CyberPatriot Mint21

Training Round 2 Answer Key

Welcome to the CyberPatriot Training Round 2! 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: 6 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 absolute path of the directory containing the python backdoor.

  On the command line type the commands:

- **`ss -tlnp`**
- **`ps -ef | grep python`**

```
chowe@linuxmint:~$ sudo ss -tlnp
State     Recv-Q    Send-Q       Local Address:Port       Peer Address:Port   Process
LISTEN    0         511                0.0.0.0:80              0.0.0.0:*       users:(("nginx",pid=914,fd=6),("nginx",pid=913,fd=6),
LISTEN    0         32                 0.0.0.0:21              0.0.0.0:*       users:(("vsftpd",pid=888,fd=3))
LISTEN    0         4096         127.0.0.53%lo:53              0.0.0.0:*       users:(("systemd-resolve",pid=696,fd=14))
LISTEN    0         128              127.0.0.1:631             0.0.0.0:*       users:(("cupsd",pid=1388,fd=7))
LISTEN    0         1                  0.0.0.0:1337            0.0.0.0:*       users:(("python3",pid=1789,fd=3))
LISTEN    0         511                   [::]:80                 [::]:*       users:(("nginx",pid=914,fd=7),("nginx",pid=913,fd=7),
LISTEN    0         128                  [::1]:631                [::]:*       users:(("cupsd",pid=1388,fd=6))
LISTEN    0         256                      *:3128                  *:*       users:(("squid",pid=1034,fd=12))
chowe@linuxmint:~$ ps -ef | grep python
root         740       1  0 02:27 ?        00:00:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
chowe       1505    1101  0 02:28 ?        00:00:00 /usr/bin/python3 /usr/bin/blueman-applet
chowe       1526    1101  0 02:28 ?        00:00:00 /usr/bin/python3 /usr/share/system-config-printer/applet.py
root        1788    1787  0 02:29 ?        00:00:00 /bin/sh -c python3 /usr/share/zod/kneelB4zod.py
root        1789    1788  0 02:29 ?        00:00:00 python3 /usr/share/zod/kneelB4zod.py
chowe       1972    1862  0 02:34 pts/0    00:00:00 grep --color=auto python
chowe@linuxmint:~$
```

Based on this information, it looks like the python script /usr/share/zod/kneelB4zod.py is listening on port 1337. Since this question asks for the absolute path of the directory, the answer is /usr/share/zod

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

- Why is fixing this problem important?

  It's important to know what processes are running, and which ones are listening on the network.

2) Forensics Question 2 Correct: 6 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 two plaintext passwords in the .pcap file.

  On the command line, run the following commands:

- **sudo apt install tshark**
- **cd ~/Desktop**
- **tshark -q -z follow,tcp,ascii,0 -r ftp_capture.pcap | grep PASS**
- **tshark -q -z follow,tcp,ascii,21 -r ftp_capture.pcap | grep PASS**

```
chowe@linuxmint:~/Desktop$ tshark -q -z follow,tcp,ascii,0 -r ftp_capture.pcap | grep PASS
PASS community
chowe@linuxmint:~/Desktop$ tshark -q -z follow,tcp,ascii,21 -r ftp_capture.pcap | grep PASS
PASS Symphonic
chowe@linuxmint:~/Desktop$
```

The two passwords were in tcp streams 0 and 21 in ftp_capture.pcap, which we displayed with tshark. The most common method to solve this would be to look through each tcp stream with either tshark, wireshark, or tcpdump.

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

- Why is fixing this problem important?

  You must be able to determine what data is being transmitted on the network in order to secure the network and systems connected to the network.

3) Forensics Question 3 Correct: 6 pts.

- How do I find this problem?

