

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."**

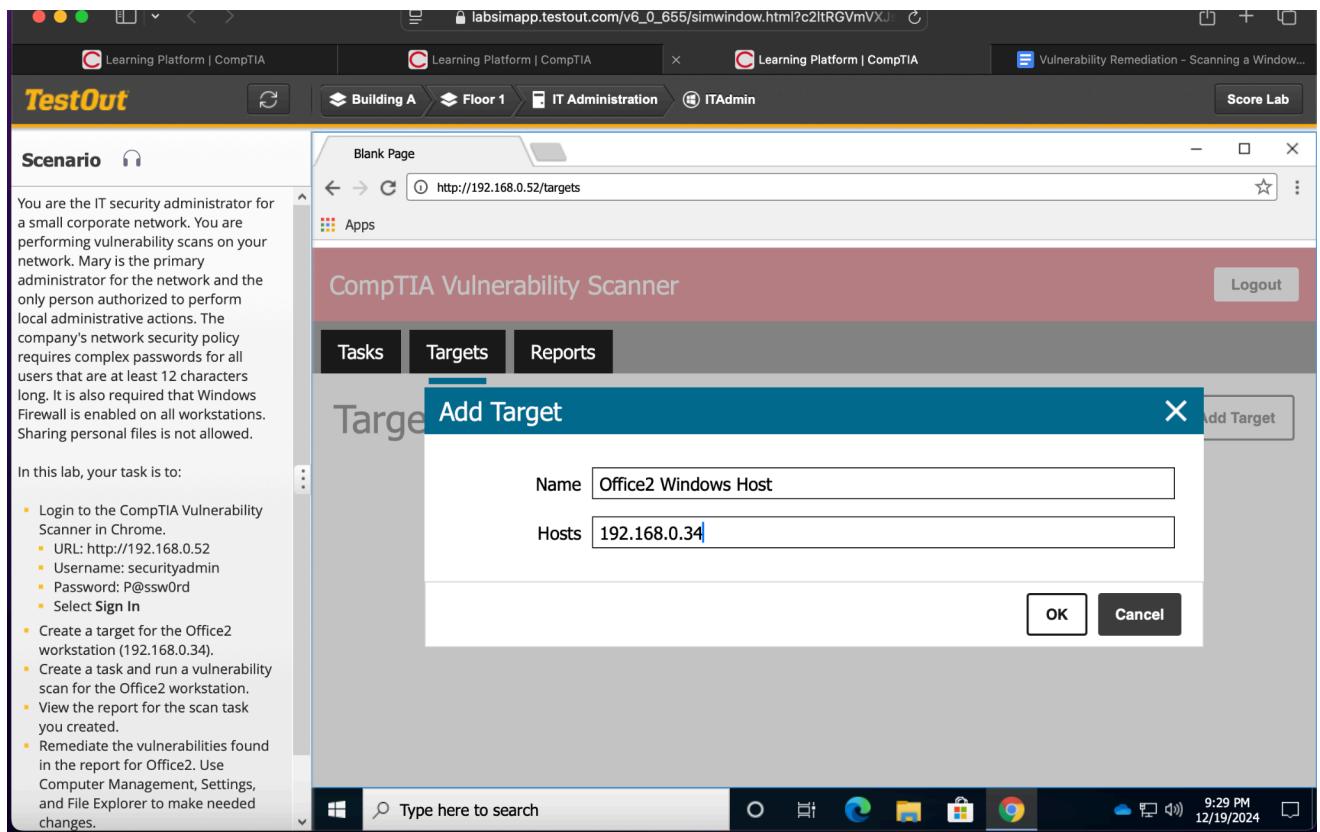
First I will start by logging in to the Vulnerability Scanner with the credentials provided. The password we're using here is not secure, it's just for demonstrate purposes.

Robert Carpenter

github.com/robertmcarpenter

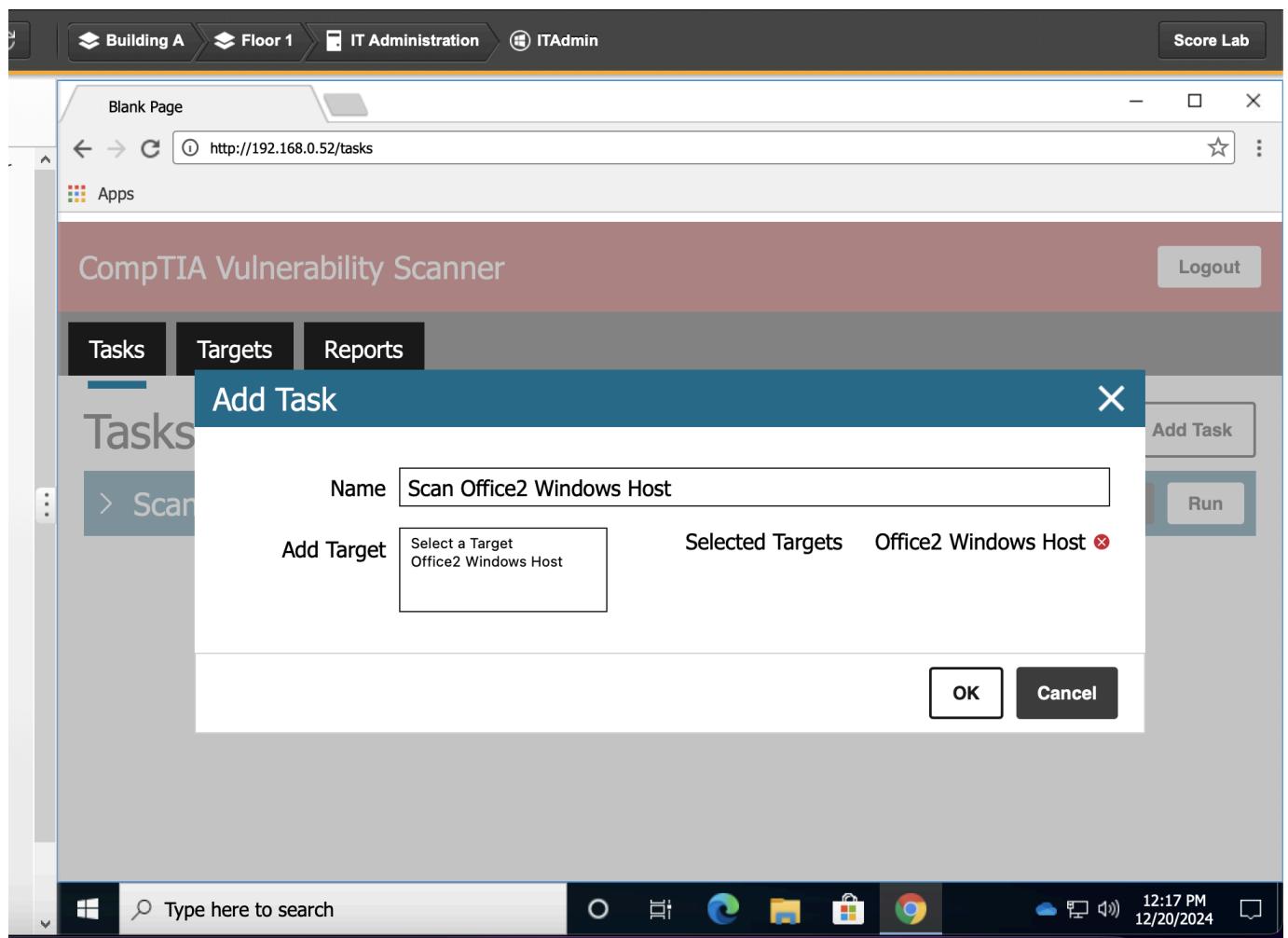
Thurs December 26th 2024

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**.

