Windows Active Directory Domain Security Lab

Nelson R. Acevedo | Cybersecurity Student

Introduction:

This project demonstrates the deployment and hardening of a Windows Active Directory domain using Windows Server 2022 in a virtualized environment. The lab simulates a small enterprise infrastructure with centralized user management, Group Policy enforcement, access control, and security monitoring.

Project Goals:

The goals of this project were:

- Create a Windows Domain.
- Join at least a client device on the domain (for testing users).
- Manage users and group centrally from Active Directory (AD)
- Improve Security and access control.

Tools:

- VMware Workstation
- Windows Server 2022
- Windows 11 Client
- Active Directory Domain Services (AD DS)
- DNS
- Group Policy Management.

Setup Steps:

1. Installed Windows Server 2022
2. Promoted to Domain Controller
3. Created OU structure: IT, HR, Users
4. Configured DNS

5. Joined Windows 11 client to domain
6. Created groups & assigned permissions

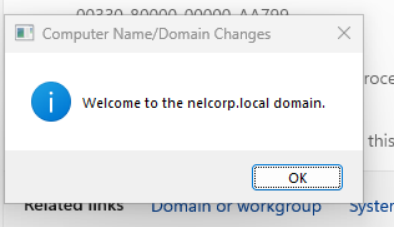
Environment Design:

Domain Name: nelcorp.local

Virtual Machines:

- DC01 – Windows Server 2022 (Domain Controller)
- CLIENT01 – Windows 11 (Domain-Joined)

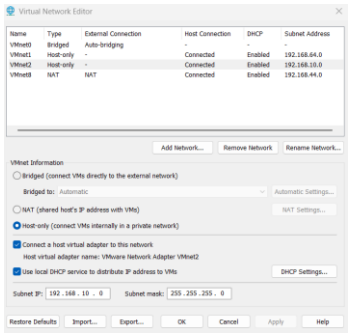
Screenshot of CLIENT01 after joining the Domain



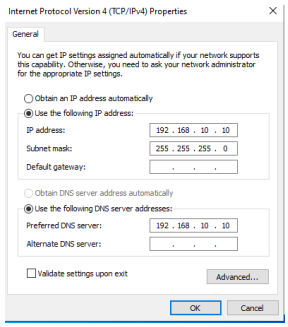
Network Design:

- VMware Internal network: VMnet2 – 192.168.10.0
- DC01 has a static ip address: 192.168.10.10
- DNS is pointing to the Domain Controller which is DC01 (this includes DC01 itself)

Network configuration in vmware – Screenshot.



Network configuration in DC01 – Screenshot

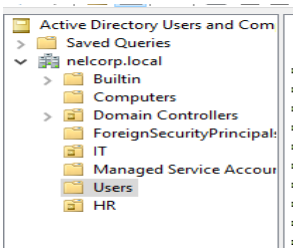


Active Directory Structure:

Organizational Units:

- IT
- HR
- Users

This Structure allows to create targeted Group policies, keeps everything organized and simulates how a real-world company works.



Screenshot – Organizational Units in Active directory domain.

Users, Groups & Access Control:

Users:

it.admin

john.hr

mary.user

Groups:

IT_Admins → Members: it.admin

HR_Users → Members: john.hr

Each group and user was created on their respective Organizational Unit. The groups allow us to add users to them and then use them for filtering group policies and allow access to share resources to specific users.

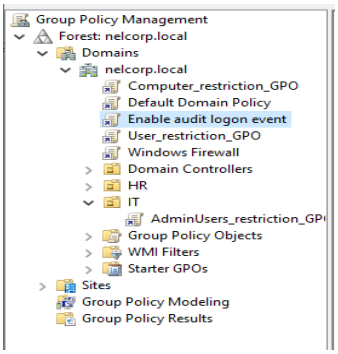
Group Policy and Security Implementation:

Group Policies and other security measures taken:

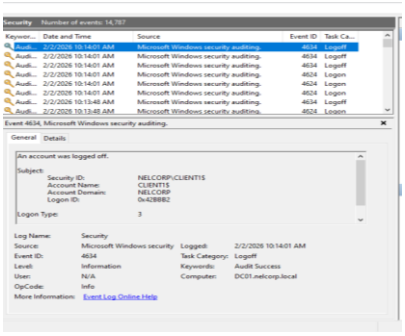
- Strong password policy.

