CyberPatriot Ubuntu 22
Training 2 Image Answer Key

Welcome to the CyberPatriot Training Round 2! 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: 7 pts.**
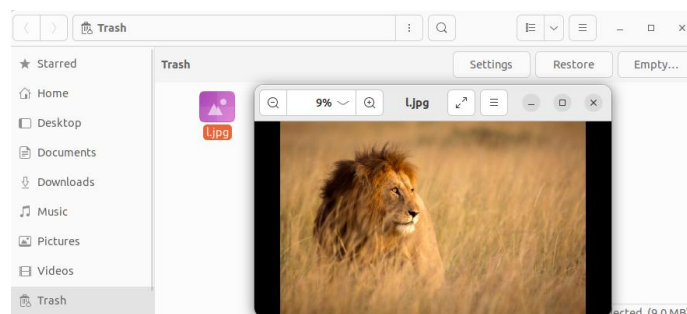
- <u>How do I find this problem?</u>

  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".

- <u>How do I solve this problem?</u>

  The question asks you to decode the contents of the task.txt file on your desktop, complete the task, and asks what animal you encountered. Use an online base64 decoder, such as https://www.base64decode.org/ to decode the contents. You are instructed to open a deleted file in the Trash.
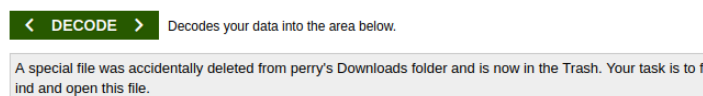
  Click the **Trash** icon on the left side of the screen, then double click on the file **l.jpg** to find the answer.

- 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. It is also important to know about the "Trash" folder, since this is where you can go to restore files that have been deleted.

2) **Forensics Question 2 Correct: 7 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 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.
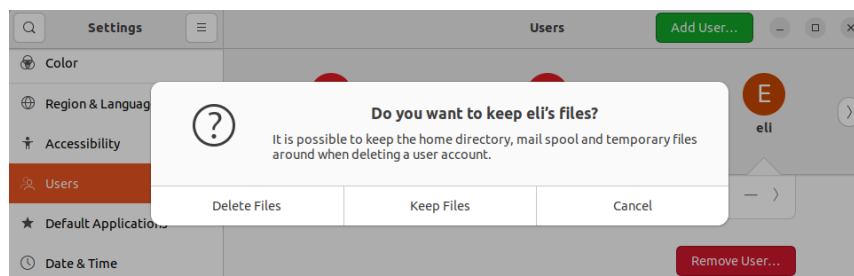
3) **Removed unauthorized user eli: 2 pts.**

- 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 the current user account. The password for your current user account can be found in the README. Select the user **eli**. 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**.

- <u>Why is fixing this problem important?</u>

  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 cornelius is not an administrator: 2 pts.**

- <u>How do I find this problem?</u>

  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.

- <u>How do I solve this problem?</u>

  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 the current user account. The password for the current user account can be found in the README. Select the user **cornelius**. Click on the toggle button next to **Administrator**.
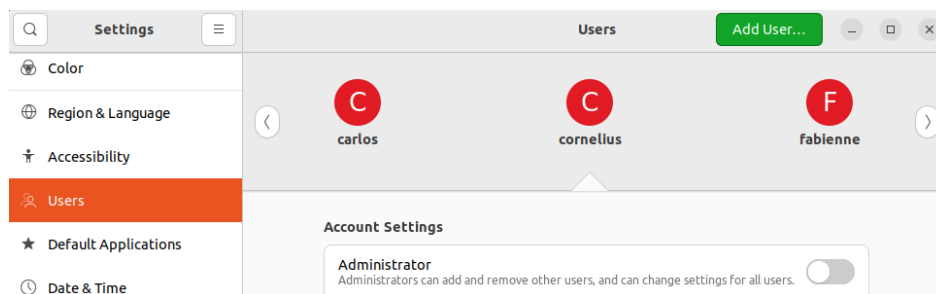
- <u>Why is fixing this problem important?</u>

  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) **Changed insecure password for user alice: 2 pts.**

- <u>How do I find this problem?</u>

  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.

