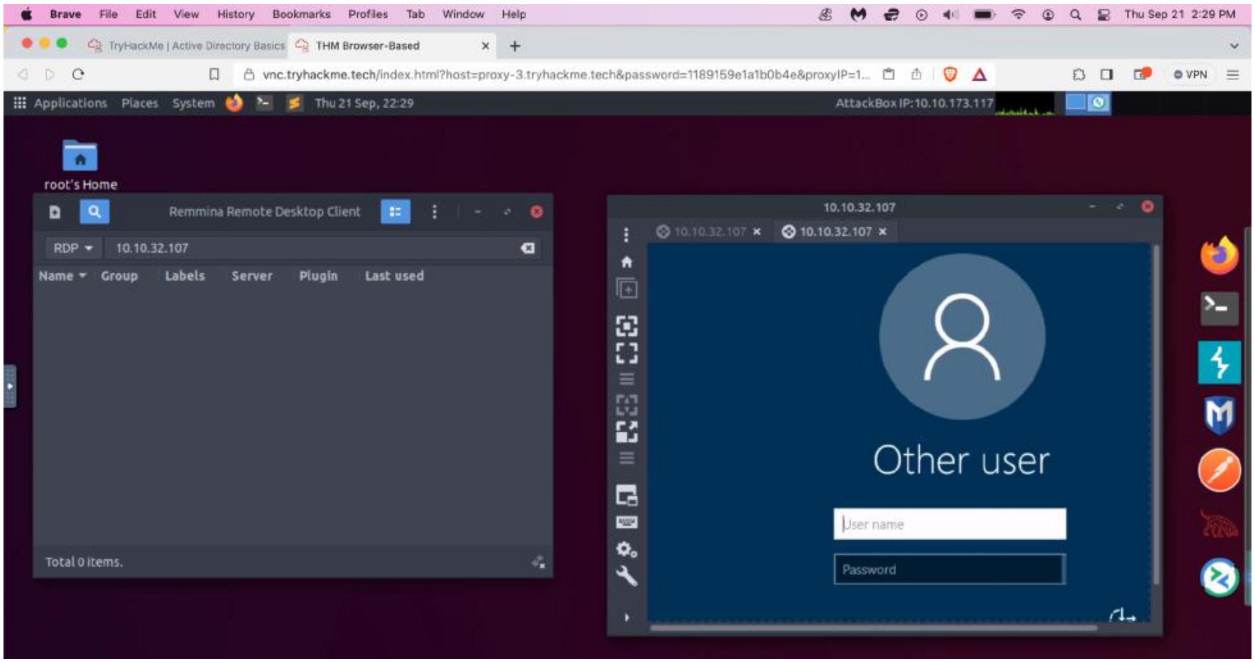
This mini lab focuses on the practice and conceptual basics of an active directory. We hear about active directory all the time on how it's so important for companies.

We will be using RDP , through Remina on the ubuntu to complete the tasks, if needed we can also use the windows virtual machine which has the active directory provided depending on convenience and capability.



Active Directory

Key Points - Active Directory Overview

- Active Directory Domain Service (AD DS) is the core of any Windows Domain, functioning as a catalog for network objects.

Users

- Users are common object types in Active Directory, categorized as security principals with authentication and resource privileges.
- Users can represent people (employees) or services (e.g., IIS or MSSQL).

Machines

- Machines are objects created for computers joining the Active Directory domain, also considered security principals.
- Machine accounts are local administrators with limited domain rights and automatically rotated, complex passwords.

Security Groups

- Security groups allow access rights to be assigned to groups instead of individual users, enhancing manageability.
- These groups are also considered security principals and can have privileges over network resources.
- Groups can include users and machines, and even other groups.
- Default security groups in a domain include Domain Admins, Server Operators, Backup Operators, Account Operators, Domain Users, Domain Computers, and Domain Controllers.

