Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

# Lab 7.2.9 Scanning a Windows Host for Vulnerabilities and Remediating Them

*From TestOut CompTIA Security+ Course*

In this lab I will be scanning a Windows Host for Vulnerabilities using a Vulnerability scanner similar to Greenbone's OpenVAS (generic non copyrighted version). Once I have a list of those vulnerabilities I will remediate them and verify they've been solved.

## The scenario for this lab is as follows:

**"You are the IT security administrator for a small corporate network. You are performing vulnerability scans on your network. Mary is the primary administrator for the network and the only person authorized to perform local administrative actions. The company's network security policy requires complex passwords for all users that are at least 12 characters long. It is also required that Windows Firewall is enabled on all workstations. Sharing personal files is not allowed.**

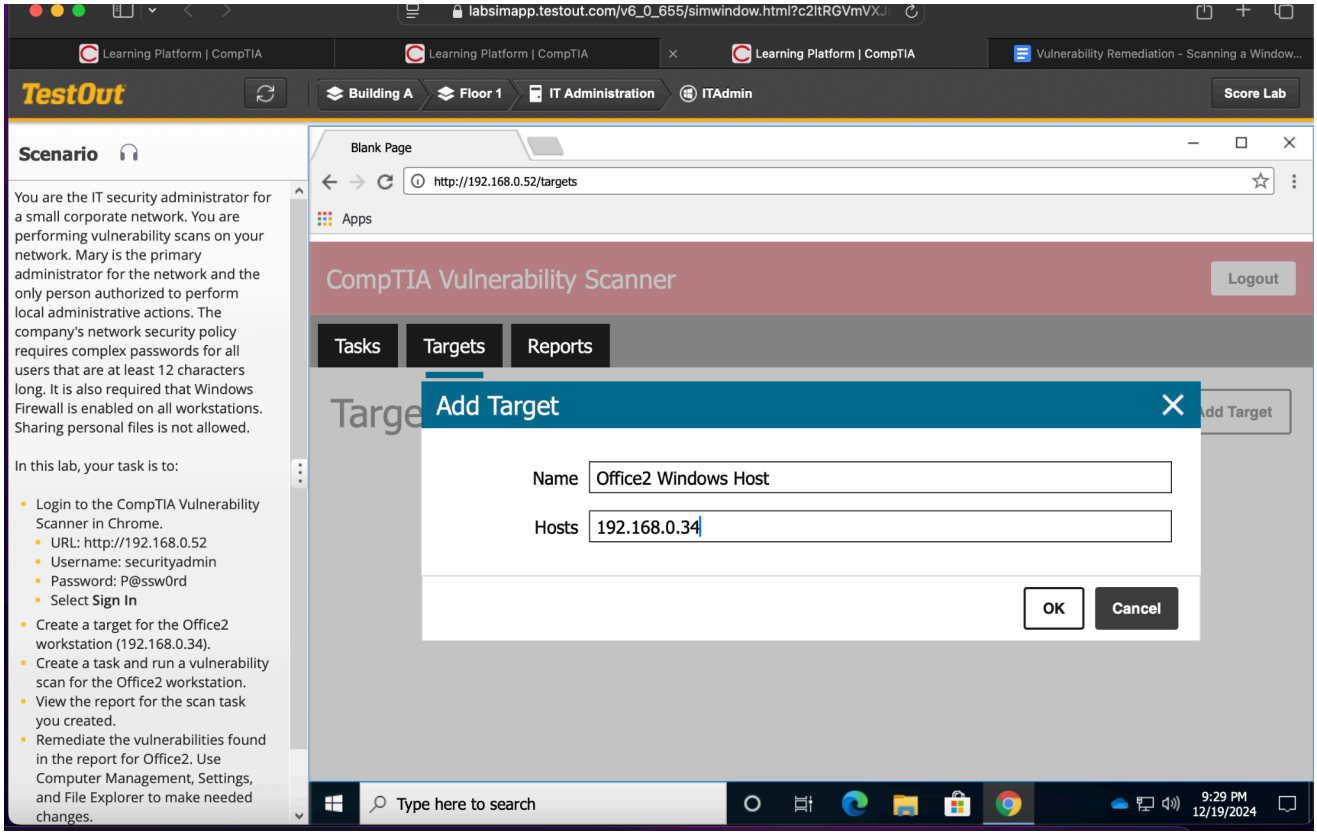
**In this lab, your task is to:**

- **Login to the CompTIA Vulnerability Scanner in Chrome.**
  - **URL: http://192.168.0.52**
  - **Username: securityadmin**
  - **Password: P@ssw0rd**
  - **Select Sign In**
- **Create a target for the Office2 workstation (192.168.0.34).**
- **Create a task and run a vulnerability scan for the Office2 workstation.**
- **View the report for the scan task you created.**
- **Remediate the vulnerabilities found in the report for Office2. Use Computer Management, Settings, and File Explorer to make needed changes.**
- **Re-run a vulnerability scan to make sure all of the issues are resolved."**

First I will start by logging in to the Vulnerability Scanner with the credentials provided. The password we're using here is not secure, it's just for demonstrate purposes.

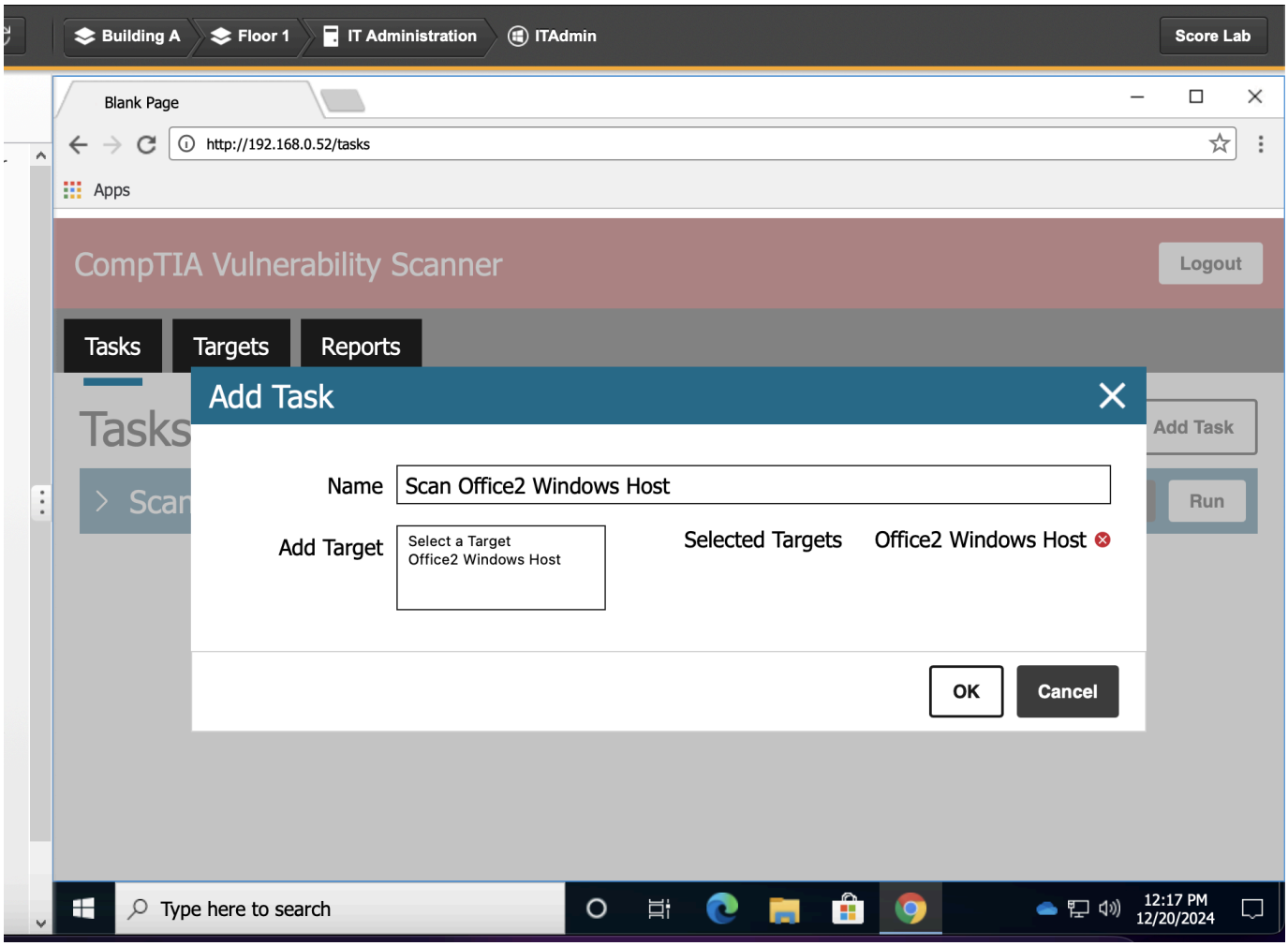
Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

