Active Directory Domain Lab & Security Hardening (Virtual Enterprise)

Executive Summary

Built a small virtual enterprise environment using VirtualBox to practice Windows domain administration and baseline security hardening. The lab includes a Windows Server Domain Controller (AD DS + DNS), a Windows 10 domain-joined client, and a Kali Linux machine for connectivity testing. Key outcomes include Organizational Unit (OU) design, user/group management, Group Policy restrictions, account lockout policy, DNS record management, and role-based file access controls.

Objectives

- Create a reproducible Windows domain lab (Server + Client) inside a controlled virtual network.
- Deploy Active Directory Domain Services (AD DS) and DNS on a Domain Controller.
- Join a Windows client to the domain and validate authentication and name resolution.
- Implement baseline security controls using Group Policy and NTFS/share permissions.
- Document steps and evidence so the lab can be rebuilt and extended (e.g., SIEM monitoring).

Lab Architecture

Virtual machines and roles:

VM	OS	Role	Network
Server20	Windows Server	Domain Controller (AD DS + DNS)	VirtualBox NAT Network: Virtualization
PC1	Windows 10	Domain-joined workstation	VirtualBox NAT Network: Virtualization
Kali	Kali Linux	Testing / admin utility VM	VirtualBox NAT Network: Virtualization

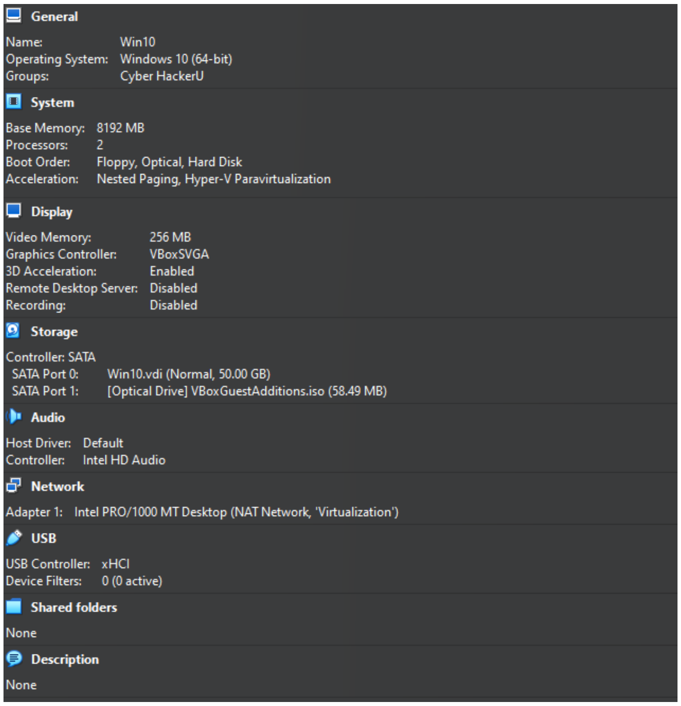
Network notes:

- Created a VirtualBox NAT Network named Virtualization and attached all VMs to it.
- Validated basic connectivity between VMs and to the internet (e.g., ping to Google DNS).
- Enabled the Windows Defender Firewall inbound rule for ICMP echo requests on the Windows 10 client to allow ping testing from Kali.

