Am I Ready for The Practice Round?

For Windows Folks. Open notes. You can use any and all resources.

Beginning Steps

1. After downloading an image and placing it in a location in your file system where you can easily access what should you do next?

- ○ Extract It **with** the Extract Passcode Given
- ○ Extract it
- ○ Open the image from the zip file

2. After extracting the image you should open it in VMware Player.

- ○ True
- ○ False

3. Next, in VMware Player should you modify the image specs to parameters acceptable for your computer. (3/4 RAM, 3/4 cores, 1/2 HDD)

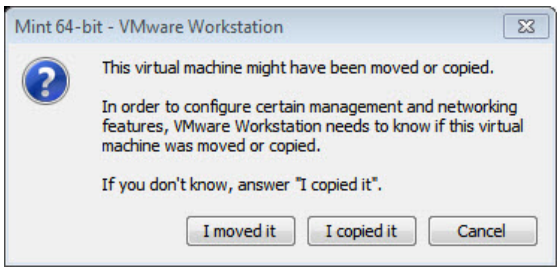
- ○ True
- ○ False

4. (In a competition scenario) Whenever you feel like it, you should hit the play VM button to boot up the machine.

- ○ True
- ○ False

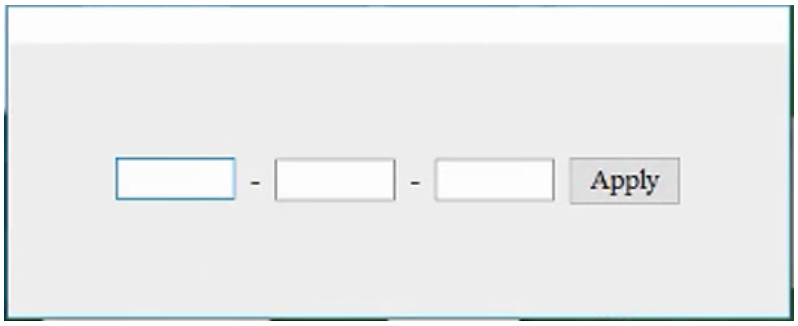
Booting Up

5. When booting up to a new VM when prompted about information pertaining to the VM you should say ....



- ○ I copied the VM
- ○ I moved the VM
- ○ Cancel

6. After agreeing to Cyberpatriots anti-online bullying or something like that statement, input the following parameter provided by leadership.



- Extract Passcode
- Unique Identifier
- Team Number

Reading the Readme (closely)

7. Statements such as "This company's security policies require that all user accounts be password protected" hints at ...

- There may be users without passwords
- Maybe a virus
- Maybe a user to remove

8. Statements such as "Employees are required to choose secure passwords" suggest and hints that ...

- All users have secure passwords
- Some user have secure passwords
- There is not a rule or policy enforced that makes and forces users choose a secure password

9. The phrase "the presence of any non-work related media files and "hacking tools" on any computers is strictly prohibited" suggest and hints

- Just to let you know.
- There is probably some bad software and applications or media files on the VM that are not allowed and need to be removed.
- You should be aware that this is a company rule to abide by when solving the image.

10. The sentence "This company currently does not use any centralized maintenance or polling tools to manage their IT equipment. " suggest and hints that ...

- Settings, policies, and files related to users are stored on the local machine.

- Settings, policies, and files related to users are not stored on the local machine and is instead stored on a server

11. The quote "This computer is for official business use only by authorized users." hints or suggest that ...

- Only authorized users exist
- Every user is unauthorized
- There may be some unauthorized former employee (user) accounts or unauthorized admin accounts present

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

- Action center is required to be on, but no action is needed
- Windows Action center may be turned off and all of it needs to be turned back on
- Some parts of Action Center need to be turned on, while other need to stay off

13. The statement "Management has decided that the default web browser for all users on this computer should be the latest stable version of Firefox" suggests