Underneath **Targets** I will add the Windows Host we are scanning which is located at **192.168.0.34.** Under **Name** I will type the name of the computer I am scanning which is Office2**.**



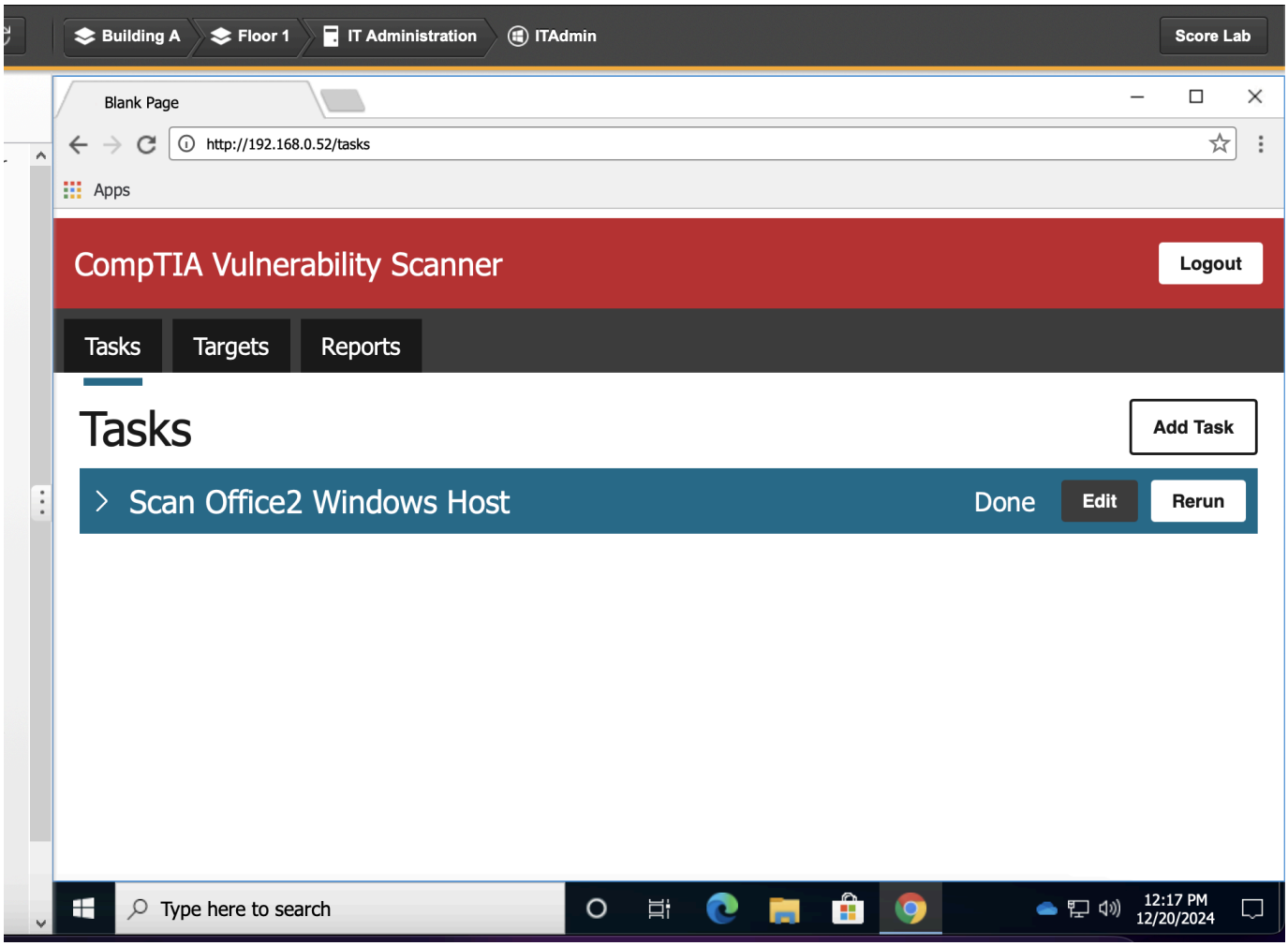

Now, I'll click the OK button to move on. In order to scan this host I will need to create a task to do so under **Tasks.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024




Once the Task has been added I can click the **Run** button to start the Vulnerability Scanner .

