CyberPatriot Mint21

Practice Image Answer Key

Welcome to the CyberPatriot Practice Round! This image will provide you with information on how to solve common vulnerabilities on a Mint 21 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?

  This question asks you for the codename of this Linux distribution.

  On the command line type **lsb_release -a**

```
twellick@mint:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Linuxmint
Description:    Linux Mint 21
Release:        21
Codename:       vanessa
twellick@mint:~$
```

  The answer to this forensics question appears next to **Codename:**

  Remember to **Save** and close the file.

- Why is fixing this problem important?

  It's important to know how to use the command line to determine system information such as the specific Linux distribution. Knowing the type of system you are working on is important when securing it.

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 for the absolute path of the directory containing prohibited (non-work related) MP3 files.

  On the command line, run the command **locate '*.mp3'**

```
twellick@mint:~$ locate '*.mp3'
'/home/twellick/Music/01 - '$'\'''Round Midnight.mp3'
/home/twellick/Music/02 - Blues For Pablo.mp3
/home/twellick/Music/03 - Blue In Green.mp3
/home/twellick/Music/04 - The Pan Piper.mp3
/home/twellick/Music/05 - Drad Dog.mp3
/home/twellick/Music/06 - Basin Street Blues.mp3
/home/twellick/Music/07 - Circle.mp3
/home/twellick/Music/08 - Sweet Pea.mp3
/usr/share/javascript/mathjax/unpacked/extensions/a11y/invalid_keypress.mp3
twellick@mint:~$
```

  It appears that there unauthorized mp3 files in the directory /home/twellick/Music

- Why is fixing this problem important?

  Understanding how to find and locate files is important to determining what is on your system, such as prohibited or unwanted files.

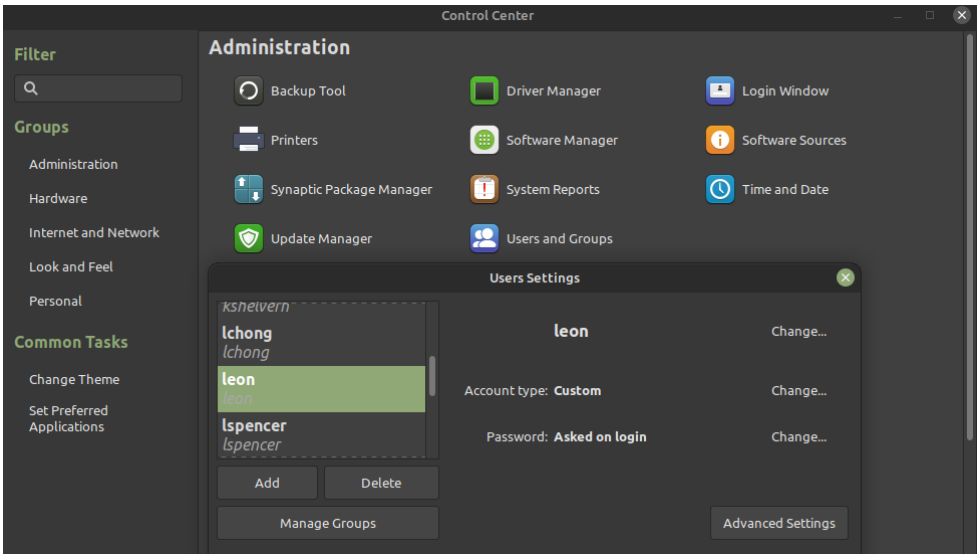
3) Removed unauthorized users leon, oirving, and romero: 4 pts. each

- 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 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?

  Inside the **MATE Menu**, on the left side of the panel, click on **Control Center**. Inside the Control Center window, click on **Users and Groups**. In the User Settings window, select the user to remove and click on **Delete**. If prompted type the password of your current user account. The password for your current user account can be found in the README. Since this is a competition environment and a further analysis of these users' files is not necessary, click **Delete Files**. Repeat the process for all three users, being sure to select each one individually by clicking on it (even if it appears to already be selected).



- Why is fixing this problem important?

  Computer access should be limited to only 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.

6) User tcolby and mralbern are not administrators: 4 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 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?

  Inside the **MATE Menu**, on the left side of the panel, click on **Control Center**. Inside the Control Center window, click on **Users and Groups**. In the User Settings window, select the user and click **Change…** next to **Account type**. If prompted type the password of your current user account. The password for your current user account can be found in the README. In the Change User Account Type window select **Desktop user** and click **OK**. Repeat the process for all three users, being sure to select each one individually by clicking on it (even if it appears to already be selected).

- 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.

8) Changed insecure password for user pmccleery: 4 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 README may list some known administrator passwords. Short, or simple word-based passwords are examples of passwords that adversaries can easily guess or brute force. In a real-world scenario,

you wouldn't know other user's password and would need to employ password auditing techniques.

- How do I solve this problem?

