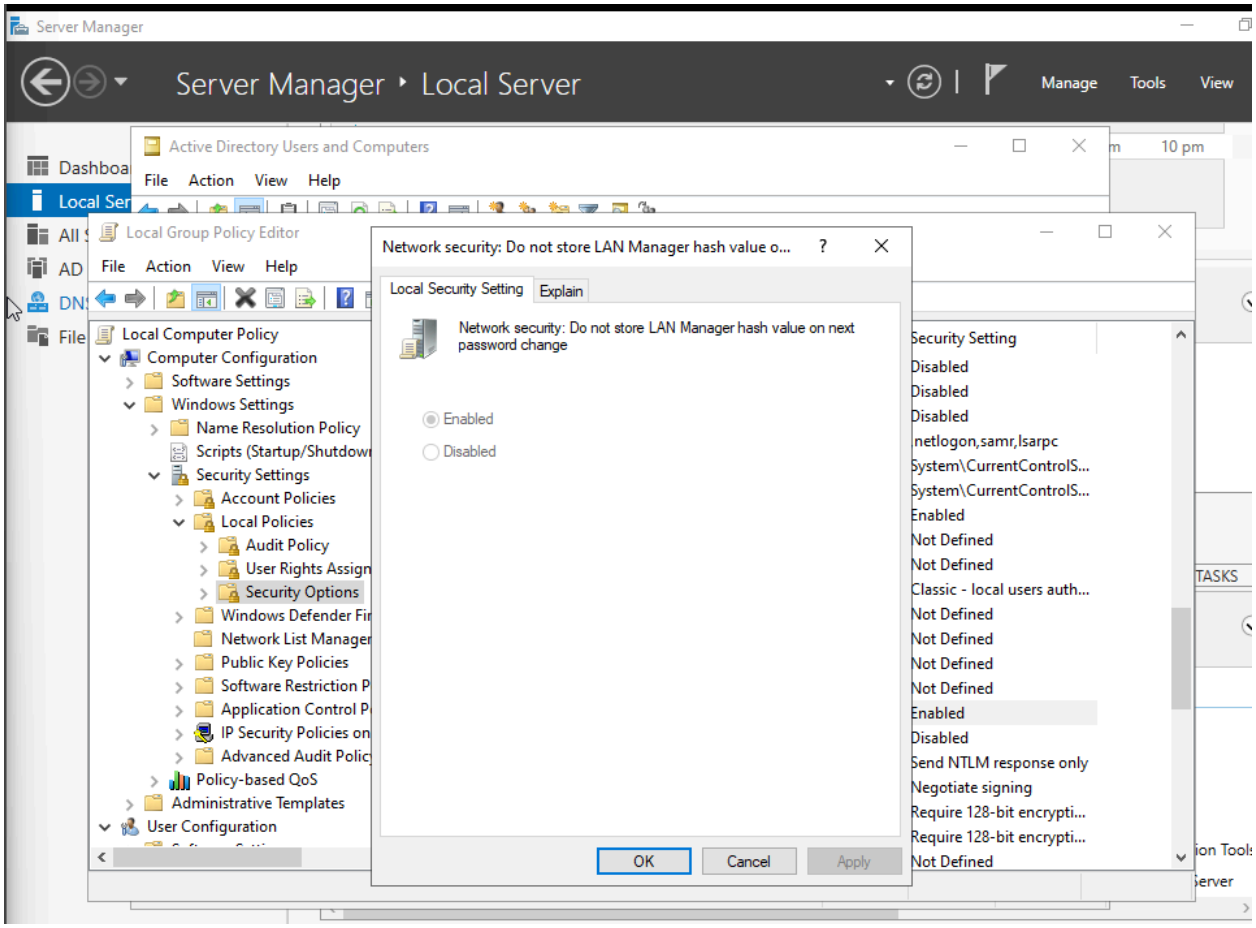
Domain controller

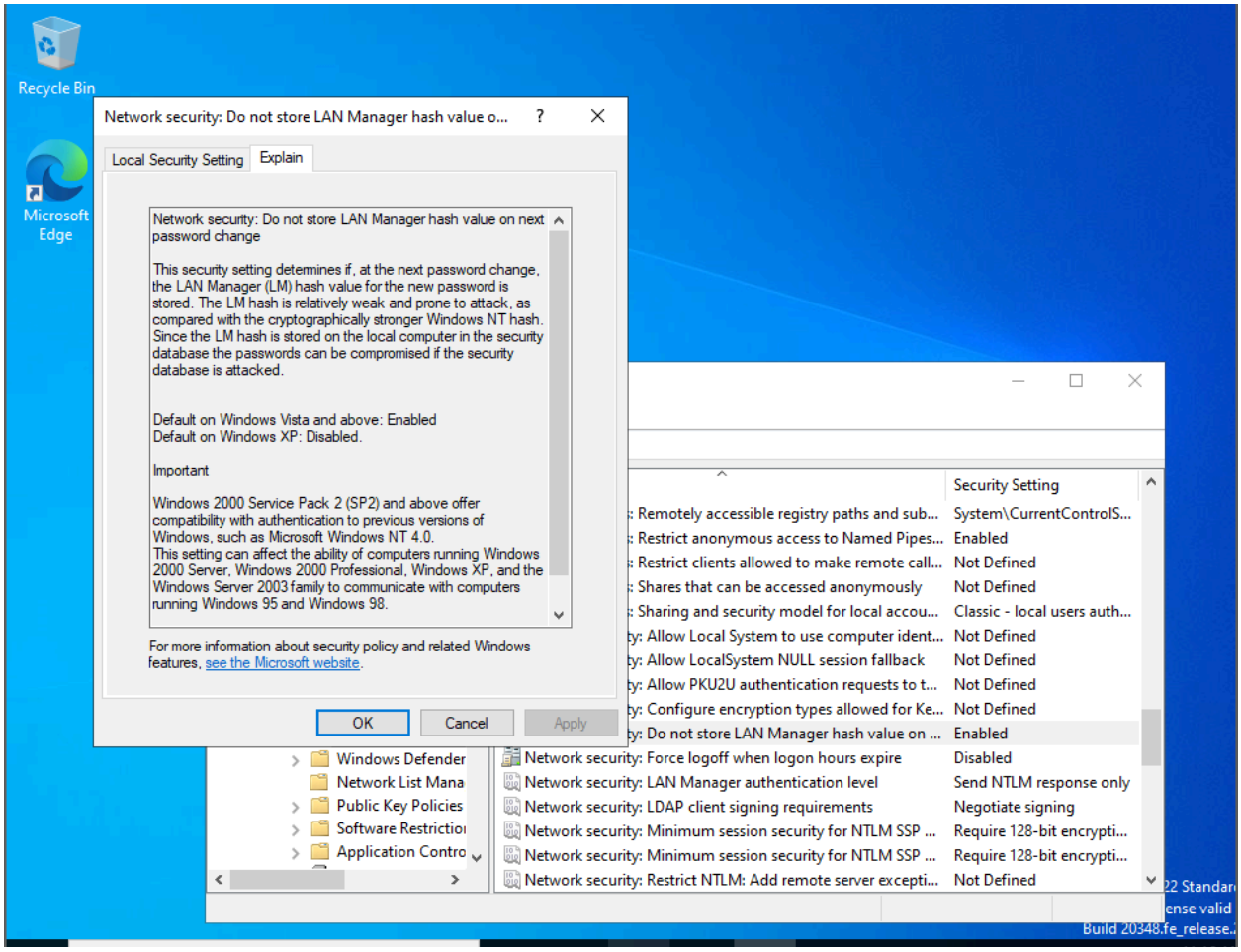
Securing authentication methods

Configuring LAN Manager hash function

Don’t allow storing LAN manager hash value on the next password change
Reasons: LM hash is weak – comparing to Windows NT hash and prone to attack

In group policy management editor > computer configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Network Security: Do not store LAN Manager hash value on next password change policy > select “Define policy setting” > Enabled

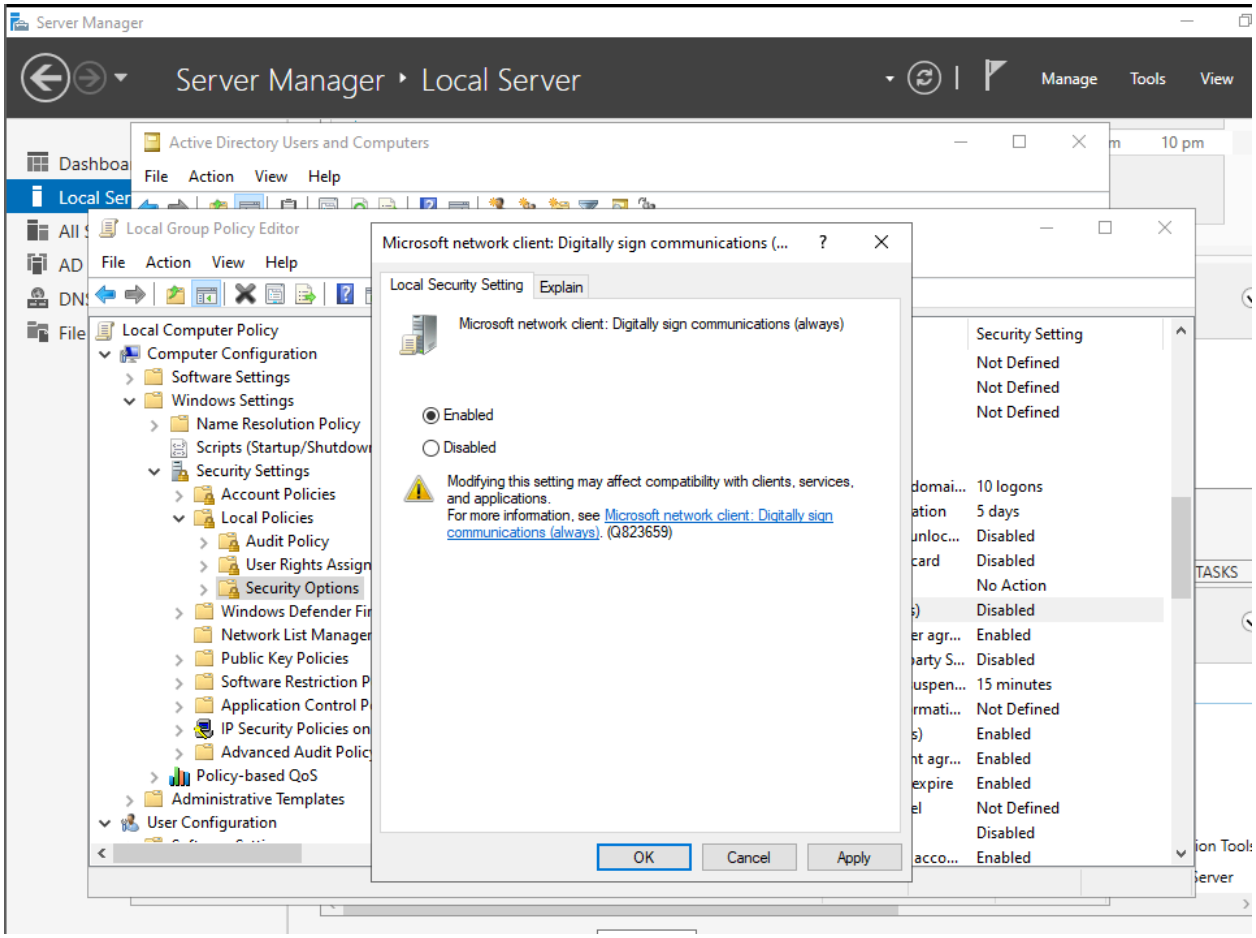

Server Manager
Server Manager ‣ Local Server
Manage
Tools
View
Active Directory Users and Computers
File Action View Help
Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdow
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assign
Security Options
Windows Defender Fir
Network List Manager
Public Key Policies
Software Restriction P
Application Control P
IP Security Policies on
Advanced Audit Polic
Policy-based QoS
Administrative Templates
User Configuration
Network security: Do not store LAN Manager hash value o...
Local Security Setting
Explain
Network security: Do not store LAN Manager hash value on next password change
Enabled
Disabled
OK
Cancel
Apply
Security Setting
Disabled
Disabled
Disabled
netlogon,samr,lsarpc
System\CurrentControlS...
System\CurrentControlS...
Enabled
Not Defined
Not Defined
Classic - local users auth...
Not Defined
Not Defined
Not Defined
Not Defined
Enabled
Disabled
Send NTLM response only
Negotiate signing
Require 128-bit encrypti...
Require 128-bit encrypti...
Not Defined
10 pm
TASKS



SMB Signing

Smb : server message block, used for file and print communication; allows secure transmission over the network. SMB signing ensures the integrity of data for both client and server, protecting against Man in the Middle (MiTM) attack.

Open Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Microsoft network server: Digitally sign communication (always) > select Enable Digitally Sign Communications

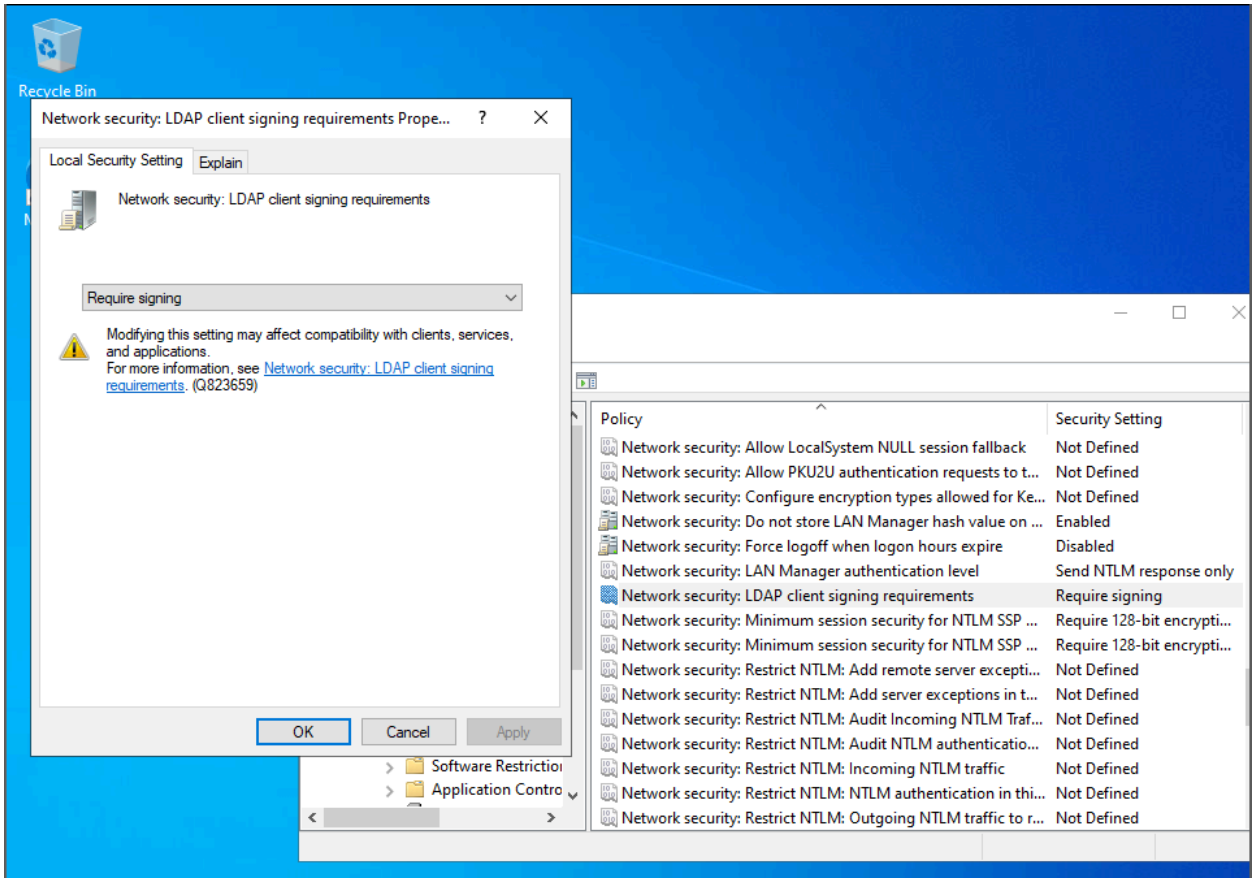


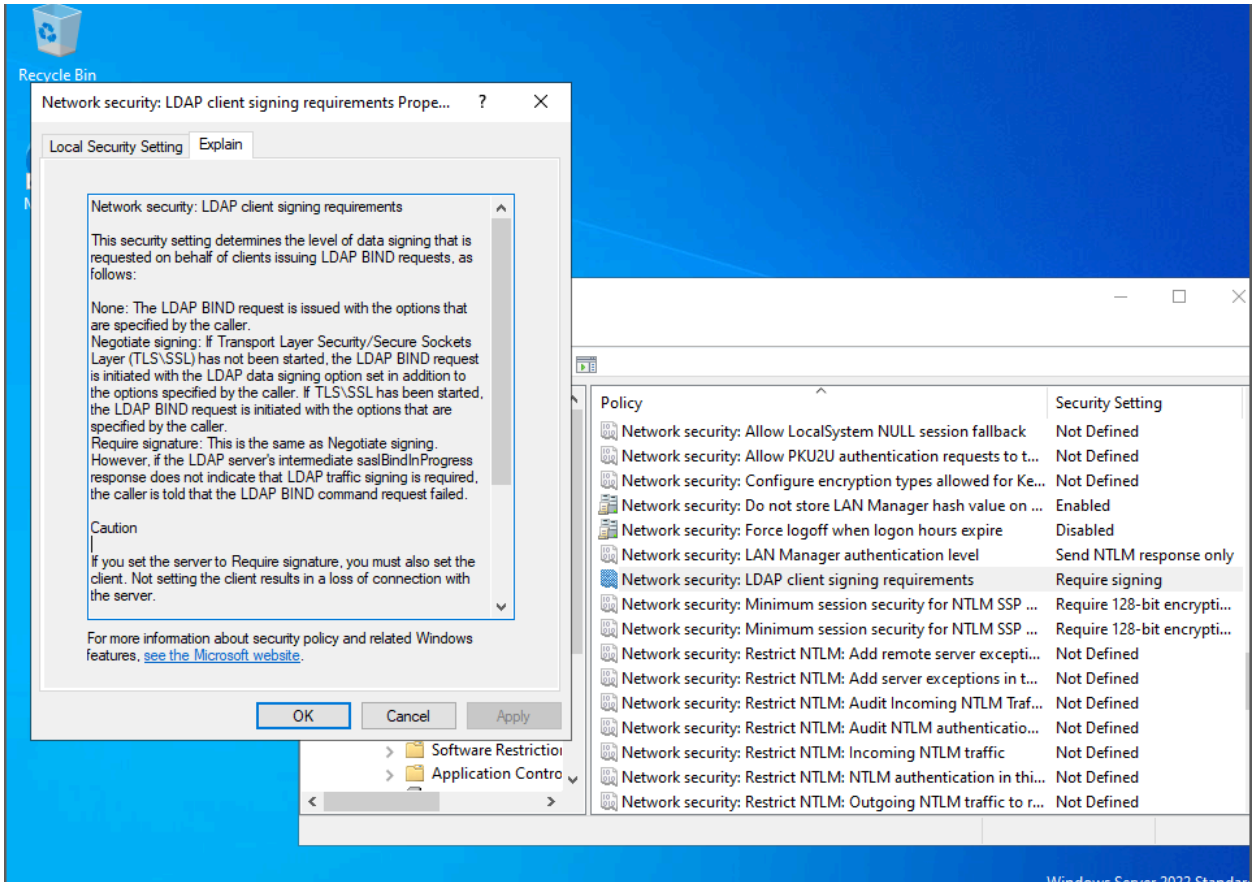
Enable smb to prevent mitm attack

Limit LDAP access

LDAP: Lightweight Directory Access Protocol, enables locating and authentication
Reasons: prevent MiTM attacks via custom LDAP requests.
Action: we need to enable LDAP signing on both server and client sides.
This is LDAP signing enabling for client side

Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Domain controller: LDAP server signing requirements > select Require signing from the dropdown


Recycle Bin
Network security: LDAP client signing requirements Prope...
Local Security Setting
Explain
Network security: LDAP client signing requirements
Require signing
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: LDAP client signing requirements. (Q823659)
OK
Cancel
Apply
Software Restrictio
Application Contro
Policy
Security Setting
Network security: Allow LocalSystem NULL session fallback
Not Defined
Network security: Allow PKU2U authentication requests to t...
Not Defined
Network security: Configure encryption types allowed for Ke...
Not Defined
Network security: Do not store LAN Manager hash value on ...
Enabled
Network security: Force logoff when logon hours expire
Disabled
Network security: LAN Manager authentication level
Send NTLM response only
Network security: LDAP client signing requirements
Require signing
Network security: Minimum session security for NTLM SSP ...
Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP ...
Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...
Not Defined
Network security: Restrict NTLM: Add server exceptions in t...
Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traf...
Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...
Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic
Not Defined
Network security: Restrict NTLM: NTLM authentication in thi...
Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to r...
Not Defined



We need to enable LDAP signing for the server side in *Domain Controller: LDAP server signing requirements*

LDAP signing for domain controller using the Microsoft guide:

How to configure the directory to require LDAP server signing for AD DS

For information about possible affects of changing security settings, see Client, service, and program issues can occur if you change security settings and user rights assignments.

