CP-X Ubuntu 14 Training Image Answer Key

Welcome to the CyberPatriot Training 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 Ten of the CyberPatriot X 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.

Finally, this answer key is a one-time only event. Answers for the CP-X Practice Round and scored rounds of competition will not be released at any time. However, Coaches will be sent categories of vulnerabilities following each online round.

Answers

1) Forensics Question 1 Correct: 20 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 1."

- How do I solve this problem?

  You will be logged into the image as Administrator "po." To find the path of the directory containing all of the prohibited .mp3 music files on the image, select Places, Home Folder, Search icon (magnifying glass icon), and type in .mp3 into the Search box. Right-click on one of the files, select Properties, and under Location you will see the path of the directory. Look at the Location for the other .mp3 files. The path of the directory is /home/po/Music/The Bands and Ensembles of the US Armed Forces/Veterans Day Honor. Remember to **Save** the file.

- Why is fixing this problem important?

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

2) Unauthorized User accounts have been removed: 10 pts.

- 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. There, you will see 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?

  Under Applications, select System Tools, System Settings and select User Accounts. Click on "Unlock" and enter your password, which will give you 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 by selecting Delete Files. Make sure to write down the name of the user you deleted.

- 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.

3) Administrator account has been changed to Standard: 10 pts.

- How do I find this problem?

  In the README file on the desktop, you will see the authorized users for the image and the account type for each user.

- How do I solve this problem?

  To make any account management changes, you must enable root permissions. Under Applications, select System Tools, System Settings and select User Accounts. Click on "Unlock" and enter your password, which will give you root access. Click on the "meimei" account and then change the user type from Administrator to Standard.

- Why is fixing this problem important?

  Ensuring account types are set correctly is very important. A Standard user given Administrative 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.

4) User accounts have secure passwords: 10 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 Training Round image, do NOT change the passwords for "po" or "oogway," but check if any other Administrators passwords are insecure. If you change any passwords, make sure you write them down.

- How do I solve this problem?

  Under Applications, System Tools, and System Settings, select User Accounts. Click on "Unlock" and enter your password. Click on one of the user accounts that is not “po” or “oogway.” You can change the password for another user by clicking the field to the right of “Password.” For information on strong passwords, see Unit Four on the Dashboard. Make sure you write down the new passwords, especially any Administrator passwords, so you do not potentially lock yourself out of the image.

- 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.

5) Check for updates daily: 10 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. The Update Manager may warn you that updates are not being installed automatically. Next, select Updates. Change the “Automatically check for updates” from “Never” to “Daily.” You will be prompted for a password, which can be found in the README file on the desktop.

- Why is fixing this problem important?

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

6) Install important updates: 10 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?

  After setting Ubuntu to check for updates daily, check the “Important security updates” and “Recommended updates” boxes from the “Install updates from” menu. Click Close and then Reload. Select Applications, System Tools, Administration, then Software Updater. Click “Install Updates.” You will be asked for your password again before the updates are installed. Restart the image after making changes to core utilities in Ubuntu.

- Why is fixing this problem important?

  Installing important Ubuntu updates, including updating Bash, will ensure your system remains secure.

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

- How do I find this problem?

  In the README file, company policy is to use only the latest, official and stable packages available.

- How do I solve this problem?

  Under Applications, go to the Ubuntu Software Center. Look at all the software on the image. In the Search box, type Samba. Any software icon that has a green circle with a check has been installed. Click on SMB/CIFS and select Remove. Enter the Administrator's password to complete the removal of the software.

- Why is fixing this problem important?

  Samba is free software used to enable file and print services on Linux systems and can be vulnerable to man-in-the-middle attacks. It is important to disable or remove unnecessary or vulnerable services.

8) Prohibited .mp3 files have been removed: 10 pts.

- How do I find this problem?

  The README file notes that all media files are prohibited on this image.

- How do I solve this problem?

  From the Forensics Question #1, you know that the .mp3 files are in the Veterans Day Honor folder for the user "po." Under Places, Home Folder, Music, The Bands and Ensembles of the US Armed Forces, highlight and right-click the Veterans Day Honor folder. Select "Move To Trash."

- Why is fixing this problem important?

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

9) Nmap program has been removed: 10 pts.

- How do I find this problem?

  The README file notes that only software for basic office tasks should be on this image. Nmap is a "Network Mapper" that does not meet these requirements and should be removed.

- How do I solve this problem?

  Click on Places, Home, then Downloads. You will find the unauthorized software called nmap-7.12.tar.bz2. Highlight the software, right-click, and select Move To Trash.

- Why is fixing this problem important?

  This software is a violation of the company's security policies. Unknown programs on a computer could contain malware or allow outside individuals access to the computer. It is important to keep only well-known software that is used for a necessary purpose on your computer.

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) A critical 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.