  Inside the **MATE Menu**, on the left side of the panel, click on **Control Center**. Inside the Control Center window, click on **Users and Groups**. In the User Settings window, select the user and click **Change…** next to **Password**. If prompted type the password of your current user account. The password for your current user account can be found in the README. In the Change User Password window select **Generate random password** and click **OK**.

- 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.

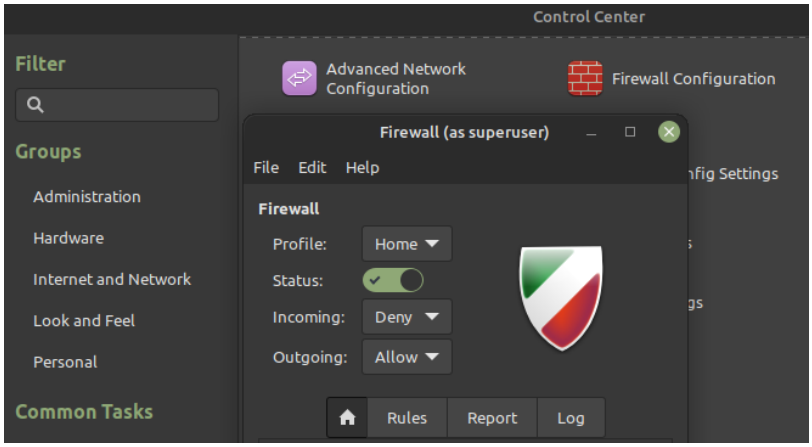
9) Uncomplicated Firewall (UFW) protection has been enabled: 6 pts.

- 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?

  Inside the **MATE Menu**, on the left side of the panel, click on **Control Center**. Inside the Control Center window, click on **Firewall Configuration**. If prompted type the password of your current user account. The password for your current user account can be found in the README. Click the toggle button next to **Status** to enable the firewall. Alternatively, you can type **sudo ufw enable** on the command line.



- 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.

10) Apache2 service has been installed and started: 6 pts.

- How do I find this problem?

  The README asks you to ensure that the Apache service is running.

- How do I solve this problem?

  On the command line, run the commands:

  - sudo apt update
  - sudo apt install -y apache2

  Apt will automatically enable and start the service for you after it is installed.

- Why is fixing this problem important?

  Knowing how to install and manage critical services is an important task to learn, and the first step towards learning how to secure critical services.

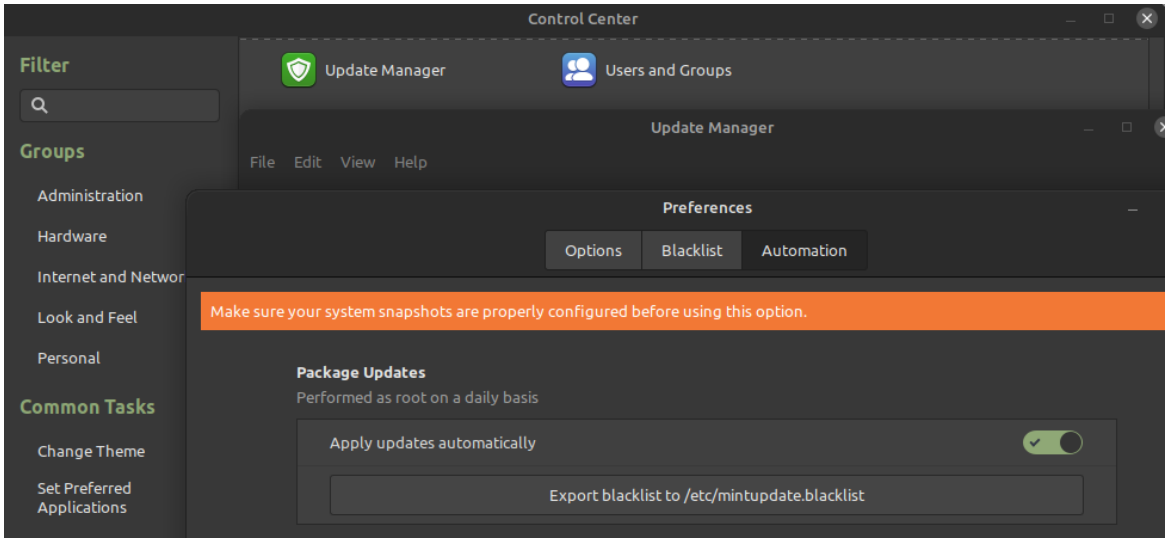
11) The update manager installs updates automatically: 5 pts.

- How do I find this problem?

  Automatically installing updates is good cybersecurity practice.

- How do I solve this problem?

  Inside the **MATE Menu**, on the left side of the panel, click on **Control Center**. Inside the Control Center window, click on **Update Manager**. Select **Edit->Preferences** and click the **Automation** tab inside the Preferences window. In the Automation tab, select Apply updates automatically. If prompted type the password of your current user account. The password for your current user account can be found in the README.