Using Group Policy

How to set the server LDAP signing requirement

1. Select Start > Run, type *mmc.exe*, and then select OK.
2. Select File > Add/Remove Snap-in, select Group Policy Management Editor, and then select Add.
3. Select Group Policy Object > Browse.
4. In the Browse for a Group Policy Object dialog box, select Default Domain Controller Policy under the Domains, OUs, and linked Group Policy Objects area, and then select OK.
5. Select Finish.
6. Select OK.
7. Select Default Domain Controller Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies, and then select Security Options.
8. Right-click Domain controller: LDAP server signing requirements, and then select Properties.
9. In the Domain controller: LDAP server signing requirements Properties dialog box, enable Define this policy setting, select Require signing in the Define this policy setting list, and then select OK.
10. In the Confirm Setting Change dialog box, select Yes.

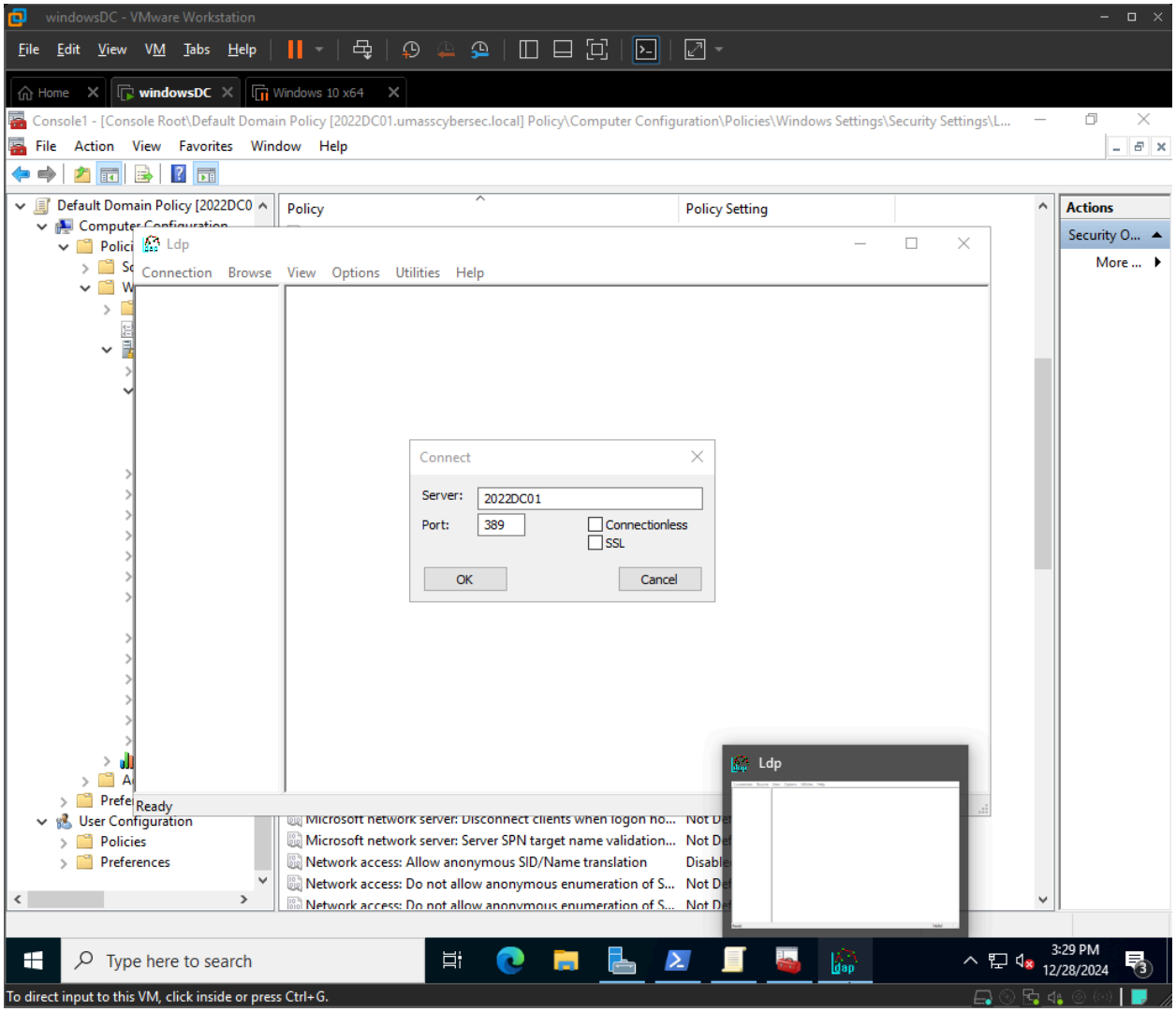
How to set the client LDAP signing requirement by using local computer policy

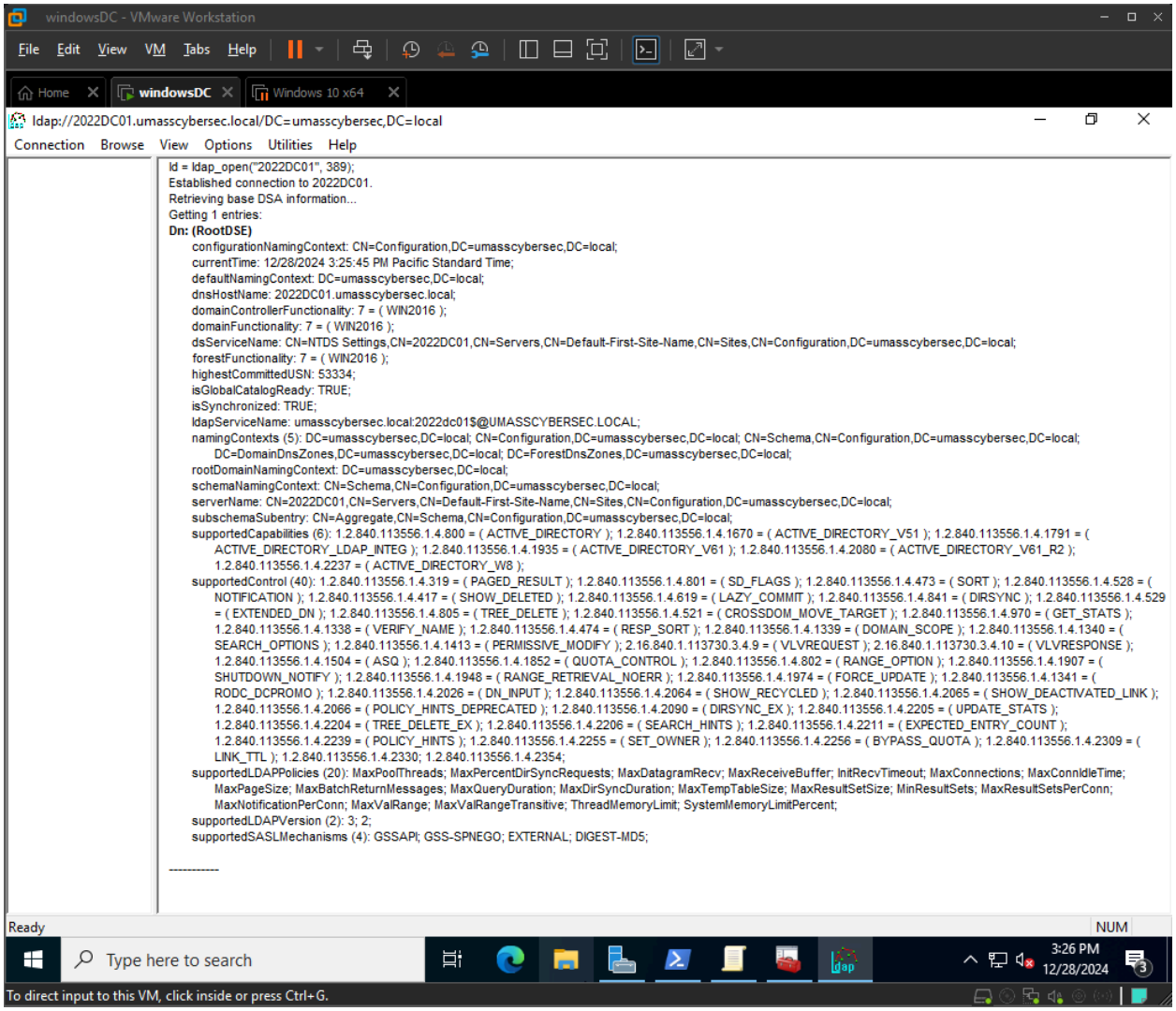
1. Select Start > Run, type *mmc.exe*, and then select OK.
2. Select File > Add/Remove Snap-in.
3. In the Add or Remove Snap-ins dialog box, select Group Policy Object Editor, and then select Add.
4. Select Finish.
5. Select OK.
6. Select Local Computer Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies, and then select Security Options.
7. Right-click Network security: LDAP client signing requirements, and then select Properties.
8. In the Network security: LDAP client signing requirements Properties dialog box, select Require signing in the list, and then select OK.
9. In the Confirm Setting Change dialog box, select Yes.

Source

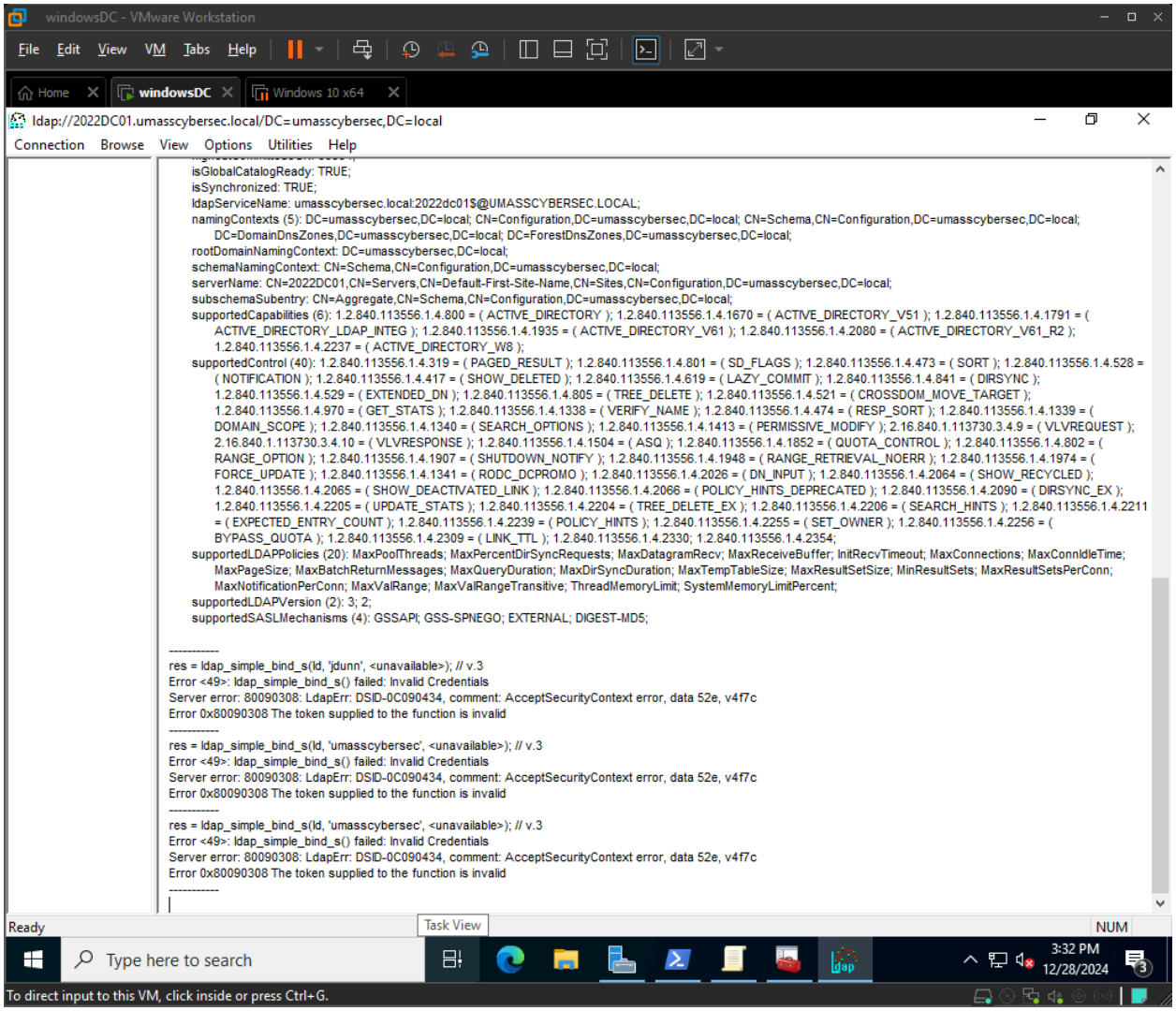
Verify LDAP signing enabling [source]

Get hostname in cmd: 2022DC01
In Start > ldp.exe > Connection > Connect

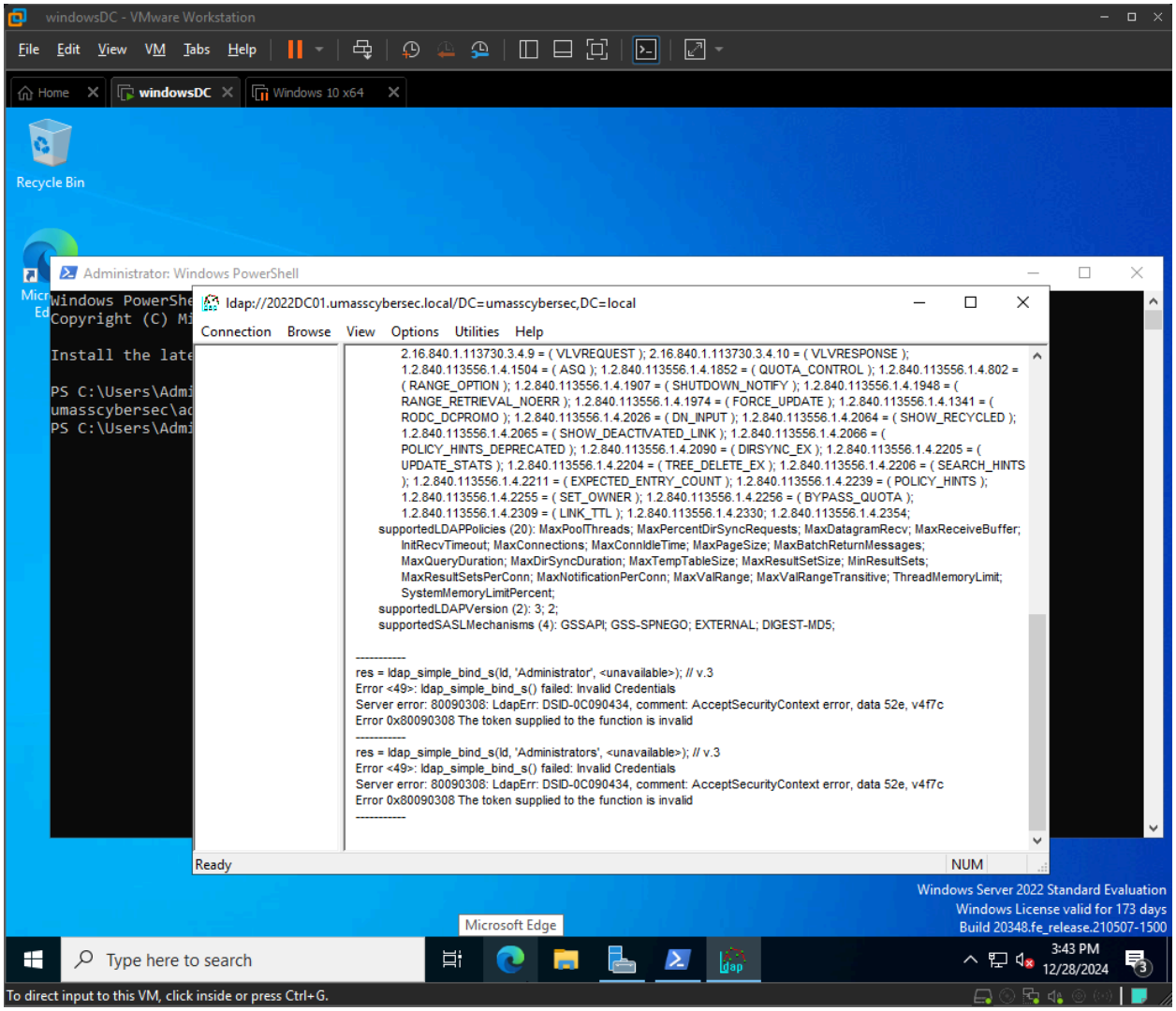




Attempted to bind:

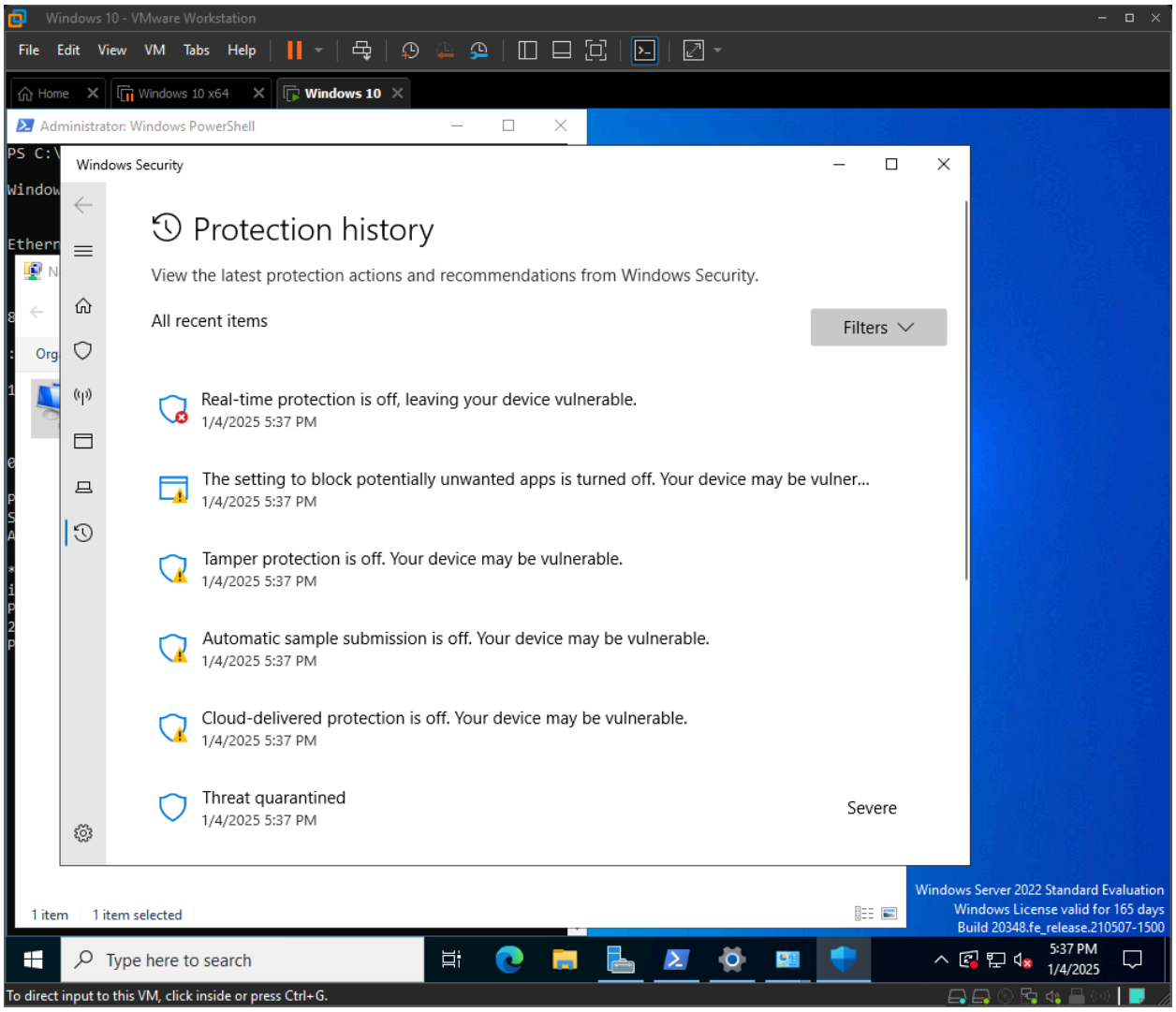


Unfortunately, when tried to bind with account that has username “umasscybersec” and password “1234567cybersec”, there is an error of invalid credentials. This shows up because of invalid passwords. But after multiple attempts with the correct credentials, I still don’t know why this happened.