I. The latest stable version of Firefox may not be present and needs to be updated

II. The latest stable version of Firefox is installed already as per managements orders

III. Firefox may not be the default web browser and need to become the default web browser

- I, I, and III
- I and II
- I and III

14. If "Critical Services: (None)" should an FTP server be present and running?

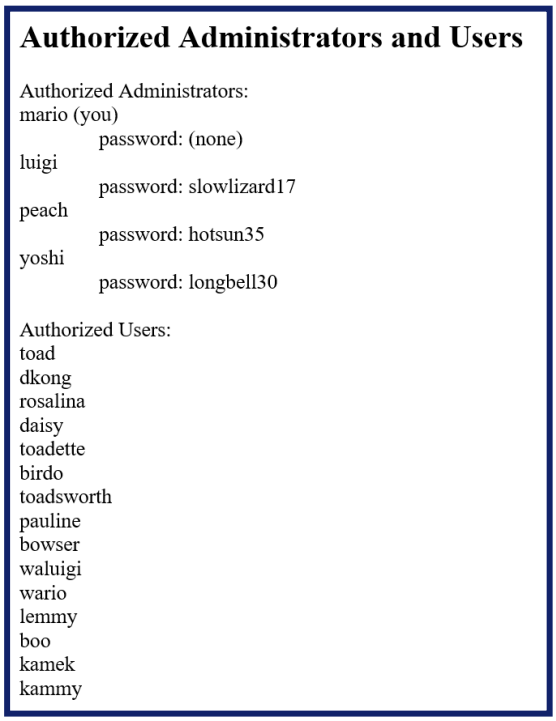
- Yes, because it would be a cool thing to have running
- No, I don't know why though
- Yes, because the readme says that it is a critical service
- No, because the readme does not specify any business critical services therefore it is considered not for business use and should be removed.

15. If "Critical Services: Remote Desktop or Virtual Network Computing" you should

- Remove it, because it is not critical and not specified in the readme
- Keep it, and do nothing with it
- Keep it and secure and lock down polices to make it more secure to run.

Authorized Users and Admins

16. Here are your given authorized users and admins from a readme



Authorized Administrators and Users

Authorized Administrators:
mario (you)
password: (none)
luigi
password: slowlizard17
peach
password: hotsun35
yoshi
password: longbell30

Authorized Users:
toad
dkong
rosalina
daisy
toadette
birdo
toadsworth
pauline
bowser
waluigi
wario
lemmy
boo
kamek
kammy

Here are the current users and admins present via Microsoft Management Console

- birdo
- boo
- bowser
- daisy
- dkong
- kamek

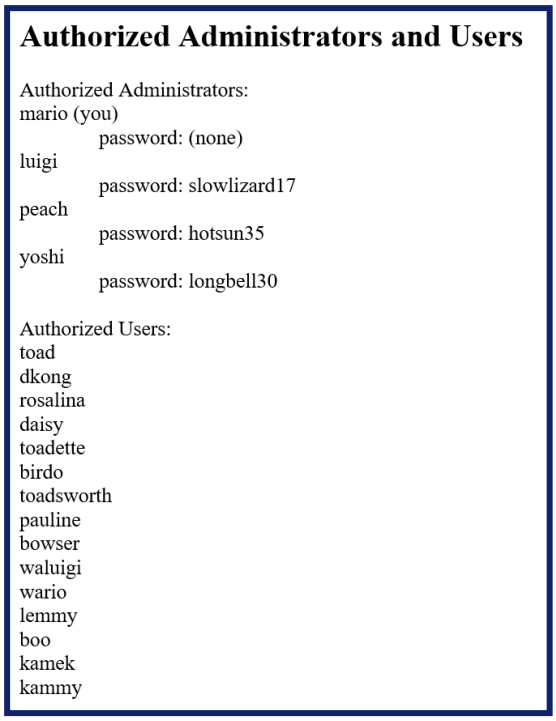
- kammy
- lemmy
- luigi
- mario
- pauline
- peach
- rosaline
- tataga
- toad
- toadette
- toadsworth
- waluigi
- wario
- wart
- yoshi

Are there any unauthorized accounts of former employees that need to be removed? (Who?) (Why?)

