CyberPatriot Windows 11 README

Please read the entire README thoroughly before modifying anything on this computer.

Unique Identifier

If you have not yet entered a valid Unique Identifier, please do so immediately by double clicking on the "CyberPatriot Set Unique Identifier" icon on the desktop. If you do not enter a valid Unique Identifier this VM may stop functioning after a short period of time.

Forensics Questions

If there are "Forensics Questions" on your Desktop, you will receive points for answering these questions correctly. Valid (scored) "Forensics Questions" will only be located directly on your Desktop. Please read all "Forensics Questions" thoroughly before modifying this computer, as you may change something that prevents you from answering the question correctly.

Competition Scenario

You work for Adams, Ferguson, & Associates (AFA), a major DC law firm that specializes in corporate law. AFA has recently merged with another law firm overseas and is in the process of upgrading their IT infrastructure.

AFA's security policies require that all user accounts be password protected. Employees are required to choose secure passwords, however this policy may not be currently enforced on this computer. The presence of any non-work related media files and "hacking tools" on any computers is strictly prohibited. This company currently does not use any centralized maintenance or polling tools to manage their IT equipment. This computer is for official business use only by authorized users. Your job is to secure this computer, within the guidelines of the scenario, while ensuring the availability of authorized business critical software and services.

Company policy states that Windows Action Center should be enabled and monitoring the security status of desktop Windows operating systems at all times.

This is a critical computer in a production environment. Please do **NOT** attempt to install Windows "Feature Updates" or "Insider Preview Builds." Please do **NOT** attempt to use the Windows recovery options "Reset this PC" or "Go back to an earlier build".

Windows 11

It is company policy to use only Windows 11 on this computer. Management has decided that the default web browser for all users on this computer should be the latest stable version of Google Chrome. Other business related software includes Notepad++, 7zip and LibreOffice. These should remain installed and kept up-to-date.

Due to recent issues installing updates, management requests that you do **NOT** install Windows Updates.

This computer has no required services at this time.

Critical Services:

- None

Authorized Administrators and Users

Authorized Administrators:
```
benjamin (you)
        password: W1llH4ck4B4con!
edarby
  password: Cr0wnC0uns3l!
jpearson
        password: Manag1ngP4rtner!
hspecter
        password: L1f3!5LikeTH1s
llitt
        password: ugotlittup
```

Authorized Users:
```
dscott
nnesbitt
pporter
kbennett
mross
rzane
dpaulsen
shuntley
jpomaville
sbandaru
sthomas
```

Competition Guidelines

- In order to provide a better competition experience, you are **NOT** required to change the password of the primary, auto-login, user account. Changing the password of a user that is set to automatically log in may lock you out of your computer.
- Authorized administrator passwords were correct the last time you did a password audit, but are not guaranteed to be currently accurate.
- Do not stop or disable the CCS Client service or process.
- Do not remove any authorized users or their home directories.
- The time zone of this image is set to UTC. Please do not change the time zone, date, or time on this image.
- You can view your current scoring report by double-clicking the "CyberPatriot Scoring Report" desktop icon.
- JavaScript is required for some error messages that appear on the "CyberPatriot Scoring Report." To ensure that you only receive correct error messages, please do not disable JavaScript.
- Some security settings may prevent the Stop Scoring application from running. If this happens, the safest way to stop scoring is to suspend the virtual machine. You should **NOT** power on the VM again before deleting.
- Malwarebytes, and possibly other antivirus products, may erroneously detect the CCS Client as malware. If this happens, please ensure that CCSClient.exe has been manually added to the allow list and restart the VM.