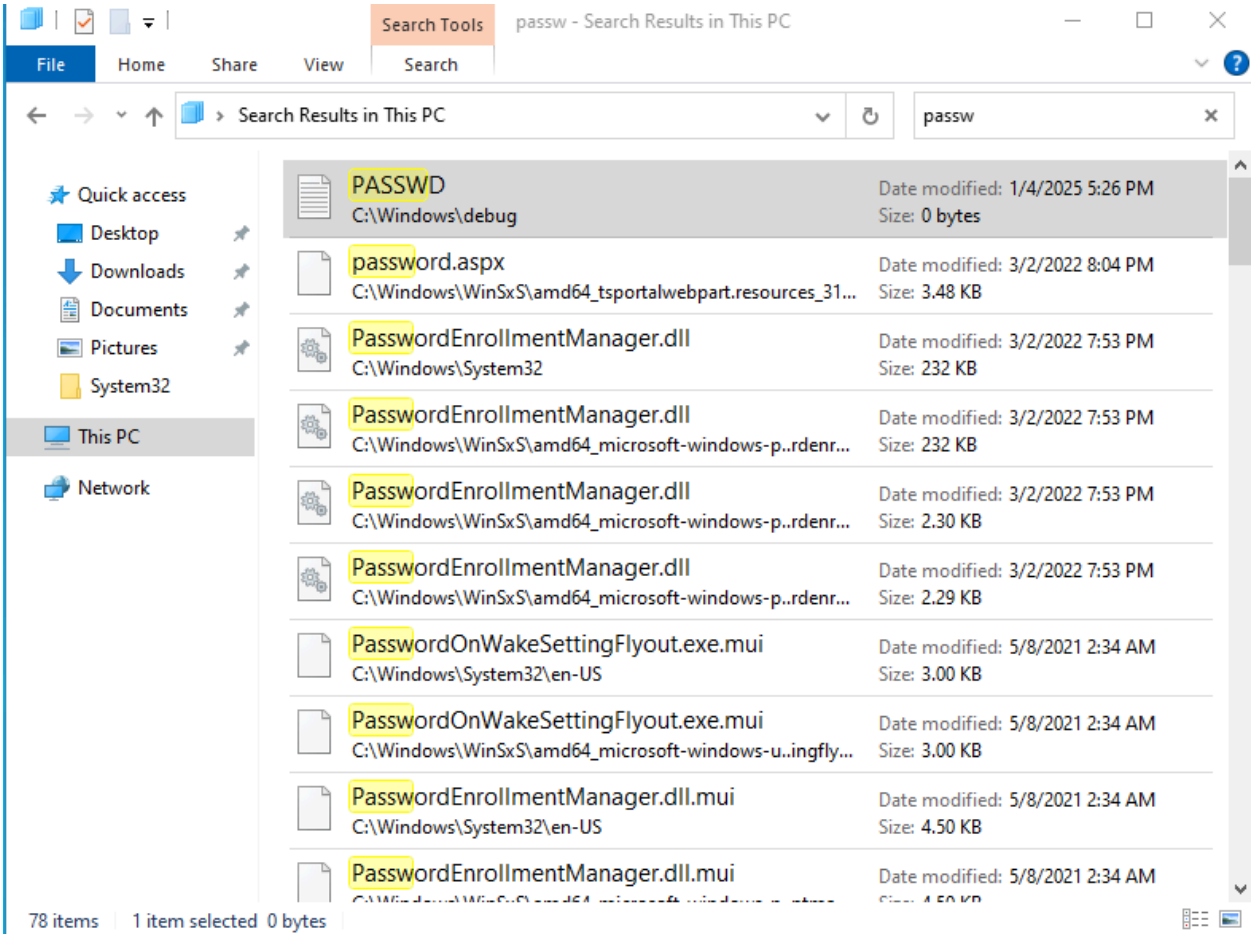


Realized that the user is Administrator. Even then, can't seem to bind.

Checking windows security

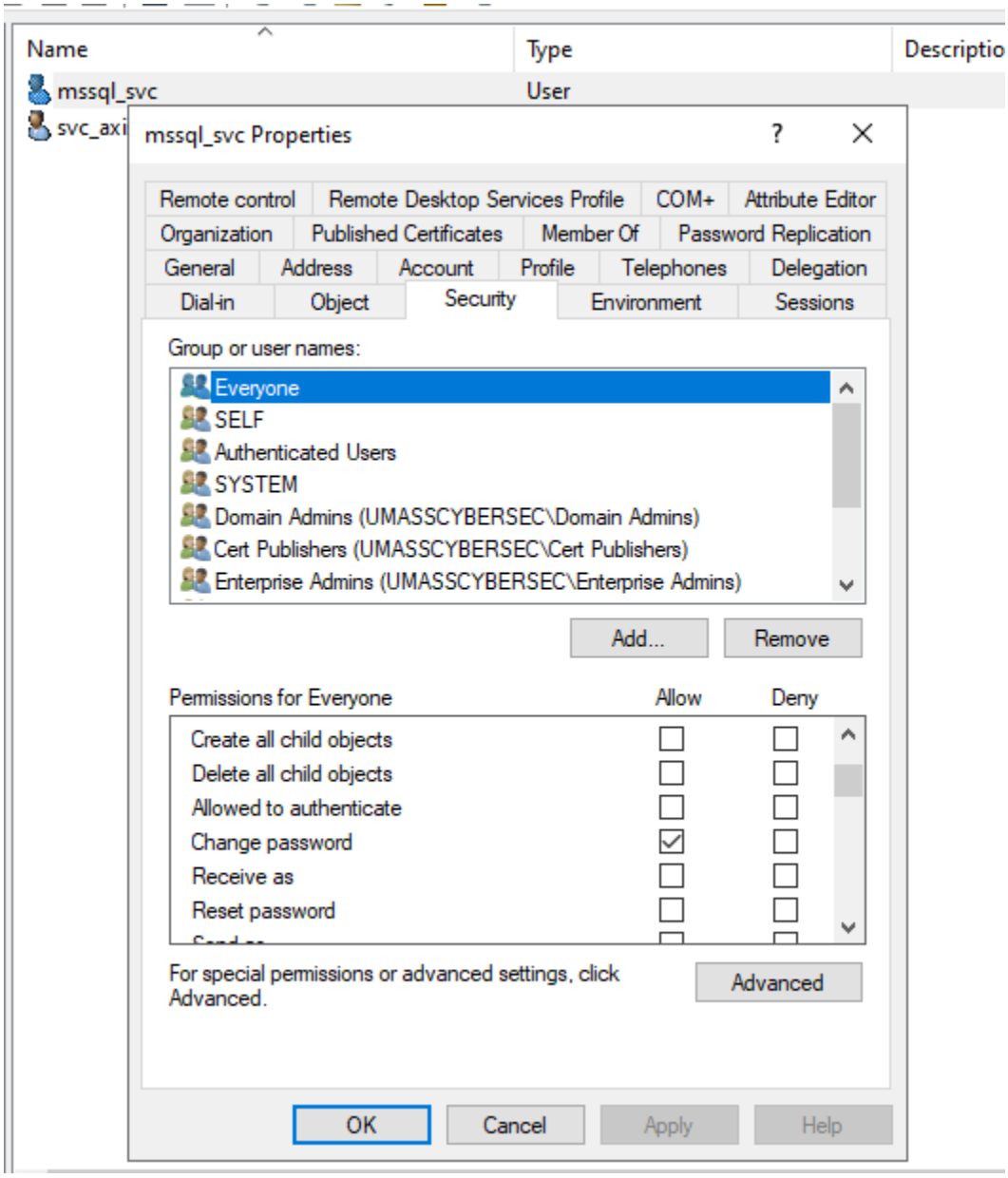


Solution: turned on protection for every warning



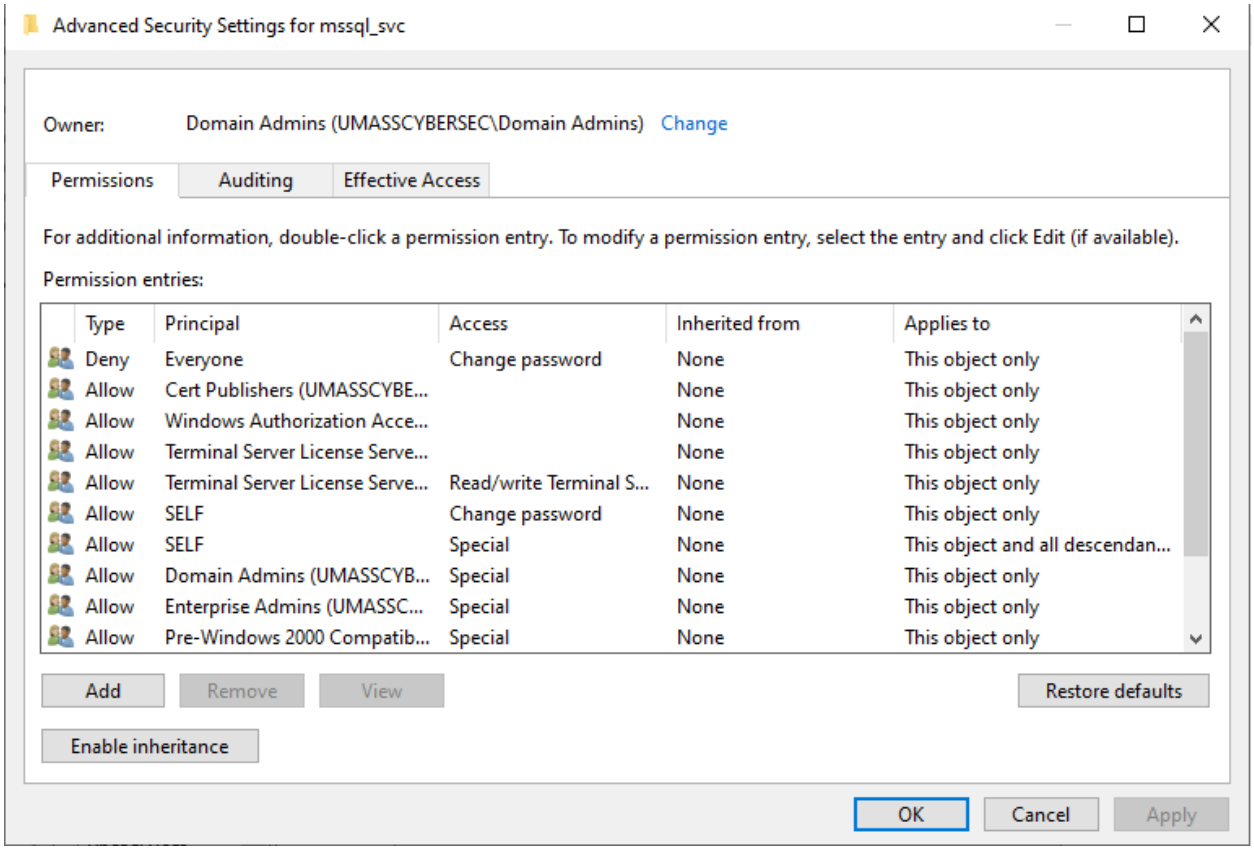
Verified that passwords are not stored in obvious or insecure locations.

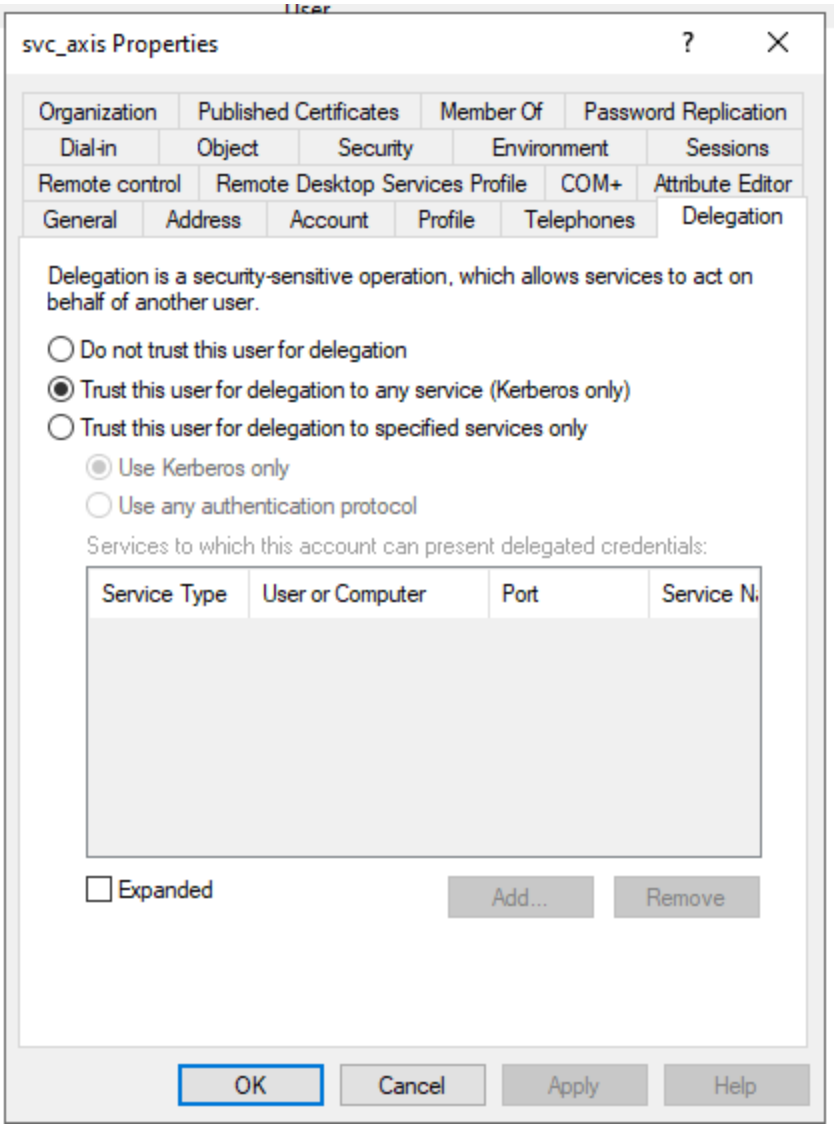
In service accounts:



→ Fix: disable everyone's permission over change password.
But this service account is a member of Everyone group. If we disable the permission to change password for this account, meaning that this account can't change its password.

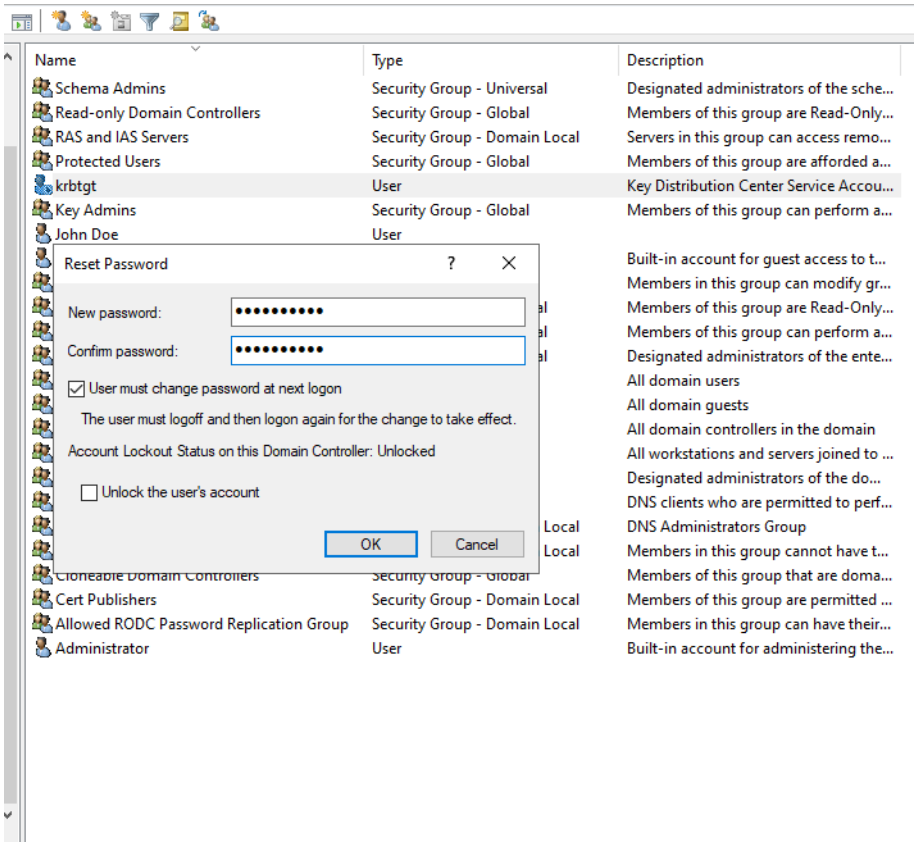
Deny permissions take precedence over Allow permissions, but explicit permissions granted to the service account still apply because they are specific to the account and not inherited from the Everyone group. So, by explicitly granting the Change Password permission to the service account itself, it can still update its own password when needed.