- ( ) No, since the users present from MMC match up with the authorized users and admins requested in the readme file

- Yes, since according to the authorized admins and users list in the reademe **bowser** and **birdo** should be removed
- Yes, since according to the authorized admins and users list in the reademe **wart** and **tatanga** should be removed

17. Here are your given authorized users and admins from a readme.



Authorized Administrators and Users

Authorized Administrators:
mario (you)
password: (none)
luigi
password: slowlizard17
peach
password: hotsun35
yoshi
password: longbell30

Authorized Users:
toad
dkong
rosalina
daisy
toadette
birdo
toadsworth
pauline
bowser
waluigi
wario
lemmy
boo
kamek
kammy

Here are the current users and admins present via Microsoft Management Console

Admins

- yoshi
- peach
- bowser
- mario
- luigi

Users

- birdo
- boo

- daisy
- dkong
- kamek
- kammy
- lemmy
- pauline
- rosaline
- tataga
- toad
- toadette
- toadsworth
- waluigi
- wario
- wart

Are there any unauthorized administrators present? Should they be removed? (Who?) (Why?)

○	Yes, there are unauthorized administrators present. They should be kept the way they are. It is very hard and difficult to do.
○	No, there are no unauthorized administrators present. They should be kept and not tampered with. It is against the rules to mess with admins.
○	Yes, there are unauthorized users. The user **bowser** should be demoted to a normal user. This should be done because according to the readme he is not an authorized administrator.
○	Yes, there are unauthorized users. The user **peach** should be demoted to a normal user. This should be done because according to the readme he is not an authorized administrator.

Passwords and Policies Regarding Passwords

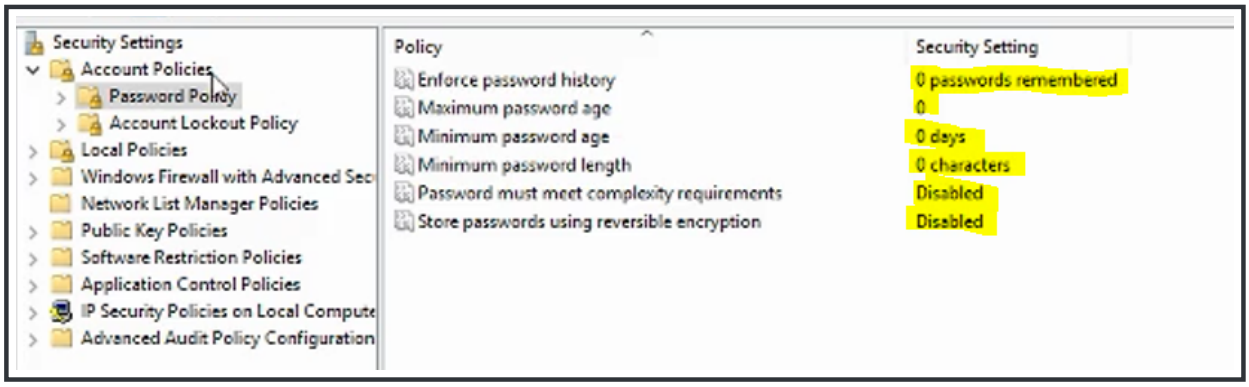
18. To ensure that all users have secure passwords you should...

○	Give every user a new password
○	Give some people a new password
○	Give nobody a new password

19.