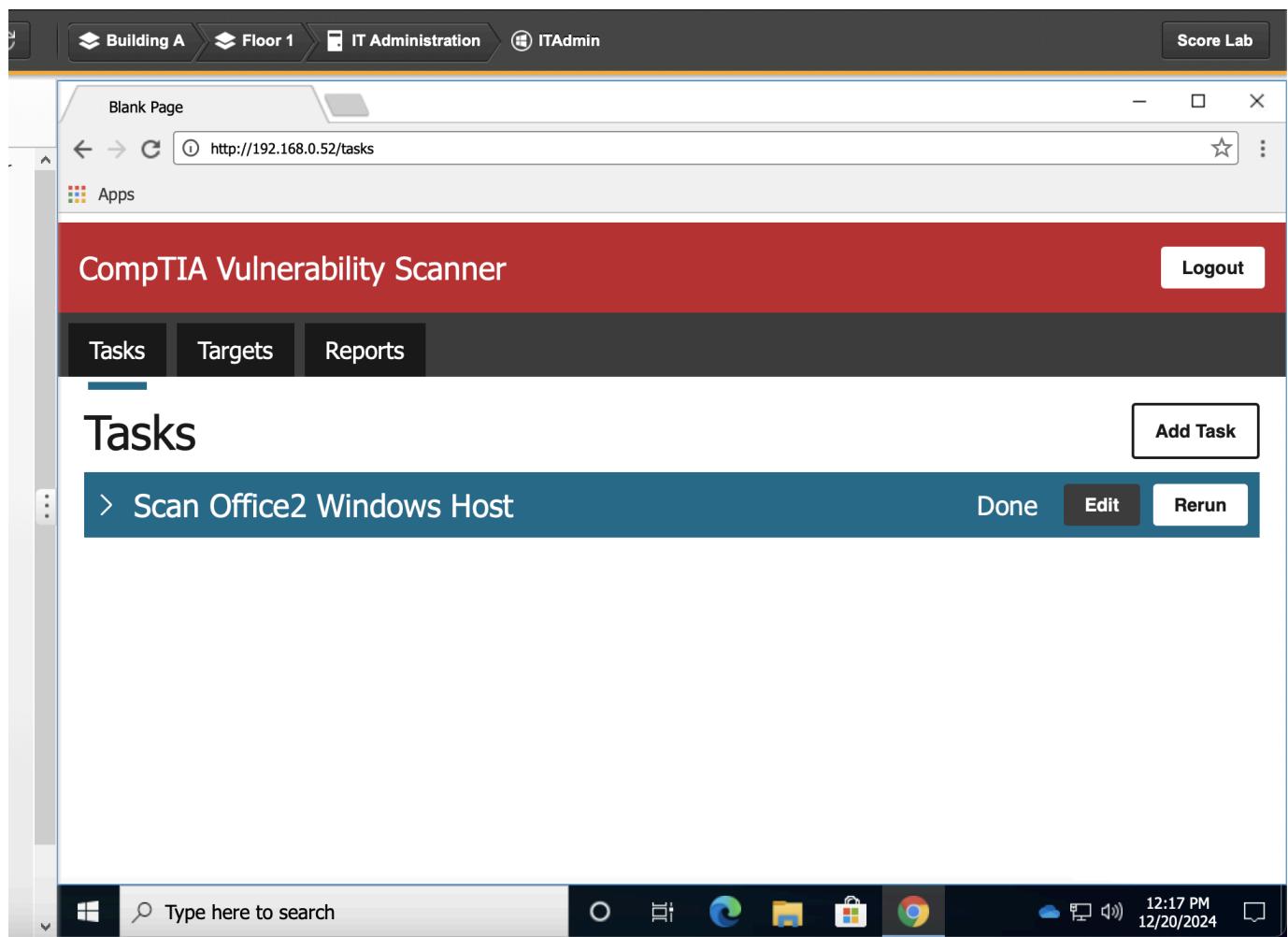
Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



The screenshot shows a web-based application titled "CompTIA Vulnerability Scanner". The top navigation bar includes icons for Building A, Floor 1, IT Administration, and ITAdmin, along with a "Score Lab" button. The main menu has tabs for Tasks, Targets, and Reports, with "Tasks" currently selected. A sub-menu under "Tasks" shows "Scan" and other options. The central area displays a modal dialog titled "Add Task". The "Name" field contains "Scan Office2 Windows Host". The "Add Target" section shows a dropdown menu with "Select a Target" and "Office2 Windows Host". To the right, "Selected Targets" are listed as "Office2 Windows Host" with a delete icon. At the bottom of the dialog are "OK" and "Cancel" buttons. The bottom of the screen shows a Windows taskbar with the Start button, a search bar, and various pinned icons like File Explorer, Edge, and Google Chrome. The date and time on the taskbar are 12/20/2024 at 12:17 PM.

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



The screenshot shows a web browser window titled "Blank Page" with the URL "http://192.168.0.52/tasks". The browser's top navigation bar includes icons for Building A, Floor 1, IT Administration, and ITAdmin, along with a "Score Lab" button. The main content area is titled "CompTIA Vulnerability Scanner" and features a red header with a "Logout" button. Below the header is a dark grey navigation bar with "Tasks", "Targets", and "Reports" tabs, where "Tasks" is currently selected. The main content area is titled "Tasks" and contains a list item: "> Scan Office2 Windows Host". To the right of this item are three buttons: "Done", "Edit", and "Rerun". The bottom of the screen shows a Windows taskbar with the Start button, a search bar, and various pinned icons like File Explorer, Edge, and Google Chrome. The system tray shows the date and time as 12/20/2024 at 12:17 PM.

