CyberCenturion Interactive Demo: Teacher Guide

Thank you for downloading the CyberCenturion Interactive Demo!

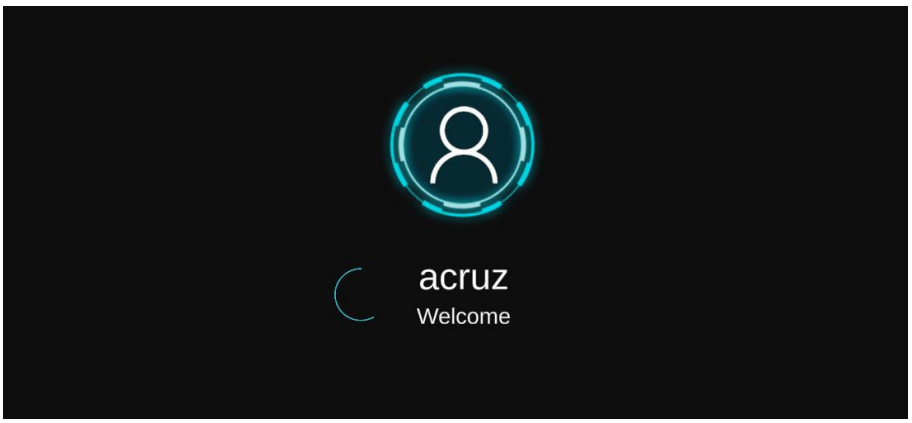
This demo has been put together to give you and your students and idea of what taking part in the CyberCenturion competition involves. The demo provides a virtual environment like those that will be used during competition rounds and allows teams to tackle a range of basic security problems.

This Teacher Guide will walk you through the main features of the demo, teams are then free to explore the available features of the virtual computer system and attempt to fix the security issues they find. **Please consult the README before use**. The README.txt file within this folder contains more information on the demo and the system requirements as well as some common errors you may encounter.

The second part of this guide walks you through some of the tasks in the demo and how to score points. It is not a full walkthrough but hopefully will point you in the right direction of further tasks!

Starting the demo

1. You must **extract the demo** before use. The demo may appear to work without extracting but you will run into issues and errors!
2. There are two versions of the demo available to use: a full-screen demo and a windowed version. Other than the size of the window they are both otherwise identical.
3. When you start the demo, you will see the user login screen below.



4. You will then be asked if you would like to start the tutorial. If this is the first time you are using the demo, **we strongly recommend that you follow the tutorial**.
5. After finishing the tutorial, you will be asked to enter the 12-character unique identifier. Take care when entering characters such as O and 0!
6. If you wish to revisit the tutorial at any point, use the Tutorial desktop shortcut.

Explore the demo

1. The first thing you should do after completing the tutorial is to **open the README**. This can be found on the desktop (this is a different README to the one in the folder you have downloaded).
2. In the CyberCenturion competition the README is a very useful document. The README provides hints and tips on what to look for on the computer system you are tasked with securing. The README also includes any rules that the system administrator has put in place such as password policies, authorised users and authorised software.
3. The **scoring report** (found on the desktop) provides an overview of the team's score. Included in the report is a score total and a breakdown on each of the current vulnerabilities that has been found. **Be careful!** It is possible to lose points for making changes to the system that make it less secure.
4. Forensics Questions are used throughout the CyberCenturion competition. These questions can be found on the desktop. The objective of the forensic question will vary from computer system to computer system but all of them will require you to explore the system in one way or another to uncover the answer. **Be careful!** Forensic question answers are case and spelling specific so take care when entering the answer.
5. It's now time to explore the computer system! The tutorial can be used to provide some further hints and tips on which areas of the computer to explore. **Good places to start are the control panel and the file explorer.**

Walkthrough

We are going to start by looking at the README as this contains clues on where we might find the security vulnerabilities.