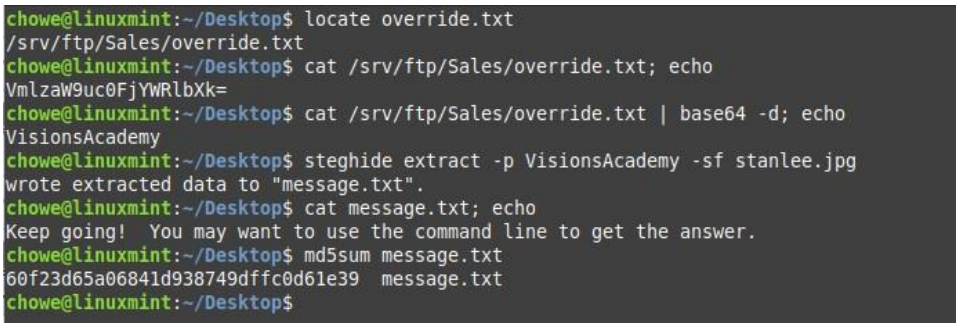
When you open an image, please read all the "Forensics Questions" thoroughly before modifying the image as you may change something that prevents you from answering the question correctly. There is a file on the Desktop here named "Forensics Question 3".

- How do I solve this problem?

This question asks you for the MD5 sum of a message embedded inside the image stanlee.jpg and notes that you will need to decode a passphrase in override.txt.

On the command line, run the following commands:

- **Locate override.txt**
- **cat /srv/ftp/Sales/override.txt; echo**
- **cat /srv/ftp/Sales/override.txt | base64 -d; echo**
- **steghide extract -p VisionsAcademy -sf stanlee.jpg**
- **cat message.txt; echo**
- **md5sum message.txt**



The content of override.txt file is base64 encoded. This contains a passphrase which can be used with steghide to extract the file message.txt from stanlee.jpg.

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

- Why is fixing this problem important?

It's important to know how to recognize different encodings, and to know how data can easily be hidden for malicious purposes such as exfiltrating sensitive information. It's also important to know how to work on the command line to be able to solve problems more effectively and easily than by using graphical applications.

4) Removed unauthorized users penguru

- 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?

  The user liv is a hidden user since her uid is less than 1000. It is easiest to remove these users using the command line. On the command line type the following commands:

  sudo deluser --remove-home penguru

- 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 ham is not an administrator: 3 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?

  One of the most powerful groups that separates administrator accounts from standard accounts is the sudo group. Members of this group are allowed to use the sudo command. We can remove may from the sudo group using the command line. On the command line type the following command:

  ```
  sudo gpasswd -d ham sudo
  ```

- 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.

7) User noir has a maximum password age: 4 pts.

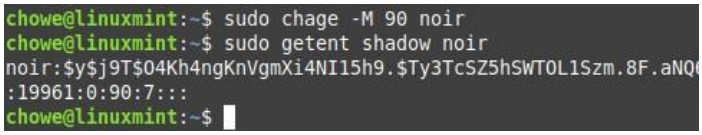
- How do I find this problem?

  Enforcing industry recommended password policies is good cybersecurity practice.

- How do I solve this problem?

  To set a maximum password age for the user noir, run the following commands:

- **sudo chage -M 90 noir**
- **sudo getent shadow noir**



- Why is fixing this problem important?

  User passwords may become compromised by disclosure of the plaintext password, password hashes, or online attacks. Changing passwords helps to mitigate the damage and risk associated with compromised passwords, password hashes, or online attacks.

8) Created the group spider: 3 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 asks you to create a group called spider and add users to the group.

- How do I solve this problem?

  On Debian based machines, like Mint, you should use the addgroup command when adding groups on the command line. On the command line run the following command:

  sudo addgroup spider

- Why is fixing this problem important?

  Knowing how to create and manage groups is important. The correct operation and security of many system functions depend on groups and group membership.

9) Added users to group spider: 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 asks you to create a group called multiverse and add users to the group.

- How do I solve this problem?

  On the command line run the following command:

  `sudo gpasswd -M may,peni,stan,miguel spider`

- Why is fixing this problem important?

