**CyberPatriot Ubuntu Study Guide**

**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).

* Check for Guest Accounts and 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) don’t worry, it should look like you’re not typing in anything> 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 the Firewall and Antivirus**

**If 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

***Important Notes:***

● 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”

● 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

● 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.

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/

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

**Users & Groups**

* Do not use root user (disabled by default) sudo passwd sudo passwd -l root
* Use sudo instead of root (/etc/sudoers) sudo visudo
* Adding users sudo adduser username
* Deleting users sudo deluser username
* Removing world readable permissions to home directory sudo chmod 0750/home/username
* Locking/Unlocking user sudo passwd -l username sudo passwd -u username
* Passwords Expiration sudo chage username sudo chage –l username Cyberpatriot

**Extra Resources:**

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

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