UNIT 10

Ubuntu Security

Learning Objectives

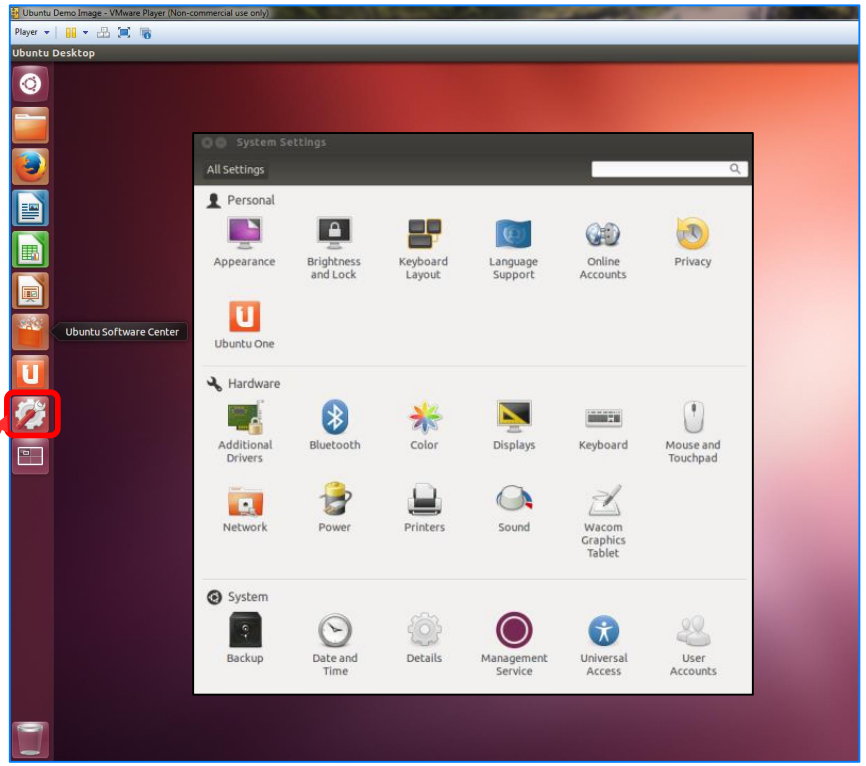
- Participants will understand how to configure major components of Linux/Ubuntu
  - Account management
  - Updates
  - Firewall
- Participants will understand how to implement user-level configurations within Ubuntu
  - Account settings
  - Group configuration
  - Authentication and the PAM file
- Participants will understand commands that will be useful for securing a Linux machine
- Participants will understand system and audit logging
  - Overview
  - Configuration

SECTION 1

Basic GUI Security

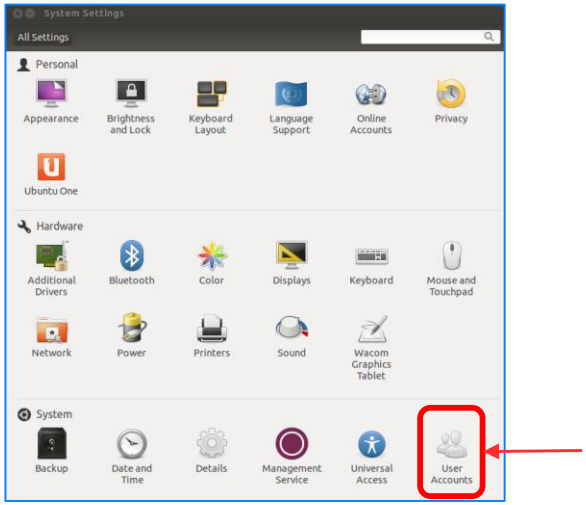
Basic Linux Security

- This unit will show you how to make many of the same security settings you made on Windows in Units 7 and 8
  - Linux has many of the same vulnerabilities, so the fixes are similar
- Linux does not have Settings or Control Panel like in Windows
- The System Settings menu offers limited security tools
- Click the System Settings button in the menu bar

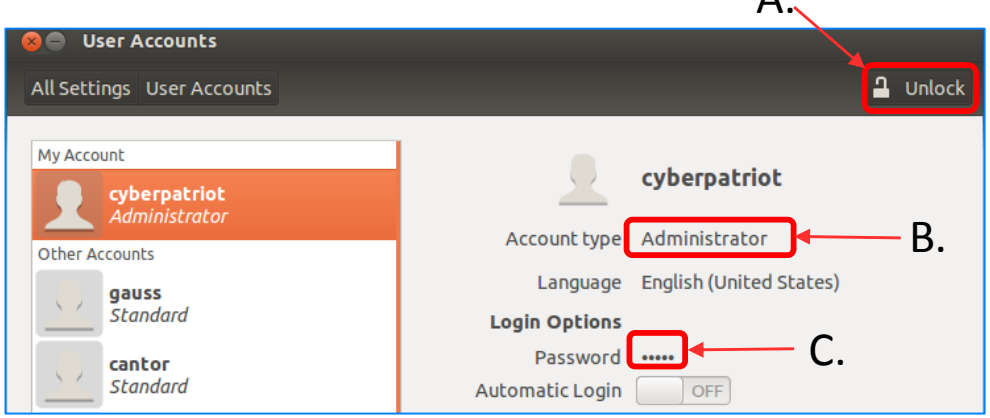


User Accounts Overview

1.



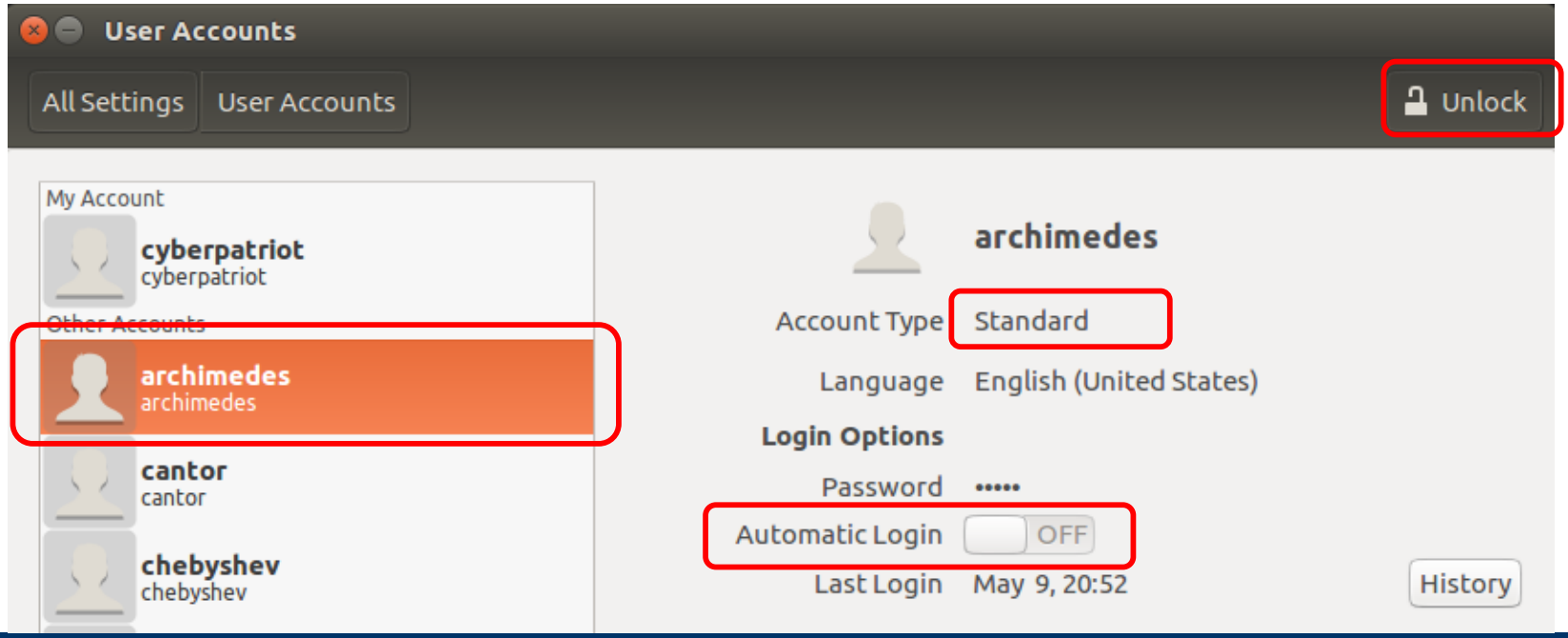
2.