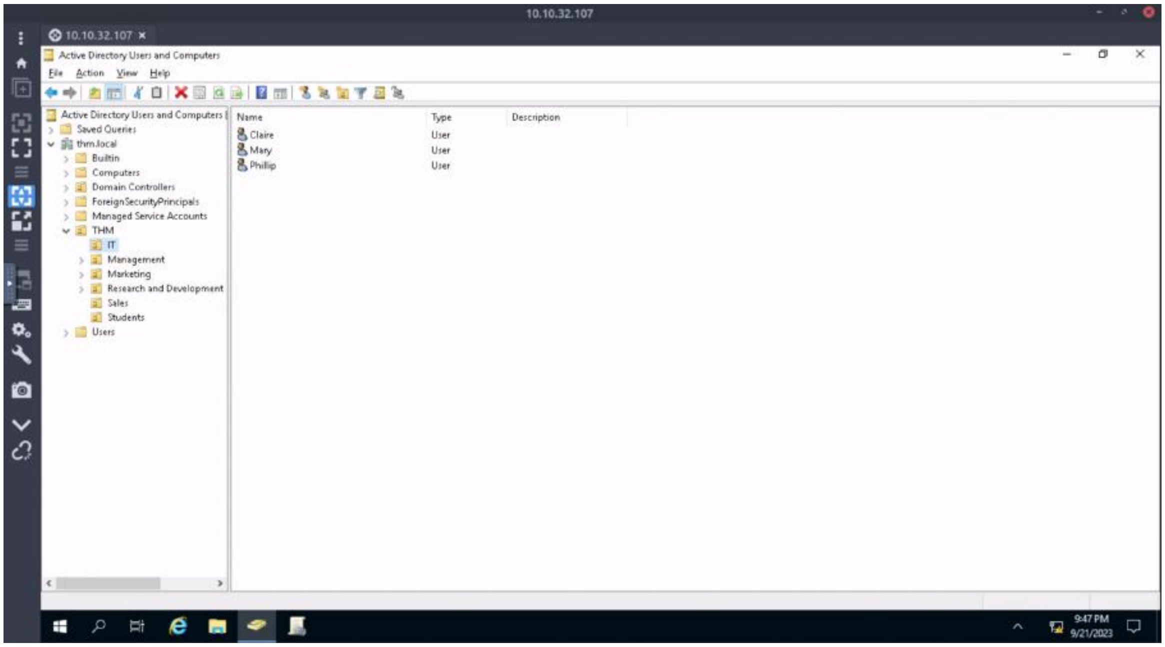
Active Directory Users and Computers

- To configure AD objects, use "Active Directory Users and Computers" on the Domain Controller.
- Objects are organized in Organizational Units (OUs), which classify users and machines for policy application.
- OUs help manage users with similar requirements, such as departmental policies.
- Users can belong to only one OU at a time.
- Example: THM OU with child OUs for different departments.

Security Groups vs OUs

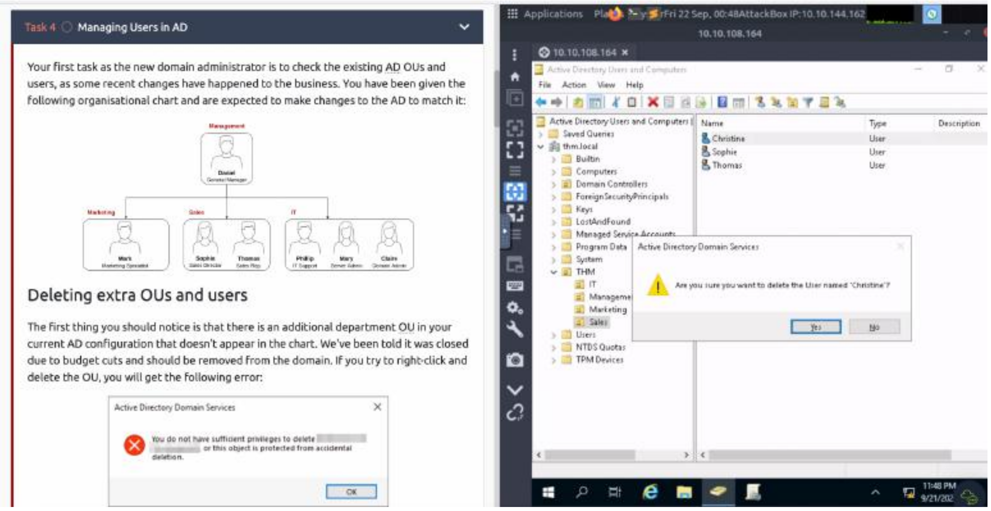
- OUs apply policies to users and computers based on their roles, with a user in only one OU.
- Security Groups grant permissions over resources, allowing users to access shared folders or network printers, with users in multiple groups.

Getting familiar with the general AD structure and the organizational unit, THM.



Name	Type	Description
Claire	User	
Mary	User	
Phillip	User	

First order of task was to delete any users in the Organizational unit that did not there, and also delete any extra Organizational units.



Task 4 ○ Managing Users in AD

Your first task as the new domain administrator is to check the existing AD OUs and users, as some recent changes have happened to the business. You have been given the following organisational chart and are expected to make changes to the AD to match it:

Deleting extra OUs and users

The first thing you should notice is that there is an additional department OU in your current AD configuration that doesn't appear in the chart. We've been told it was closed due to budget cuts and should be removed from the domain. If you try to right-click and delete the OU, you will get the following error:

Active Directory Domain Services

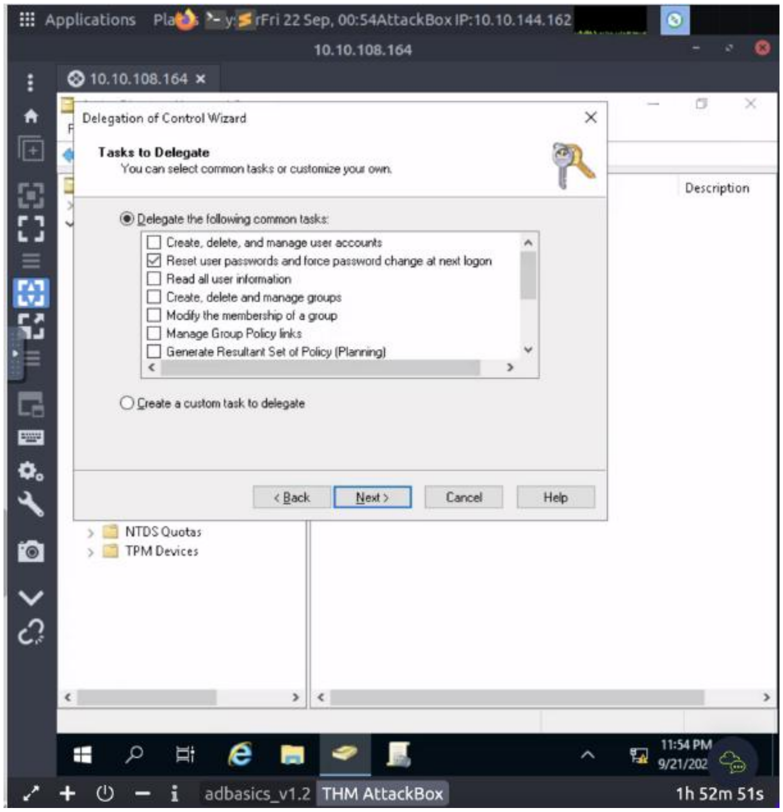
You do not have sufficient privileges to delete or this object is protected from accidental deletion.

Name	Type	Description
Christine	User	
Sophie	User	
Thomas	User	

Active Directory Domain Services

Are you sure you want to delete the User named 'Christine'?

Next we will delegate controls to the user phillip that will reset any password for the user in the sales department



Delegation of Control Wizard

Tasks to Delegate

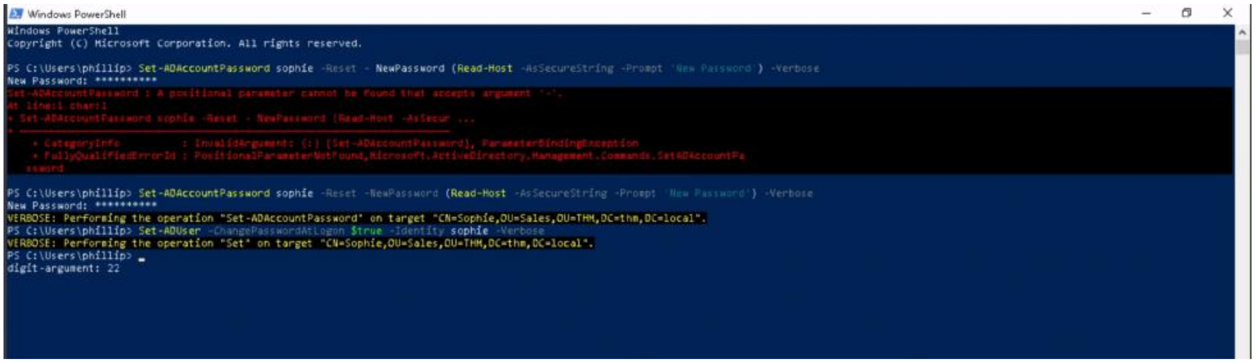
You can select common tasks or customize your own.

● Delegate the following common tasks:

- □ Create, delete, and manage user accounts
- ☑ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate

So after we delegated control to phillip, we logged in via RDP and used the Powershell command to reset the password for a users account. In this case the user will be sophie.

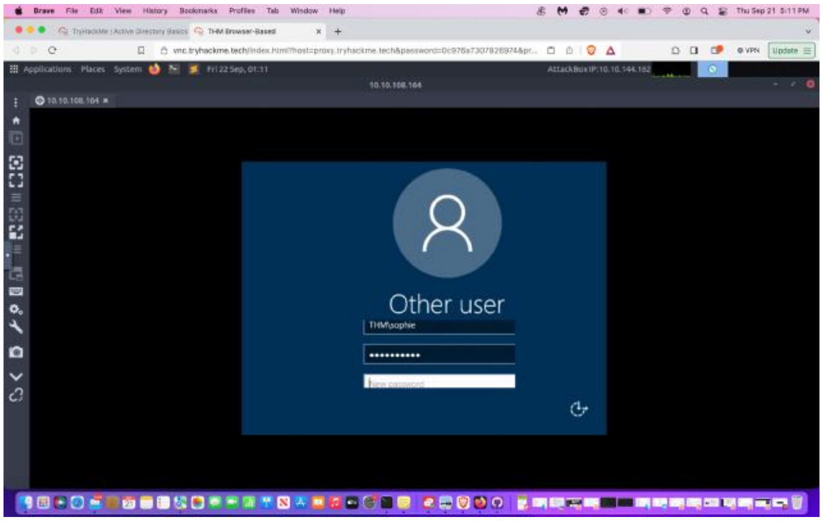


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\phillip> Set-ADAccountPassword sophie -Reset - NewPassword (Read-Host -AsSecureString -Prompt 'New Password') -Verbose
New Password: **********
Set-ADAccountPassword : A positional parameter cannot be found that accepts argument '-'.
At line:1 char:1
+ Set-ADAccountPassword sophie -Reset - NewPassword (Read-Host -AsSecur ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-ADAccountPassword], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.ActiveDirectory.Management.Commands.SetADAccountPa
   ssword

