Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024

Lab 4.5.8: Securing Default Local Accounts on Windows

In this lab, I will be securing the default Administrator and Guest accounts which are automatically created with on a Windows Installation.

The scenario for this lab is as follows:

“You work as the IT security administrator for a small corporate network. You are improving office computers' security by renaming and disabling default accounts.

In this lab, your task is to perform the following on the Office1 computer:

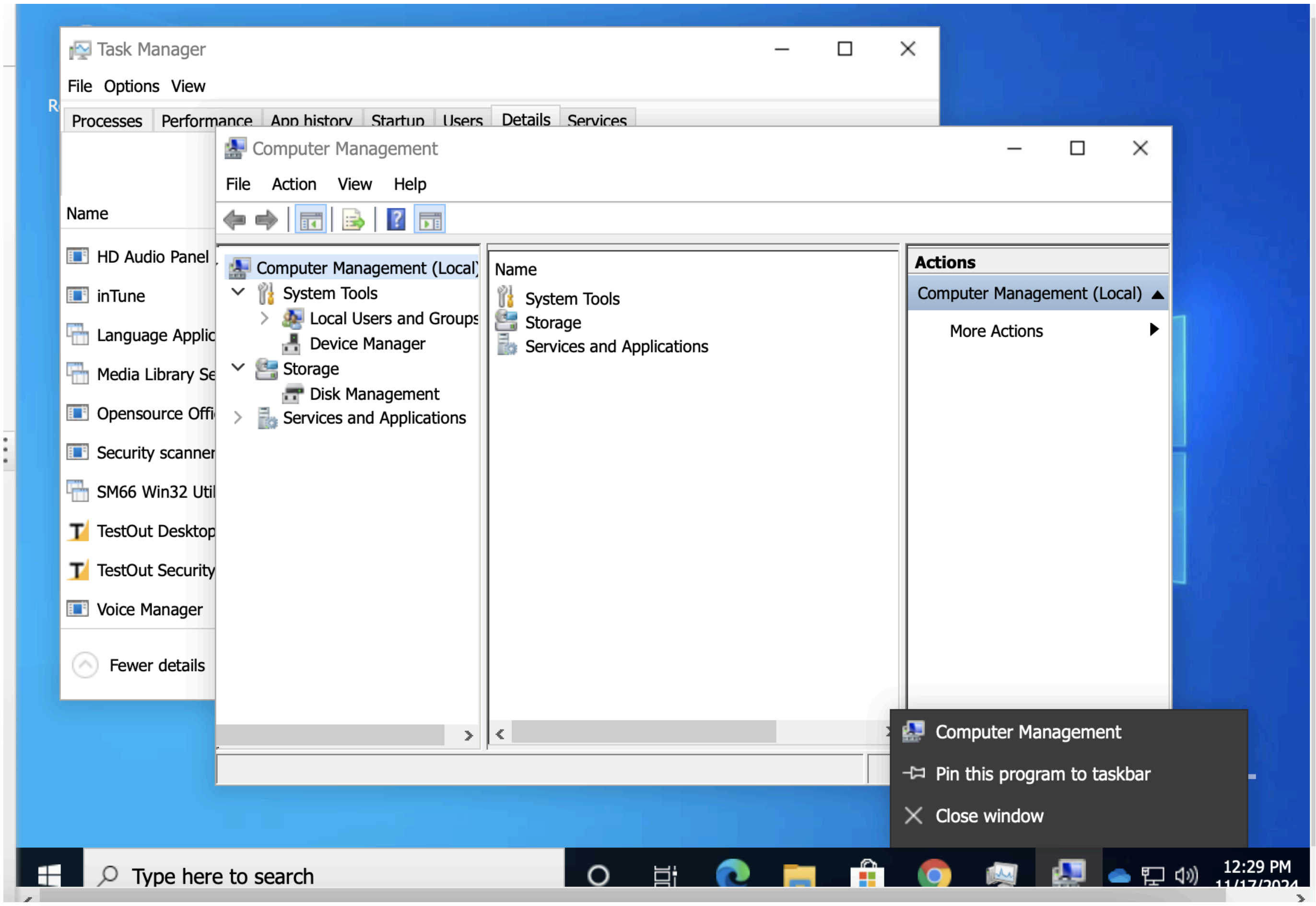
1. **Rename the Administrator account, Yoda.**
2. **Disable the Guest account.**
3. **Verify that *Password never expires* is not selected for any local users. This forces them to change their passwords regularly.**
4. **Delete any user accounts with *User must change password at next logon* selected. This indicates that a user has never logged in.**

“

Since we are working with local accounts and not on our Windows Server Manager we will want to use the Computer Management function that is built-in to Windows. With this tool we can modify and change policies pertaining to our users.