- Click User Accounts in the System Settings window
- As in Windows, it is important to restrict root (Admin) privileges and password protect all accounts
  - A. To make account management changes, you must enact root permissions by clicking Unlock and authenticate yourself by entering your password
  - B. Switch users from Administrator to Standard User by clicking next to Account Type
  - C. Change passwords by clicking the asterisks next to the Password option

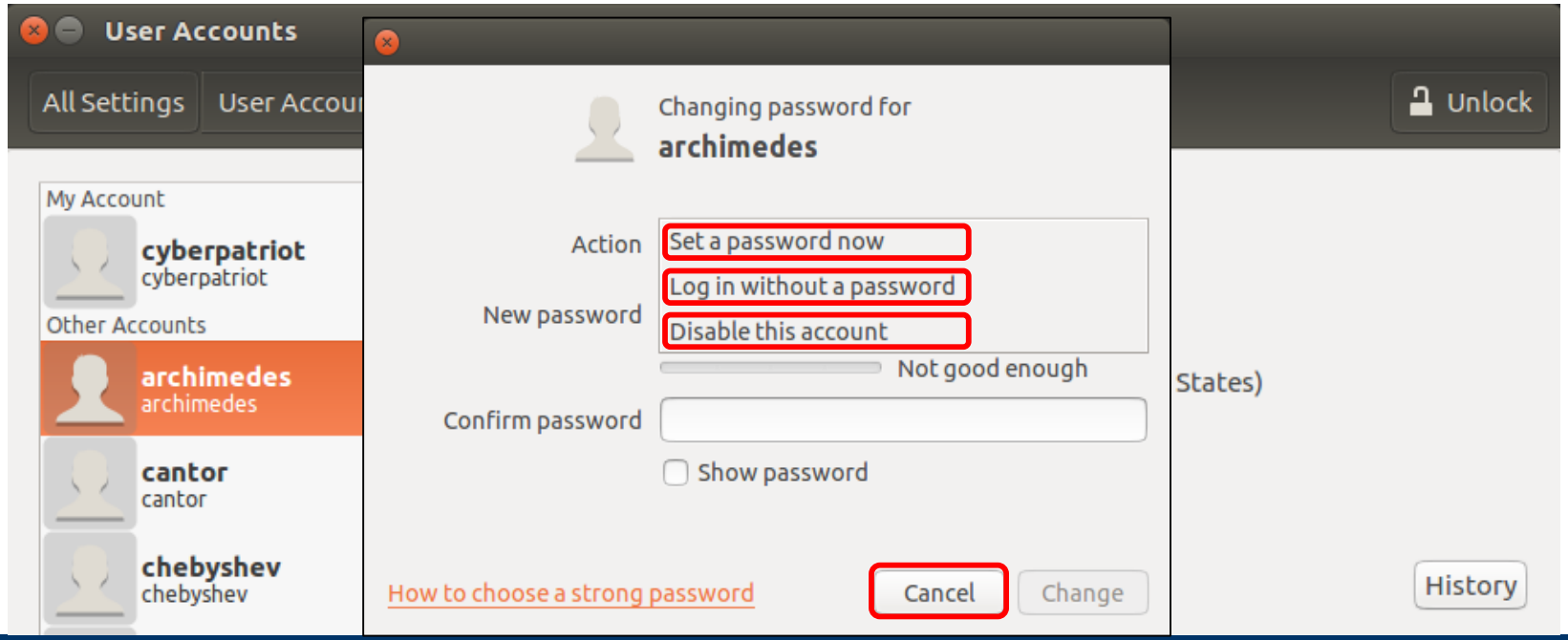
User Accounts – Account Type

- Select the user **archimedes**
- To make changes, click **Unlock** and authenticate
- Keep **Automatic Login** set to off
- The user account type can be changed by clicking the field next to **Account Type**