PS C:\Users\phillip> Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password') -Verbose
New Password: **********
VERBOSE: Performing the operation "Set-ADAccountPassword" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
PS C:\Users\phillip> Set-ADUser -ChangePasswordAtLogon $true -Identity sophie -Verbose
VERBOSE: Performing the operation "Set" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
PS C:\Users\phillip> _
digit-argument: 22
```

Once we are done with that the powershell command we can log in throught RDP on Sophies account, and reset the password.



Brave File Edit View History Bookmarks Profiles Tab Window Help
Thu Sep 21 5:11 PM
TryHackMe | Active Directory Basics
THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=0c976a7307826974&pr...
VPN
Update
Applications Places System
Fri 22 Sep, 01:11
AttackBox IP:10.10.144.162
10.10.108.104
10.10.108.104

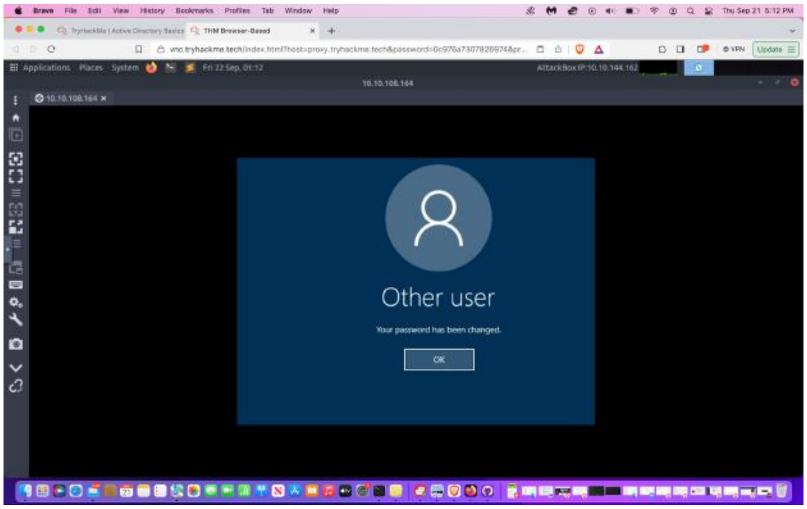
Other user