Account Policies	Polices or rules that force and govern areas of security focused on user accounts.
Password Policy	An area in local security policy to require and force users to create and choose strong passwords
Account Lockout Policy	The area in local security policy to govern what happens and what is logged when successful and unsuccessful (wrong password) logins occur

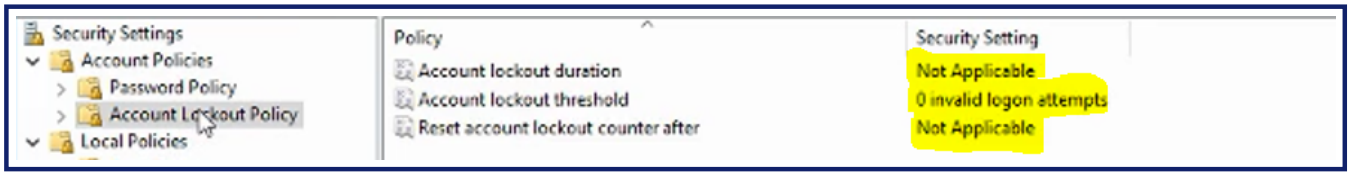
20. Here are the current password policies being implemented or applied:



What should the highlighted fields be changed to?

Password history	5 passwords remembered
Maximum password age	90 days for users and 30 for admins
Minimum password age	10-30 days
Minimum password length	8 characters
Complexity requirements	Enabled
Reverse encryption	Disabled

Here is the current lockout policy being enforced:



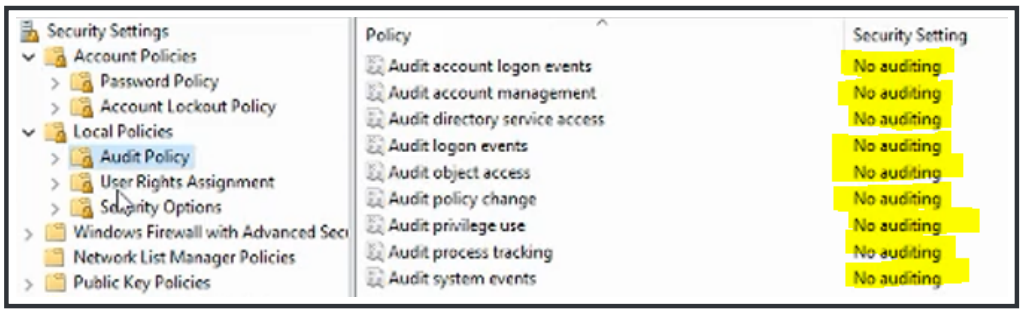
21.

What should the highlighted areas be changed to?

Account Lockout Duration	30 minutes
Account Lockout Threshold	3-10 invalid login attempts
Reset account lockout counter after	30 minutes

22.

Here are the current audit policies being implemented or applied:



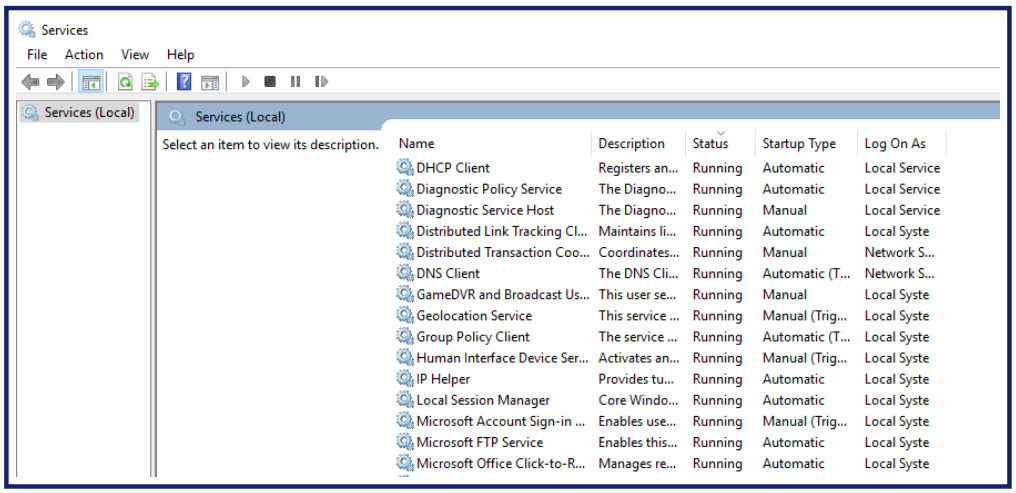
What should the highlighted fields be changed to audit?

