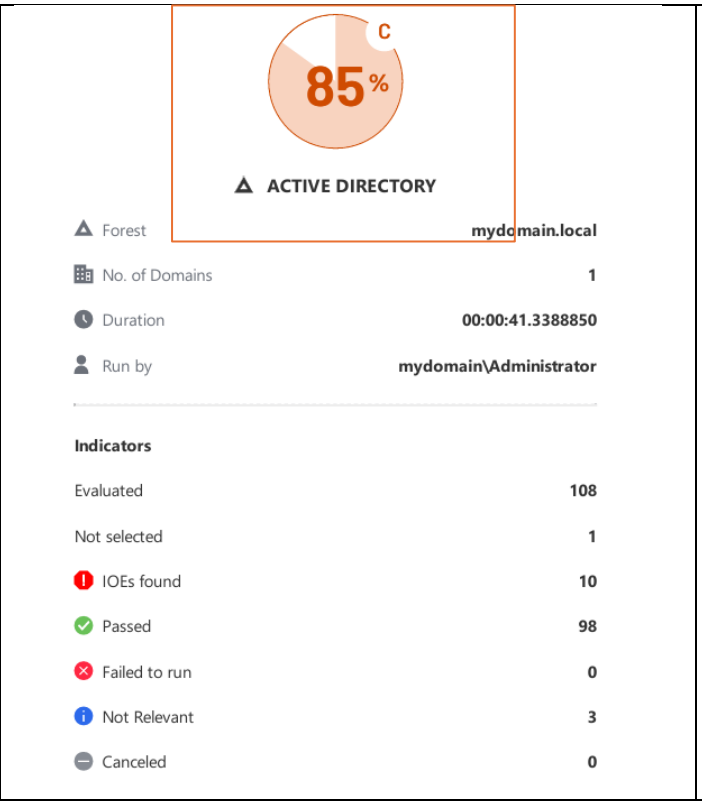
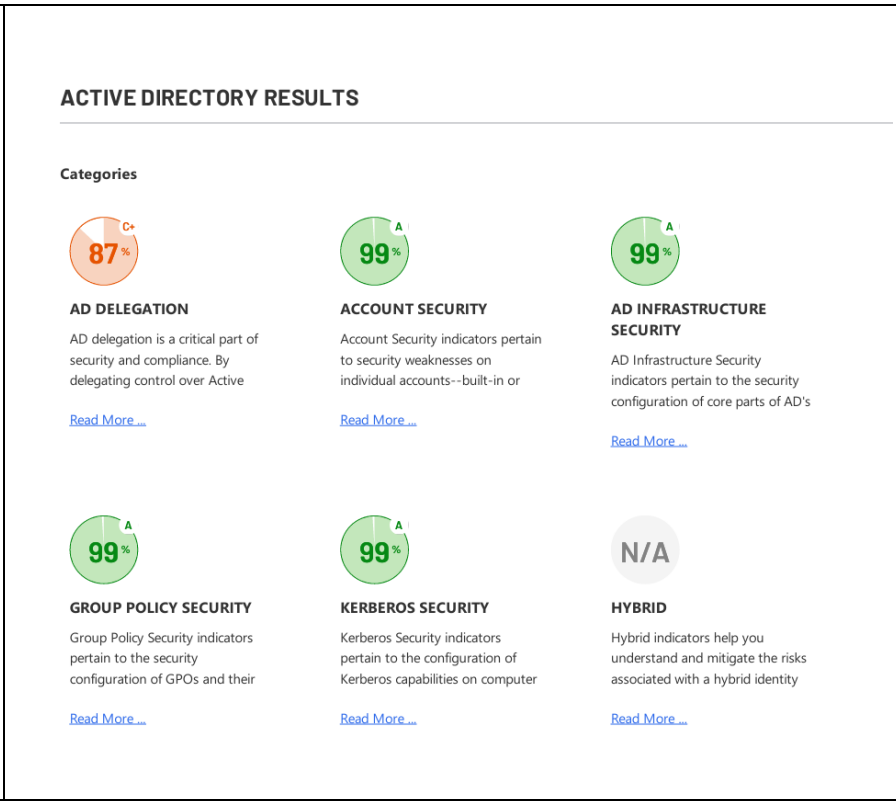


Figure 22 nessus Scan results Summary

Security Assessment Report from Purpleknight





ADDITIONAL IOEs FOUND

NAME	PLATFORM	SEVERITY LEVEL	ACTION
• Abnormal Password Refresh	AD	Warning	Read More...
• Built-in domain Administrator account used within the last two weeks	AD	Warning	Read More...
• Changes to Pre-Windows 2000 Compatible Access Group membership	AD	Warning	Read More...
• LDAP signing is not required on Domain Controllers	AD	Warning	Read More...
• RC4 or DES encryption type are supported by Domain Controllers	AD	Warning	Read More...
• Changes to Default Domain Policy or Default Domain Controllers Policy in the last 7 days	AD	Informational	Read More...
• gMSA not in use	AD	Informational	Read More...
• Recent privileged account creation activity	AD	Informational	Read More...
• Unprivileged users can add computer accounts to the domain	AD	Informational	Read More...