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

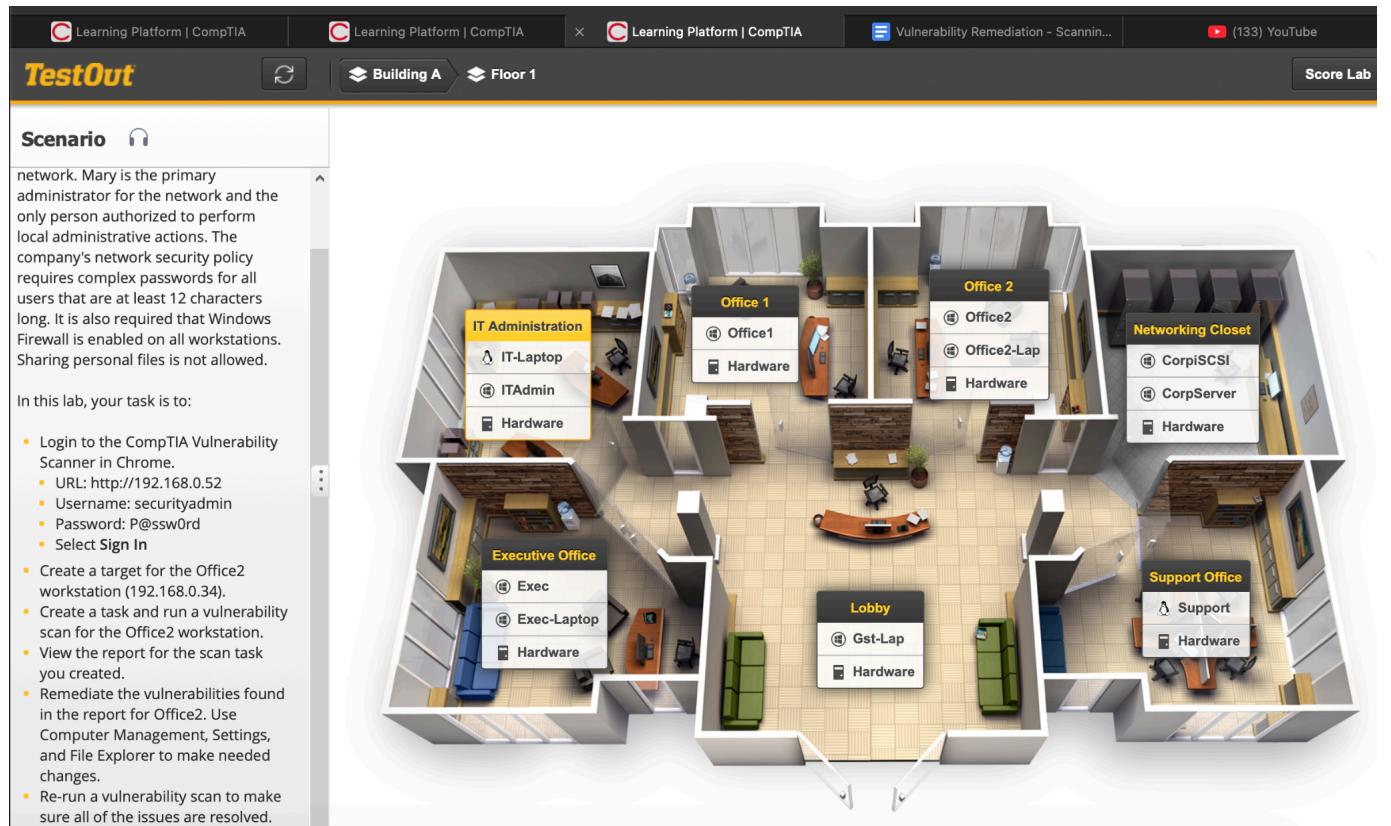
Vulnerability: 8: Windows Firewall

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.

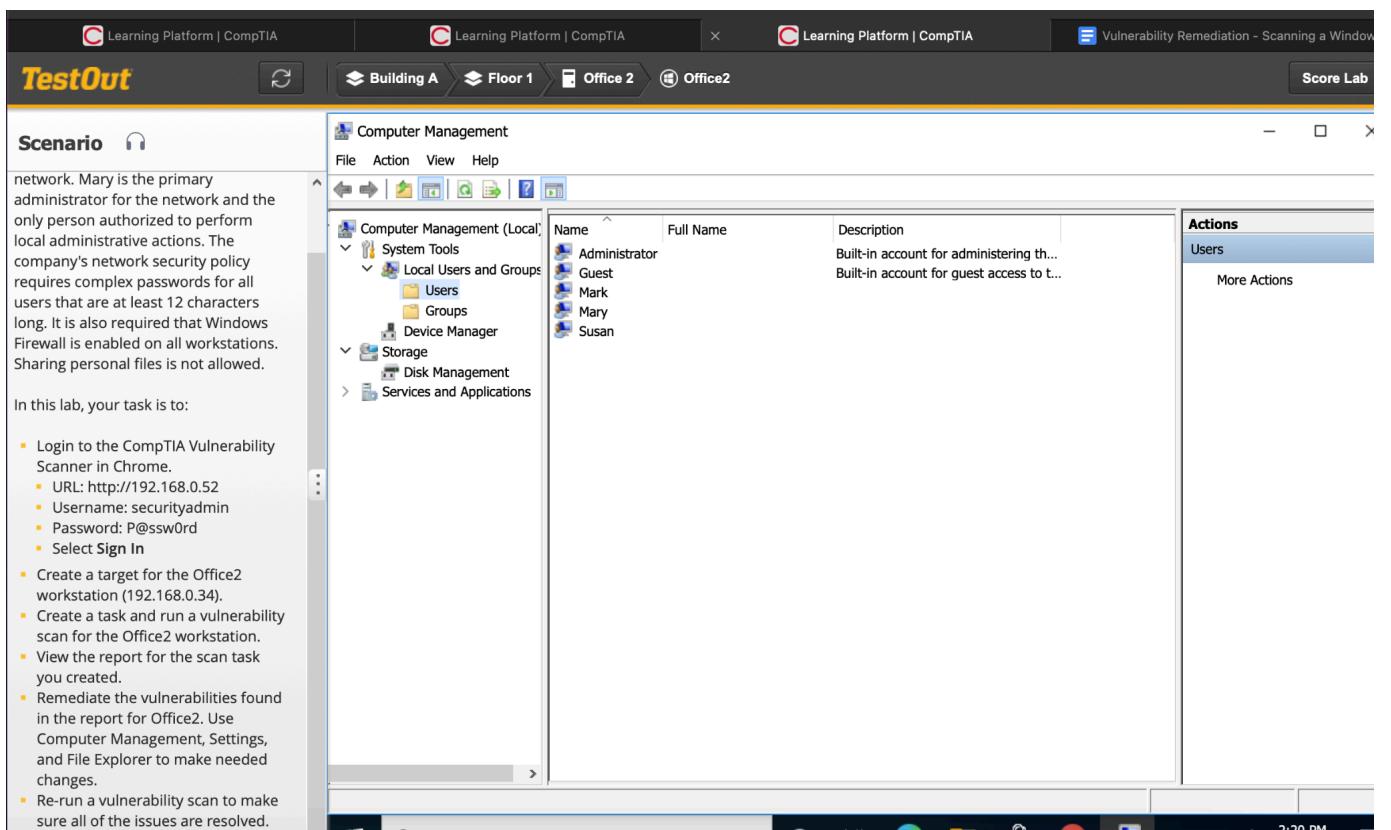
Now that I know what vulnerabilities there are, I can switch over to that computer and remediate / patch them. Since this is a hypothetical corporate environment I'll need to "walk" over to that computer. I'll do that now:



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



The screenshot shows a Windows desktop environment with multiple windows open. The main window is titled 'Computer Management' and displays a list of users under 'Local Users and Groups'. The users listed are:

Name	Full Name	Description
Administrator		Built-in account for administering th...
Guest		Built-in account for guest access to t...
Mark		
Mary		
Susan		

The left sidebar of the 'Computer Management' window shows various management tools: Computer Management (Local), System Tools, Local Users and Groups (selected), Device Manager, Storage, and Services and Applications.