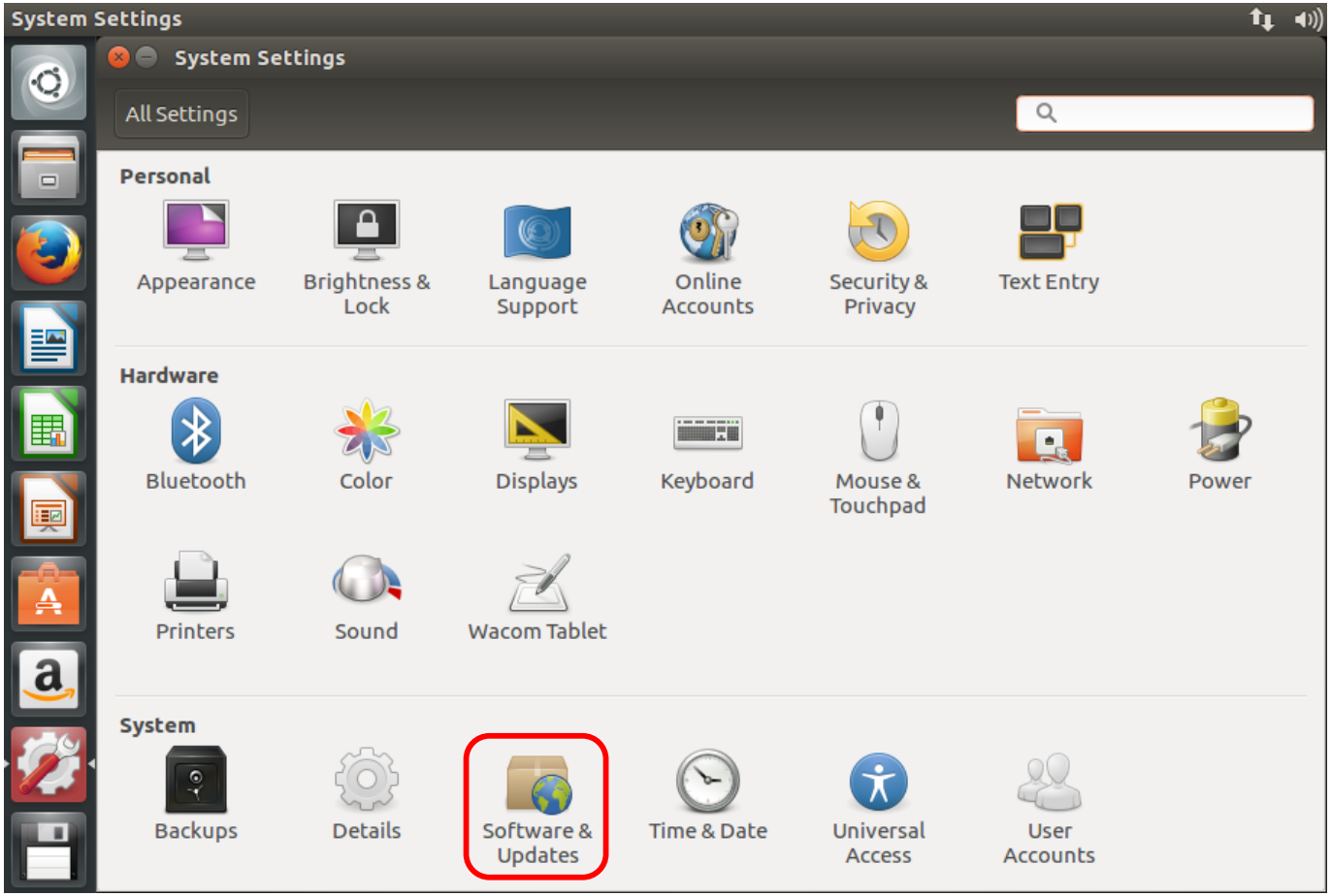
User Account -- Passwords

- Click the field next to **Password**
  - **Set a password now** allows you to change a user's password
  - Do not select **Log in without a password**
  - The third option allows you to disable or enable an account
- Press **Cancel** to return to the **User Accounts** windows



Configuring Updates

- Click **Software & Updates** in the System Settings window

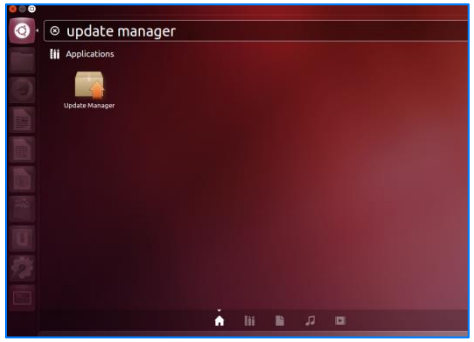


Installing Updates Overview

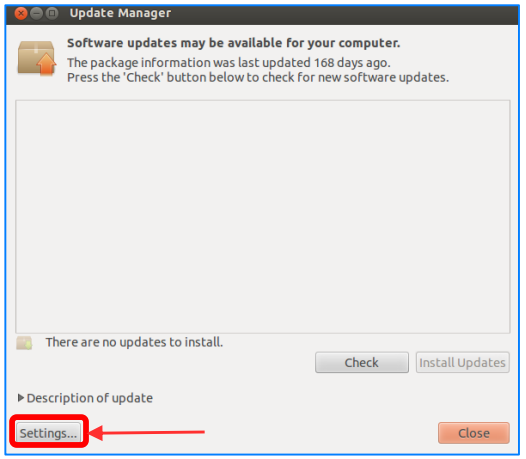
- The open-source community regularly develops improvements and patches for Ubuntu
- You should install these updates regularly

1. Click the Ubuntu button in the menu bar and search for Update Manager
2. Click Settings on the Update Manager Screen
3. To set automatic updates, go to the Updates Tab and make sure “Automatically check for updates” is set to “Daily”
4. After applying the changes, install any available updates from the main Update Manager window

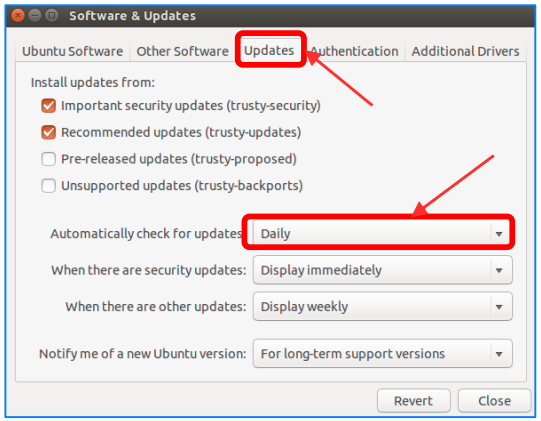
1.



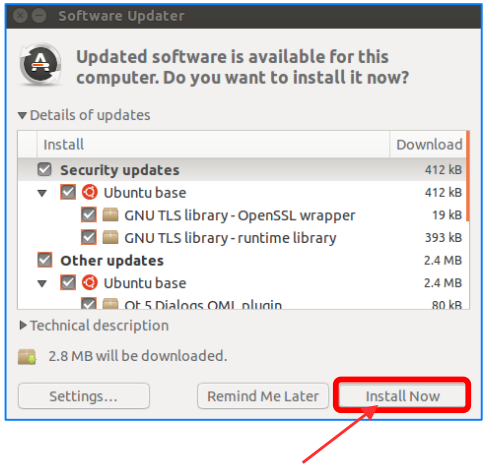
2.



3.