Figure 23.1 Security Assessment Report from PurpleKnight

Ping Castle Finding before remediation

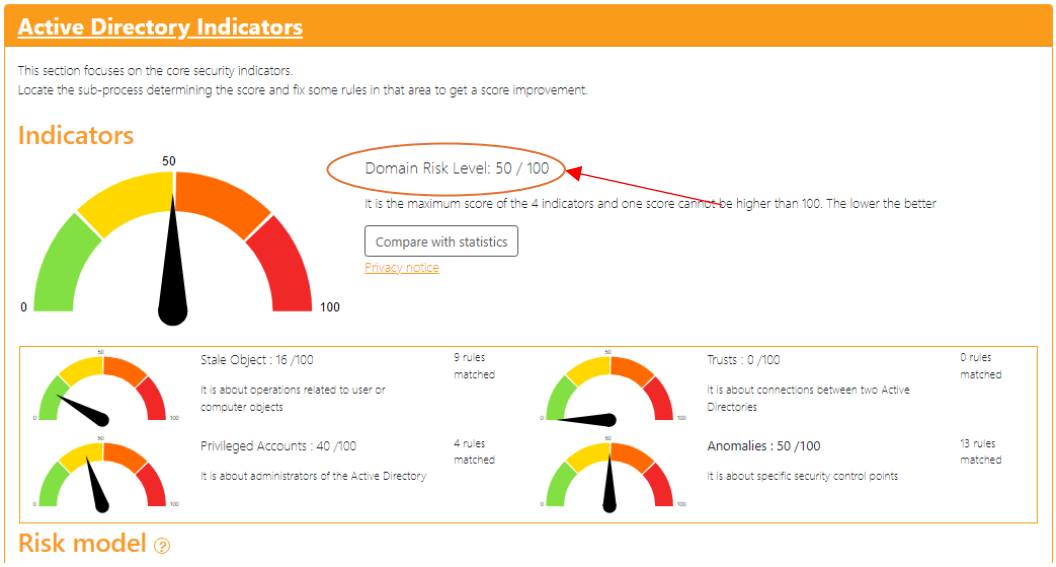


Figure 24 Ping Castle Finding before remediation

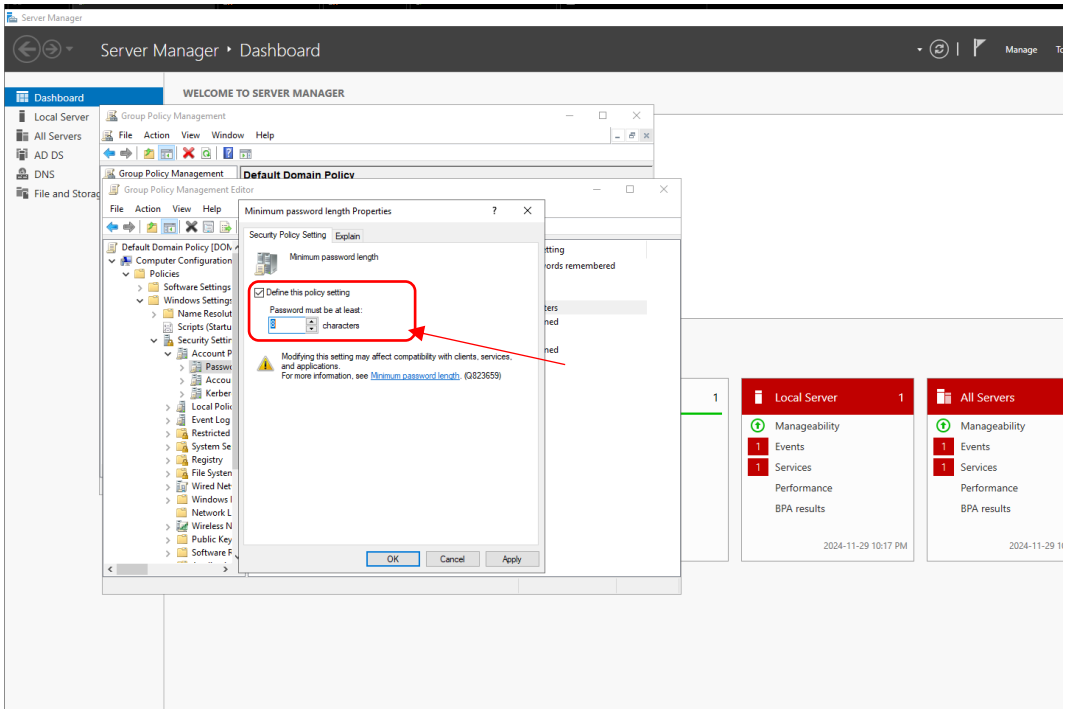


Figure 25 Updating Password Policy

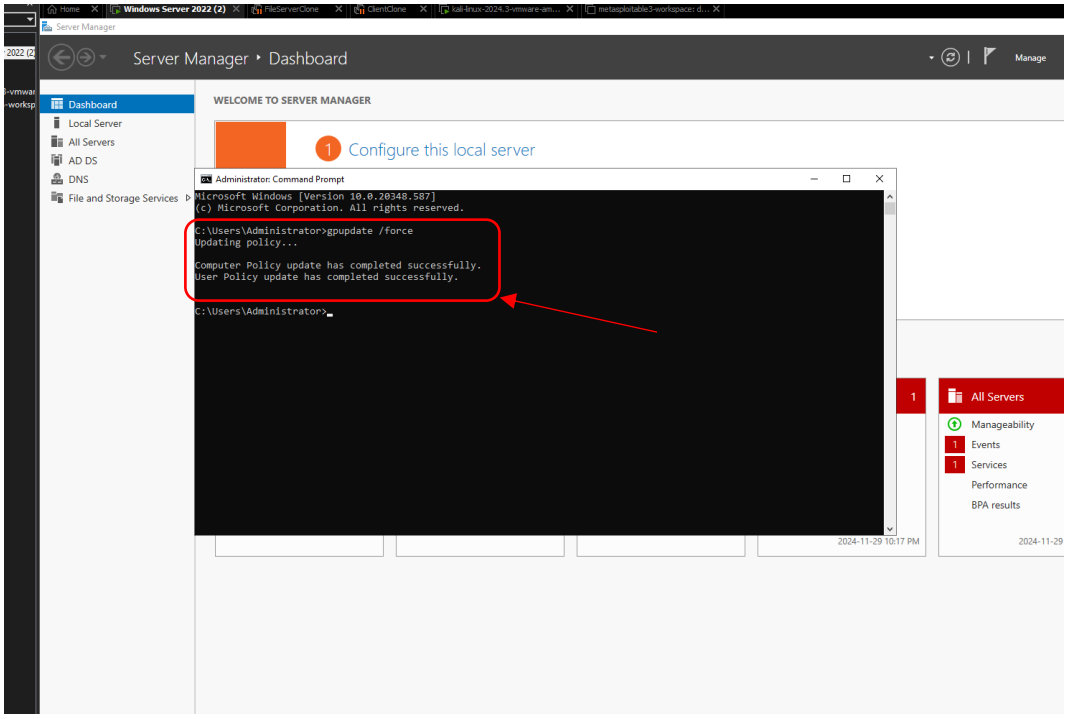


Figure 26 updating Group policy

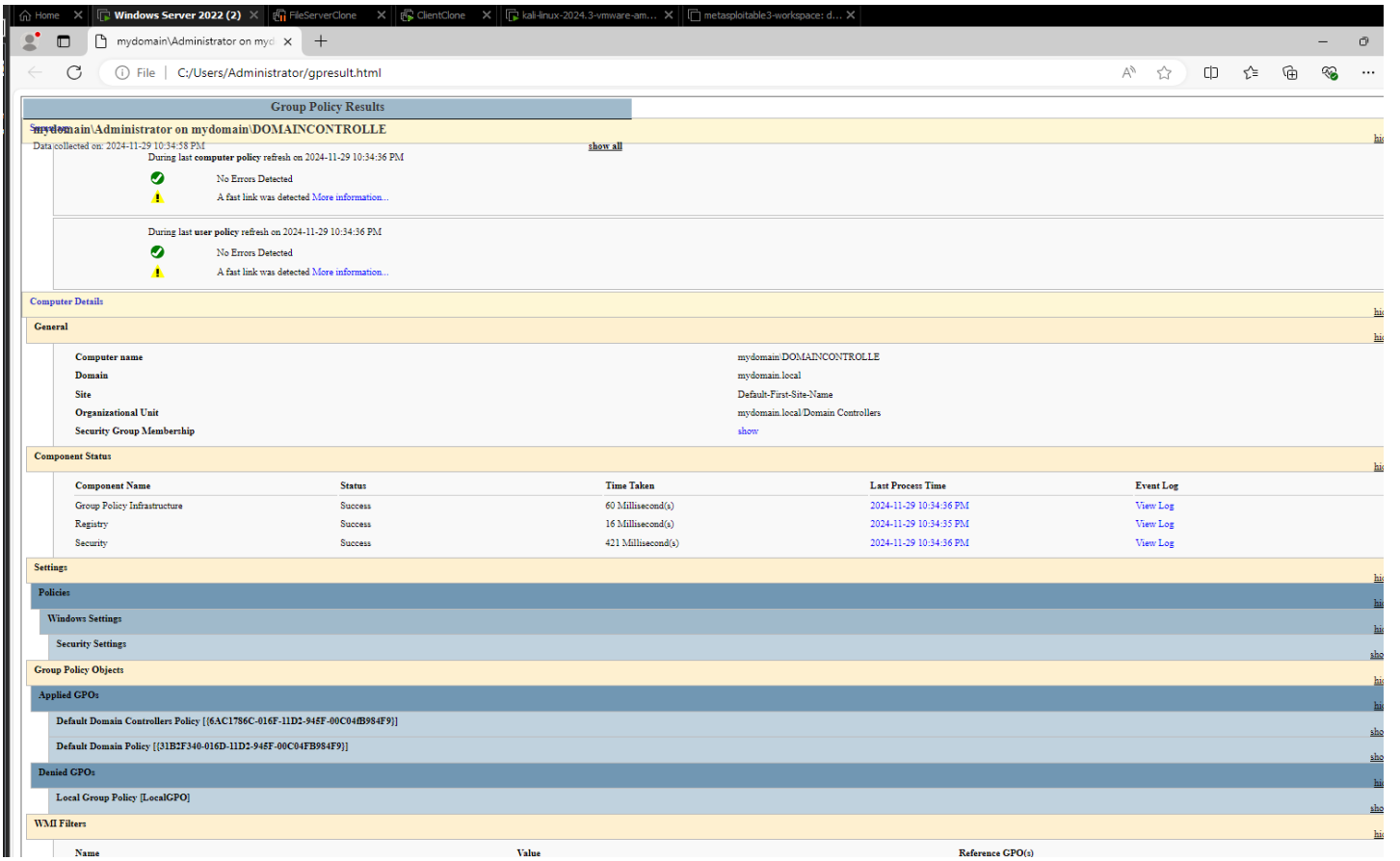


Figure 27 Group Policy results

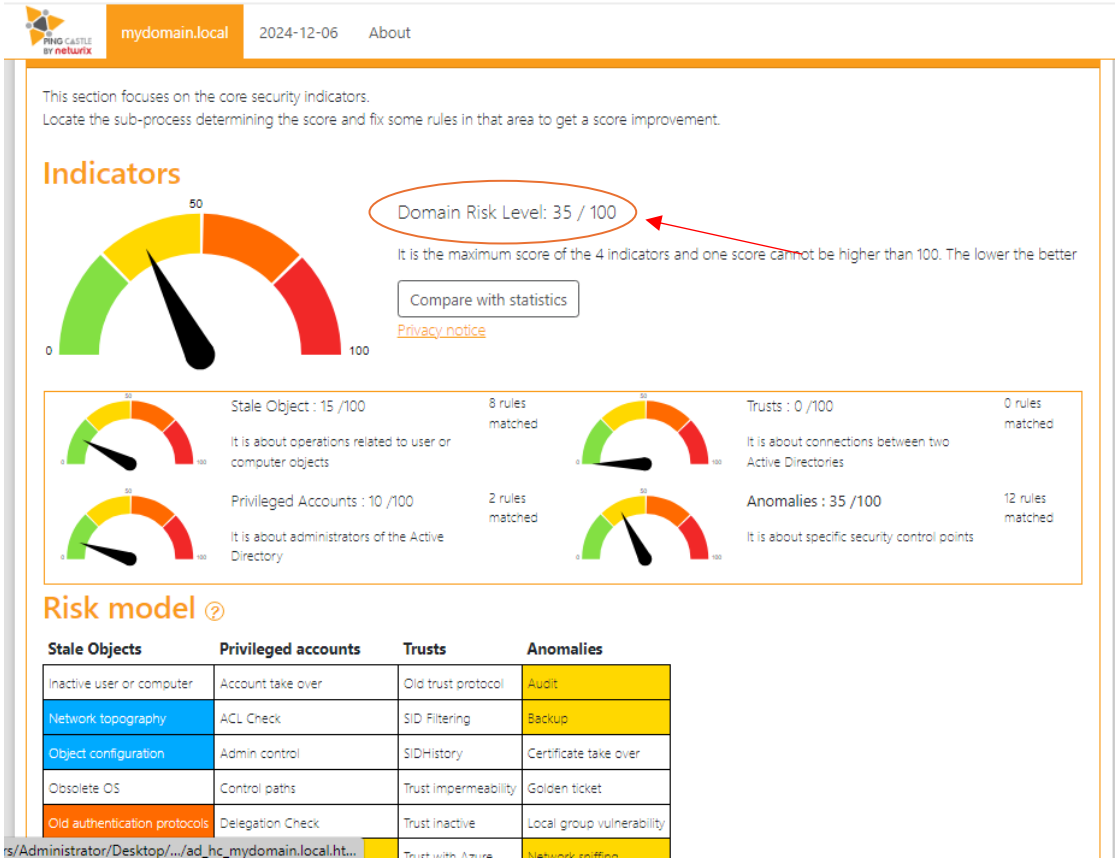


Figure 28 Ping castle results after remediation

BloodHound Analysis for Active Directory Vulnerabilities:

Setup and Execution: Data was collected using SharpHound and imported into BloodHound for visualization and analysis.

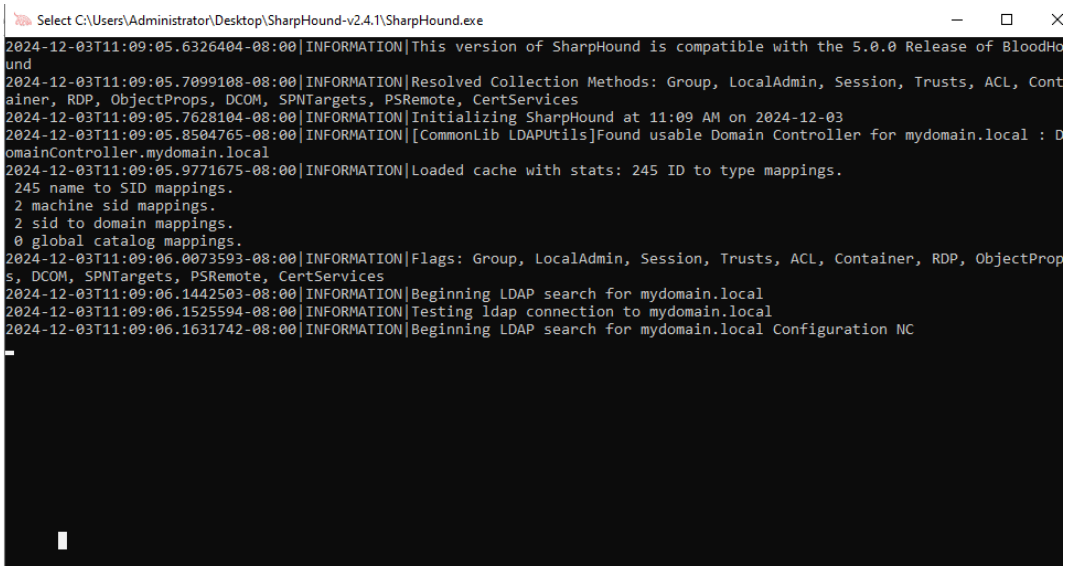


Figure 29 SharpHound Execution

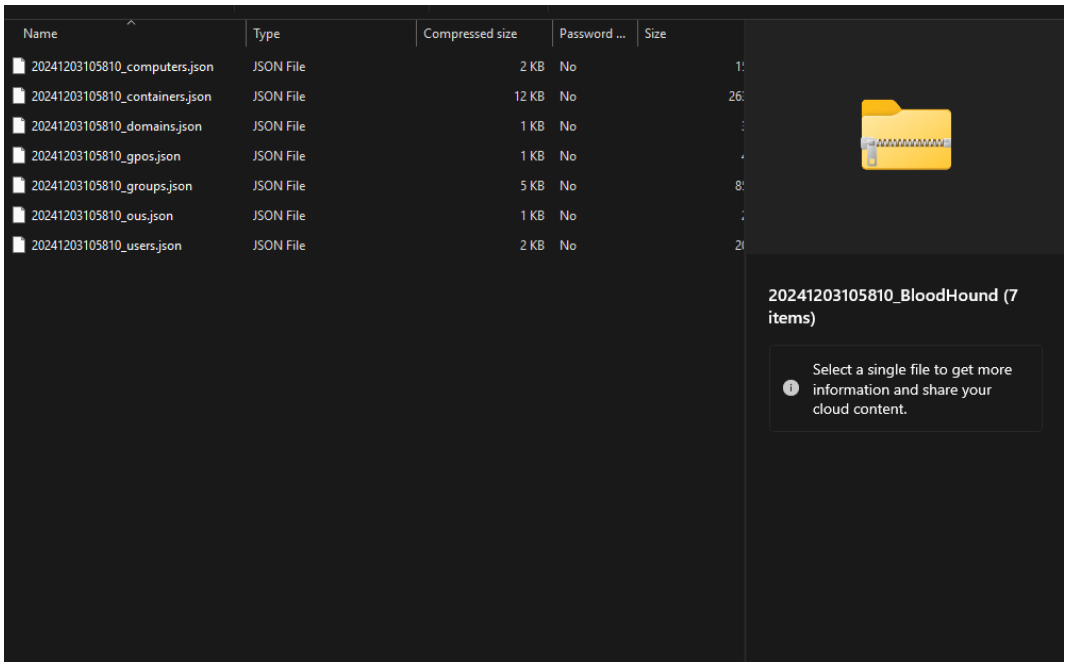


Figure 30 SharpHound output to be imported into BloodHound

Key Observations:

Green Node: Represents the Administrator account (ADMINISTRATOR@MYDOMAIN.LOCAL).

Yellow Node: Represents the Domain Admins group (DOMAIN ADMINS@MYDOMAIN.LOCAL). The connecting line labeled MemberOf indicates a direct group membership relationship, meaning the administrator account is a member of the Domain Admins group.

Critical Findings:

The Administrator account is inherently highly privileged, and its membership in the Domain Admins group confirms it has unrestricted administrative access to the domain.

A lack of additional security configurations, such as account delegation restrictions, increases the risk of exploitation.

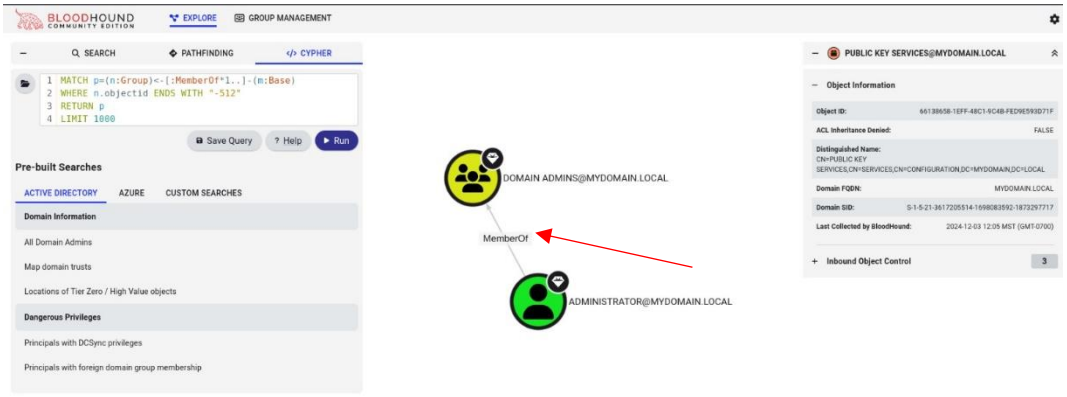


Figure 31 Representation of Damin admin group

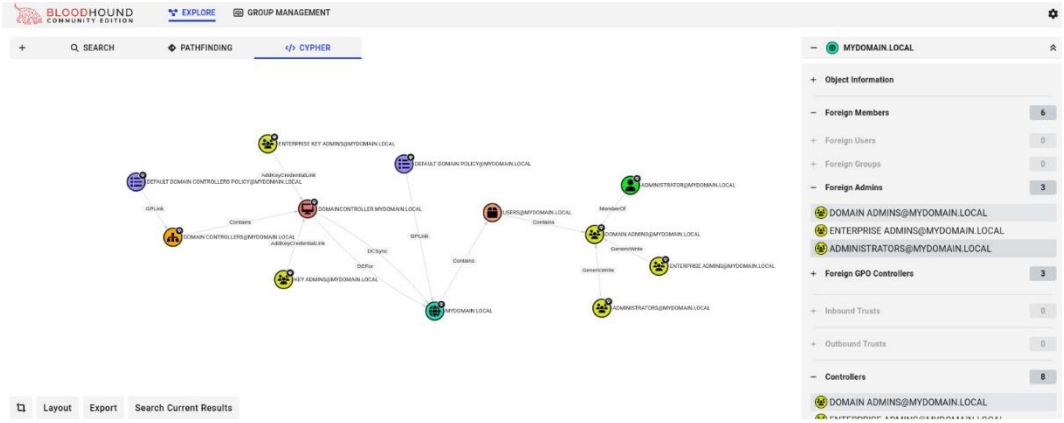


Figure 32 "Mapping Domain Object Relationships and Privileged Roles in MYDOMAIN.LOCAL Using BloodHound"

This BloodHound graph above shows **domain object relationships** in MYDOMAIN.LOCAL, highlighting:

- Key admin groups: **Domain Admins**, **Enterprise Admins**, and **Administrators**.
- Privileges such as **GenericWrite** and **AddKeyCredentialLink** on objects like **Domain Controllers** and GPOs.
- **Administrator account** as a member of **Domain Admins** with control over critical resources.

