Report: Security Baselines & Compliance

1. Introduction

Maintaining security compliance and enforcing configuration baselines are critical components of a well-managed enterprise IT environment. In this phase, we focus on applying standardized, industry-accepted security frameworks to ensure Active Directory and Windows systems are resilient against modern threats. By leveraging tools like the Microsoft Security Compliance Toolkit, NSA and CIS hardening guides, and Windows Defender Application Control (WDAC), we aim to reduce attack surfaces, enforce script-level security, and ensure consistent application of security settings. Additionally, a mock Active Directory (AD) audit is conducted to simulate real-world compliance assessments and uncover any gaps in existing configurations. These tasks not only improve the technical posture of systems but also help organizations meet regulatory requirements and internal governance standards.

2. Objective

The primary objective of these tasks is to enhance the overall security posture of the Active Directory environment and Windows systems by enforcing standardized security baselines and hardening measures. Applying the Microsoft Security Compliance Toolkit ensures that systems conform to Microsoft's recommended security settings, reducing misconfigurations and vulnerabilities. Hardening Domain Controllers using NSA and CIS benchmarks strengthens critical infrastructure by implementing proven security controls for authentication, auditing, and access. Implementing Windows Defender Application Control (WDAC) further protects endpoints by restricting unauthorized scripts and executables, mitigating risks from malware and malicious code. Finally, conducting a mock Active Directory security audit enables the identification of security gaps and compliance issues, allowing for proactive remediation and improved governance readiness. Together, these objectives aim to create a secure, compliant, and resilient enterprise environment.

Key goals include:

- **Enforce Standardized Security Configurations**
  Apply Microsoft's Security Compliance Toolkit baselines to ensure consistent and secure system settings across all Windows devices.

- **Strengthen Domain Controller Security**
  Implement NSA and CIS benchmark guidelines to harden Domain Controllers, safeguarding core Active Directory infrastructure from attacks.

- **Prevent Execution of Unauthorized Code**
  Use Windows Defender Application Control (WDAC) to restrict scripts and applications, blocking untrusted or malicious code execution.

- **Assess Active Directory Security Posture**
  Conduct a mock security audit to evaluate current Active Directory configurations, permissions, and compliance with security policies.

- **Identify and Remediate Security Gaps**
  Document audit findings and provide actionable insights to address vulnerabilities, improve compliance, and enhance overall network security.

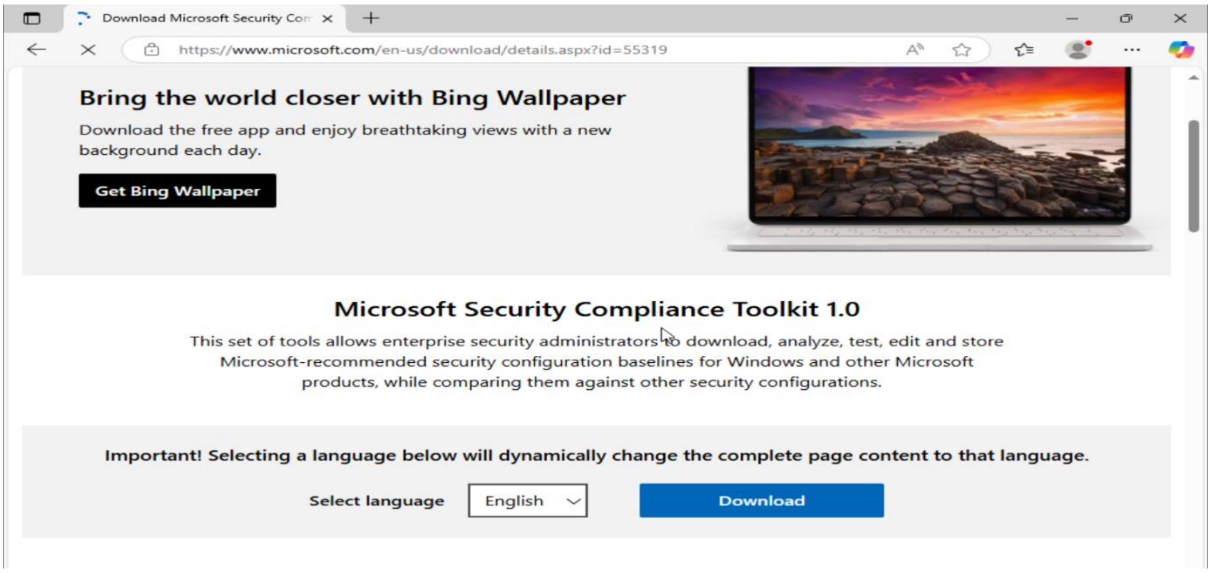
3. Methodology

The methodology describes applying standardized security baselines using Microsoft's toolkit, hardening Domain Controllers with NSA/CIS benchmarks, and enforcing script control through Windows Defender Application Control. It also includes conducting a mock Active Directory audit to evaluate security and identify weaknesses. This structured approach ensures consistent security configurations, stronger protections, and improved compliance across the environment.

3.1 Apply Microsoft Security Compliance Toolkit Baselines

- Download the latest Security Compliance Toolkit (SCT).
- Extract the toolkit and open the desired baseline folder.
- Import the Group Policy Objects (GPOs) using the **Policy Analyzer** or **LGPO.exe** tool.
- Use the Group Policy Management Console (GPMC) to link imported GPOs to appropriate OUs or domains.
- Run gpupdate /force on target machines to apply baseline policies immediately.

(Downloaded the toolkit and Extracted it.)


Download Microsoft Security Con
https://www.microsoft.com/en-us/download/details.aspx?id=55319

Bring the world closer with Bing Wallpaper

Download the free app and enjoy breathtaking views with a new background each day.

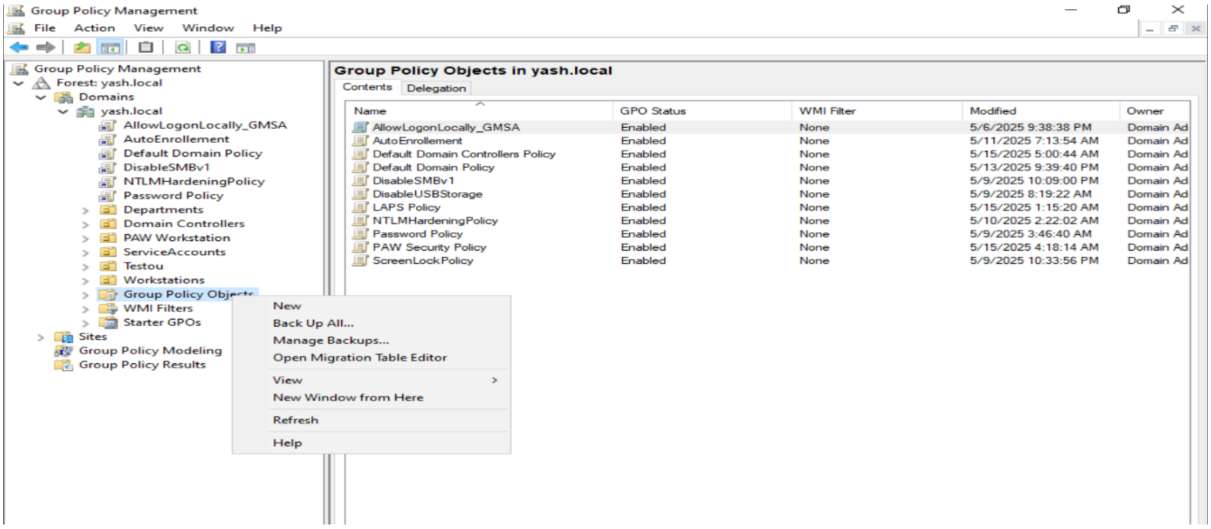
Microsoft Security Compliance Toolkit 1.0

This set of tools allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.

Important! Selecting a language below will dynamically change the complete page content to that language.

Select language: English

(Creating a new GPO.)

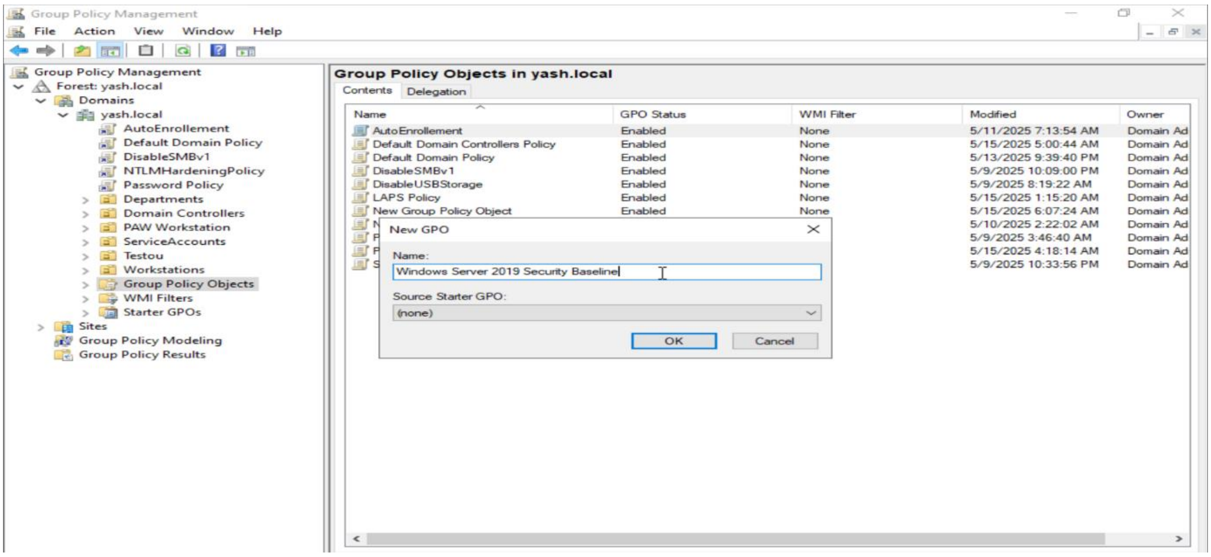


Group Policy Objects in yash.local

Contents | Delegation

Name	GPO Status	WMI Filter	Modified	Owner
AllowLogonLocally_GMSA	Enabled	None	5/6/2025 9:38:38 PM	Domain Ad
AutoEnrollement	Enabled	None	5/11/2025 7:13:54 AM	Domain Ad
Default Domain Controllers Policy	Enabled	None	5/15/2025 5:00:44 AM	Domain Ad
Default Domain Policy	Enabled	None	5/13/2025 9:39:40 PM	Domain Ad
DisableSMBv1	Enabled	None	5/9/2025 10:09:00 PM	Domain Ad
DisableUSBStorage	Enabled	None	5/9/2025 8:19:22 AM	Domain Ad
LAPS Policy	Enabled	None	5/15/2025 1:15:20 AM	Domain Ad
NTLMHardeningPolicy	Enabled	None	5/10/2025 2:22:02 AM	Domain Ad
Password Policy	Enabled	None	5/9/2025 3:46:40 AM	Domain Ad
PAW Security Policy	Enabled	None	5/15/2025 4:18:14 AM	Domain Ad
ScreenLockPolicy	Enabled	None	5/9/2025 10:33:56 PM	Domain Ad

(Created a new GPO .)