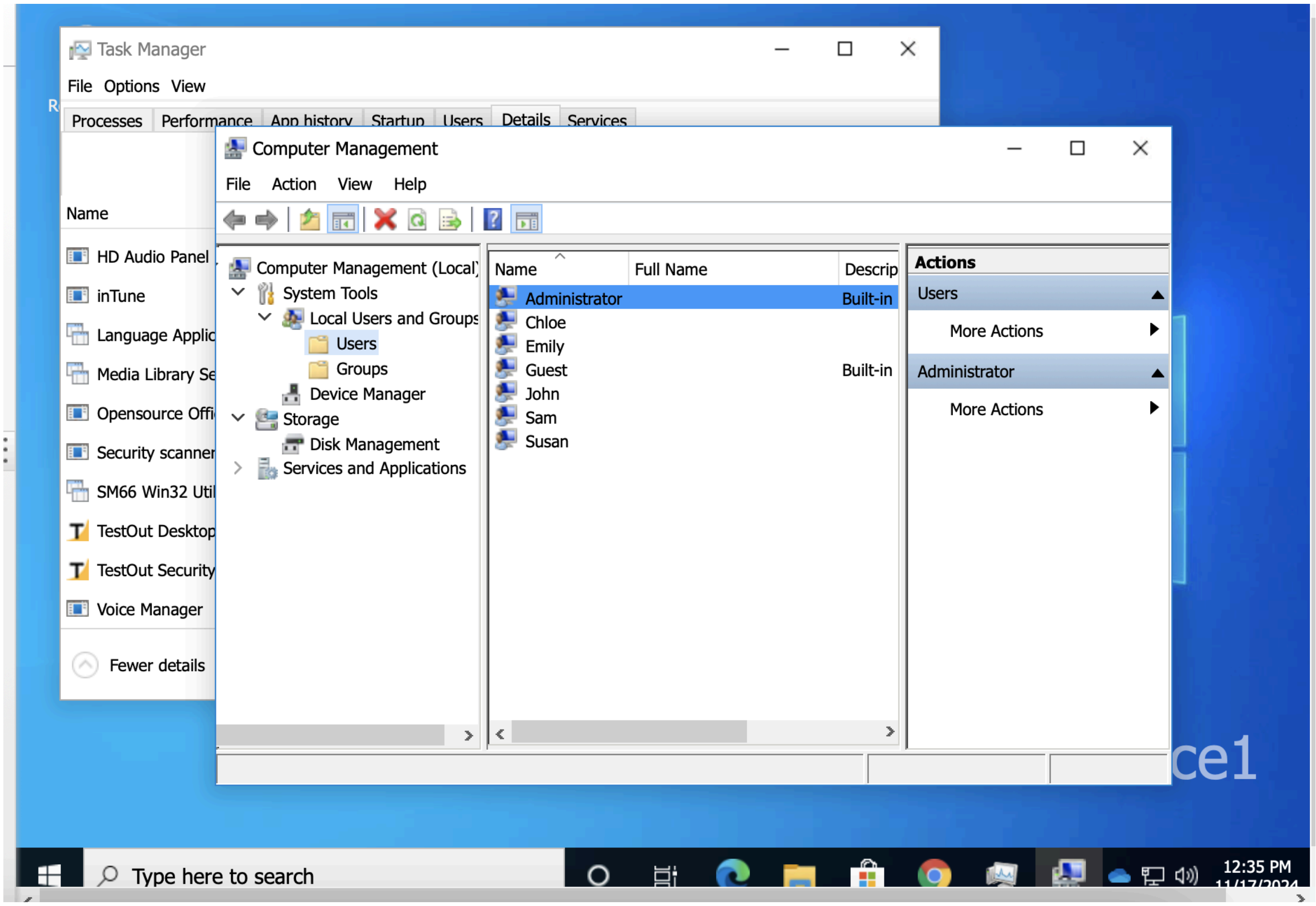
Type ‘Computer management” into your search bar or right-click the Windows logo and select it from the menu that pops up.