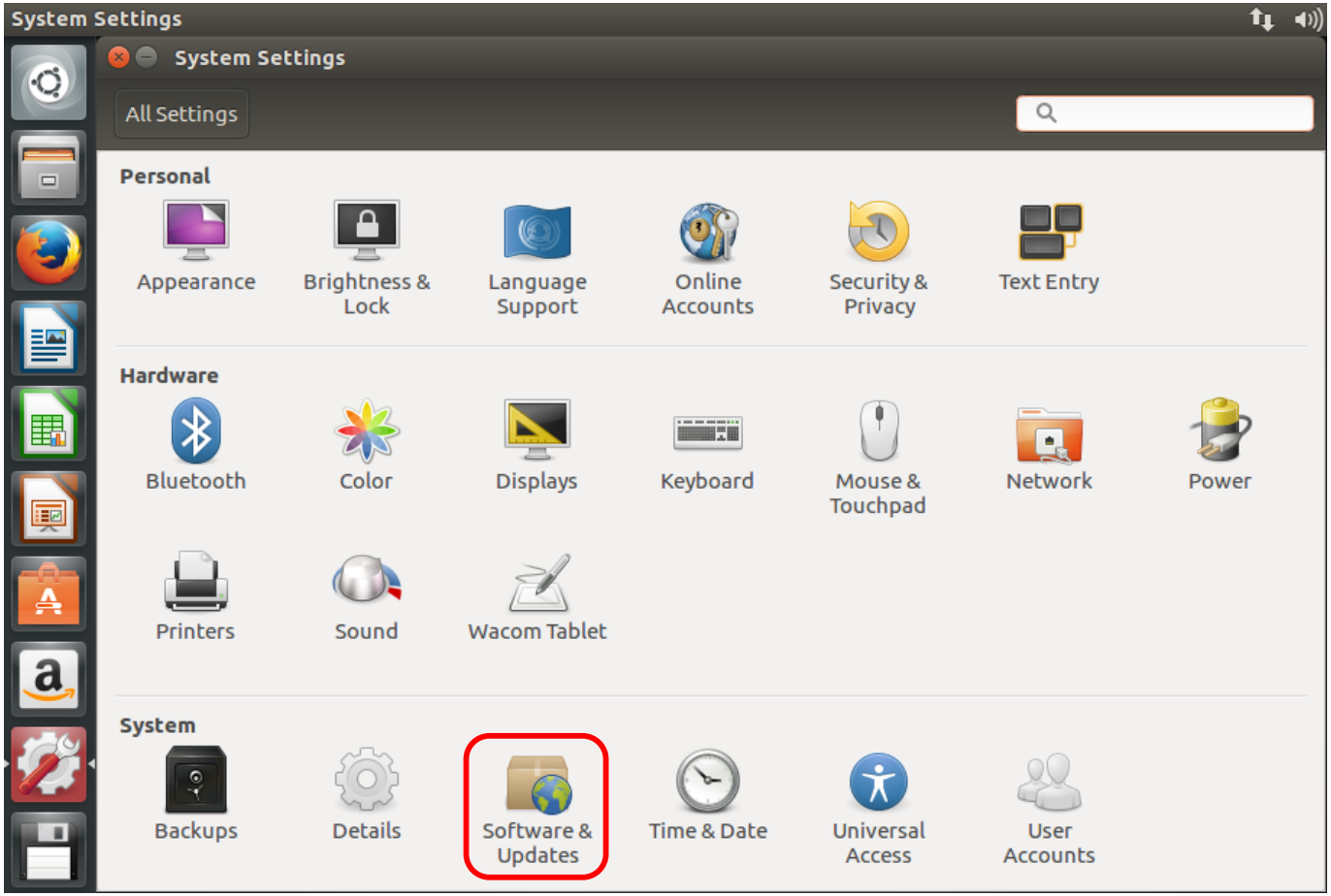


4.