Group Policy Objects in yash.local

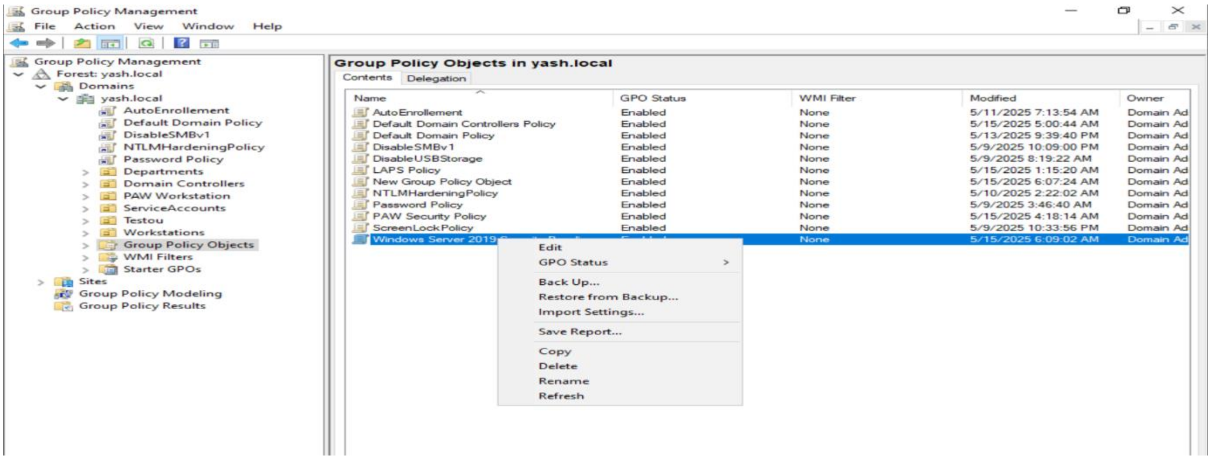
Name	GPO Status	WMI Filter	Modified	Owner
AutoEnrollement	Enabled	None	5/11/2025 7:13:54 AM	Domain Ad
Default Domain Controllers Policy	Enabled	None	5/15/2025 5:00:44 AM	Domain Ad
Default Domain Policy	Enabled	None	5/13/2025 9:39:40 PM	Domain Ad
DisableSMBv1	Enabled	None	5/9/2025 10:09:00 PM	Domain Ad
DisableUSBStorage	Enabled	None	5/9/2025 8:19:22 AM	Domain Ad
LAPS Policy	Enabled	None	5/15/2025 1:15:20 AM	Domain Ad
New Group Policy Object	Enabled	None	5/15/2025 6:07:24 AM	Domain Ad
N			5/10/2025 2:22:02 AM	Domain Ad
P			5/9/2025 3:46:40 AM	Domain Ad
P			5/15/2025 4:18:14 AM	Domain Ad
S			5/9/2025 10:33:56 PM	Domain Ad

New GPO

Name: Windows Server 2019 Security Baseline

Source Starter GPO: (none)

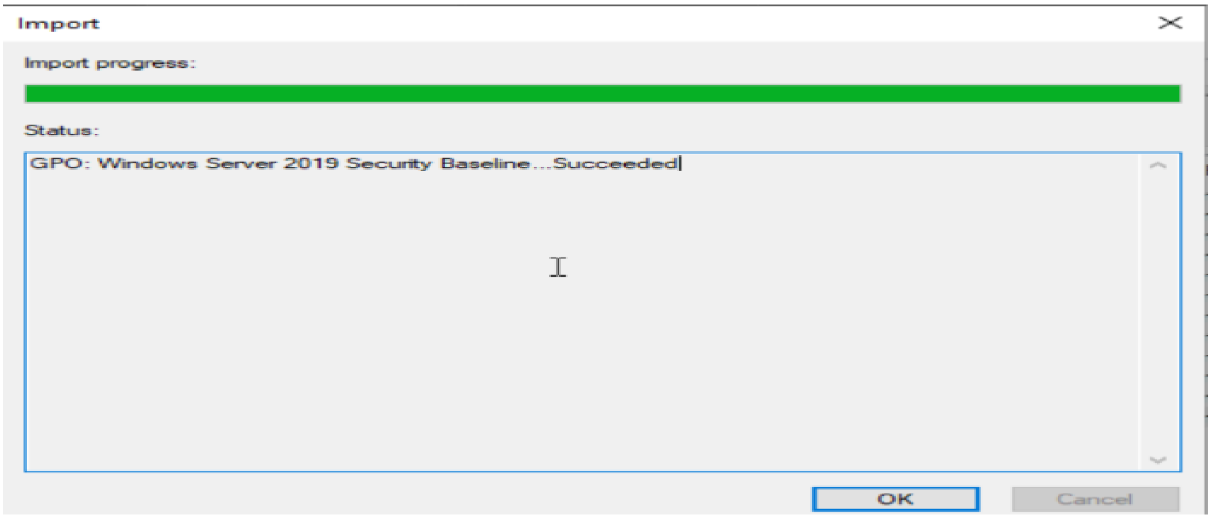
(Import the file from toolkit.)



Group Policy Objects in yash.local

Name	GPO Status	WMI Filter	Modified	Owner
AutoEnrollement	Enabled	None	5/11/2025 7:13:54 AM	Domain Ad
Default Domain Controllers Policy	Enabled	None	5/15/2025 5:00:44 AM	Domain Ad
Default Domain Policy	Enabled	None	5/13/2025 9:39:40 PM	Domain Ad
DisableSMBv1	Enabled	None	5/9/2025 10:09:00 PM	Domain Ad
DisableUSBStorage	Enabled	None	5/9/2025 8:19:22 AM	Domain Ad
LAPS Policy	Enabled	None	5/15/2025 1:15:20 AM	Domain Ad
New Group Policy Object	Enabled	None	5/15/2025 6:07:24 AM	Domain Ad
NTLMHardeningPolicy	Enabled	None	5/10/2025 2:22:02 AM	Domain Ad
Password Policy	Enabled	None	5/9/2025 3:46:40 AM	Domain Ad
PAW Security Policy	Enabled	None	5/15/2025 4:18:14 AM	Domain Ad
ScreenLockPolicy	Enabled	None	5/9/2025 10:33:56 PM	Domain Ad
Windows Server 2019		None	5/15/2025 6:09:02 AM	Domain Ad

(Imported Successful.)

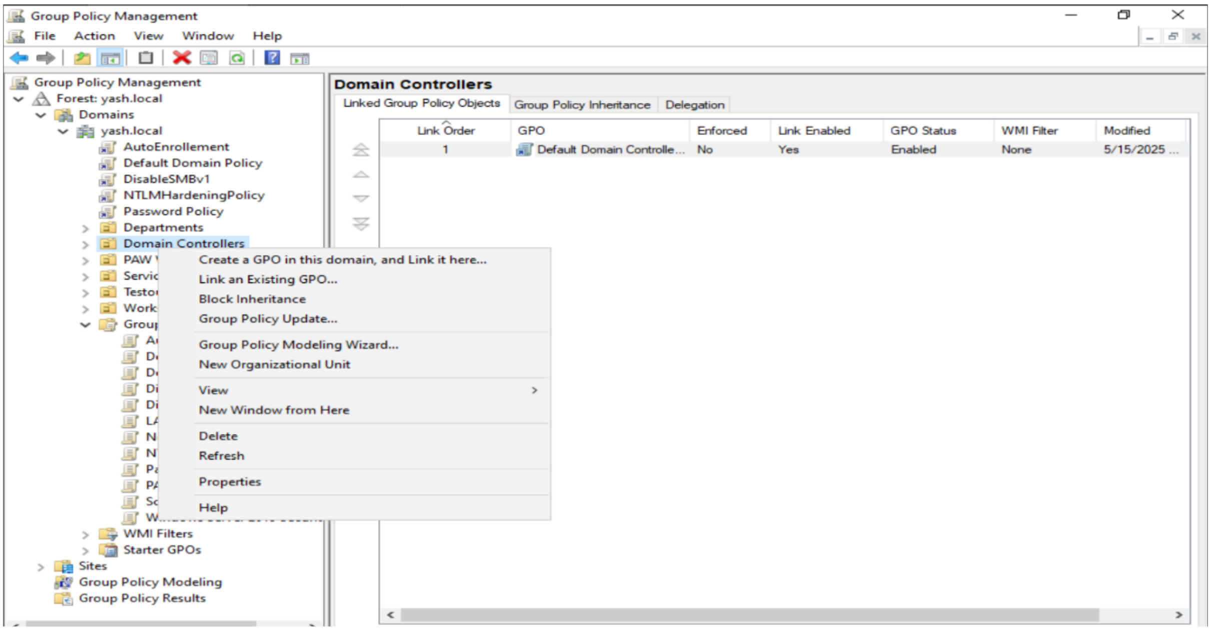


Import progress:

Status:

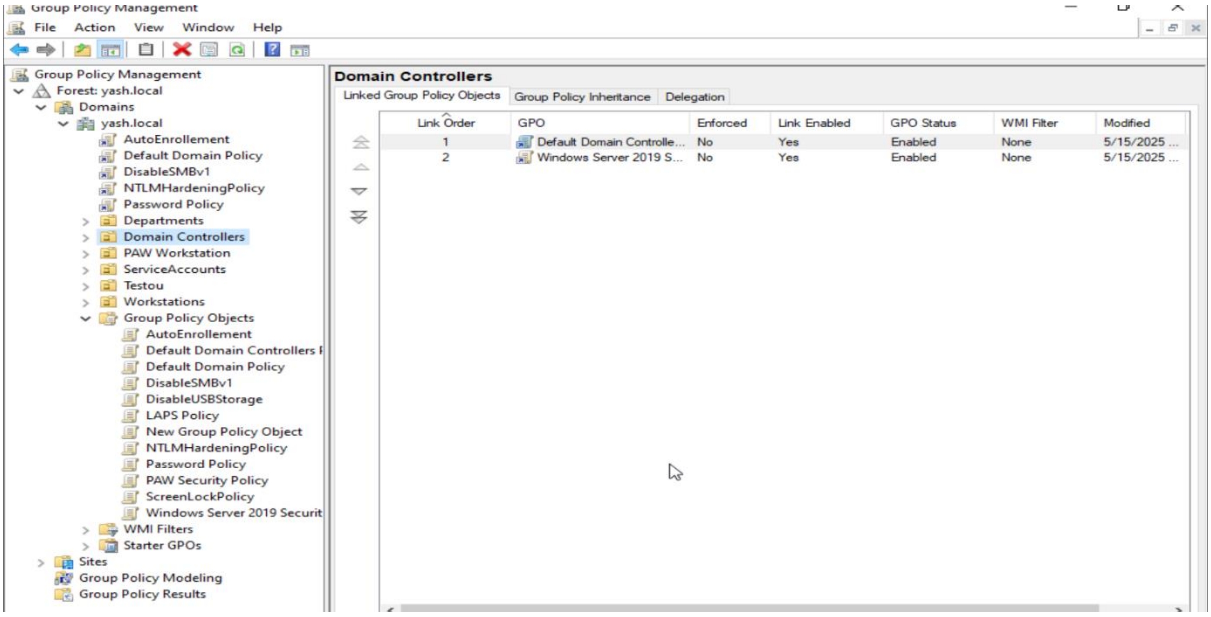
GPO: Windows Server 2019 Security Baseline...Succeeded

(Link the GPO to this OU.)



