# CP-XV Exhibition Round Ubuntu 16 Answer Key

Welcome to the CyberPatriot Exhibition Round! This image will provide you with information on how to solve common vulnerabilities on an Ubuntu operating system. In doing so, it will help you on your way as you build your cybersecurity skills.

The vulnerabilities in this image are some of the most basic ones found during a CyberPatriot competition. Even if you do very well with these vulnerabilities, you will experience greater difficulty as the season progresses. To score well in each round, it is important to not only use this image and the training materials on the CyberPatriot website and the Coach, Mentor, and Team Assistant Dashboard; but to also use additional outside information on cybersecurity practices, including the expertise of your Technical Mentor(s). Also, the README file on the desktop in this image may be more detailed than those you see during the competition. You will have to use your own knowledge, not just the hints in this file, to achieve a high score during the actual competition.

Below are the answers to the problems that are being scored in this image. Each one includes information on how the problem was found (if applicable), how it was solved, and why it is important from a cybersecurity standpoint. More information on these specific vulnerabilities can be found in Unit Nine and Unit Ten of the CyberPatriot Training Materials on the Dashboard when your Coach, Mentor, or Team Assistant signs into www.uscyberpatriot.org (not the archived Training Materials on the public side of the CyberPatriot site). However, researching these vulnerabilities (and more advanced ones) on your own is also highly encouraged!

It is also possible to lose points during the competition. Simple penalties that may arise are noted below the answers. There are many ways to solve some of the problems below. This answer key just shows one method in each case.

Coaches will be sent categories of vulnerabilities following each online round.

## Answers

**1) Forensics Question 1 correct: 10 pts.**

- How do I find this problem?

  You should always look on the desktop of the image to see if there are questions for you to answer. There is a file on the desktop called "Forensics Question 1."

- How do I solve this problem?

  You will be logged into the image as Administrator “ballen.” To find the path of the directory containing all of the prohibited .mp3 music files on the image, first click the **Files** icon on the **Launcher** (left side of the screen). Then, click the Search icon (magnifying glass icon), and type in “.mp3” without quotes into the Search box. Right-click on one of the files, select **Properties**, and under **Location** you will see the path of the directory. The path of the directory containing the prohibited mp3 files is “/home/ballen/Downloads/Allegro Classical”. Highlight the path and copy and paste as your answer. Remember to **Save** the file.

- Why is fixing this problem important?

  Keeping personal music on the computer is a violation of the company's policies.

**2) Forensics Question 2 correct: 10 pts.**

- How do I find this problem?

  You should always look on the desktop of the image to see if there are questions for you to answer about existing vulnerabilities. There is a file on the desktop called "Forensics Question 2."

- How do I solve this problem?

  Bring up a **Terminal** (Ctrl+Alt+T). Type "id mrory" without quotes and press **Enter**. From the output of the command you can see that the UID of mrory is 1018. Alternatively, the command "getent passwd mrory" will give you the UID as well. Remember to **Save** the file.

- Why is fixing this problem important?

  Knowing user account details can help you more easily detect unauthorized users and system misconfigurations that that lead to security vulnerabilities.

**3) Forensics Question 3 correct: 10 pts.**

- How do I find this problem?

  You should always look on the desktop of the image to see if there are questions for you to answer about existing vulnerabilities. There is a file on the desktop called "Forensics Question 3."

- How do I solve this problem?

  Bring up a **Terminal** (Ctrl+Alt+T). Type "getent group flash" without the quotes and press **Enter**. From the output of the command you can see the users of the group. Remember to **Save** the file.

- Why is fixing this problem important?

  Knowing groups and their members is helpful in detecting unauthorized behaviors and permissions. This is especially important in access control management of critical system environments.

**4) Removed unauthorized users: 5 pts. each**

- How do I find this problem?

  One of the first things you should do when starting an image during a competition is check the README file on the desktop. The README shows the authorized Administrators and Users for the image. These are the only users that should have accounts. All others should be removed.

- How do I solve this problem?

  Click the **Settings** icon on the top right-hand corner.

  From this menu, select **System Settings…**, then **User Accounts**. Click on "Unlock" and enter the password for ballen from the README. Click on **Authenticate**. As an Administrator, you will have root access. Click on the account to be removed and then select the minus sign in the bottom left of the window to delete the account. When prompted to keep the user's files, select

**Delete Files**. Make sure to write down the name of the user you deleted. Remember, removing some unauthorized users may not be scored checks. This is part of the competition.