THM\sophie

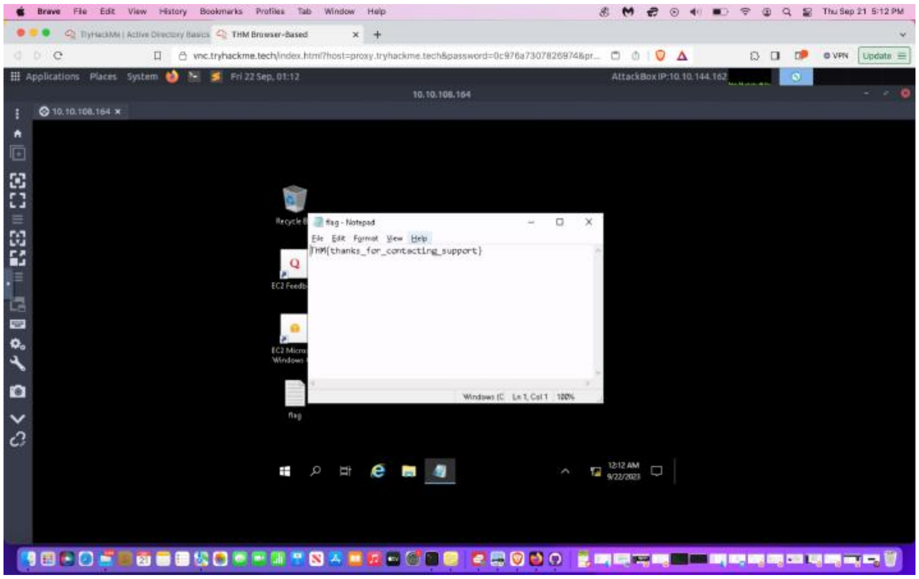
•••••••••••

New password

Through the process of delegation we have been able to change Sophies password,

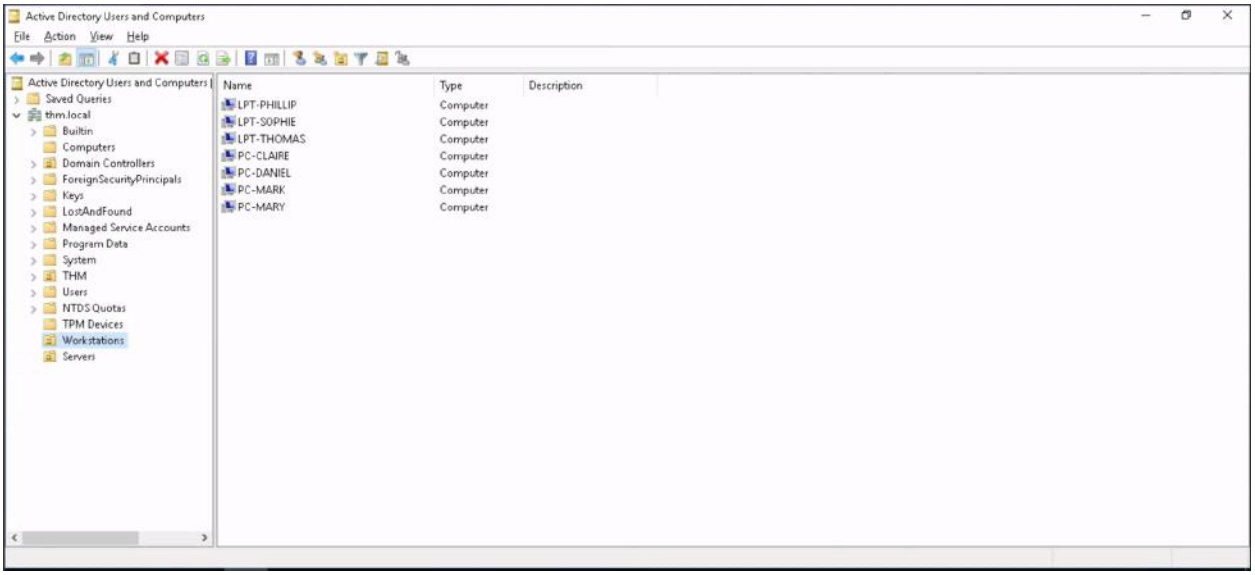


Your password has been changed.



THM{thanks_for_contacting_support}

Over here we just created a 2 new OU’s, server and workstation. We placed the computers and laptops to workstation OU , and the servers to the Servers OU.

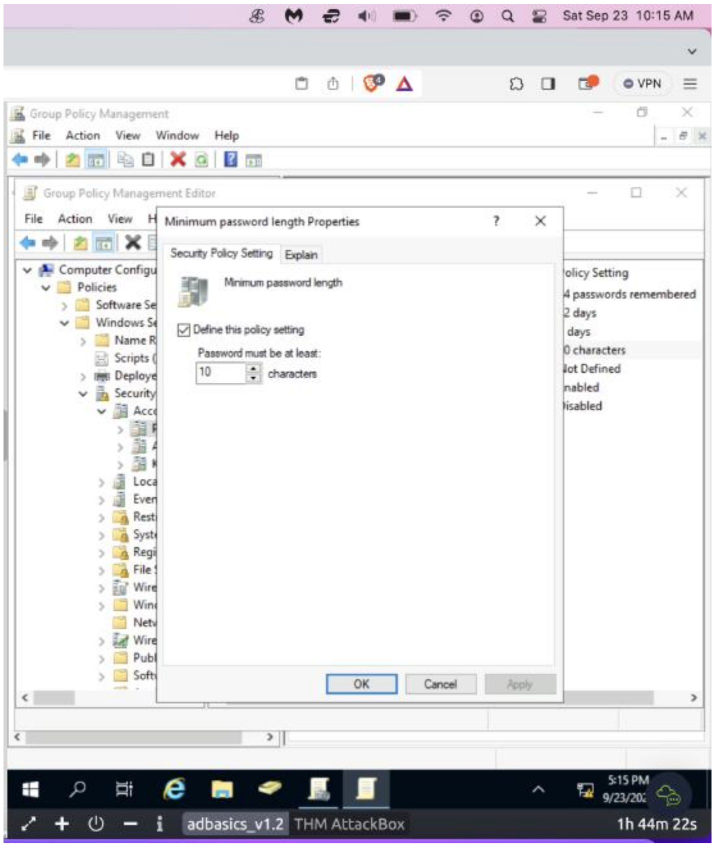


Name	Type	Description
LPT-PHILLIP	Computer	
LPT-SOPHIE	Computer	
LPT-THOMAS	Computer	
PC-CLAIRE	Computer	
PC-DANIEL	Computer	
PC-MARK	Computer	
PC-MARY	Computer	

Group Policy Objectives

In this portion we will create a few group policies which will be implemented. A practical action we can do is changing the password requirements to 10 characters. Keep in mind that the group policy objective will impact the entire domain affecting all of the computers.

