CyberPatriot Ubuntu 22
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. 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.

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: 8 pts.

- How do I find this problem?

  When you open an image, please read all the "Forensics Questions" thoroughly before modifying the image as you may change something that prevents you from answering the question correctly. There is a file on the Desktop here named "Forensics Question 1".

- How do I solve this problem?

  The question asks you to decode the message left for you on your Desktop.

  The message is encoded into base64.

  To decode the message, use an online base64 decoder, like https://www.base64decode.org/

  Agent P,

  Doofenshmirtz claims to have given up evil. He even signed this "I Give Up Evil" affidavit to apply for work at the agency.
  We're making Doofenshmirtz your responsibility during his probation period.
  Show him the ropes, and don't let him out of your sight.

  Monogram out!

The answer to this question is “affidavit”

- Why is fixing this problem important?

  Having a grasp of simple encoding techniques, such as using base64, is a key skill. It allows us to uncover hidden messages that have been transformed using these techniques.

2) Forensics Question 2 Correct: 8 pts.

- How do I find this problem?

  When you open an image, please read all the "Forensics Questions" thoroughly before modifying the image as you may change something that prevents you from answering the question correctly. There is a file on the Desktop here named "Forensics Question 2”.

- How do I solve this problem?

  This question asks you to find the absolute path of the directory containing prohibited MP3 files.

  In a terminal type **locate '*.mp3'**. In the output of locate you can see the file system location of files with the extension .mp3. The mp3 files under linda’s Music directory appear to be non-work related.

  The answer to this question is the absolute path to the mp3 files starting with the root directory **/**.

- Why is fixing this problem important?

  Knowing how to efficiently find files of different types on a Linux operating system will help you quickly identify many different types of security issues such as prohibited files and software, sensitive information, backdoors, services, and important configuration files.

3) Removed unauthorized user balloony: 6 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. The authorized administrators and users listed in the README are the only users that should exist on the system (aside from legitimate built-in system accounts and those used for services). All unauthorized user accounts should be removed.

- How do I solve this problem?

  Click the **Show Applications** button on the bottom of the Launcher and click **Settings.** Scroll down and click on **Users**, then click **Unlock** in the upper right corner of the Settings window. If prompted type the password of your current user account. The password for your current user account can be found in the README. Select the user **balloony**. Click on **Remove User…** Since this is a competition environment and a further analysis of this user’s files is not necessary, click **Delete Files**.

- 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 unauthorized 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. Unauthorized user accounts also give adversaries a greater attack surface. For example, unauthorized user accounts increase the risk of having a user account compromised via password cracking.

4) User doofenshmirtz is not an administrator: 6 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. The authorized administrators listed in the README are the only users that are authorized have administrator level access. All users not in the list of authorized administrators should have their administrator level access removed.

- How do I solve this problem?

  Click the **Show Applications** button on the bottom of the Launcher and click **Settings.** Scroll down and click on **Users**, then click **Unlock** in the upper right corner of the Settings window. If prompted type the password of your current user account. The password for your current user account can be found in the README. Select the user **doofenshmirtz**. Click on the toggle button next to **Administrator**.

- Why is fixing this problem important?

  Administrator level access gives individuals the ability to modify critical system files and functions and should be limited to authorized individuals only. The more users with administrator level access, the higher your risk, since compromising an account with administrator level access gives an adversary complete control of the system.

5) User lawrence is not an administrator: 6 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. The authorized administrators listed in the README are the only users that are authorized have administrator level access. All users not in the list of authorized administrators should have their administrator level access removed.

- How do I solve this problem?

  Click the **Show Applications** button on the bottom of the Launcher and click **Settings.** Scroll down and click on **Users**, then click **Unlock** in the upper right corner of the Settings window. If prompted type the password of your current user account. The password for your current user account can be found in the README. Select the user **lawrence**. Click on the toggle button next to **Administrator**.

- Why is fixing this problem important?

