CP-VIII Ubuntu Introductory Image Answer Key

Welcome to the CyberPatriot Introductory Image! 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 do 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 also other 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 exist 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 of the CyberPatriot VIII 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 our 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. Feel free to explore the topics more and find the method that you like best.

Finally, this answer key is a one-time only event. Answers for the CP-VIII 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: 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 valid users for the image. These are the only users that should have an account. All others should be removed. You should also always look on the image desktop to see if there are questions for you to answer about the vulnerabilities that exist in the image. There is a file on the desktop here called "Scored Questions." You can see that the question on this image asks you about users you have deleted from the image.

- How do I solve this problem?

  Open the System Settings and access User Accounts. Click on "Unlock" and then enter your password (found in the README file on the desktop), which will give you root access. From here, click on the users that are not listed on the valid user list in the README file and select the minus button to delete their accounts. Make sure to write down the names of the users you deleted. You will need this information in a moment. After deleting the invalid users, go to the "Scored Questions" file on the desktop. Follow the directions in the file to enter the names of the users you deleted. (If you deleted the users before writing their names down, the answers are "gytha" and "magrat" without the quotation marks.)

- 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, invalid individuals may be able to log on to the computer and make changes that could affect the safety and security of the users. Also, it is important to document the steps you take when you are fixing vulnerabilities. That way, if you make a mistake, you can undo actions. By documenting problems you can prevent them from happening in the future and fix them more quickly if they arise again.

---

2) User accounts have secure passwords: 10 pts.

- How do I find this problem?

  According to the README file, all users on this image other than the "student" account have passwords of "password" without quotation marks. This is a very insecure password. Giving users stronger passwords is a good cybersecurity practice.

- How do I solve this problem?

  Open the System Settings and access User Accounts. Click on "Unlock" and then enter your password, which will give you root access. Click on one of the user accounts that is not "student." From here, click the field to the right of "Password." You can then change the password for another user. While all you need to do for this vulnerability is change the passwords for the all other users to something other than "password," it is good practice to make the new passwords strong one. For information on strong passwords, see Unit Four on the Dashboard. Do not change the password for the "CyberPatriot" account. This is your account and for the purposes of the competition, you do not need to change the password.

- 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 guess the code to access a user's files. Strong passwords make it much more likely that only the actual holder of the account can access it.

3 and 4) Administrator account has been changed to User: 10 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. There, you will see the valid users for the image and the account type each should have.

- How do I solve this problem?

  Open the System Settings and access User Accounts. Click on "Unlock" and then enter your password, which will give you root access. Click on the lobsang account and then change his user type from Administrator to Standard. Do the same for the user teppic.

- Why is fixing this problem important?

  Ensuring account types are set correctly is very important. A standard user accidentally 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.

---

5 and 6) Former employee accounts have been removed: 10 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. There, you will see the valid users for the image. These are the only users that should have an account. All others should be removed.

- How do I solve this problem?

  Open the System Settings and access User Accounts. Click on "Unlock" and then enter your password, which will give you root access. Click on the account to be removed and then click the minus sign in the bottom left of the window to delete the account. Make sure to write down the names of the users 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, invalid individuals may be able to log on to the computer and make changes that could affect the safety and security of legitimate users.

---

7) Check for updates daily: 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?

  Click the icon on the top right hand corner. From this menu, select the fourth option down, which will read “Software up to date.” The update manager may warn you that updates are not being installed automatically. Next, click on “settings.” You will be prompted for a password, which can be found in the README file on the desktop. After entering the password and gaining

permission to change the software update settings, change the “Automatically check for updates” field from “Never” to “Daily.”

- Why is fixing this problem important?

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

---

8) 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 at the prompt that say software information is not up to date. The list of updates will then populate in the Update Manager window. Click “Install Updates.”

- Why is fixing this problem important?

  Installing important Ubuntu updates will ensure your system remains secure.

---

9) A firewall has been installed: 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?

  Click on the Ubuntu Software Center icon on the left menu bar. In the top left search box, type “firewall” then hit enter. Select the “Firewall Configuration” result and click Install. Enter your password at the authentication popup. Once installation has finished, click the new Firewall Configuration icon on the left menu bar. Click the unlock button and enter your password. Toggle the Status button to the On position to activate the firewall.

- Why is fixing this problem important?

  Installing important Ubuntu updates will ensure your system remains secure.

---

10) Risky file has been removed: 10 pts.

- How do I find this problem?

  Any file with an alarming name, such as Password or Credit Card Info, should be investigated and removed.

- How do I solve this problem?

  Open up the Home folder, then delete the text file called “Passwords.”

- Why is fixing this problem important?

  Files containing information that can compromise system security should be removed.

Penalties

---

1) Important cron files/directories removed: -10 pts.

- Why is this a penalty?

  Cron is a service that can schedule specific commands in the background of the Ubuntu operating system. One of the most common uses of cron is downloading email from the Internet. The README file indicates that this machine is used for office tasks such as checking email. It is therefore a good idea to keep all cron files and directories.

---

2) Valid users have been deleted: -10 pts.

- Why is this a penalty?

  The README file notes the list of valid users for this machine. By removing valid user accounts, you are making it impossible for them to access this computer and do their jobs.

---

3) Valid user directories have been deleted: -10 pts.

- Why is this a penalty?

  The README file notes the list of valid users for this machine. By removing valid user directories from the image, you are removing important files and folders that these individuals need to complete their duties.