- <u>How do I solve this problem?</u>

  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 the current user account. The password for your current user account can be found in the README. Select the user **alice**. 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**.
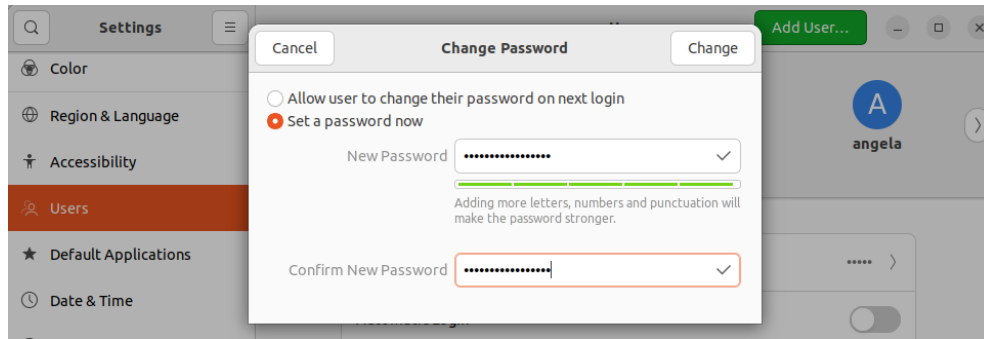
- Why is fixing this problem important?

  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.

6) Added mariya to group pioneers: 5 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 mariya pioneers**. If prompted by sudo for a password, type the current user's password. The password for the 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.

7) A default minimum password age is set: 3 pts.

- How do I find this problem?

  Enforcing industry recommended password policies is good cybersecurity practice.

- How do I solve this problem?

  In a terminal, type **gedit admin:///etc/login.defs** to edit the file. 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.

  Find a line in the file that contains **PASS_MIN_DAYS 0** and change it to be **PASS_MIN_DAYS 2**. This will set a default minimum password age for all new users. Click **Save** before closing the file to make sure your changes

take effect. Guidelines recommend setting a minimum password age of 1-3 days inclusive.

```
158 #
159 # Password aging controls:
160 #
161 #       PASS_MAX_DAYS   Maximum number of days a password may be used.
162 #       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
163 #       PASS_WARN_AGE   Number of days warning given before a password expires.
164 #
165 PASS_MAX_DAYS   99999
166 PASS_MIN_DAYS   2
167 PASS_WARN_AGE   7
```

- <u>Why is fixing this problem important?</u>

   Having a password on a user account that is too short 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.

8) **A minimum password length is required: 4 pts.**

- <u>How do I find this problem?</u>

   Enforcing industry recommended password policies is good cybersecurity practice.

- <u>How do I solve this problem?</u>

   In a terminal, type **gedit admin:///etc/pam.d/common-password** to edit the file. 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.

   Find a line in the file that contains **password requisite pam_pwquality.so retry=3** and append option **minlen=10**. This will set the requirement that all users must have passwords that are at least 10 characters long. Click **Save** before closing the file to make sure your changes take effect. A required password length of 10 or higher is recommended.

```
24 # here are the per-package modules (the "Primary" block)
25 password       requisite                   pam_pwquality.so retry=3 minlen=10
26 password       [success=2 default=ignore]  pam_unix.so obscure use_authtok try_first_pass yescrypt
27 password       sufficient                  pam_sss.so use_authtok
```

- <u>Why is fixing this problem important?</u>

   Having a password on a user account that is too short 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.

9) **An account lockout policy is configured: 3 pts.**

- <u>How do I find this problem?</u>

   Enforcing industry recommended password policies is good cybersecurity practice.

- <u>How do I solve this problem?</u>

   In a terminal, type **sudo touch /usr/share/pam-configs/faillock**, then **gedit admin:///usr/share/pam-configs/faillock** to edit the file. If prompted type the password of the current user account. The password for the current user account can be found in the README.

```
perry@ubuntu:~$ sudo touch /usr/share/pam-configs/faillock
[sudo] password for perry:
perry@ubuntu:~$ gedit admin:///usr/share/pam-configs/faillock
```
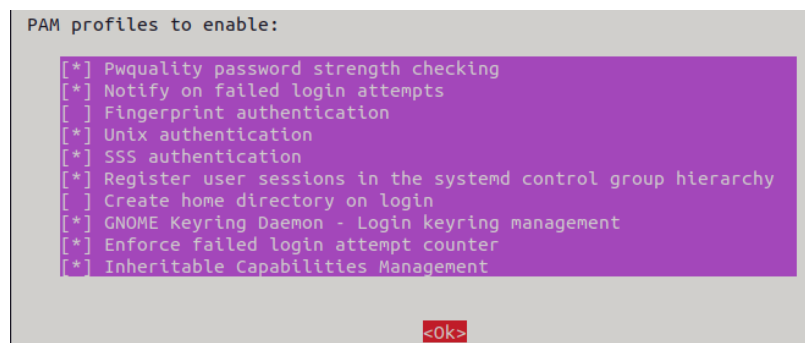
In **/usr/share/pam-configs/faillock** type the following text:

```
Name: Enforce failed login attempt counter
Default: no
Priority: 0
Auth-Type: Primary
Auth:
    [default=die]   pam_faillock.so authfail
    sufficient  pam_faillock.so authsucc
```