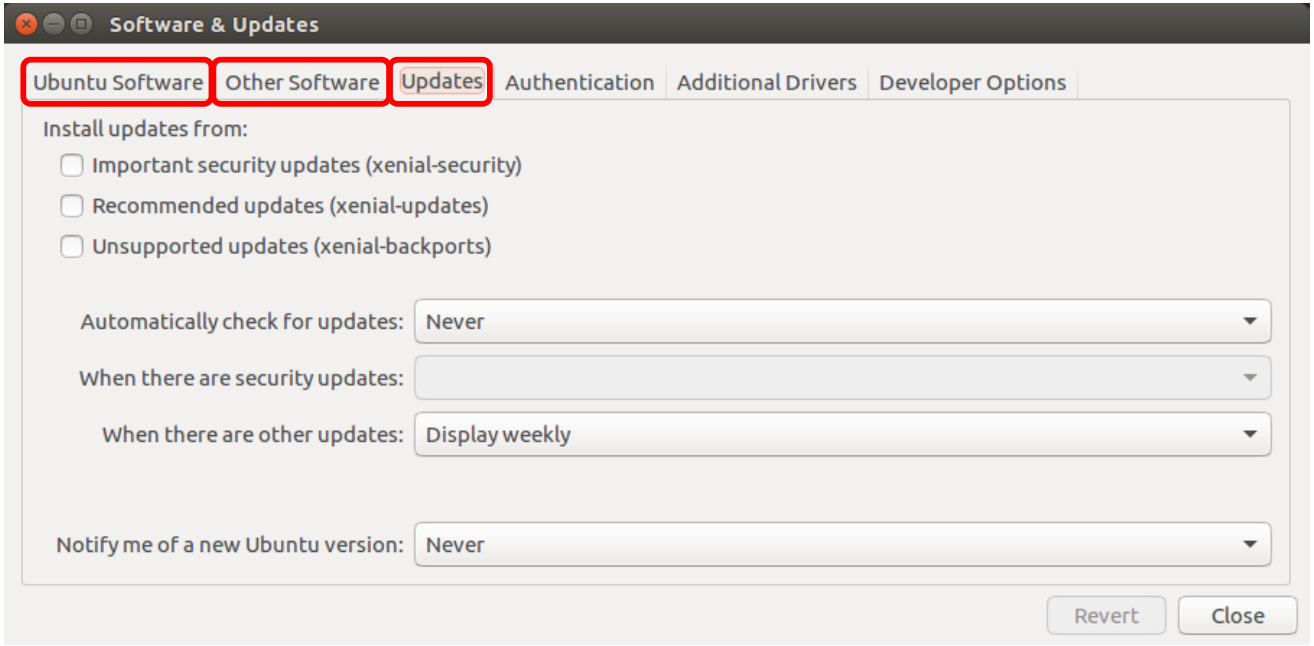
Configuring Updates

- Click **Software & Updates** in the System Settings window



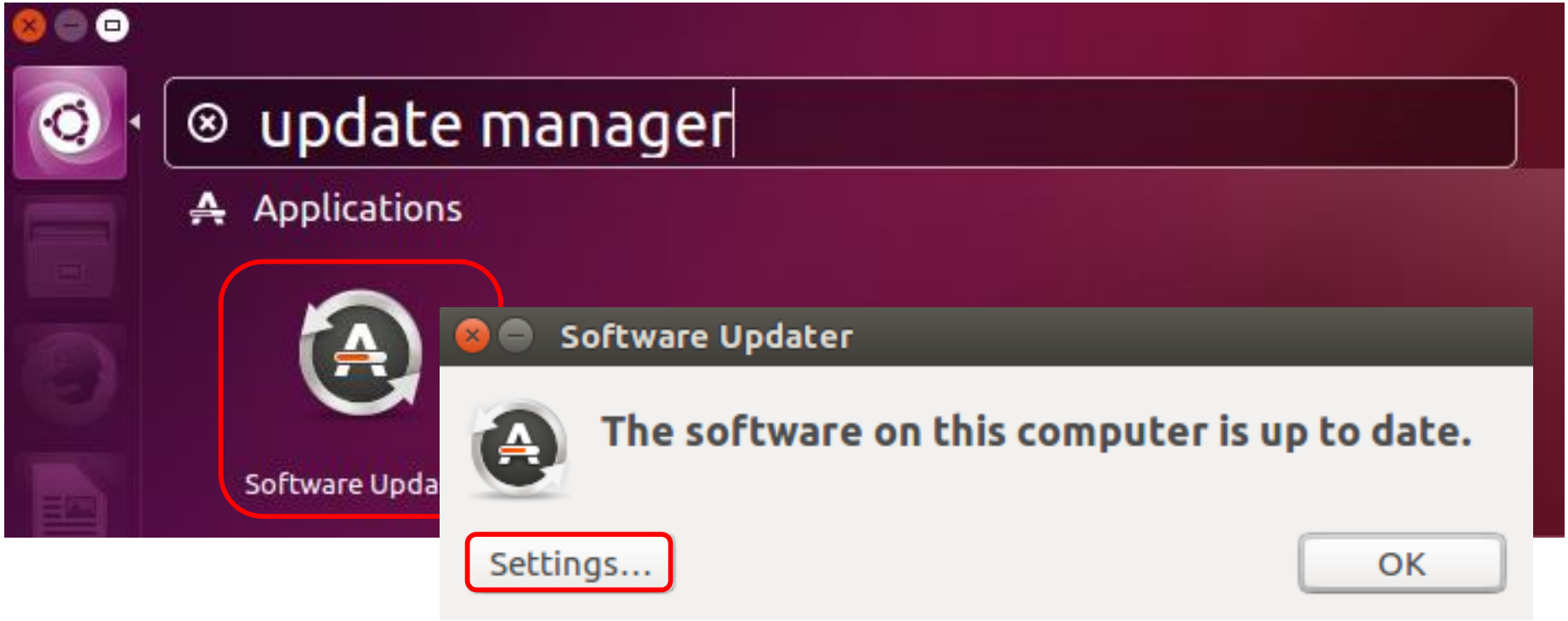
Update Policy

- Three Important Tabs
  - Ubuntu Software
  - Other Software
  - Updates



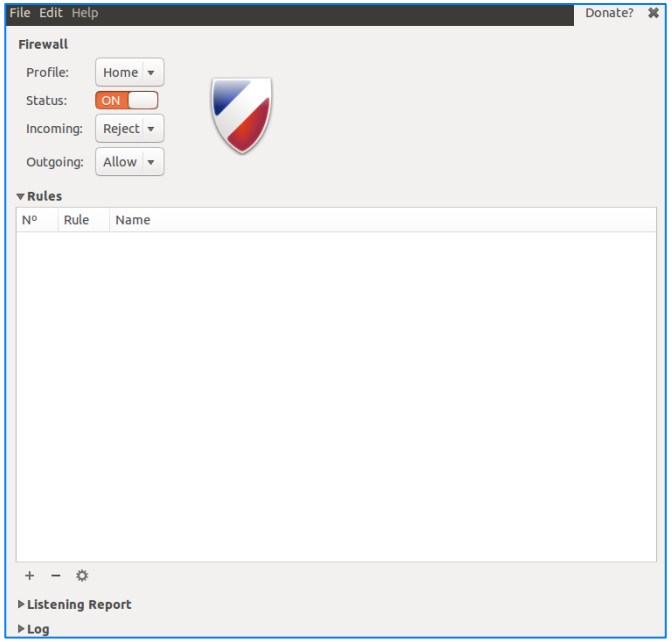
Installing Updates

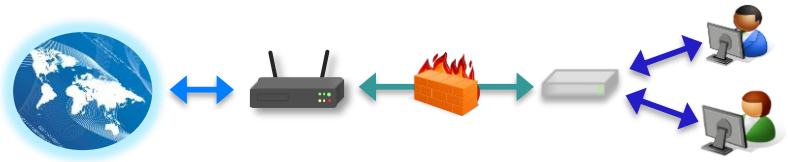
- Click the Ubuntu button in the left-hand menu and search for Update Manager



Enabling the Firewall

- Enable the Ubuntu Built-in Firewall (UFW) to prevent unauthorized access to the computer
  - The UFW is deactivated by default
- By default, UFW is only accessible by command line
- You can download Gufw, a graphical firewall interface, from the Software Center and use it to make changes to the UFW in the GUI
  - You might need to install Ubuntu updates before installing Gufw

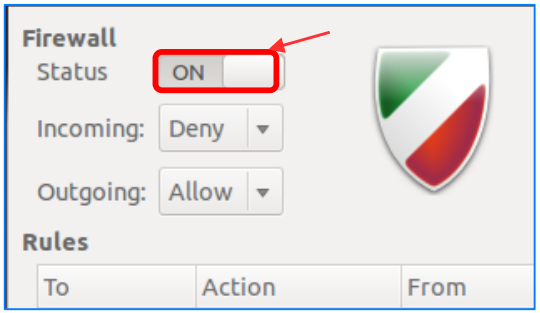




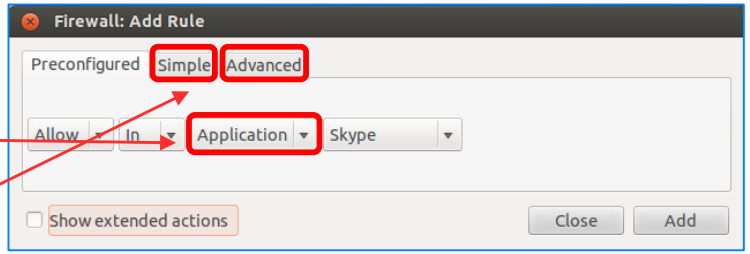
Source: https://help.ubuntu.com/community/UFW

Using Gufw

- After downloading Gufw from the Software Center, click the Ubuntu button in your menu bar → Search → Firewall Configuration
- Click the Unlock button on the Gufw window → Enact root permissions by authenticating → Turn Firewall Status On
- The default (and recommended) rules governing traffic are to Deny all incoming traffic and Allow all outgoing traffic
- The Reject option is the same as Deny, but also sends a notification to the sender that connection has been blocked



- The Preconfigured rule panel allows incoming and/or outgoing traffic to be controlled for certain applications or services
  - Similar to the Windows Firewall Exceptions list
  - Open entire ports by clicking the Simple or Advanced tabs



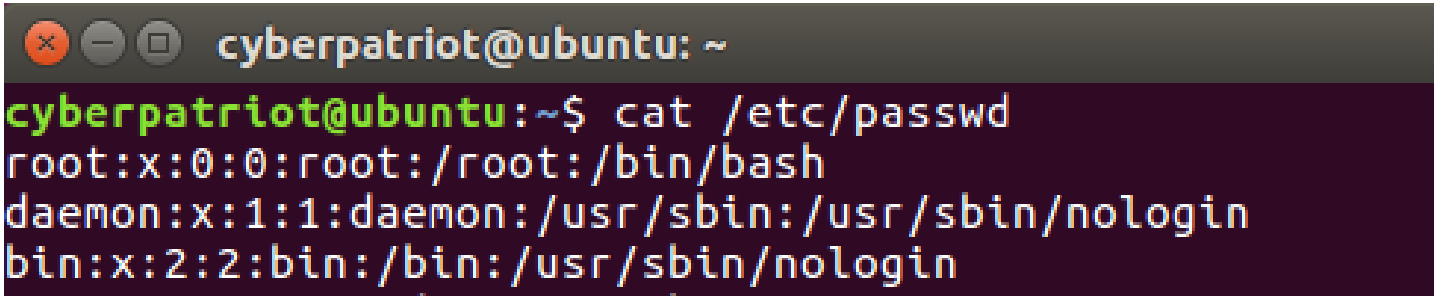
Source: https://help.ubuntu.com/community/Gufw