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024




Once it says **Done** , I can navigate over to the **Reports** tab on the top menu bar. On this page I can view the results of the scan. Let's see what it found:

**"Office2 Windows Host Report**

**Vulnerability: 1: Local Account Locked Out**

**Host: 192.168.0.34**

**Some user accounts are locked out.**

**Vulnerability: 2: Administrator Account Renamed**

**Host: 192.168.0.34**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024
**The administrator account should be renamed.**

**Vulnerability: 3: Administrators**

**Host: 192.168.0.34**

**More than 2 Administrators found on this computer. Administrator Mary Susan**

**Vulnerability: 4: Folder Shares**

**Host: 192.168.0.34**

**Folders are shared from this computer. C:\MyMusic**

**Vulnerability: 5: Guest Account**

**Host: 192.168.0.34**

**The guest account is not disabled on this computer.**

**Vulnerability: 6: Password Expiration**

**Host: 192.168.0.34**

**User account passwords do not have a valid expiration date. Mary**

**Vulnerability: 7: Local Account Passwords**

**Host: 192.168.0.34**

**User accounts do not have strong passwords. Mary**

**Vulnerability: 8: Windows Firewall**

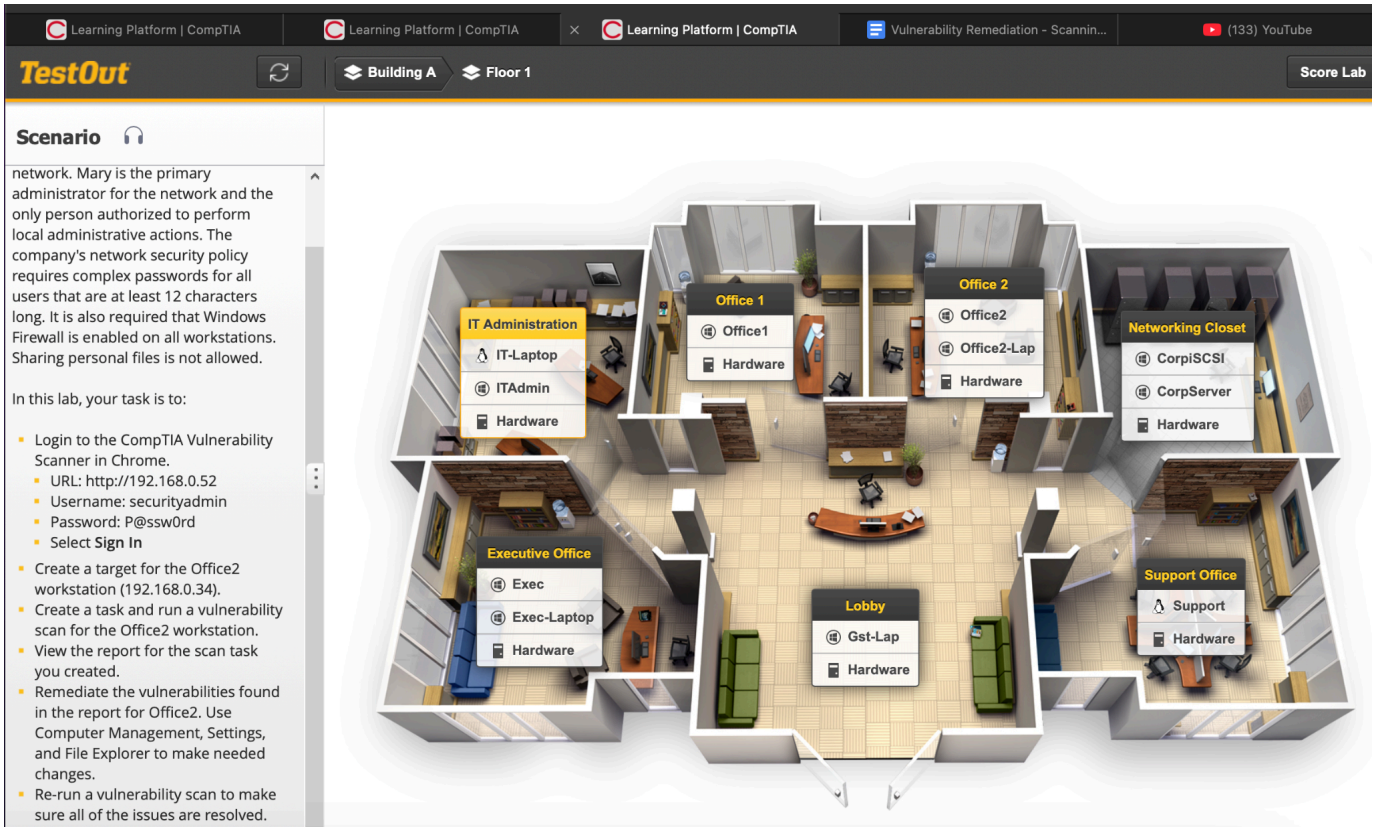
**Host: 192.168.0.34**

**Windows Firewall is disabled on this computer. Domain Firewall is Off Private Firewall is Off Guest or Public Firewall is Off “**

A total of 8 Vulnerabilities have been found! This is really bad because it gives an attacker too many options and attack vectors to that system.

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

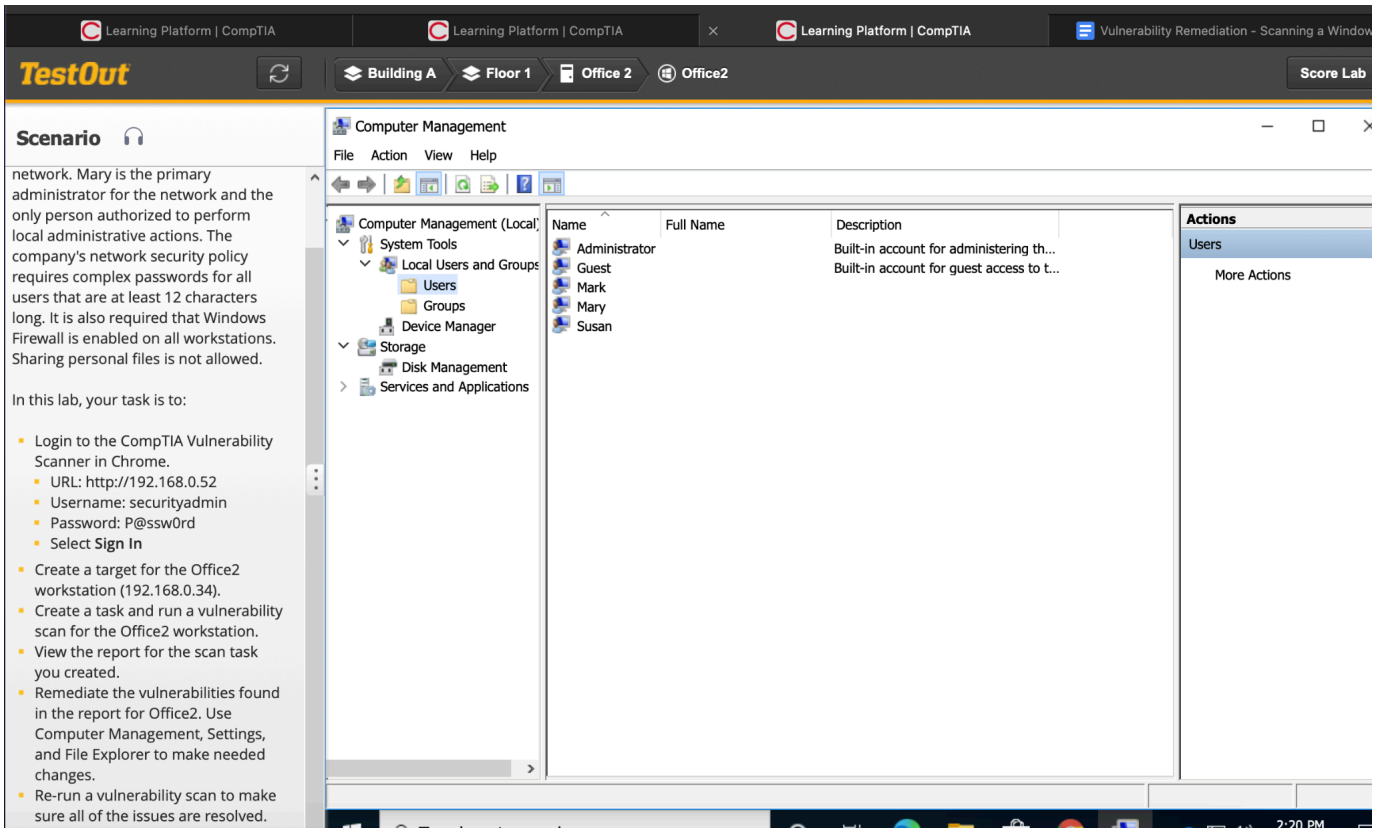
Now that I know what vulnerabilities there are, I can switch over to that computer and remediate / patch them. Since this is a hypothetical corporate environment I'll need to "walk" over to that computer. I'll do that now:




Clicking on "Office2" bring up the desktop GUI environment.

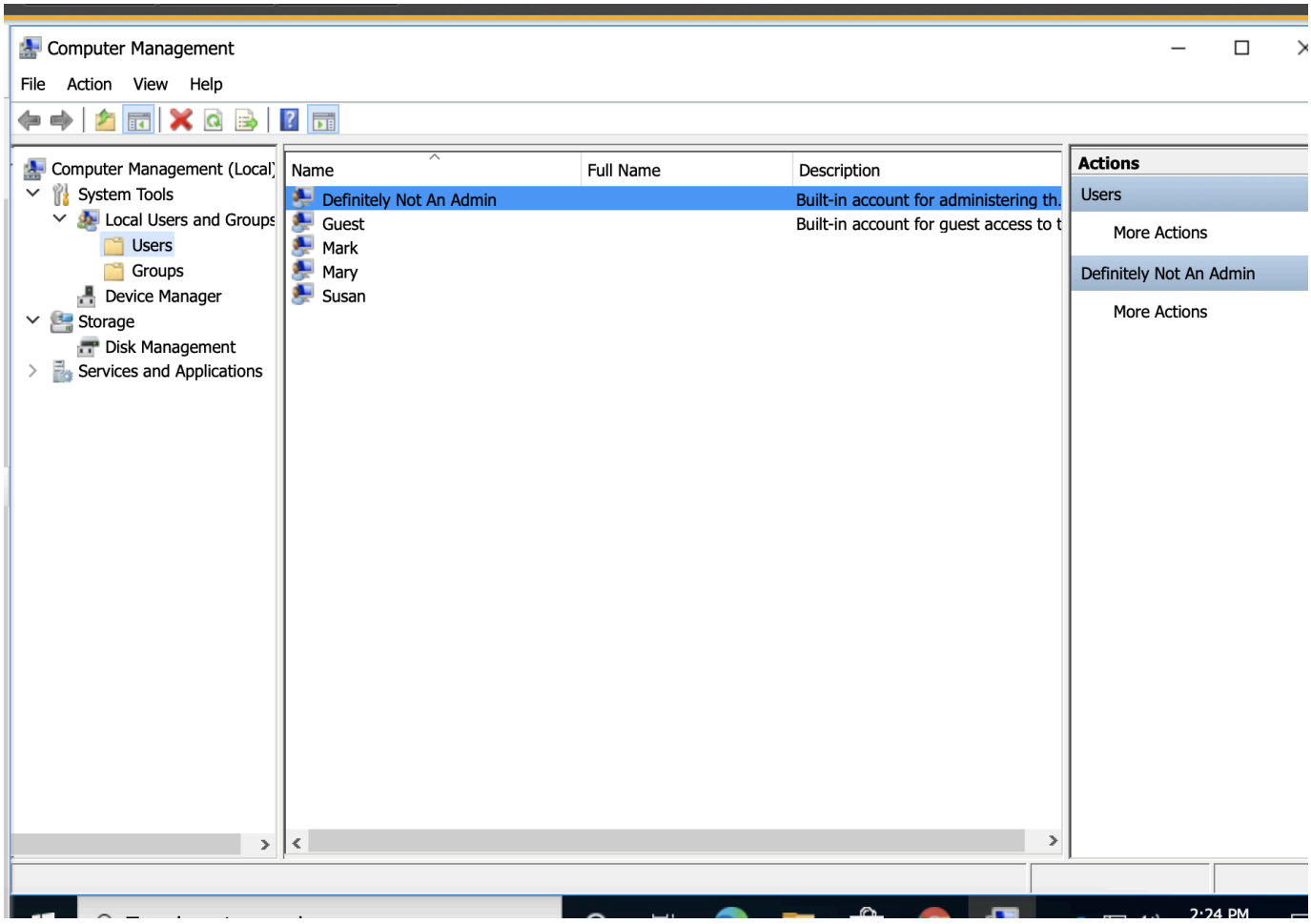
Vulnerability #1 and #2 says that there are user accounts locked out on this Windows machine as well as the built-in Administrator account. I will go to **Computer Management > Local Users and Groups.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024




I need to obfuscate the Built-In Administrator account to make it less obvious that this account is privileged. To do that I'll right-click on the account and select **Rename**.

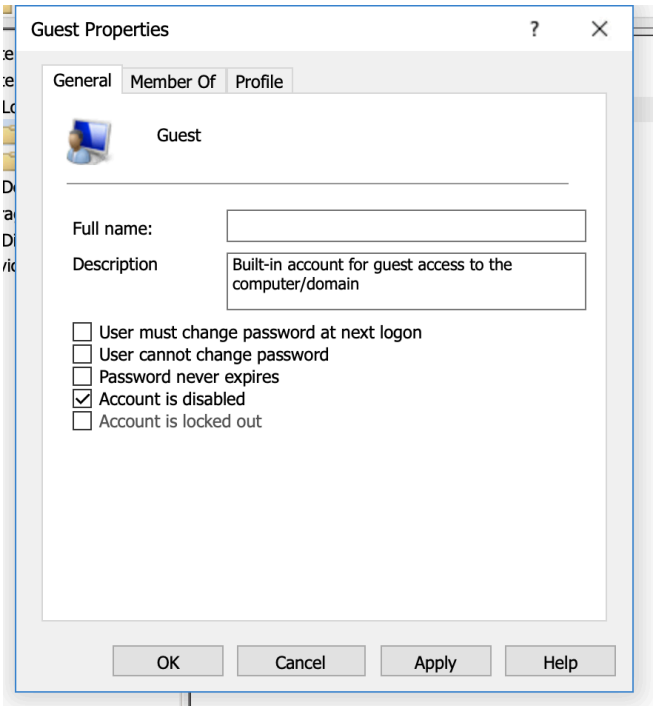
Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



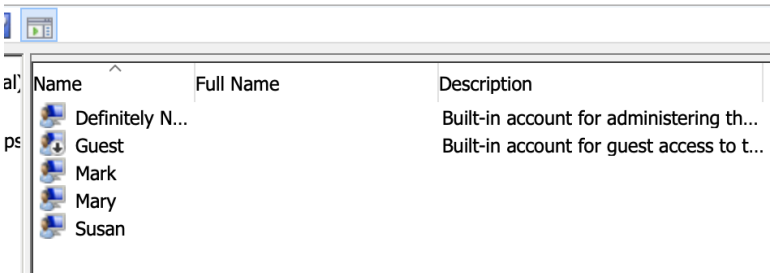

Since I am here , I can tackle **Vulnerability #5** which is to disable the Guest account. We only want authorized users to use this computer not any Guests.