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



Our first goal is to rename the built in Administrator account in order to obfuscate it from our users.

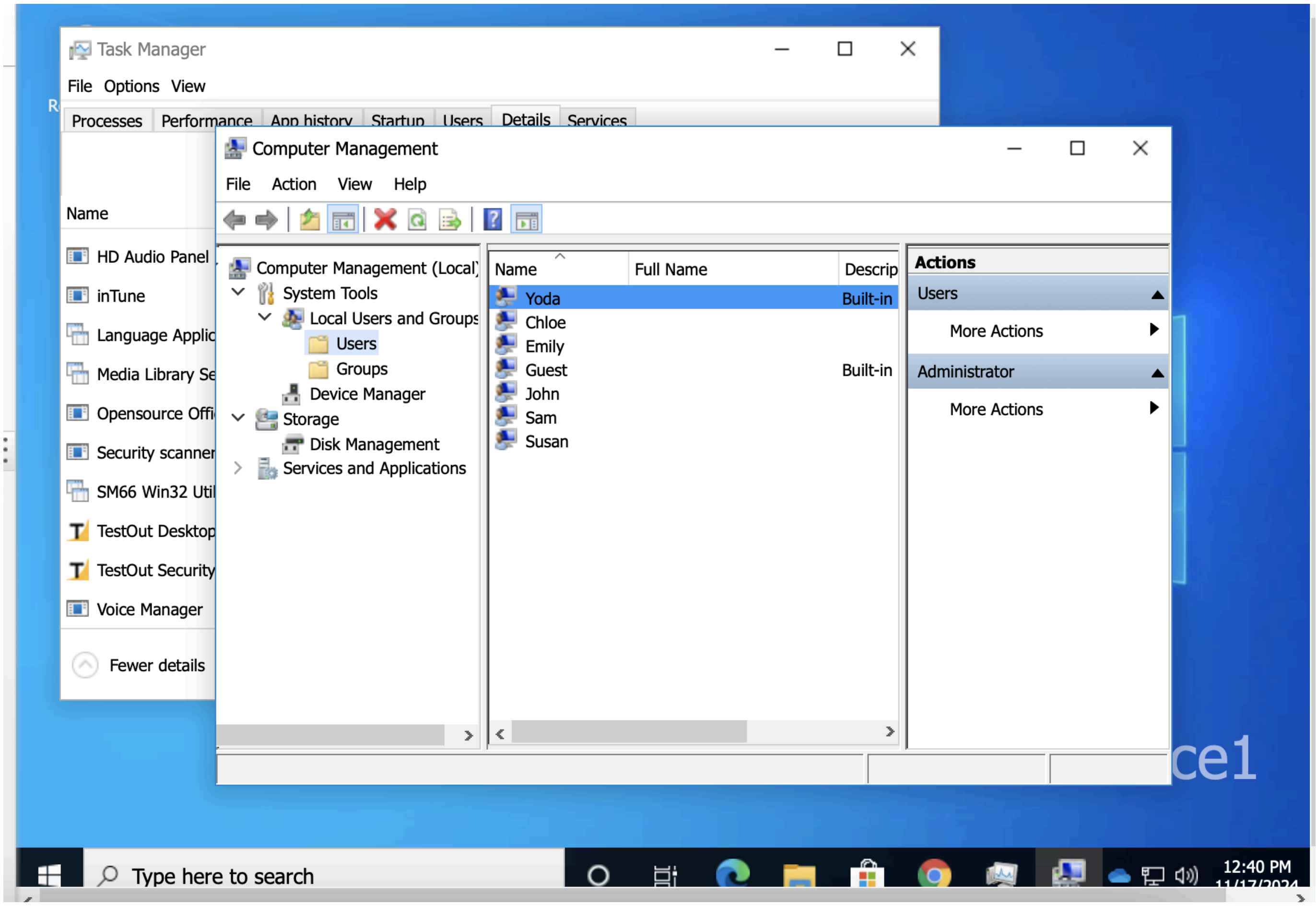
Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



Name	Full Name	Descrip
Administrator		Built-in
Chloe		
Emily		
Guest		Built-in
John		
Sam		
Susan		

From here we just need to right-click the Admin. Account and select “Rename”. The text field around Administartor is highlighted which is prompting us for changes that we would like to make. I’m going to rename the account to the requested name of “Yoda”. After typing that we see:

