Field Checklist:

This is a checklist for Ubuntu in Cyberpatriots:

First do the forensics questions.

Easy things:

* Make Firefox default browser.
* Make sure the Firefox security settings are set to the highest level of security.
* Update Firefox using sudo apt-get install Firefox
* Uninstall any suspicious apps or games:
  + CHECK THE UBUNTU MENU FOR ANY APPS
  + If unsure about any apps, google it
  + Use dpkg -l | grep “keyword” to find the package
* Enable the firewall, UFW. Use sudo ufw enable and sudo ufw status to check if the firewall is on.
* Disable root login for ssh

Moderate things:

* Check the users. Delete any unneeded accounts and add any important accounts.
  + Use userdel to delete users
  + Use deluser to remove users from groups
* Make sure the users have the proper permissions. This can be changed quite easily through the gui. You could check the sudoers file
* Disable the guest user
* Disable FTP.

Hard things:

* Use locates to find suspicious files. These files are often found in user’s home folders. Find can be used but it is recursive.
* Make sure all accounts are using strong passwords
  + Use the password given by the website

Sources:

[CyberPatriot\_Linux\_CheckList.pdf (lacapnm.org)](http://lacapnm.org/Cadets/STEM/CyberPatriot/SeasonVIII/CyberPatriot_Linux_CheckList.pdf)

[Forty-Bot/linux-checklist (github.com)](https://github.com/Forty-Bot/linux-checklist)