Right-clicking the account and selecting **Properties** brings up a menu. On this menu I can click the checkbox which says **Disable this account.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



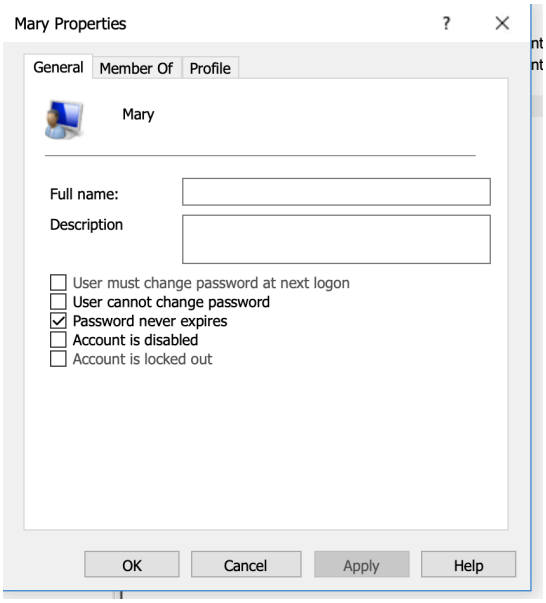

After I click **Account is Disabled** I will click **Apply** then **OK.**




Notice the black arrow next to the account. This means that the account is now disabled.

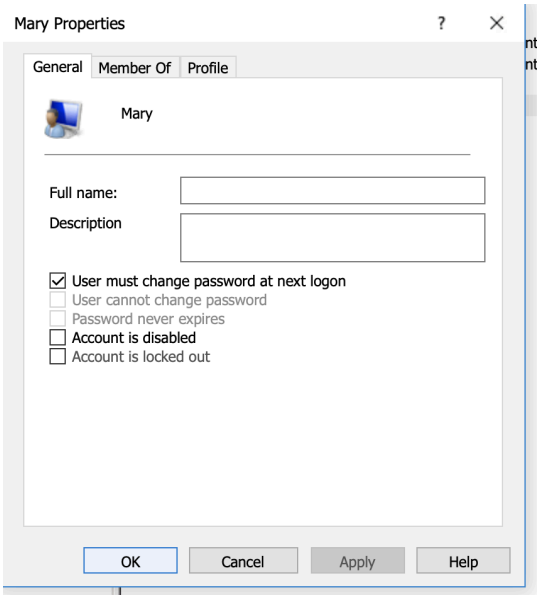
Let's now reset the password for Mary's account. Her account is locked out which means someone (or her) tried to log on and after multiple failed attempts the account was locked. I will right click Mary's account and select **Properties.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

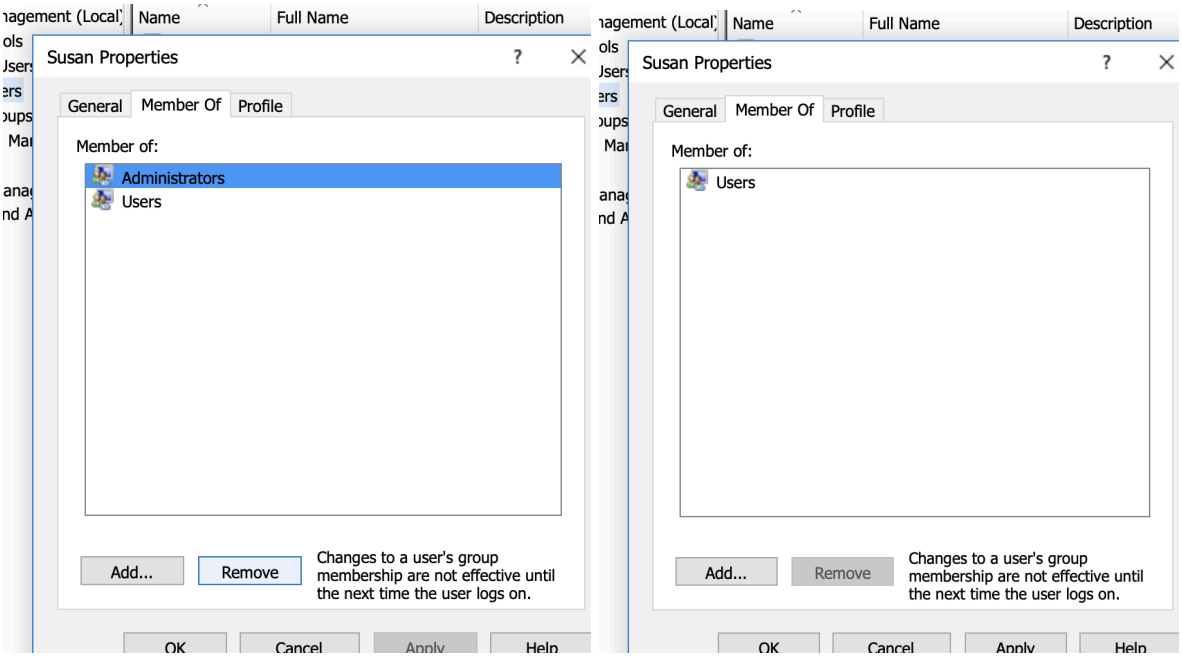



Notice that the checkbox **Password Never expires** is checked. This is not good , we want our users to have passwords changed on a schedule to prevent attackers from using any compromised passwords they might find.