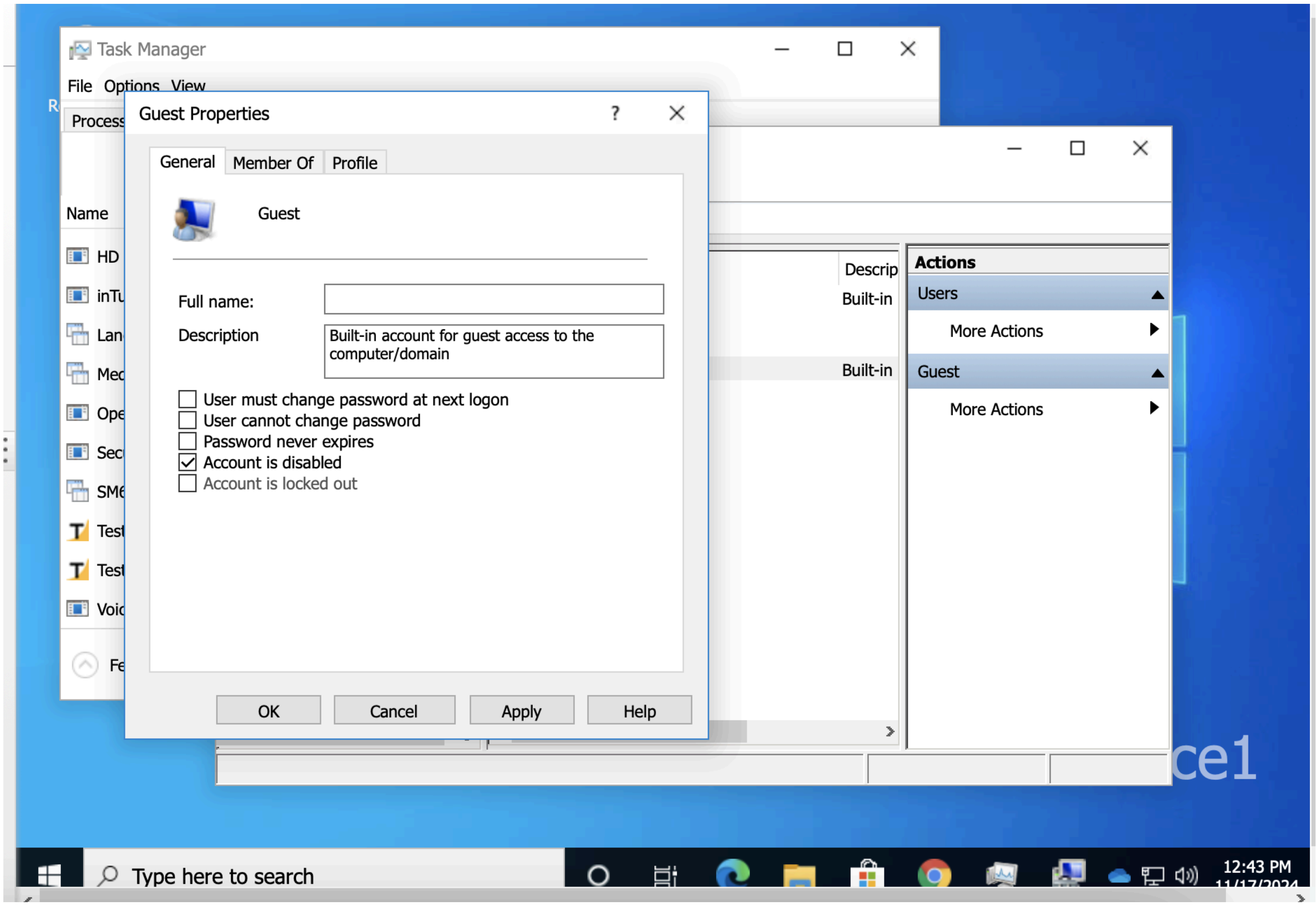
Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



Name	Full Name	Descrip
Yoda		Built-in
Chloe		
Emily		
Guest		Built-in
John		
Sam		
Susan		

Task #1 completed! Now let’s go ahead and navigate down to the “Guest” account and right-click it to edit it’s properties. In the window that pops up I will check the box for “Disable this account.”