Scenario (left panel):

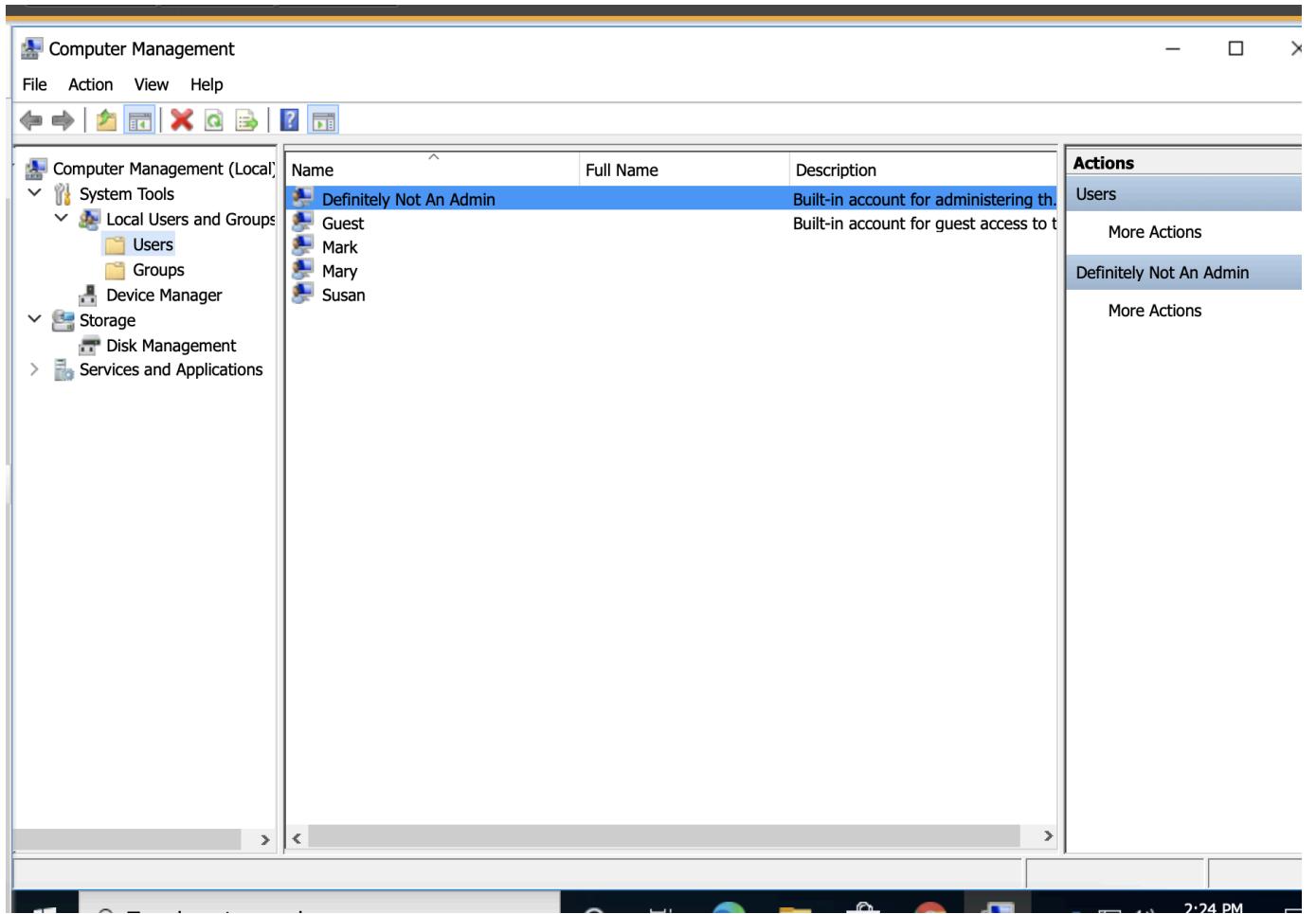
network. Mary is the primary administrator for the network and the only person authorized to perform local administrative actions. The company's network security policy requires complex passwords for all users that are at least 12 characters long. It is also required that Windows Firewall is enabled 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.

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



The screenshot shows the Windows Computer Management console with the Local Users and Groups snap-in open. The left navigation pane shows various system tools like System Tools, Local Users and Groups, Device Manager, Storage, and Disk Management. The Local Users and Groups node is expanded, and the Users node is selected. The main pane displays a table of users:

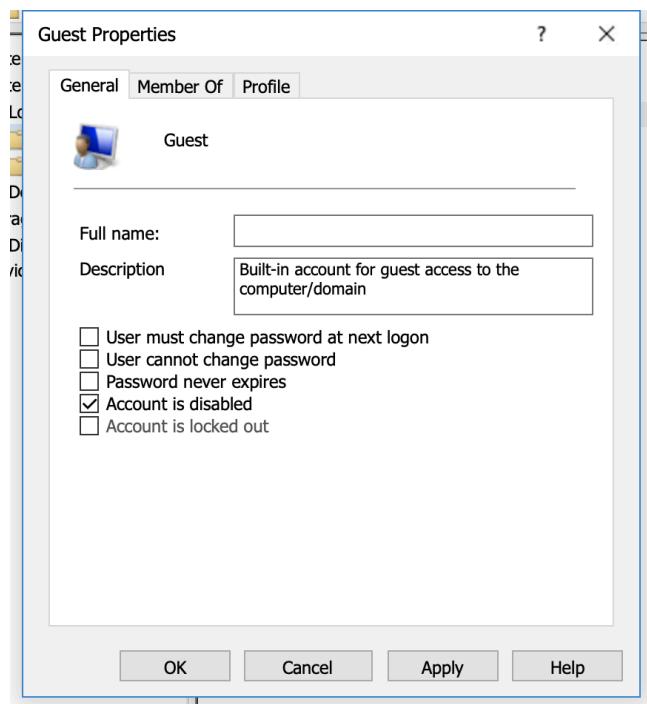
Name	Full Name	Description
Definitely Not An Admin		Built-in account for administering the computer.
Guest		Built-in account for guest access to the computer.
Mark		
Mary		
Susan		

The 'Actions' pane on the right shows 'Users' and 'More Actions' for the selected account 'Definitely Not An Admin'. The status bar at the bottom indicates the time as 2:24 PM.

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



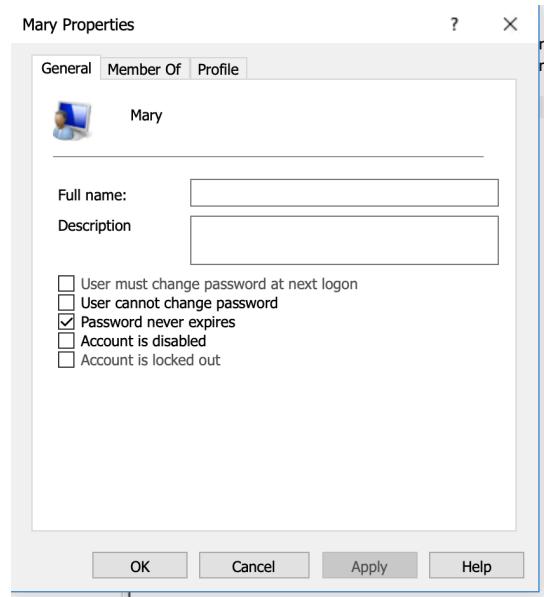
After I click **Account is Disabled** I will click **Apply** then **OK**.