I will un check that **Password Never expires** box and then check the box **User must change password at next logon.**



Now that's complete , I'll hit **Apply** then **OK.** Vulnerability #3 says that Susan is an administrator on this machine. This is not good because it introduces "**Shadow IT"** to the organization and presents another attack opportunity for attackers to get root/admin access. I'll right click Susan's name and hit **Properties.** On the top menu bar I'll click **Member Of** and then **Remove.**

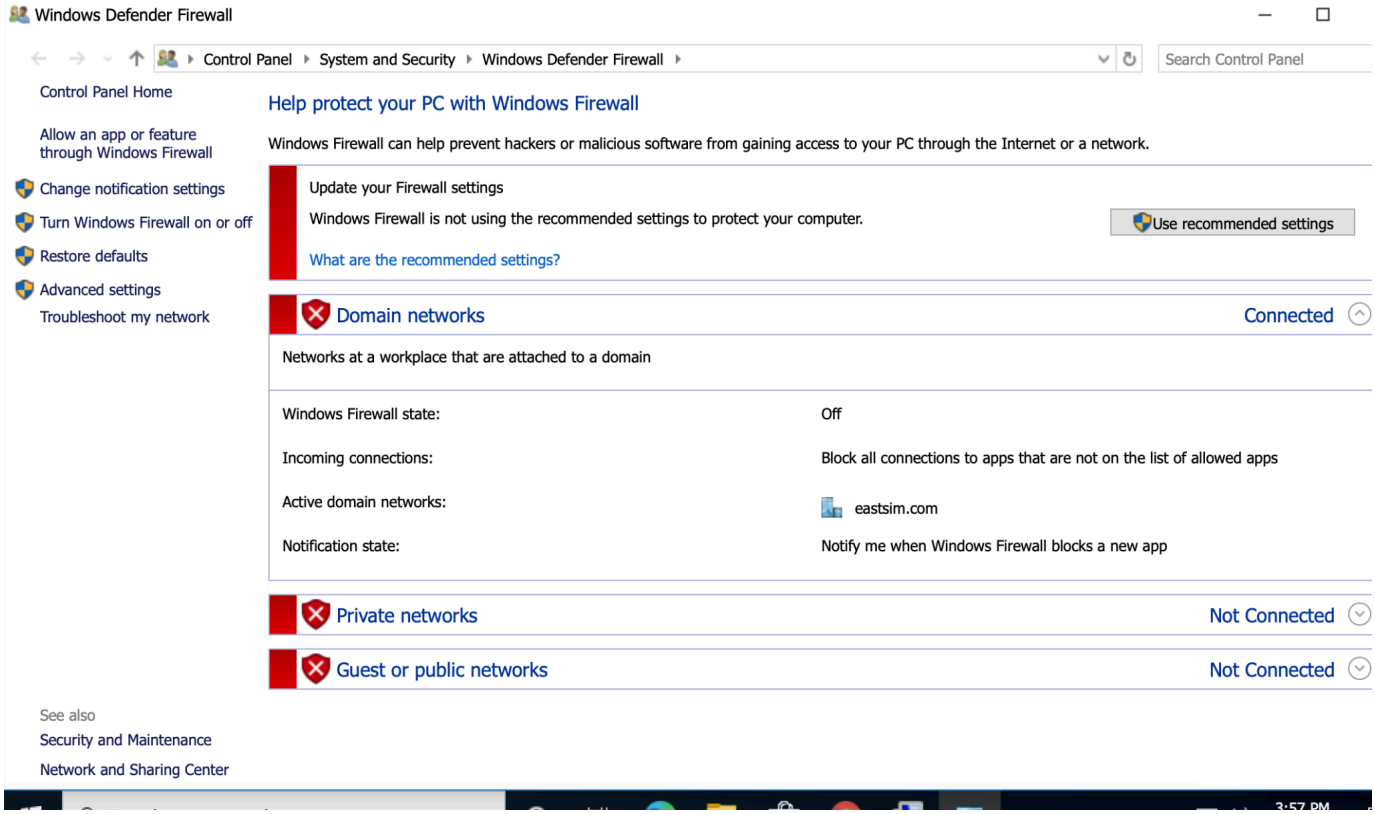



Once that's done I'll hit **Apply** then **OK.**

Now that we are done with the users accounts we can move on to remediating **Vulnerability #8 Windows Firewall is OFF.**

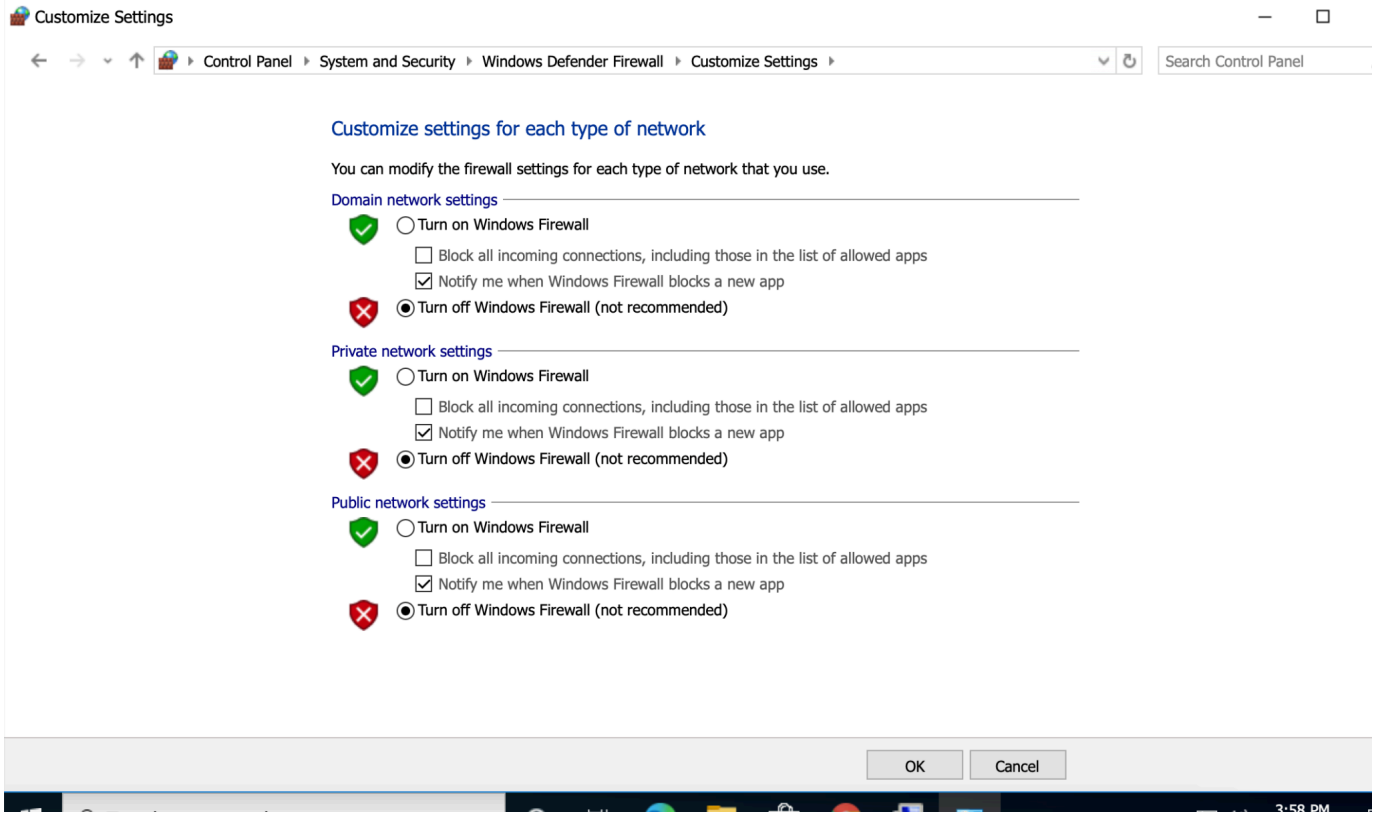
I will navigate to the **Windows Firewall** configuration by typing it in the search bar or by right clicking the Windows Logo and hitting **Settings.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