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



Guest Properties

General | Member Of | Profile

Guest

Full name:

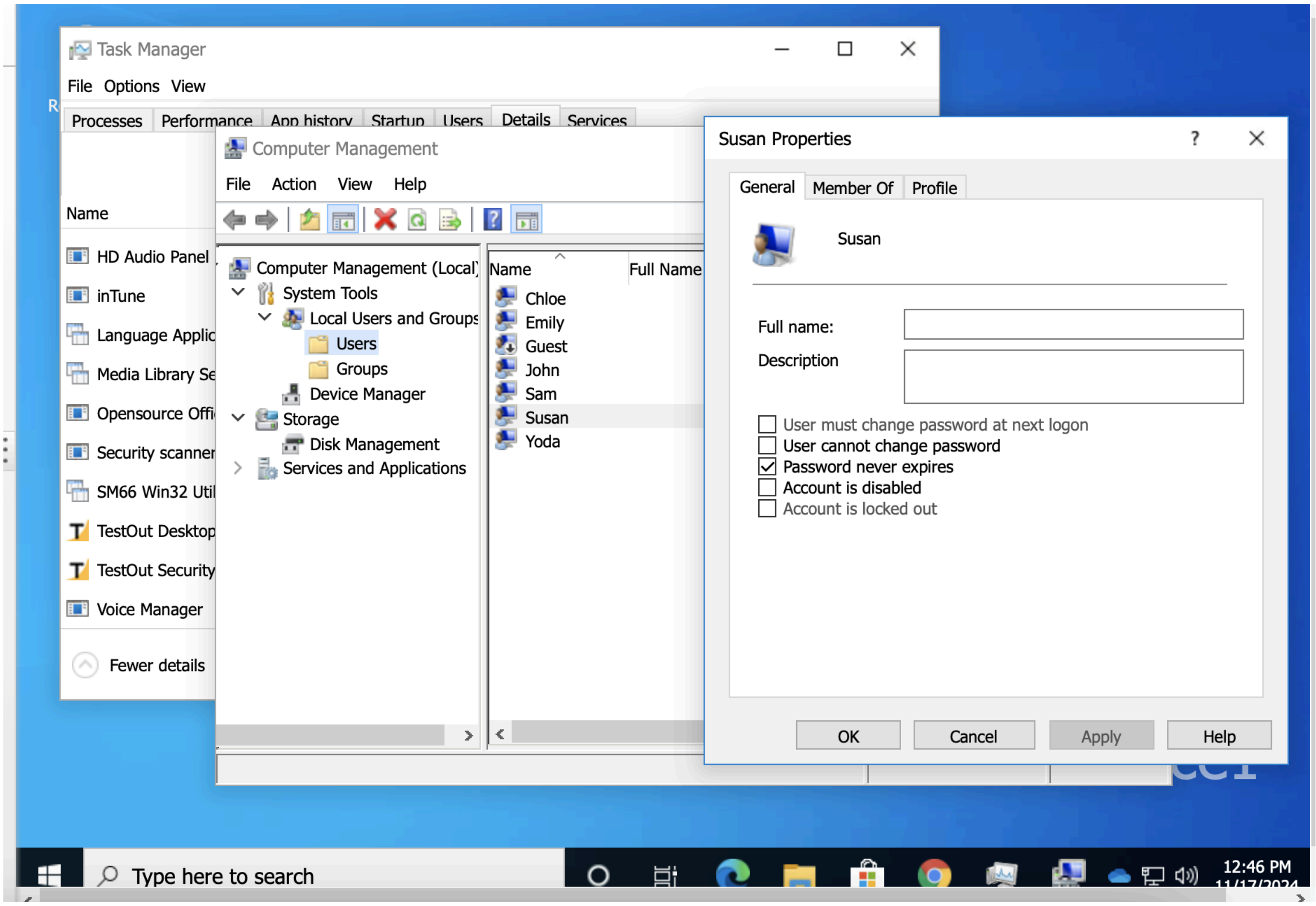
Description: Built-in account for guest access to the computer/domain

□ User must change password at next logon
□ User cannot change password
□ Password never expires
☑ Account is disabled
□ Account is locked out

After, I’ll hit Apply and then OK. Moving on to step #3 we want to check every account and make sure that their passwords have an expiration date.

The setting in the above window we will want to uncheck is “Password Never Expires.” Let’s check all users. AH HA!