SECTION 2

Basic Command Line Security

The Password file

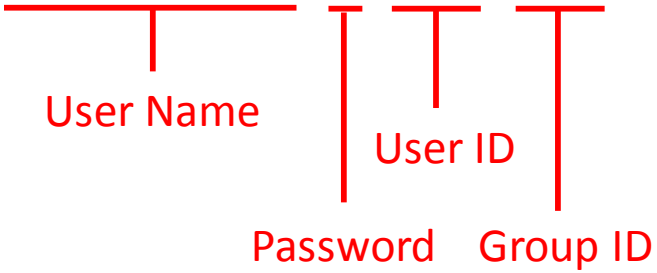
- /etc/passwd
  - Usually does not contain passwords (anymore)
  - Contains user information
- Type `cat /etc/passwd`



- Type `man 5 passwd` to view the manual for the password file
  - When you are done, press `q` to quit

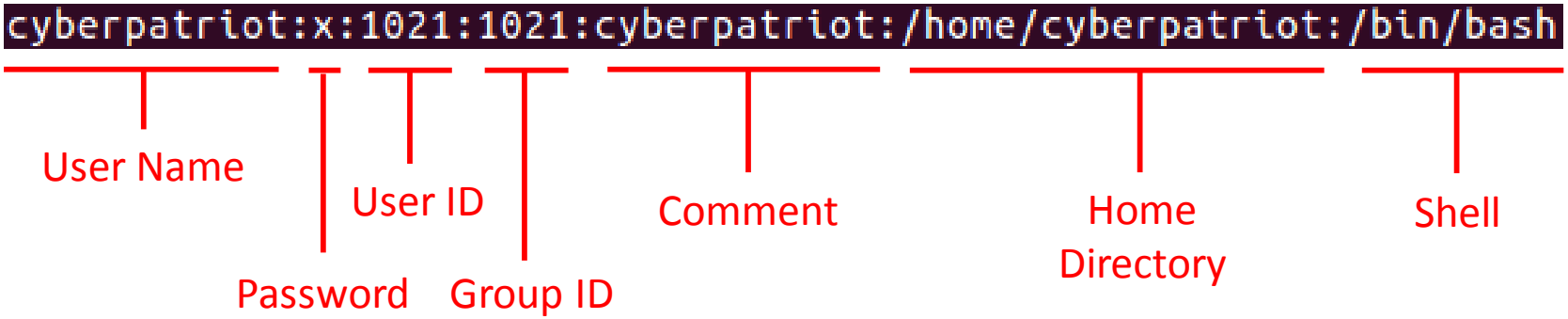
The Password File

```
cyberpatriot:x:1021:1021:cyberpatriot:/home/cyberpatriot:/bin/bash
```



- User Name
  - The name associated with this user account
  - This is primarily used by humans to identify a user account
- Password
  - x denotes password is stored in shadow file
- User ID – Numerical user ID, or “UID”
  - The OS internally identifies users using their UID not Username
- Group ID – Numerical primary group ID, or “GID”

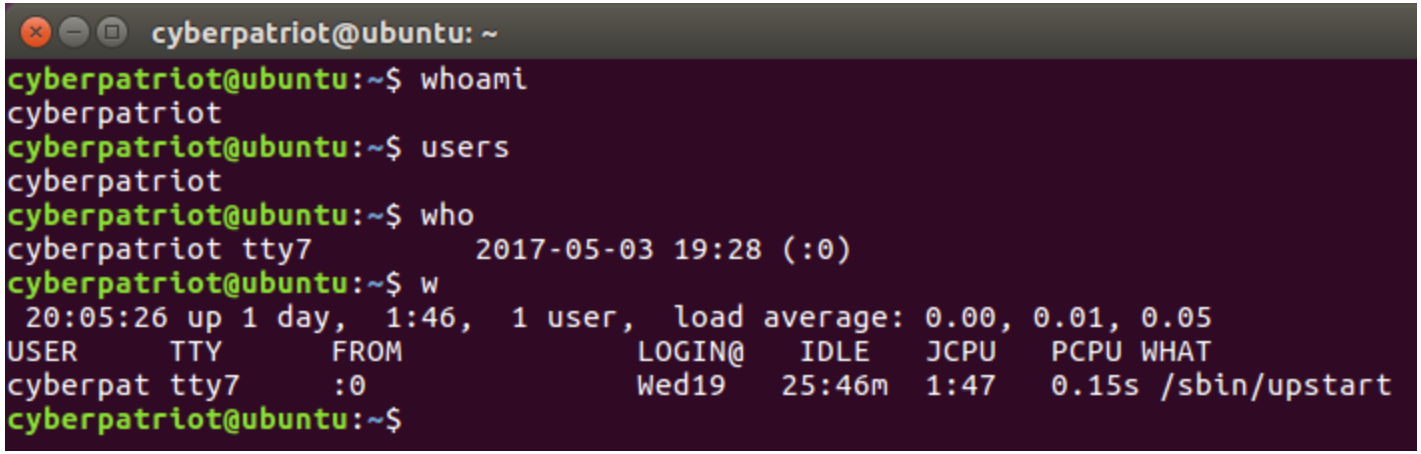
The Password File



- Comment
  - Typically used to store the users “real name”
- Home Directory
  - The current working directory when this user log in
- Shell
  - The shell (or command) that gets executed when you log in
  - How this user interacts with the computer when logging in on the command line

Listing Users

- Try running the following commands in the terminal:
  - whoami
    - Prints your current username
  - users
    - Prints the user names of users currently logged in to the current host
  - who
    - Prints information about users who are currently logged in
  - w
    - Displays information about the users currently on the machine, and their processes



The gedit Command

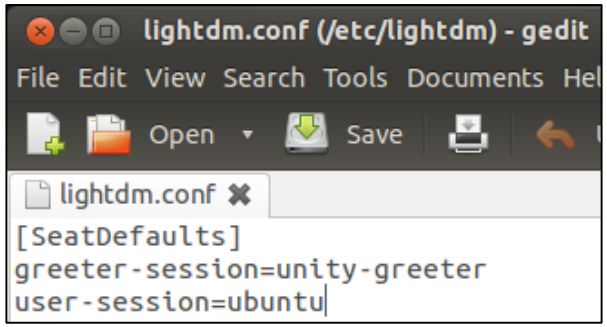
- Gedit is one of many text editor commands in Ubuntu
  - Syntax: gedit [filepath]
  - Unlike with other text editors, using gedit will cause a second window to pop-up where you can easily change the text of a file
  - This command will allow you to edit security policy files
- You need to enact root permissions before using gedit to edit files that cannot be accessed by standard users (e.g. system and security files)
- When using gedit for the first time, go to Edit → Preferences → Uncheck "Create a backup copy of files" to avoid saving issues
- Try using gedit by opening Terminal and entering gedit hello2.txt
  - You will not be prompted to authenticate because this is a public file

Using gedit to Turn off the Guest Account

- Like in Windows, the Ubuntu guest account is turned on by default
  - You should disable it so people can't access the computer anonymously
- The guest account is controlled by LightDM, the display manager controlling the Ubuntu login screen
- To turn off the guest account, edit the LightDM file:
  - After root authenticating, type `gedit /etc/lightdm/lightdm.conf`

```
root@ubuntu:/home/cyberpatriot# gedit /etc/lightdm/lightdm.conf
```