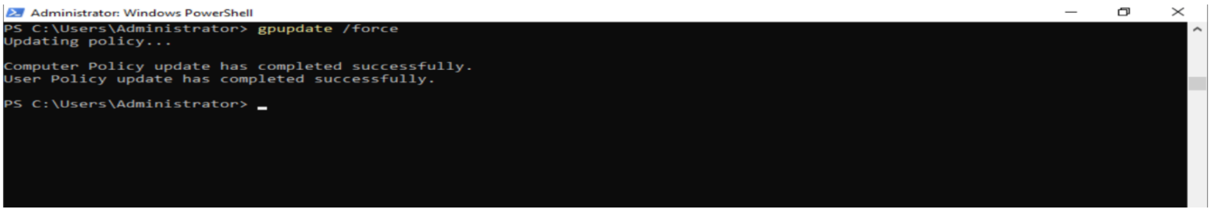
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified
1	Default Domain Controlle...	No	Yes	Enabled	None	5/15/2025 ...

(Verify the linked GPO.)



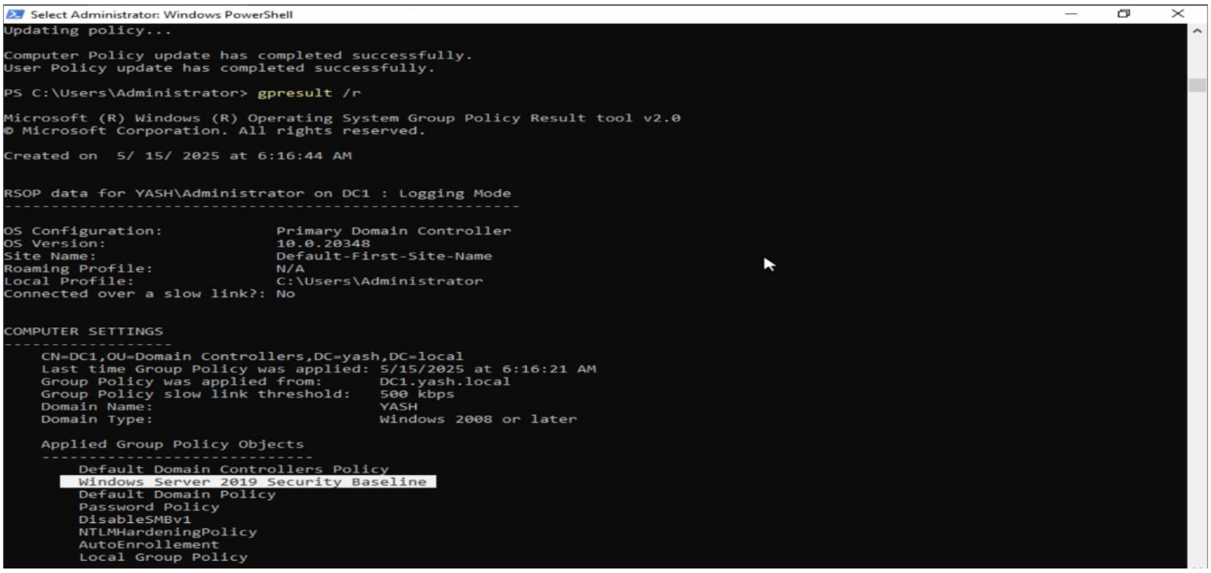
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified
1	Default Domain Controlle...	No	Yes	Enabled	None	5/15/2025 ...
2	Windows Server 2019 S...	No	Yes	Enabled	None	5/15/2025 ...

(Updated the policy.)



```
PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator> _
```

(As we can see the policy is updated successfully.)

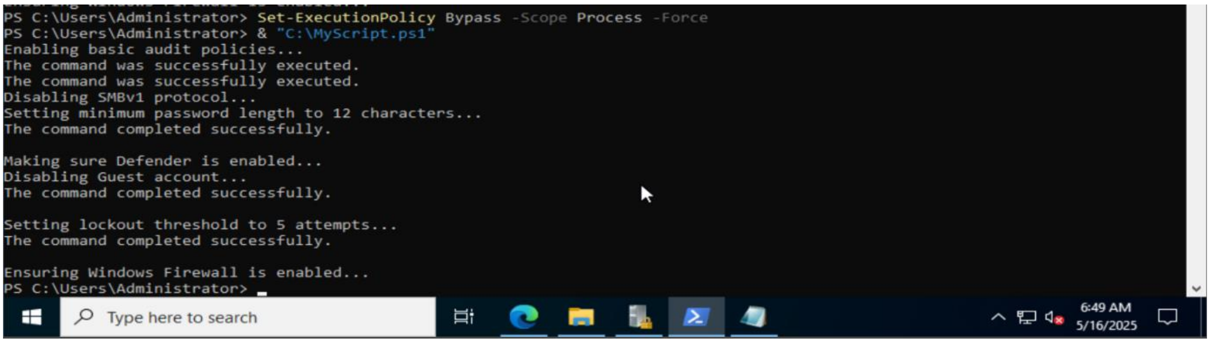


```
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  5/ 15/ 2025 at 6:16:44 AM


RSOP data for YASH\Administrator on DC1 : Logging Mode
-------------------------------------------------------

OS Configuration:            Primary Domain Controller
OS Version:                  10.0.20348
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\Administrator
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=DC1,OU=Domain Controllers,DC=yash,DC=local
    Last time Group Policy was applied: 5/15/2025 at 6:16:21 AM
    Group Policy was applied from:      DC1.yash.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        YASH
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        Default Domain Controllers Policy
        Windows Server 2019 Security Baseline
        Default Domain Policy
        Password Policy
        DisableSMBv1
        NTLMHardeningPolicy
        AutoEnrollement
        Local Group Policy
```

3.2 Harden Domain Controllers Using NSA Benchmarks

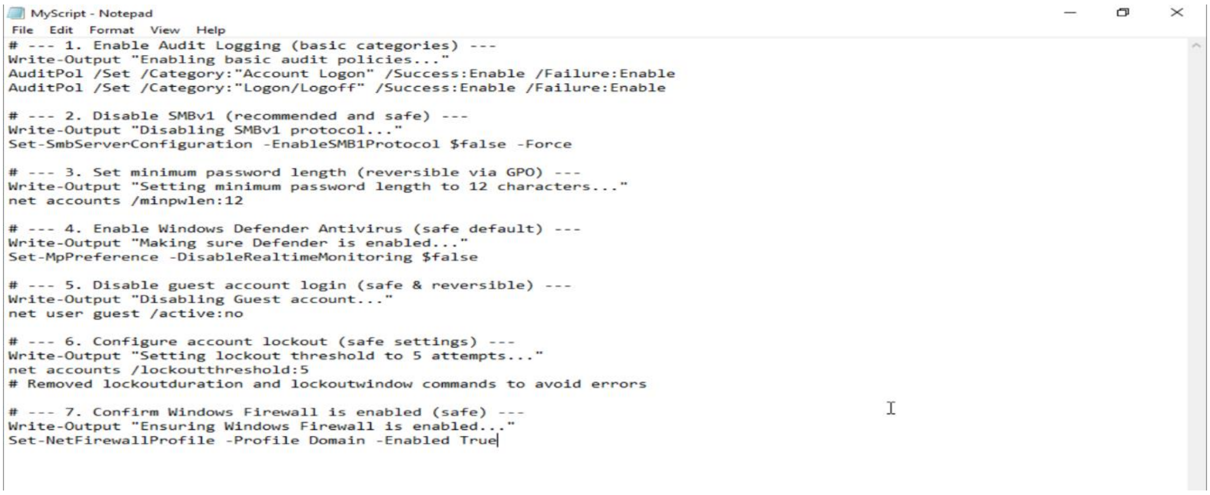
Level 1 Center for Internet Security (CIS) controls were applied to the domain controller through a PowerShell script. Key configurations verified included enforcement of a complex password policy, restrictions on NTLM authentication, SMB signing enforcement, audit policies, and user rights assignments. Domain controller services, network shares, and user accounts were checked to ensure alignment with CIS benchmark guidelines.

(Done hardening using the script.)



```
PS C:\Users\Administrator> Set-ExecutionPolicy Bypass -Scope Process -Force
PS C:\Users\Administrator> & "C:\MyScript.ps1"
Enabling basic audit policies...
The command was successfully executed.
The command was successfully executed.
Disabling SMBv1 protocol...
Setting minimum password length to 12 characters...
The command completed successfully.

Making sure Defender is enabled...
Disabling Guest account...
The command completed successfully.

Setting lockout threshold to 5 attempts...
The command completed successfully.

Ensuring Windows Firewall is enabled...
PS C:\Users\Administrator> _
```

(The script I used.)

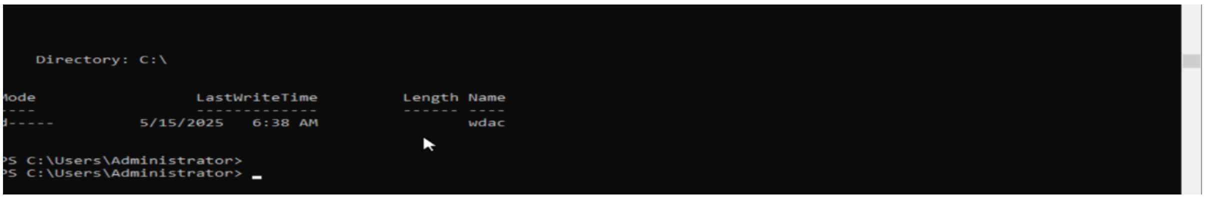


```
# --- 1. Enable Audit Logging (basic categories) ---
Write-Output "Enabling basic audit policies..."
AuditPol /Set /Category:"Account Logon" /Success:Enable /Failure:Enable
AuditPol /Set /Category:"Logon/Logoff" /Success:Enable /Failure:Enable

# --- 2. Disable SMBv1 (recommended and safe) ---
Write-Output "Disabling SMBv1 protocol..."
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force

# --- 3. Set minimum password length (reversible via GPO) ---
Write-Output "Setting minimum password length to 12 characters..."
net accounts /minpwlen:12

# --- 4. Enable Windows Defender Antivirus (safe default) ---
Write-Output "Making sure Defender is enabled..."
Set-MpPreference -DisableRealtimeMonitoring $false

# --- 5. Disable guest account login (safe & reversible) ---
Write-Output "Disabling Guest account..."
net user guest /active:no

# --- 6. Configure account lockout (safe settings) ---
Write-Output "Setting lockout threshold to 5 attempts..."
net accounts /lockoutthreshold:5
# Removed lockoutduration and lockoutwindow commands to avoid errors

# --- 7. Confirm Windows Firewall is enabled (safe) ---
Write-Output "Ensuring Windows Firewall is enabled..."
Set-NetFirewallProfile -Profile Domain -Enabled True
```

3.3 Implement Windows Defender Application Control (WDAC)

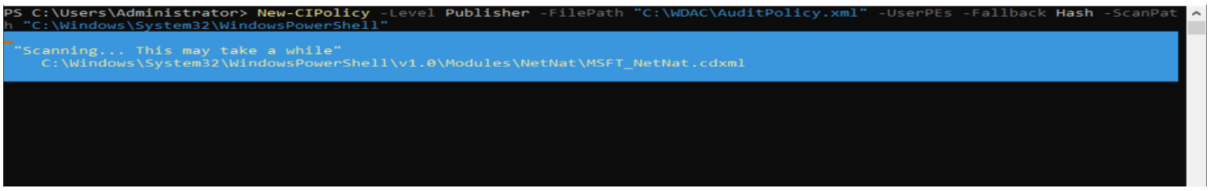
- Open Windows PowerShell as Administrator on the target system.
- Create a WDAC policy XML file using New-CIPolicy cmdlet to define allowed applications and scripts.
- Convert the XML to a binary policy file using ConvertFrom-CIPolicy.
- Deploy the WDAC policy via Group Policy or by placing the policy file in the system's CodeIntegrity folder.
- Reboot the system and monitor WDAC enforcement via Event Viewer logs (Microsoft-Windows-CodeIntegrity/Operational).