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



Chloe
Emily
Guest
John
Sam
Susan
Yoda

Susan Properties

General | Member Of | Profile

Susan

Full name:

Description

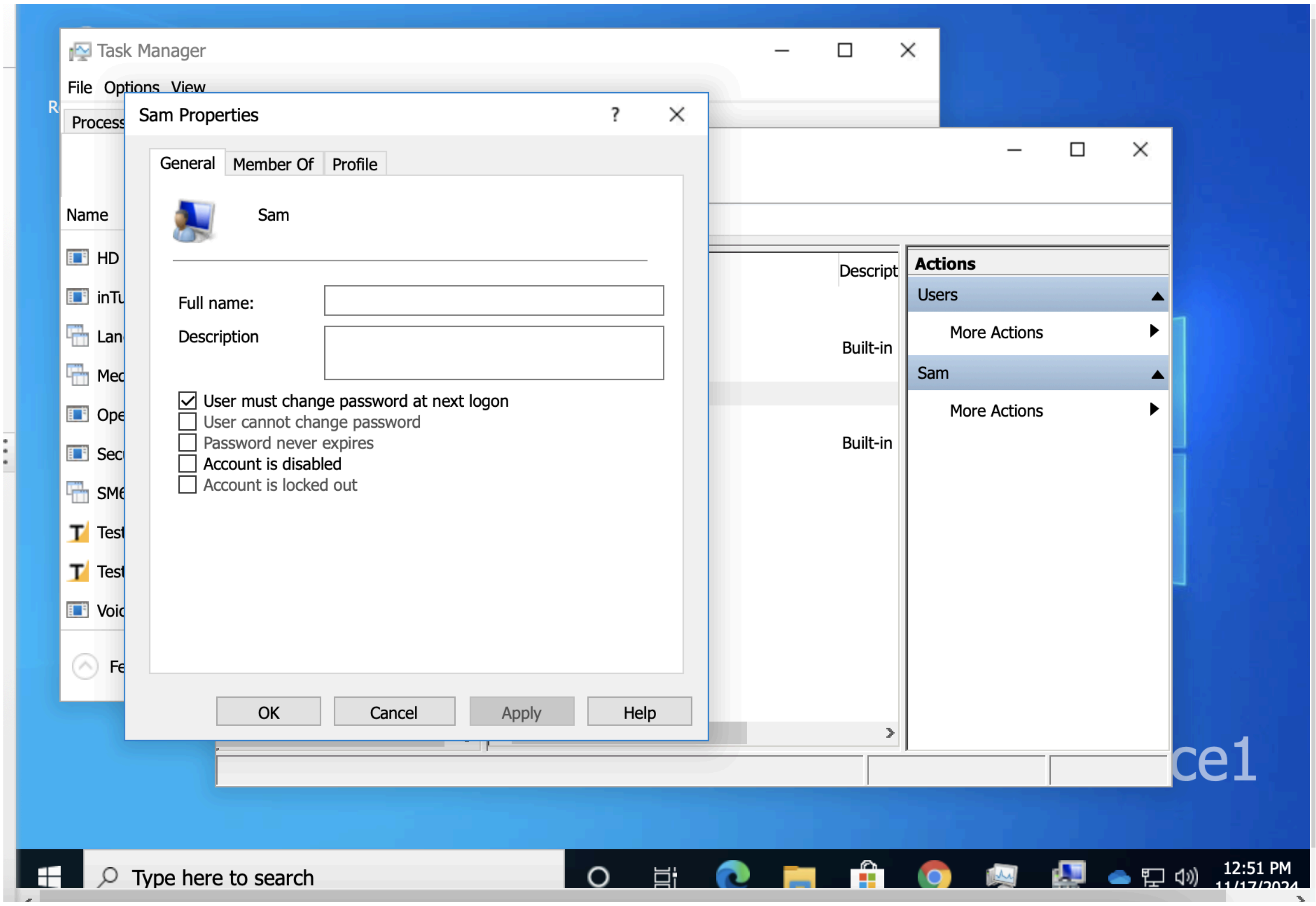
☐ User must change password at next logon
☐ User cannot change password
☑ Password never expires
☐ Account is disabled
☐ Account is locked out

Here, we can see that the box is checked for Susan. We need to uncheck the box and then hit Apply then OK. This will enforce the fact that Susan will need to regularly change her password (on her Local account on this Local Machine). Moving along to the other users we see that no other have the box checked.

In this case we can move on to Step #4 which is to delete any accounts that have the box “User must change password at next logon.” The reason is because if the user had INDEED logged in, that box would not currently be checked. The box is automatically unchecked by Windows once the user changes their password on their first login. What this implies is that these are unused accounts. Disabling these can help to eliminate another attack vector on our system.