  Administrator level access gives individuals the ability to modify critical system files and functions and should be limited to authorized individuals only. The more users with administrator level access, the higher your risk, since compromising an account with administrator level access gives an adversary complete control of the system.

6) Changed insecure password for user pinky: 6 pts.

- How do I find this problem?

  Ensuring users have strong passwords is an important principle of cybersecurity. In this instance the README tells you the passwords of the authorized administrators. In practice, security professionals use password auditing tools to help identify users with weak passwords.

- How do I solve this problem?

  Click the **Show Applications** button on the bottom of the Launcher and click **Settings.** Scroll down and click on **Users**, then click **Unlock** in the upper right corner of the Settings window. If prompted type the password of your current user account. The password for your current user account can be found in the README. Select the user **pinky**. Click the line labeled **Password**. Select **Set a password now**. Choose a secure password and type it into the **New Password** and **Confirm New Password** text boxes, and click **Change**.

- Why is fixing this problem important?

  Weak passwords can be easily and quickly compromised by adversaries via various password cracking techniques. A compromised user account, even if it is not an administrator, can easily and quickly lead to a compromised system and network.

7) Added candace to group firesidegirls: 8 pts.

- How do I find this problem?

  The README requests that you add a user to a group.

- How do I solve this problem?

  In a terminal, type **sudo gpasswd -a candace firesidegirls**. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- Why is fixing this problem important?

  One important aspect of working as a security or IT professional is supporting business operations and knowing how to do administrative tasks when requested. Additionally, knowing how system administration tasks are performed and the consequences of those actions is important as a security professional, because you must know in detail how an operating system works before you can defend it.

8) Uncomplicated Firewall (UFW) protection has been enabled: 6 pts.

- How do I find this problem?

  Enabling a host-based firewall is very important to system security. The README tells you that the only company approved firewall is UFW. You can check the status of UFW by typing **sudo ufw status**. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- How do I solve this problem?

  In a terminal, type **sudo ufw enable**. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- 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.

9) Nginx service has been disabled or removed: 6 pts.

- How do I find this problem?

  Stopping and disabling insecure or unnecessary services is an important principle of good cybersecurity. Many services need to be running to ensure normal and secure operation of computer systems. Reading about the services on your system and doing research can help you determine the importance of a service and if it is necessary for normal operation. Additionally, business-critical services listed in the README should remain running at all times. Running services can be found by running the command **systemctl list-units --type=service --state=active** in a terminal.

- How do I solve this problem?

  In a terminal, type **sudo systemctl stop nginx** to stop the service. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README. After stopping the service, type **sudo systemctl disable nginx** to prevent it from starting automatically in the future.

- Why is fixing this problem important?

  Disabling unnecessary services can limit your attack surface. The fewer 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.

10) The system automatically checks for updates daily: 6 pts.

- How do I find this problem?

  Automatically checking for security updates is an important cybersecurity principle. In Ubuntu, this can be checked and configured in the **Software & Updates** application.

- How do I solve this problem?

  Click the **Show Applications** button on the bottom of the Launcher and click **Software & Updates** (you may select Settings on the pop-up box). In the **Updates** tab, select the dropdown box next to Automatically check for updates, and choose **Daily**. If prompted type the password of your current user account. The password for your current user account can be found in the README. Click **Close** (or Cancel if prompted to apply updates).

- Why is fixing this problem important?

  When security vulnerabilities are found in software, the software vendor publishes updates that patch the security vulnerabilities. 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.
  This setting does not apply any updates to the software on the system, or configure what updates to check for, but it does automatically check for updates so that you may be notified when updates are available.

11) Firefox has been updated: 5 pts.

- How do I find this problem?

  Updating installed applications and services to fix security vulnerabilities is an important principle of good cybersecurity.

- How do I solve this problem?

  Click the **Show Applications** button on the bottom of the Launcher on the bottom of the Launcher and click **Software Updater**. You may click **Install Now** to update all installed software, or to only update Firefox first select only **Firefox** under **Details**.

- Why is fixing this problem important?