- Successful Logins
- Failure Logins
- Successful and Failure Logins

Services

23.

You are checking through the services currently running on a computer. See below

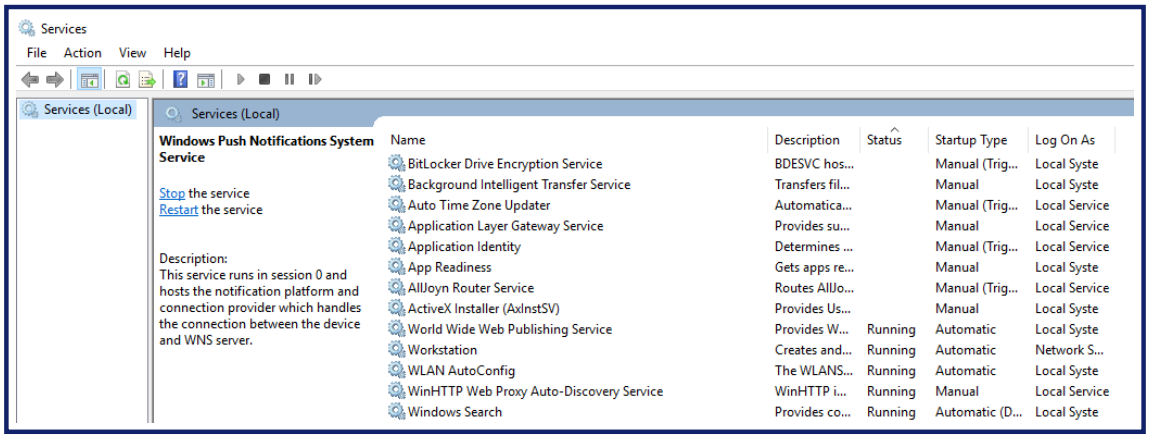


Is there anything alarming that is running? If so what is it and what should you do?

- No, there is nothing alarming and no action should be taken
- Yes, there is something alarming. I am just not sure what to do
- Yes, there is something alarming. It is the FTP service that is running in the background. The FTP service should be stopped and disabled from running in the future
- Yes, there is something alarming. It is the Diagnostic Service Host service running in the background. This service should be stopped and disabled from running in the future

24.

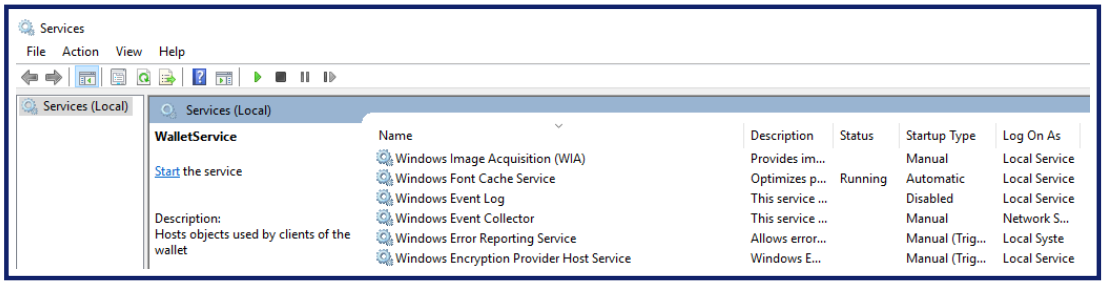
You are checking through the services currently running on a computer. See below



Is there anything alarming that is running? If so what is it and what should you do?

