9/16/2020

Basic Ubuntu Security

Attack Plan for Training Round

Written by: Noah Sedlik
MIRA COSTA CYBERSECURITY CLUB 2020-21

Please note: It is easy to get stuck into the cycle of simply following the instructions without internalizing what is going on. **The goal is to get this process ingrained into your head** so you don't have to reference this guide. *Please* try to understand **how** and **why** we ask you to do the following steps. You'll find it more rewarding and will be able to pick up advanced concepts much more quickly.

Good Luck!
Dave Jha
Co-Founder and President, Cyber Security Program (2016-2018)

Additional note: this is a basic Ubuntu attack plan to introduce Ubuntu security for those who do not have much experience. If you already know much of this material, good for you! There will be more advanced concepts coming soon for our future meetings :)

- Noah Sedlik

`Also, if you find an error or have feedback, please let me know! Thank you!`

Contents

Before you Start 3
Pre-Competition 3
Competition time 3
Prerequisite Knowledge 3
What is Linux? 3
File Structure 4
Command Line Basics 5
Basic Terminal Commands 6
Editing text files 7
SUDO 8
Man pages 8
Competition 9
Forensics Questions 9
Checksums 9
Locating Files 9
User IDs 9
Groups 10
User Accounts 10
Password Policy 11
Local Security Policy 11
Disabling Guest Account 11
Programs and Services 12
Firewall Configuration 12
Problematic Services / Prohibited Software / Media Files 13
Adding / Removing / Updating Programs 13
Common Malicious Programs ..... **Error! Bookmark not defined.**
Automatic Updates 1
Software Updates 1
Browser Security 1
Prohibited Media Files 2

Before you Start

Pre-Competition

1) Make sure the proper versions of 7-Zip, WinMD5, and VMware Workstation Player are installed
2) Download and transfer images to all computers
3) Have team Unique ID and extraction password ready
4) Ensure there is enough storage in the hard drive

Competition time

1) Give the VM enough RAM (4 GB is sufficient)
2) Enter the Unique Identifier
3) Record changes and points earned during the competition (helps if you need to restart the image)

A recommended order for securing a computer:

1) README FIRST!!!!!!
2) **Forensics questions***
3) User Accounts
4) Password Policy
5) Local Security Policy
6) Enable / Disable Services
7) Enable Automatic Updates
8) Update Software
9) Configure Browser Security
10) Remove Prohibited Software / Media Files
11) Update OS

*** ALWAYS complete forensics questions before altering the computer because you may be unable to complete them otherwise**

Prerequisite Knowledge

This section outlines some basic information that will be helpful to know before diving into the competition. If you have experience with Ubuntu in the past, this may be repeat information and you can move on to the next section.

What is Linux?

From the wiki page:

> Linux is a family of open source Unix-like operating systems based on the Linux kernel, an operating system kernel first released on September 17, 1991, by Linus Torvalds. Linux is typically packaged in a Linux distribution.

Essentially, Linux is a family of operating systems like Windows or MacOS, except that the code is open-source, meaning that anyone can read the code. The open-source-ness also allows anyone to make their own code, leading to different “distributions” or “flavors” of the operating system. These “flavors” have

been created by people who need an OS with a specific purpose. In our case, we are using the **Ubuntu** flavor which was developed by Canonical, and is intended primarily for personal computers or servers.

File Structure

Filesystem Hierarchy Standard

In Windows, there are generally a few important folders like `C:\`, `Program Files`, `Users`, etc.

In Linux, however, there are many more directories, each containing files related to the parent directory's purpose. A visual representation is below for those curious:

