There are color codes corresponding to what images you'll find these challenges on.
Black - Mandatory for nearly all images
Green - Easy Round 1 or Round 2 Images
Orange - Round 2 or State Round
Red - Black magic super hard images (Nationals)

1. **Read the README. Get root passwords and authorized users.**
2. **Answer forensic questions.** If you need to find files use the command "find /home -name '*' -type f" You can change "/home" to "/" if you want to search the entire computer.
3. **Manage users.** Delete any that aren't supposed to exist. Undisable the accounts that are supposed to exist. Make sure everyone who should be admin is admin and everyone who is supposed to be standard is standard. Add any that are needed. Make sure to unlock and re-lock. System Settings> Users and Groups > Unlock.
4. **Look in the README for "insecure" passwords.** Change those users' passwords.
5. **System Settings>Software&Updates** have it check for recommended updates once a day.
6. **Delete all non-work related files** (If specified in readme) use: find / -name '*.<file extension>' -type f -delete. Remove .mp3, .mov, .mp4, .avi, .mpg, .mpeg, .flac, .m4a, .flv, .ogg, .gif, .png, .jpg, and .jpeg.
7. **"Sudo ufw enable"** Allow any ports in the README
8. **"sysctl -n net.ipv4.tcp_syncookies"** stops bad cookies.
9. **"Sudo nano /etc/apt/sources.list"** Check for any bad sources
10. **"Sudo nano /etc/hosts"** Check for any redirects
11. **"Sudo crontab -e"** - check for anything in there, it might be malicious.
12. "**Sudo nano /etc/lightdm/lightdm.conf**" allow_guest=false. Then do "sudo service lightdm restart" (make sure you aren't doing any updates when you restart lightdm)
13. **Remove hacking tools.** Open Ubuntu Software center and look at recently installed software for "nmap", "ophcrack", or anything else that looks suspicious. If in doubt look up its name.
14. **Remove non-work related software**. Anything that looks like a game should be removed. If in doubt look it up. If you find a file called "passwords.txt" make sure to delete it.
15. **Go to terminal and "sudo apt-get update" and then "sudo apt-get upgrade" and "sudo apt-get dist-upgrade".** Let the apps update while you are doing other stuff.
    a. After Updates Complete:
        i. **"sudo restart lightdm"**This gives points for editing lightdm.conf
16. **"Sudo nano /etc/ssh/sshd_config"** PermitRootLogin to no. You might need to stop ssh, edit config, and restart. "Sudo service ssh restart"
17. **"Sudo nano /etc/pam.d/common-password"** Install "sudo apt-get install libpam-cracklib" and then add "password requisite pam_cracklib.so minlen=10" to the end of the file.
    a. **"Sudo nano /etc/pam.d/common-password"** Use ^W and look for "pam_unix.so" add "minlen=8" to the end of this line

18. **“Sudo apt-get install bum”** Use bum to look for bad services. Remove apache, nginx, bind9 (DNS), ssh, or FTP unless otherwise stated in the README. Type “sudo bum” to start bum.
19. **Disable samba** (unless readme says otherwise) using “Sudo service smbd stop” and “Sudo service samba stop” (also uninstall samba too)
20. **“Sudo nano /etc/login.defs”** change/add to:
    PASS_MAX_DAYS 90
    PASS_MIN_DAYS 7
    PASS_WARN_AGE 14
21. **“Sudo nano /etc/pam.d/common-auth”** Add “auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800” (all on one line) to the end of the file. This denies password attempts and adds a lockout period.
    a. **“Sudo nano /etc/pam.d/common-auth”** Use ^W to find “pam_tally2.so” add “deny=5 unlock_time=1800” to the end of the line. This denies password attempts and adds a lockout period.
22. **“Sudo visudo”** Make sure only the default account can sudo.
23. **Purge netcat**. Use sudo apt-get purge netcat nc netcat-* to purge all forms of netcat.
24. **Secure Ports.** Follow these steps:
    a. **`Sudo ss -ln | grep tcp`** This lists all open ports
    b. Look at the list of open ports and use **sudo lsof - i :<Port>** to get the program
    c. Determine if the port is a backdoor (if it has nc or netcat in the name it is a backdoor)
    d. Determine if the program is supposed to be on the computer
    e. These ports are safe: 22, 53, 631, 35509
25. **Correct file permissions**: Execute the following commands to put correct file permissions on important system files (with sudo):
    a. chmod -R 444 /var/log
    b. chmod 440 /etc/passwd
    c. chmod 440 /etc/shadow
    d. chmod 440 /etc/group
    e. chmod -R 444 /etc/ssh

Disable FTP services:
Bring up a terminal, and type “service --status-all” and press Enter
Type “sudo apt-get remove pure-ftpd” and press Enter. Type the password, and press enter. Hit yes, and enter.

Nmap is prohibited software. (If applicable) to remove:
In the terminal, type “sudo apt-get remove zenmap” or “sudo apt-get remove nmap” and press Enter. Type the password, hit enter, then say yes and hit enter.

Other malicious software:
“sudo apt-get remove ophcrack” This is a hacking tool.

Antivirus:
“sudo apt-get install clamtk” This installs an antivirus.

Do you hate the Ubuntu Software Center?
Use this terminal command to search installed packages: `sudo apt list --installed | grep <NAME>`

Do you love using the command line to install and remove stuff?
To install stuff: `sudo apt-get install <PACKAGE NAME>`
To remove stuff: `sudo apt-get remove <PACKAGE NAME>`

COMMANDS

Shortcuts:

- **Ctrl Alt T**
  - Opens a terminal window
- **ls**
  - Use the "ls" command to know what files are in the directory you are in.
  - **ls -a**
    - Hidden files in the directory
  - **ls -al**
    - Lists files and directories with detailed information like permissions,size, owner, etc.
- **cd**
  - A command that lets you move into a specific directory
  - **cd Downloads**
    - This command will move you into the Downloads folder
  - **cd ..**
    - Moves you up one level in the directory hierarchy
  - **cd /**
    - Moves you to the root directory
- **rm**
  - rm stands for remove and it allows you to remove files
  - **rm -r**
    - Removes an entire directory
- **man**
  - Pulls up a manual and description of user commands
  - **man cd**
    - Manual page for the cd command
- **--help**
  - **cd -help**
    - Explains and shows how the cd command can be used
- **locate**
  - This command shows you the directory for files
  - **locate -i**
    - Does the same thing however -i ignores case
- **cat**
  - Shows the content of a file
- **nano**
  - This is a text editor that allows you to change permissions to files
- **sudo**
  - Stands for SuperUser Do
  - This allows you to any command with administrative/root privileges
- **apt-get**
  - This command allows you to install packages and updates/upgrades

- **chmod**
    - Use **chmod** to make a file executable and to change the permissions granted to it in Linux.
- **grep**
    - It is used to search for a string of characters in a specified file
    - grep “string” “filename” (ignore the “”)
- **find**
    - Another tool for finding files
- ***
    - The asterisk is used as a wildcard, it is most helpful for looking for files of a certain extension type for example
        - **find / -iname “*.mp3”** will output all mp3 files in the root directory
- **clear**
    - Clears the directory
- **pwd**
    - Shows the current directory location

User management commands of linux

- **sudo adduser username**
    - Adds a new user
- **sudo passwd -l 'username'**
    - To change the password of a user

Dash commands:

- **-i**
    - Ignores case
- **/**
    - root
-

Sudo apt install net-tools

ifconfig