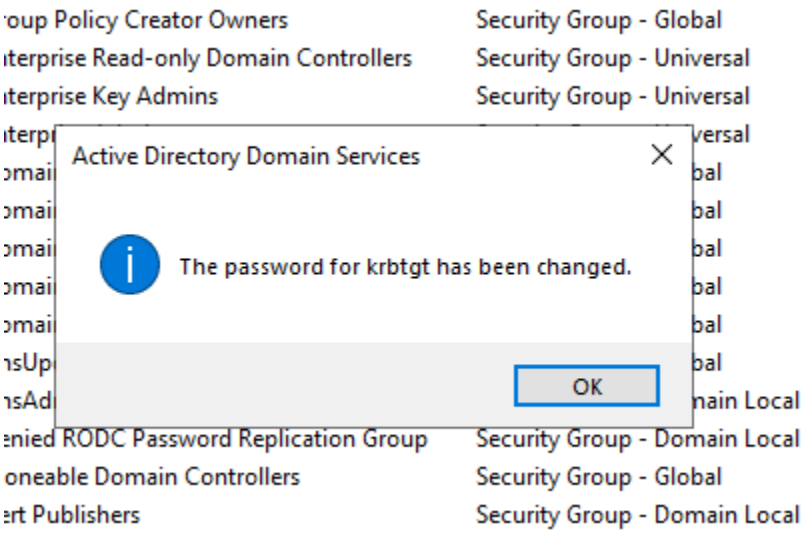

Advanced Security Settings for mssql_svc
Owner: Domain Admins (UMASSCYBERSEC\Domain Admins) Change
Permissions
Auditing
Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type
Principal
Access
Inherited from
Applies to
Deny Everyone Change password None This object only
Allow Cert Publishers (UMASSCYBE... None This object only
Allow Windows Authorization Acce... None This object only
Allow Terminal Server License Serve... None This object only
Allow Terminal Server License Serve... Read/write Terminal S... None This object only
Allow SELF Change password None This object only
Allow SELF Special None This object and all descendan...
Allow Domain Admins (UMASSCYB... Special None This object only
Allow Enterprise Admins (UMASSC... Special None This object only
Allow Pre-Windows 2000 Compatib... Special None This object only
Add
Remove
View
Restore defaults
Enable inheritance
OK
Cancel
Apply



Krbtgt password reset

If a hacker gains access to the krbtgt account, they can forge kerberos tickets, aka golden tickets, to gain unauthorized access to the domain. Resetting the krbtgt password invalidates all active kerberos tickets, forcing users and services to reauthenticate.



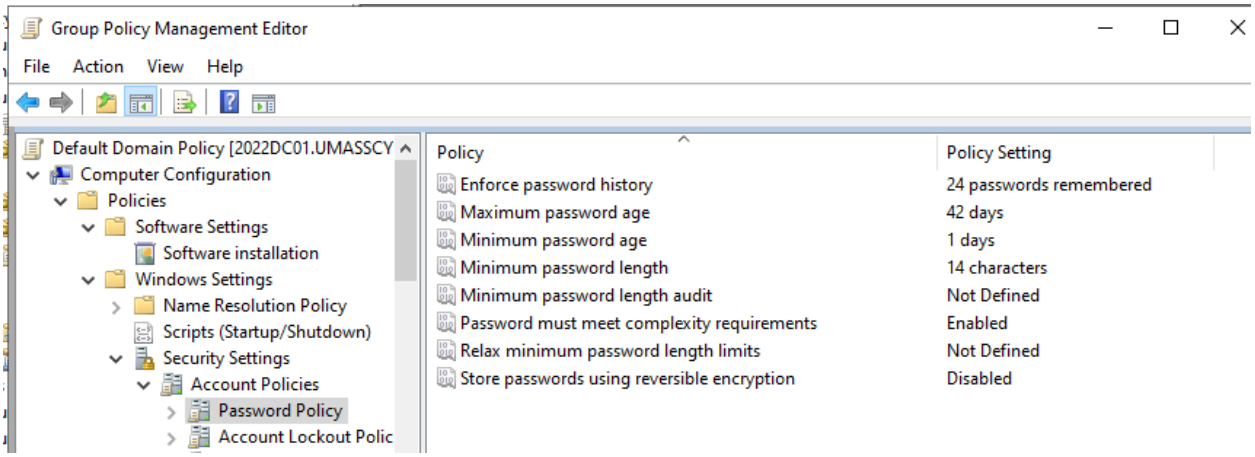


***Note:** Only after doing this did I realize I shouldn't reset the krbtgt password as it may disrupt authentication services if not handled properly.
Used Search-ADAccount -AccountDisabled cmdlet to identify disabled accounts in Active Directory. Confirmed that only krbtgt is disabled, as expected. Keeping the krbtgt disabled ensures that attackers cannot interact with or authenticate as this account directly. And this

account should never be enabled in normal circumstances.

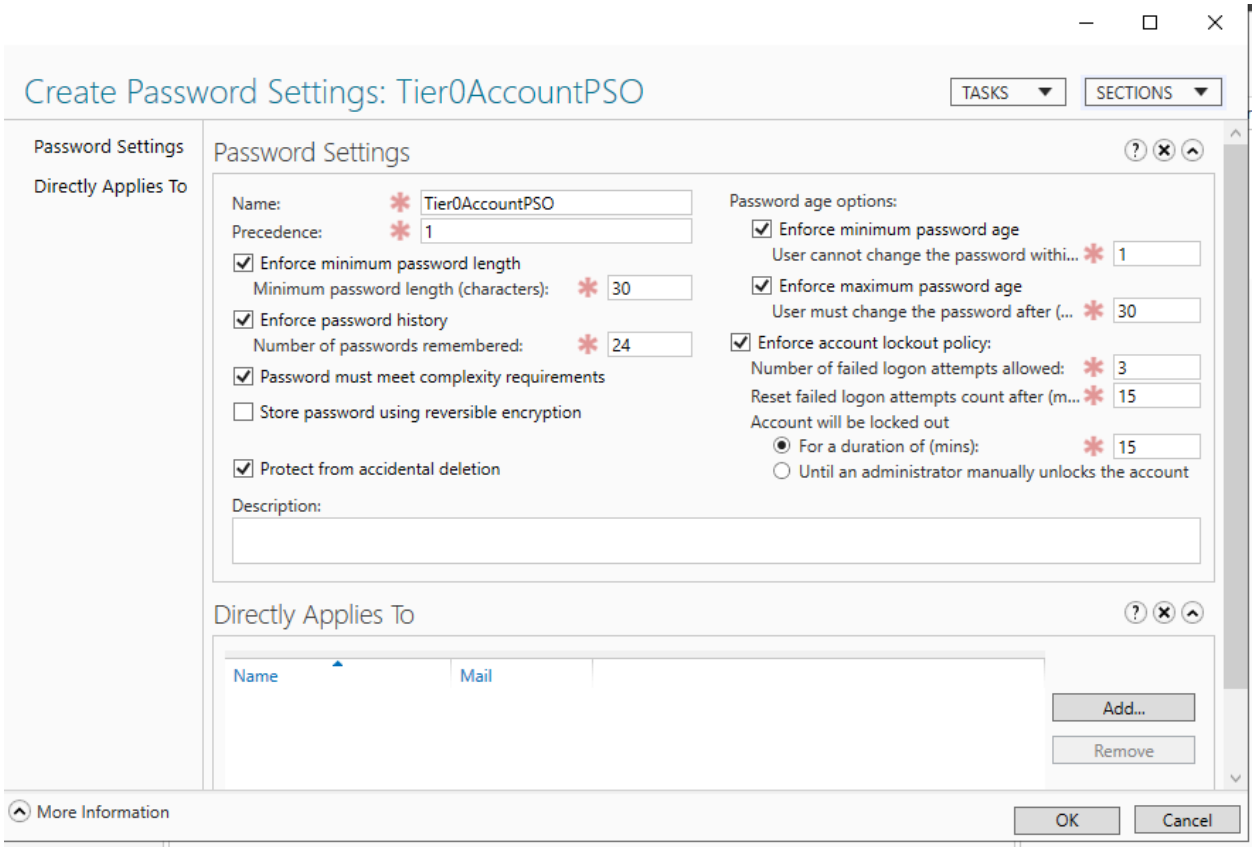
```
PS C:\Users\Administrator> search-adaccount -usersonly -accountdisabled


AccountExpirationDate :
DistinguishedName     : CN=krbtgt,CN=Users,DC=umasscybersec,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : krbtgt
ObjectClass           : user
ObjectGUID            : 8a9434f6-03b6-4ded-aef4-8f6c803650f9
PasswordExpired       : False
PasswordNeverExpires  : False
SamAccountName        : krbtgt
SID                   : S-1-5-21-907977273-330564314-3450818407-502
UserPrincipalName     :
```

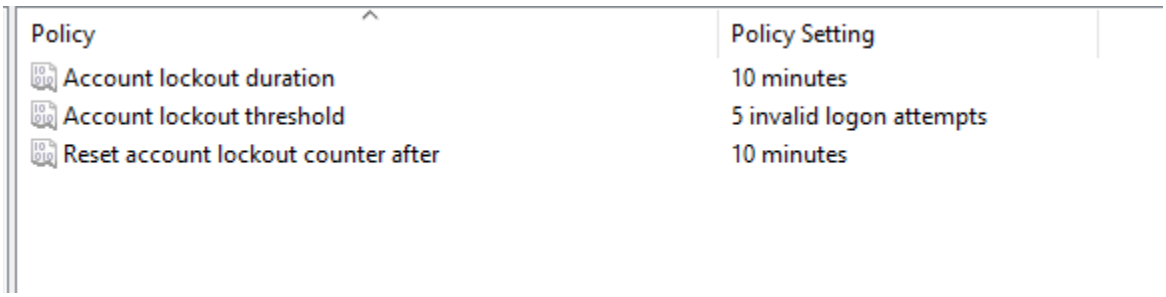
Policy Updates

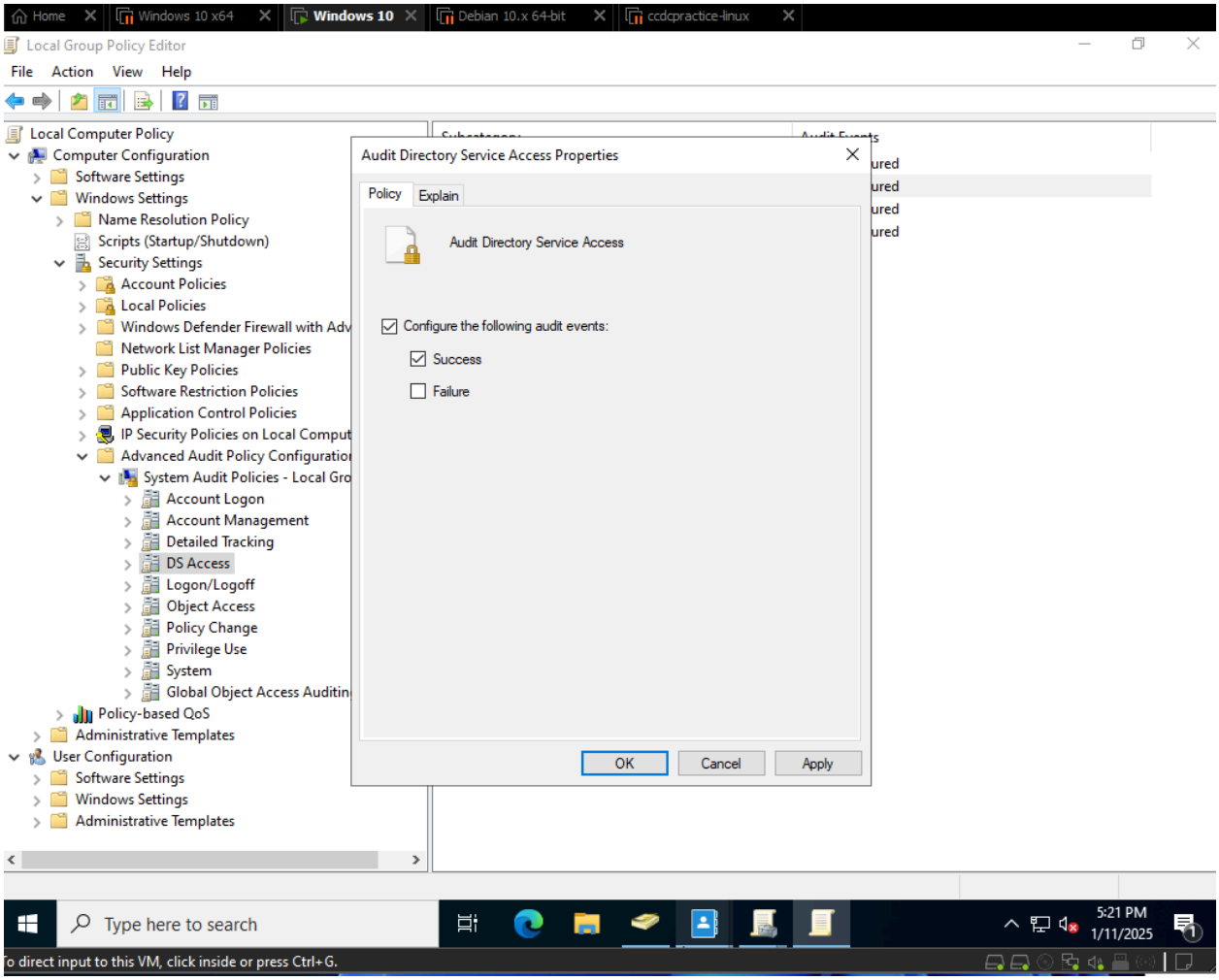


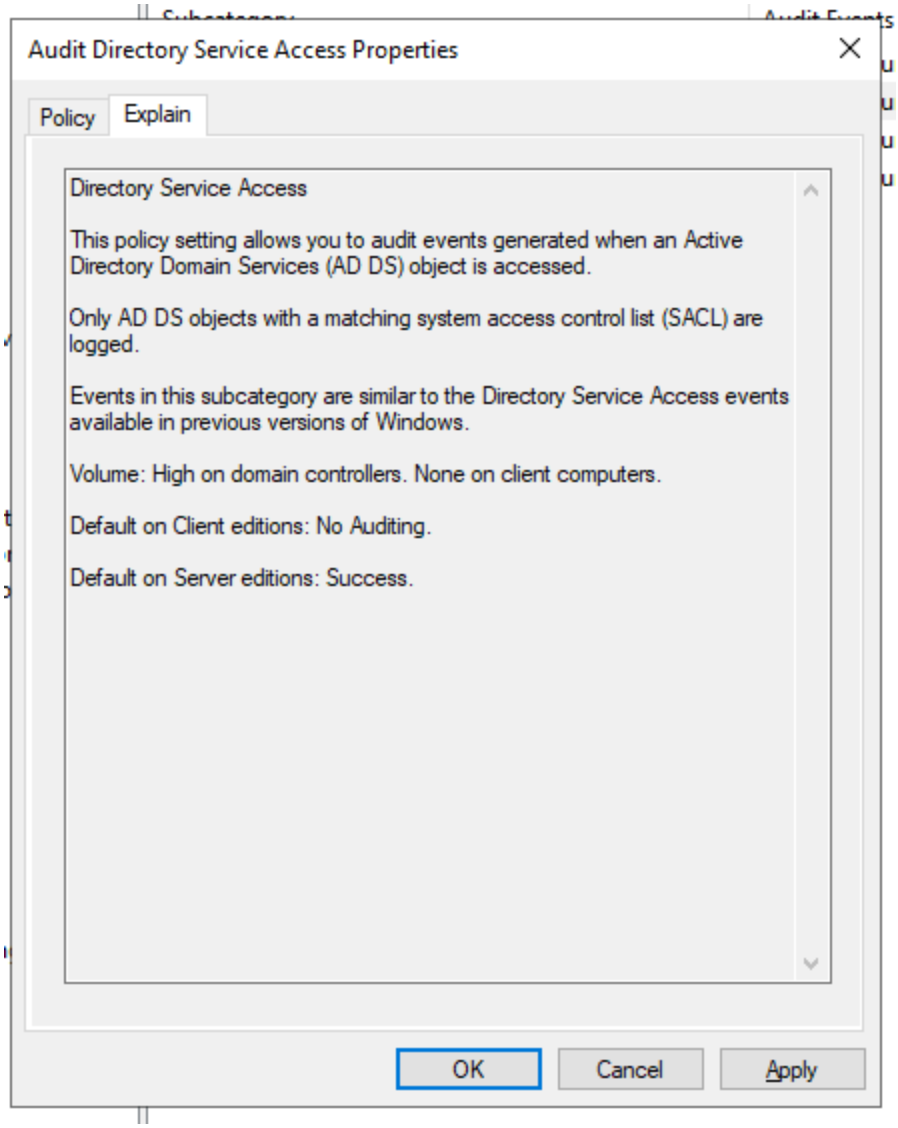
Updated password policy to enforce a minimum of 14 characters.

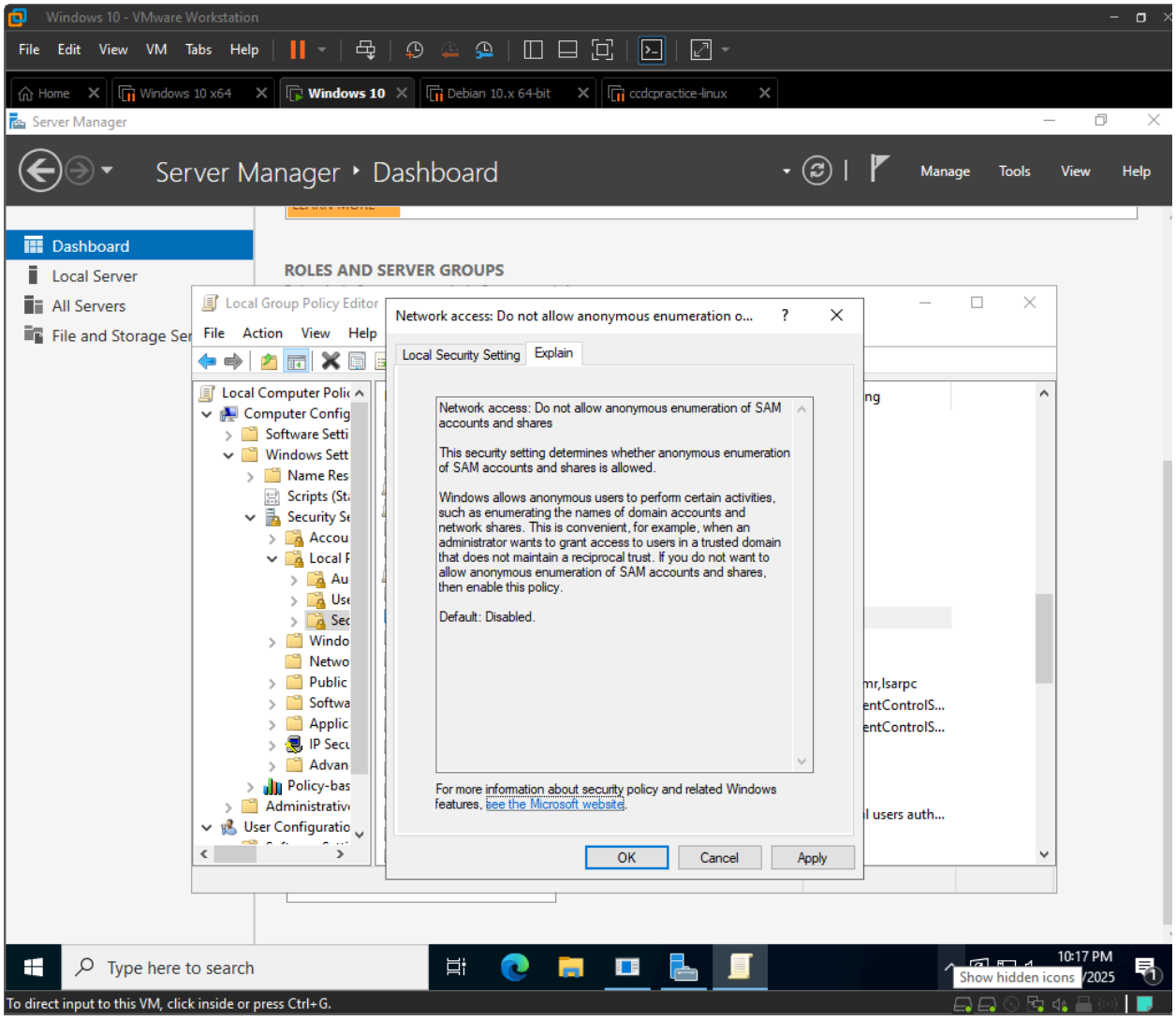
Changed the Administrator password.