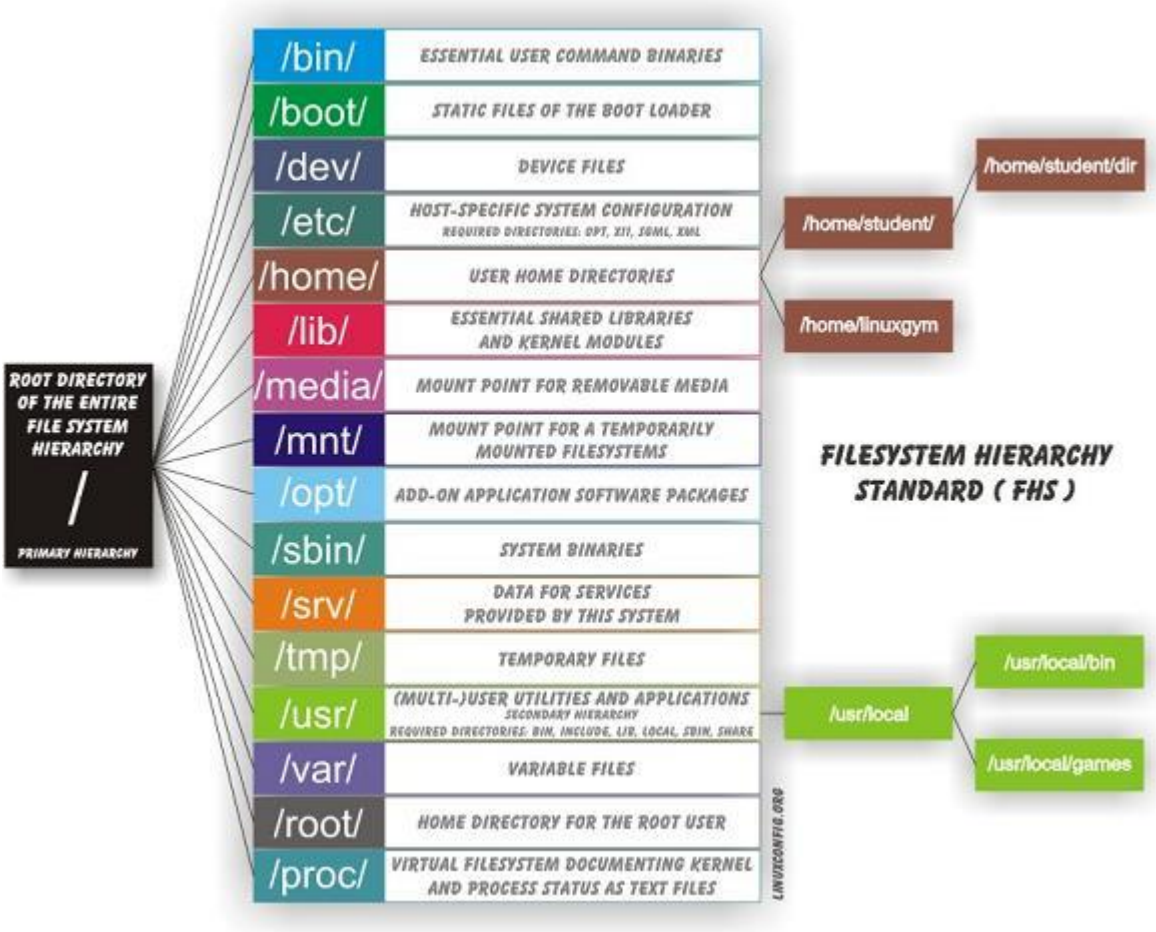


Image from: https://askubuntu.com/questions/138547/how-to-understand-the-ubuntu-file-system-layout

If you want to read more, check out the Linux Filesystem Hierarchy Standard (FHS)

Note: The directory of the entire file system is the **Root directory**. Every other directory is nested under the **root directory**.

Generally, you do not need to remember the purpose of each of these filesystems. For CyberPatriot, however, it was worth remembering the most important directories which you will access most often: `/home/` and `/etc/`

/home/ contains the directories of all users

/etc/ contains the directories and files of system configuration files

Important note: CyberPatriot's scoring engine is located under the **/opt/** directory. Generally, the competition will not ask you to make changes within that directory, and doing so may break the scoring engine.

File Paths

A file path is the term for the location of a file on a computer. Windows uses backslashes while Linux uses forward slashes.