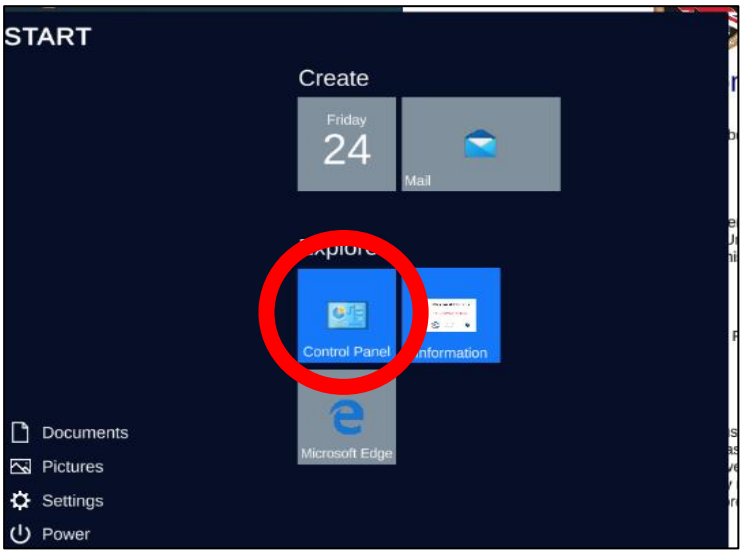
From the README we can pick out the following information:

1. The default web browser should be Microsoft Edge but Firefox must also be installed on the system.
2. There are no critical services.
3. All user accounts must be password protected.
4. Non-work-related media files are prohibited.
5. Hacking tools are prohibited.
6. We can also see a list of authorised administrators and authorised users, with their password, if applicable.

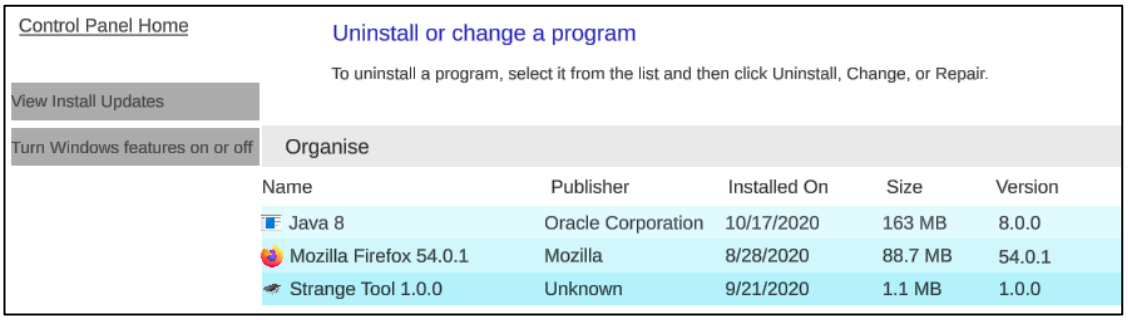
Removing malicious software

We will start with checking if there is any unauthorised software on the computer.

1. Open the start menu and the control panel.



2. Select ‘Programs and Features’
    a. **Note:** In a full image you will be able to explore all the features of the control panel. For the purposes of the demo only 'Administrative Tools’, ‘Programs and Features’ and ‘User Accounts’ are accessible.
3. We can now see a list of installed programs.



4. Remember, the README gave us some information on what programs and features are allowed on the computer. Firefox is **required.** ‘Hacking tools’ are **prohibited**. There are **no other essential services**.
5. With this in mind, we should **remove the ‘Strange Tool 1.0.0’**, as it’s not clear what this is, and it may be a malicious piece of software.
6. Select ‘Strange Tool 1.0.0’ and then press ‘Uninstall’.
7. **You should now receive some points. Congratulations! You have made the first change to secure the system.**

What happens if we remove ‘Mozilla Firefox 54.0.1’?

If we remove Mozilla Firefox in the same way, we will **lose points**! The README tells us that **Mozilla Firefox is an essential service**, so we should not remove it from the system.