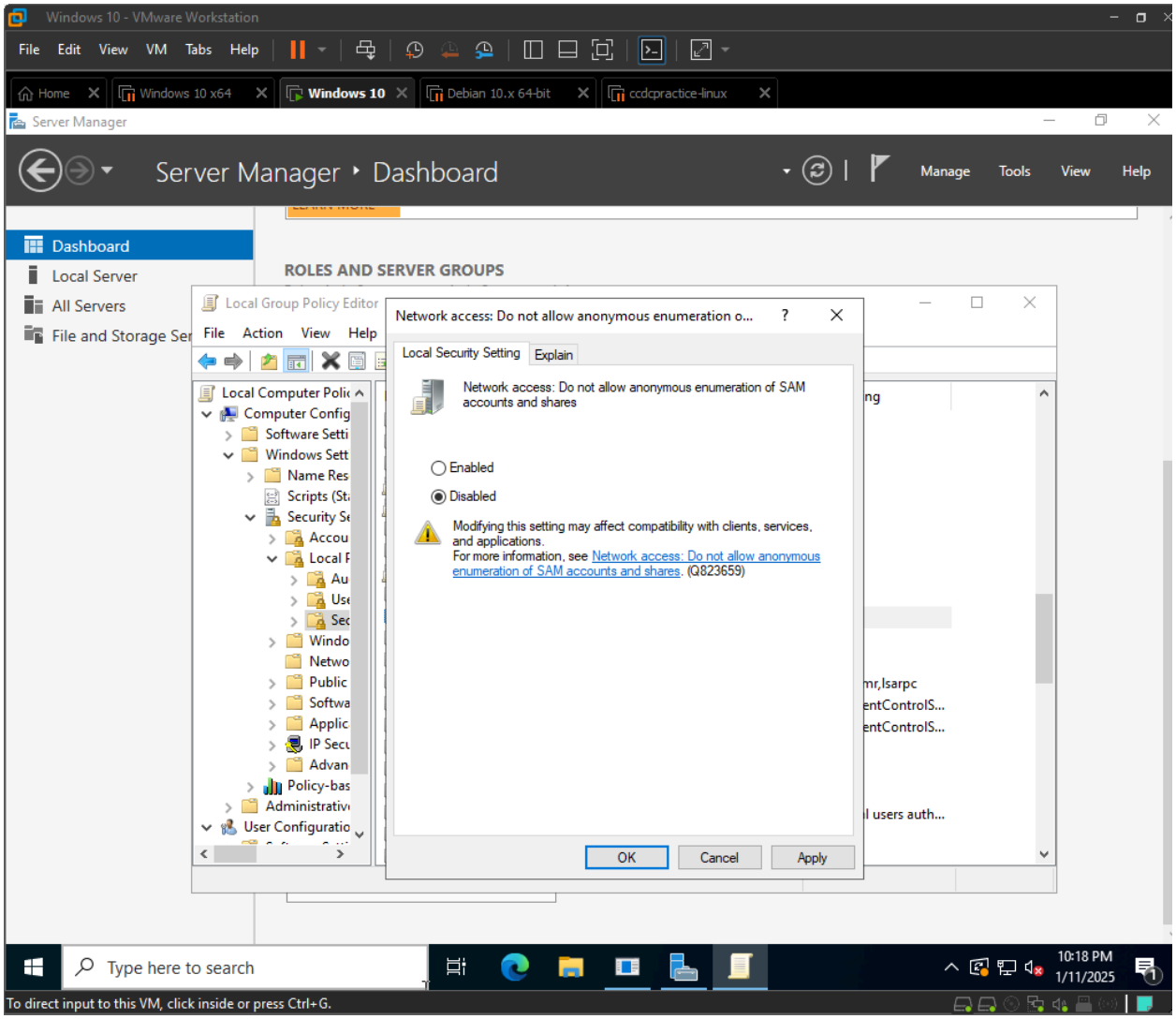

Create Password Settings: Tier0AccountPSO
TASKS
SECTIONS
Password Settings
Directly Applies To
Password Settings
Name:
Tier0AccountPSO
Precedence:
1
Enforce minimum password length
Minimum password length (characters):
30
Enforce password history
Number of passwords remembered:
24
Password must meet complexity requirements
Store password using reversible encryption
Protect from accidental deletion
Password age options:
Enforce minimum password age
User cannot change the password withi...
1
Enforce maximum password age
User must change the password after (...
30
Enforce account lockout policy:
Number of failed logon attempts allowed:
3
Reset failed logon attempts count after (m...
15
Account will be locked out
For a duration of (mins):
15
Until an administrator manually unlocks the account
Description:
Directly Applies To
Name
Mail
Add...
Remove
More Information
OK
Cancel

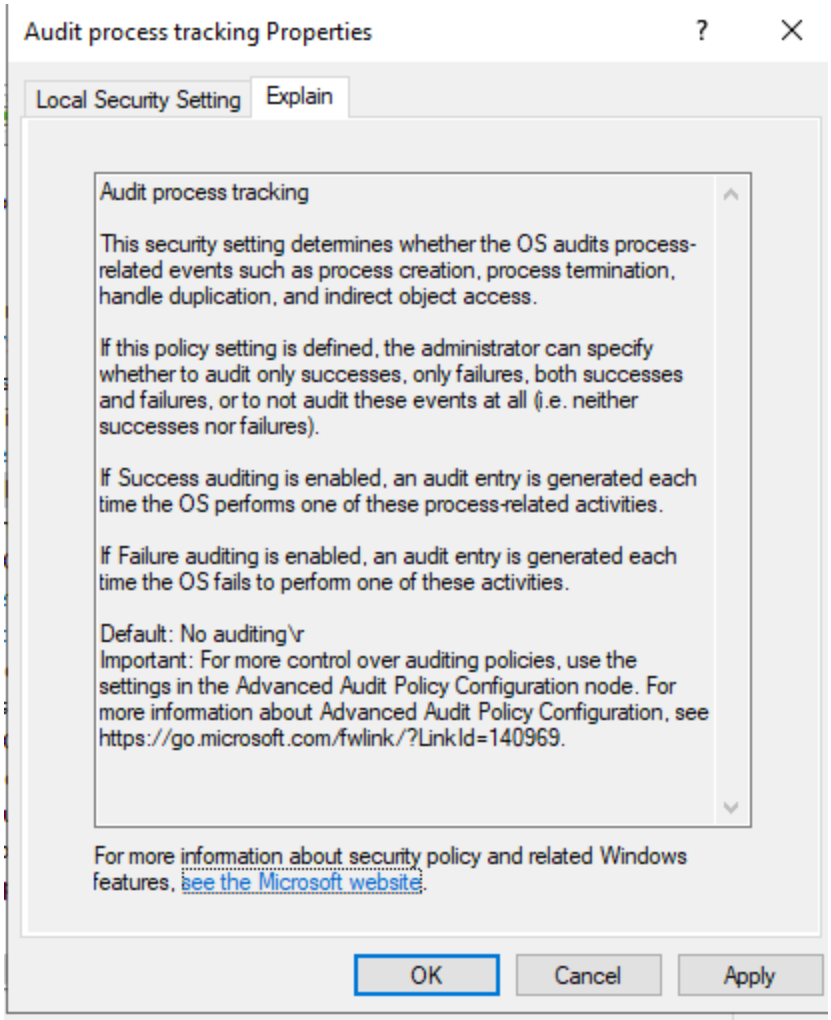

Policy
Policy Setting
Account lockout duration
10 minutes
Account lockout threshold
5 invalid logon attempts
Reset account lockout counter after
10 minutes


Home
Windows 10 x64
Windows 10
Debian 10.x 64-bit
ccdcpractice-linux
Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adv
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Comput
Advanced Audit Policy Configuratio
System Audit Policies - Local Gro
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditin
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Audit Directory Service Access Properties
Policy
Explain
Audit Directory Service Access
Configure the following audit events:
Success
Failure
OK
Cancel
Apply
Type here to search
5:21 PM
1/11/2025
To direct input to this VM, click inside or press Ctrl+G.

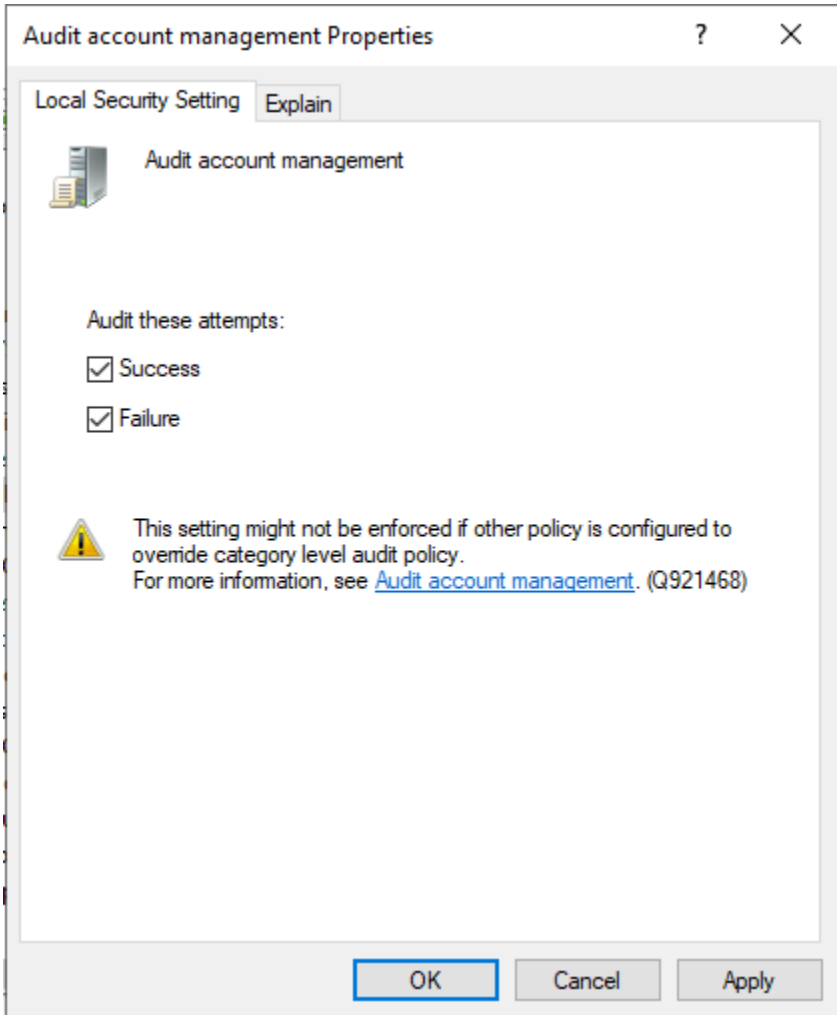

Audit Directory Service Access Properties
Policy
Explain
Directory Service Access
This policy setting allows you to audit events generated when an Active Directory Domain Services (AD DS) object is accessed.
Only AD DS objects with a matching system access control list (SACL) are logged.
Events in this subcategory are similar to the Directory Service Access events available in previous versions of Windows.
Volume: High on domain controllers. None on client computers.
Default on Client editions: No Auditing.
Default on Server editions: Success.
OK
Cancel
Apply

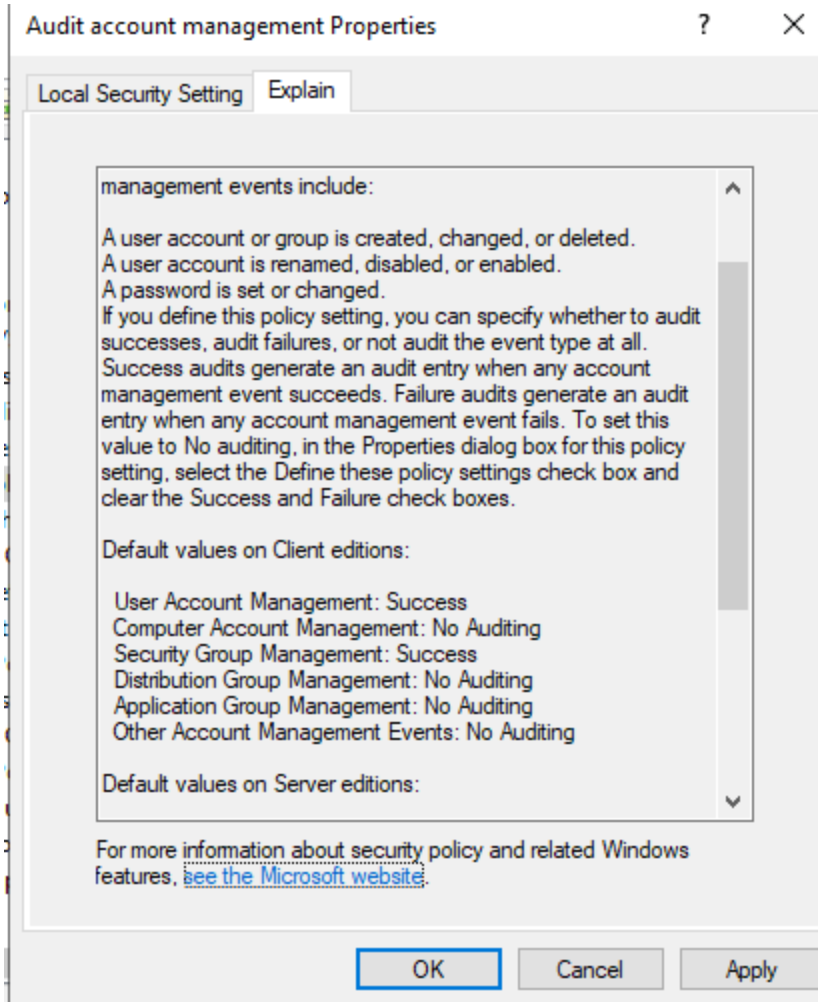

Windows 10 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
Windows 10
Debian 10.x 64-bit
ccdcpractice-linux
Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Ser
ROLES AND SERVER GROUPS
Local Group Policy Editor
File Action View Help
Local Computer Polic
Computer Config
Software Setti
Windows Sett
Name Res
Scripts (St
Security Se
Accou
Local P
Au
Use
Sec
Windo
Netwo
Public
Softwa
Applic
IP Secu
Advan
Policy-bas
Administrativ
User Configuratio
Network access: Do not allow anonymous enumeration o...
Local Security Setting
Explain
Network access: Do not allow anonymous enumeration of SAM accounts and shares
This security setting determines whether anonymous enumeration of SAM accounts and shares is allowed.
Windows allows anonymous users to perform certain activities, such as enumerating the names of domain accounts and network shares. This is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. If you do not want to allow anonymous enumeration of SAM accounts and shares, then enable this policy.
Default: Disabled.
For more information about security policy and related Windows features, see the Microsoft website.
OK
Cancel
Apply
mr,lsarpc
entControlS...
entControlS...
l users auth...
Type here to search
10:17 PM
Show hidden icons
/2025
To direct input to this VM, click inside or press Ctrl+G.


Windows 10 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
Windows 10
Debian 10.x 64-bit
ccdcpractice-linux
Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Ser
ROLES AND SERVER GROUPS
Local Group Policy Editor
File Action View Help
Local Computer Polic
Computer Config
Software Setti
Windows Sett
Name Res
Scripts (St
Security Se
Accou
Local P
Au
Use
Sec
Windo
Netwo
Public
Softwa
Applic
IP Secu
Advan
Policy-bas
Administrativ
User Configuratio
Network access: Do not allow anonymous enumeration o...
Local Security Setting
Explain
Network access: Do not allow anonymous enumeration of SAM accounts and shares
Enabled
Disabled
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network access: Do not allow anonymous enumeration of SAM accounts and shares. (Q823659)
OK
Cancel
Apply
mr,lsarpc
entControlS...
entControlS...
l users auth...
Type here to search
10:18 PM
1/11/2025
To direct input to this VM, click inside or press Ctrl+G.