(Created a folder in C.)

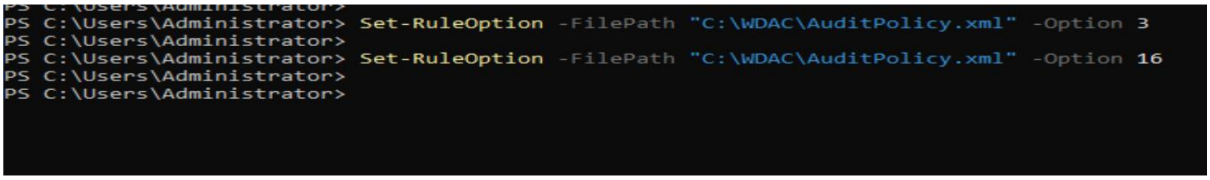


```
    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/15/2025   6:38 AM                wdac


PS C:\Users\Administrator>
PS C:\Users\Administrator> _
```

(Created WDAC policy.)

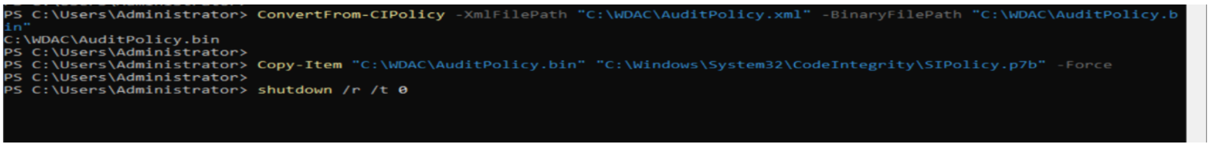


```
PS C:\Users\Administrator> New-CIPolicy -Level Publisher -FilePath "C:\WDAC\AuditPolicy.xml" -UserPEs -Fallback Hash -ScanPat
h "C:\Windows\System32\WindowsPowerShell"

 "Scanning... This may take a while"
    C:\Windows\System32\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml
```



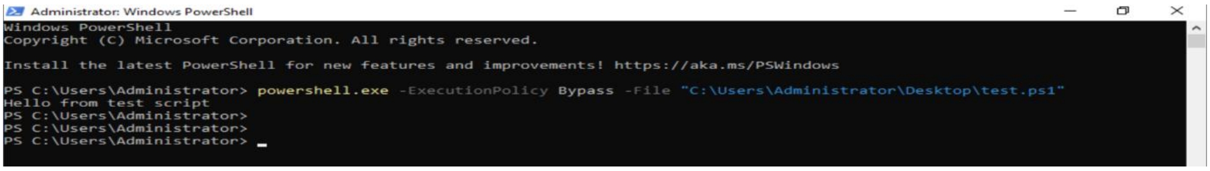
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Set-RuleOption -FilePath "C:\WDAC\AuditPolicy.xml" -Option 3
PS C:\Users\Administrator>
PS C:\Users\Administrator> Set-RuleOption -FilePath "C:\WDAC\AuditPolicy.xml" -Option 16
PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

(Convert it to binary.)



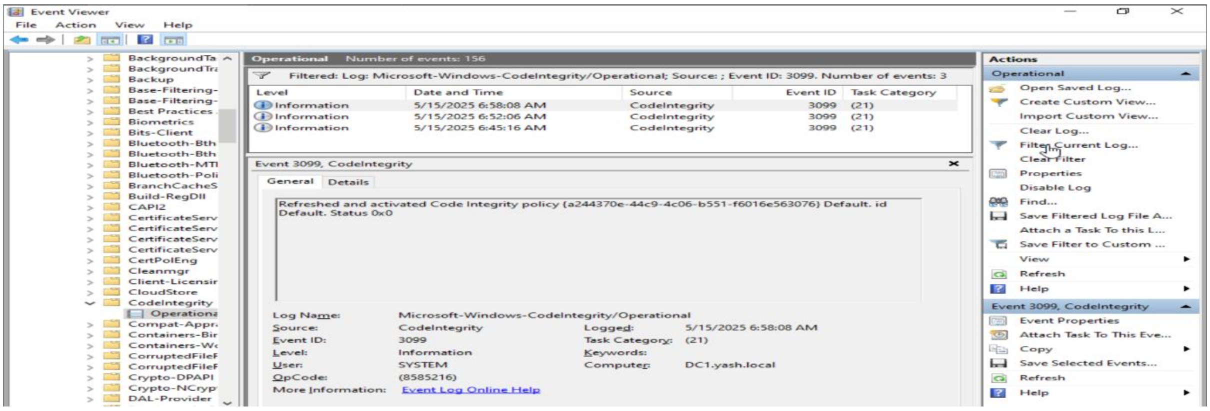
```
PS C:\Users\Administrator> ConvertFrom-CIPolicy -XmlFilePath "C:\WDAC\AuditPolicy.xml" -BinaryFilePath "C:\WDAC\AuditPolicy.b
in"
C:\WDAC\AuditPolicy.bin
PS C:\Users\Administrator>
PS C:\Users\Administrator> Copy-Item "C:\WDAC\AuditPolicy.bin" "C:\Windows\System32\CodeIntegrity\SIPolicy.p7b" -Force
PS C:\Users\Administrator>
PS C:\Users\Administrator> shutdown /r /t 0
```

(Run a script.)



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> powershell.exe -ExecutionPolicy Bypass -File "C:\Users\Administrator\Desktop\test.ps1"
Hello from test script
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> _
```

(Logs with event id 3099.)



Operational Number of events: 156

Filtered: Log: Microsoft-Windows-CodeIntegrity/Operational; Source: ; Event ID: 3099. Number of events: 3

Level	Date and Time	Source	Event ID	Task Category
Information	5/15/2025 6:58:08 AM	CodeIntegrity	3099	(21)
Information	5/15/2025 6:52:06 AM	CodeIntegrity	3099	(21)
Information	5/15/2025 6:45:16 AM	CodeIntegrity	3099	(21)

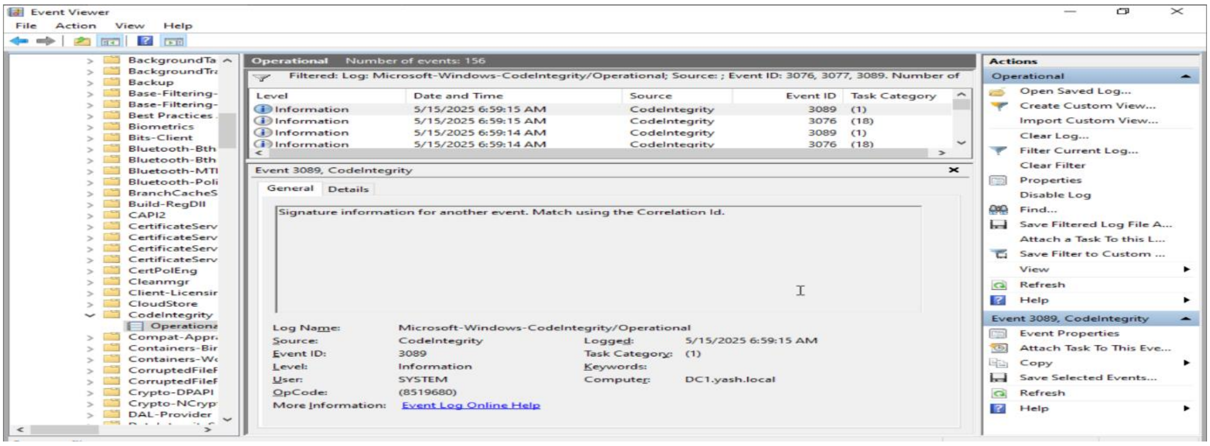
Event 3099, CodeIntegrity

General Details

Refreshed and activated Code Integrity policy {a244370e-44c9-4c06-b551-f6016e563076} Default. id Default. Status 0x0

Log Name: Microsoft-Windows-CodeIntegrity/Operational
Source: CodeIntegrity Logged: 5/15/2025 6:58:08 AM
Event ID: 3099 Task Category: (21)
Level: Information Keywords:
User: SYSTEM Computer: DC1.yash.local
OpCode: (8585216)
More Information: Event Log Online Help

(Now we can see the logs 3076 , 3077 , 3089 event ids)



Operational Number of events: 156

Filtered: Log: Microsoft-Windows-CodeIntegrity/Operational; Source: ; Event ID: 3076, 3077, 3089. Number of

Level	Date and Time	Source	Event ID	Task Category
Information	5/15/2025 6:59:15 AM	CodeIntegrity	3089	(1)
Information	5/15/2025 6:59:15 AM	CodeIntegrity	3076	(18)
Information	5/15/2025 6:59:14 AM	CodeIntegrity	3089	(1)
Information	5/15/2025 6:59:14 AM	CodeIntegrity	3076	(18)

Event 3089, CodeIntegrity

General Details

Signature information for another event. Match using the Correlation Id.

Log Name: Microsoft-Windows-CodeIntegrity/Operational
Source: CodeIntegrity Logged: 5/15/2025 6:59:15 AM
Event ID: 3089 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: DC1.yash.local
OpCode: (8519680)
More Information: Event Log Online Help

3.4 Conduct a Mock Active Directory Security Audit

- Use PowerShell scripts or tools like **BloodHound**, **PingCastle**, or **ADAudit** to collect AD security data.
- Review critical areas such as:

  User and group permissions (especially privileged groups)

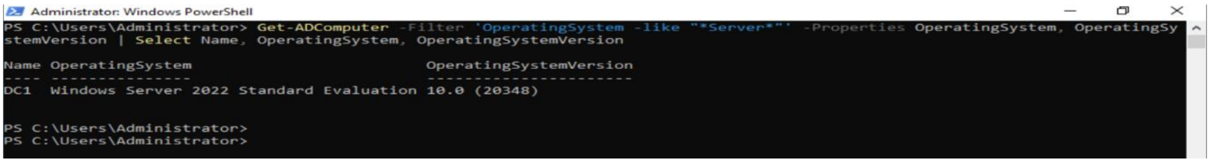
  Password policies and account lockout settings

  Delegated administrative rights and service accounts

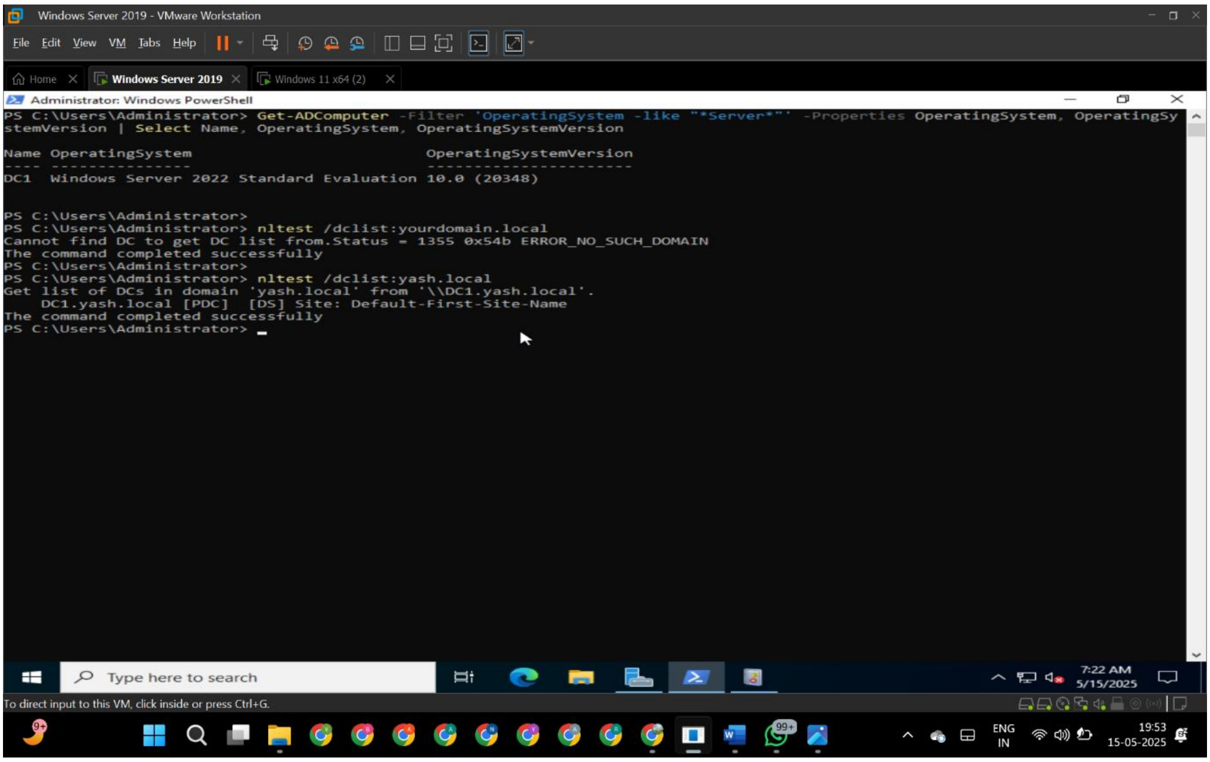
  Audit policy configurations and log retention settings

- Document findings highlighting security gaps, policy violations, or weak configurations.
- Provide actionable recommendations based on findings to improve AD security posture.

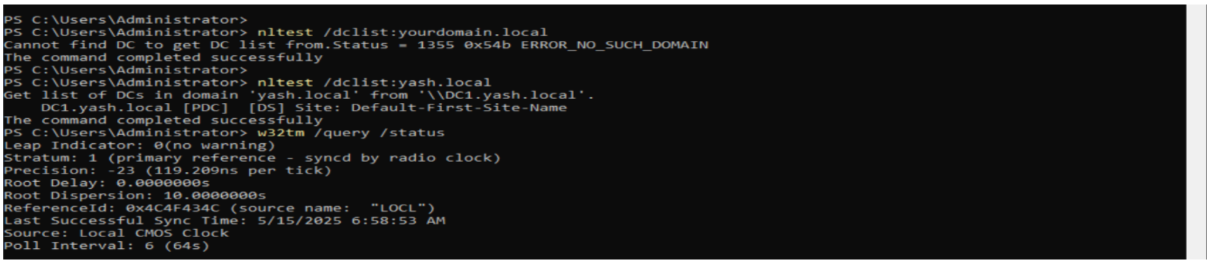
(We completed a Mock Security Audit)



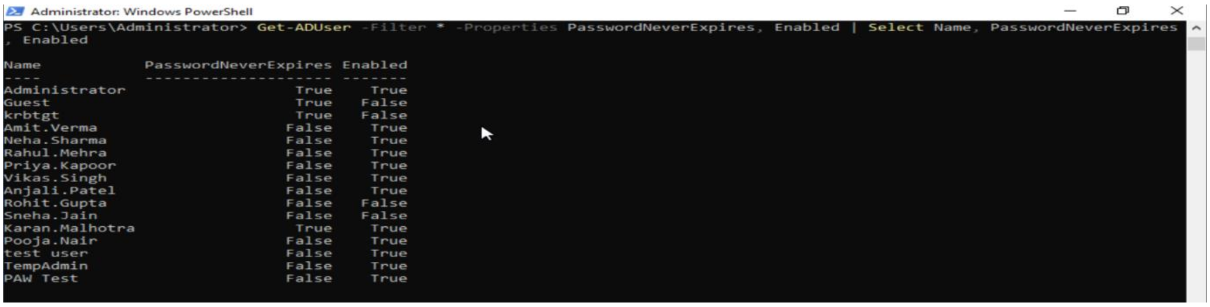
```
PS C:\Users\Administrator> Get-ADComputer -Filter 'OperatingSystem -like "*Server*"' -Properties OperatingSystem, OperatingSy
stemVersion | Select Name, OperatingSystem, OperatingSystemVersion