- Why is fixing this problem important?

  New packages with security updates are released regularly. Keeping your software, service, and kernel up to date removes known vulnerabilities from your system.

12) Systemd, OpenSSH, Chromium, and Gimp have been updated: 5 pts. each

- How do I find this problem?

  Installing updates is good cybersecurity practice.

- How do I solve this problem?

It is recommended that you update all of the packages on your system at the same time. To do this, run the following commands:

- sudo apt update
- sudo apt full-upgrade -y

Apt may ask you some questions that require an answer, such as asking if configuration files should be updated or kept for openssh-server. Keeping the local version is usually the safer choice, and changing a configuration file may break services. However, installing the package maintainer's version is sometimes the more secure choice.

In this specific case, for openssh-server, it is safe to select **install the package maintainer's version** but that might not always be the case during a competition.

- Why is fixing this problem important?

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

16) Prohibited MP3 files are removed: 5 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 twellick's Music directory appear to be non-work related. Type **sudo rm /home/twellick/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.

```
twellick@mint:~$ locate '*.mp3'
'/home/twellick/Music/01 - '$'\'''Round Midnight.mp3'
/home/twellick/Music/02 - Blues For Pablo.mp3
/home/twellick/Music/03 - Blue In Green.mp3
/home/twellick/Music/04 - The Pan Piper.mp3
/home/twellick/Music/05 - Drad Dog.mp3
/home/twellick/Music/06 - Basin Street Blues.mp3
/home/twellick/Music/07 - Circle.mp3
/home/twellick/Music/08 - Sweet Pea.mp3
/usr/share/javascript/mathjax/unpacked/extensions/a11y/invalid_keypress.mp3
twellick@mint:~$ sudo rm -f /home/twellick/Music/*.mp3
[sudo] password for twellick:
twellick@mint:~$
```

- 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**.**

17) Prohibited software Wireshark and ophcrack removed: 6 pts. each

- 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 links

to Wireshark and Ophcrack on the MATE desktop.

- How do I solve this problem?

  On the command line run **sudo apt purge -y ophcrack* wireshark***

```
twellick@mint:~$ sudo apt purge -y ophcrack* wireshark*
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'ophcrack' for glob 'ophcrack*'
Note, selecting 'ophcrack-cli' for glob 'ophcrack*'
Note, selecting 'wireshark-dev' for glob 'wireshark*'
Note, selecting 'wireshark-doc' for glob 'wireshark*'
Note, selecting 'wireshark-gtk' for glob 'wireshark*'
Note, selecting 'wireshark-qt' for glob 'wireshark*'
Note, selecting 'wireshark-common' for glob 'wireshark*'
Note, selecting 'wireshark' for glob 'wireshark*'
```

- 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.

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

- How do I find this problem?

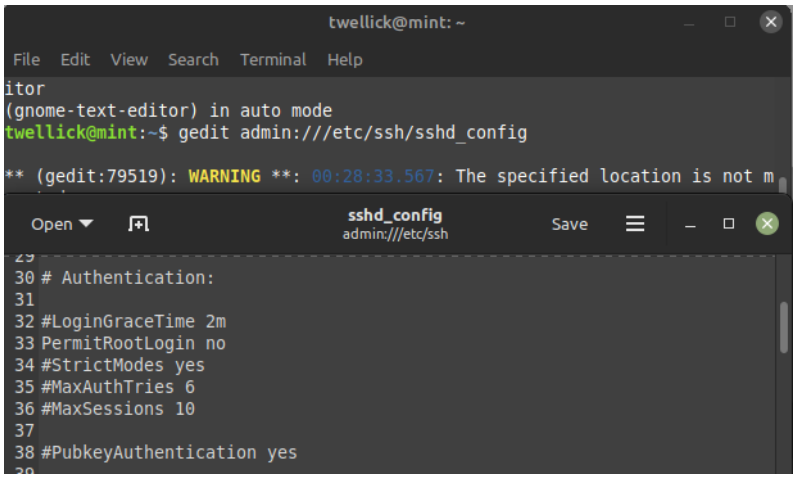
  OpenSSH Server is listed in the README as a critical service. It's important to research how to secure critical services without breaking the required functionality of the service.

- How do I solve this problem?

  In a terminal run the following commands:

  - **sudo apt update**
  - **sudo apt install -y gedit**
  - **gedit admin:///etc/ssh/sshd_config.**

  If prompted type the password of the current user account and click Authenticate. The password for the current user account can be found in the README.



Change 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) WARNING: VirtualBox is unsupported: -0 pts.

- Why is this a penalty?

  This is a warning to inform the user that VirtualBox is **NOT** supported to run the CyberPatriot 18 competition images. Failure to use the version of VMWare Workstation Pro specified on the CyberPatriot website may result in issues that will not be considered for appeals.

2) 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.