Audit process tracking Properties
Local Security Setting
Explain
Audit process tracking
This security setting determines whether the OS audits process-related events such as process creation, process termination, handle duplication, and indirect object access.
If this policy setting is defined, the administrator can specify whether to audit only successes, only failures, both successes and failures, or to not audit these events at all (i.e. neither successes nor failures).
If Success auditing is enabled, an audit entry is generated each time the OS performs one of these process-related activities.
If Failure auditing is enabled, an audit entry is generated each time the OS fails to perform one of these activities.
Default: No auditing\r
Important: For more control over auditing policies, use the settings in the Advanced Audit Policy Configuration node. For more information about Advanced Audit Policy Configuration, see https://go.microsoft.com/fwlink/?LinkId=140969.
For more information about security policy and related Windows features, see the Microsoft website.
OK
Cancel
Apply

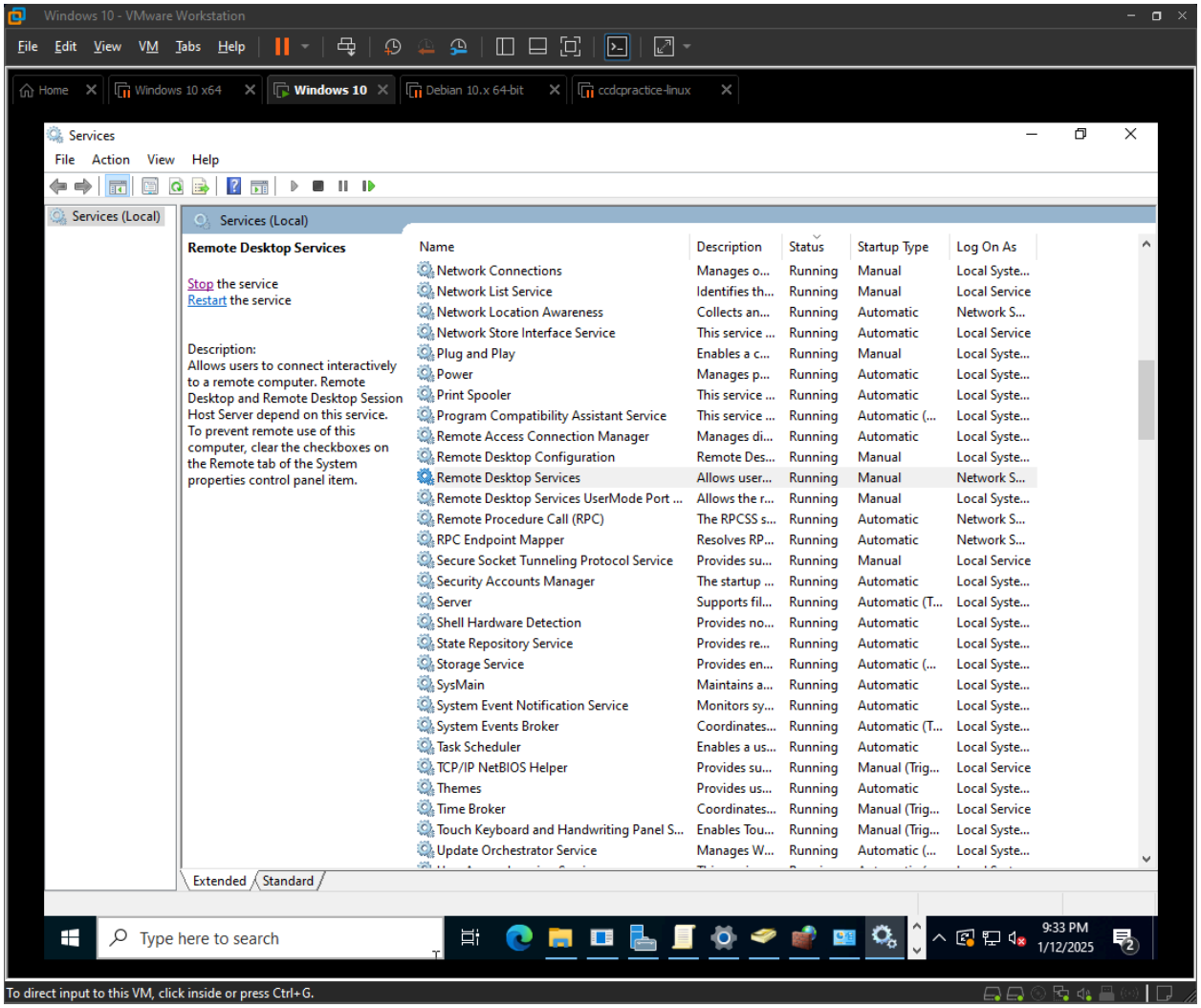
Set audit account management to success + failure





Monitoring running services

Go to services



Checking backdoors

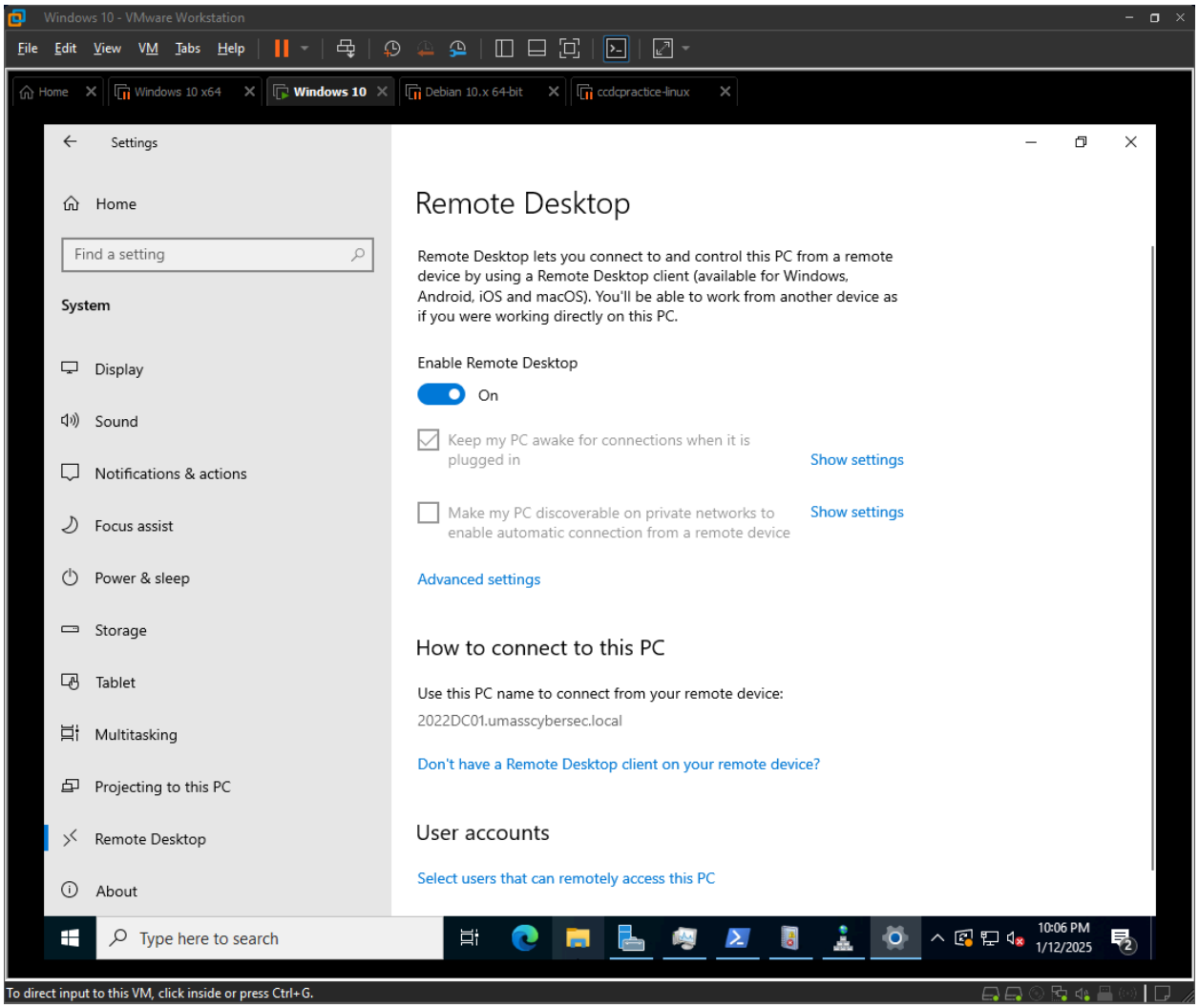
Find suspicious users

Using net user /domain in cmd to find all the users on this DC. There were no suspicious account.

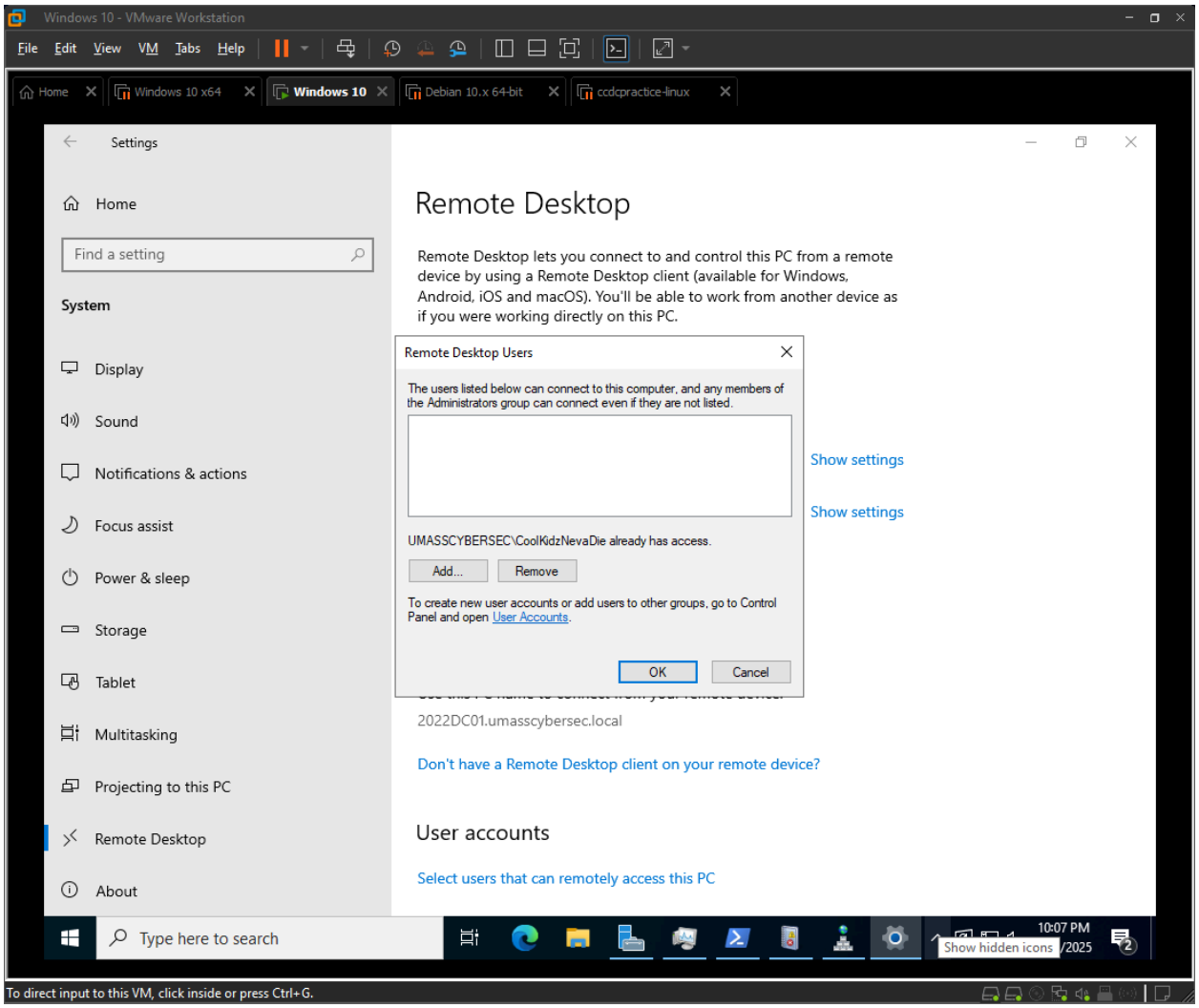
```
C:\Users\Administrator>net user /domain

User accounts for \\2022DC01

-------------------------------------------------------------------------------
CoolKidzNevaDie          Guest                  jdoe
jdunn                    krbtgt                 mssql_svc
svc_axis
The command completed successfully.
```

Checking RDP

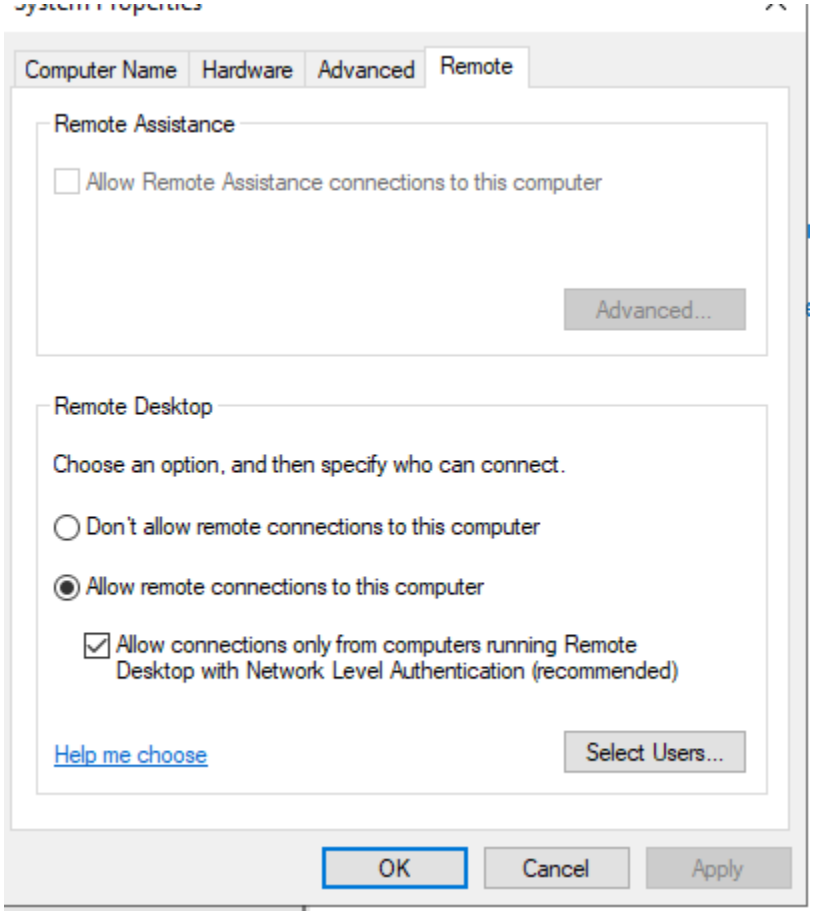
Attackers may exploit RDP to gain access to a system. We need to ensure that RDP is enabled if necessary.



Verified that only authorized users (in this case, administrator) can connect to the computer via RDP.



Enabled Network Level Authentication (NLA) for RDP



Check for potential netcat

What I did:

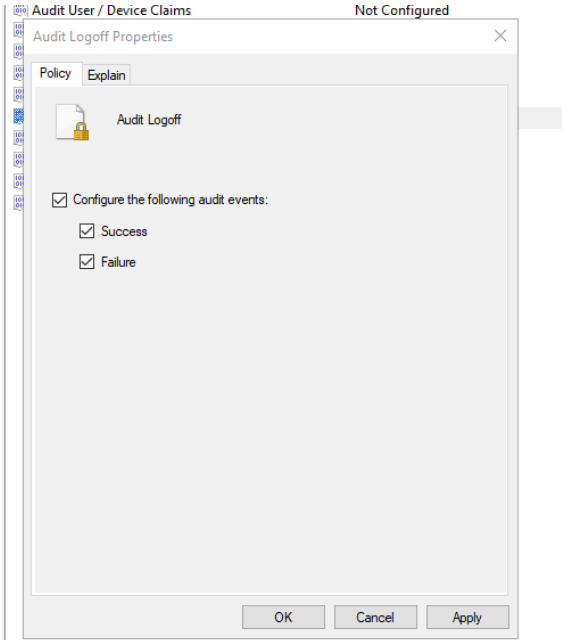
- Used netstat -anb | findstr nc to detect any active network connections and filter results containing the string “nc”

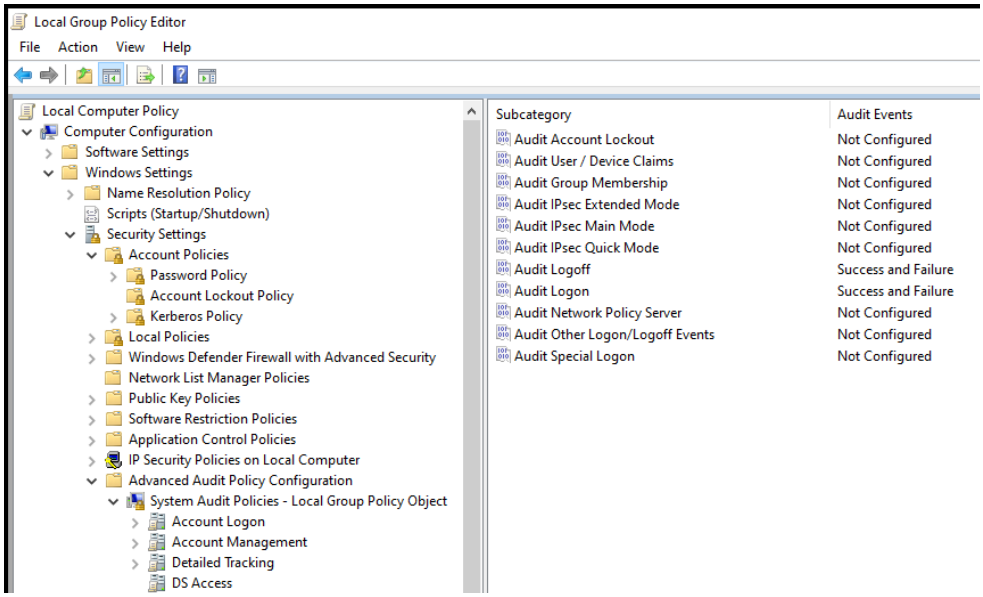
```
PS C:\Users\Administrator> netstat -anb | findstr nc
PS C:\Users\Administrator> _
```

  But netcat binaries could be named differently. So doing this doesn’t guarantee that there is no netcat activity.

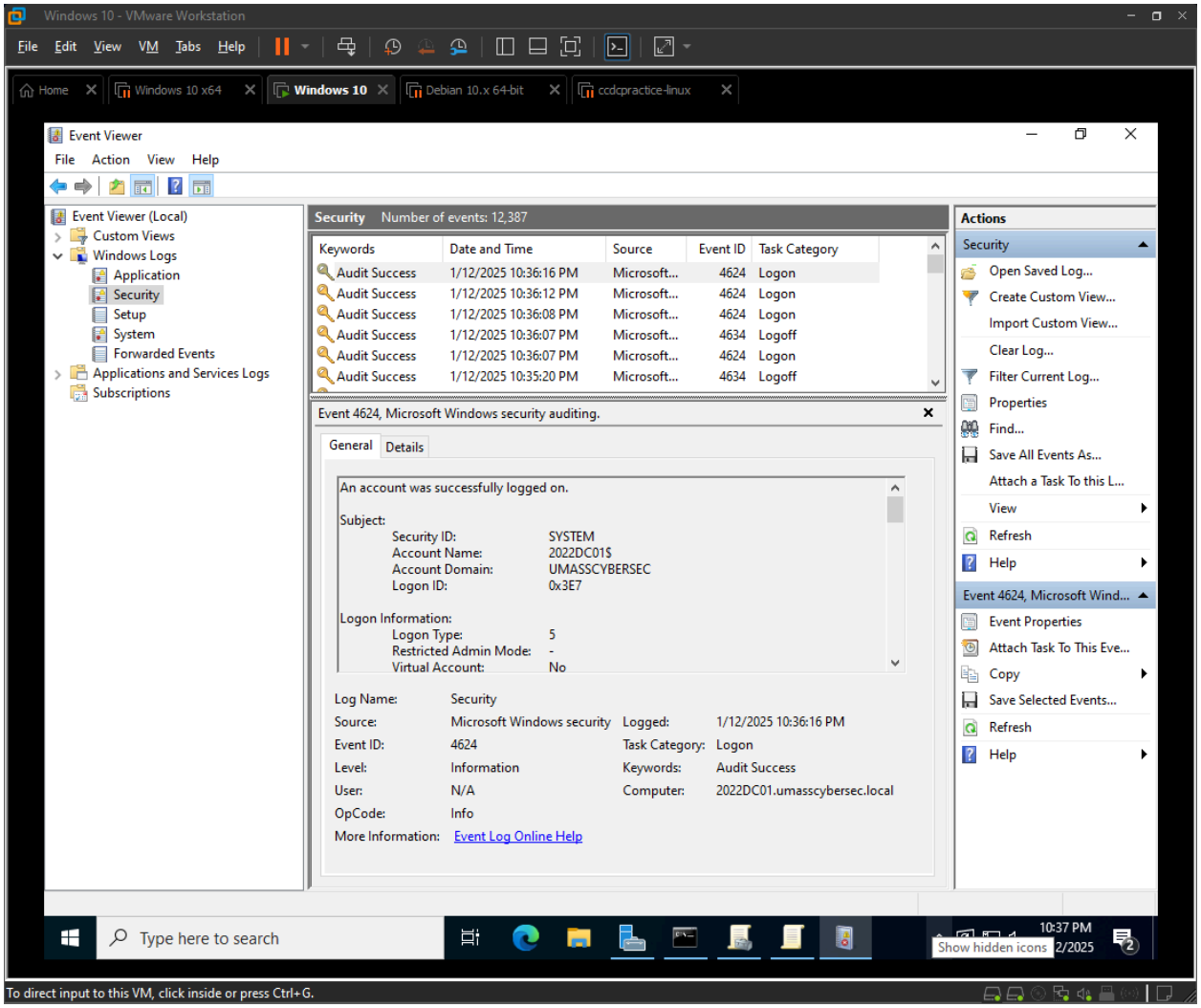
- I checked the task manager and looked for processes resembling netcat or similar names.
- Verified that no processes were consuming an unusual amount of memory

Audit log on /log off by editing local group policies

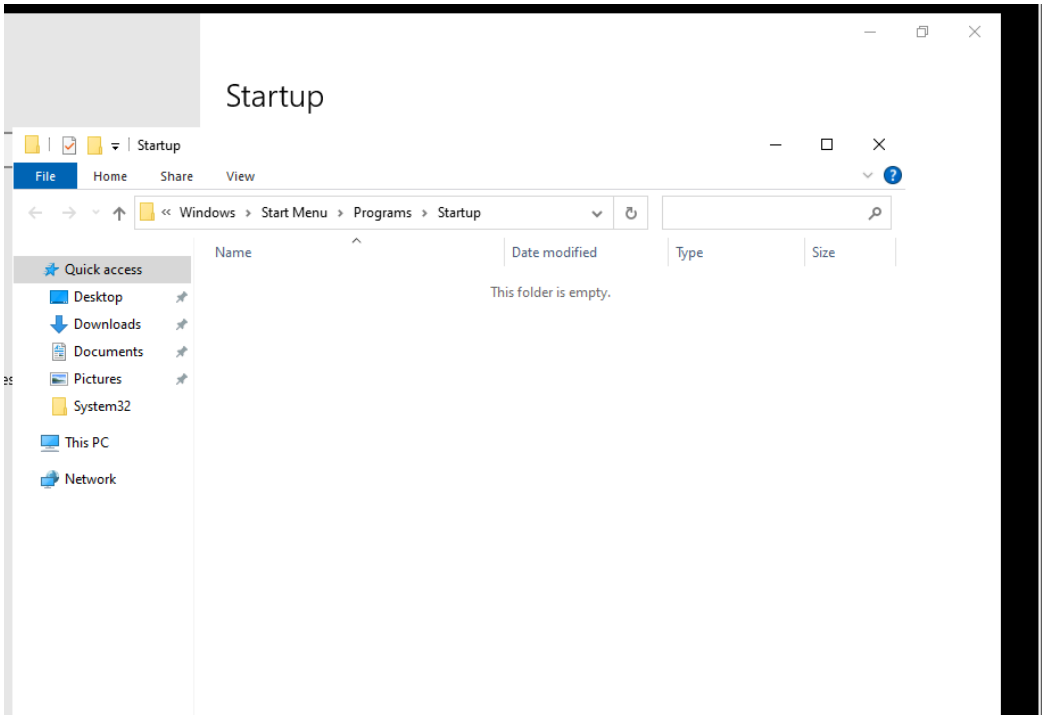




Enabling success or failure means we can track successful and failed log in and out. This practice is useful for monitoring users' activities.
For example, we can then open Event Viewer, navigate to Windows Logs > Security to view successful or failed logon and see which user logged in, from where, and via what method as shown below.