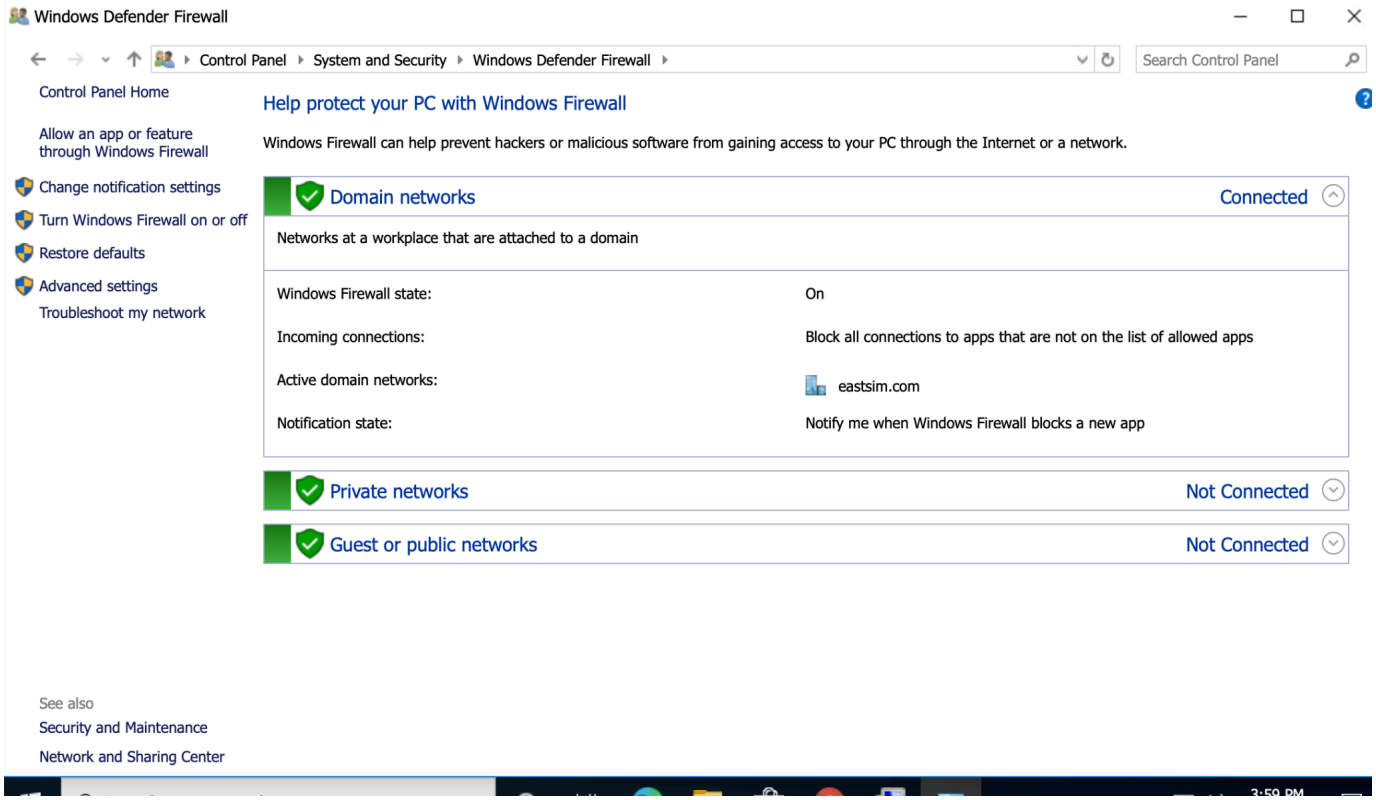

From the left pane I will select **Turn Windows Firewall on or off.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024




Notice how all the entries here are in the **OFF** state. I will need to check the boxes so that they are in the **ON** state.

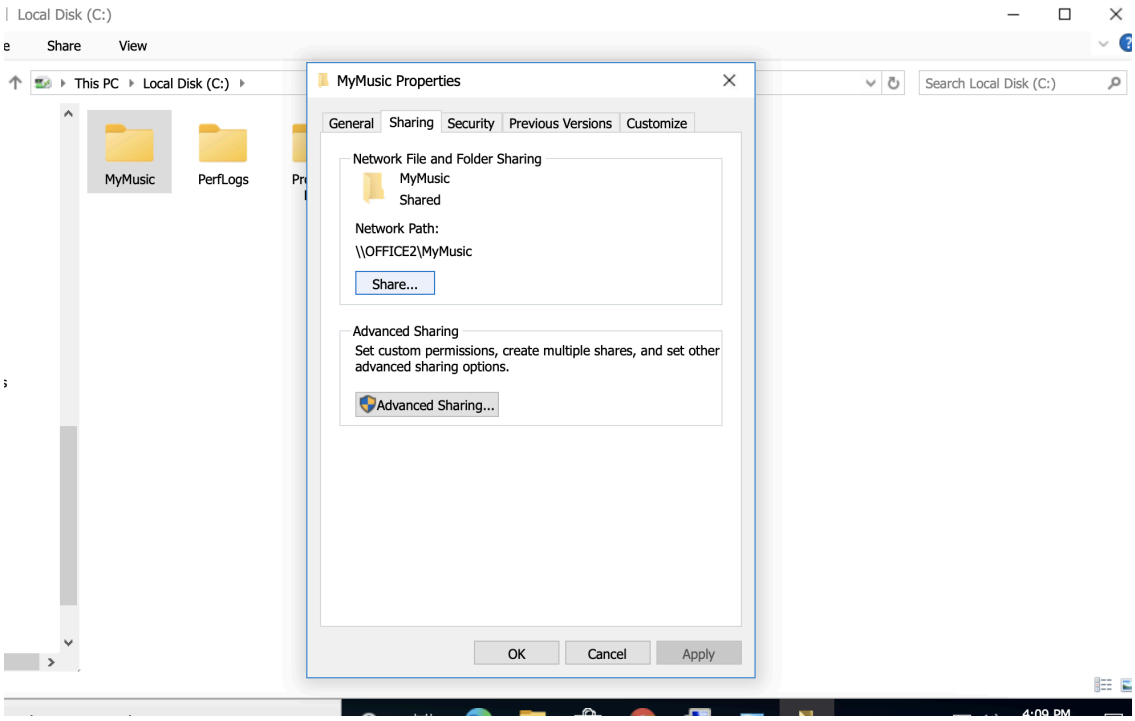
Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024




Now that the Firewall is configured we can move on to remediating **Vulnerability #4: Folders are shared from this computer. C:\MyMusic.**