Sam happens to be one of those users. We can simply just delete their account.

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



Sam Properties

General | Member Of | Profile

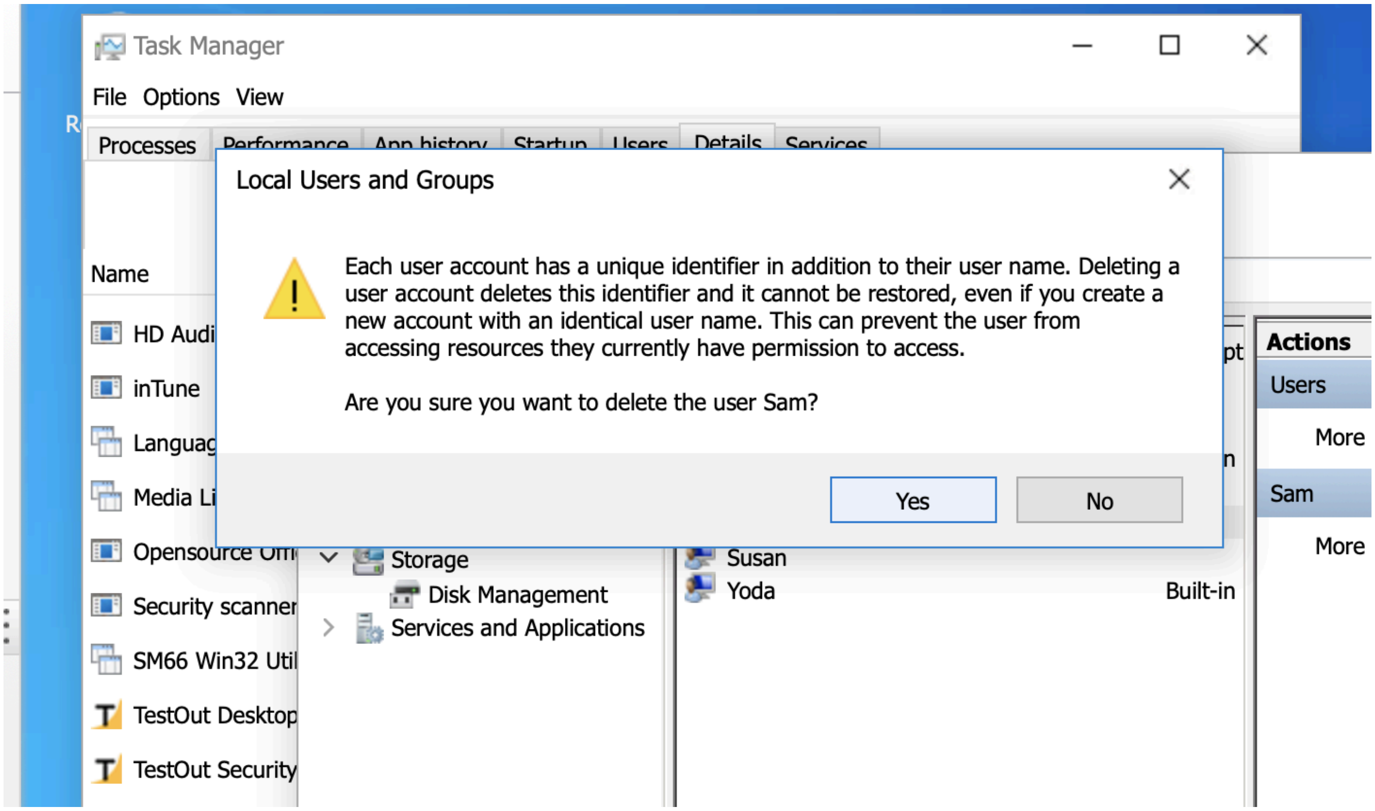
Sam

Full name:

Description

☑ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Account is disabled
☐ Account is locked out