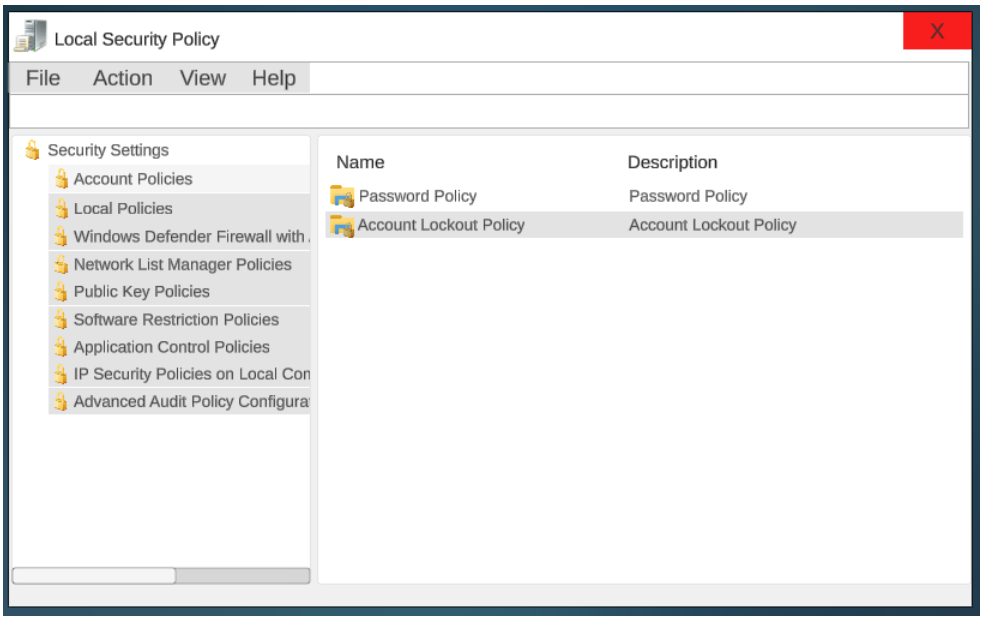
What happens if we remove ‘Java 8’?

Nothing! There are no essential services other than Mozilla Firefox and Microsoft Edge, so you won’t be penalised for removing Java 8. You also won’t score any points, as Java 8 is not a malicious piece of software.

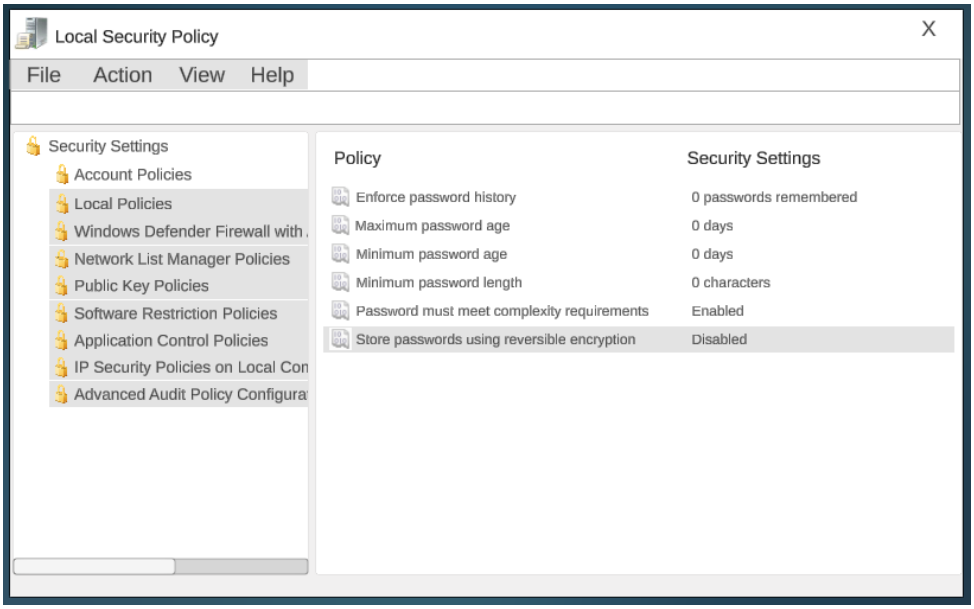
Establishing good security policies

We will now look at how we can make sure the security policies in place are suitable.