Implementation Overview

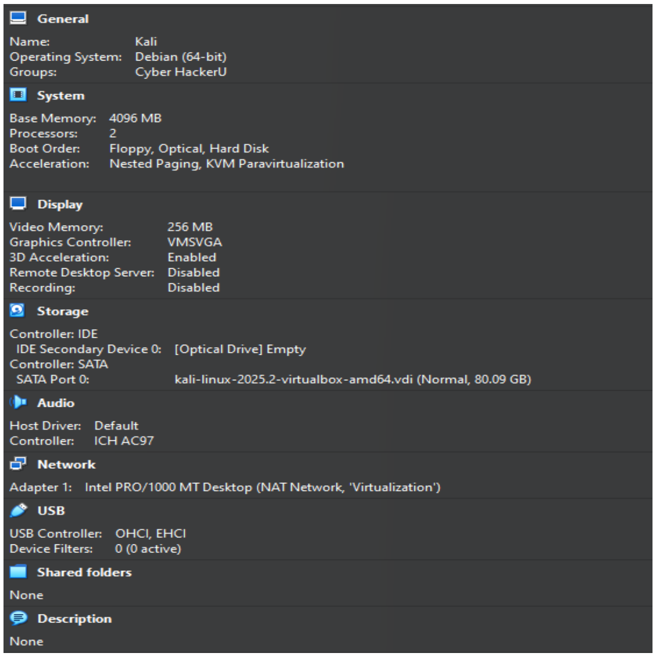
1) Build the virtual environment

- Created a Windows 10 VM and installed Guest Additions.



```
General
Name:               Win10
Operating System:   Windows 10 (64-bit)
Groups:             Cyber HackerU
System
Base Memory:   8192 MB
Processors:    2
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  Nested Paging, Hyper-V Paravirtualization
Display
Video Memory:           256 MB
Graphics Controller:    VBoxSVGA
3D Acceleration:        Enabled
Remote Desktop Server:  Disabled
Recording:              Disabled
Storage
Controller: SATA
 SATA Port 0:     Win10.vdi (Normal, 50.00 GB)
 SATA Port 1:     [Optical Drive] VBoxGuestAdditions.iso (58.49 MB)
Audio
Host Driver:   Default
Controller:    Intel HD Audio
Network
Adapter 1:   Intel PRO/1000 MT Desktop (NAT Network, 'Virtualization')
USB
USB Controller:   xHCI
Device Filters:   0 (0 active)
Shared folders
None
Description
None
```

- Imported/created a Kali Linux VM.



General

Name: Kali
Operating System: Debian (64-bit)
Groups: Cyber HackerU

System

Base Memory: 4096 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 256 MB
Graphics Controller: VMSVGA
3D Acceleration: Enabled
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2025.2-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'Virtualization')

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

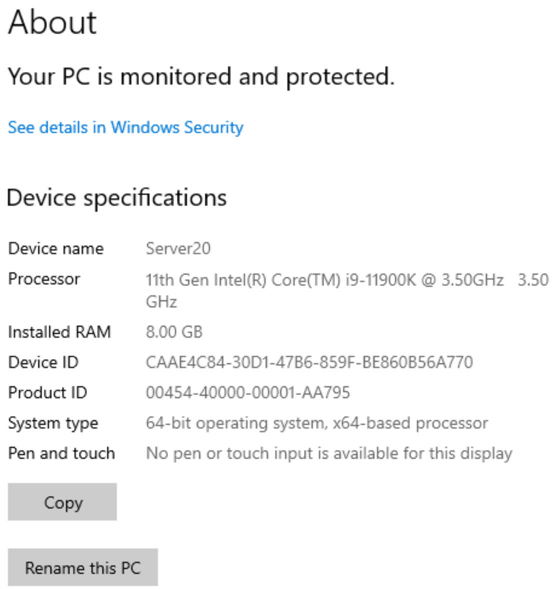
Shared folders

None

Description

None

- Created a Windows Server VM and named it Server20.



About

Your PC is monitored and protected.

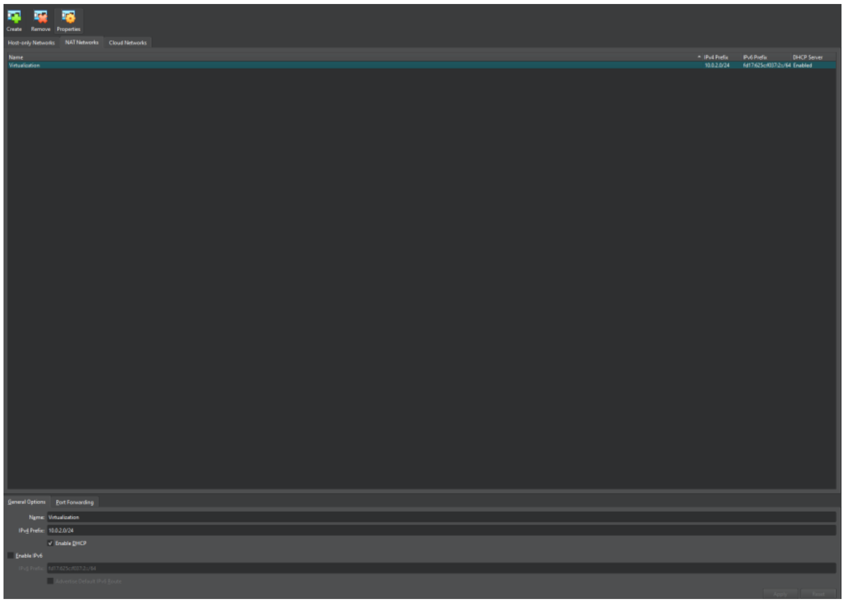
See details in Windows Security

Device specifications

Device name Server20
Processor 11th Gen Intel(R) Core(TM) i9-11900K @ 3.50GHz 3.50 GHz
Installed RAM 8.00 GB
Device ID CAAE4C84-30D1-47B6-859F-BE860B56A770
Product ID 00454-40000-00001-AA795
System type 64-bit operating system, x64-based processor
Pen and touch No pen or touch input is available for this display

2) Configure networking

- Created NAT Network Virtualization in VirtualBox.