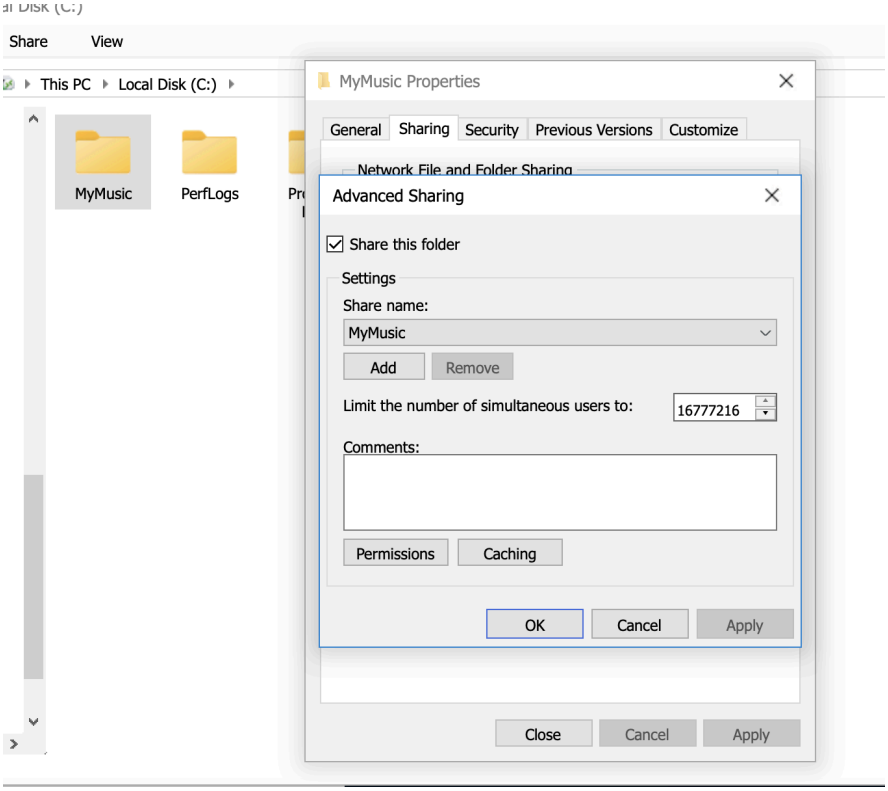
Now I need to clear the Local Fire share C:\MyMusic. I will navigate to the Folder on this computer listed above and select **Properties.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

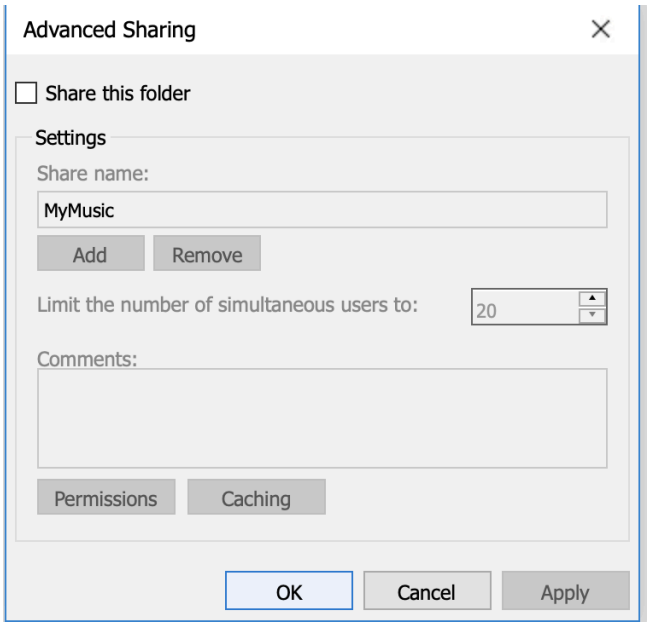



Now I will click the **Advanced Sharing** button to view the properties of this **SMB share.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

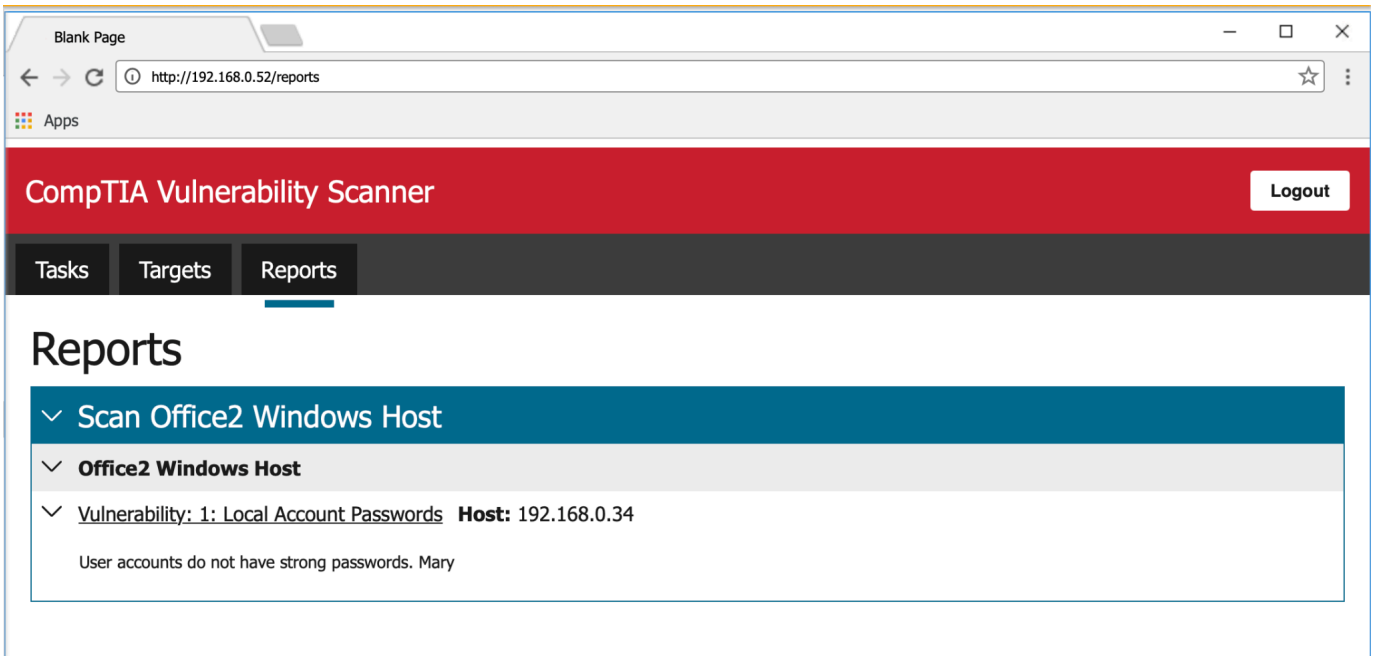



I will uncheck the box that says **Share this Folder** then hit **Apply** then **OK.**



Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

Now that I've remediated all of the vulnerabilities I will go back to my scanning machine and re run the scan to verify all of the issues have been resolved.




Note that the vulnerability for Mary's password is still here because we clicked **User must change password on first logon.** This vulnerability will clear once Mary sets a new password.

This now concludes the lab!

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024