```
Computer Configurations -> Policies -> Windows Setting -> Security Settings -> Account Policies -> Password Policy
```



Minimum password length Properties

Security Policy Setting | Explain

Minimum password length

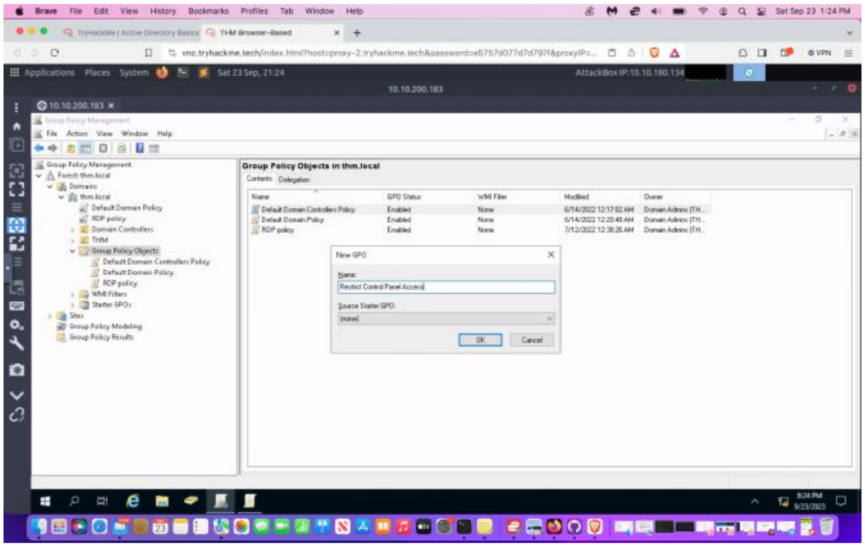
☑ Define this policy setting

Password must be at least:

10 characters

Create New GPO

We will create a new GPO called restrict control panel access. However this time it will affect specific users, not all though. The reason for this is to block non IT- users from accessing the control panel.



Group Policy Objects in thm.local

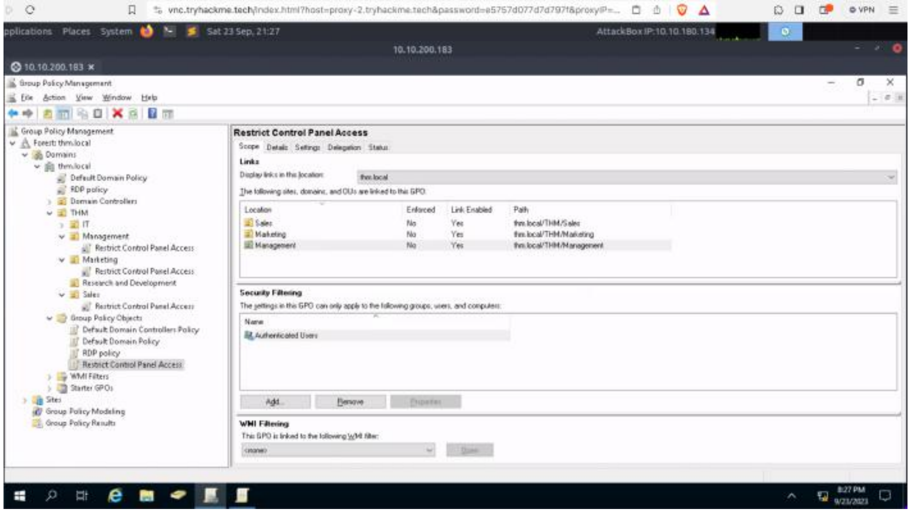
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	6/14/2022 12:17:02 AM	Domain Admins (TH...
Default Domain Policy	Enabled	None	6/14/2022 12:20:48 AM	Domain Admins (TH...
RDP policy	Enabled	None	7/12/2022 12:38:26 AM	Domain Admins (TH...

New GPO

Name: Restrict Control Panel Access

Source Starter GPO: (none)

Next we can implement which groups the policy will be enforced upon. For this purpose we have enforced it on Marketing , Management, and sales.



Restrict Control Panel Access

Links

Display links in this location: thm.local

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

Location	Enforced	Link Enabled	Path
Sales	No	Yes	thm.local/THM/Sales
Marketing	No	Yes	thm.local/THM/Marketing
Management	No	Yes	thm.local/THM/Management

Security Filtering

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

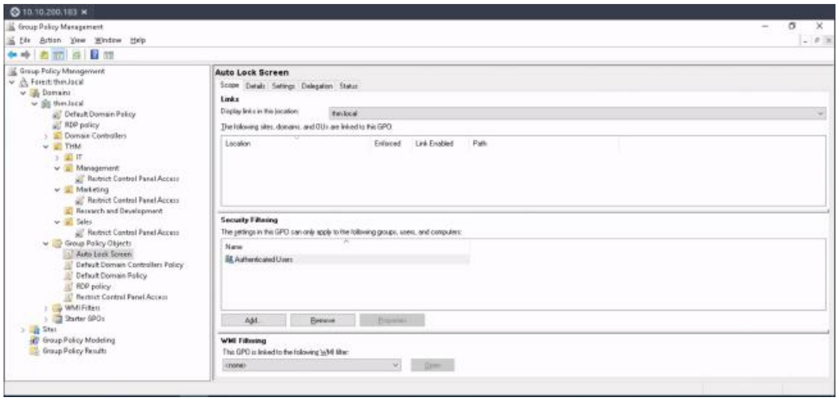
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter: <none>

Create a new GPO, call it Auto Lock Screen

Finally we will create a policy called Auto lock screen. We will set the time limit to about 5 minutes. This should be applied to the root domain since we want the GPO to impact all of the computers.



Group Policy Management

- Group Policy Management
  - Forest: thm.local
    - Domains
      - thm.local
        - Default Domain Policy
        - RDP policy
        - Domain Controllers
        - THM
          - IT
          - Management