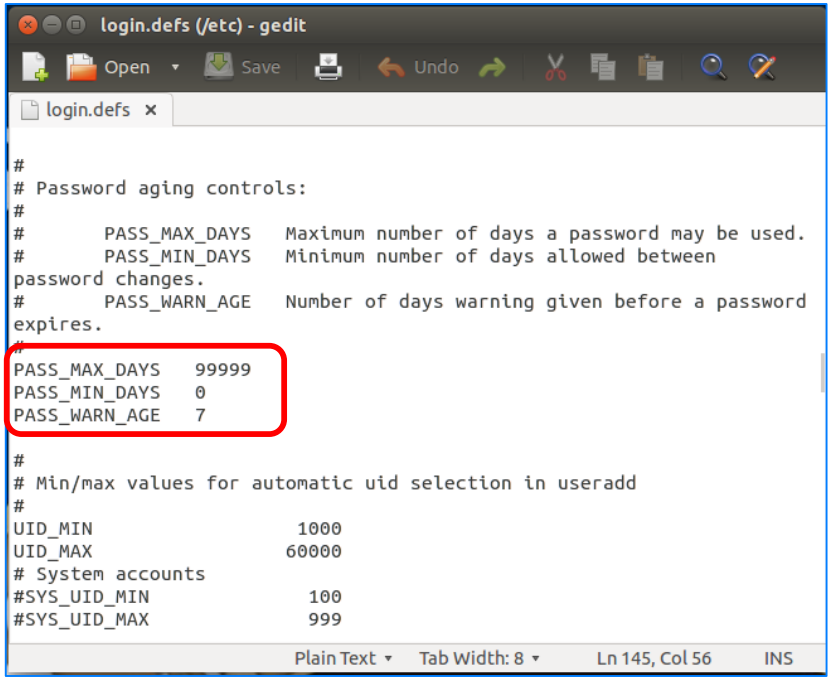
  - Add the line `allow-guest=false` to the end of the Light DM file that pops up and click Save
  - Restart your system and click your username button in the top-right corner of your desktop. The guest account should be disabled.



Sources: https://help.ubuntu.com/8.04/serverguide/C/user-management.html, http://askubuntu.com/questions/451526/removing-guest-session-at-login-in-ubuntu-14-04

Using gedit to Edit Password History

- Type `gedit /etc/login.defs`
- This is a much longer file. To easily find the section to edit, `type Ctrl+F and then "PASS_MAX_AGE"`
- Modify the following variables to the same recommended settings used in Windows:
  - Maximum Password Duration:
    - PASS_MAX_DAYS 90
  - Minimum Password Duration:
    - PASS_MIN_DAYS 10
  - Days Before Expiration to Warn Users to Change Their Password:
    - PASS_WARN_AGE 7
- Save the file and close it



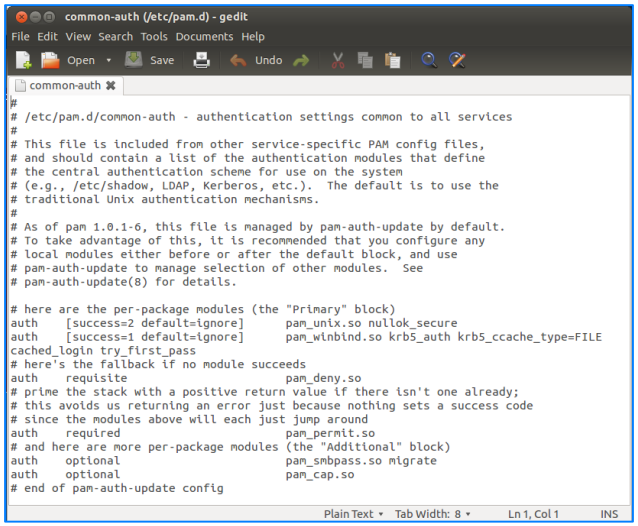
Sources: http://xmodulo.com/2013/12/set-password-policy-linux.html,

Using gedit to Set Account Policy

- Type `gedit /etc/pam.d/common-auth`
- This file allows you to set an account lockout policy
- Add this line to the end of the file:

```
auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800
```

- Save the file and close it



Sets the number of allowed failed login attempts (in this case 5)

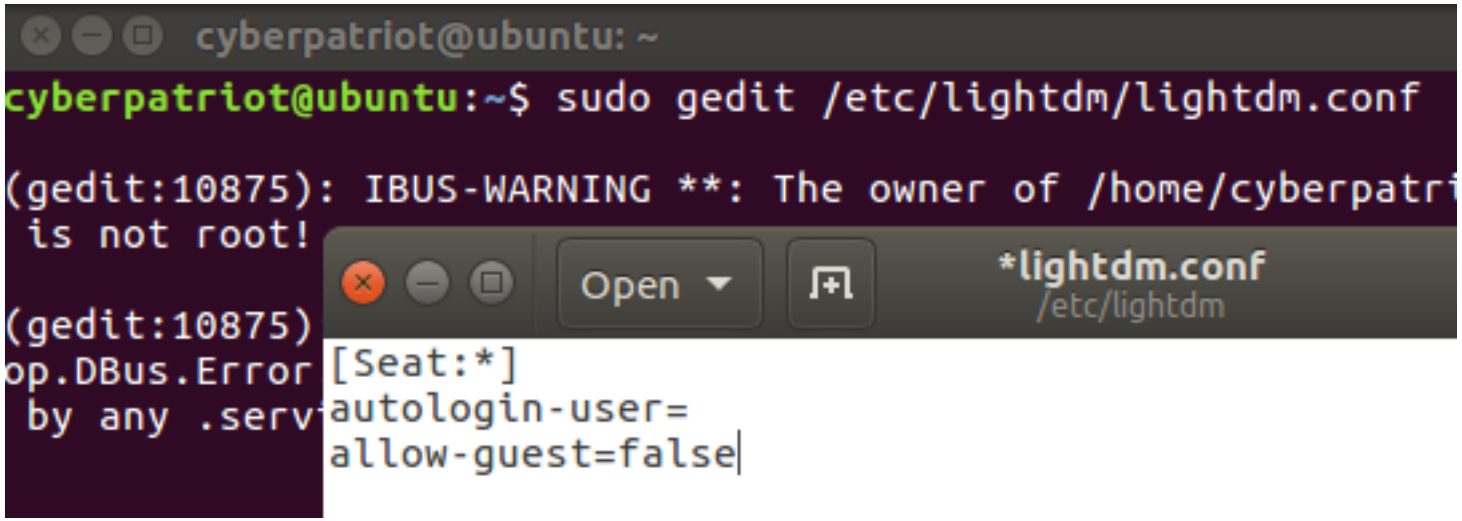
Sets the account lockout duration in seconds (in this case, 30 minutes)

Source: http://linux.die.net/man/8/pam_tally

SECTION 3
Advanced Ubuntu Security

Turn off the Guest Account

- Turned on by default
- LightDM: display manager controlling the login screen
- Type `sudo gedit /etc/lightdm/lightdm.conf`
- Add the line `allow-guest=false` under `[Seat:*]`