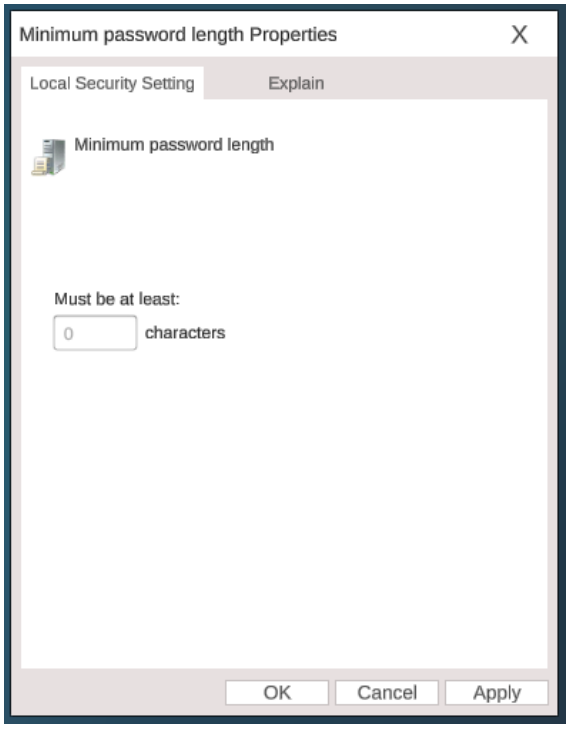
1. Go back to the control panel and select ‘Administrative Tools’.
2. Only one option is available to us in the demo, that’s ‘Local Security Policy’. Select it.
3. Security policy settings are the backbone of much of the security of the computer system you are working with. In the demo we are just going to look at Password Policy but there is lots more to explore and become familiar with!



4. Select ‘Password Policy’.



5. A good password policy has numerous features and you will be familiar with many of them – think of the restrictions that are in place when you create a new account on a website!
6. We are going to look at the 'minimum password length' policy. Select it.
7. We can see that currently there is no minimum length required for passwords. This is a bad policy! The longer the password the harder it is to guess!



These days, hackers can use software to 'brute force' (automatically work through every possibility) and 'crack' a password in no time at all if a poor security policy is in place. Typical times it might take a hacker can be seen in the table.

Password length	Time to crack
4 characters	Instantly
7 characters	6 minutes
10 characters	5 years

8. Set a minimum password length of 10 characters. Whilst the longer the password is the better, we also need to strike a balance between security and user friendliness – if a password is very difficult to remember a user may be tempted to write it down somewhere and this is bad practice!

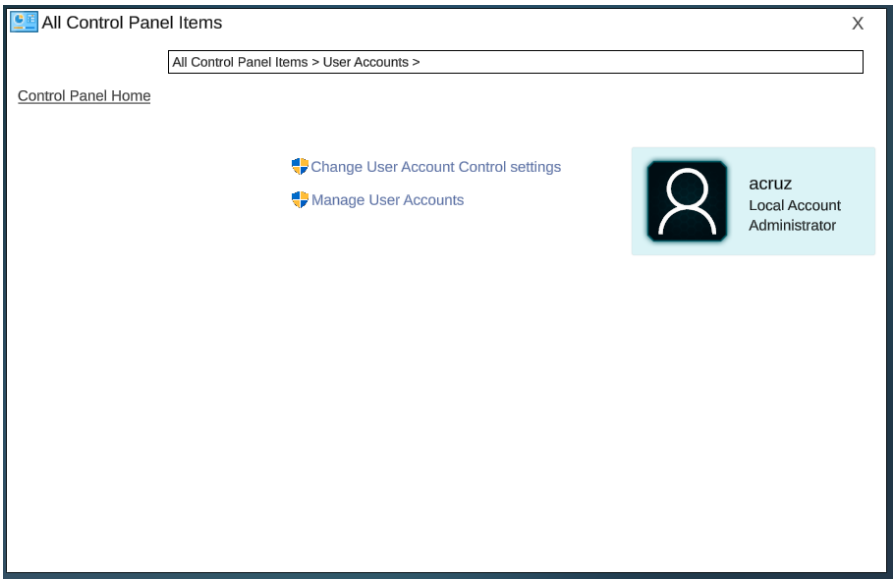
Setting a suitable password length is just one of the aspects of a good security policy, we should also consider things such as minimum and maximum password age and whether a password history is enforced.

We are not going to explore these in the demo. However, the CyberCenturion resources provide more information and the answer key gives specific guidance on good policies to enact in this demo.