Save the file and close gedit when you are finished. Back in the terminal, type **sudo touch /usr/share/pam-configs/faillock_notify**, then **gedit admin:///usr/share/pam-configs/faillock_notify** to edit the file. If prompted type the password of the current user account. The password for the current user account can be found in the README. In **/usr/share/pam-configs/faillock_notify** type the following text:

```
Name: Notify on failed login attempts
Default: no
Priority: 1024
Auth-Type: Primary
Auth:
    requisite   pam_faillock.so preauth
```

Save the file and close gedit when you are finished. Back in the terminal type **sudo pam-auth-update**. Select, with the spacebar, **Notify on failed login attempts**, and **Enforce failed login attempt counter**, and then select **<Ok>**.

```
PAM profiles to enable:

    [*] Pwquality password strength checking
    [*] Notify on failed login attempts
    [ ] Fingerprint authentication
    [*] Unix authentication
    [*] SSS authentication
    [*] Register user sessions in the systemd control group hierarchy
    [ ] Create home directory on login
    [*] GNOME Keyring Daemon - Login keyring management
    [*] Enforce failed login attempt counter
    [*] Inheritable Capabilities Management


                        <Ok>
```

- <u>Why is fixing this problem important?</u>

Setting secure account lockout policies limits your risk of having a password compromised. When an adversary performs a brute force attack this will stop or slow down their attack, greatly increasing the time required to compromise a user account.

10) Null passwords do not authenticate: 3 pts.

- <u>How do I find this problem?</u>

Enforcing industry recommended password policies is good cybersecurity practice.

- <u>How do I solve this problem?</u>

In a terminal, type **gedit admin:///etc/pam.d/common-auth** to edit the file. 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.

Find a line in the file that contains **auth [success=2 default=ignore] pam_unix.so nullok** and remove the option **nullok**.

```
16 # here are the per-package modules (the "Primary" block)
17 auth    [success=2 default=ignore]     pam_unix.so
18 auth    [success=1 default=ignore]     pam_sss.so use_first_pass
19 # here's the fallback if no module succeeds
20 auth    requisite                      pam_deny.so
```

- <u>Why is fixing this problem important?</u>

  The "nullok" text included in the common-auth file allows accounts with empty passwords to login without a password prompt. This would make it easy for an attacker to gain access to your user accounts without having a password. The nullok option is always insecure, the nullok_secure option is a reasonable default, but having neither of the options set is the most secure configuration.

11) IPv4 TCP SYN cookies have been enabled: 4 pts.

- <u>How do I find this problem?</u>

  Enforcing industry recommended security options is good cybersecurity practice.

- <u>How do I solve this problem?</u>

  In a terminal, type **gedit admin:///etc/sysctl.conf**. If prompted type the password of the current user account. The password for the current user account can be found in the README. **Change** net.ipv4.tcp_syncookies=0 to be **net.ipv4.tcp_syncookies=1**

```
22 # Uncomment the next line to enable TCP/IP SYN cookies
23 # See http://lwn.net/Articles/277146/
24 # Note: This may impact IPv6 TCP sessions too
25 net.ipv4.tcp_syncookies=1
```

  Save the file and close gedit. In the terminal type **sudo sysctl --system** to apply the settings. If prompted for a password by sudo, type the current user's password. The password for the current user account can be found in the README.

- <u>Why is fixing this problem important?</u>

  SYN cookies are a networking technique used to resist SYN flood attacks, a type of denial of service attack.

12) IPv4 forwarding has been disabled: 4 pts.

- <u>How do I find this problem?</u>

  Enforcing industry recommended security options is good cybersecurity practice.