Name	Full Name	Description
Definitely N...		Built-in account for administering th...
Guest		Built-in account for guest access to t...
Mark		
Mary		
Susan		

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

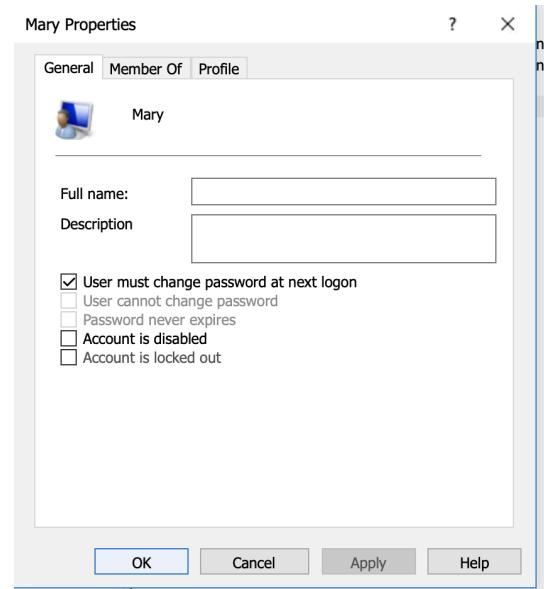
Let's now reset the password for Mary's account. Her account is locked out which means someone (or her) tried to log on and after multiple failed attempts the account was locked. I will right click Mary's account and select **Properties**.

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

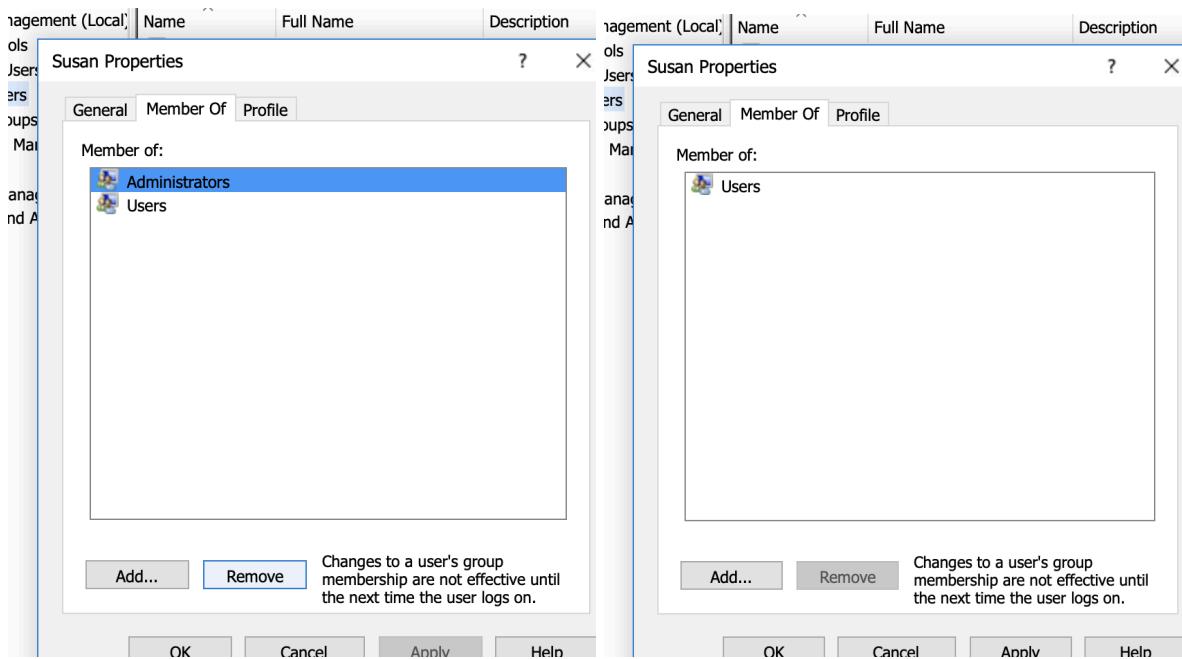


Notice that the checkbox **Password Never expires** is checked. This is not good , we want our users to have passwords changed on a schedule to prevent attackers from using any compromised passwords they might find.

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**.



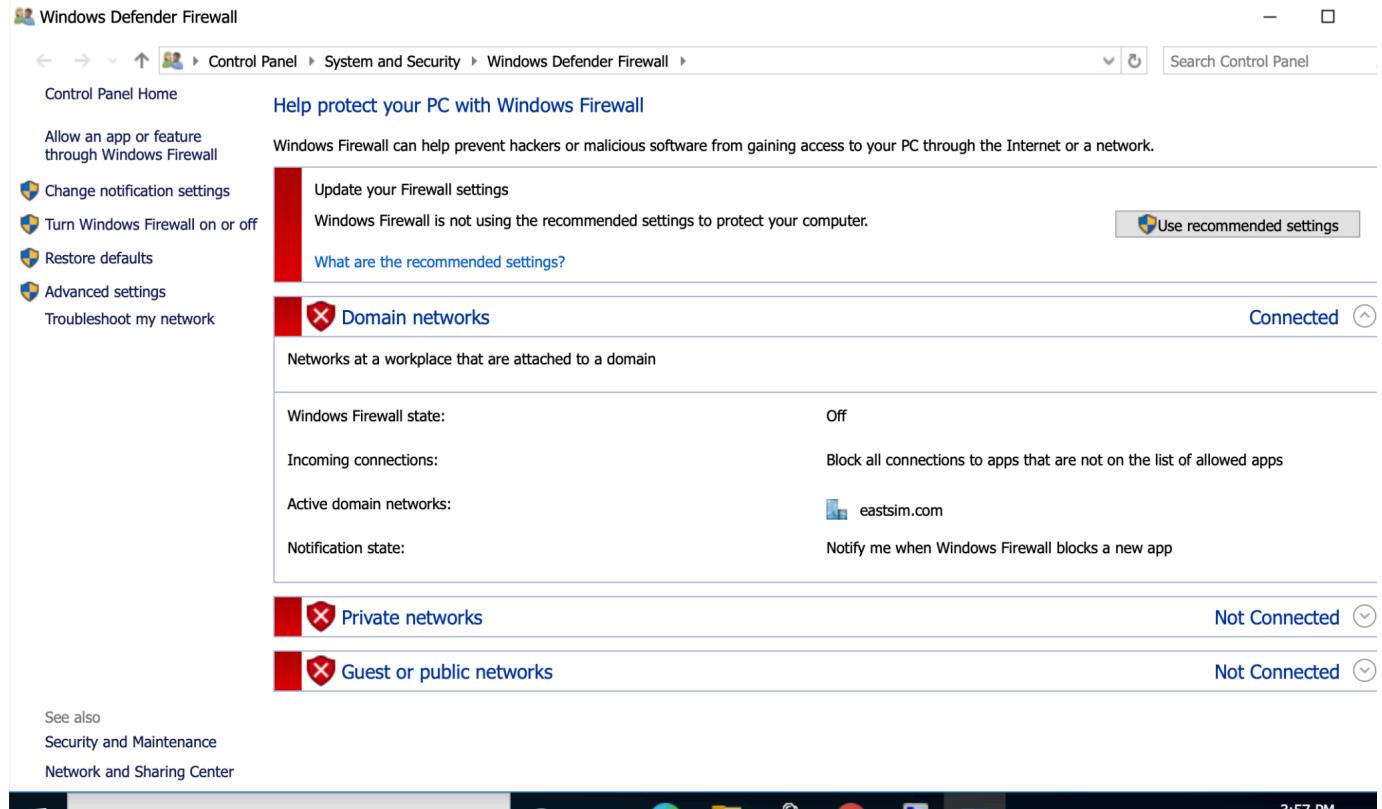
Once that's done I'll hit **Apply** then **OK**.