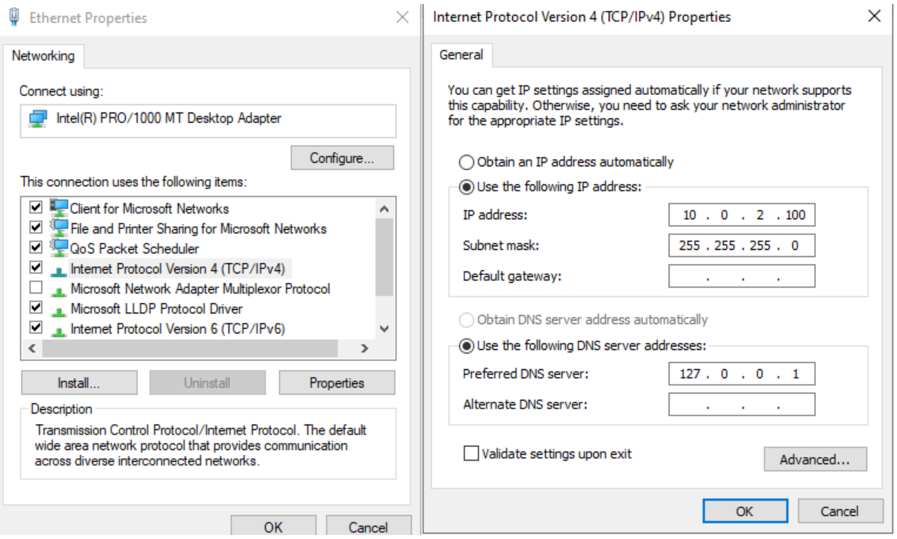
Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
Virtualization	10.0.2.0/24	fd17:625c:f037:2::/64	Enabled

Name: Virtualization
IPv4 Prefix: 10.0.2.0/24
☑ Enable DHCP
□ Enable IPv6
IPv6 Prefix: fd17:625c:f037:2::/64
□ Advertise Default IPv6 Route

- Attached Server20, PC1, and Kali to the same NAT Network.
- Verified connectivity between hosts and external DNS using ping.

3) Promote Windows Server to Domain Controller

- Configured a static IP on Server.
- Set Server DNS to localhost (127.0.0.1) prior to AD DS installation.



Connect using:
Intel(R) PRO/1000 MT Desktop Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

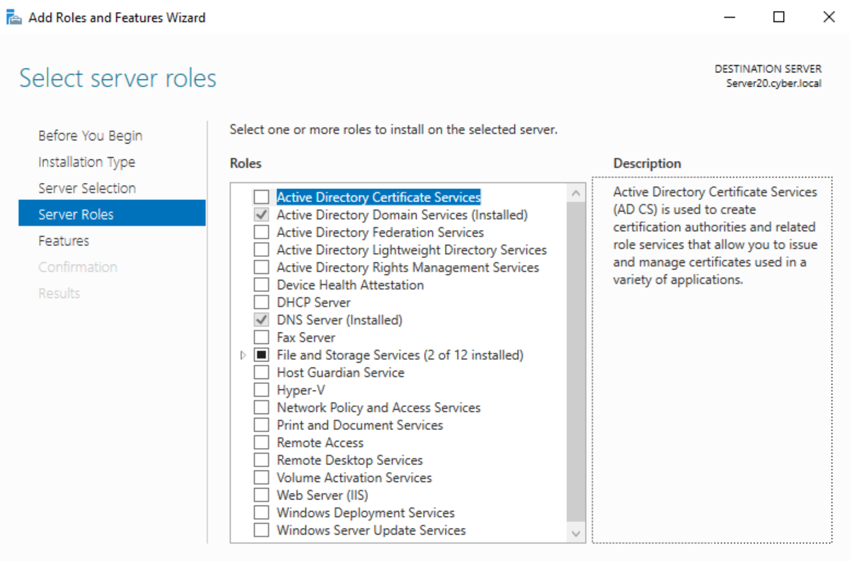
IP address: 10 . 0 . 2 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 127 . 0 . 0 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

- Installed the Active Directory Domain Services role and promoted Server to a Domain Controller.