- Disabled Control Panel for standard users.
- Automatic workstation lock after inactivity.
- Enforced Windows Defender Firewall.
- Disabled default Administrator account.
- Enabled audit logon and logoff events.
- Disabled default Guest account.

This policies and security measures assure that our domain is secure and give us a way to monitor users' activity. By disabling default accounts, we protect our domain from brute force attacks. **Note:** In my case the default Administrator Account was disabled after creating a dedicated administrative account called "it.admin". However, if this dedicated administrative account were not available, the default Administrator account could've been renamed.



Screenshot – Group policies manager



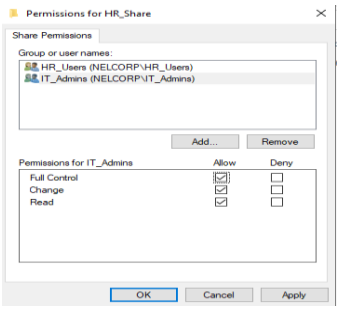
Screenshot – Audit Logon and Logoff events in Event Viewer

File Server & Permissions:

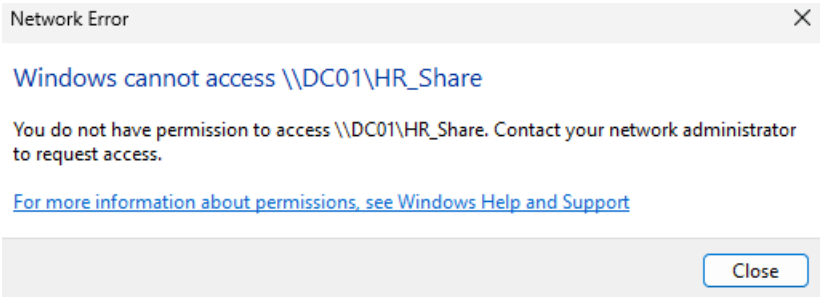
I created a secure share folder with a file inside with NTFS permissions and Share permissions to only allow access to allowed User Groups.

- HR_Users and IT_Admins → Access Allowed.
- Other Users → Access Denied.

This proves access control by using User Groups filtering.



Screenshot - Share Permissions

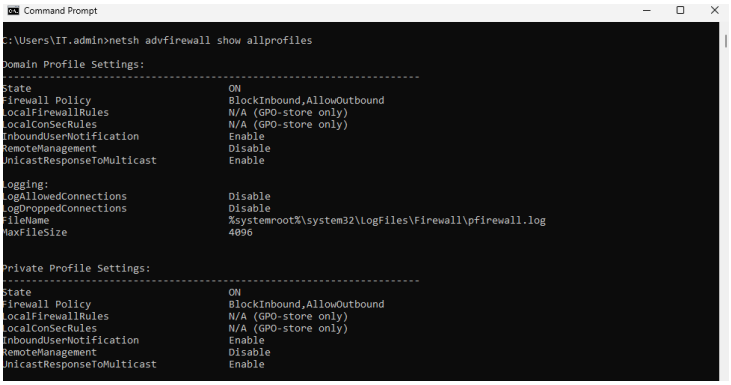


Screenshot - Access denied message for not allowed users

Testing & Validation:

The followed validations and tests were made to ensured everything worked fine:

- Confirmed GPO applications to specific users (not all users are allowed to do the same).
- Tested file share on both authorized and unauthorized users.
- Verified GPOs and firewall status on the client's device.
- Confirmed that Audit logon and logoff event were being sent to the Domain Controller's Event Viewer.



Challenges & Lessons Learned:

Challenges:

- **DNS misconfigurations:**
  - 🚨 Challenge: DNS misconfigured — domain join failed.
  - 🛠️ Fix: Updated DC01 DNS settings to point to itself.

- **Group Policies not applied to specific Organizational Unit (OU) due to incorrect OU configuration:**
    - 🚨 Challenge: I thought that having a user who was a member of a group in an Organizational Unit (OU) made it part of that OU - This resulted in policies not being applied correctly.
    - 🛠️ Fix: Move the users from the User OU to their respective Ous.

Lessons Learned:

- DNS is crucial for Windows Domains.
- Having a user inside of a user group that is inside of an OU doesn't make it part of that OU. The user itself has to be moved to the OU.
- Every Group policy or any other security measure has to be tested and troubleshoot if it fails.