It maps potential paths to **privileged roles** via misconfigurations.

The image below image shows a BloodHound-generated graph of the "Authenticated Users" group in MYDOMAIN.LOCAL. It highlights the group hierarchy, its members (such as DOMAIN USERS, DOMAIN COMPUTERS, and individual accounts like AUGUST, JUNE, and the domain administrator), and their relationships within the Active Directory environment.

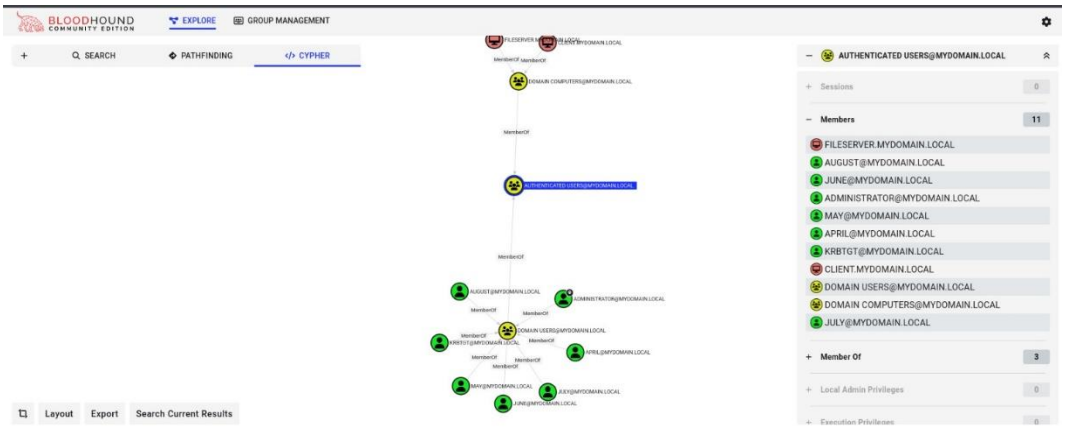


Figure 33"Visualizing Authenticated Users Group Memberships and Relationships in MYDOMAIN.LOCAL Using BloodHound"

The graph below visualizes relationships and permissions among different entities within the domain (MYDOMAIN.LOCAL), including user groups like Domain Admins, Enterprise Admins, Administrators, and domain controllers. Connections between nodes indicate specific permissions, group memberships, or relationships, such as "MemberOf" and "GetChangesAll". The right-hand panel lists various groups and controllers, providing detailed organizational information.

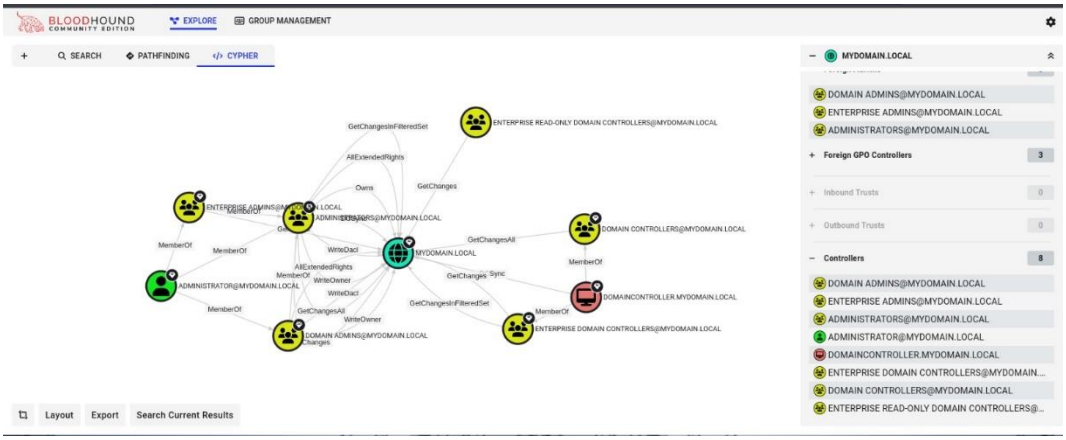


Figure 34 Visualizing Active Directory relationships and permissions for security analysis.

Hardening Steps and Rationale

Password Policies

- **Action**: Minimum password length set to 12 characters with complexity requirements.
- **Rationale**: Prevents brute force attacks by requiring stronger, harder-to-guess passwords.

Account Lockout Policies

- **Action**: Lockout threshold set to 5 failed attempts, with a lockout duration of 15 minutes.
- **Rationale**: Reduces the risk of brute force attacks.

Delegation Protections

- **Action**: Enabled "Sensitive and cannot be delegated" for all privileged accounts.
- **Rationale**: Prevents impersonation through delegated service accounts.

Computer Registration Restrictions

- **Action**: Reduced ms-DS-MachineAccountQuota to 0 and removed SeMachineAccountPrivilege for basic users.
- **Rationale**: Ensures only authorized administrators can join machines to the domain.

Network Security Enhancements

- **Action**: Configured LAN Manager authentication to NTLMv2 only and refused LM/NTLM.
- **Rationale**: Strengthened authentication protocols to mitigate credential theft risks.

Windows Firewall Configurations

- **Action**: Enabled inbound connections blocking by default and allowed exceptions for critical services.
- **Rationale**: Minimized the attack surface by controlling network access.

Vulnerability Scans

- **Action:** Regular scans using Nessus, Ping Castle, and BloodHound to identify and resolve emerging threats. BloodHound will complement these tools by uncovering misconfigurations and potential privilege escalation paths within the domain.
- **Rationale:** Ensures compliance with best practices, improves security posture, and provides a holistic view of vulnerabilities, including those related to network

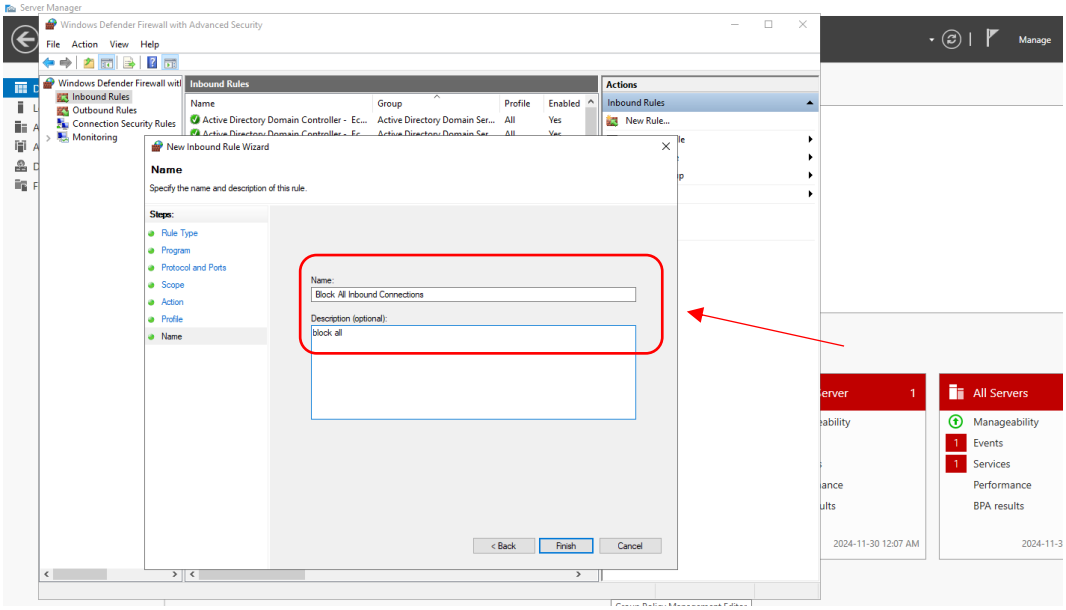


Figure 35 Changing Firewall Configurations

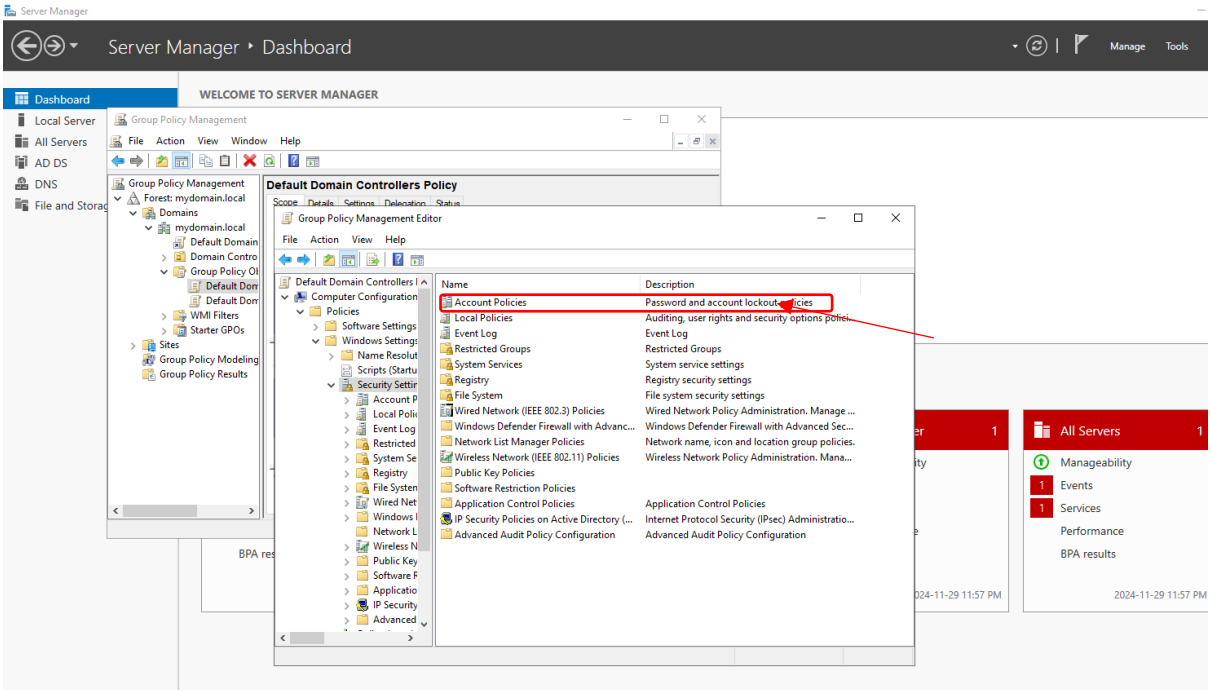


Figure 36 Changes for password policy and Account lockout

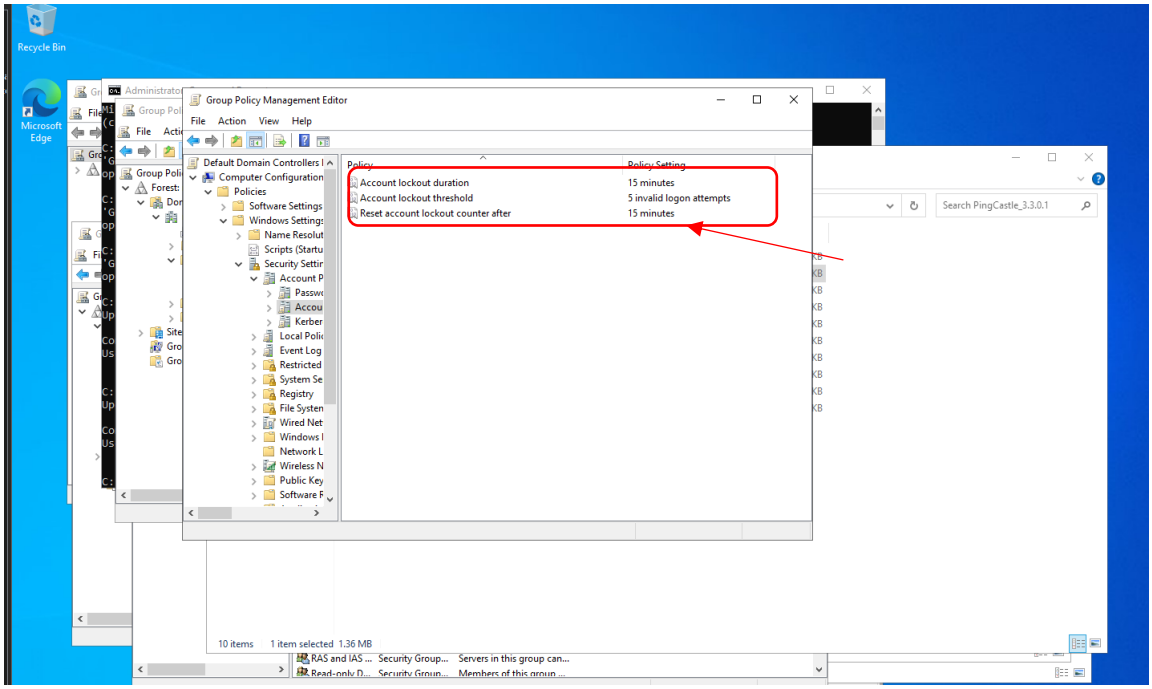


Figure 37 Account Lockout and threshold policy

Interactive Logon Messages

Steps to Configure Interactive Logon Messages:

1. **Open Group Policy Management:**
    - Follow the steps in **Account Lockout Policy** to access the Group Policy Management Console.
2. Log in to the Domain Controller:
3. Use an administrative account on your Windows Server acting as the Domain Controller.
4. Open Group Policy Management:
5. Press Windows + R, type gpmc.msc, and press Enter.
6. Edit the Default Domain Policy:

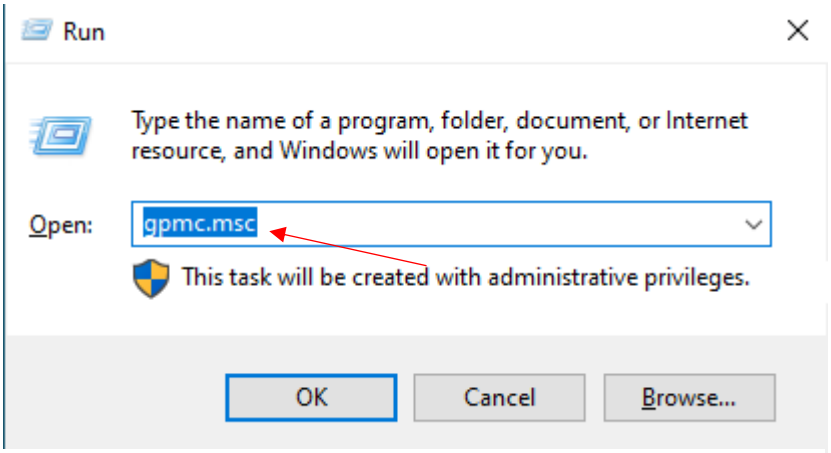


Figure 38 this task will take you to the group policy manager

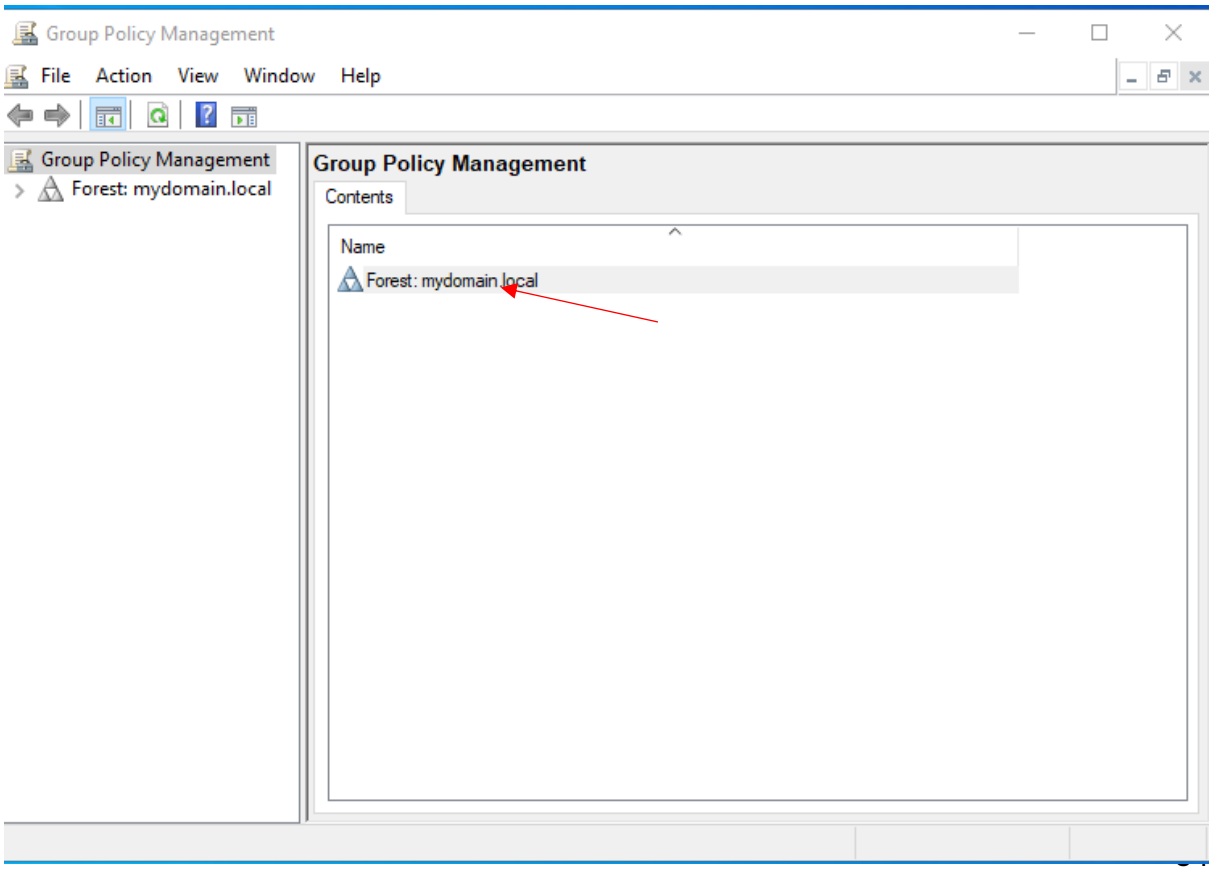


Figure 39 Group policy manager interface

7.Edit the Policy:

- In the Default Domain Policy (or a new GPO), navigate to

  "Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options "

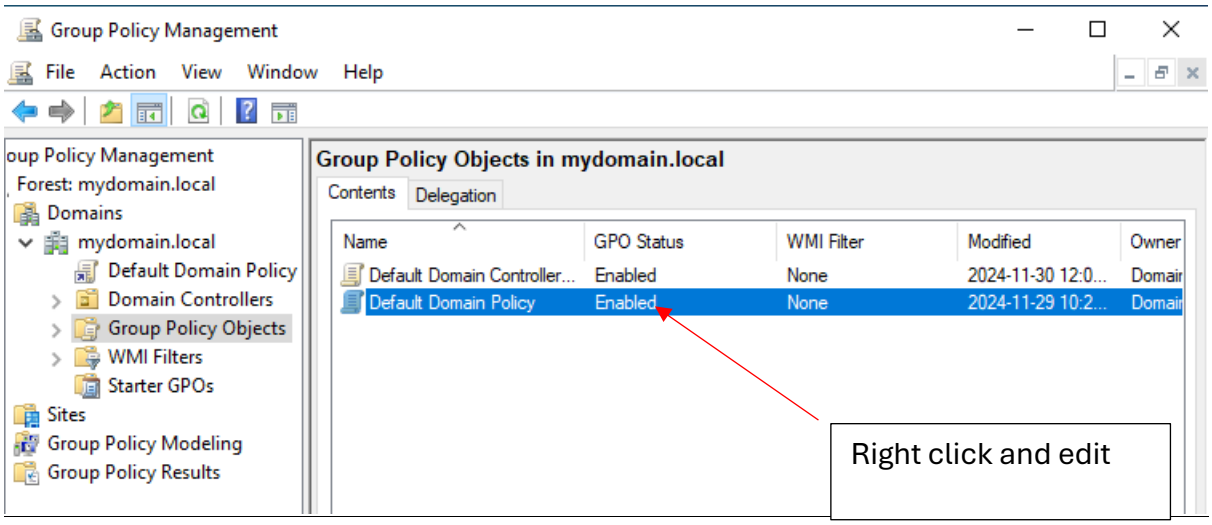


Figure 41 Navigate the default Domain Policy

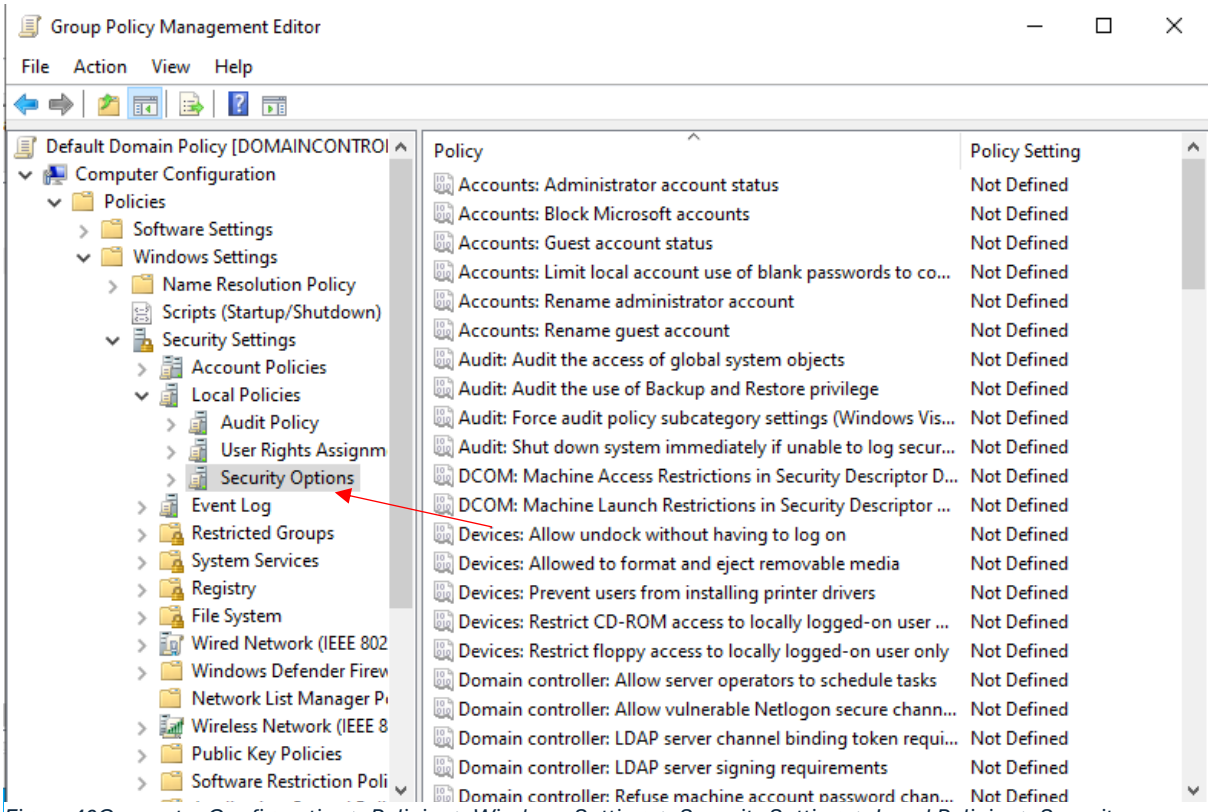


Figure 40Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options "

Set the Message Title and Text:

- Locate:
    - **Interactive Logon: Message title for users attempting to log on.**
    - **Interactive Logon: Message text for users attempting to log on.**
- Title Example: "WARNING: Authorized Access Only".
- Message Example: This system is for authorized users only. Unauthorized access is prohibited and may result in criminal and civil penalties. All activities are monitored.

