Active Directory Basics

Windows Domains: **Group under the administration in a business.**
Network in a single repository : **Active Directory**
Server that runs active directory : **Domain Controller**

Main advantages having a configured windows domain are:
Centralised Identify Management - All users across network configured from active directory with minimum effort.
Managing Security Policies - Configure security policies from active directory and apply them to users and computers across the network.

Users:
Most common in an active directory. Users are one of the objects known as security principles. They can be authenticated by the domain and can be assigned privileges over resources like files.

Users can represent 2 types of entities:
People: Representing people in the organisation to access a network, eg. Employees.
Services: Every service requires a user to run. But users will only have specific privileges needed to run their specific service.

For every computer that joins the active directory domain, a machine object is created. Machines are also considered security principles. They are assigned an account just as a regular user.

Machine account passwords are automatically rotated comprised of 120 random characters.

Security Groups:
Allows you to define the users access rights, what they can and cannot access. This allows better manageability as you can add users to existing group and will automatically inherit the privileges of the group configuration.

Domain Admins:
Admin privileges over the entire domain. Can administer any computer on the domain including the DCs.
Server Operators:
Users in this group can administer Domain Controllers. They cannot change any administrative group memberships.
Backup Operators:

Users in this group are allowed to access any file. Ignoring their permissions, used to perform data backup on computers for example.

Account Operators:

Users in this group can create or modify accounts on the domain.

Domain users:

Includes all existing user accounts on the domain.

Domain computers:

Includes all existing computers in the domain.

Domain controllers:

Includes all existing DCs on the domain.

REMOTE DESKTOP TASK:

We are given a task to log into a hypothetical employee called “Phillip” and because we are the admin we have his username and password:

Username: phillip

Password: Claire2008

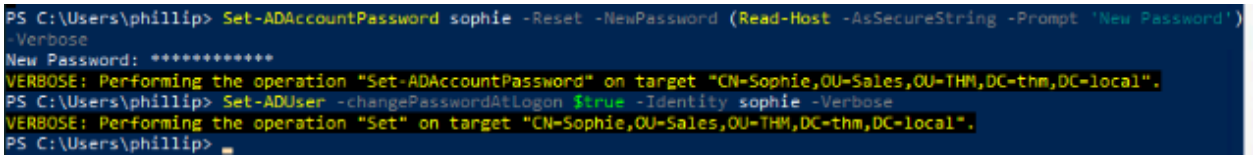
So we launch the remote desktop app and connect to the IP: 10.10.90.19 and log in using both the username and password provided. Once logged in, we can officially use powershell to demonstrate our new powers, in the previous scenario as the admin, I gave Phillip the ability to reset user passwords as a delegate. He has these powers only because he is head of the theoretical IT department which in principle, would have access to these abilities in a real world scenario.

```
Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host
-AsSecureString -Prompt 'New Password') -Verbose
```

Using this command I set the new password to:
Hackerman123

```
Set-ADUser -ChangePasswordAtLogon $true -Identity sophie
-Verbose
```

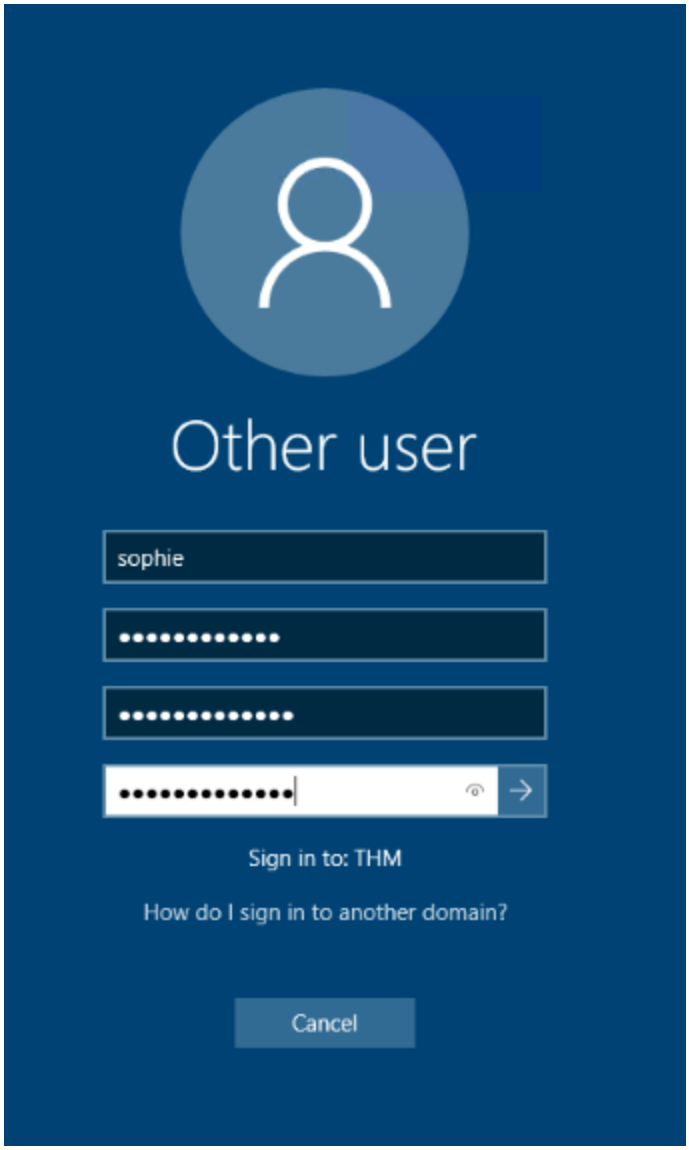
Using this command, this would set the new password on the account in question which is Sophie.