Name OperatingSystem                         OperatingSystemVersion
---- ---------------                         ----------------------
DC1  Windows Server 2022 Standard Evaluation 10.0 (20348)


PS C:\Users\Administrator>
PS C:\Users\Administrator>
```


Windows Server 2019 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
Windows Server 2019
Windows 11 x64 (2)
Administrator: Windows PowerShell
Type here to search
7:22 AM
5/15/2025
To direct input to this VM, click inside or press Ctrl+G.
ENG
IN
19:53
15-05-2025

```
PS C:\Users\Administrator> Get-ADComputer -Filter 'OperatingSystem -like "*Server*"' -Properties OperatingSystem, OperatingSy
stemVersion | Select Name, OperatingSystem, OperatingSystemVersion

Name OperatingSystem                         OperatingSystemVersion
---- ---------------                         ----------------------
DC1  Windows Server 2022 Standard Evaluation 10.0 (20348)


PS C:\Users\Administrator>
PS C:\Users\Administrator> nltest /dclist:yourdomain.local
Cannot find DC to get DC list from.Status = 1355 0x54b ERROR_NO_SUCH_DOMAIN
The command completed successfully
PS C:\Users\Administrator>
PS C:\Users\Administrator> nltest /dclist:yash.local
Get list of DCs in domain 'yash.local' from '\\DC1.yash.local'.
    DC1.yash.local [PDC]  [DS] Site: Default-First-Site-Name
The command completed successfully
PS C:\Users\Administrator> _
```

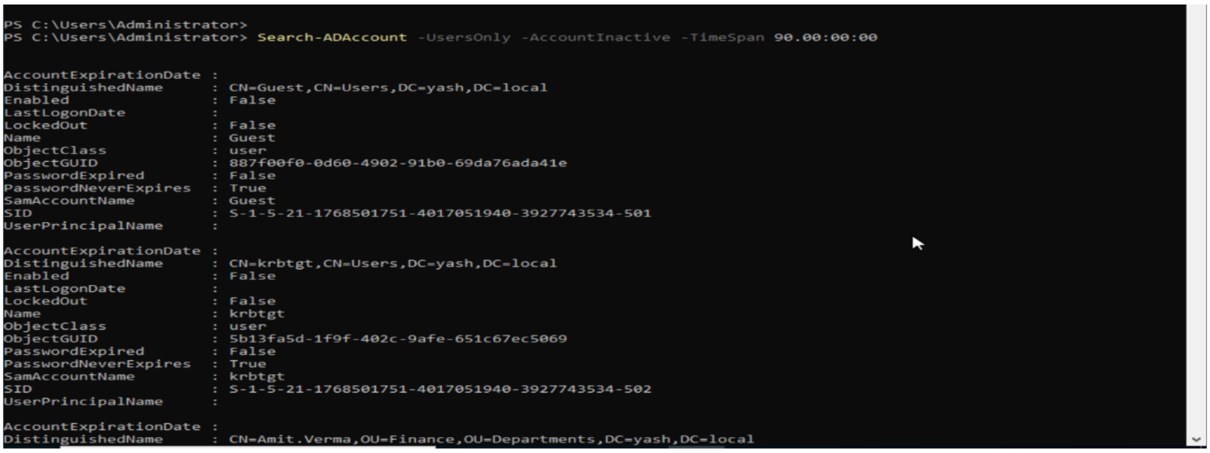


```
PS C:\Users\Administrator>
PS C:\Users\Administrator> nltest /dclist:yourdomain.local
Cannot find DC to get DC list from.Status = 1355 0x54b ERROR_NO_SUCH_DOMAIN
The command completed successfully
PS C:\Users\Administrator>
PS C:\Users\Administrator> nltest /dclist:yash.local
Get list of DCs in domain 'yash.local' from '\\DC1.yash.local'.
    DC1.yash.local [PDC]  [DS] Site: Default-First-Site-Name
The command completed successfully
PS C:\Users\Administrator> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 1 (primary reference - syncd by radio clock)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0000000s
Root Dispersion: 10.0000000s
ReferenceId: 0x4C4F434C (source name:  "LOCL")
Last Successful Sync Time: 5/15/2025 6:58:53 AM
Source: Local CMOS Clock
Poll Interval: 6 (64s)
```

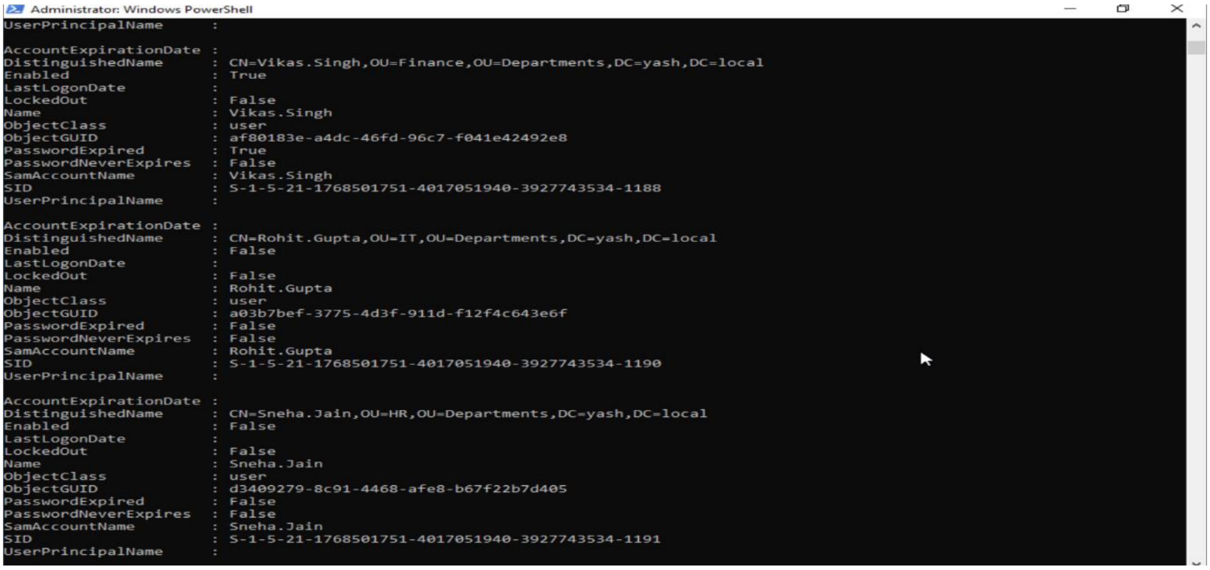


Administrator: Windows PowerShell

```
PS C:\Users\Administrator> Get-ADUser -Filter * -Properties PasswordNeverExpires, Enabled | Select Name, PasswordNeverExpires
, Enabled