            - Restrict Control Panel Access
          - Marketing
            - Restrict Control Panel Access
          - Research and Development
          - Sales
            - Restrict Control Panel Access
        - Group Policy Objects
          - Auto Lock Screen
          - Default Domain Controllers Policy
          - Default Domain Policy
          - RDP policy
          - Restrict Control Panel Access
        - WMI Filters
        - Starter GPOs
    - Sites
  - Group Policy Modeling
  - Group Policy Results

Auto Lock Screen

Scope | Details | Settings | Delegation | Status

Links

Display links in this location: thm.local

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

Location	Enforced	Link Enabled	Path

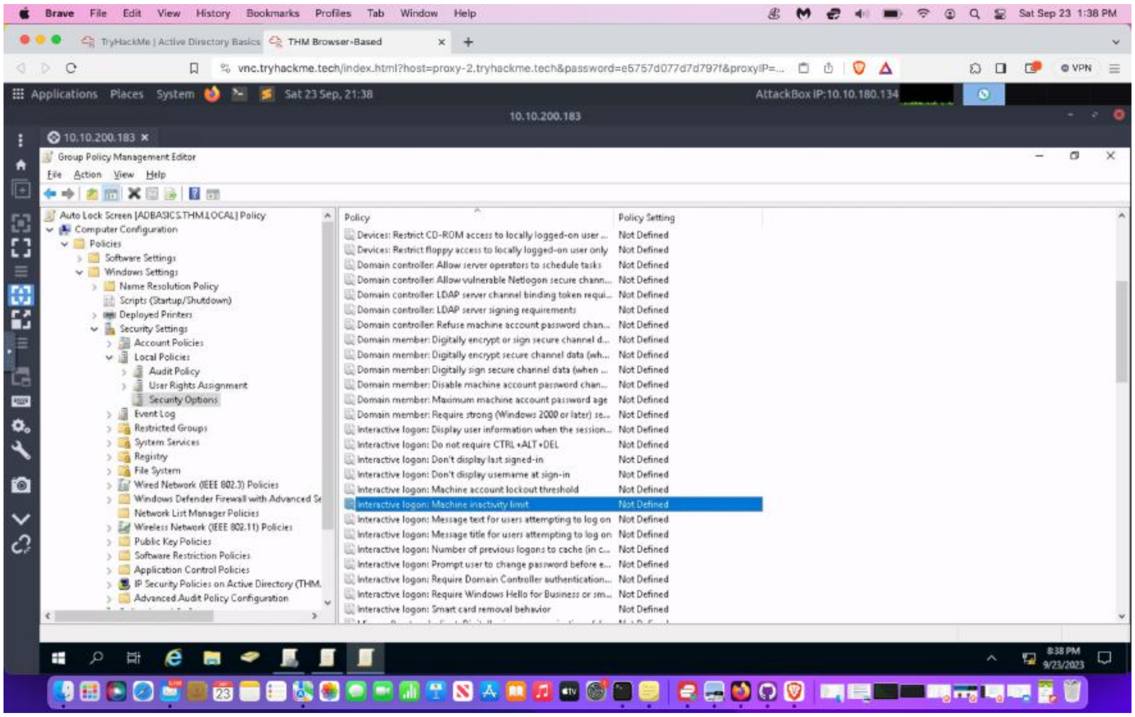
Security Filtering

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

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter: <none>



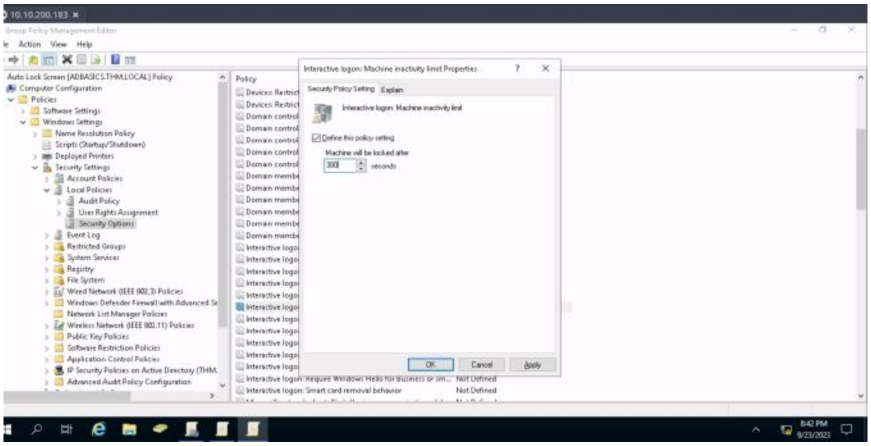
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=e5757d077d7d797f&proxyIP=...

AttackBox IP:10.10.180.134

Group Policy Management Editor

- Auto Lock Screen [ADBASICS.THM.LOCAL] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Defender Firewall with Advanced Se
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
          - Software Restriction Policies
          - Application Control Policies
          - IP Security Policies on Active Directory (THM.
          - Advanced Audit Policy Configuration

Policy	Policy Setting
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) se...	Not Defined
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Not Defined
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in c...	Not Defined
Interactive logon: Prompt user to change password before e...	Not Defined
Interactive logon: Require Domain Controller authentication...	Not Defined
Interactive logon: Require Windows Hello for Business or sm...	Not Defined
Interactive logon: Smart card removal behavior	Not Defined



Interactive logon: Machine inactivity limit Properties

Security Policy Setting | Explain