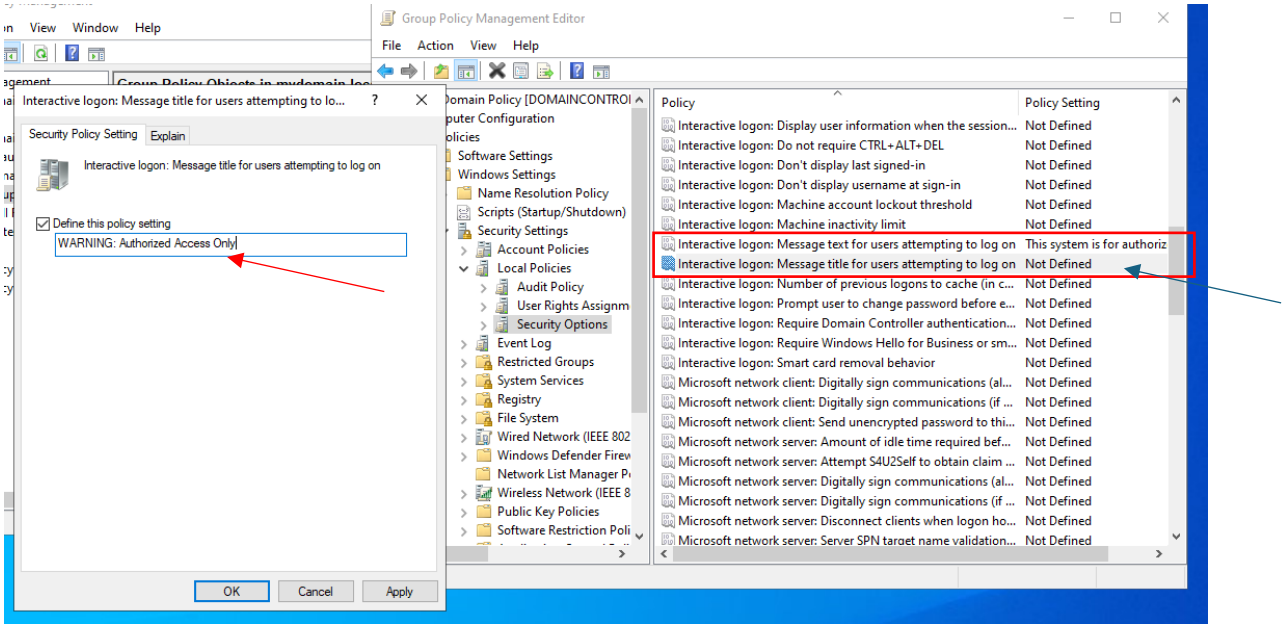


Figure 42 Set Title and Text

Apply and Test:

- Run gpupdate /force on the Domain Controller.
- Log out and back in on the Client Machine to confirm the logon message appears.

Firewall Rules

Steps to Restrict Ports for AD Communication:

1. **Log in to Each Server:**
    - Perform the steps below on the Domain Controller, File Server, and Client Machine.

2. **Open Windows Firewall:**
    - Press Windows + R, type wf.msc, and press Enter.
3. **Create Inbound Rules for AD Ports:**
    - In the left-hand pane, click **Inbound Rules**.
    - Click **New Rule** > **Port** > **TCP** > Specify Ports:
      53, 88, 135, 389, 445, 636, 3268, 3269, 464
    - Select **Allow the connection**, name the rule, and finish.

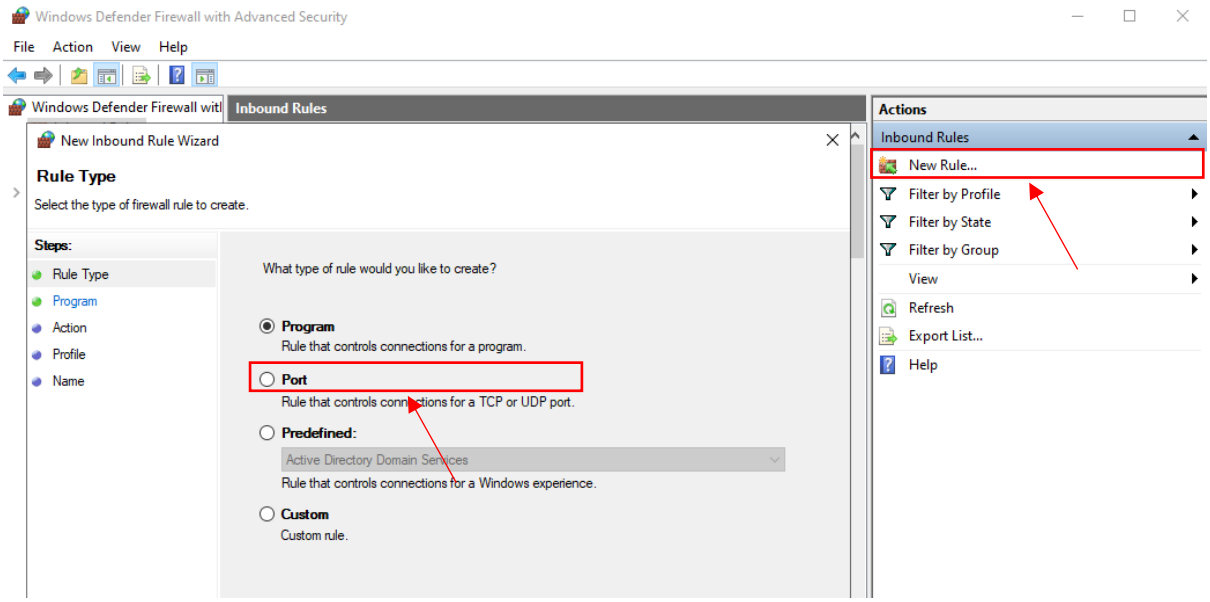


Figure 43 IIn the left-hand pane, click Inbound Rules. New rule > port ... next

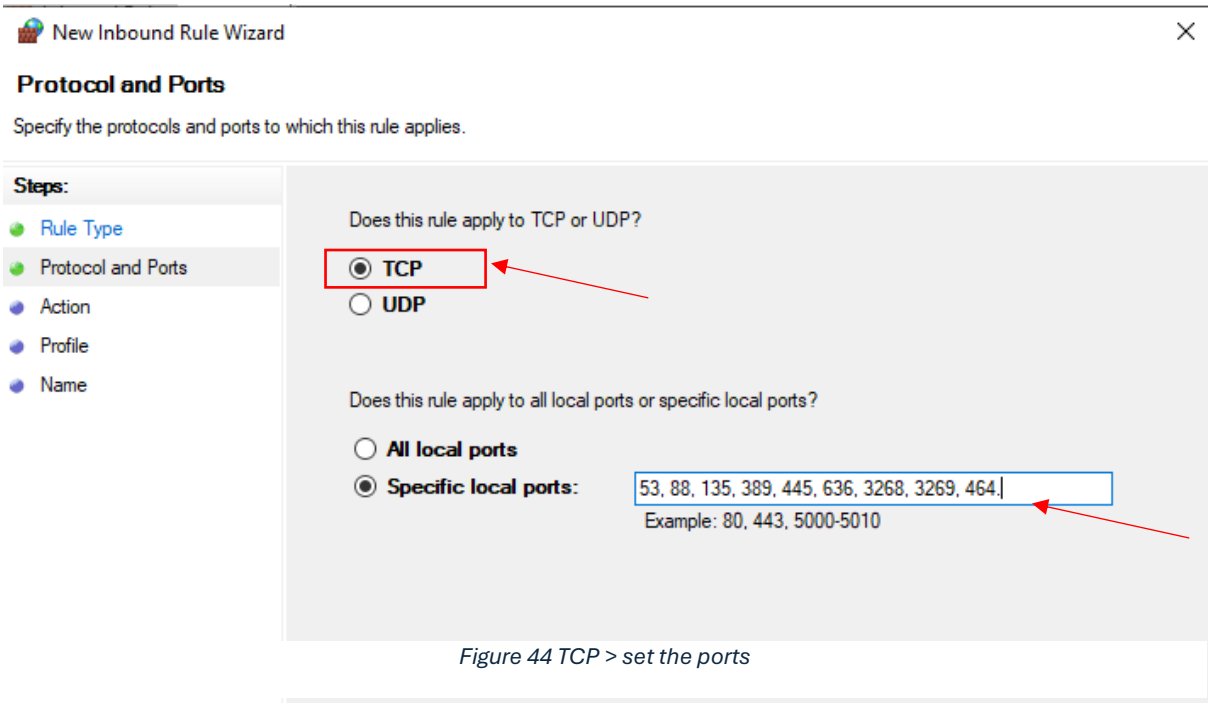


Figure 44 TCP > set the ports

4. **Create Outbound Rules for AD Ports:**
    - Follow similar steps under **Outbound Rules**, allowing only the necessary AD ports.
5. **Block Unnecessary Ports:**
    - Create additional inbound and outbound rules to block all non-essential ports.
6. **Configure Dynamic RPC Ports:**
    - Open regedit and navigate to:

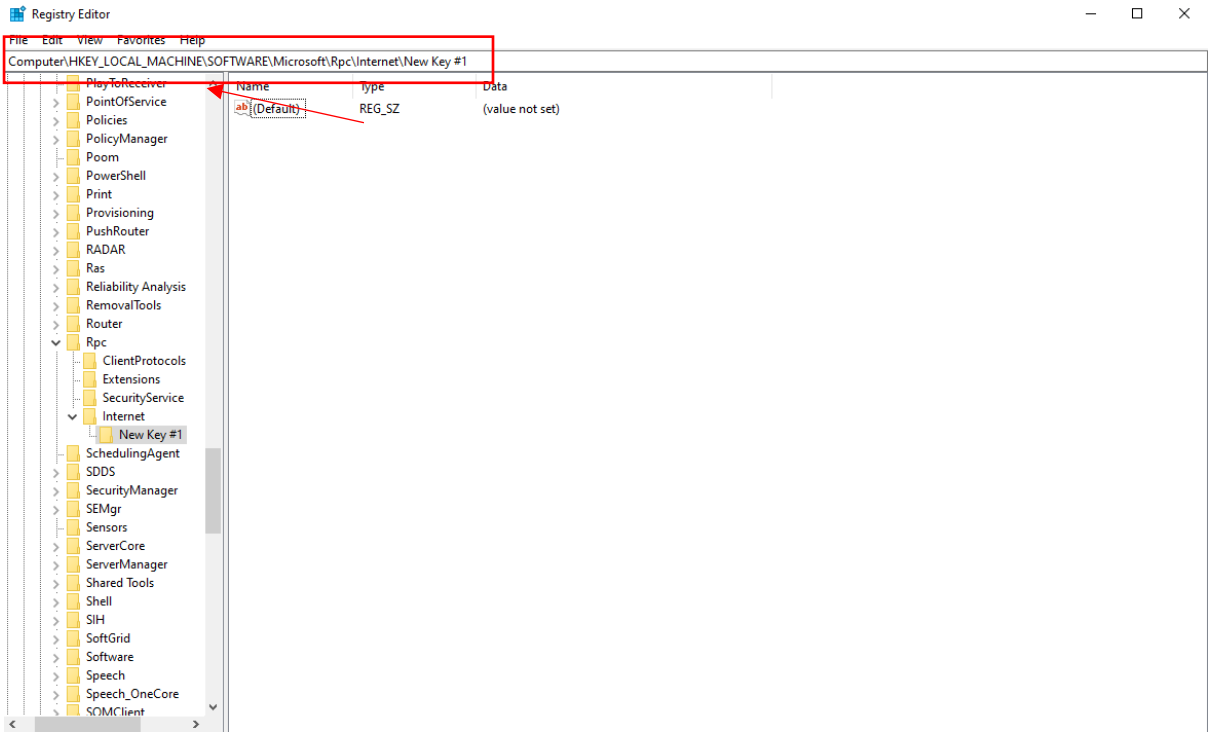


Figure 45 HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet

- Modify or create the following keys:
    - Ports: Set a range (e.g., 49152-49200).
    - PortsInternetAvailable: Set to Y.
    - UseInternetPorts: Set to Y.