Name              PasswordNeverExpires Enabled
----              -------------------- -------
Administrator                     True    True
Guest                             True   False
krbtgt                            True   False
Amit.Verma                       False    True
Neha.Sharma                      False    True
Rahul.Mehra                      False    True
Priya.Kapoor                     False    True
Vikas.Singh                      False    True
Anjali.Patel                     False    True
Rohit.Gupta                      False   False
Sneha.Jain                       False   False
Karan.Malhotra                    True    True
Pooja.Nair                       False    True
test user                        False    True
TempAdmin                        False    True
PAW Test                         False    True
```

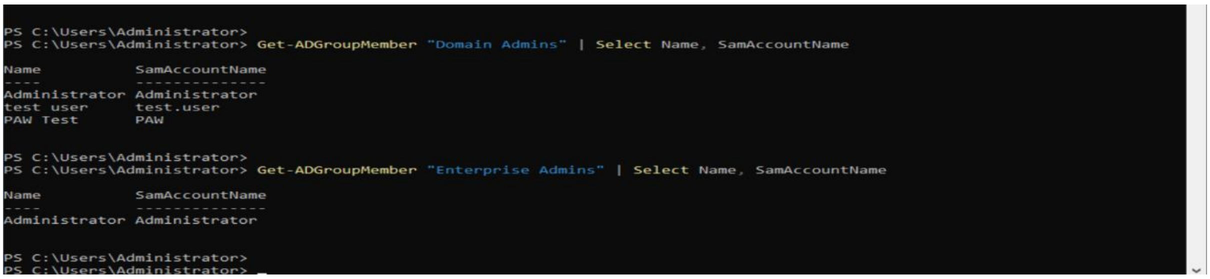


```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Search-ADAccount -UsersOnly -AccountInactive -TimeSpan 90.00:00:00


AccountExpirationDate :
DistinguishedName     : CN=Guest,CN=Users,DC=yash,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : Guest
ObjectClass           : user
ObjectGUID            : 887f00f0-0d60-4902-91b0-69da76ada41e
PasswordExpired       : False
PasswordNeverExpires  : True
SamAccountName        : Guest
SID                   : S-1-5-21-1768501751-4017051940-3927743534-501
UserPrincipalName     :

AccountExpirationDate :
DistinguishedName     : CN=krbtgt,CN=Users,DC=yash,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : krbtgt
ObjectClass           : user
ObjectGUID            : 5b13fa5d-1f9f-402c-9afe-651c67ec5069
PasswordExpired       : False
PasswordNeverExpires  : True
SamAccountName        : krbtgt
SID                   : S-1-5-21-1768501751-4017051940-3927743534-502
UserPrincipalName     :

AccountExpirationDate :
DistinguishedName     : CN=Amit.Verma,OU=Finance,OU=Departments,DC=yash,DC=local
```

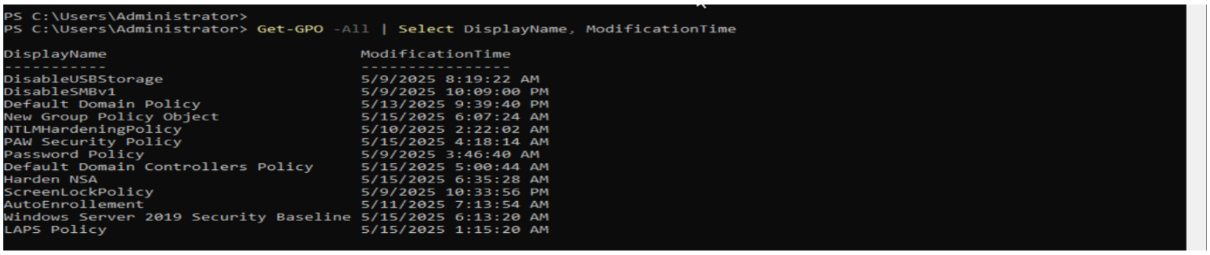


Administrator: Windows PowerShell

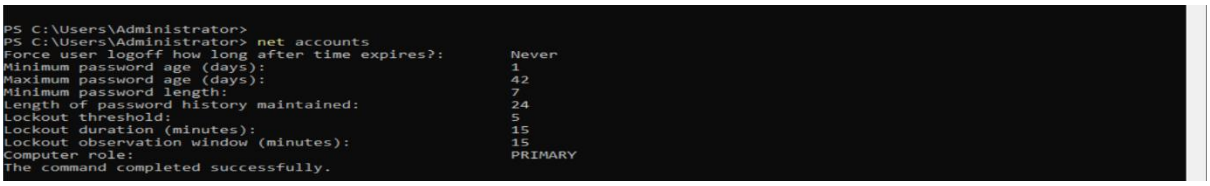
```
UserPrincipalName     :

AccountExpirationDate :
DistinguishedName     : CN=Vikas.Singh,OU=Finance,OU=Departments,DC=yash,DC=local
Enabled               : True
LastLogonDate         :
LockedOut             : False
Name                  : Vikas.Singh
ObjectClass           : user
ObjectGUID            : af80183e-a4dc-46fd-96c7-f041e42492e8
PasswordExpired       : True
PasswordNeverExpires  : False
SamAccountName        : Vikas.Singh
SID                   : S-1-5-21-1768501751-4017051940-3927743534-1188
UserPrincipalName     :

AccountExpirationDate :
DistinguishedName     : CN=Rohit.Gupta,OU=IT,OU=Departments,DC=yash,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : Rohit.Gupta
ObjectClass           : user
ObjectGUID            : a03b7bef-3775-4d3f-911d-f12f4c643e6f
PasswordExpired       : False
PasswordNeverExpires  : False
SamAccountName        : Rohit.Gupta
SID                   : S-1-5-21-1768501751-4017051940-3927743534-1190
UserPrincipalName     :

AccountExpirationDate :
DistinguishedName     : CN=Sneha.Jain,OU=HR,OU=Departments,DC=yash,DC=local
Enabled               : False
LastLogonDate         :
LockedOut             : False
Name                  : Sneha.Jain
ObjectClass           : user
ObjectGUID            : d3409279-8c91-4468-afe8-b67f22b7d405
PasswordExpired       : False
PasswordNeverExpires  : False
SamAccountName        : Sneha.Jain
SID                   : S-1-5-21-1768501751-4017051940-3927743534-1191
UserPrincipalName     :
```



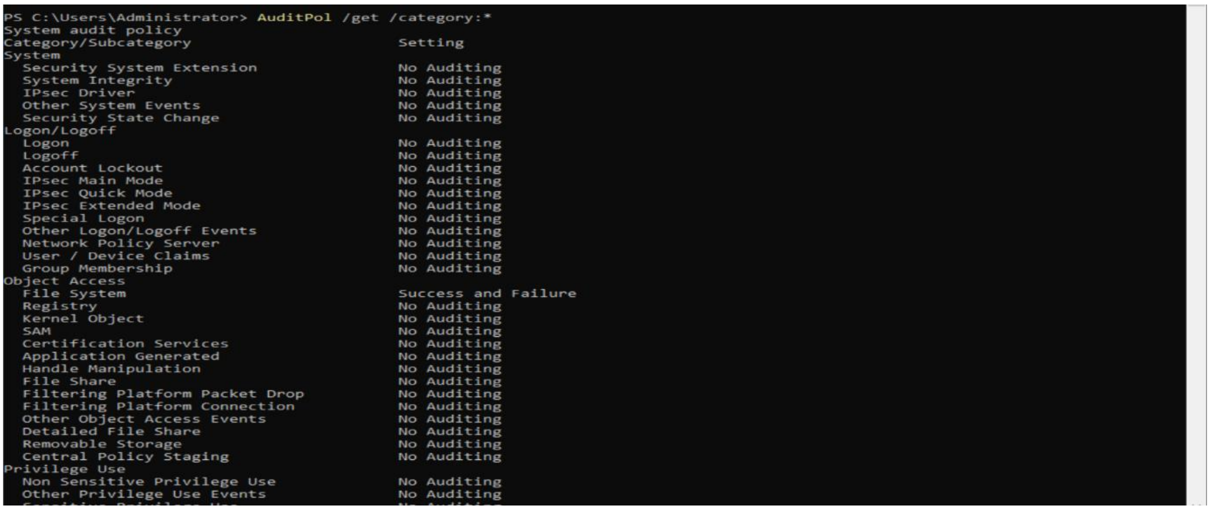
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADGroupMember "Domain Admins" | Select Name, SamAccountName

Name          SamAccountName
----          --------------
Administrator Administrator
test user     test.user
PAW Test      PAW


PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADGroupMember "Enterprise Admins" | Select Name, SamAccountName

Name          SamAccountName
----          --------------
Administrator Administrator


PS C:\Users\Administrator>
PS C:\Users\Administrator> _
```



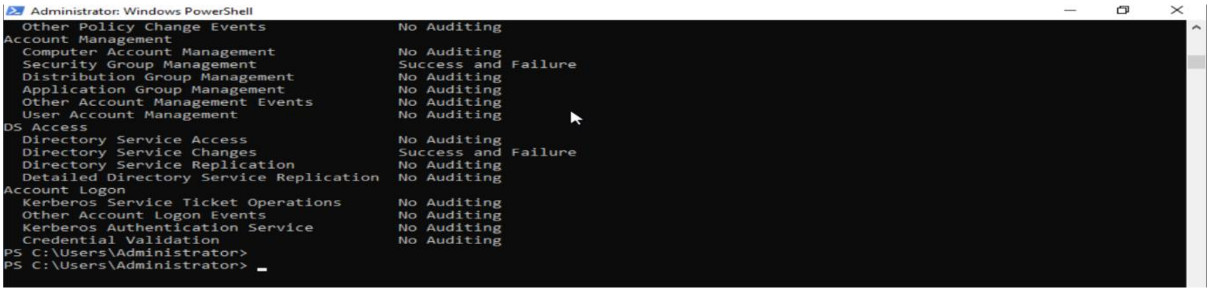
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-GPO -All | Select DisplayName, ModificationTime

DisplayName                          ModificationTime
-----------                          ----------------
DisableUSBStorage                    5/9/2025 8:19:22 AM
DisableSMBv1                         5/9/2025 10:09:00 PM
Default Domain Policy                5/13/2025 9:39:40 PM
New Group Policy Object              5/15/2025 6:07:24 AM
NTLMHardeningPolicy                  5/10/2025 2:22:02 AM
PAW Security Policy                  5/15/2025 4:18:14 AM
Password Policy                      5/9/2025 3:46:40 AM
Default Domain Controllers Policy    5/15/2025 5:00:44 AM
Harden NSA                           5/15/2025 6:35:28 AM
ScreenLockPolicy                     5/9/2025 10:33:56 PM
AutoEnrollement                      5/11/2025 7:13:54 AM
Windows Server 2019 Security Baseline 5/15/2025 6:13:20 AM
LAPS Policy                          5/15/2025 1:15:20 AM
```



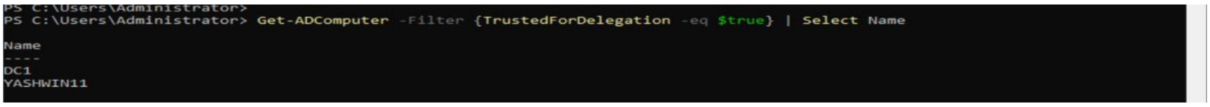
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          42
Minimum password length:                              7
Length of password history maintained:                24
Lockout threshold:                                    5
Lockout duration (minutes):                           15
Lockout observation window (minutes):                 15
Computer role:                                        PRIMARY
The command completed successfully.
```