- Why is fixing this problem important?

  Computer access should be limited to just those who need to use it to complete their tasks. By leaving these user accounts on the image, unauthorized individuals may be able to log on to the computer and make changes that could affect the safety and security of legitimate users.

**5) User hwells is not an administrator: 10 pts.**

- How do I find this problem?

  In the README file on the desktop, you will see Authorized Administrators and Users for the image and the account type for each user.

- How do I solve this problem?

  Click the **Settings** icon on the top right-hand corner. From this menu, select **System Settings…**, then **User Accounts**. Click on "Unlock" and enter the password for ballen, then **Authenticate**. Click on the user "hwells" and change the **Account Type** from Administrator to **Standard**.

- Why is fixing this problem important?

  Ensuring account types are set correctly is very important. A Standard user given Administrator permissions can accidentally or purposefully cause significant damage to a system because they would have access to all files on the system, not just their own.

**6) Changed insecure password for user jwells: 5 pts.**

- How do I find this problem?

  The README file lists the Authorized Administrators and Users with their passwords for this image. For the purposes of this round's image, do NOT change the password for "ballen." Check if any other Administrator passwords are insecure.

- How do I solve this problem?

  Click the **Settings** icon on the top right-hand corner. From this menu, select **System Settings…**, then **User Accounts**. Click on "Unlock" and enter the password for ballen, which will give you root access. Click on the user "jwells." You can change the password for a user by clicking the field to the right of "Password." For information on strong passwords, see Unit Four on the Dashboard. **IMPORTANT**: Make sure you write down the new passwords, especially any Administrator passwords, so you do not potentially lock yourself out of the image. Close the **User Accounts** window when finished.

- Why is fixing this problem important?

  Having a weak password on a user account makes it extremely vulnerable to attacks by outside individuals. With a weak password, an attacker can more easily gain access to a user's files. Strong passwords make it much more likely that only the authorized user of the account can access it.

**7) Uncomplicated Firewall (UFW) protection has been enabled: 10 pts.**

- How do I find this problem?

  Bring up the run dialog by typing Alt+F2. Type "gufw" (Graphical Uncomplicated Firewall), and press **Enter**. Type the password for ballen, then **Authenticate** to launch gufw. In the **Firewall** window you can see that the **Status** is set to **OFF.**

- How do I solve this problem?

  Inside the **Firewall** window, click the slider next to **OFF**. You should see the status turn **ON** and the shield turn green and red.

- Why is fixing this problem important?

  Enabling and properly configuring a firewall is critical to ensuring that you are only allowing known, authorized traffic in and out of your computer.

**8) Samba service has been disabled or removed: 10 pts.**

- How do I find this problem?

  Bring up a **Terminal** (Ctrl+Alt+T). Type "service --status-all" and press **Enter**.

- How do I solve this problem?

  If you do not already have a Terminal open, bring up a **Terminal** (Ctrl+Alt+T). Type "sudo apt-get remove samba" and press **Enter**. Type the password for ballen, and press **Enter**. Type "Y" for Yes, then **Enter** to continue to remove samba.

- Why is fixing this problem important?

  Disabling unnecessary services can limit your attack surface. The less services an adversary has to attack and potentially exploit, the lower your risk. Adversaries may attack known or unknown vulnerabilities in services to obtain information, escalate privileges, or gain unauthorized access.

**9) The system automatically checks for updates daily: 5 pts.**

- How do I find this problem?

  Keeping your operating system and software updated is a good cybersecurity practice in general.

- How do I solve this problem?

  Click the **Settings** icon on the top right-hand corner. From this menu, select **System Settings…**, then **Software & Updates**. Next, select the **Updates** tab. Change the "Automatically check for updates" from "Never" to "Daily." You will be prompted for the password for ballen, then select **Authenticate** to make the change.

- Why is fixing this problem important?

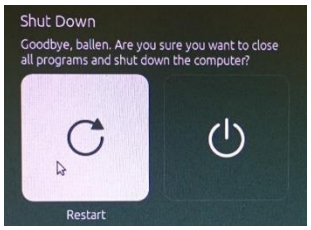
  Setting Ubuntu to check for updates on a daily basis ensures you will not miss any critical patches.

**10) Install updates from important security updates: 5 pts.**

- How do I find this problem?