7. **Restart the Servers:**
    - Reboot the Domain Controller and other servers to apply changes.
8. **Test with PowerShell:**
    - Run the following command to ensure required ports are open:

powershell

Test-NetConnection -ComputerName <DomainController_IP> -Port 88

Block SMB v1

Steps to Disable SMBv1:

1. **Log in to Each Server (Domain Controller, File Server, Client):**
2. **Check SMBv1 Status:**
    - Open PowerShell and run:

Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

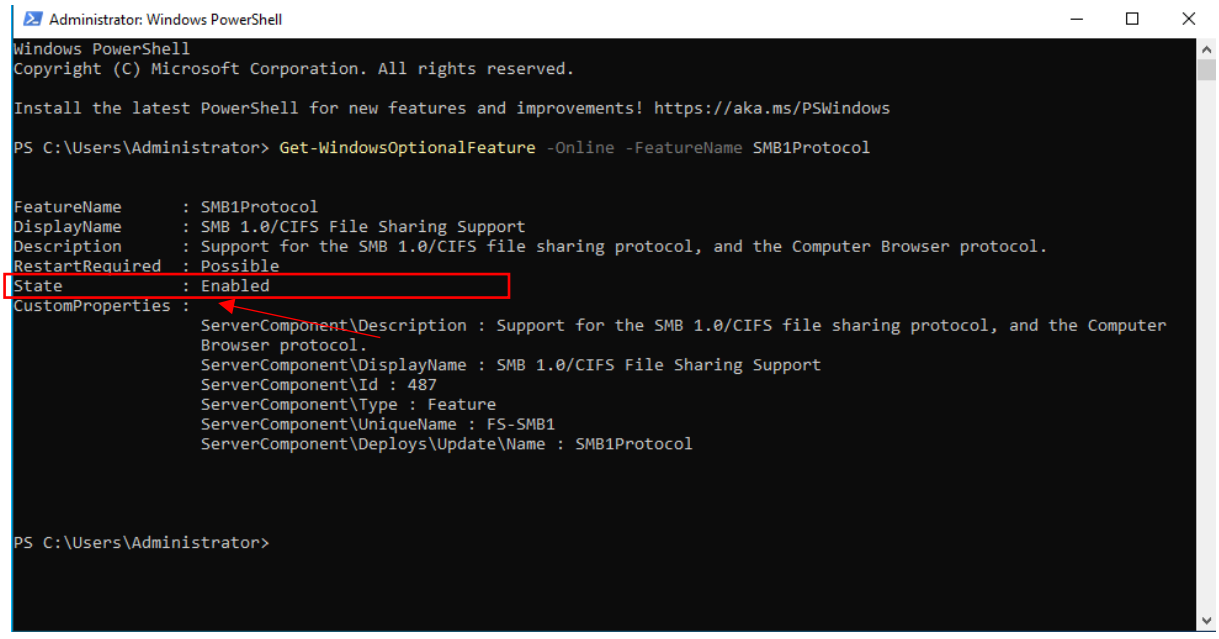


Figure 46 Check state of SMB v1

Disable SMBv1 Using PowerShell:

- Run the command

Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -Remove

Reboot the server after completing the command:

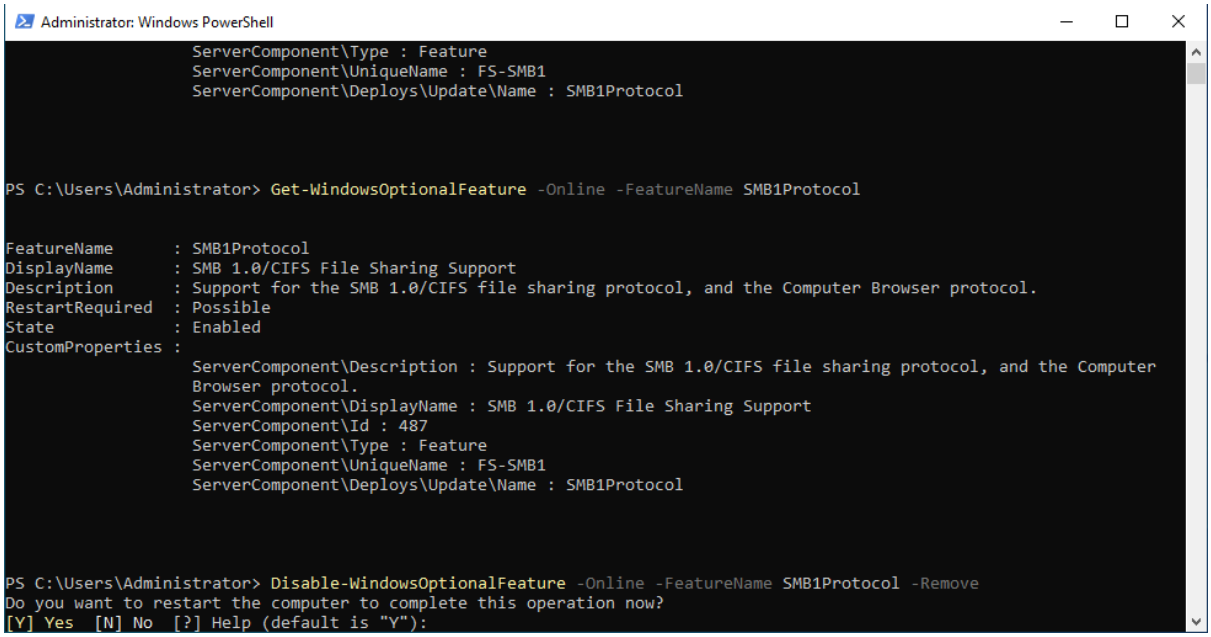
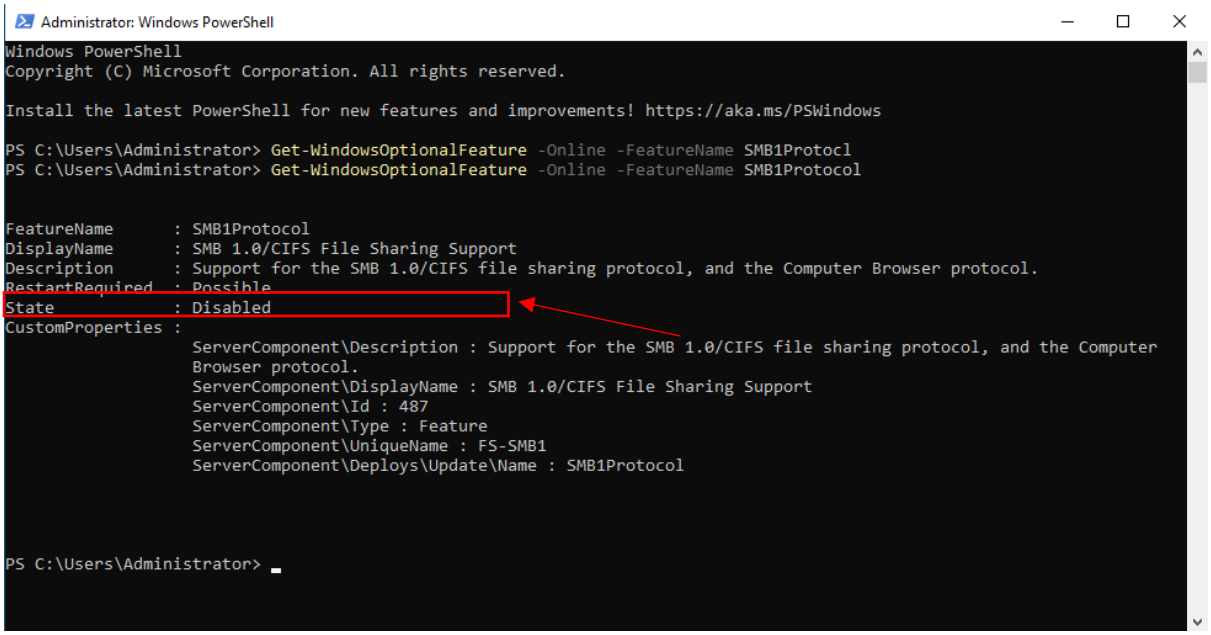


Figure 47 hit Y when prompted

Verify SMBv1 is Disabled:

- After reboot, check the status again:
- Blocking SMBv1 mitigates vulnerabilities exploited by ransomware like WannaCry



Use Group Policy to Disable LM and NTLMv1

Group Policy provides a centralized way to manage security settings.

Steps:

1. **Open Group Policy Editor**:
    - Press **Win + R**, type gpedit.msc, and press **Enter**.
2. **Navigate to Security Options**:
    - Go to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.

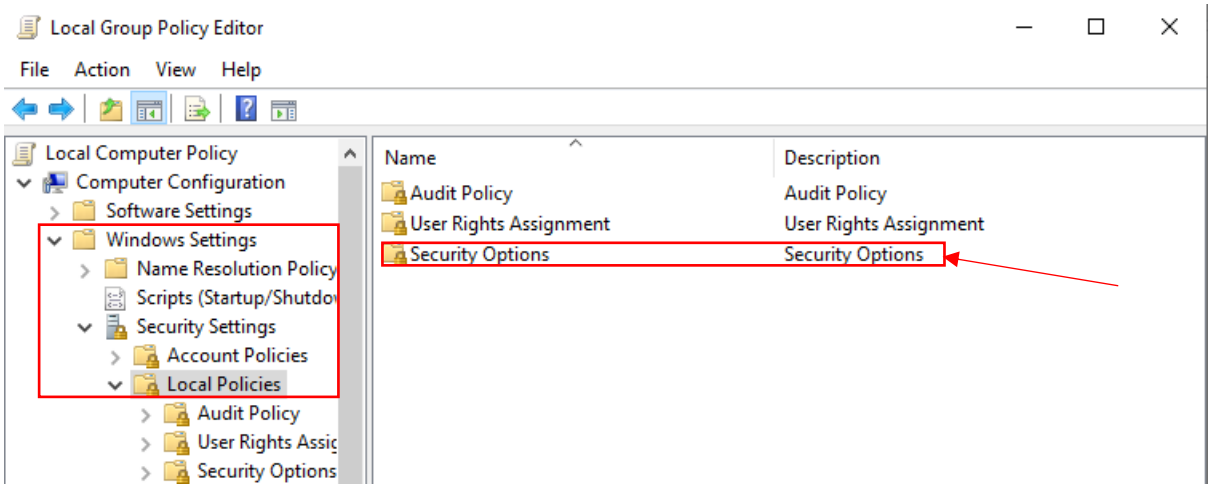


Figure 48 Navigate to Security Options

3. **Locate - Network Security: LAN Manager Authentication Level**:
    - Find the policy called **Network Security: LAN Manager authentication level**.
4. **Set LAN Manager Authentication Level**:
    - Double-click the policy.
    - From the dropdown menu, select **Send NTLMv2 response only. Refuse LM & NTLM**.

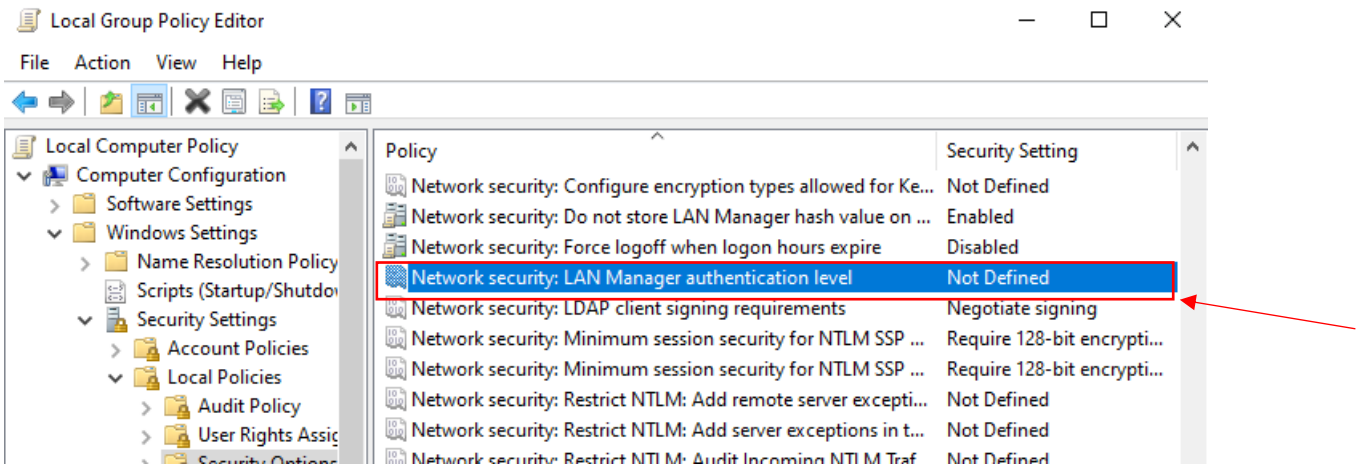


Figure 49 Find the policy called Network Security: LAN Manager authentication level.

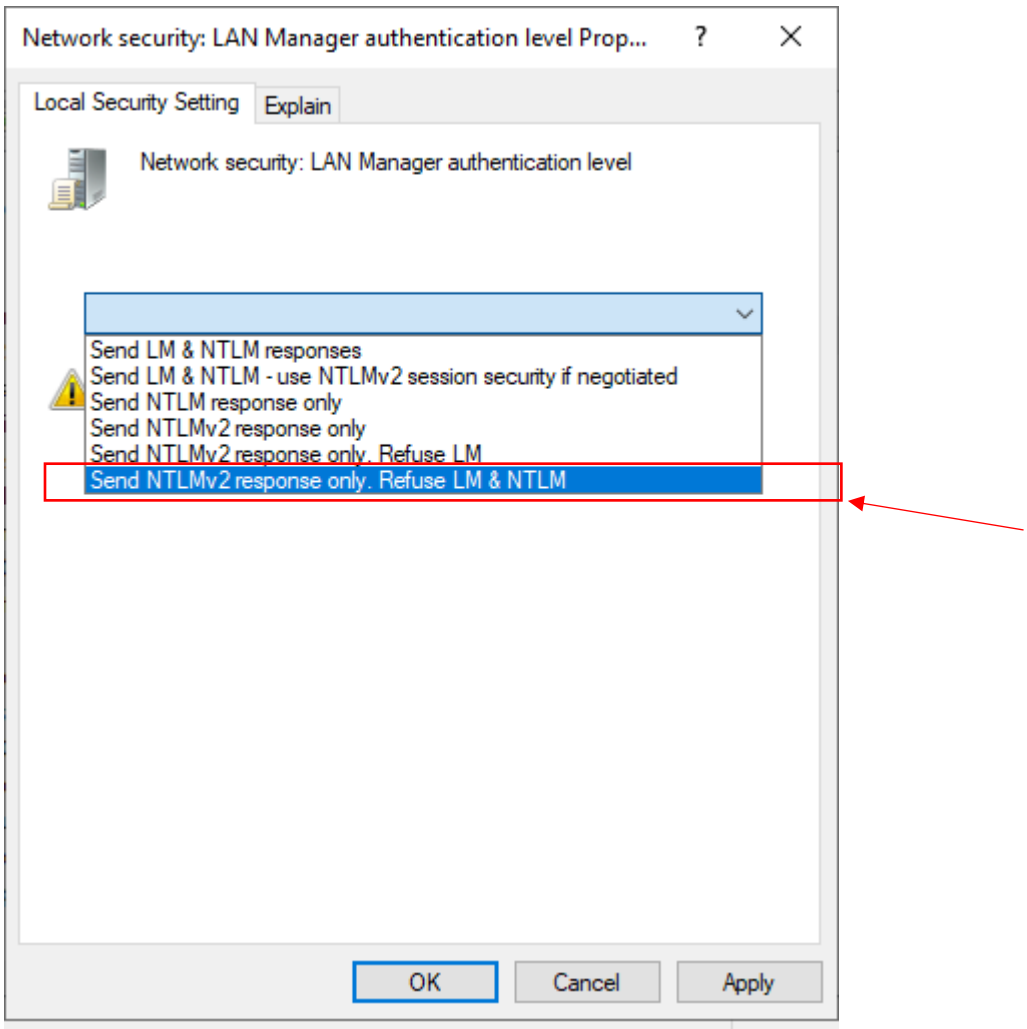


Figure 50 From the dropdown menu, select Send NTLMv2 response only. Refuse LM & NTLM.