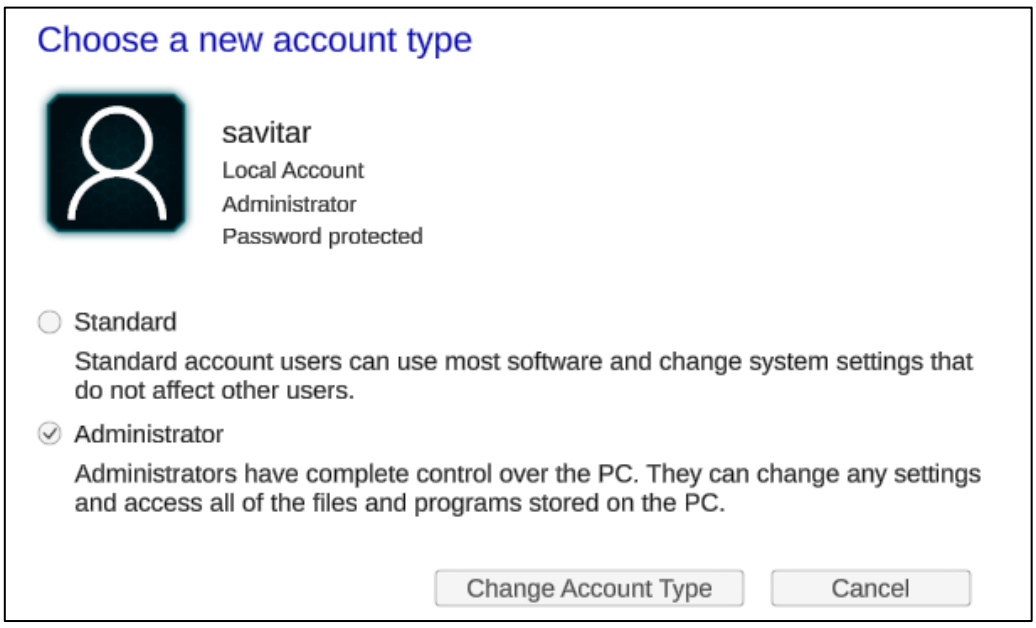
Checking authorised users

The README tells us which users are authorised to use the computer and of those, which are authorised administrators. Let's look to see how this compares to the current situation.

1. Once again open the control panel. This time, select 'User Accounts'.



2. Select ‘Manage user accounts’. We can now see a list of current users.
3. One of the first things we should look at is comparing the list of authorised administrators to the list given in the README.
4. We can see that ‘savitar’ is currently an administrator, however, the README tells us they should be a normal user!
5. Select the ‘savitar’ account.
6. Select ‘change the account type’



7. Change the account type to ‘Standard’. Confirm the change by pressing ‘Change account Type’
8. Congratulations! We have just taken another step to securing the system and scored some more points.