  Knowing how to create and manage groups is important. The correct operation and security of many system functions depend on groups and group membership.

10) Root password is no longer blank: 4 pts.

- How do I find this problem?

  Blank passwords are a security risk. Users with blank passwords can be identified by examining the shadow file.

- How do I solve this problem?

  On the command line run the following command:

  - **`sudo getent shadow root`**
  - **`sudo passwd -l root`**
  - **`sudo getent shadow root`**

```
chowe@linuxmint:~$ sudo getent shadow root
root::19830:0:99999:7:::
chowe@linuxmint:~$ sudo passwd -l root
passwd: password expiry information changed.
chowe@linuxmint:~$ sudo getent shadow root
root:!:19830:0:99999:7:::
chowe@linuxmint:~$
```

- Why is fixing this problem important?

  Blank passwords are a security risk. Disabling root's password is generally more secure than setting a password for the root account.

11) A minimum password length is required: 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, run the command:

  - **gedit admin:///etc/pam.d/common-password**

  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. Append **minlen=10** to the following line:

  password [success=1 default=ignore] pam_unix.so obscure yescrypt

  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        [success=1 default=ignore]      pam_unix.so obscure yescrypt minlen=10
26 # here's the fallback if no module succeeds
27 password        requisite                       pam_deny.so
```

- Why is fixing this problem important?

  Having a password on a user account that is too short makes it much more vulnerable to attacks. A single compromised password can easily lead to the compromise of the entire system or even the entire network.

12) Previous passwords are remembered 3 pts.

- How do I find this problem?
  Enforcing industry recommended password policies is a good cybersecurity practice.

- How do I solve this problem?
  In a terminal, run the command:

  sudo gedit /etc/pam.d/common-password

  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.

  On the line where it says pam_unix.so, add the following text to the end of the line:

  remember=3

  Click Save before closing the file.

  Why is fixing this problem important?

  Setting the password policy to remember previous passwords prevents users from resetting their password to a password that was already used. If an old password was obtained by an attacker, it's best to have users reset to new passwords each time they reset. This prevents attackers gaining access to your system by using an old password that is being reused.

13) An account lockout policy is configured: 4 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, run the following commands. If prompted type the password of the current user account. The password for the current user account can be found in the README.

  - **sudo touch /usr/share/pam-configs/faillock** ○ **gedit admin:///usr/share/pam-configs/faillock**

```
chowe@linuxmint:~$ sudo touch /usr/share/pam-configs/faillock
chowe@linuxmint:~$ gedit admin:///usr/share/pam-configs/faillock
```

  In **/usr/share/pam-configs/faillock** type the following text:

```
Name: Lockout on failed logins
Default: no
Priority: 0 Auth-Type:
Primary Auth:
      [default=die]            pam_faillock.so authfail
```

  Save the file and close gedit when you are finished. Back in the terminal, run the following commands:

  - **sudo touch /usr/share/pam-configs/faillock_reset** ○ **gedit admin:///usr/share/pam-configs/faillock_reset**

  In **/usr/share/pam-configs/faillock_reset** type the following text:

```
Name: Reset lockout on success
Default: no
Priority: 0
Auth-Type: Additional Auth:
      required                 pam_faillock.so authsucc
```

  Save the file and close gedit when you are finished. Back in the terminal run the command

  - **sudo pam-auth-update**

  Save the file and close gedit when you are finished. Back in the terminal, run the following commands:

  - **sudo touch /usr/share/pam-configs/faillock_notify** ○ **gedit admin:///usr/share/pam-configs/faillock_notify**

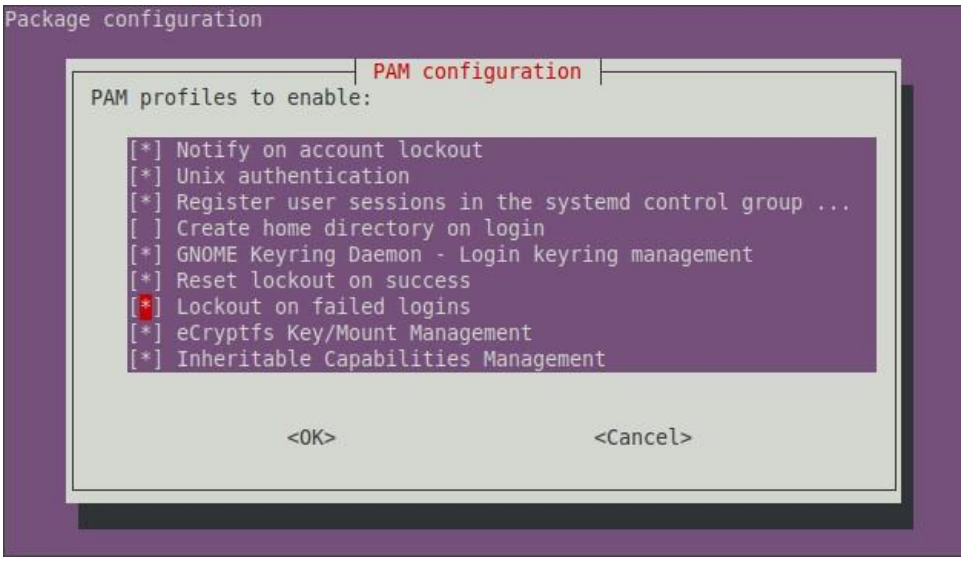
  In **/usr/share/pam-configs/faillock_notify** type the following text:

```
Name: Notify on account lockout
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 run the command

  - **sudo pam-auth-update**

Using the tab key and the spacebar, select <OK>. Then, ysing the arrow keys and the spacebar, select **Notify on account lockout**, **Reset lockout on success, Lockout on failed logins**, and then select **<OK>**.



- Why is fixing this problem important?

  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.

14) Null passwords do not authenticate: 4 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/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 try_first_pass Remove

  the option **nullok**.

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

- Why is fixing this problem important?

  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.

15) Address space layout randomization enabled: 4 pts.

- How do I find this problem?

  Enforcing industry recommended security options is good cybersecurity practice.

- How do I solve this problem?

  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** kernel.randomize_va_space=0 to be **kernel.randomize_va_space=2**

```
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

kernel.randomize_va_space = 2
```

  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.

- Why is fixing this problem important?

  Address space randomization is important in helping to reduce the effectiveness of exploits that take advantage of programming errors, such as buffer overflow vulnerabilities.

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

- How do I find this problem?

  Enforcing industry recommended security options is good cybersecurity practice.

- How do I solve this problem?

  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**

```
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
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.

- Why is fixing this problem important?

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

17) Uncomplicated Firewall (UFW) protection has been enabled: 3 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.

18) 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.

```
chowe@linuxmint:~$ sudo systemctl disable --now nginx
Synchronizing state of nginx.service with SysV service script with /lib/systemd/
Executing: /lib/systemd/systemd-sysv-install disable nginx
Removed /etc/systemd/system/multi-user.target.wants/nginx.service.
```

- 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.

19) Squid proxy 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 squid** 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. Squid can take up to a minute to stop.