Windows 10 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
Windows 10
Debian 10.x 64-bit
ccdcpractice-linux
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Subscriptions
Security Number of events: 12,387
Keywords Date and Time Source Event ID Task Category
Audit Success 1/12/2025 10:36:16 PM Microsoft... 4624 Logon
Audit Success 1/12/2025 10:36:12 PM Microsoft... 4624 Logon
Audit Success 1/12/2025 10:36:08 PM Microsoft... 4624 Logon
Audit Success 1/12/2025 10:36:07 PM Microsoft... 4634 Logoff
Audit Success 1/12/2025 10:36:07 PM Microsoft... 4624 Logon
Audit Success 1/12/2025 10:35:20 PM Microsoft... 4634 Logoff
Event 4624, Microsoft Windows security auditing.
General Details
An account was successfully logged on.
Subject:
Security ID: SYSTEM
Account Name: 2022DC01$
Account Domain: UMASSCYBERSEC
Logon ID: 0x3E7
Logon Information:
Logon Type: 5
Restricted Admin Mode: -
Virtual Account: No
Log Name: Security
Source: Microsoft Windows security
Logged: 1/12/2025 10:36:16 PM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: 2022DC01.umasscybersec.local
OpCode: Info
More Information: Event Log Online Help
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this L...
View
Refresh
Help
Event 4624, Microsoft Wind...
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help
Type here to search
10:37 PM
Show hidden icons
2/2025
To direct input to this VM, click inside or press Ctrl+G.

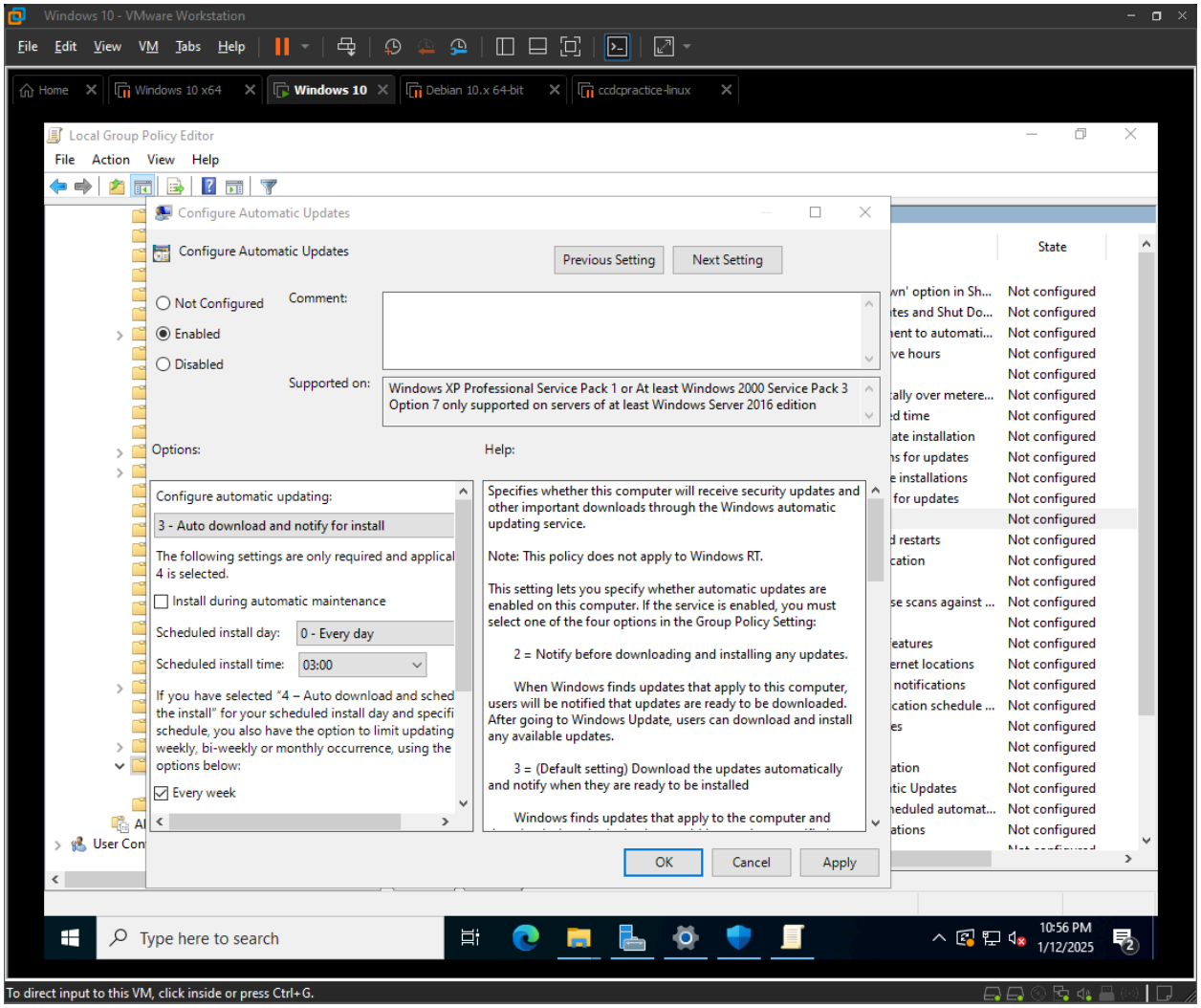
Checking startup folder to find potential backdoors



The startup folder might contain malicious programs or scripts that run automatically when the system boots. But here, since there isn't any suspicious program, I assume the folder is safe.

Checking automatic updates in windows

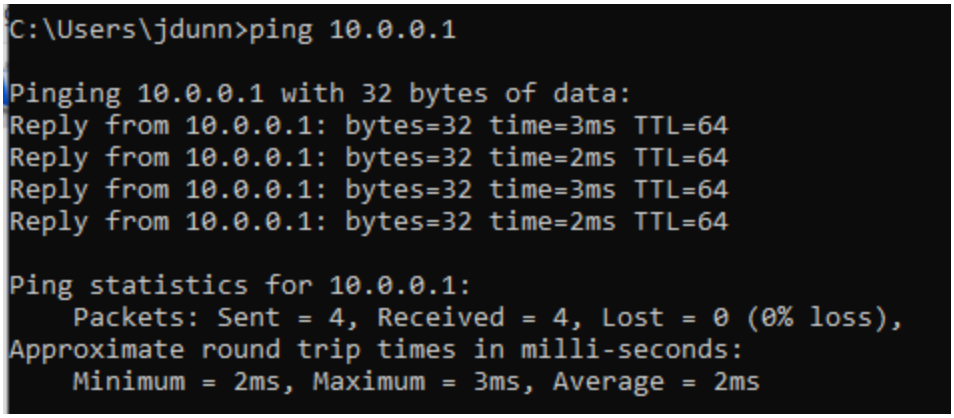
Opened Edit Group Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates > Enabled



Confirmed compatibility with Windows Server 2022 and enabled the policy. Our VM is in Windows Server 2022 so it can be supported by this policy.

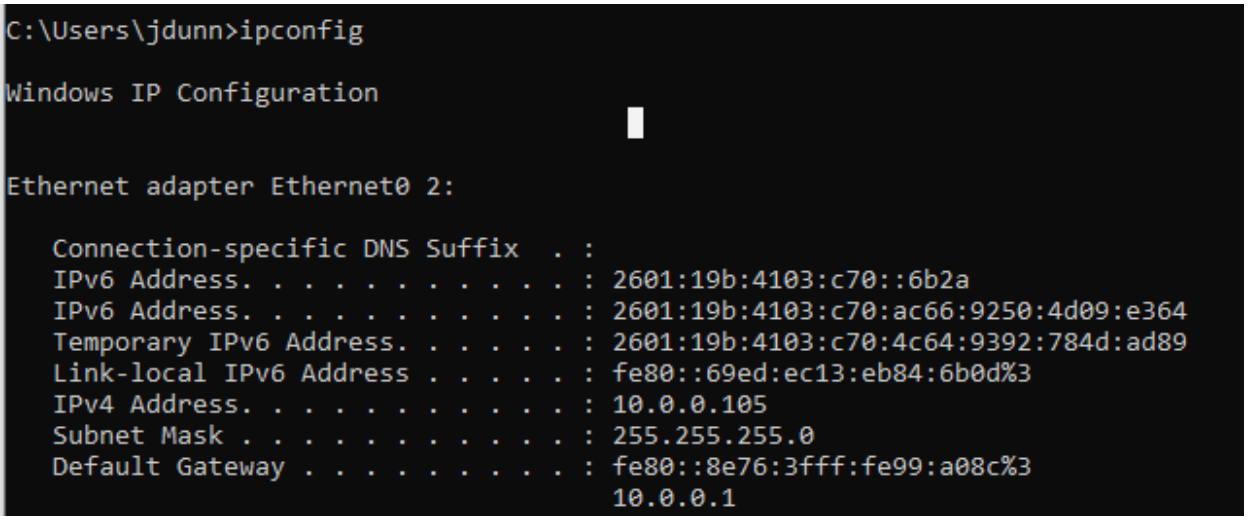
Struggling setting up DNS

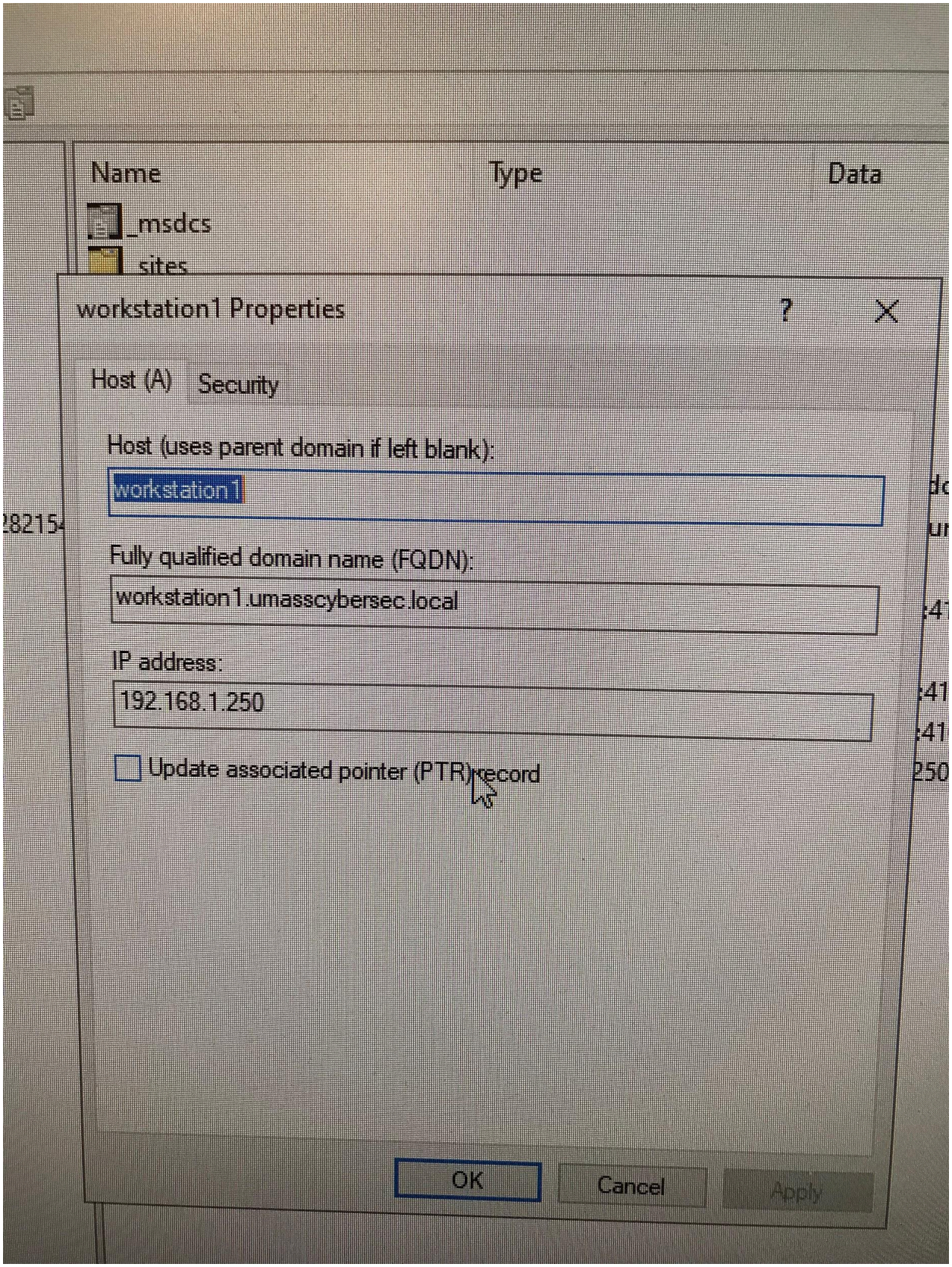
From the workstation1, I could ping default gateway 10.0.0.1.

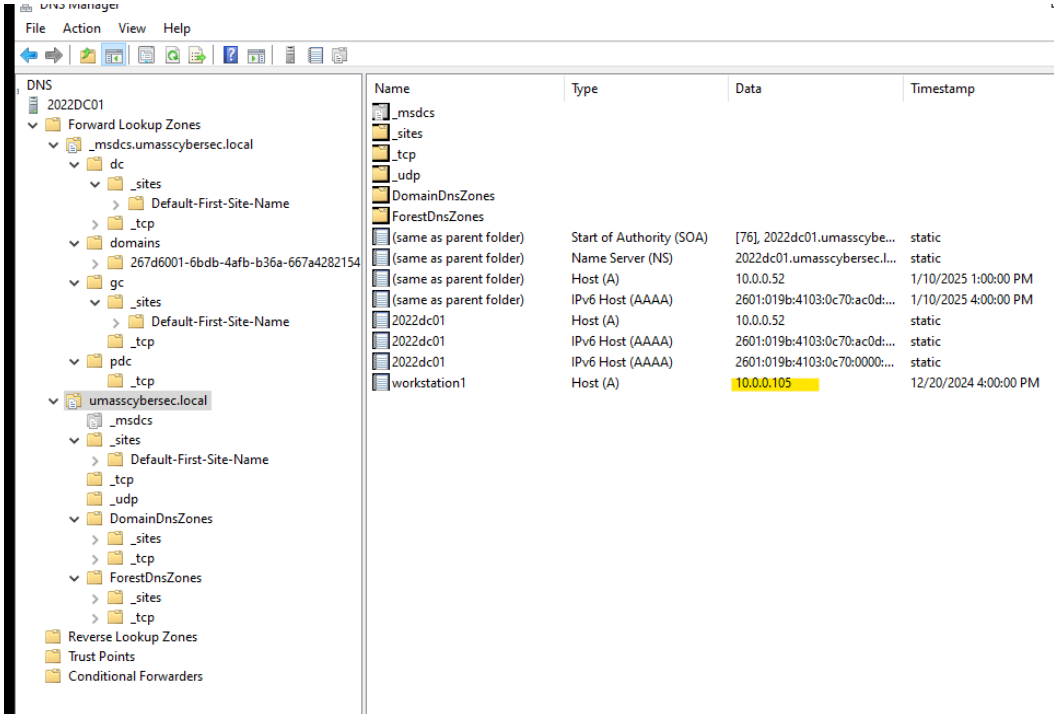


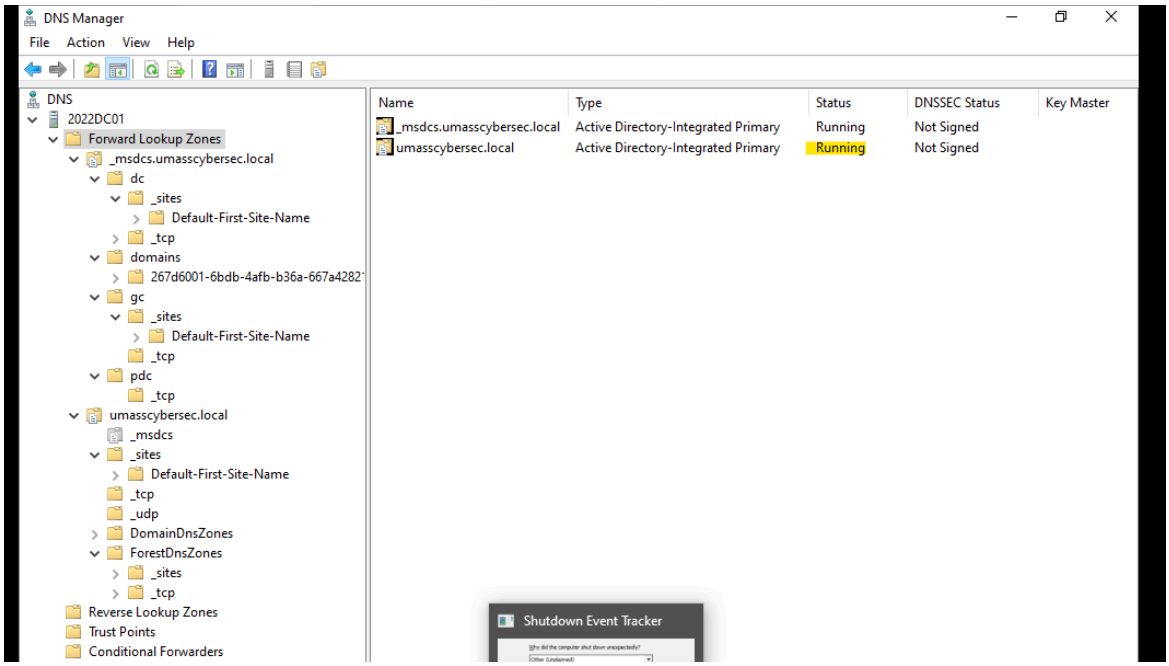
Can ping 2202dc01

There are misconfigurations. In the DNS Manager on the DC, the IP of workstation1 is 192. , different from what we got using “ipconfig” on the workstation1 itself (10.0.0.105). So I edited the IP address of the workstation1 in the DNS manager on DC.