- <u>How do I solve this problem?</u>

  In a terminal, type **gedit admin:///etc/sysctl.conf**. If prompted type the password of the current user account. The password for the current user account can be found in the README. **Change** net.ipv4.ip_forward=1 to be **net.ipv4.ip_forward=0**

```
27 # Uncomment the next line to enable packet forwarding for IPv4
28 net.ipv4.ip_forward=0
```

Save the file and close gedit. In the terminal type **sudo sysctl --system** to apply the settings. If prompted for a password by sudo, type the current user's password. The password for the current user account can be found in the README.

- <u>Why is fixing this problem important?</u>

IP forwarding, if enabled, will allow Linux to act as a network firewall, or router by forwarding packets. It is recommended to disable this functionality if you do not need it, as it can expose you to additional types of vulnerabilities and attacks.

13) Uncomplicated Firewall (UFW) protection has been enabled: 5 pts.

- <u>How do I find this problem?</u>

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.

- <u>How do I solve this problem?</u>

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

- <u>Why is fixing this problem important?</u>

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

14) Insecure permissions on shadow file fixed: 5 pts.

- <u>How do I find this problem?</u>

Auditing the permissions of files on your system is important to maintaining the security of your system.

- <u>How do I solve this problem?</u>

In a terminal, type **ls -alF /etc/shadow** to view the current permissions of the shadow file. Notice the shadow file is world readable. Type **sudo chmod 640 /etc/shadow** to remove all world permissions from the shadow file. If prompted by sudo for a password, type the current user's password. The password for the current user account can be found in the README.

```
perry@ubuntu:~$ ls -alF /etc/shadow
-rw-r--r-- 1 root shadow 4386 Oct  6 03:29 /etc/shadow
perry@ubuntu:~$ sudo chmod 640 /etc/shadow
[sudo] password for perry:
perry@ubuntu:~$ ls -alF /etc/shadow
-rw-r----- 1 root shadow 4386 Oct  6 03:29 /etc/shadow
perry@ubuntu:~$
```

- <u>Why is fixing this problem important?</u>

Insecure permissions on some files, including the shadow file, can lead to vulnerabilities. If the shadow file is world readable, anyone on your system can obtain password hashes and attempt to crack them.

15) X2Go has been installed: 5pts.

- How do I find this problem?

  The ReadMe states that X2GO is required software that needs to be installed.

- How do I solve this problem?

  In a terminal, type **sudo apt update** and press **Enter**. Next, type **sudo apt install x2goserver** to install the service. If prompted by sudo for a password, type the current user's password. The password for the current user account can be found in the README. Press **Enter** to continue the installation.

- Why is fixing this problem important?

  Installing the required software ensures that employees have everything that they need to perform their jobs on their company computer. X2Go is a remote desktop software that allows a user to access and manage another computer from a different location. This program is often used by IT administrators.

16) Nginx service has been disabled or removed: 4 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, any 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 disable --now nginx** to disable and stop the service. If prompted by sudo for a password, type the current user's password. The password for the current user account can be found in the README.

- Why is fixing this problem important?

  Disabling unnecessary services can reduce your attack surface. The fewer services an adversary can 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.

17) FTP service has been disabled or removed: 4 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, any 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.

- <u>How do I solve this problem?</u>

  In a terminal, type **sudo systemctl disable --now vsftpd** to disable and stop the service. If prompted by sudo for a password, type the current user's password. The password for the current user account can be found in the README.

  ```
  perry@ubuntu:~$ sudo systemctl disable --now vsftpd
  [sudo] password for perry:
  Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
  Executing: /lib/systemd/systemd-sysv-install disable vsftpd
  Removed /etc/systemd/system/multi-user.target.wants/vsftpd.service.
  ```

- <u>Why is fixing this problem important?</u>

  Disabling unnecessary services can reduce your attack surface. The fewer services an adversary can 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.