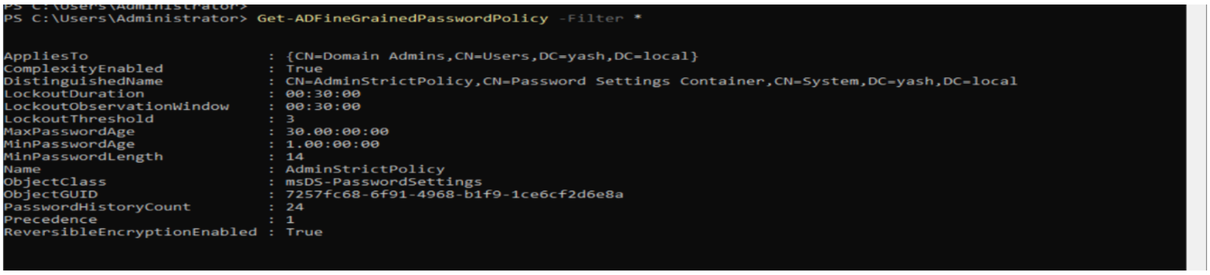
```
PS C:\Users\Administrator> AuditPol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   No Auditing
  Logoff                                  No Auditing
  Account Lockout                         No Auditing
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           No Auditing
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             Success and Failure
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
```



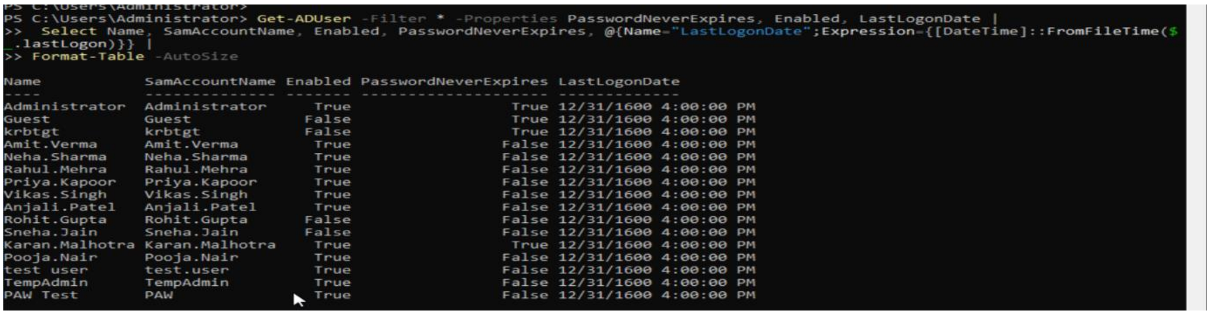
```
  Other Policy Change Events              No Auditing
Account Management
  Computer Account Management             No Auditing
  Security Group Management               Success and Failure
  Distribution Group Management           No Auditing
  Application Group Management            No Auditing
  Other Account Management Events         No Auditing
  User Account Management                 No Auditing
DS Access
  Directory Service Access                No Auditing
  Directory Service Changes               Success and Failure
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations      No Auditing
  Other Account Logon Events              No Auditing
  Kerberos Authentication Service         No Auditing
  Credential Validation                   No Auditing
PS C:\Users\Administrator>
PS C:\Users\Administrator> _
```



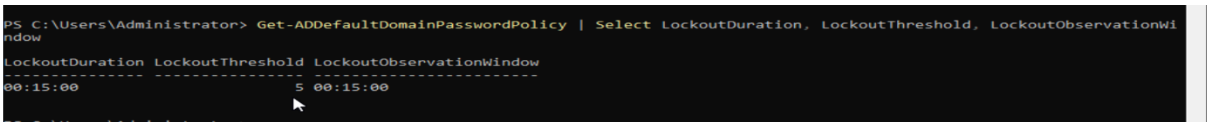
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADComputer -Filter {TrustedForDelegation -eq $true} | Select Name

Name
----
DC1
YASHWIN11
```



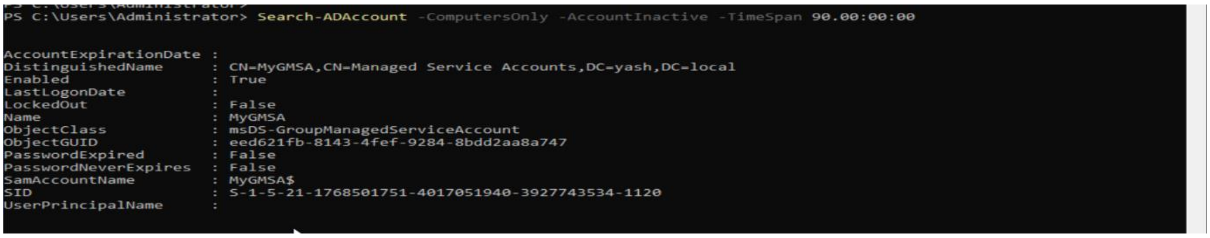
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADFineGrainedPasswordPolicy -Filter *


AppliesTo                   : {CN=Domain Admins,CN=Users,DC=yash,DC=local}
ComplexityEnabled           : True
DistinguishedName           : CN=AdminStrictPolicy,CN=Password Settings Container,CN=System,DC=yash,DC=local
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 3
MaxPasswordAge              : 30.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 14
Name                        : AdminStrictPolicy
ObjectClass                 : msDS-PasswordSettings
ObjectGUID                  : 7257fc68-6f91-4968-b1f9-1ce6cf2d6e8a
PasswordHistoryCount        : 24
Precedence                  : 1
ReversibleEncryptionEnabled : True
```



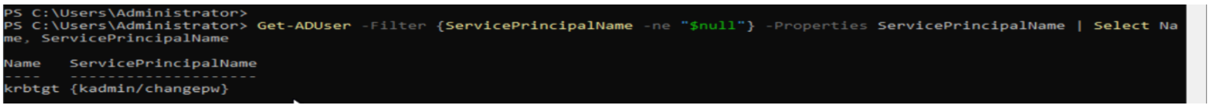
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADUser -Filter * -Properties PasswordNeverExpires, Enabled, LastLogonDate |
>>  Select Name, SamAccountName, Enabled, PasswordNeverExpires, @{Name="LastLogonDate";Expression={[DateTime]::FromFileTime($
_.lastLogon)}} |
>> Format-Table -AutoSize

Name            SamAccountName Enabled PasswordNeverExpires LastLogonDate
----            -------------- ------- -------------------- -------------
Administrator   Administrator     True                 True 12/31/1600 4:00:00 PM
Guest           Guest            False                 True 12/31/1600 4:00:00 PM
krbtgt          krbtgt           False                 True 12/31/1600 4:00:00 PM
Amit.Verma      Amit.Verma        True                False 12/31/1600 4:00:00 PM
Neha.Sharma     Neha.Sharma       True                False 12/31/1600 4:00:00 PM
Rahul.Mehra     Rahul.Mehra       True                False 12/31/1600 4:00:00 PM
Priya.Kapoor    Priya.Kapoor      True                False 12/31/1600 4:00:00 PM
Vikas.Singh     Vikas.Singh       True                False 12/31/1600 4:00:00 PM
Anjali.Patel    Anjali.Patel      True                False 12/31/1600 4:00:00 PM
Rohit.Gupta     Rohit.Gupta      False                False 12/31/1600 4:00:00 PM
Sneha.Jain      Sneha.Jain       False                False 12/31/1600 4:00:00 PM
Karan.Malhotra  Karan.Malhotra    True                 True 12/31/1600 4:00:00 PM
Pooja.Nair      Pooja.Nair        True                False 12/31/1600 4:00:00 PM
test user       test.user         True                False 12/31/1600 4:00:00 PM
TempAdmin       TempAdmin         True                False 12/31/1600 4:00:00 PM
PAW Test        PAW               True                False 12/31/1600 4:00:00 PM
```



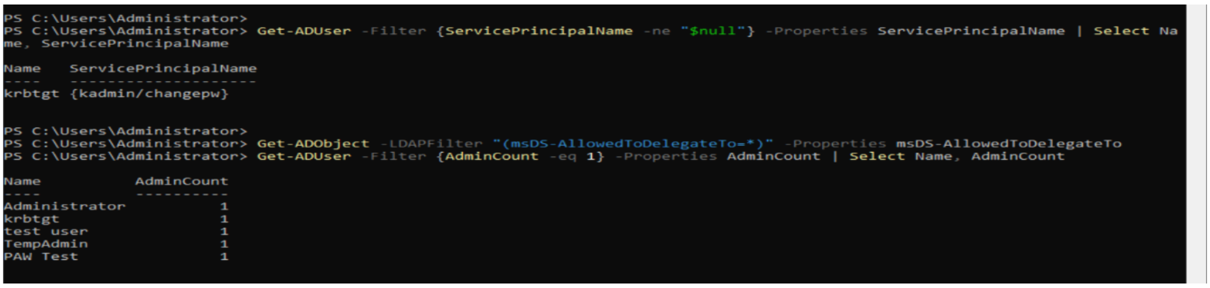
```
PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy | Select LockoutDuration, LockoutThreshold, LockoutObservationWi
ndow

LockoutDuration LockoutThreshold LockoutObservationWindow
--------------- ---------------- ------------------------
00:15:00                       5 00:15:00
```



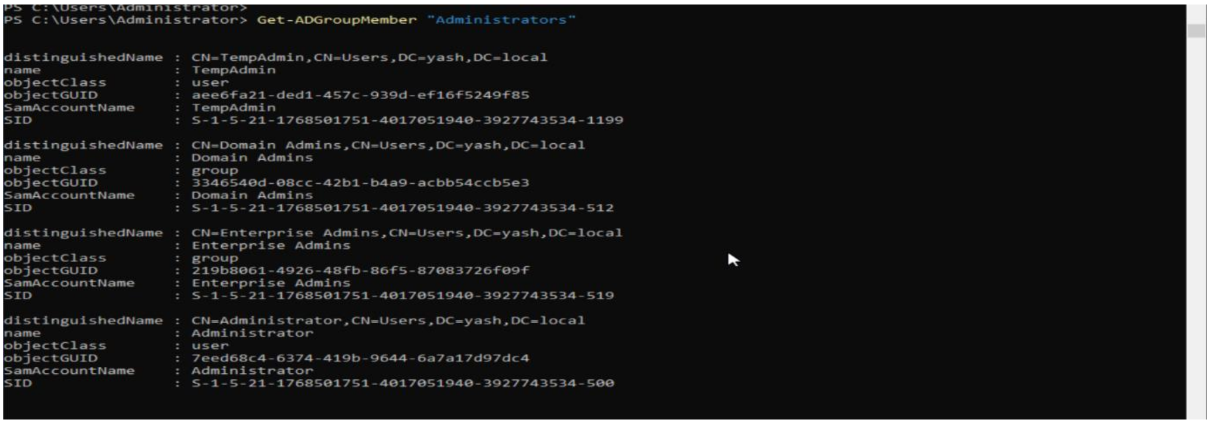
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Search-ADAccount -ComputersOnly -AccountInactive -TimeSpan 90.00:00:00


AccountExpirationDate :
DistinguishedName     : CN=MyGMSA,CN=Managed Service Accounts,DC=yash,DC=local
Enabled               : True
LastLogonDate         :
LockedOut             : False
Name                  : MyGMSA
ObjectClass           : msDS-GroupManagedServiceAccount
ObjectGUID            : eed621fb-8143-4fef-9284-8bdd2aa8a747
PasswordExpired       : False
PasswordNeverExpires  : False
SamAccountName        : MyGMSA$
SID                   : S-1-5-21-1768501751-4017051940-3927743534-1120
UserPrincipalName     :
```