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

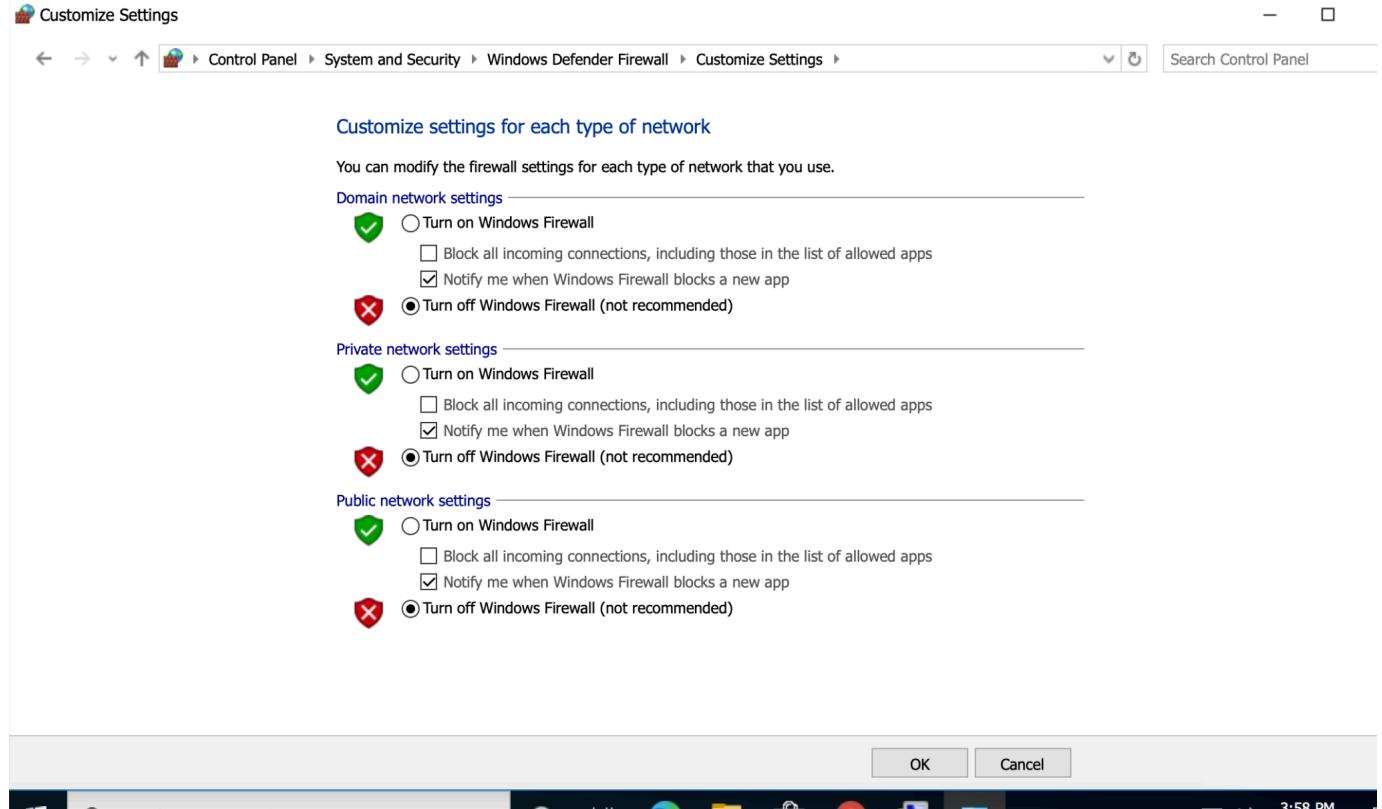


The screenshot shows the Windows Defender Firewall settings in the Control Panel. The left pane lists options like 'Control Panel Home', 'Allow an app or feature through Windows Firewall', 'Change notification settings', 'Turn Windows Firewall on or off' (which is selected), 'Restore defaults', 'Advanced settings', and 'Troubleshoot my network'. The right pane displays information about Domain networks, showing it is 'Connected'. It also shows the Windows Firewall state is 'Off', incoming connections are set to 'Block all connections to apps that are not on the list of allowed apps', and active domain networks include 'eastsim.com'. Notifications are set to 'Notify me when Windows Firewall blocks a new app'. Below this, sections for Private networks and Guest or public networks are shown as 'Not Connected'. At the bottom left, 'See also' links to Security and Maintenance and Network and Sharing Center are listed.