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

- <u>How do I find this problem?</u>

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

- <u>How do I solve this problem?</u>

  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 the current user account. The password for the current user account can be found in the README. Click **Close**.
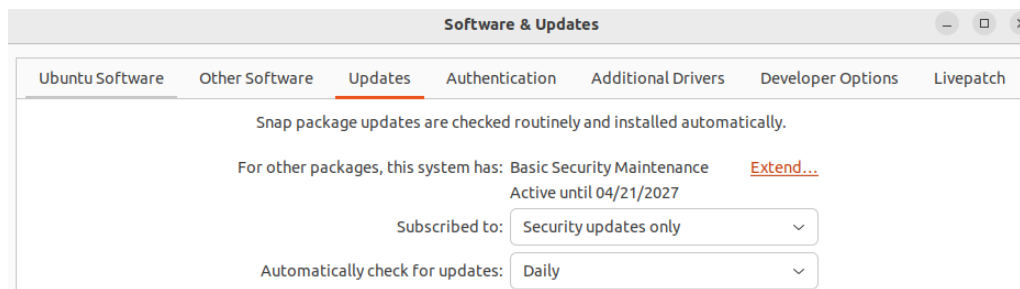
- <u>Why is fixing this problem important?</u>

  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.
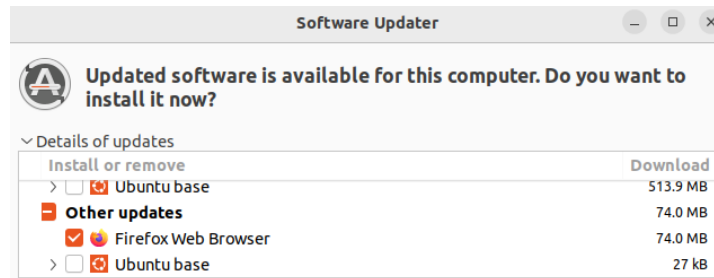
19) Firefox has been updated: 4 pts.

- <u>How do I find this problem?</u>

  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.

20) Thunderbird has been updated: 4 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**.
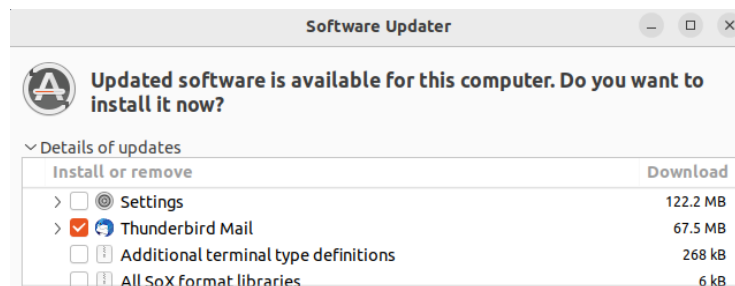
- Why is fixing this problem important?

  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.

21) Prohibited MP3 files are removed: 4 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.

  ```
  perry@ubuntu:~$ locate '*.mp3'
  '/home/linda/Music/Ain'$'\'''t Got Rhythm.mp3'
  '/home/linda/Music/Couldn'$'\'''t Kick My Way Right Into Her Heart.mp3'
  /home/linda/Music/Fabulous.mp3
  /home/linda/Music/You Snuck Your Way Right Into My Heart.mp3
  perry@ubuntu:~$ sudo rm /home/linda/Music/*.mp3
  ```

- 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.

22) Prohibited software AisleRiot removed: 4 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 AisleRiot 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 purge aisleriot** and press **Enter**. Type **Enter** when prompted to continue and remove the application. Then, type **sudo apt autoremove -y** and **Enter.**

  ```
  perry@ubuntu:~$ sudo apt purge aisleriot
  [sudo] password for perry:
  Reading package lists... Done
  Building dependency tree... Done
  Reading state information... Done
  The following packages were automatically installed and are no longer required:
    guile-2.2-libs libgc1
  Use 'sudo apt autoremove' to remove them.
  The following packages will be REMOVED:
    aisleriot*
  0 upgraded, 0 newly installed, 1 to remove and 392 not upgraded.
  After this operation, 9,019 kB disk space will be freed.
  Do you want to continue? [Y/n]
  ```

- 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.

23) Removed netcat backdoor: 5 pts.

- How do I find this problem?