For example: a file located on the desktop called document.txt will have the path:

Windows: C:\Users\noah\Desktop\document.txt

The file path says to retrieve the document in:

1) C drive
2) Users folder
3) Noah folder
4) Desktop folder
5) File named document.txt

Ubuntu: /home/noah/Desktop/document.txt

Likewise, the file path says to retrieve the document in:

1) root directory (indicated by the initial forward slash highlighted in green)
2) home directory
3) noah directory
4) Desktop directory
5) File named document.txt

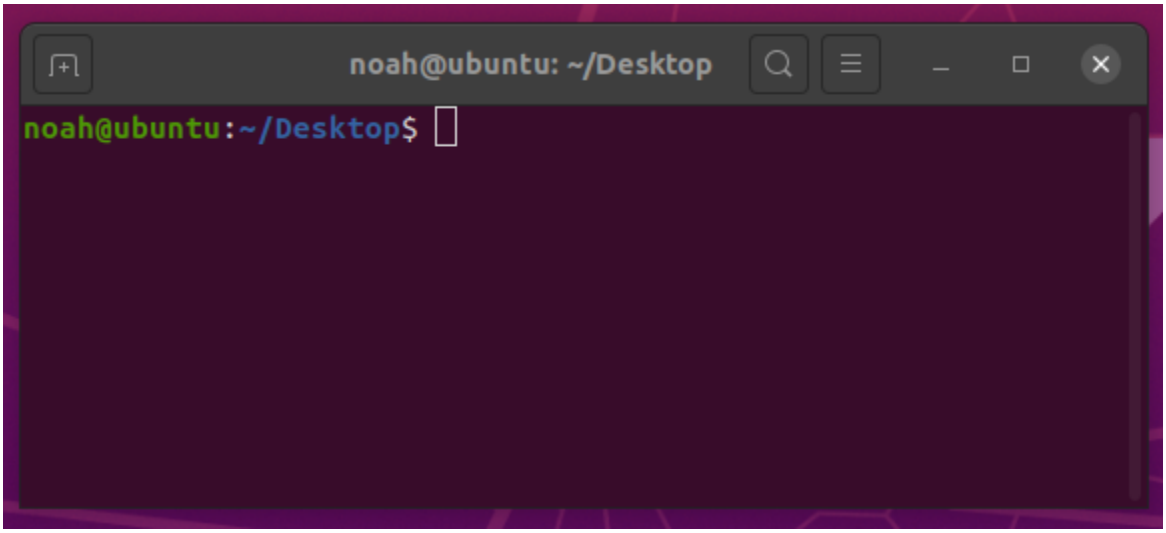
Changing directories can be done in the command line using the `CD` command which is covered in the section labeled Basic Terminal Commands

Command Line Basics

In Windows and MacOS, almost all tasks are done with a **Graphical User Interface (GUI)**. A GUI is a program that allows users to visually interact with the computer. On the other hand, a **Command Line Interface (CLI)** is very prevalent in Linux operating systems because most tasks are accomplished easier and far more efficient.

Unlike Windows (which has control panel, registry editor, etc.), many programs in a Linux system are configured by running commands or editing configuration files. Thus, it is important to practice using the command line to get comfortable working with a **CLI**.

Access the CLI: The command line in Ubuntu is accessed via the **Terminal** window. Right click on the Ubuntu desktop and click "Open Terminal." You can also press the Windows key to bring up the search menu and search for "Terminal."



This will bring up a terminal window that will look similar to this.

noah: the current user

@ubuntu: the name of the system (in this case, ubuntu)

:~/Desktop: this shows the current directory. The tilde **~** is shorthand for `/home/noah/` aka the user's home directory. Therefore, actual directory is `/home/noah/Desktop`

You enter commands into the terminal by typing the command and pressing enter. Luckily, it is not too scary and gets easier with practice.

Basic Terminal Commands

ls

`ls` stands for "list," and lists all the files in your current directory.

```
noah@ubuntu:~/Desktop$ ls
file.txt     pictures     media.mp3     music.wav
```

`ls` tells us that there are 3 files (and 1 directory, see below) in the **~/Desktop** directory: `file.txt`, **`pictures`**, `media.mp3`, and `music.wav`

cd

In the above example, notice how there is no file extension for **`pictures`**. This means that **`pictures`** is a directory (aka folder) located within the Desktop directory. Thus, we can move from **~/Desktop** to **~/Desktop/pictures** with the `cd` command

CD, short for change directory, allows you to specify a folder to move into.

```
noah@ubuntu:~/Desktop$ ls
file.txt     pictures     media.mp3     music.wav

noah@ubuntu:~/Desktop$ cd pictures

noah@ubuntu:~/Desktop/pictures$
```

Notice how the current directory (after **:** and before the **$** now reads ~/Desktop/pictures. This indicates that the terminal window is in the **pictures** directory. The `ls` command can be used once again to see the contents of the folder, and the process can be repeated to move throughout the Linux filesystem.