Select server roles

DESTINATION SERVER
Server20.cyber.local

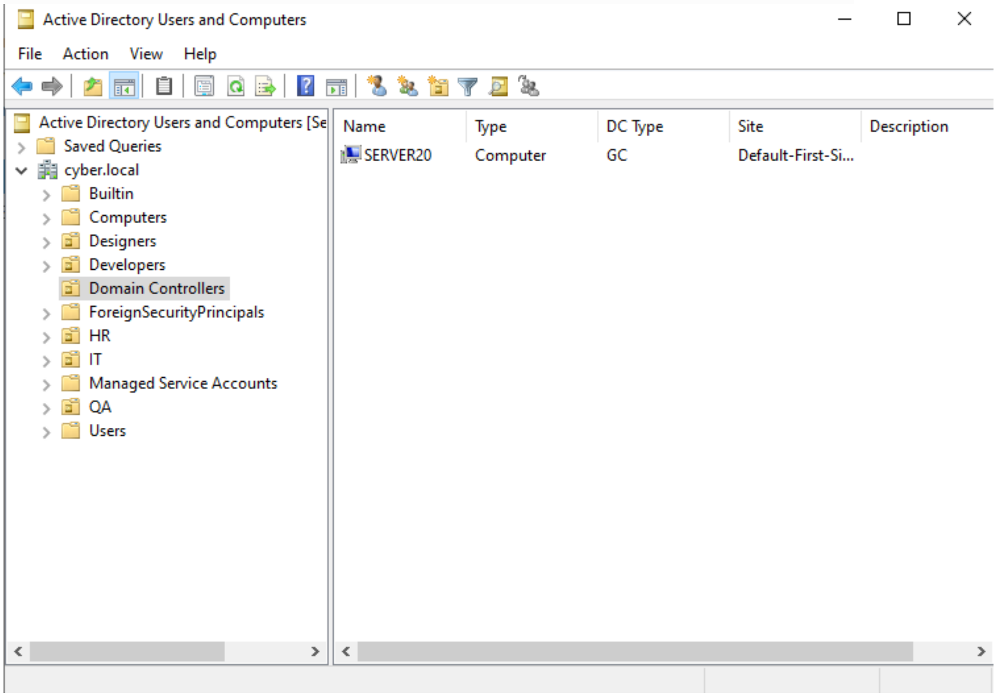
Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

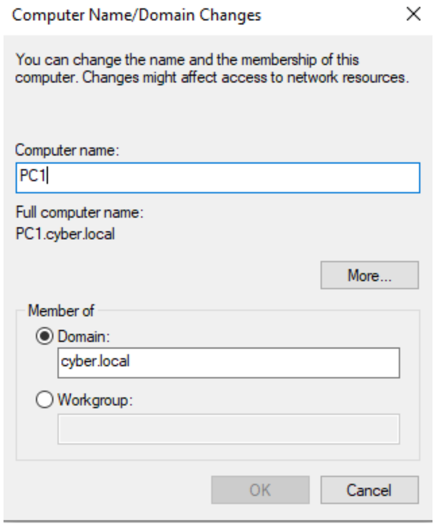


- Active Directory Users and Computers [Se
  - Saved Queries
  - cyber.local
    - Builtin
    - Computers
    - Designers
    - Developers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - HR
    - IT
    - Managed Service Accounts
    - QA
    - Users

Name	Type	DC Type	Site	Description
SERVER20	Computer	GC	Default-First-Si...	

4) Join Windows client to the domain

- Renamed the Windows client to PC1.



Computer Name/Domain Changes

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

Computer name: PC1

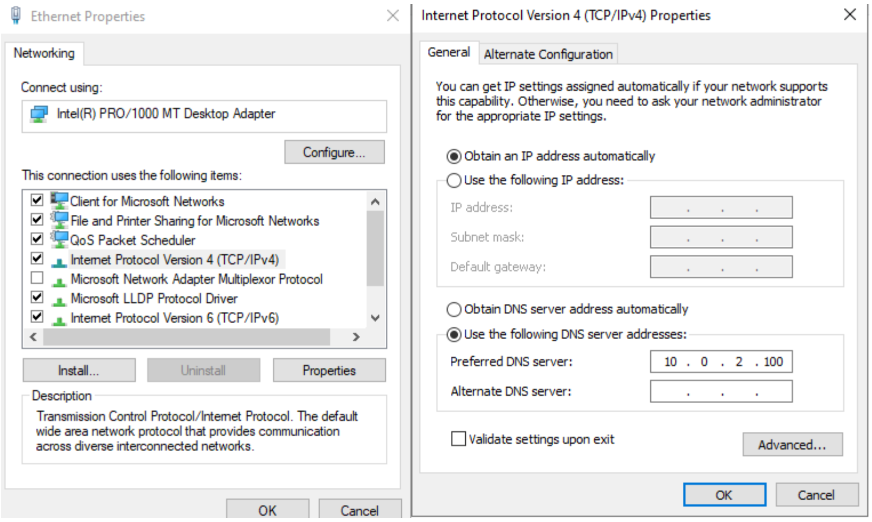
Full computer name: PC1.cyber.local

Member of

● Domain: cyber.local

○ Workgroup:

- Configured PC1 DNS to point to the Domain Controller (Server).