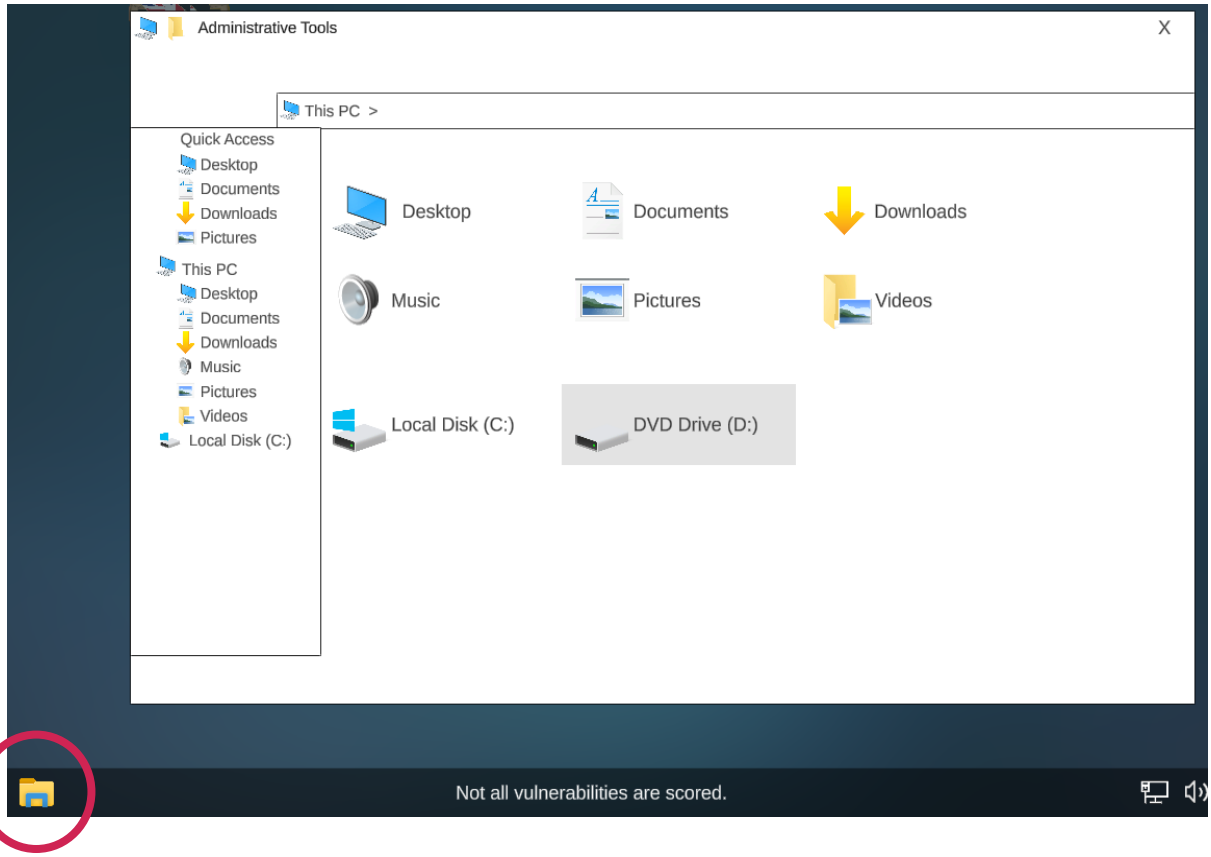
There is lots to unpick within the User Accounts section! We will look at one further element and leave it to you to explore the rest.

1. The README gives us a list of current administrator passwords, we can see that the password for ‘jwells’ is currently ‘quick’. This is not a secure password!
2. Select the user ‘jwells’ and then select ‘Change the password’
3. We now need to set a new, secure password that is inline with the current policy.
4. Set a secure password of your choice.
5. Congratulations, we have taken a further step to securing the system and scored some more points!