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

Robert Carpenter
github.com/robertmcarpenter

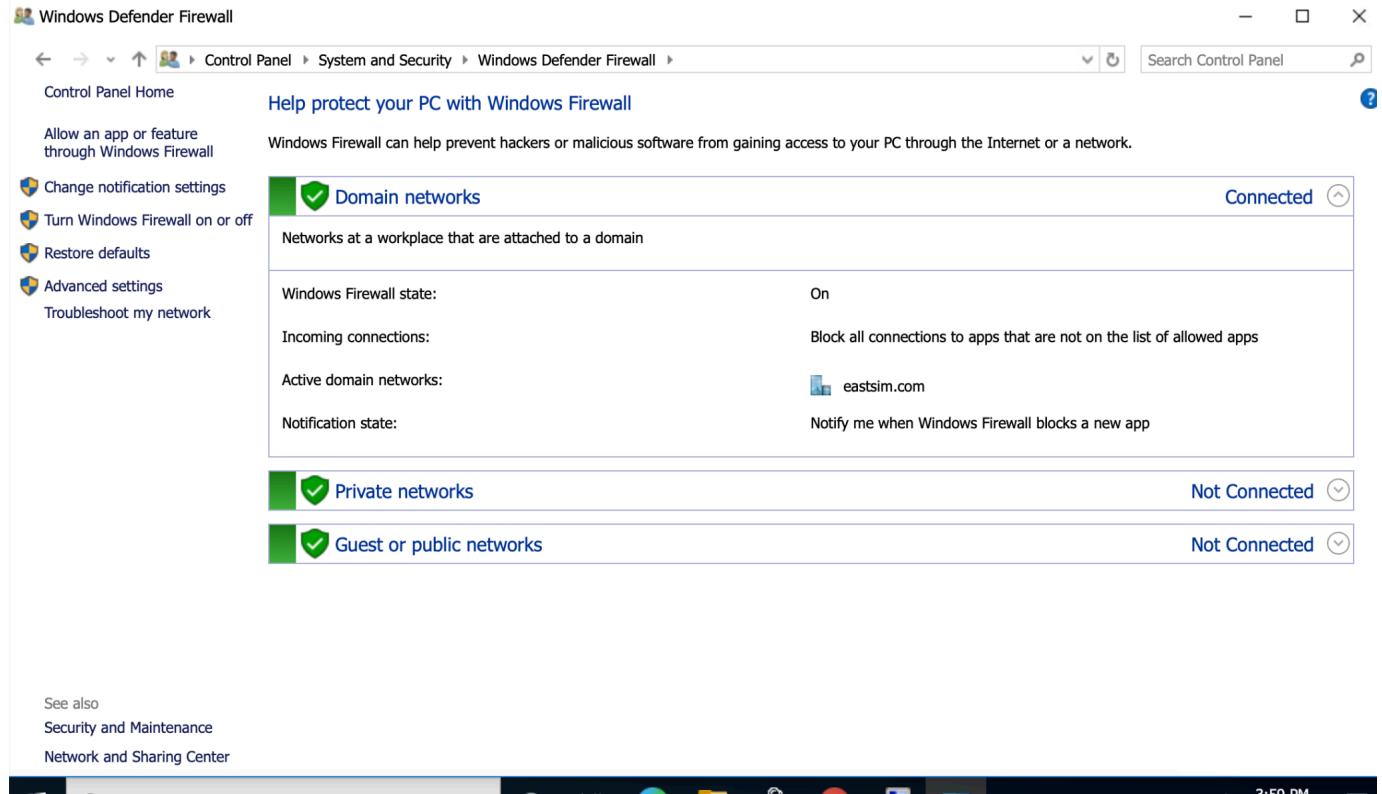
Thurs December 26th 2024



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

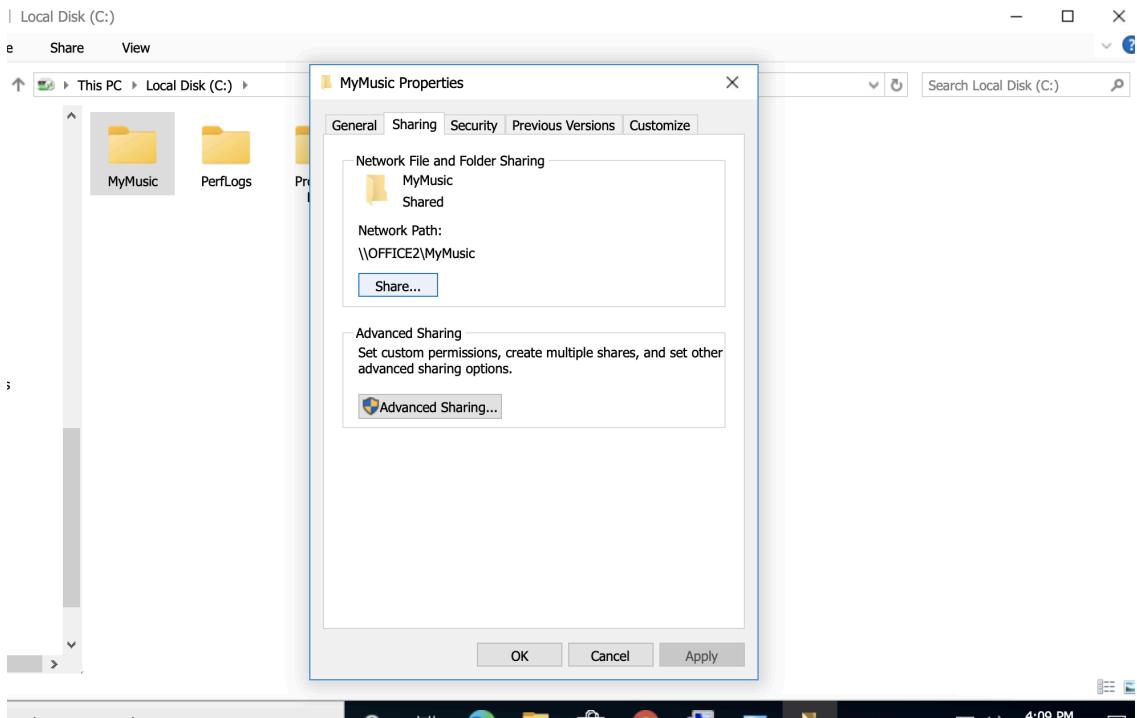


The screenshot shows the Windows Defender Firewall settings in the Control Panel. The main title is "Help protect your PC with Windows Firewall". It includes a link to "Control Panel Home" and a search bar. On the left, there's a sidebar with links like "Allow an app or feature through Windows Firewall", "Change notification settings", "Turn Windows Firewall on or off", "Restore defaults", "Advanced settings", and "Troubleshoot my network". The main content area is divided into sections for "Domain networks", "Private networks", and "Guest or public networks". Under "Domain networks", the status is "Connected". It shows the "Windows Firewall state" as "On", "Incoming connections" as "Block all connections to apps that are not on the list of allowed apps", and "Active domain networks" as "eastsim.com". The "Notification state" is set to "Notify me when Windows Firewall blocks a new app". The other two sections, "Private networks" and "Guest or public networks", both show "Not Connected". At the bottom, there's a "See also" section with links to "Security and Maintenance" and "Network and Sharing Center". The taskbar at the bottom shows several pinned icons.

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

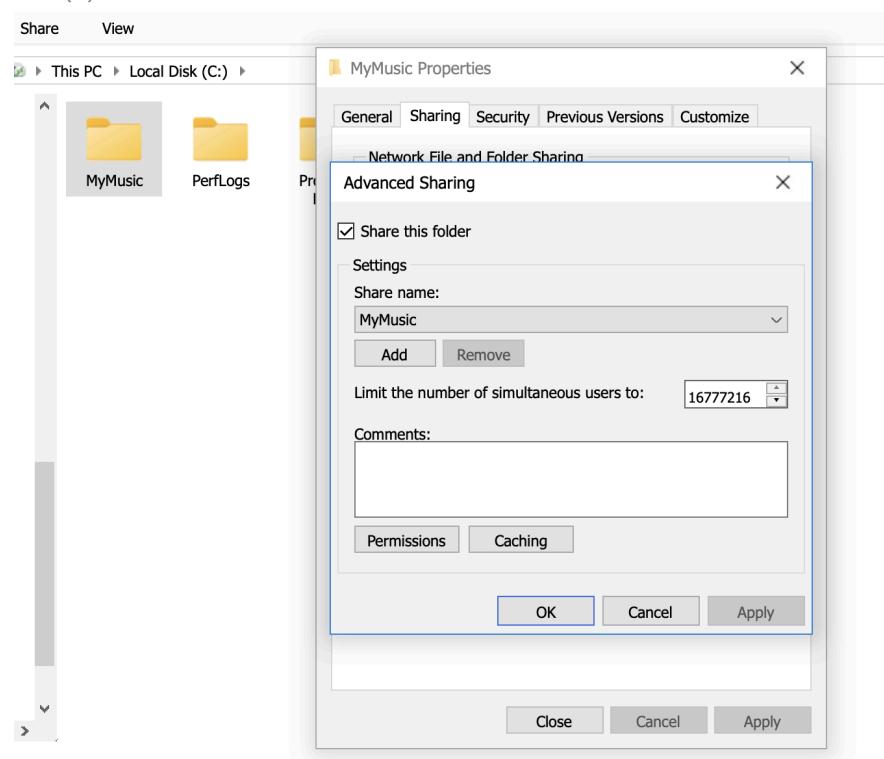
Now I need to clear the Local Fire share C:\MyMusic. I will navigate to the Folder on this computer listed above and select **Properties**.