To step out of the current directory:

```
noah@ubuntu:~/Desktop/pictures$ cd ..
noah@ubuntu:~/Desktop$
```

OR

```
noah@ubuntu:~/Desktop/pictures$ cd /home/noah/Desktop
noah@ubuntu:~/Desktop$
```

OR

```
noah@ubuntu:~/Desktop/pictures$ cd ~/Desktop
noah@ubuntu:~/Desktop$
```

Remember that ~/ is a shortcut for /home/noah/ so command works. Likewise, to shift to a different directory, enter the file path of that directory

Example: to switch into /etc/cron.d

```
noah@ubuntu:~/Desktop$ cd /etc/cron.d
noah@ubuntu:/etc/cron.d$
```

Editing text files

In Linux, many options are set by editing configuration files. You can use a variety of text editors to get the job done.

Gedit

Gedit (pronounced “G-Edit” or “Get-It” if you’re lazy) is the Linux version of notepad and is the simplest to use. I recommend it the most for new users

To edit a text file:

```
noah@ubuntu:~/Desktop$ gedit /etc/login.defs
```

This will open up a text editor window and allow you to edit the file. Make sure to hit save when you are done.

If the save button is greyed out, you may need to administrator privileges to edit the file. In this case, run gedit with sudo (see SUDO section for more details)

SUDO

Usually, you do not want to allow a user to delete every single file in the operating system. There is a simple command, however, that will do just that. That said, how do you prevent a user from executing said command or, more generally, stop them from modifying the system and making unwanted changes? The answer: **sudo**

SUDO stands for Superuser-Do and stops people from messing up entire file systems because of careless errors. Only computer administrators can use sudo (preventing Dave the Intern from changing firewall permissions, for example), and it must be used before executing a command that requires administrator permissions.

For example, the command to enable the firewall is:

```
noah@ubuntu:~$ ufw enable
```

However, that command requires administrator permissions. Thus, we need to preface it with `sudo`:

```
noah@ubuntu:~$ sudo ufw enable
[sudo] password for noah:
```

The system will prompt your user for their admin password (the password will be hidden from the screen) and, when typed successfully, will allow you to enable the firewall.

Generally, if a command does not work, try running it with sudo.

Man pages

If you want to get more information about a specific command, its man page (aka manual) is a good way to get more information.

To learn about cd:

```
noah@ubuntu:~/Desktop$ man ls
```

If you are unsure about a command, check its man page or Google it.

Competition

Forensics Questions

Forensics questions ask you to perform various tasks and answer questions to earn points. As mentioned earlier, **DO THESE FIRST**. Making other changes could destroy the information required to completed the questions

Checksums

Sometimes, a question will ask you to compute the hash of a specific file. A hash is a unique sequence of characters that people often use to check if a file has been altered. Fortunately, checking a hash in Ubuntu is easy.

For example, the following command calculates an MD5 checksum:

```
noah@ubuntu:~$ md5sum file.txt
d41d8cd98f00b204e9800998ecf8427e  file.txt
```

To calculate other types of checksums, a simple google search will do the trick

Locating Files

To find files with a specific file extension (e.g. .txt .mp3 .mp4 etc.), the `locate` command is very helpful

```
noah@ubuntu:~$ locate *.mp4
/home/noah/Desktop/video.mp4

noah@ubuntu:~$ locate *.txt
/home/noah/Desktop/README.txt
```

Run the command with * in front of the extension to search for all files with that extension in the current or underlying directories. To search for a specific file, simply run the command with the name of the file

```
noah@ubuntu:~$ locate Mozart.mp3
/home/noah/Downloads/Mozart.mp3
```