Ethernet Properties

Networking

Connect using: Intel(R) PRO/1000 MT Desktop Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

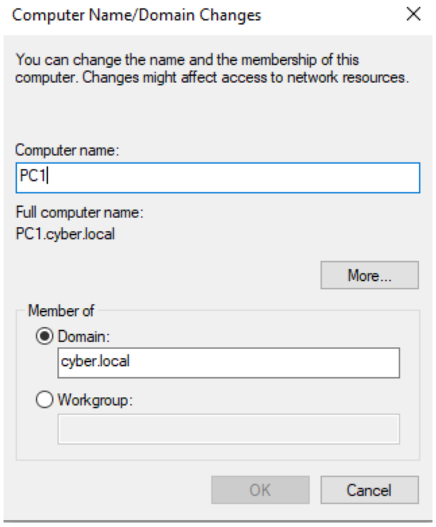
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 2 . 100
Alternate DNS server: . . .

☐ Validate settings upon exit

- Joined PC1 to the domain and validated domain logon.



Computer Name/Domain Changes

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

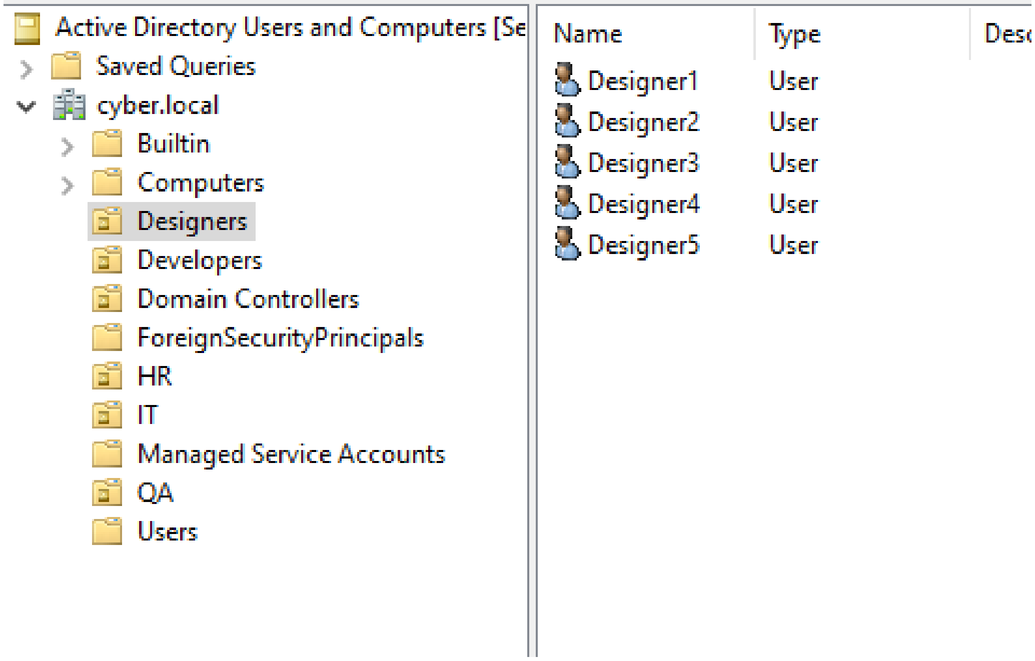
Computer name:
PC1

Full computer name:
PC1.cyber.local

Member of
● Domain:
cyber.local
○ Workgroup:

5) Identity & DNS management

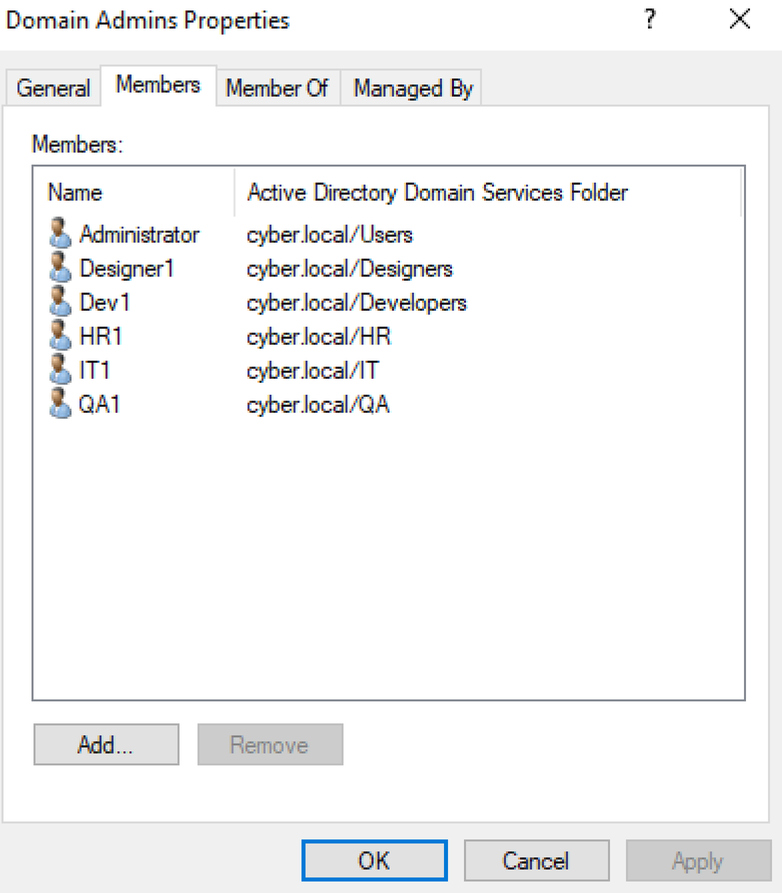
- Created OUs and users (5 users across departments).



Active Directory Users and Computers [Se
- Saved Queries
- cyber.local
  - Builtin
  - Computers
  - Designers
  - Developers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - HR
  - IT
  - Managed Service Accounts
  - QA
  - Users

Name	Type	Desc
Designer1	User	
Designer2	User	
Designer3	User	
Designer4	User	
Designer5	User	

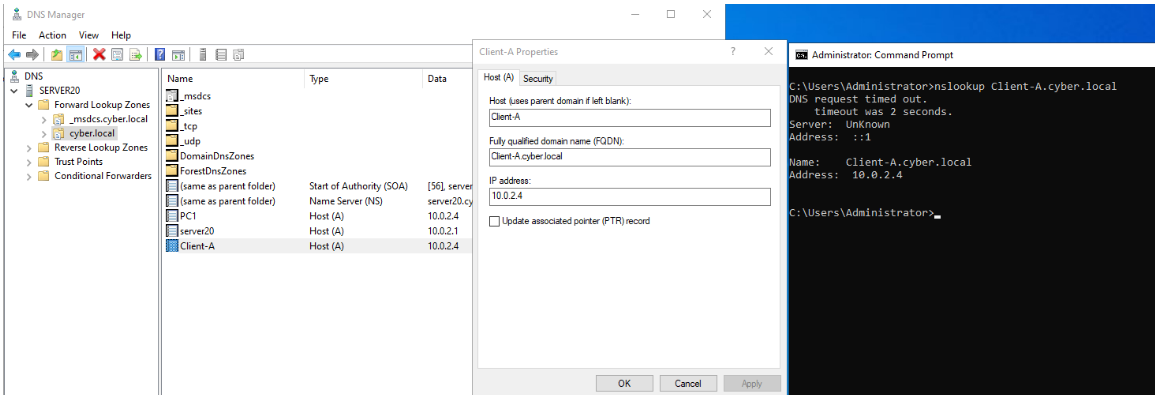
- Delegated privileges by adding one user per department to the Domain Admins group (for lab practice).



Members:

Name	Active Directory Domain Services Folder
Administrator	cyber.local/Users
Designer1	cyber.local/Designers
Dev1	cyber.local/Developers
HR1	cyber.local/HR
IT1	cyber.local/IT
QA1	cyber.local/QA

- Created a DNS record for the Windows 10 client named Client-A.



Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[56], server
(same as parent folder)	Name Server (NS)	server20.cy
PC1	Host (A)	10.0.2.4
server20	Host (A)	10.0.2.1
Client-A	Host (A)	10.0.2.4