5. **Apply and Close**:
    - Click **Apply** and **OK**

- Run gpupdate /force to apply the policy immediately.
- Reboot systems for changes to take effect.

Enable the Recycle Bin

The Recycle Bin feature must be enabled at the **forest level**. Note that this action is irreversible—you cannot disable the Recycle Bin once it is enabled.

Prerequisites

- Ensure the forest functional level is **Windows Server 2008 R2** or higher. You can check this by running:

  Get-ADForest | Select-Object ForestMode

  Using PowerShell

1. Open **PowerShell as Administrator**.
2. Enable the Recycle Bin feature with the following command:

   Enable-ADOptionalFeature -Identity "Recycle Bin Feature" -Scope ForestOrConfigurationSet -Target "mydomain.local"

   Replace mydomain.local with the name of your domain.
3. Confirm the feature is enabled:
   - Re-run the command to check the status:

   Get-ADOptionalFeature -Filter {name -like "Recycle Bin Feature"} | Select-Object Name, Ena

Check Audit Policy Using Group Policy

Audit policies are typically applied to domain controllers through Group Policy.

Steps:

1. **Open Group Policy Management**:
   - Press **Win + R**, type gpmc.msc, and press **Enter**.
2. **Locate the Group Policy for Domain Controllers**:
   - Navigate to:

Forest > Domains > YourDomain > Domain Controllers

- Right-click on the **Default Domain Controllers Policy** and select **Edit**.

3. **Navigate to Audit Policies**:
    - In the Group Policy Management Editor, go to:

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy

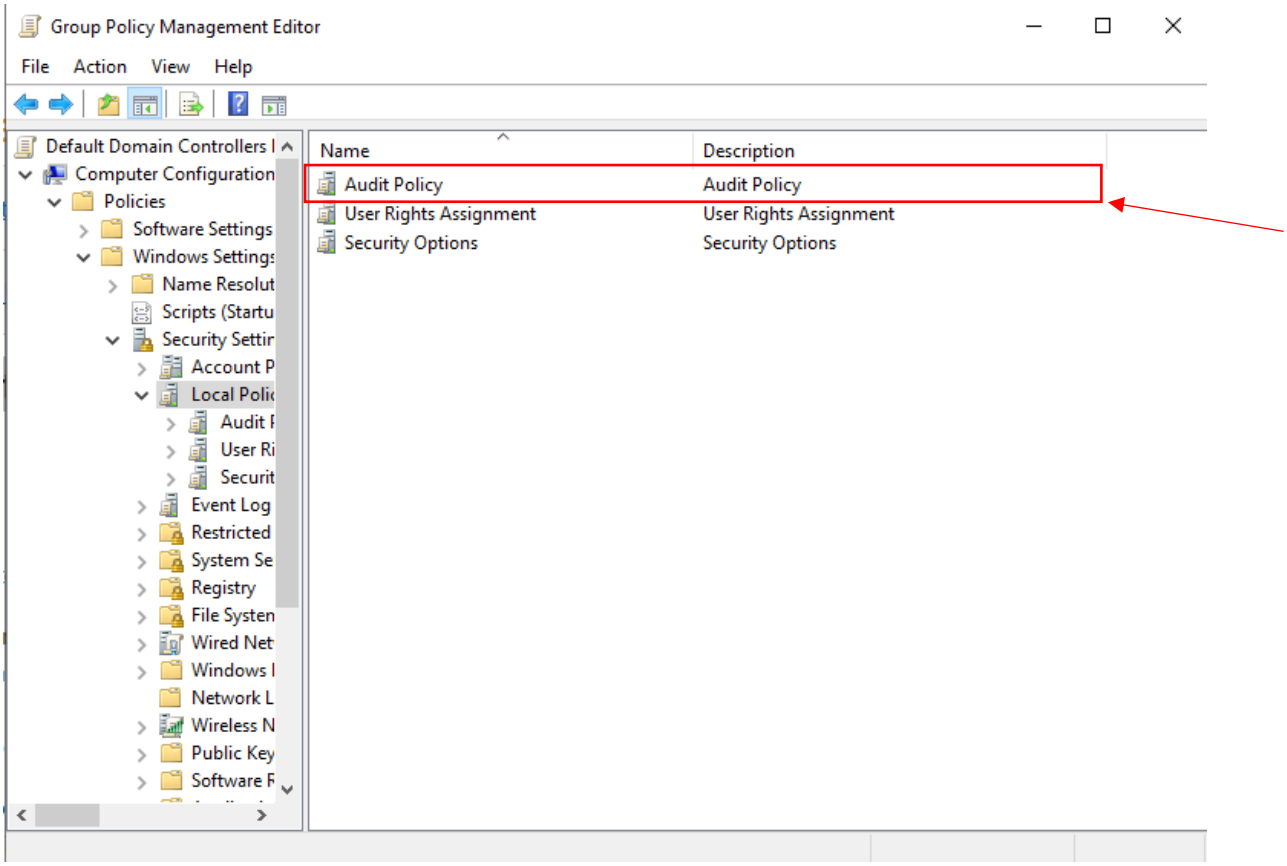


Figure 51 Navitage to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy

4. **Verify Audit Settings**: Check the following policies are configured appropriately:
    - **Audit Account Logon Events**:
        - Success and Failure
    - **Audit Logon Events**:
        - Success and Failure
    - **Audit Directory Service Access**:
        - Success and Failure
    - **Audit Account Management**:

- Success and Failure

- **Audit Policy Change**:
  - Success and Failure
- **Audit Object Access**:
  - Success (and Failure, if sensitive objects are being monitored)

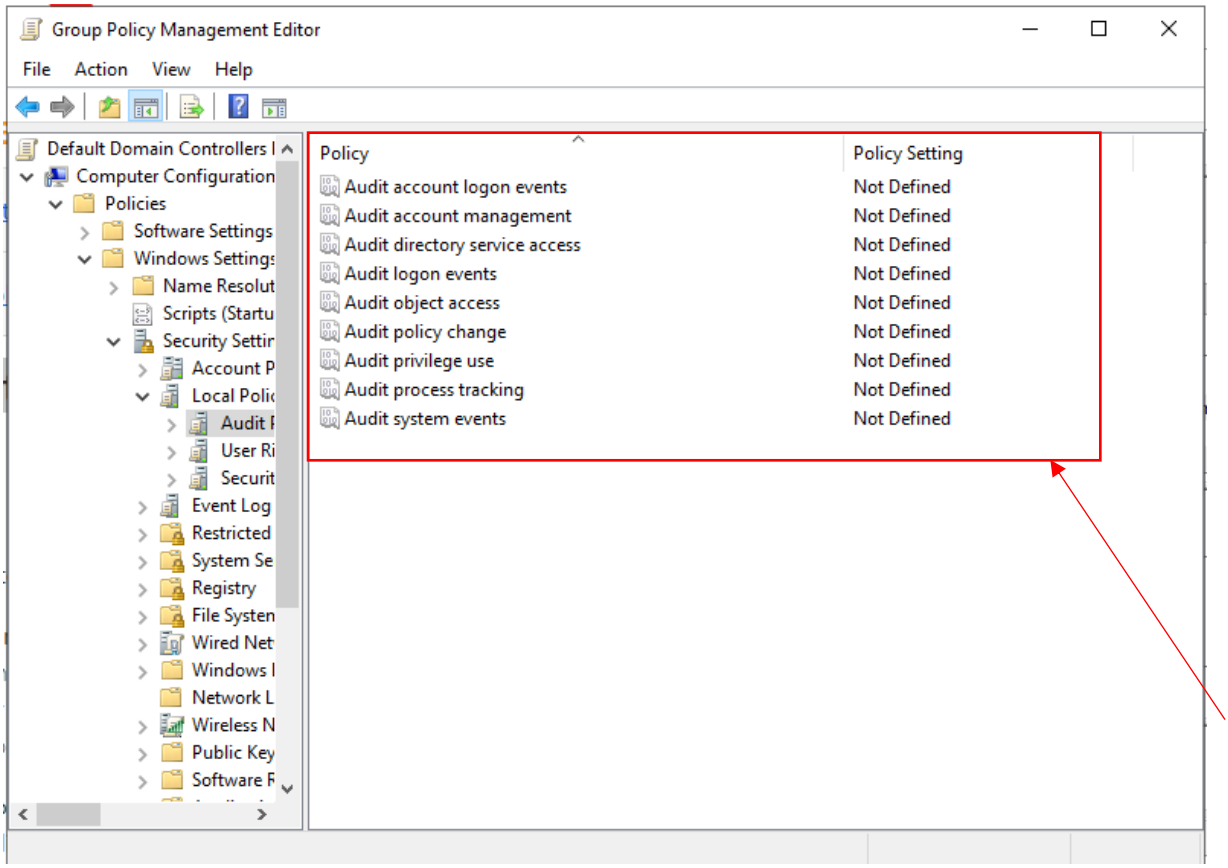


Figure 52 Verify Audit Settings

5. **Advanced Audit Policy Configuration (Optional)**:
   - Navigate to:

Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies

- Verify the following settings:
  - **Account Logon** > **Logon/Logoff Events**
  - **Policy Change** > **Audit Policy Change**

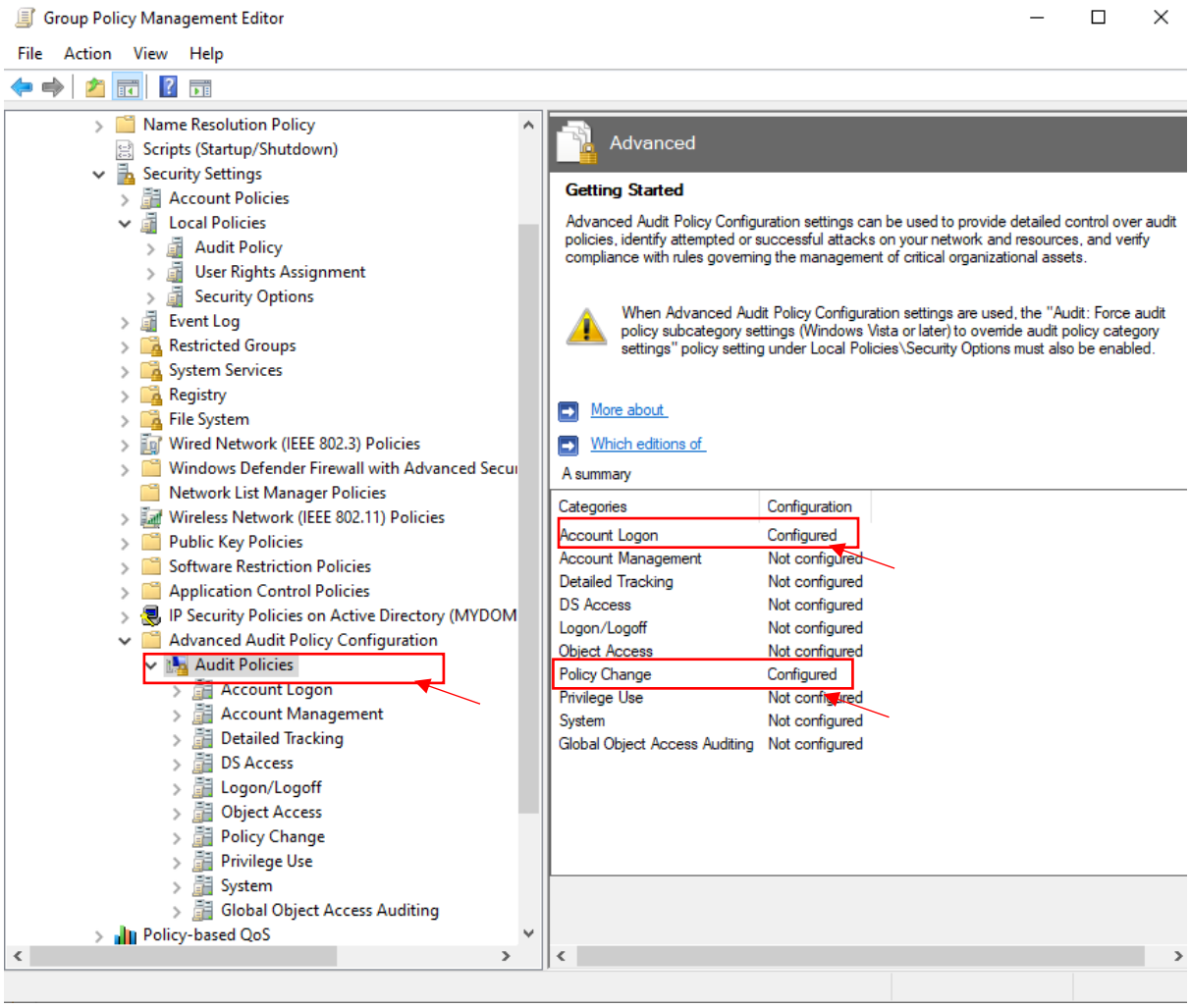


Figure 53 Verify the following settings: Account Logon > Logon/Logoff Events , Policy Change > Audit Policy Change

6. **Close and Apply**:

   - Close the Group Policy Management Editor.