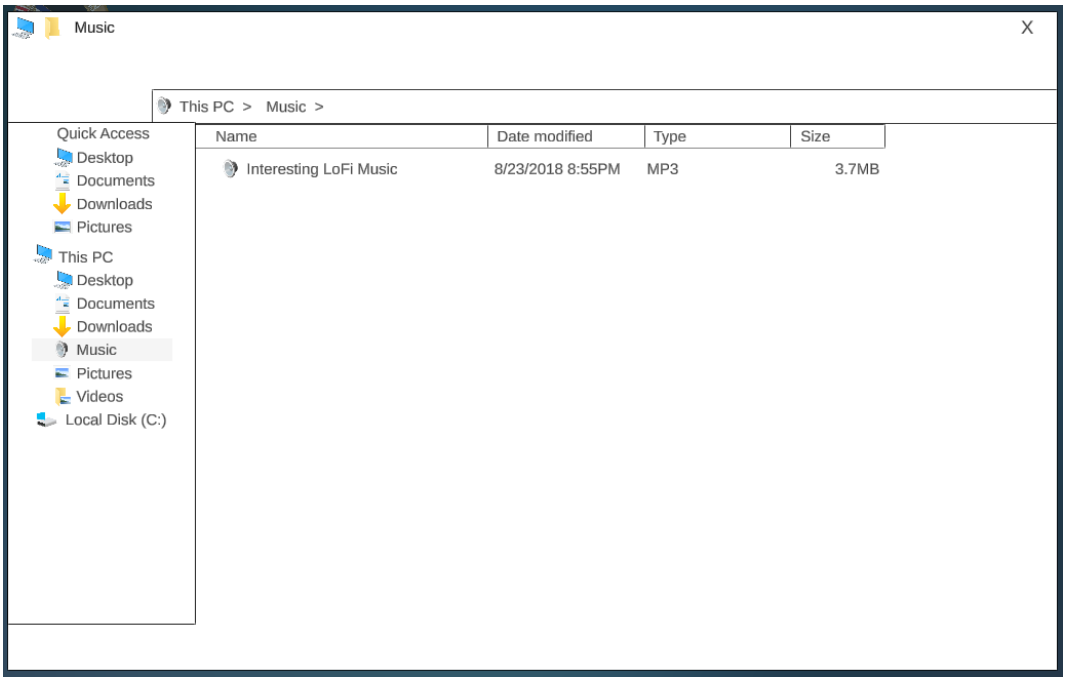
Removing unauthorised files

We will now look at how we can remove unauthorised files on the computer system. For this we will use the ‘File Explorer’ rather than the control panel. You will likely be familiar with the file explorer. The file explorer is a way of viewing, moving, and accessing the files on a computer.

1. Open the file explorer by selecting the shortcut on the taskbar.
2. The README tells us that non-work media files are unauthorised. We will explore the ‘Documents’, ‘Downloads’, ’Music’, ’Pictures’ and ‘Videos’.



3. In the ‘Music’ folder we can see ‘Interesting LoFi Music’. From the filename it is safe to assume this is non-work related, so we should delete it.