Host (uses parent domain if left blank): Client-A

Fully qualified domain name (FQDN): Client-A.cyber.local

IP address: 10.0.2.4

□ Update associated pointer (PTR) record

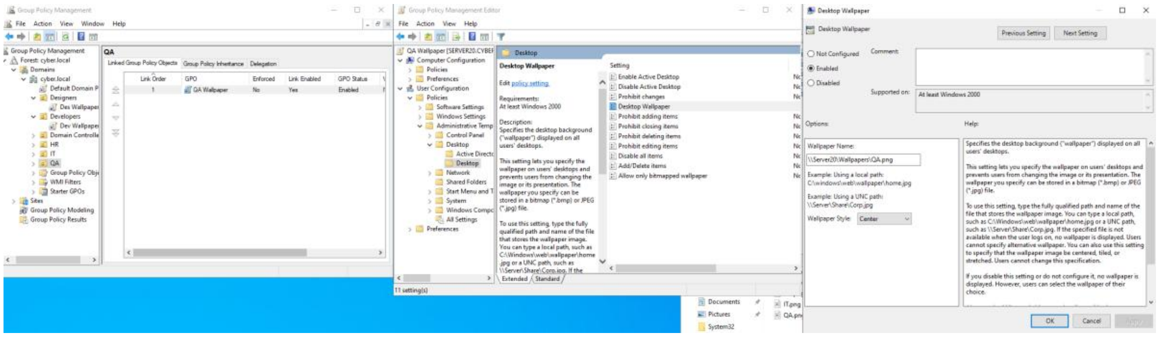
```
C:\Users\Administrator>nslookup Client-A.cyber.local
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    Client-A.cyber.local
Address:  10.0.2.4


C:\Users\Administrator>_
```

6) Security controls (GPO + access control)

- Created per-department policies including wallpaper assignment.



Link Order	GPO	Enforced	Link Enabled	GPO Status
1	QA Wallpaper	No	Yes	Enabled

Desktop Wallpaper

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

Wallpaper Name: \\Server20\Wallpapers\QA.png

Example: Using a local path: C:\windows\web\wallpaper\home.jpg

Example: Using a UNC path: \\Server\Share\Corp.jpg

Wallpaper Style: Center

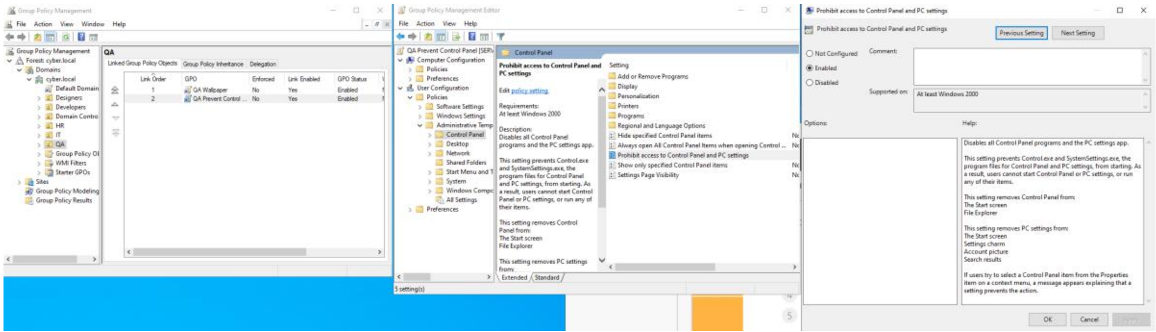
Specifies the desktop background ("wallpaper") displayed on all users' desktops.

This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.

To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home.jpg or a UNC path, such as \\Server\Share\Corp.jpg. If the specified file is not available when the user logs on, no wallpaper is displayed. Users cannot specify alternative wallpaper. You can also use this setting to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification.

If you disable this setting or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice.

- Blocked Control Panel access for QA; blocked CMD for HR.



Link Order	GPO	Enforced	Link Enabled	GPO Status
1	QA Wallpaper	No	Yes	Enabled
2	QA Prevent Control ...	No	Yes	Enabled

Prohibit access to Control Panel and PC settings

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

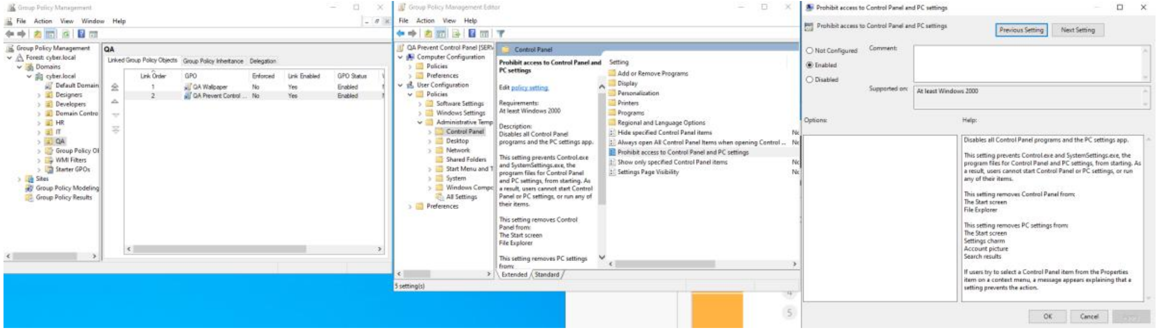
Disables all Control Panel programs and the PC settings app.

This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:
The Start screen
File Explorer

This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.