C:\Users\jdunn>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0 2:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2601:19b:4103:c70::6b2a
IPv6 Address. . . . . : 2601:19b:4103:c70:ac66:9250:4d09:e364
Temporary IPv6 Address. . . . . : 2601:19b:4103:c70:4c64:9392:784d:ad89
Link-local IPv6 Address . . . . . : fe80::69ed:ec13:eb84:6b0d%3
IPv4 Address. . . . . : 10.0.0.105
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::8e76:3fff:fe99:a08c%3
10.0.0.1


Name
Type
Data
_msdcs
_sites
workstation1 Properties
?
Host (A)
Security
Host (uses parent domain if left blank):
workstation1
Fully qualified domain name (FQDN):
workstation1.umasscybersec.local
IP address:
192.168.1.250
Update associated pointer (PTR) record
OK
Cancel
Apply

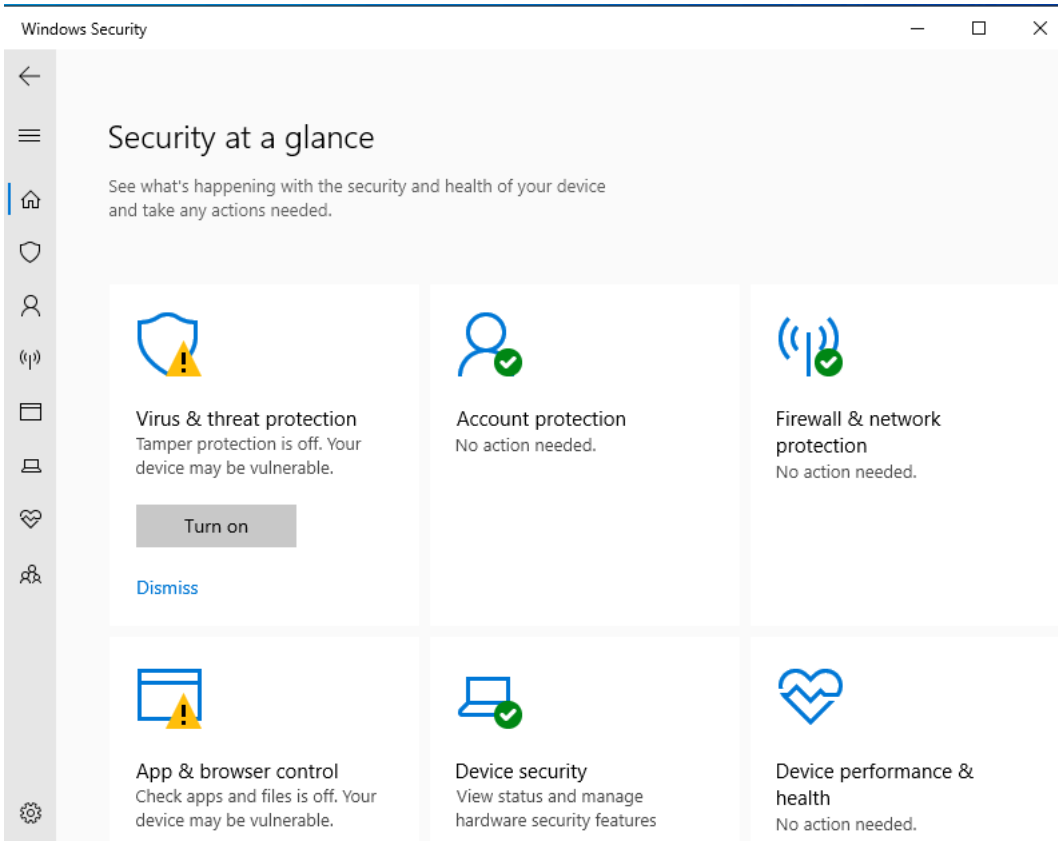




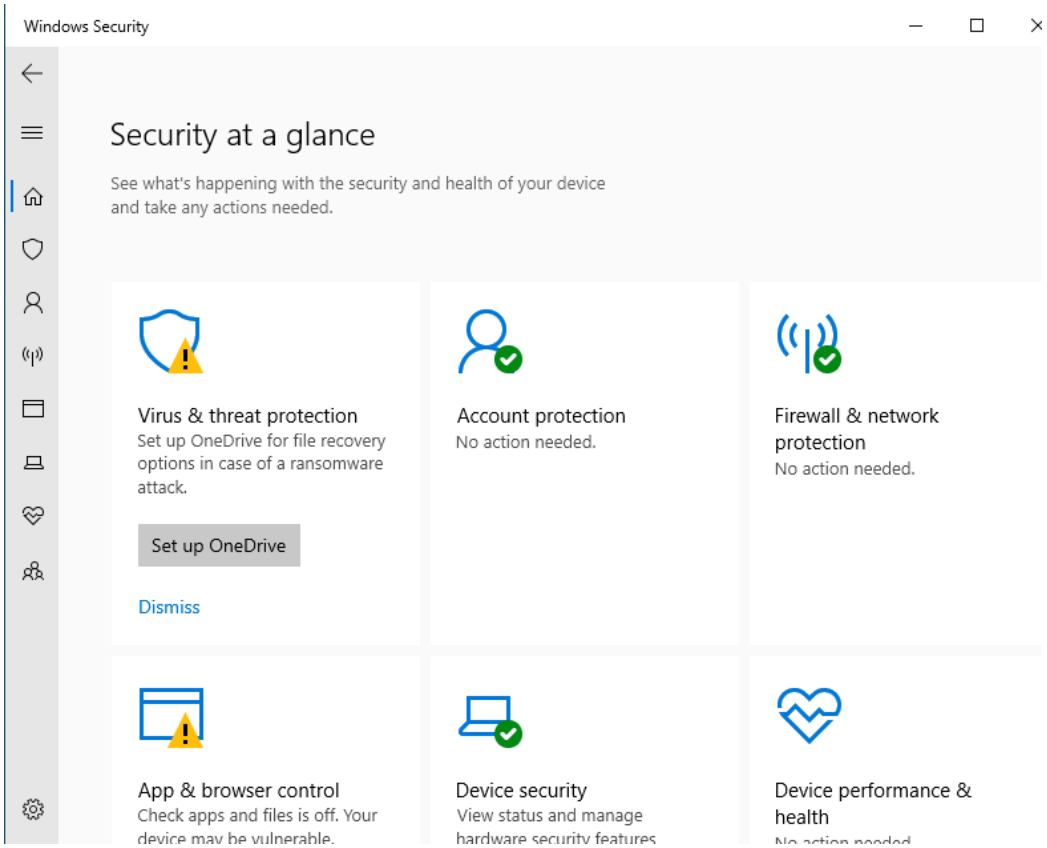
(to be continued – I didn't have enough time to investigate this further)

Workstation1

Windows Security: Check firewall & network protection

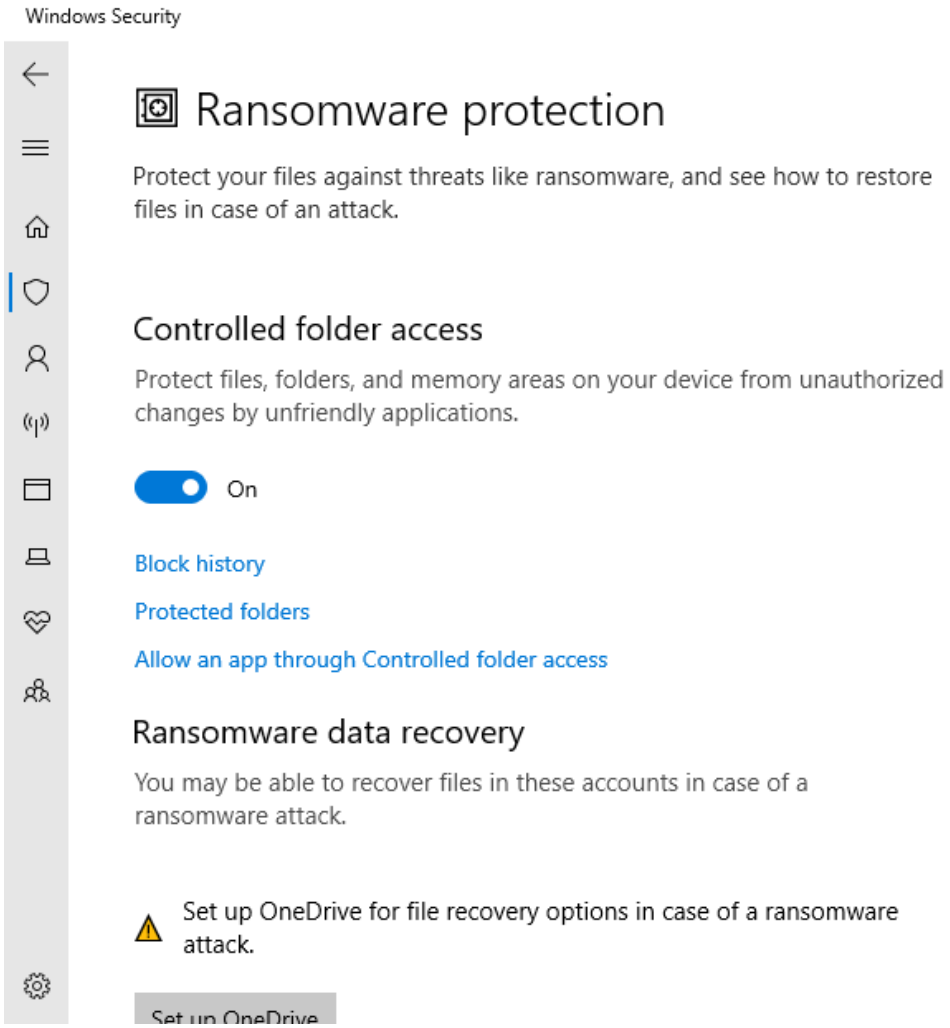


I tried to turn threat protection on with the admin credentials.



It asked to set up OneDrive for ransomware protection, but that requires an email, so I didn't do it.

In ransomware protection, I turned on controlled folder access. Ransomware protection includes tools to detect, block, and recover from ransomware attacks – a type of malware that encrypts your files and demands payment to restore access. So, when turning on controlled folder access, we can protect common directories like Documents, Pictures, Videos, Music, Desktop,etc.


Windows Security
Ransomware protection
Protect your files against threats like ransomware, and see how to restore files in case of an attack.
Controlled folder access
Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.
On
Block history
Protected folders
Allow an app through Controlled folder access
Ransomware data recovery
You may be able to recover files in these accounts in case of a ransomware attack.
Set up OneDrive for file recovery options in case of a ransomware attack.
Set up OneDrive

Here are the protected folders:

Documents
C:\Users\jdunn\Documents

Documents
C:\Users\Public\Documents

Pictures
C:\Users\jdunn\Pictures

Pictures
C:\Users\Public\Pictures

Videos
C:\Users\Public\Videos

Videos
C:\Users\jdunn\Videos

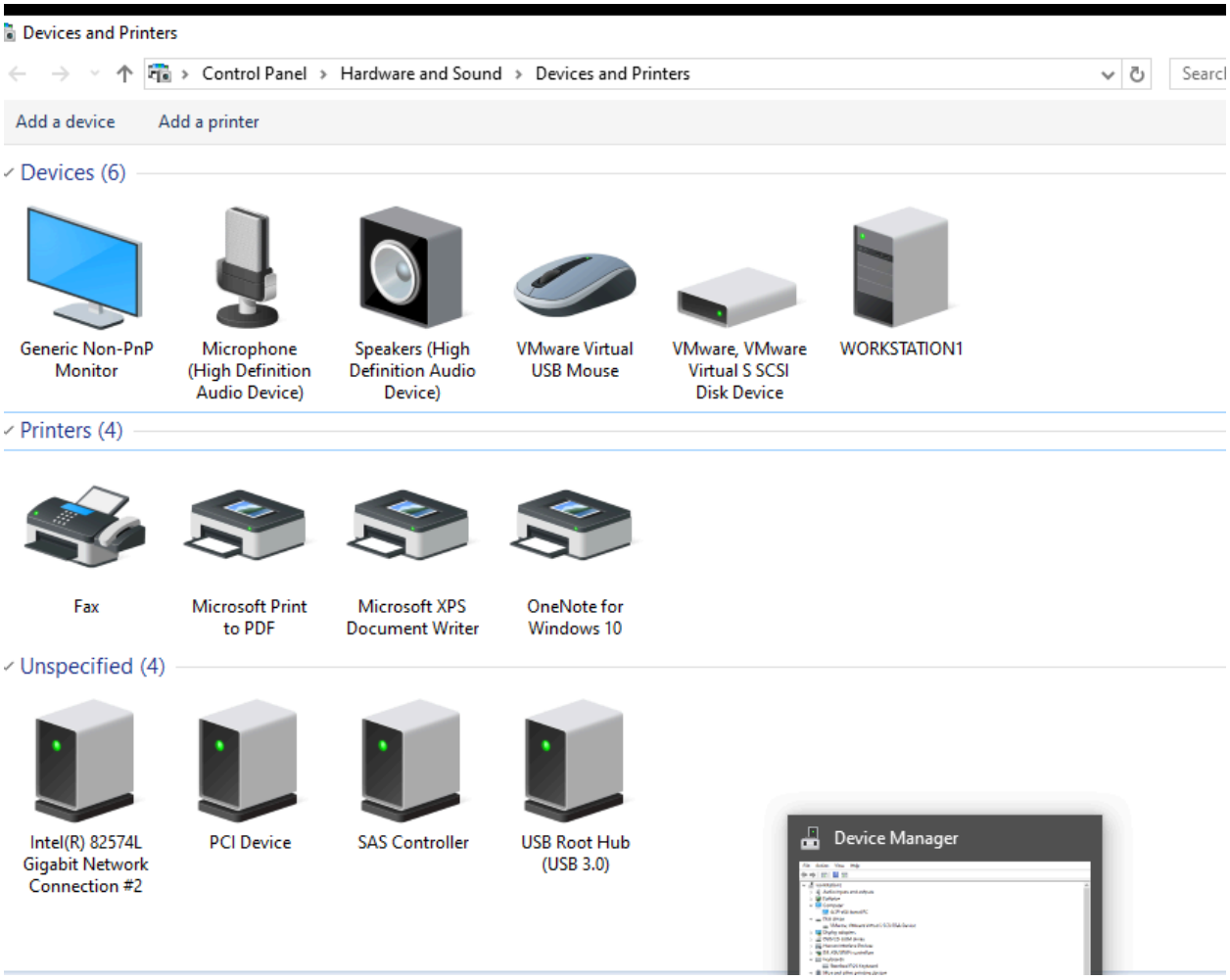
Music
C:\Users\jdunn\Music

Music
C:\Users\Public\Music

Favorites
C:\Users\jdunn\Favorites

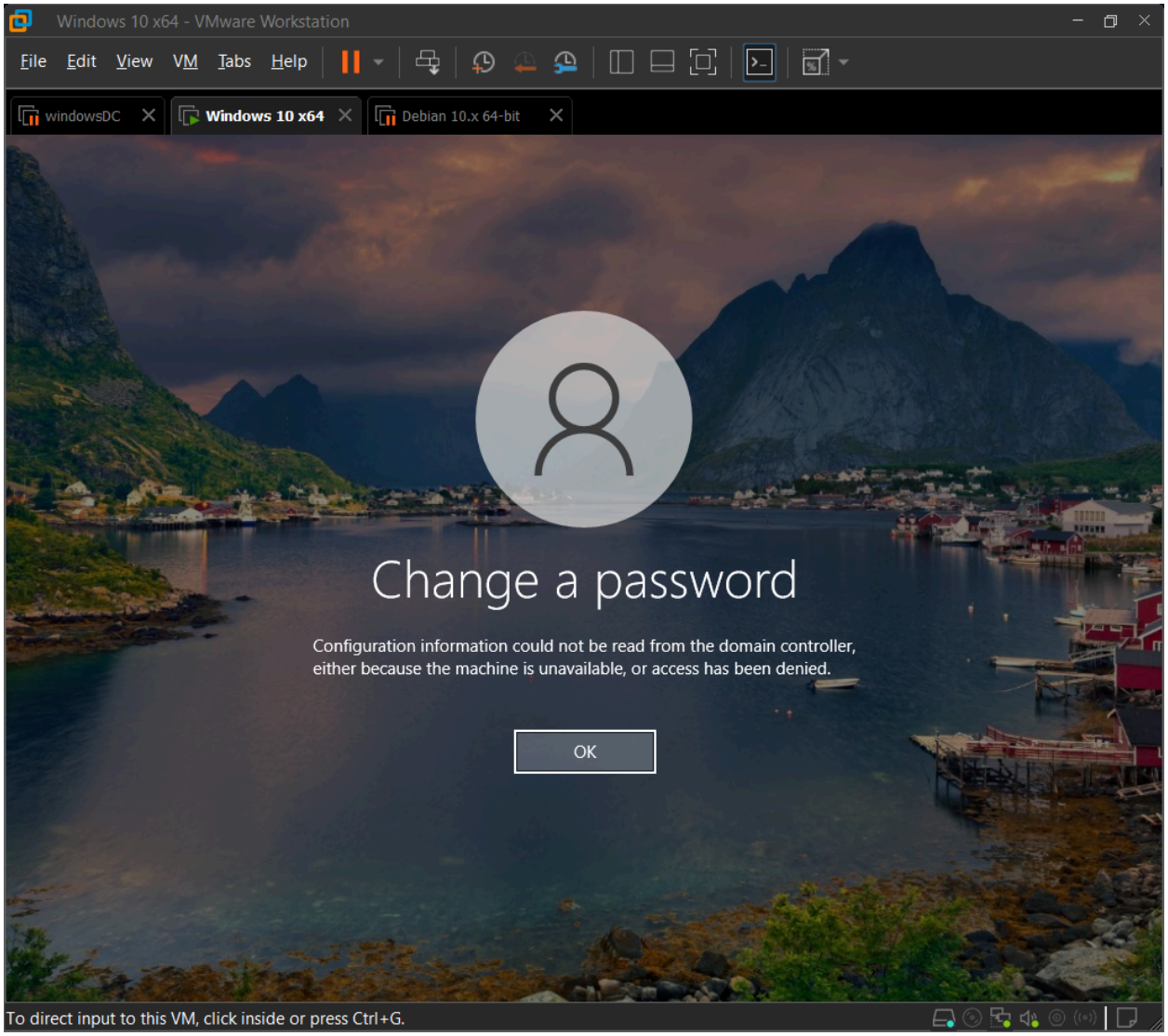
securing printers – printer vulnerabilities

All the devices and printers connected. None of them seems suspicious so I did not investigate further.



Trying to change jdoe password

Hit Ctrl+Alt+insert > Change a password



Config information could not be read from the domain controller means the machine is unable to talk to it normally.
This happens because I couldn't connect the workstation with the DC but I wasn't able to figure this out with the allotted time.