OK | Cancel | Apply | Help



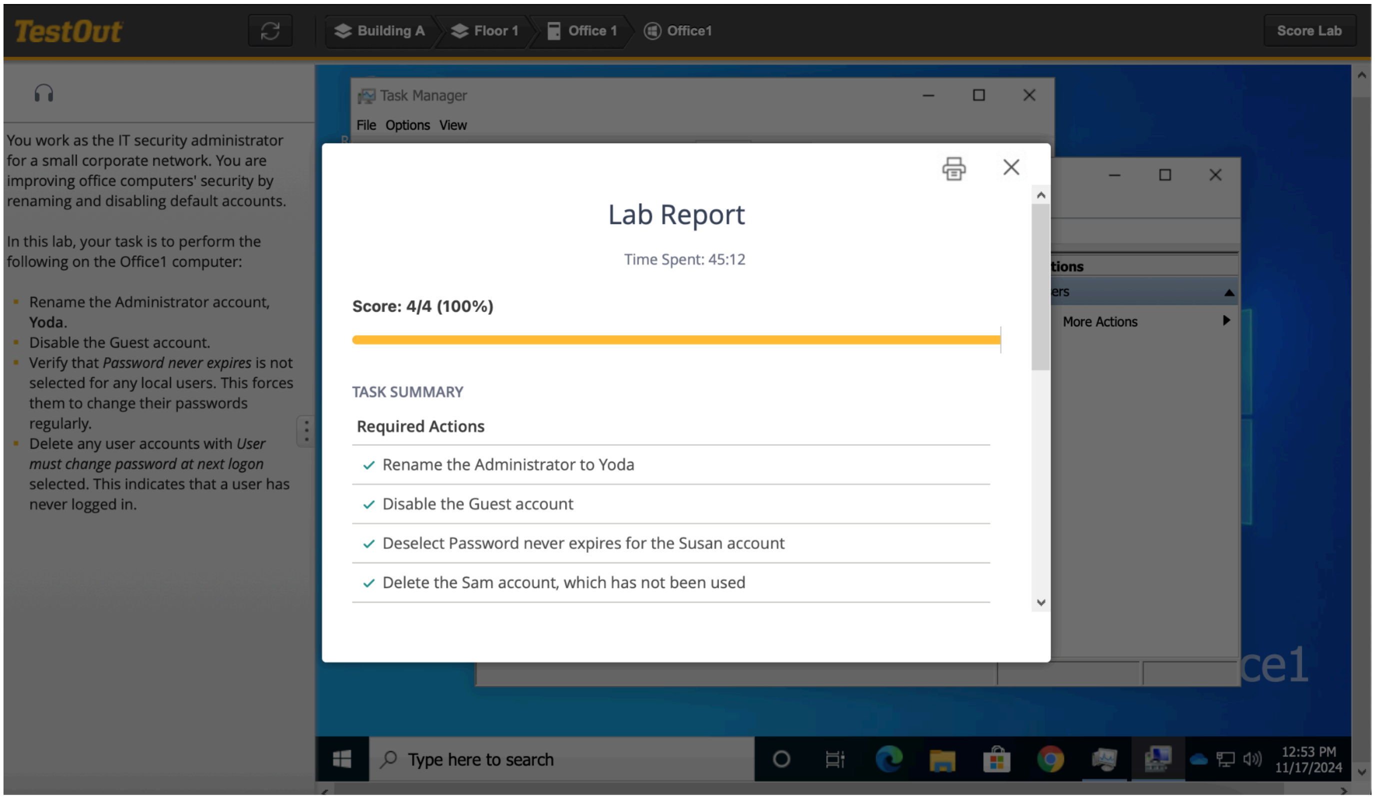
Local Users and Groups

Each user account has a unique identifier in addition to their user name. Deleting a user account deletes this identifier and it cannot be restored, even if you create a new account with an identical user name. This can prevent the user from accessing resources they currently have permission to access.

Are you sure you want to delete the user Sam?

Hit “Yes” on the dialog box that comes up! We are now finished with all tasks required and can finish the lab.

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



You work as the IT security administrator for a small corporate network. You are improving office computers' security by renaming and disabling default accounts.

In this lab, your task is to perform the following on the Office1 computer:

- Rename the Administrator account, Yoda.
- Disable the Guest account.
- Verify that *Password never expires* is not selected for any local users. This forces them to change their passwords regularly.
- Delete any user accounts with *User must change password at next logon* selected. This indicates that a user has never logged in.

Lab Report

Time Spent: 45:12

Score: 4/4 (100%)

TASK SUMMARY

Required Actions

- ✓ Rename the Administrator to Yoda
- ✓ Disable the Guest account
- ✓ Deselect Password never expires for the Susan account
- ✓ Delete the Sam account, which has not been used