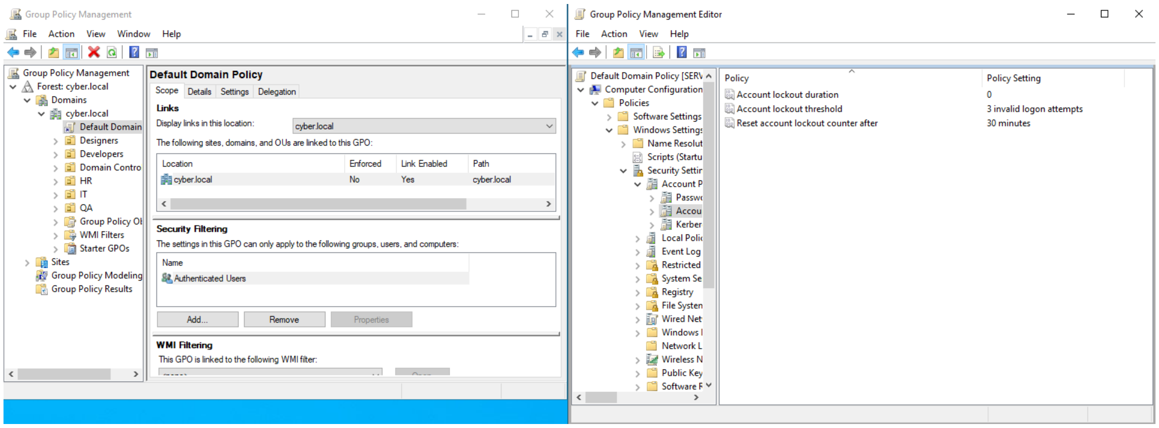
Link Order	GPO	Enforced	Link Enabled	GPO Status
1	QA Wallpaper	No	Yes	Enabled
2	QA Prevent Control ...	No	Yes	Enabled

Prohibit access to Control Panel and PC settings

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

- Configured account lockout after 3 failed logon attempts; only an administrator can unlock accounts.



Default Domain Policy

Links

Display links in this location: cyber.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
cyber.local	No	Yes	cyber.local

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

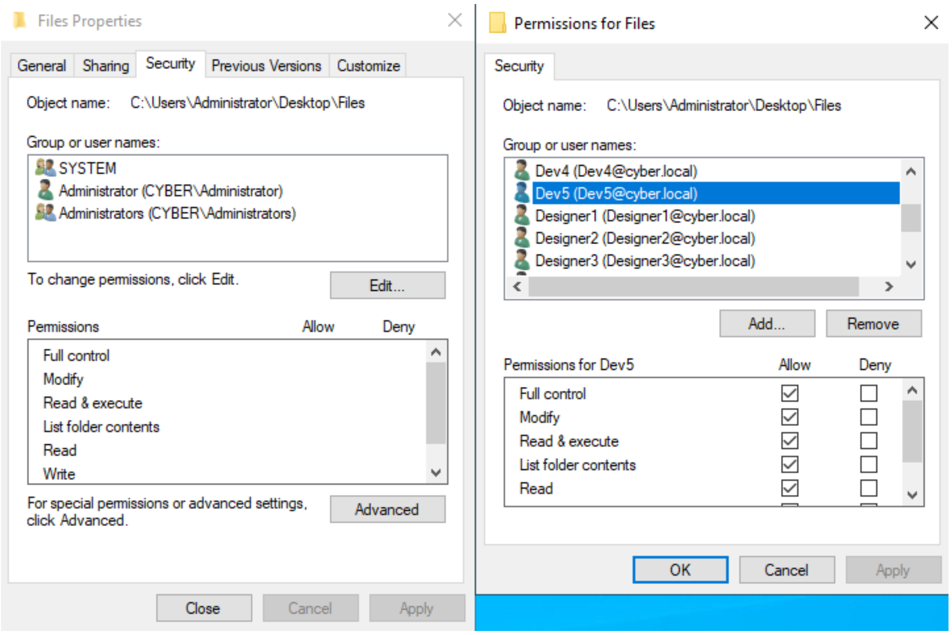
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

Policy	Policy Setting
Account lockout duration	0
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

- Created a shared Files folder and restricted access to Designers and Developers only.



Object name: C:\Users\Administrator\Desktop\Files

Group or user names:

SYSTEM
Administrator (CYBER\Administrator)
Administrators (CYBER\Administrators)

To change permissions, click Edit.

Permissions	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

For special permissions or advanced settings, click Advanced.

Object name: C:\Users\Administrator\Desktop\Files

Group or user names:

Dev4 (Dev4@cyber.local)
Dev5 (Dev5@cyber.local)
Designer1 (Designer1@cyber.local)
Designer2 (Designer2@cyber.local)
Designer3 (Designer3@cyber.local)

Permissions for Dev5	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□