  When security vulnerabilities are found in software, the software vendor publishes updates that patch the security vulnerabilities. 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.

12) Thunderbird has been updated: 5 pts.

- How do I find this problem?

  Updating installed applications and services to fix security vulnerabilities is an important principle of good cybersecurity.

- How do I solve this problem?

  Click the **Show Applications** button on the bottom of the Launcher and click **Software Updater**. You may click **Install Now** to update all installed software, or to only update Thunderbird first select only **Thunderbird** under **Details**.

- Why is fixing this problem important?

  When security vulnerabilities are found in software, the software vendor publishes updates that patch the security vulnerabilities. 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.

13) Prohibited MP3 files are removed: 6 pts.

- How do I find this problem?

  The README specifically states that non-work related media files are prohibited. There are several ways and commands that can be used to find files and file types including **locate, find,** and **file**.

- How do I solve this problem?

  In a terminal type **locate ' *.mp3'**. In the output of locate you can see the file system location of files with the extension .mp3. The mp3 files under linda's Music directory appear to be non-work related. Type **sudo rm /home/linda/Music/*.mp3** If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- Why is fixing this problem important?

  In addition to being specifically prohibited in the README, media files can also be used to compromise media viewer/player software and could introduce unwanted legal and regulatory issues.

14) Prohibited software ophcrack removed: 6 pts.

- How do I find this problem?

  Removing unauthorized and potentially unwanted programs from a computer is an important cybersecurity principle. Third party software installed on the system should be limited to the software listed in the README, and software required for normal operation of the operating system and services. In this case you can see that ophcrack is installed by clicking the **Show Applications** button and looking at all the programs.

- How do I solve this problem?

  This program does not show up in Ubuntu Software. In a terminal type **sudo apt remove ophcrack** and press **Enter**. Type **Yes** or **y** to remove the application.

- Why is fixing this problem important?

  Removing unauthorized software from your system is important for limiting your risk and reducing your attack surface. Unauthorized programs may leak confidential information, interfere with business-critical software and services, contain various malware and security vulnerabilities, or could introduce unwanted legal and regulatory issues.

15) Prohibited software Wireshark removed: 6 pts.

- How do I find this problem?

  Removing unauthorized and potentially unwanted programs from a computer is an important cybersecurity principle. Third party software installed on the system should be limited to the software listed in the README, and software required for normal operation of the operating system and services. In this case you can see that Wireshark is installed by clicking the **Show Applications** button and looking at all the programs.

- How do I solve this problem?

  This program does not show up in Ubuntu Software. In a terminal type **sudo apt remove wireshark -y** and press **Enter**. Then type **sudo apt autoremove -y** and press **Enter**.

- Why is fixing this problem important?

  Removing unauthorized software from your system is important for limiting your risk and reducing your attack surface. Unauthorized programs may leak confidential information, interfere with business-critical software and services, contain various malware and security vulnerabilities, or could introduce unwanted legal and regulatory issues.

16) SSH root login has been disabled: 6 pts.

- How do I find this problem?

  OpenSSH Server is listed in the README as a critical service. It's important to research how to secure critical services without breaking the required functionality of the service.

- How do I solve this problem?

  In a terminal type **sudo gedit /etc/ssh/sshd_config**. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

  Change the line that says **PermitRootLogin yes** to **PermitRootLogin no**. Save the file and exit.

- Why is fixing this problem important?

  The user root is a known user account on the vast majority of Linux and Unix systems giving adversaries an edge when trying to guess passwords for user accounts. Additionally, the root user is a superuser with the ability to do anything on the system. If the root user account gets compromised the entire system is compromised.

Penalties

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

- Why is this a penalty?

  The README specifies that the OpenSSH server is a critical service.

2) Firefox has been removed: -5 pts.

- Why is this a penalty?

  The README states that Firefox is required software.

3) Thunderbird has been removed: -5 pts.

- Why is this a penalty?

  The README states that Thunderbird is required software.

4) Perl has been removed: -5 pts.

- Why is this a penalty?

  The README states that Perl is required software.