- No, there is nothing alarming and no action should be taken
- Yes, there is something alarming. I am just not sure what to do
- Yes, there is something alarming. It is the Local Session Manager service running in the background. This service should be stopped and disabled from running in the future
- Yes, there is something alarming. It is the "World Wide Web Publishing Service" service that is running in the background. The "WWW Publishing Service" service should be stopped and disabled from running in the future

You are checking through the services currently running on a computer. See below



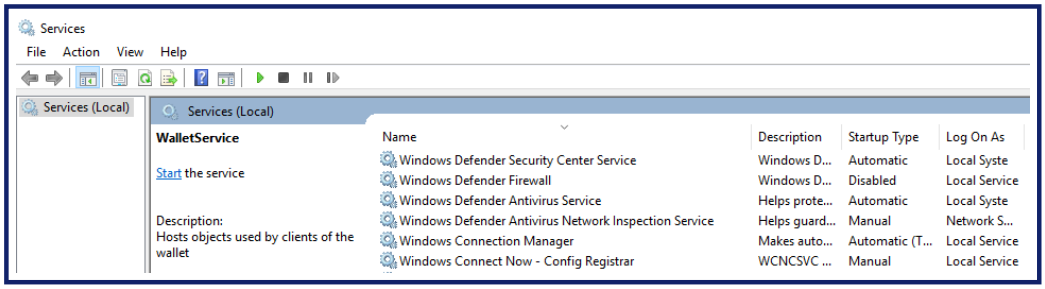
25.

Is there anything alarming that is running? If so what is it and what should you do?

- Yes, there is something alarming. I am just not sure what to do
- Yes, there is something alarming. It is the Windows Font Cache service running in the background. This service should be stopped and disabled from running in the future
- Yes, there is something alarming. It is the "Windows Event Log" service that records every action in a log book of sorts. The "Windows Event Log" service should be started so that in the future it can successfully log interactions on this particular machine
- No, there is nothing alarming and no action should be taken

26.

You are checking through the services currently running on a computer. See below



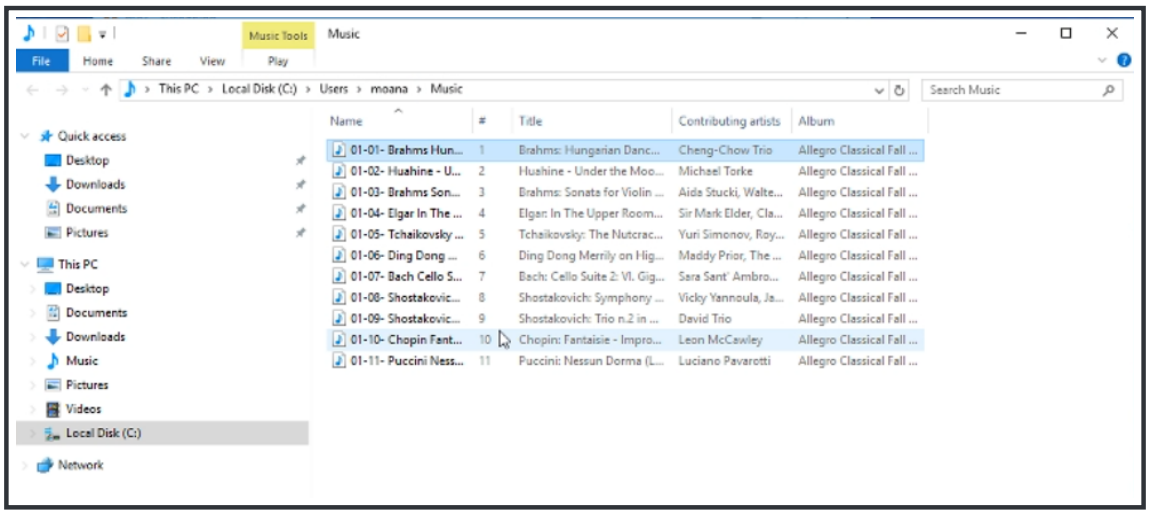
Is there anything alarming that is running? If so what is it and what should you do?