User IDs

In Ubuntu, every user in a system will have a unique User ID. The `id` command returns the UID of the specified user (current user if there is no user supplied).

```
noah@ubuntu:~$ id
uid=1000(noah) gid=1000(noah) groups=1000(noah)

noah@ubuntu:~$ id noah
```

```
uid=1000(noah) gid=1000(noah) groups=1000(noah)

noah@ubuntu:~$ id neal
uid=1001(neal) gid=1001(neal) groups=1001(neal)
```

The UID environment variable also contains the user ID :)

```
noah@ubuntu:~$ echo $UID
1000
```

Groups

To see every group along with its members, you can inspect the file located at `/etc/group`

```
noah@ubuntu:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
…
…
noah:x:1000:
sambashare:x:132:noah
neal:x:1001:
jack:x:1002:
cole:x:1003:
secretgroup:x:1021:noah,jack,cole
```

Noah, Jack, and Cole are members of the group called **secretgroup**

User Accounts

In Ubuntu, there are two types of users: Standard and Administrator. Administrators simply have elevated permissions, can execute commands with `sudo`, etc.

After finishing the forensics questions, go through the readme and note which users should be Standard and which should be Administrators. User account control is easiest using the **graphical user interface**.

To access the GUI: hit the windows key to enter the search menu and search for “user accounts”; click the “unlock” button in the top right and enter the password for that user (found in the README) to make changes.

To add / remove users: if the README does not mention a user, remove them by selecting the user and clicking the **minus** button at the bottom of the window (if prompted, choose to delete their files). Similarly, add a user by clicking the **plus** button in the bottom left.

The order for securing user accounts:

1) Read the README
2) Remove unauthorized users
3) Change account type to standard if the user is not supposed to be administrator (or vice versa)
4) Go through each user and change all insecure passwords

a. It is best to decide on one password, like **CyberPatriot1!**, and change all users to that password

Also, it is okay for **Automatic Login** to be enabled for your user

Password Policy

This section quickly gets complicated because of the standard Unix-like complexity dealing with PAM (Pluggable Authentication Module), which is used to verify passwords :/

For now, modifying the default login file is sufficient to gain points.

Open the login.defs file located at /etc/login.defs and edit the parameters to your liking

```
noah@ubuntu:~$ sudo gedit /etc/login.defs
…
…
PASS_MIN_DAYS 7
PASS_MAX_DAYS 90
PASS_WARN_AGE 14
…
```

Remember to hit save!!! If you cannot save the file (assuming you are using gEdit, you likely forgot to run the command with sudo)

As an alternative, you can run the `chage` command to update the password policies for specific users

```
noah@ubuntu:~$ chage -m 30 -M 90 -W 14 noah

-m sets minimum password age
-M sets maximum password age
-W sets # of days a warning is issued before a password change is required

noah is the user whose password policy will change
```

Local Security Policy

Disabling Guest Account

Guest account is a security risk because it allows everyone access to the computer system. LightDM is a display manager in Ubuntu and starts the greeter (aka the login screen). Therefore, disable the guest account in the LightDM configuration file at `/etc/lightdm/lightdm.conf`

First, open the file

```
noah@ubuntu:~$ sudo gedit /etc/lightdm/lightdm.conf
```

Then, navigate to the bottom and add the line

```
allow-guest=false
```

Then, save the file, exit, and restart with the following command:

```
noah@ubuntu:~$ sudo restart lightdm
```

WARNING: this step will log you out. Make sure you are not in the middle of doing something else, and that you know the password of at least one administrator in the event the system locks you out.

Programs and Services

Firewall Configuration

Configuring the firewall can be done both graphically and through the command line interface.

Command Line Interface (CLI)

Enabling the firewall with Ubuntu's built-in Uncomplicated Firewall (UFW) is usually enough to earn points:

```
noah@ubuntu:~$ sudo ufw enable
```

Likewise, a port or a service can be allowed / blocked in the terminal. See the man page for a full list of UFW commands. Some examples are listed below:

```
To allow a port (80)
noah@ubuntu:~$ sudo ufw allow 80
Rules updated
Rules updated (v6)

To deny a port (80)
noah@ubuntu:~$ sudo ufw deny 80
Rules updated
Rules updated (v6)

To allow a service (ssh)
noah@ubuntu:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
```

Graphically with GUFW (GUI)

GUFW is a graphical version of UFW. It can be easier to use if you are dealing with multiple firewall rules and is straightforward to use.