     Apply the settings to the domain controllers: gpupdate /force

Challenges Faced

Network Configuration Issues

- **Challenge**:
  During the initial setup, communication issues arose between the **Windows Server 2022 (Domain Controller)**, **Windows client**, and **Kali Linux**. The machines were configured on different subnets, which prevented them from properly communicating with each other. This issue was especially noticeabl
- e when trying to ping from one VM to another, leading to failed attempts at connectivity.

- **Solution**:
  To resolve this, We aligned all the VMs (Windows Server, Windows client, and Kali Linux) on the same subnet. After reviewing the IP addresses and subnet masks, We modified the network configurations on each machine to ensure that they all had IPs in the **192.168.56.x** range with a subnet mask of **255.255.255.0**. This ensured that all machines could communicate directly with each other. After updating the IP configurations, I verified connectivity by running **ping tests** from one VM to another. The ping tests were successful, and the network was functional.

- **Lessons Learned**:
  This challenge emphasized the importance of consistent and accurate network configuration in a virtualized environment. Ensuring that all VMs are aligned on the same subnet and have the correct gateway settings is critical for seamless communication. It also reinforced the need to troubleshoot basic connectivity issues first before moving on to more complex configurations.

Default Permissions

- **Challenge**:
  Another challenge was the default **ms-DS-MachineAccountQuota** setting in Active Directory, which allows basic users to register up to 10 computers in the domain. This default configuration is a potential security risk because it permits users without administrative privileges to register computers in the domain, which could lead to unauthorized devices being added to the network.

- **Solution**:
  To address this, I manually modified the **ms-DS-MachineAccountQuota** value to 0, effectively preventing any user from registering computers in the domain. Additionally, I restricted the **SeMachineAccountPrivilege** to only **Domain Admins**, which ensures that only authorized administrators can add computers to the domain. These changes were applied using **Group Policy** and **PowerShell** commands to adjust the machine account quota and permissions.

- **Lessons Learned**:
  This issue highlighted the importance of reviewing and modifying **default permissions** during initial setup. While **Active Directory** is a powerful tool for managing domain resources, the default configurations might not always be aligned with security best practices. Restricting privileges such as computer registration is essential to ensure that only trusted entities can join devices to the domain, preventing unauthorized access.

3. Delegation Flag Limitations

- **Challenge**:
  Enabling the **"Sensitive and cannot be delegated"** flag for privileged accounts posed a significant challenge. By default, this flag is not enabled on many privileged accounts in Active Directory, making those accounts susceptible to impersonation attacks through delegation. This configuration setting had to be applied to all accounts within high-privilege groups, such as **Domain Admins** and **Enterprise Admins**, to prevent unauthorized delegation of these accounts.

However, manually enabling this setting for each account in Active Directory was time-consuming and prone to human error, especially with a large number of privileged accounts.

- **Solution**:
  To efficiently apply the **"Sensitive and cannot be delegated"** flag to all relevant accounts, I used **PowerShell scripts**. The script was designed to identify all users in **Domain Admins**, **Enterprise Admins**, and **Administrators** groups, then automatically enable the delegation flag for each of these accounts. The script was as follows:

```
$AdminGroups = @("Domain Admins", "Enterprise Admins", "Administrators")

foreach ($Group in $AdminGroups) {

    Get-ADGroupMember -Identity $Group | ForEach-Object {

        Set-ADUser -Identity $_.SamAccountName -Add
    @{userAccountControl="1048576"}

}

    }
```

This script added the 1048576 flag (which represents **"Sensitive and cannot be delegated"**) to the **userAccountControl** attribute for all identified accounts in the specified groups.

- **Lessons Learned**:
  This challenge underscored the importance of automation when managing large environments. Manual configuration for security settings on individual accounts can be error-prone and inefficient. Using **PowerShell scripting** to apply consistent security measures across multiple accounts is a more reliable and scalable solution. It also reinforced the idea that security should be applied uniformly to all privileged accounts, especially in a domain environment, to minimize the risk of delegation attacks.

Key Learnings

Systems Security

1. **Principle of Least Privilege and RBAC (Role-Based Access Control):**
    - Configuring and managing an Active Directory (AD) environment emphasized the importance of minimizing access rights to only what is necessary for users and groups to perform their tasks. This principle of least privilege is vital for reducing the attack surface and limiting the damage that a compromised account can cause.
    - Through RBAC, we understood the granular control that AD provides, allowing permissions to be assigned at various levels, from files and folders to domain-wide roles. This experience reinforced how vital it is to document and maintain these permissions for scalability and security.
2. **Group Policy Management:**
    - Implementing Group Policies (GPOs) showcased how powerful centralized management can be in enforcing consistent security settings across all domain-joined devices. For example, policies for password complexity, account lockouts, and screensaver settings were applied uniformly, reducing the likelihood of misconfigurations.
    - GPOs also provided insight into how automation can simplify managing large-scale environments, especially in scenarios involving compliance requirements.
3. **Permission Testing and Validation:**
    - The iterative process of testing permissions highlighted potential pitfalls, such as unintended inheritance or misconfigured rules. Learning to use AD's auditing tools provided valuable insights into tracking access attempts and failures.

Virtualization Security

1. **Efficiency Through Virtualization:**
    - Virtualization with tools like linked clones allowed us to quickly replicate environments, saving time and resources. This setup facilitated isolated testing, enabling us to troubleshoot without impacting the base configurations.
    - We also recognized the importance of proper resource allocation and snapshot management to ensure system stability and reliability.

2. **Network Segmentation and Misconfiguration Risks:**
    - Configuring virtual networks underscored how interconnected systems can expose vulnerabilities if not properly segmented. For example, incorrect DNS settings or open virtual adapters could allow unintended traffic, compromising the domain's integrity.
    - Implementing a virtual firewall and reviewing traffic flow between machines taught us how critical network security is in a domain environment.
3. **Encryption and Hardening Techniques:**
    - Virtualization provided a safe environment to experiment with features like BitLocker encryption, Enhanced PIN, and securing virtual machine snapshots. These practices illustrated how encryption protects data integrity even in scenarios where the VM files are accessed outside the environment.

Tool Utilization

1. **Nessus and Ping Castle:**
    - Nessus enabled us to identify vulnerabilities in our configurations by providing comprehensive scans with actionable insights. For instance, it flagged outdated protocols and misconfigured firewall rules.
    - Ping Castle highlighted potential weaknesses specific to Active Directory, including risks like weak password policies and privilege escalation paths, allowing us to make informed improvements.

2. **PurpleKnight for AD Security Assessment:**
    - PurpleKnight provided an additional layer of insight into the security posture of our Active Directory environment. Its ability to scan and flag critical misconfigurations, such as account lockout settings, stale accounts, and improper privilege assignments, made it a valuable tool in our security assessment process.
    - The detailed report generated by PurpleKnight offered prioritized recommendations, which we used to address high-risk issues, further hardening our environment.

3. **Bloodhound for AD Analysis:**
    - Bloodhound introduced us to the concept of "attack paths" within Active Directory, helping us visualize how attackers could escalate privileges through misconfigurations or overly permissive settings. This tool was instrumental in teaching us how to mitigate potential lateral movement threats.
4. **Hardening Through Benchmarks:**
    - Using CIS benchmarks and Microsoft guidelines helped us systematically improve the environment's security posture. These resources ensured we didn't overlook critical aspects like disabling SMBv1 and configuring secure local admin accounts.

Team Collaboration and Research

1. **Effective Division of Labor:**
    - Dividing tasks based on individual strengths allowed us to tackle complex configurations more efficiently. This approach ensured that tasks like setting up the domain, securing the environment, and testing permissions were handled in parallel without redundancy.
2. **Deepening Research Skills:**
    - The project required extensive research to identify best practices for hardening Active Directory and securing virtualized environments. Evaluating sources, synthesizing information, and applying relevant strategies enriched our learning process.
3. **Problem-Solving Under Pressure:**
    - Technical hurdles, such as troubleshooting login issues or resolving failed domain joins, fostered collaboration and critical thinking. By brainstorming solutions and sharing knowledge, we grew more adept at resolving real-world challenges.

Reflection

This lab project was not only a technical challenge but also a valuable exercise in applying theoretical knowledge to practical scenarios. It deepened our understanding of security principles, system administration, and Active Directory management while emphasizing the importance of teamwork and communication.

The hands-on experience provided a strong foundation in setting up and securing virtualized systems. It prepared us for real-world situations by developing skills in vulnerability assessment, permission management, and security hardening. The challenges we faced served as opportunities to enhance our adaptability and problem-solving capabilities, leaving us better equipped for future professional endeavors in systems and virtualization security.

Conclusion

This project demonstrated the successful configuration and security hardening of a Windows Server 2022 domain environment, emphasizing the importance of aligning with industry-recognized security best practices. By creating a fully functional Active Directory setup with a Domain Controller, File Server, and Client machine, we gained hands-on experience in deploying and managing enterprise-level infrastructure. The effective implementation of Role-Based Access Control (RBAC) and Group Policies further ensured that the environment was not only operational but also secure and compliant with organizational security standards.

The challenges encountered during the project, including network misconfigurations, permission testing, and integrating advanced security tools, underscored the critical need for continuous monitoring, robust policy enforcement, and proactive security hardening. These challenges provided valuable learning opportunities, allowing us to explore advanced tools like Nessus, Ping Castle, PurpleKnight, and Bloodhound. These tools enabled us to identify and address vulnerabilities, reinforcing the importance of using automated security assessment solutions in real-world environments.

Moreover, the project highlighted the crucial role of virtualization in modern IT infrastructure. Virtualization not only streamlined the setup process but also underscored the security implications of misconfigured virtual networks and systems. By implementing encryption techniques, securing virtual machine snapshots, and applying hardening benchmarks, we ensured that our virtualized environment met high-security standards.

In today's digital landscape, where systems face constant threats from cyberattacks and misconfigurations, the importance of securing both physical and virtualized systems cannot be overstated. This project reinforced the need for a layered security approach, emphasizing preventive measures, regular audits, and the application of best practices in systems and virtualization security. Through this experience, we are better equipped to handle complex infrastructure challenges and to contribute to building resilient, secure IT environments in professional settings.

Scanning Reports Links:

https://drive.google.com/drive/folders/1Cy03eLT-qXxeH51FEoLZhpQBVi7kYvWp?usp=sharing

REFERENCES

- **Microsoft Documentation**
  - Microsoft Corporation. "Active Directory Users and Computers Overview." https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/active-directory-users-and-computers
- **Group Policy Management**
  - Microsoft Corporation. "What is Group Policy?" https://learn.microsoft.com/en-us/windows-server/identity/guided-group-policy-management
- **Ping Castle**
  - Ping Castle. "Active Directory Security Assessment Tool Documentation." https://www.pingcastle.com/documentation/
- **Nessus Vulnerability Scanning**
  - Tenable Inc. "Nessus Essentials User Guide." https://www.tenable.com/products/nessus/nessus-essentials
- **Account Lockout Policies**
  - Microsoft Corporation. "Account Lockout Policy Configuration." https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy
- **User Account Delegation**
  - Microsoft Corporation. "Understanding the 'Sensitive and Cannot Be Delegated' Account Option." https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/user-account-delegation

- **Active Directory Hardening**
  - Center for Internet Security. "CIS Microsoft Windows Server 2022 Benchmark." https://www.cisecurity.org/benchmark/microsoft_windows_server
- **SeMachineAccountPrivilege and ms-DS-MachineAccountQuota**
  - Microsoft Corporation. "Restricting Workstation Join Rights in Active Directory." https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/add-workstations-to-domain
- **Windows Firewall**
  - Microsoft Corporation. "Windows Defender Firewall with Advanced Security Administration Guide." https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security
- **PowerShell Scripting**
  - Microsoft Corporation. "PowerShell Documentation and Examples." https://learn.microsoft.com/en-us/powershell/