Interactive logon: Machine inactivity limit

☑ Define this policy setting

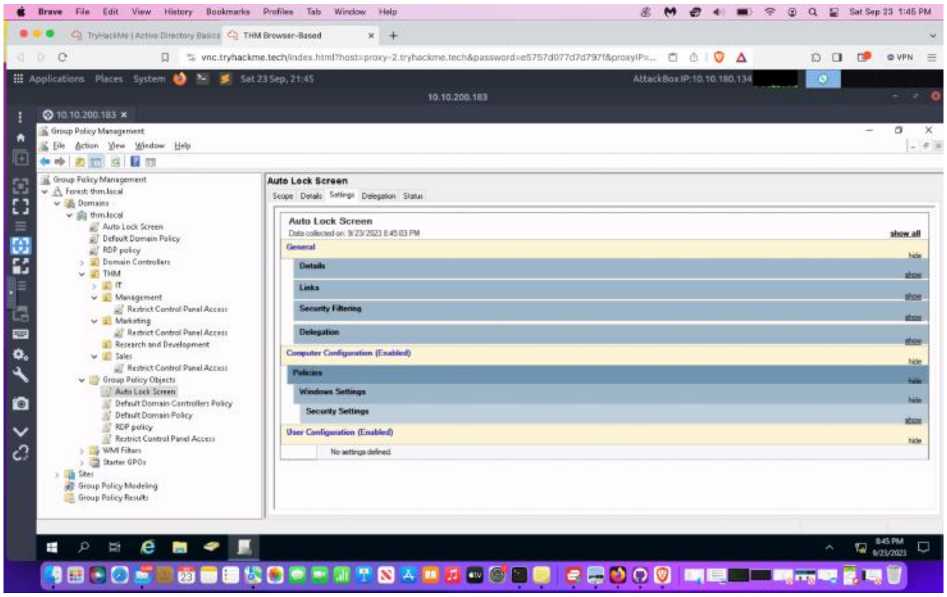
Machine will be locked after

300 seconds

OK | Cancel | Apply

10.10.200.183
Group Policy Management Editor
File Action View Help
Auto Lock Screen [ADBASICS.THM.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (THM...
Advanced Audit Policy Configuration
Policy
Interactive logon: Require Windows Hello for Business or sm... Not Defined
Interactive logon: Smart card removal behavior Not Defined
8:42 PM
9/23/2023

We'll configure the inactivity limit to be 5 minutes, which means that if a user leaves their session open without any activity, their computer will automatically lock. Once we finish making this change in the Group Policy Object (GPO) editor, we'll link the GPO to the root domain by simply dragging and dropping it onto the root domain.



Auto Lock Screen

Scope | Details | Settings | Delegation | Status

Auto Lock Screen

Data collected on: 9/23/2023 8:45:03 PM

show all

General — hide

Details — show

Links — show

Security Filtering — show

Delegation — show

Computer Configuration (Enabled) — hide

Policies — hide

Windows Settings — hide

Security Settings — show

User Configuration (Enabled) — hide

No settings defined.

Brave File Edit View History Bookmarks Profiles Tab Window Help
Sat Sep 23 1:45 PM
TryHackMe | Active Directory Basics
THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=e5757d077d7d797f&proxyIP=...
VPN
Applications Places System
Sat 23 Sep, 21:45
AttackBox IP:10.10.180.134
10.10.200.183
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: thm.local
Domains
thm.local
Auto Lock Screen
Default Domain Policy
RDP policy
Domain Controllers
THM
IT
Management
Restrict Control Panel Access
Marketing
Restrict Control Panel Access
Research and Development
Sales
Restrict Control Panel Access
Group Policy Objects
Auto Lock Screen
Default Domain Controllers Policy
Default Domain Policy
RDP policy
Restrict Control Panel Access
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
8:45 PM
9/23/2023