- **https://www.maketecheasier.com/secure-newly-installed-ubuntu/**
- **Open readme file**
- **Delete unauthorized give passwords; Disable Guest account**
- **Update software** with 'Software Updater' program. (This also updates firefox)
- Ctrl+Alt+T is Terminal. Always keep it open.
    - **Precede every command with 'sudo'.** This grants root permissions to that specific command.
- **Change update settings** with (sudo nano /etc/apt/apt.conf.d/10periodic)
    - Change APT::Periodic::Update-Package-Lists to 1
- **Execute "sudo ufw enable"** to enable the built-in firewall easily
- Go to Software Center and **look at installed programs - uninstall unauthorized ones.**
    - Sudo apt-get remove <module> to really uninstall something
- **Turn on minimum password length**. Guide here.
- **Read Forensics Questions!**
- Use "gedit" function to open files to edit
- **Password settings** (login.defs) Edit the file – sudo nano /etc/login.defs also: /etc/pam.d/common-passwords has remember and minlen; do those
    - Key areas – PASS_MAX_DAYS, PASS_MIN_DAYS, PASS_WARN_AGE
    - Look here for specific requirements here:https://s3.amazonaws.com/cpvii/Training+materials/Unit+Eight+-+Ubuntu+Security.pdf
- Disable root users using "sudo passwd -l root"
- **DO NOT UPDATE TO THE NEXT DISTRO VERSION**
- **Do not allow root account to login** in using SSH! (sshd_config)
    - Edit the file – sudo nano /etc/ssh/sshd_config
    - Look for PermitRootLogin and set to no
- sudo nano /etc/lightdm/lightdm.conf
    - remove line with autologin-user
    - Add the following line to disable guest account: allow_guest=false
- If they're not critical services, **remove FTP & Telnet**:
    - This is kind of weird because there is no such thing as a service called "ftp". Instead, it's called vsftpd. Use `sudo apt-get remove vsftpd` to remove the program
    - To remove telnet, use "sudo apt-get remove telnet"
- **Read README** and do the following:
    - **Delete unauthorized users** in System Settings>User Accounts
        - Remove any root users, only keep administrators.
    - **Find unauthorized files** (mp3s, etc.). CHECK DOWNLOADS! In console, type

- Use “ sudo find . -type f -name “*.mp3” ” (Substitute mp3 for ogg, doc, and docx to get more music files, and documents respectively)

More info:
https://s3.amazonaws.com/cpvii/Training+materials/Unit+Nine+-+Additional+Topics+and+Resources.pdf

To edit security stuff in a file requires root access most of the time, assuming file is /file/config

To open via a terminal: `sudoedit /file/config`

## Reconfigure shared memory

- By default, the shared memory space (/run/shm) is mounted read/write, with the ability to execute programs. This has been noted in the security community as vulnerable, with many exploits available where “/run/shm” is used while attacking running services. For most desktop and server configurations, it is advisable to mount this as read-only by adding the following line to the file “/etc/fstab.”

Open the “/etc/fstab” file: `sudoedit /etc/fstab`

Add the following line to the end of the file: `none /run/shm tmpfs defaults,ro 0 0`

## Deny “su” program to non-admins

To deny Guest account access to the “su” program, type the following in a terminal

```
sudo dpkg-statoverride --update --add root sudo 4750 /bin/su
```

```
chmod 0700 /home/username
```

- By entering the line above your files will be protected from other users on the computer, before this any user could access all your files.

```
chmod 0750 /home/username
```

- Changes permissions for users directories