  Keeping your operating system and software up to date is a good cybersecurity practice in general.

- How do I solve this problem?




  Under "Install updates from," check the boxes for **Important security updates** and **Recommended updates.** Click **Close** and the **Reload**. Click the **Search your computer** in the upper left corner on the Launcher (under the word Terminal). Type "update," and then select **Software Updater**. Click **Install Now**. You will be asked for your password again before the updates are installed. Restart the image by selecting **Settings**, **Shutdown**, then the **Restart** button to complete the updates.

  Note: Occasionally **Software Updater** will inform you that it failed to download package files. If you see this message, your best course of action is to try again. Installing updates is important to security; however, on this specific image you receive no points for installing updates, therefore you may safely skip using the **Software Updater** on this image if desired.

- Why is fixing this problem important?

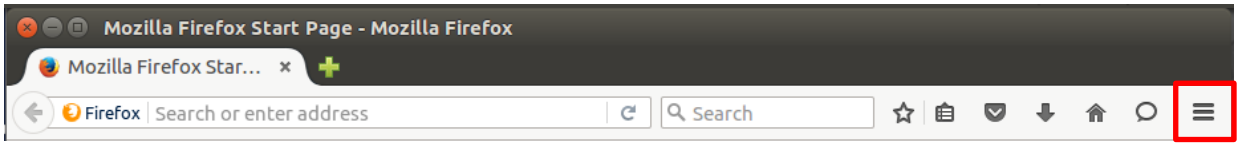
  Adversaries can more easily compromise your system if software is present that has known security vulnerabilities. Ensuring software is up to date removes known security vulnerabilities.

**11) Firefox pop-up blocker enabled: 5 pts.**

- How do I find this problem?

  The README file notes that Firefox should be the default web browser on the computer. Settings on a browser should always be updated and configured with secure settings.

- How do I solve this problem?




  Open FireFox → Click on the three lines on the top right of the browser → Select the menu button on the top right to enter **Preferences** → Select the **Content** tab on the left-hand side of the window → Check the box next to **Block pop-up windows**.

- Why is fixing this problem important?

  As the default web browser used, the security settings should be configured to mitigate browser-based vulnerabilities. The pop-up blocker should be enabled to block windows automatically opened by the original accessed site. These pop-ups are typically used for advertisements, which may present an opportunity for social engineering and unauthorized downloads.

**12) Prohibited MP3 files are removed: 5 pts.**

- How do I find this problem?

  The README file notes that all media files are prohibited on this image. From the Forensics Question #1, you know that the .mp3 files are in "/home/ballen/Downloads/Allegro Classical."

- How do I solve this problem?

  Click the **Files** icon on the left side of the Launcher, then double click on the **Downloads** folder. Right click the **Allegro Classical** folder and select **Move to Trash**.

- Why is fixing this problem important?

  Keeping personal music on the computer is a violation of the company's policies as stated in the Readme file.

**13) Prohibited software Nmap and Zenmap removed: 5 pts.**

- How do I find this problem?

  The README file notes that only software for basic office tasks should be on this image. There is a Zenmap icon on the Launcher.

- How do I solve this problem?

  Bring up a Terminal (Ctrl+Alt+T). Type "sudo apt-get remove zenmap nmap" and press **Enter**. Type the password for ballen, and press **Enter**. Type "Y" for Yes, then **Enter** to continue to remove Zenmap and nmap.

- Why is fixing this problem important?

  This software is a violation of the company's security policies. Installing applications such as network mappers and vulnerability scanners will allow authorized users and potential attackers easier access to information about your network.

---

## Penalties

**1) Authorized users have been deleted: -5 pts.**

- Why is this a penalty?

  The README file lists authorized users for this machine. By removing authorized user accounts, they will be unable to access this computer and do their jobs.

**2) Authorized user directories have been deleted: -5 pts.**

- Why is this a penalty?

  By removing authorized user directories from the image, you are removing important files and folders that these individuals need to complete their duties.

**3) Firefox has been removed: -5 pts.**

- Why is this a penalty?

  The README file notes that all authorized users must be able to use Firefox, therefore Firefox needs to remain installed on the computer.

**4) OpenSSH service has been stopped or removed: -5 pts.**

- Why is this a penalty?

  The README file notes that all authorized users must be able to log in remotely using SSH. Therefore, sshd is a critical service that needs to be enabled.