CyberPatriot Ubuntu 14.04 Toolkit

★ https://www.uscyberpatriot.org/competition/training-materials/training-modules

★ https://help.ubuntu.com/stable/ubuntu-help/prefs.html?_ga=2.29614591.1369854527.1510691524-341247159.1510691524

★ https://wiki.ubuntu.com/Security/Features

★ https://wiki.ubuntu.com/BasicSecurity

★ http://ubuntuhandbook.org/?s=passwordm

★ https://github.com/Forty-Bot/linux-checklist

★ http://r2d2.cochise.edu/guilmetted/CyberPatriot/Check%20List%20Session%20for%20Ubuntu%20Linux%20(20130919).pdf

★ http://mhs-cyberpatriot.wikia.com/wiki/General_Ubuntu_Checklist

★ http://www.lacapnm.org/Cadets/STEM/CyberPatriot/SeasonVIII/CyberPatriot_Linux_CheckList.pdf

★ https://www.reddit.com/r/cyberpatriot/comments/48x34x/400400_linux_checklist/

❑ **Forensic Question**

❑ **Penguin is Good!**

❑ **Change User to Administrator/Standard**

  ❑ Icon above files> search “user”>user accounts> select user> unlock> type in password> select Administrator/Standard> select ideal account type.

❑ **Delete a User**

  ❑ Icon above files> search “user”>user accounts> select user> unlock> type in password> select the - button at the bottom left of the window.

❑ **View User’s Files**

  ❑ Files> computer> home> select suspicious user> select any folder you want.

❑ **File Location/Pathway (Ex. User’s Unauthorized Media)**

  ❑ Files> computer> home> select user> select folder> hover mouse over the latest folder tab in the folder pathway> right click> copy> paste where you want it.

- ❑ **User’s ID**
    - ❑ Ctrl+Alt+T> type in “`sudo`”> type in “`id -u <username>`” (Ex. “`id -u Sam`)> User ID is the #### number (Ex. `1001`).
    - ❑ Guest Accounts
    - ❑ Remote Users
- ❑ **Change Password**
    - ❑ Icon above files> search “user”>user accounts> select user> unlock> type in password> select the dots next to password> fill out information> change.
    - ❑ Ctrl+Alt+T> type in “`sudo`”> type in “`passwd <username>`” (Ex. “`passwd Sam`) <u>don’t worry, it should look like you’re not typing in anything</u>> type in current password> press ENTER> type in new password> press ENTER> retype in new password> press ENTER.
- ❑ **Change Minimum Password Length**
    - ❑ Ctrl+Alt+T> type in “sudo”> type in “`sudo nano /etc/pam.d/common-password`”> type in user password (don’t worry, it should look like you’re not typing in anything)> find the line that says “`password     [success=1 default=ignore] pam_unix.so obscure sha512`”> Add “ `minlen=#`” to the end of the line (#=minimum password length AKA 8)> Ctrl+X> type “Y”> press ENTER.
    - ❑ ^remove the “`obscure`” to remove complexibility of the password.
- ❑ **Update Notification Policy**
    - ❑ Icon above files> search “soft”> Software & Updates> select updates> check “Important security updates” and “Recommended updates”> set DAILY for Automatically check for updates> set DISPLAY IMMEDIATELY for When there are security updates> set DISPLAY IMMEDIATELY for When there are other updates> set FOR LONG-TERM SUPPORT VERSIONS for Notify me of a new Ubuntu version> do NOT click revert> click close.
- ❑ **Update**

- ❑ **Firewall**
- ❑ **Antivirus**
- ❑ **Locked Out AKA Password Not Working (Might Work)**
  - ❑ Press `Ctrl+Alt+F1` and type in your username and password, then execute:
  - ❑ `sudo rm .Xauthority sudo reboot`

Notes From Mentor!

- Sudo is used to install and delete, as well as run commands
- Root is used to find things.
- Finding specific files: commands: “find” and “locate”. Command “pwd” (print wois used to find the path of a file.
- Locate*.pdf
- Update DB, then run locate!
- Man command (help button) example: locate man. If this doesn’t work, then use help.
- Check the Linux training.
- https://www.snort.org/ Used to stop network intrusion from a certain source
- WIRESHARK IS A-OK!!! Actually, USE WIRESHARK!!!!!!!!!!

Don’t even bother to wait for the update manager to pop up and remind you there are updates. Open the dash (either click on the Ubuntu logo icon in the upper left corner or click the Super key/Windows key on your keyboard), search for updates, and click the Software Updater launcher. When the updater runs (Figure 1, above), okay any updates that are available. Bug fixes tend to happen frequently soon after the release.

Unity 7 is a completely polished desktop now. If you still love GNOME, KDE, or one of their variations such as the GNOME-based Cinnamon you're not going to love **Unity**. There are, of course, versions of **Ubuntu 14.04** that use other desktops. These include: **Ubuntu** GNOME; Kubuntu with KDE, and Lubuntu with LXDE.

A GNOME is the equivalent of the windows start button.
IN GENERAL:
Take a look at the author
Look at website
Look for sources
Last updated time
Use http://whois.domaintools.com/

Ubuntu Checklist Cyberpatriot

Basic Security Checklist – Ubuntu Linux 12.04 Focus
READ THE SCENARIO, AND THEN READ THE SCENARIO AGAIN!
A more familiar Interface
o sudo apt-get install gnome-session-fallback Updates

o Applications > System Tools > Administration > Update Manager

o Enabling automatic security updates Update Manager -> Settings Firewall

o In Ubuntu all ports are blocked by default

o Default firewall – ufw (turned off by default) sudo ufw status sudo ufw enable/disable

o Firestarter for graphical interface (recommended) sudo apt-get install firestarter Preferences User Accounts

o Users & Groups

o Do not use root user (disabled by default) sudo passwd sudo passwd -l root

o Use sudo instead of root (/etc/sudoers) sudo visudo OR sudo gedit /etc/sudoers james ALL=(ALL) ALL sudo adduser user_name sudo

o Adding users sudo adduser username

o Deleting users sudo deluser username

o Removing world readable permissions to home directory sudo chmod 0750 /home/username

o Locking/Unlocking user sudo passwd -l username sudo passwd -u username

o Passwords Expiration sudo chage username sudo chage –l username Cyberpatriot VI Checklist (Ubuntu Linux 12.04) Page 2 Antivirus

o ClamTK (under Accessories) Uninstall Applications

o Applications → Ubuntu Software Center

o Installed Software section o Select application and click Remove Processes

o To see processes ps aux or top System Monitor o Know what default processes are (screenshot/snip) Logs

o Some of the logs

/var/log/messages : General log messages

/var/log/boot : System boot log

/var/log/debug : Debugging log messages

/var/log/auth.log : User login and authentication logs

/var/log/daemon.log

/var/log/kern.log

: Kernel log file o Viewing logs tail, more, cat, less, grep GNOME System Log Viewer

: Running services such as squid, ntpd and others log message to this file