To install:

```
noah@ubuntu:~$ sudo apt-get install gufw
```

Then run the program by typing `gufw` into the command line

```
noah@ubuntu:~$ sudo gufw
```

Choose one of the firewall profiles, making sure that incoming is set to **reject** and outgoing is set to **allow**. On the **rules** tab, you can set custom firewall rules

Problematic Services / Prohibited Software / Media Files

The following command will list every service and its status:

```
noah@ubuntu:~$ service --status-all
[+] apache2
[+] cron
[-] ssh
[-] ufw
```

[+] means that a program is running, [-] means that a program is not running

In general, make sure to only run services stated in the README. Not all services need to be stopped; some of the problematic ones are listed below:

- SSH
- Telnet
- Apache (or apache2)
- FTP
- MySql
- Filezilla
- Samba

To start a service:

```
noah@ubuntu:~$ sudo service ssh start
```

To stop a service:

```
noah@ubuntu:~$ sudo service apache2 stop
```

Generally, it is a good idea to both stop AND uninstall unnecessary programs to gain points

```
noah@ubuntu:~$ sudo apt-get remove apache2
noah@ubuntu:~$ sudo apt-get remove pure-ftpd
```

Adding / Removing / Updating Programs

Software is most often added, removed, and updated using the command line via Ubuntu's Advanced Package Tool (APT). The Ubuntu Software Center can also be used to graphically install / uninstall programs, but is only recommended because it is easy to view all currently installed programs.

Command Line Interface (Recommended)

Many programs are not in the software center, so it is important to be proficient using APT in the command line. The syntax is as follows:

```
noah@ubuntu:~$ sudo apt-get install [program]

noah@ubuntu:~$ sudo apt-get remove [program]
```

Example: the competition will often reward points for removing unwanted or malicious programs. For example, **nmap** is a malicious tool that scans networks and often installed on the images. To remove the program, type:

```
noah@ubuntu:~$ sudo apt-get remove nmap
```

NOTE: zenmap is a graphical version of the **nmap** program and is usually installed alongside **nmap**. In the competition, remove both to earn points.

```
noah@ubuntu:~$ sudo apt-get remove nmap

noah@ubuntu:~$ sudo apt-get remove zenmap
```

NOTE: Sometimes, a program will have a slightly different command to install it. For example, configuring SSH via APT is slightly different:

```
noah@ubuntu:~$ sudo apt-get install openssh-server

noah@ubuntu:~$ sudo apt-get remove openssh-server

noah@ubuntu:~$ sudo apt-get update openssh-server
```

If you are trying to figure out how to install / remove / update a specific program, a google search will do the trick.

Graphically via Ubuntu Software Center

The **Ubuntu Software Center** allows for easy management of the installed programs. Many of the programs are bundled alongside Ubuntu and do not need to be removed (see below).

To access the GUI: hit the windows key to enter the search menu and search for “software”; the handbag icon that should be labeled something like “Ubuntu Software.” Once in the program, go to the “installed” tab to scroll through the list of installed programs. Any programs that come pre-installed with Ubuntu do not need to be removed (Calendar, Cheese, Rhythmbox, LibreOffice, etc.).

Common Malicious Programs

This is a good list of the most common malicious programs that you should remove in the competition. Of course, there may be programs installed that the list does not include. If you are unsure of a program, do a google search and decide for yourself. If you uninstall it and lose points, make sure to reinstall.

- John the Ripper
- Tcpdump

- Reaver
- Ophcrack
- Netcat
- Bind9
- Any app that is part of the Aircrack suite:
    - airbase-ng
    - aircrack-ng
    - airdecap-ng
    - airdecloak-ng
    - airdrop-ng
    - aireplay-ng
    - airgraph-ng
    - airmon-ng
    - airodump-ng
    - airolib-ng
    - airserv-ng
    - airtun-ng
    - besside-ng
    - dcrack
    - easside-ng
    - packetforge-ng
    - tkiptun-ng
    - wesside-ng

Any installed videogames (apart from pre-installed games like Solitaire, Mahjong, Minesweeper, etc.) should be removed (for example, a commonly installed game that should be removed is **Civilization** or **Civ**).