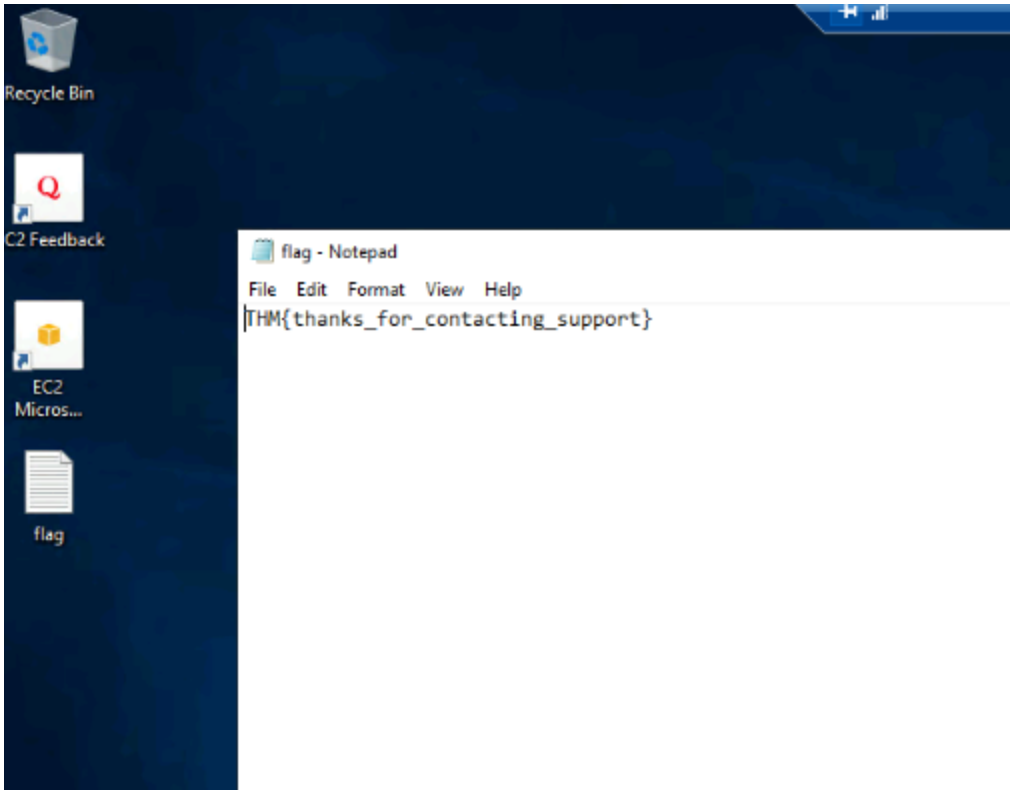
So now, we will remote desktop over the same IP and use the credentials

Username: sophie

Password: Hackerman123



Okay so something didn't work but something did!
I changed the password from: Hackerman123 to Hackerman1234
Seems to have worked, we are officially into her account and the flag has been sighted on the desktop.



THM{thanks_for_contacting_support}

What a fun little scenario!