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

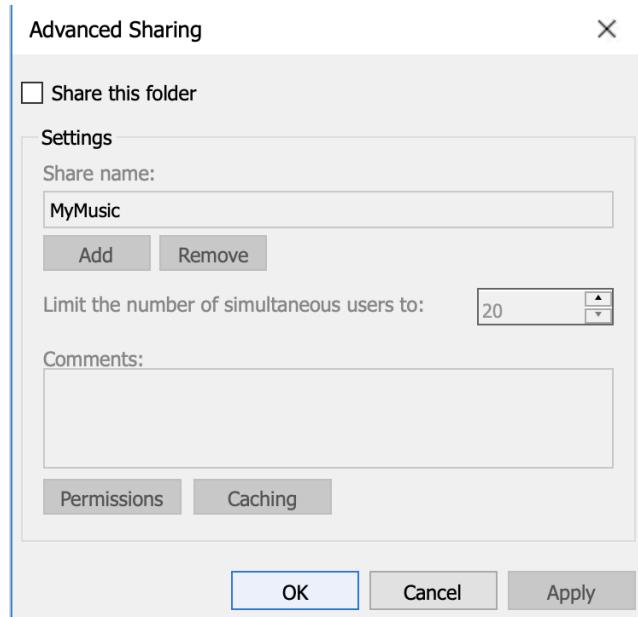


Now I will click the **Advanced Sharing** button to view the properties of this **SMB share**.

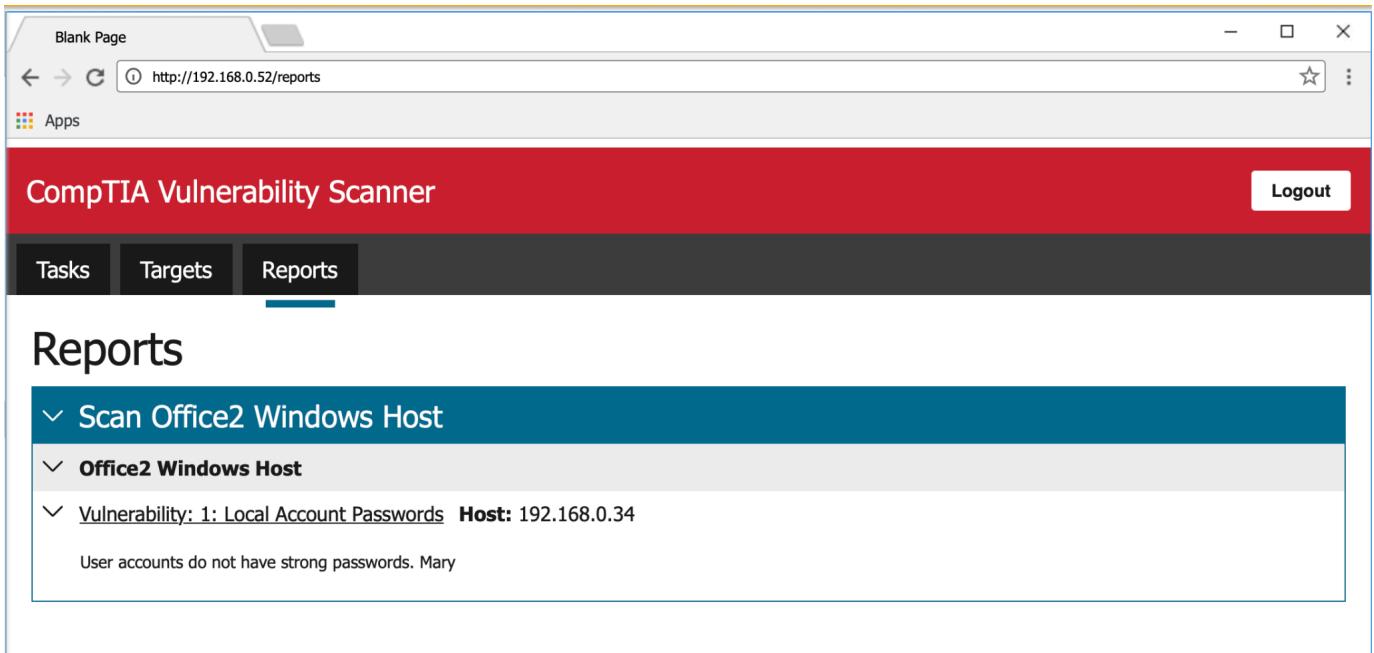
Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



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



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.



The screenshot shows a web browser window titled "Blank Page" with the URL "http://192.168.0.52/reports". The page is titled "CompTIA Vulnerability Scanner" and has a "Logout" button. A navigation bar at the top includes "Tasks", "Targets", and "Reports", with "Reports" being the active tab. The main content area is titled "Reports" and shows a list under "Scan Office2 Windows Host". The first item in the list is "Office2 Windows Host", which is expanded to show a vulnerability: "Vulnerability: 1: Local Account Passwords Host: 192.168.0.34". Below this, a note states: "User accounts do not have strong passwords. Mary".

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!

The screenshot shows a Windows 10 desktop environment. In the foreground, a TestOut application window is open, displaying a scenario about a user named Mary. The scenario details her role as the primary administrator and her password requirements. It also lists tasks such as logging in to the CompTIA Vulnerability Scanner and creating a target for the Office2 workstation. A 'Lab Report' window is overlaid on the TestOut interface, showing a score of 6/6 (100%) and a time spent of 22:35. The report includes a 'TASK SUMMARY' section with four required actions, each with a 'Show Details' link. In the background, the Windows Control Panel is visible, specifically the 'Windows Defender Firewall' settings. The taskbar at the bottom shows various pinned icons, including File Explorer, Edge, and Google Chrome.

Scenario

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.

Lab Report

Time Spent: 22:35

Score: 6/6 (100%)

TASK SUMMARY

Required Actions

- ✓ Remediate the Administrator account
- ✓ Disable the Guest account
- ✓ Remediate the Mary account [Show Details](#)
- ✓ Remediate the Susan account [Show Details](#)

See also

[Security and Maintenance](#)

[Network and Sharing Center](#)