```
chowe@linuxmint:~$ sudo systemctl disable --now squid
Synchronizing state of squid.service with SysV service script with /lib/systemd/
Executing: /lib/systemd/systemd-sysv-install disable squid
Removed /etc/systemd/system/multi-user.target.wants/squid.service.
```

- 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.

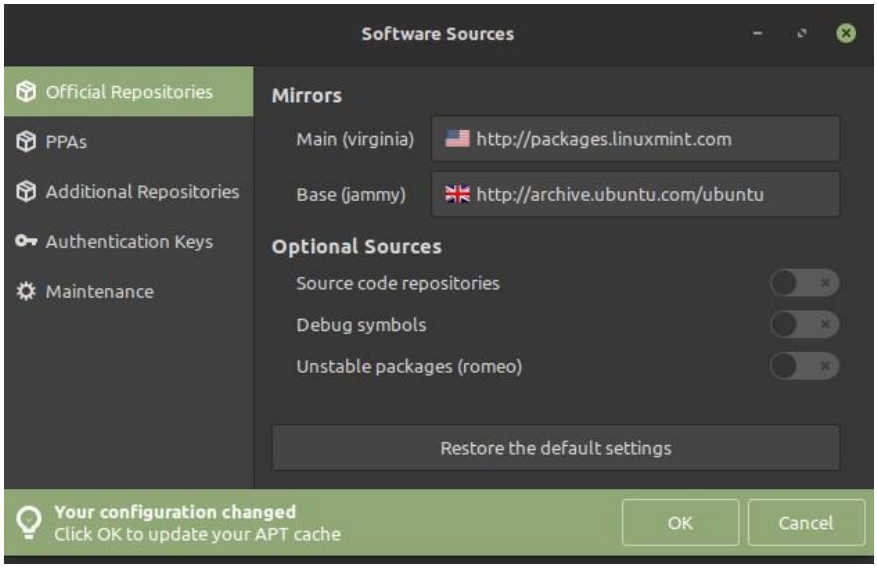
20) The update manager installs updates automatically: 3 pts.

- How do I find this problem?

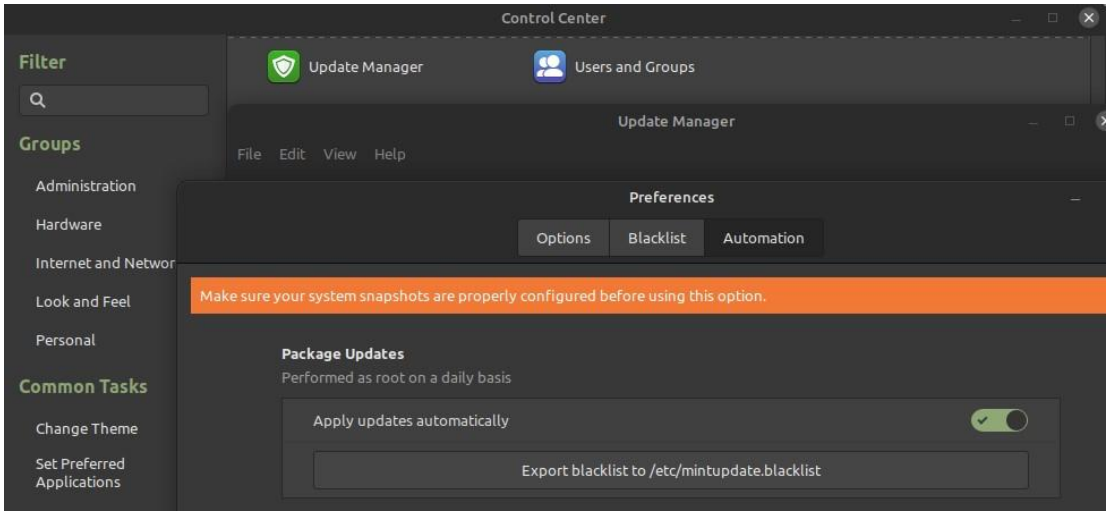
  Automatically installing updates is good cybersecurity practice.

- 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**. As soon as you start Update Manager it may inform you that Your APT configuration is corrupt. If this happens, click **OK** to switch to another Linux Mint mirror. If prompted, type the current user's password, the select **restore default settings**, then **OK**. After the software sources have been updated, close the Software Sources window, and return to the Update Manager Window. This is necessary to get credit for the next item "**Vsftpd has been updated**"



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.



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

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

21) Vsftpd updated: 3 pts.

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

  Installing updates is good cybersecurity practice.

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

  First, make sure your software sources are configured. Instructions for this can be found above under "**The update manager installs updates automatically**"

  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.

22) Prohibited OGG 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 run the following commands:

- **`sudo locate '*.ogg'.`**
- **`sudo sh -c "rm /home/steve/Music/*/*/*.ogg"`**

  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**.**

23) Removed prohibited software archive pyrdp: 4 pts.

- How do I find this problem?

  The README lists required software and critical services. The pyrdp archive appears to be unauthorized and unwanted software.

- How do I solve this problem?

  In a terminal run the following commands:

- **`locate *.zip.`**
- **`sudo rm /usr/games/pyrdp-master.zip`**

  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.