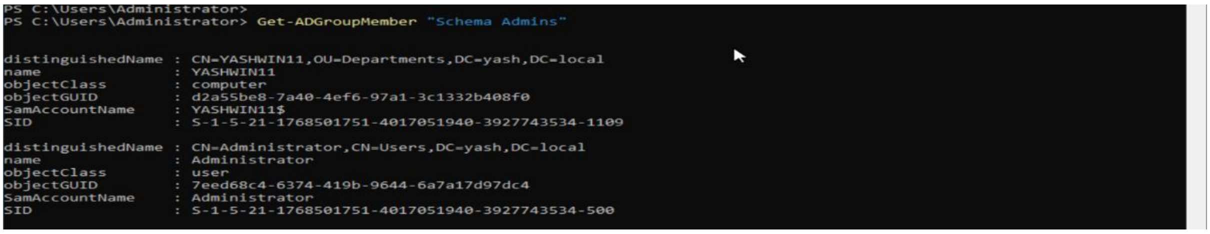
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName | Select Na
me, ServicePrincipalName

Name   ServicePrincipalName
----   --------------------
krbtgt {kadmin/changepw}
```



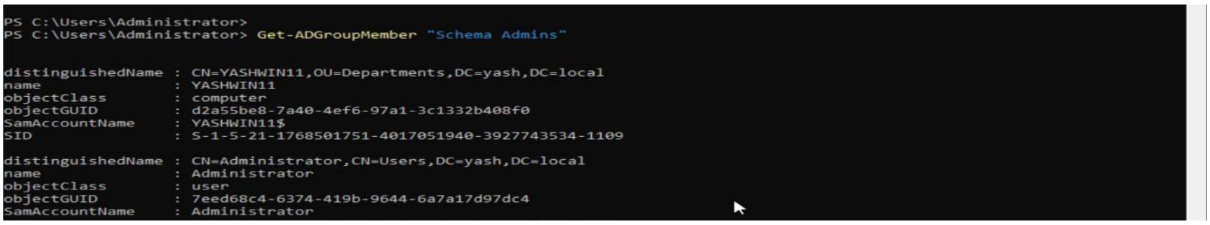
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName | Select Na
me, ServicePrincipalName

Name   ServicePrincipalName
----   --------------------
krbtgt {kadmin/changepw}


PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADObject -LDAPFilter "(msDS-AllowedToDelegateTo=*)" -Properties msDS-AllowedToDelegateTo
PS C:\Users\Administrator> Get-ADUser -Filter {AdminCount -eq 1} -Properties AdminCount | Select Name, AdminCount

Name          AdminCount
----          ----------
Administrator          1
krbtgt                 1
test user              1
TempAdmin              1
PAW Test               1
```



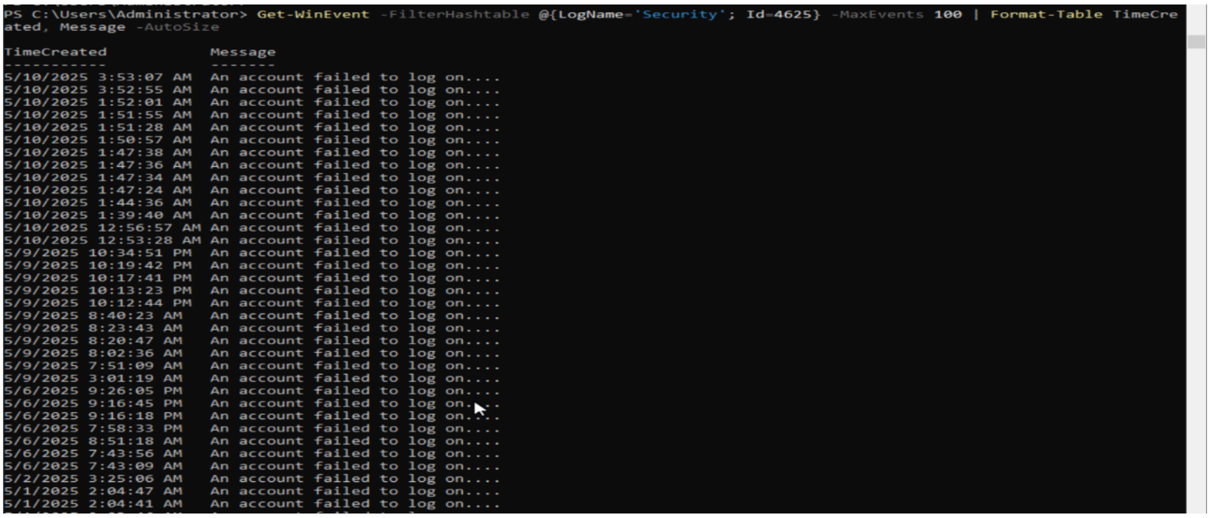
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADGroupMember "Administrators"


distinguishedName : CN=TempAdmin,CN=Users,DC=yash,DC=local
name              : TempAdmin
objectClass       : user
objectGUID        : aee6fa21-ded1-457c-939d-ef16f5249f85
SamAccountName    : TempAdmin
SID               : S-1-5-21-1768501751-4017051940-3927743534-1199

distinguishedName : CN=Domain Admins,CN=Users,DC=yash,DC=local
name              : Domain Admins
objectClass       : group
objectGUID        : 3346540d-08cc-42b1-b4a9-acbb54ccb5e3
SamAccountName    : Domain Admins
SID               : S-1-5-21-1768501751-4017051940-3927743534-512

distinguishedName : CN=Enterprise Admins,CN=Users,DC=yash,DC=local
name              : Enterprise Admins
objectClass       : group
objectGUID        : 219b8061-4926-48fb-86f5-87083726f09f
SamAccountName    : Enterprise Admins
SID               : S-1-5-21-1768501751-4017051940-3927743534-519

distinguishedName : CN=Administrator,CN=Users,DC=yash,DC=local
name              : Administrator
objectClass       : user
objectGUID        : 7eed68c4-6374-419b-9644-6a7a17d97dc4
SamAccountName    : Administrator
SID               : S-1-5-21-1768501751-4017051940-3927743534-500
```



```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADGroupMember "Schema Admins"


distinguishedName : CN=YASHWIN11,OU=Departments,DC=yash,DC=local
name              : YASHWIN11
objectClass       : computer
objectGUID        : d2a55be8-7a40-4ef6-97a1-3c1332b408f0
SamAccountName    : YASHWIN11$
SID               : S-1-5-21-1768501751-4017051940-3927743534-1109

distinguishedName : CN=Administrator,CN=Users,DC=yash,DC=local
name              : Administrator
objectClass       : user
objectGUID        : 7eed68c4-6374-419b-9644-6a7a17d97dc4
SamAccountName    : Administrator
SID               : S-1-5-21-1768501751-4017051940-3927743534-500
```



```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADGroupMember "Schema Admins"


distinguishedName : CN=YASHWIN11,OU=Departments,DC=yash,DC=local
name              : YASHWIN11
objectClass       : computer
objectGUID        : d2a55be8-7a40-4ef6-97a1-3c1332b408f0
SamAccountName    : YASHWIN11$
SID               : S-1-5-21-1768501751-4017051940-3927743534-1109

distinguishedName : CN=Administrator,CN=Users,DC=yash,DC=local
name              : Administrator
objectClass       : user
objectGUID        : 7eed68c4-6374-419b-9644-6a7a17d97dc4
SamAccountName    : Administrator
```



```
PS C:\Users\Administrator> Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625} -MaxEvents 100 | Format-Table TimeCre
ated, Message -AutoSize

TimeCreated           Message
-----------           -------
5/10/2025 3:53:07 AM  An account failed to log on....
5/10/2025 3:52:55 AM  An account failed to log on....
5/10/2025 1:52:01 AM  An account failed to log on....
5/10/2025 1:51:55 AM  An account failed to log on....
5/10/2025 1:51:28 AM  An account failed to log on....
5/10/2025 1:50:57 AM  An account failed to log on....
5/10/2025 1:47:38 AM  An account failed to log on....
5/10/2025 1:47:36 AM  An account failed to log on....
5/10/2025 1:47:34 AM  An account failed to log on....
5/10/2025 1:47:24 AM  An account failed to log on....
5/10/2025 1:44:36 AM  An account failed to log on....
5/10/2025 1:39:40 AM  An account failed to log on....
5/10/2025 12:56:57 AM An account failed to log on....
5/10/2025 12:53:28 AM An account failed to log on....
5/9/2025 10:34:51 PM  An account failed to log on....
5/9/2025 10:19:42 PM  An account failed to log on....
5/9/2025 10:17:41 PM  An account failed to log on....
5/9/2025 10:13:23 PM  An account failed to log on....
5/9/2025 10:12:44 PM  An account failed to log on....
5/9/2025 8:40:23 AM   An account failed to log on....
5/9/2025 8:23:43 AM   An account failed to log on....
5/9/2025 8:20:47 AM   An account failed to log on....
5/9/2025 8:02:36 AM   An account failed to log on....
5/9/2025 7:51:09 AM   An account failed to log on....
5/9/2025 3:01:19 AM   An account failed to log on....
5/6/2025 9:26:05 PM   An account failed to log on....
5/6/2025 9:16:45 PM   An account failed to log on....
5/6/2025 9:16:18 PM   An account failed to log on....
5/6/2025 7:58:33 PM   An account failed to log on....
5/6/2025 8:51:18 AM   An account failed to log on....
5/6/2025 7:43:56 AM   An account failed to log on....
5/6/2025 7:43:09 AM   An account failed to log on....
5/2/2025 3:25:06 AM   An account failed to log on....
5/1/2025 2:04:47 AM   An account failed to log on....
5/1/2025 2:04:41 AM   An account failed to log on....
```

4. Results And Findings

This section presents the outcomes observed after implementing the security tasks, showing how the environment responded and confirming whether objectives were met.

4.1 **Implementation Success**

The security baselines and hardening configurations were successfully applied across target systems, reducing default vulnerabilities.

4.2 **Enhanced Domain Controller Security**

NSA/CIS benchmarks strengthened authentication and audit policies, improving the overall resilience of Domain Controllers.

4.3 **Effective Script Control**

Windows Defender Application Control prevented unauthorized script execution, reducing the risk of malware and untrusted code.

4.4 **Identified Security Gaps**

The mock Active Directory audit revealed weaknesses in user permissions and auditing policies that require attention.

4.5 **Improved Compliance Posture**

Systems showed greater alignment with industry best practices and compliance requirements after baseline enforcement.

5. Recommendations

This section suggests practical steps to further strengthen security based on findings.

5.1 **Automate Baseline Deployment**

Use automation tools to consistently apply and update security baselines across all relevant systems.

5.2 **Regularly Update Hardening Policies**

Keep NSA/CIS benchmarks and security policies current to address emerging threats and software updates.

5.3 **Expand WDAC Coverage**

Broaden Windows Defender Application Control policies to include additional endpoints and scripts.

5.4 **Schedule Periodic Security Audits**

Perform regular Active Directory audits to detect new vulnerabilities and ensure ongoing compliance.

5.5 **Train Staff on Security Best Practices**

Educate administrators and helpdesk staff on security protocols and the importance of least privilege principles.

6. Conclusion

In conclusion, the concerted efforts to apply Microsoft security baselines, harden domain controllers according to NSA and CIS benchmarks, implement Windows Defender Application Control, and conduct a thorough Active Directory security audit have collectively fortified the organization’s IT environment. These initiatives have not only mitigated known vulnerabilities but also established a proactive defense mechanism against emerging threats by enforcing strict access controls and reducing attack surfaces. The mock audit provided valuable insights into existing security gaps, enabling targeted remediation and continuous improvement. By aligning technical controls with industry best practices and compliance standards, the organization is better equipped to maintain regulatory adherence and safeguard critical infrastructure. This holistic approach enhances overall security posture, fosters accountability, and lays the groundwork for a resilient, secure, and well-governed IT ecosystem capable of withstanding evolving cyber challenges.