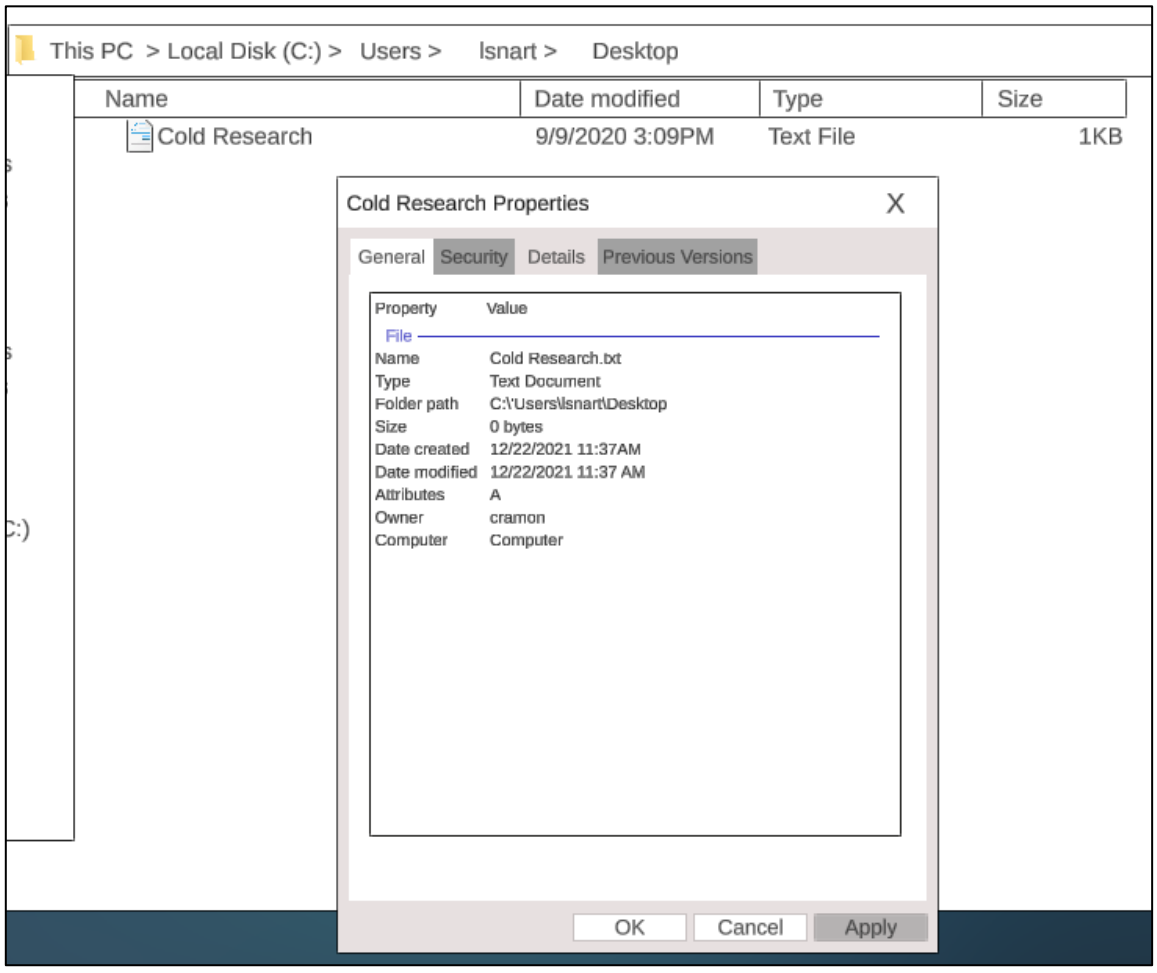


4. Right-click the file and select ‘Delete’. Congratulations, you have just earned some more points!

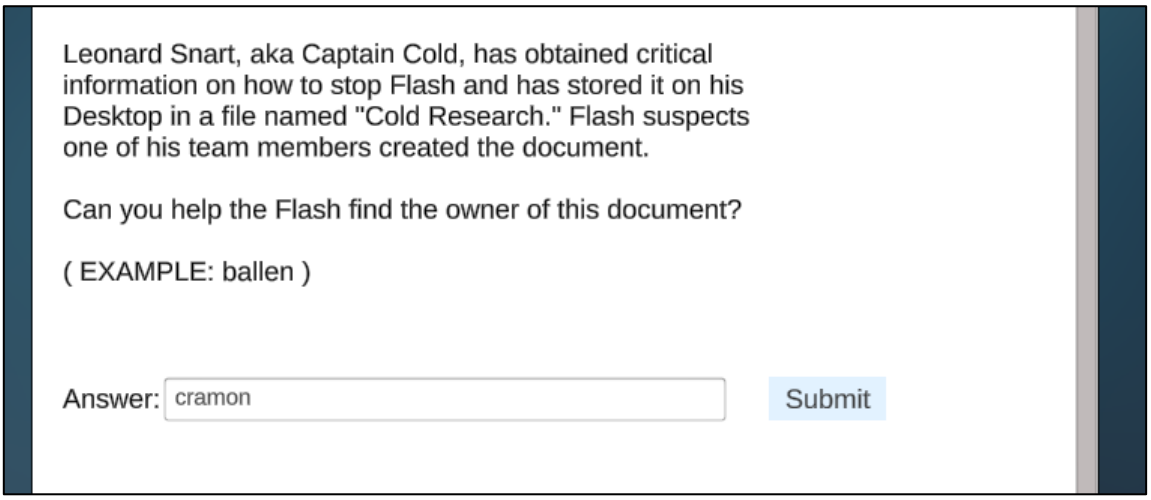
Answering forensics questions

Forensics questions are an important part of every CyberCenturion image and should not be ignored!

1. Open ‘Forensics Question 1’ on the desktop. The first part of the file tells us how to use and answer the forensics question. Scroll down to find the question we need to answer.
2. The question tells us that Leonard Snart has obtained critical information on how to stop Flash and stored it on his desktop. Flash needs to know where the information came from.
3. Leonard Snart is the user ‘lsnart’. We can’t log in as ‘lsnart’ but because we are logged in as an administrator we can see Leonard’s files!
4. Use the file explorer to navigate to lsnart’s desktop: **Local Disk (C:)/Users/lsnart/Desktop**
5. We can see the ‘Cold Research’ file on the desktop. Flash needs to know who created the file. To find this out, right click the file and select ‘Properties’ and then the ‘Details’ tab.
6. This has revealed the information Flash is looking for! We can see that the owner is ‘cramon’.



7. Enter this in the answer space provided in the Forensics Question 1 file. Be careful! Answers must be spelt correctly and in the correct case.



We've now explored the main elements of the demo image and are well on our way to scoring 100 out of 100! Take the time to explore the rest of the image and find the rest of the security vulnerabilities. In the CyberCenturion competition rounds you must work against the clock to secure as many elements of the system as possible, in the demo you have as much time as you need!

Remember to come back to the demo README to make sure that the changes you make to the system are in line with the policies set!

Good luck!

Note: The CyberCenturion demo image features an answer key (found in the README). The **answer key contains a full list of all the vulnerabilities** that can be found and corrected, check it out if you get stuck!