```
chowe@linuxmint:~$ locate *.zip
/usr/games/pyrdp-master.zip
/usr/lib/libreoffice/share/config/images_colibre.zip
/usr/lib/libreoffice/share/config/images_helpimg.zip
/usr/lib/libreoffice/share/config/wizard/web/buttons/elementary.zip
/usr/lib/libreoffice/share/config/wizard/web/buttons/round-white.zip
/usr/lib/libreoffice/share/config/wizard/web/buttons/simple.zip
/usr/lib/libreoffice/share/config/wizard/web/buttons/sukapura.zip
/usr/share/libreoffice/share/config/images_colibre.zip
/usr/share/libreoffice/share/config/images_helpimg.zip
chowe@linuxmint:~$ sudo rm /usr/games/pyrdp-master.zip
```

- Why is fixing this problem important?

  Unauthorized software can be a security risk and may contain vulnerabilities, or give malicious users the access to additional tools**.**

24) Prohibited software doona and xproble removed: 3 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 doona xprobe`**

```
chowe@linuxmint:~$ sudo apt purge -y doona xprobe
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

- 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.

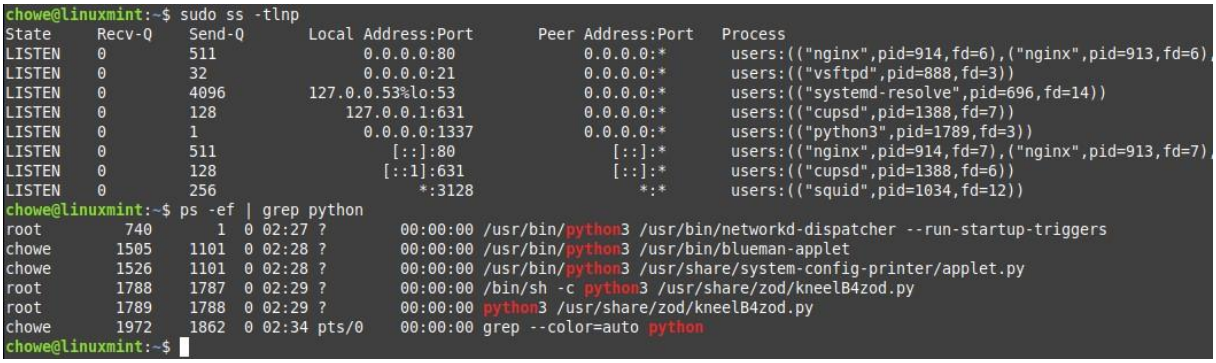
26) Removed zod backdoor: 6 pts.

- 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?

  When answering Forensics Question 1 a python backdoor was discovered:



In a terminal run the following commands to stop and remove the backdoor:

- **sudo rm -f /usr/share/zod/kneelB4zod.py**
- **sudo pkill -f kneelB4zod.py**

- Why is fixing this problem important?

  Backdoors allow unauthorized individuals to be able to access your machine over the network, often as root.

Penalties

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

- Why is this a penalty?

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

2) Important files removed from public FTP directories: -5 pts.

- Why is this a penalty?

  Important, authorized, and work-related files should not be deleted or the service will not be able to provide the intended functionality.