Automatic Updates

Enabling automatic updates must be done via the "Software and Updates" GUI.

IMPORTANT NOTE: enabling the proper settings using the GUI must be done before attempting to update programs via the CLI. Otherwise, it may not work properly.

To access the GUI: hit the windows key to enter the search menu and search for "Software and Updates"; this will open up a window that allows you to configure multiple options about updating.

Scroll through the tabs. Generally, the options will be similar to the following, and recommended settings are indicated by a **+** or **–** on the left:

Ubuntu Software:

```
Downloadable from the Internet
[X] Canonical-supported free and open-source software
[X] Community-maintained free and open-source software
[-] Proprietary drivers for devices
[-] Software restricted by copyright or legal issues
[-] Source code
```

Updates:

```
Install updates from:
[X] Important security updates
[X] Recommended updates
[-] Unsupported updates

Automatically check for updates: Daily
When there are security updates: Download and install immediately
When there are other updates: Display immediately
Notify me of a new Ubuntu version: For long-term support versions
```

NOTE: After completing this step, Ubuntu may prompt you with an option to install or update programs. It is a good idea to wait for a lunch break to update as the installation may take some time and you will be unable to add, remove, or update programs using **APT** while the computer is updating.

Software Updates

After selecting the appropriate settings outlined in the Automatic Updates section, the computer will prompt you to update the programs. As mentioned earlier, this will take time and you cannot use **APT** while updating so it is good to update during a break in the competition.

Again, do this **AFTER SELECTING THE APPROPRIATE SETTINGS IN AUTOMATIC UPDATES SECTION** as you don't want to have to update twice.

To update all programs:

```
noah@ubuntu:~$ sudo apt-get update
```

To install newer versions of every package:

```
noah@ubuntu:~$ sudo apt-get dist-upgrade
```

NOTE: If you will take a long break, automatically run the commands one after the other:

```
noah@ubuntu:~$ sudo apt-get update && sudo apt-get dist-upgrade
if you can't read that symbol, those are two ampersands && in the middle
```

It, if you are stuck on a couple of points, run these commands near the end of the competition to check for any programs that may need updating.

Browser Security

Often, securing Firefox can net a few points in the competition, and can be secured by opening the browser, clicking the 3-lines to open a dropdown menu, and clicking the cog labeled "preferences" or "settings." A good checklist is as follows:

1) Make Firefox the default browser
2) Always ask where to save downloads
3) Make Google default search engine (unless otherwise specified)
4) Block all pop-up windows
5) Secure the apps in the Applications window
6) Request that sites do not track you
7) Use tracking protection in private windows
8) Warn when sites try to install add-ons
9) Block reported sites
10) Block reported web forgeries
11) Remember logins for sites
12) Do **NOT** use a master password
13) Warn when websites try to redirect or reload the page
14) Automatically update search engines

Prohibited Media Files

The section on Forensics questions already covers locating files, but there may be other files on the computer that should be removed.

Again, the locate command can be easily used to find files with a certain extension:

```
noah@ubuntu:~$ locate *.mp3

noah@ubuntu:~$ locate *.mp4

noah@ubuntu:~$ locate *.png

noah@ubuntu:~$ locate *.mov

etc…
```

Typically, the media files will be in the directory of another user on the same. If some are found, you can navigate to that directory via the file system GUI and delete the files, or you can use the CLI to delete them. In general, you should remove any media files if a user owns them.

Removing a media file:

```
noah@ubuntu:~$ locate *.mp3
/home/noah/Desktop/beethoven.mp3
/home/noah/Desktop/mozart.mp3

noah@ubuntu:~$ rm /home/noah/Desktop/beethoven.mp3
noah@ubuntu:~$ rm /home/noah/Desktop/mozart.mp3
```

^^the `rm` command removes a file.