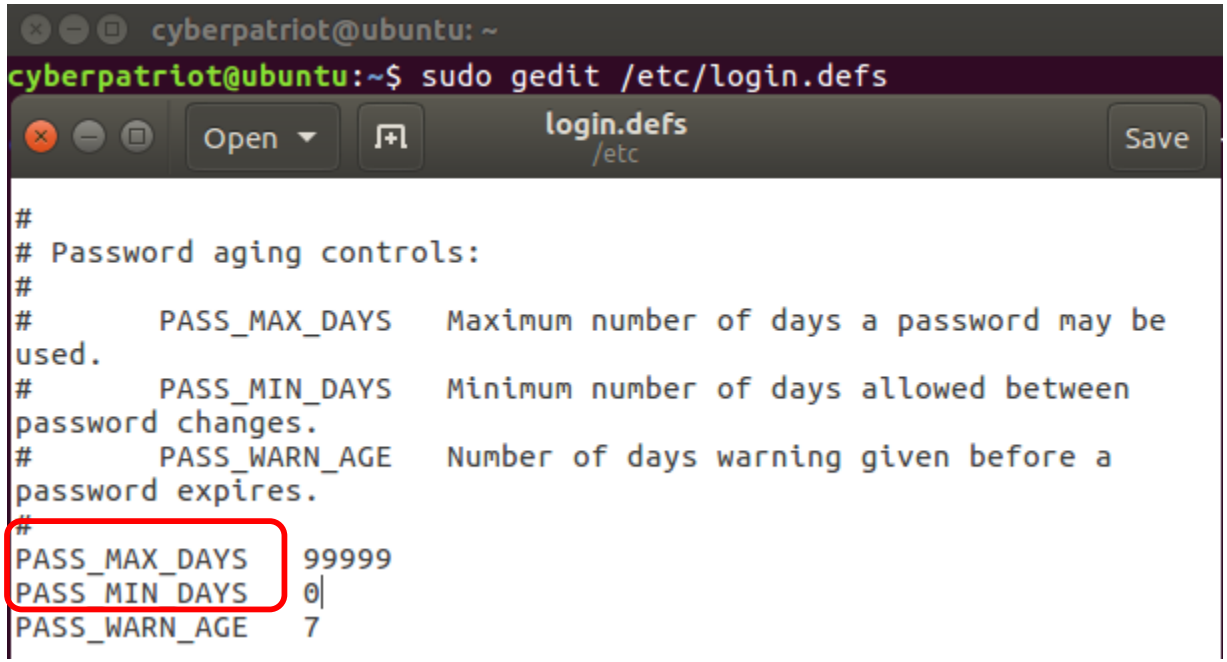
Password Age Policy

- In a terminal, type sudo gedit /etc/login.defs

Maximum Password Duration: PASS_MAX_DAYS 90

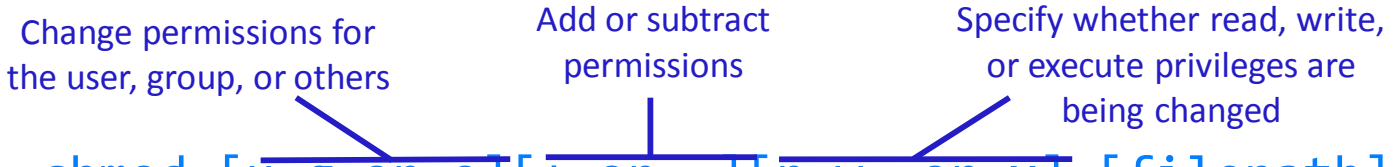
Minimum Password Duration: PASS_MIN_DAYS 5

Password Warning Before Expiration: PASS_WARN_AGE 7



The chmod Command

- Chmod allows you to change file permissions



  - Do not put spaces between the three fields after "chmod"
- Example:
  1. Type `chmod o-r hello2.txt`
  2. Type `ls -l hello2.txt`
  3. If your permissions originally matched those on the last slide, you should see hello2.txt's new file permissions as shown below

```
cyberpatriot@ubuntu:~$ ls -l hello2.txt
-rw-rw---- 1 cyberpatriot cybercamp 57 May 29 09:34 hello.txt
```

Sources: http://condor.depaul.edu/dpowebpg/support/chmod.html, https://help.ubuntu.com/community/FilePermissions

Groups

- Work very similarly to Windows
  - Root permissions are required

1. To list all groups:

```
cat /etc/group
```

2. To add a group:

```
addgroup [groupname]
```

3. To add a user to a group:

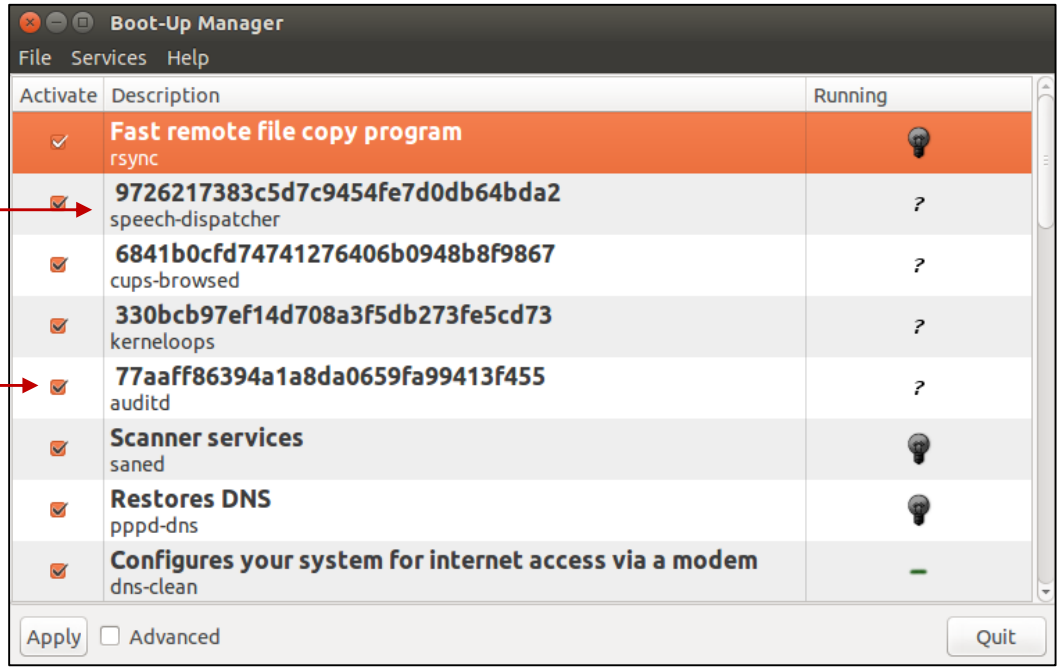
```
adduser [username] [groupname]
```

Services

- Can be viewed and managed in the GUI
- To install, type `apt-get install bum in` Terminal
- After installing, type `bum` to run

To start a service, right-click it and select “Start”

To enable a service, check the box next to it



When a service is started, the light bulb will light up. When stopped, the light bulb will be dark.