  Removing malware such as backdoors, keyloggers, sniffers, viruses, trojans, worms, botnets, among others, is
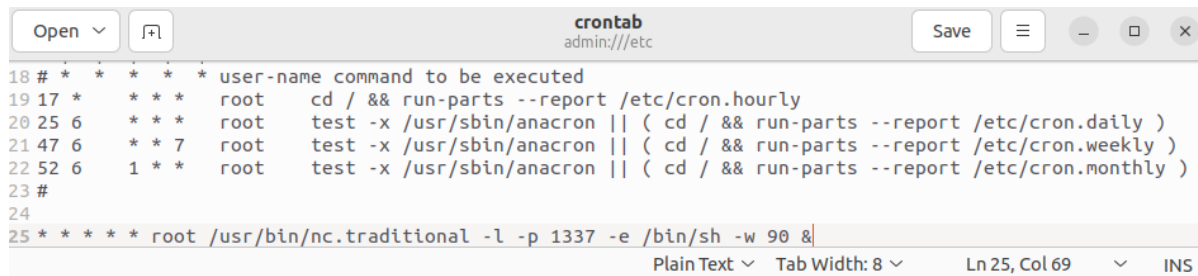
very important. Malware can often be found by using antivirus and antimalware scanners. Malware that is currently running can be found by analyzing the currently running processes, network traffic, and open ports. Programs such as **ps**, **ss**, and **lsof** can help when looking for malware.

- How do I solve this problem?

  In a terminal type **sudo ss -tlnp**. If prompted by sudo for a password, type the current user's password. The password for the current user account can be found in the README. Notice nc.traditional is listening on port 1337.

```
perry@ubuntu:~$ sudo ss -tlnp
State    Recv-Q   Send-Q    Local Address:Port     Peer Address:Port   Process
LISTEN   0        4096            0.0.0.0:59309         0.0.0.0:*       users:(("rpc.statd",pid=1011,fd=9))
LISTEN   0        4096            0.0.0.0:111           0.0.0.0:*       users:(("rpcbind",pid=633,fd=4),("systemd",pid=1,fd=65))
LISTEN   0        4096       127.0.0.53%lo:53           0.0.0.0:*       users:(("systemd-resolve",pid=643,fd=14))
LISTEN   0        128             0.0.0.0:22            0.0.0.0:*       users:(("sshd",pid=904,fd=3))
LISTEN   0        128         127.0.0.1:631             0.0.0.0:*       users:(("cupsd",pid=951,fd=7))
LISTEN   0        1               0.0.0.0:1337          0.0.0.0:*       users:(("nc.traditional",pid=12890,fd=3))
LISTEN   0        4096            0.0.0.0:42201         0.0.0.0:*       users:(("rpc.mountd",pid=1012,fd=5))
```

  In a terminal, type **gedit admin:///etc/crontab** to edit the main crontab file. 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. Remove the line containing **/usr/bin/nc.traditional**

```
                                            crontab
  Open  ⌄   ⊞                             admin:///etc                      Save   ≡   –  □  ✕

18 # *   *   *   *   * user-name command to be executed
19 17 *     * * *    root    cd / && run-parts --report /etc/cron.hourly
20 25 6     * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
21 47 6     * * 7    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
22 52 6     1 * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
23 #
24
25 * * * * * root /usr/bin/nc.traditional -l -p 1337 -e /bin/sh -w 90 &

                                          Plain Text ⌄   Tab Width: 8 ⌄      Ln 25, Col 69      ⌄    INS
```

  In a terminal, type **sudo pkill -f nc.traditional**, then **which nc.traditional**, then **sudo rm /usr/bin/nc.traditional** If prompted by sudo for a password, type the current user's password. The password for the current user account can be found in the README

```
perry@ubuntu:~$ sudo pkill -f nc.traditional
[sudo] password for perry:
perry@ubuntu:~$ which nc.traditional
/usr/bin/nc.traditional
perry@ubuntu:~$ sudo rm /usr/bin/nc.traditional
```

- Why is fixing this problem important?

  Malware, including backdoors, keyloggers, sniffers, viruses, trojans, worms on your system means your system has been compromised. In the real world you may want to take actions such as contacting law enforcement, imaging the disk drive for later analysis, conducting a forensics investigation, isolating the system, and eventually wiping it. Since this is a competition environment, answer any related forensics questions and then remove all signs of the malware.

24) SSH root login has been disabled: 5 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 **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.

- <u>Why is fixing this problem important?</u>

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, disabled, or removed: -5 pts.**

- <u>Why is this a penalty?</u>

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

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

- <u>Why is this a penalty?</u>

The README states that Firefox is required software.

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

- <u>Why is this a penalty?</u>

The README states that Thunderbird is required software.

4) **Perl has been removed: -5 pts.**

- <u>Why is this a penalty?</u>

The README states that Perl is required software.