- Yes, there is something alarming. I am just not sure what to do
- Yes, there is something alarming. It is the "Windows Defender Firewall" service that can potential stop malicious connections and actions from occurring on a machine. The "Windows Event Log" service should be started so that in the future it can successfully log interactions on this particular machine
- Yes, there is something alarming. It is the Windows Connection Manager running in the background. This service should be stopped and disabled from running in the future
- No, there is nothing alarming and no action should be taken

Files and Applications

27.

You stumble upon some media files. The readme specifically says "media files are prohibited" See below.

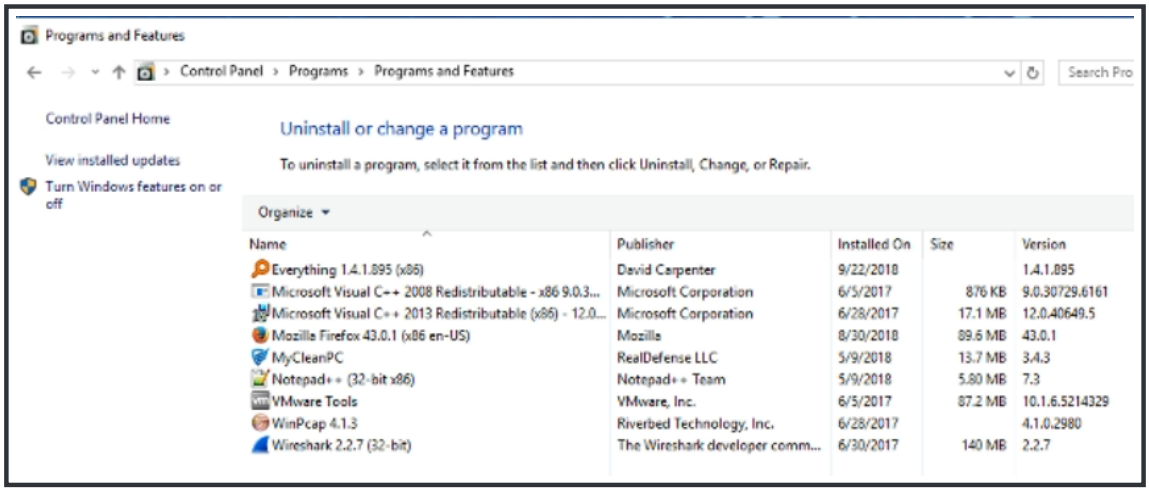


What should you do?

- Do not remove them because the readme said so
- Remove each mp3 file since the readme specifies no media files are allowed

- Listen to each file to see if it is bad. If it uses explicit language delete it.

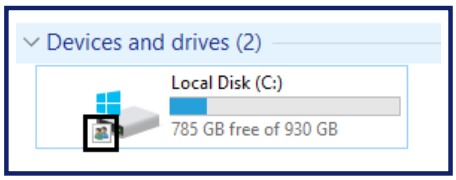
28. When solving an image you see the following applications are installed. The readme specifically says "hacking tools" are prohibited" See below.



What should you do?

- Remove the prohibited applications. In this case Wireshark and MyCleanPC
- Keep the prohibited applications because you are unsure what to do
- Remove the prohibited items. In this case Notepad++ and Firefox

29. You open file explorer and notice that the following icon (outlined in photo) is adjacent to the C drive. See below.



What does this mean? What should you do?

- Nothing. No action should be taken
- Something I am not sure what. Maybe something vulnerable
- File sharing is being conducted currently for the C drive. You should disable file sharing for the C drive because it leaves you machine vulnerable and is not specified in the readme.

Updates

30. When should windows updates be started (begin the download process)? (Keep in mind updates often take lots of time and space)

- At the middle of the time window when you are bored
- At the beginning of the time window when you have ample time and resources to devote toward completing updates
- At the end as a fail safe to earn guaranteed points.

31. You are told in the readme that firefox should be the "latest stable version". Based on the information below what should your next step be?

- Nothing
- Update Firefox once
- Update Firefox until you reach the latest stable version