CyberPatriots Basic Linux Checklist

User Management:

Check users: cat /etc/passwd with the ones in README.

- To remove one sudo deluser ‘username’
- To add one sudo adduser ‘username’

Check sudo’s: getent group sudo with ones in README.

- To delete one from sudo sudo deluser ‘username’ sudo

Check/Fix bad admin passwords: (you can see them on README)

- To change someones password sudo passwd ‘username’
- (A safe password example: Blue-Tiger01!)

Fix user groups if said in the README:

- To see users in a specific group getent group ‘groupname’
- To add a user to a group sudo gpasswd -a ‘username’ ‘groupname’
- To remove a user from a group sudo gpasswd -d ‘username’ ‘groupname’

Disable Guest User:

- Check your display manager run: cat /etc/X11/default-display-manager
- If its lightdm run: sudo nano /etc/lightdm/lightdm.conf
- Add or switch allow-guest=false

- Restart(make sure you have saved your password somewhere and have no updates or processes running as you restart) sudo systemctl restart lightdm
- If its gdm3 run: sudo nano /etc/gdm3/custom.conf
- Add (under ‘daemon’) or switch AllowGuest=false
- Restart(make sure you have saved your password somewhere and have no updates or processes running as you restart) sudo systemctl restart gdm3

Updates:

- Check for updates daily: Software&Upfdates< Updates< Check Daily
- Update software: <Software updater> (this also updates firefox and thunderbird usually :)
- Some firefox settings:

Go firefox< settings< data and privacy< adjust whatever you think is safer… I recommend ; dont save log-ins, block pop-ups, warn when websites try install anything.

Add/configure firewall:

- Install firewall: sudo apt install gufw
- Edit firewall settings: gufw
- Reccomened settings: status-ON, Incoming-REJECT

Editing PAM files and policies:
Disable root login:

- Edit: sudo nano /etc/ssh/sshd_config
- Change permit root login yes to permit root login no Save the file.

Enforce password history/leght /and complexity requirements:

- Edit: sudo nano /etc/pam.d/common-password

- Add ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 to the line that has pam_pwquality.so or pam_ cracklib.so (idk why there is a link)
- Add remember=5 minlen=8 to the end of the line that has pam_unix.so

Save the file by <ctrlO> <enter> <ctrlX>

Enforce password duration rules:

- Edit: sudo nano /etc/login.defs
- Set:
- PASS_MAX_DAYS 90
- PASS_MIN_DAYS 10
- PASS_WARN_AGE 7

Save the file.

Set Account Lockout Policy:

Check which package is used in you computer by:

Run ls /lib/x86_64-linux-gnu/security/pam_faillock.so if some file comes up you use failock

Run ls /lib/x86_64-linux-gnu/security/pam_tally2.so if some file comes up you use tally2

Edit: sudo nano /etc/pam.d/common-auth

Add:

If you use failock: add auth required pam_faillock.so preauth audit deny=5 unlock_time=1800 to the top of the file

If you use tally2: add auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800 to the top of the file

Remove Unnecesary Applications:

- Remove the suspicious ones by sudo apt remove ‘name’
- If that wont work run sudo apt remove ‘name’ -y

Look for media files:

- locate '*.mp3' (you can do this with mp4, .mov , .avi …etc)
- Delete the files you find
  - To delete a single file sudo rm /path/to/file ‘fileName’
  - To delete many files in the same place sudo rm /path/to/files/*.mp3

Check Running Services (google them or ask chatgpt):

- To view them sudo systemctl list-units --type=service --state=running
- To stop them sudo systemctl stop ‘name’ and sudo systemctl disable ‘name’