fKEY:

Things about user accounts

Passwords

Logs, System Services, Applications and System Generals

Misc.

**READ THE README!!**

* <http://www.linuxtopia.org/LinuxSecurity/>
* [**http://www.cyberciti.biz/tips/linux-security.html**](http://www.cyberciti.biz/tips/linux-security.html)
* <http://its.virginia.edu/unixsys/sec/>
* [**http://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html**](http://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html)
* <http://www.puschitz.com/SecuringLinux.shtml>
* <http://bastille-linux.sourceforge.net/>
* [**http://www.sans.org/score/checklists/linuxchecklist.pdf**](http://www.sans.org/score/checklists/linuxchecklist.pdf)
* [**http://www.nsa.gov/ia/mitigation\_guidance/security\_configuration\_guides/operating\_systems.shtml**](http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml)
* [**http://cyberpatriotarchives.com/Checklists/**](http://cyberpatriotarchives.com/Checklists/)

**Check these links once you don’t know what to do. Ask Abhi if you don’t know if the script does it or not:**

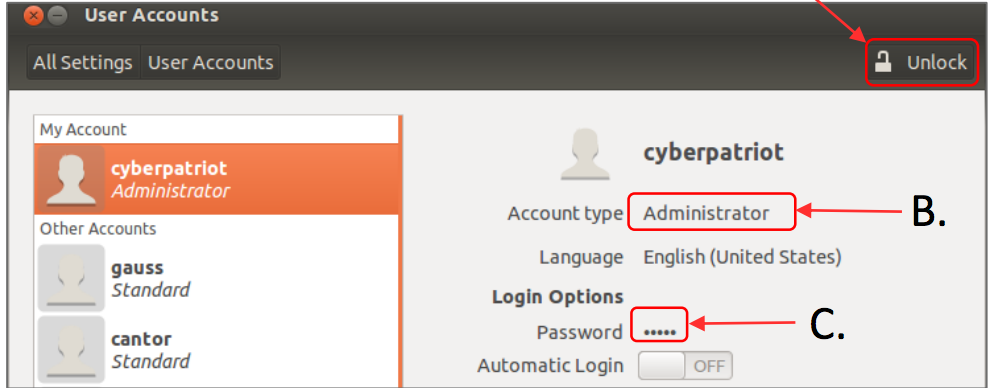
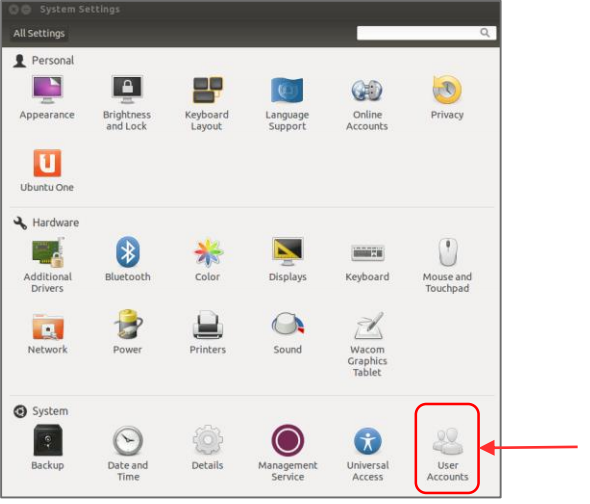
* [**https://www.process.st/server-security/**](https://www.process.st/server-security/)
* [**https://www.pontikis.net/blog/remove-old-kernels-debian-ubuntu**](https://www.pontikis.net/blog/remove-old-kernels-debian-ubuntu)

**CHECK FOR UNAUTHORIZED ADMINISTRATORS**

**CHECK FOR BACKDOORS - NETCAT, ETC.**

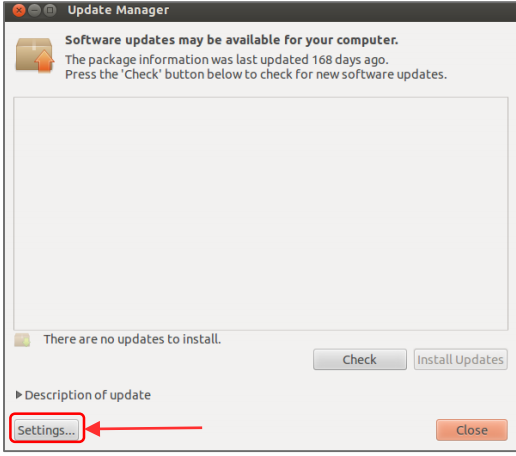
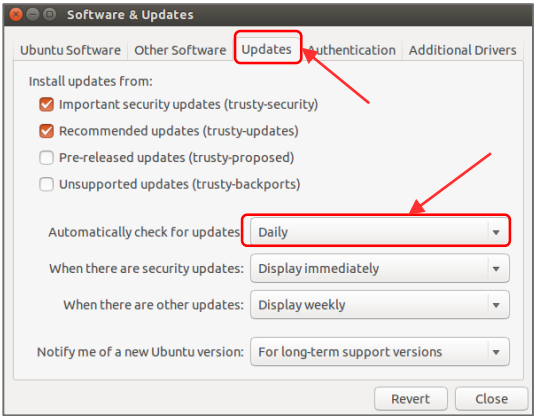
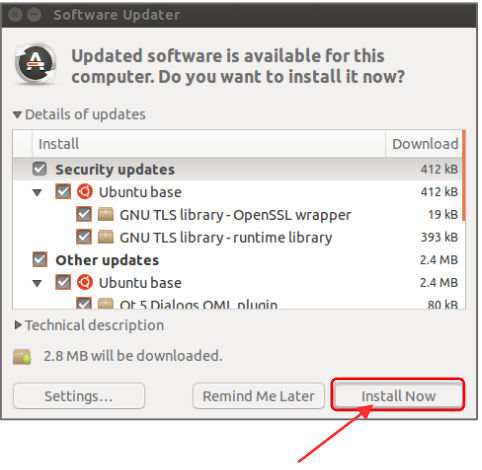
**Try to solve the forensic questions at the beginning to make sure that none of the updates and changes that are made during.**

**UNAUTHORIZED ADMINISTRATORS**

* Go to System Settings
* Go to the User Accounts
* Click on the top right to unlock the accounts
  + You’ll be prompted to give the password but it should be given to you during the README
* Match the list of administrators (the easiest way to do, personal opinion, is to go to *sudo gedit /etc/groups/* and match the list of administrators to the list given to you in readme.)
* If you find any unauthorized administrators, then change their authority! GIVEN THEM THE IRON ARM OF JUSTICE!
  + 

**Update**

* Applications > System Tools > Administration > Update Manager

1. 
2. 
3. 
4. 

* Enabling automatic security updates
  + Update manager -> settings
* sudo apt-get update packageName
* sudo apt-get upgrade
* Update Firefox -> About Firefox (or go to the website and redownload it) -- apt-get upgrade firefox
* Update System -> Go to the far right corner, and go to about Ubuntu, there you can check for updates

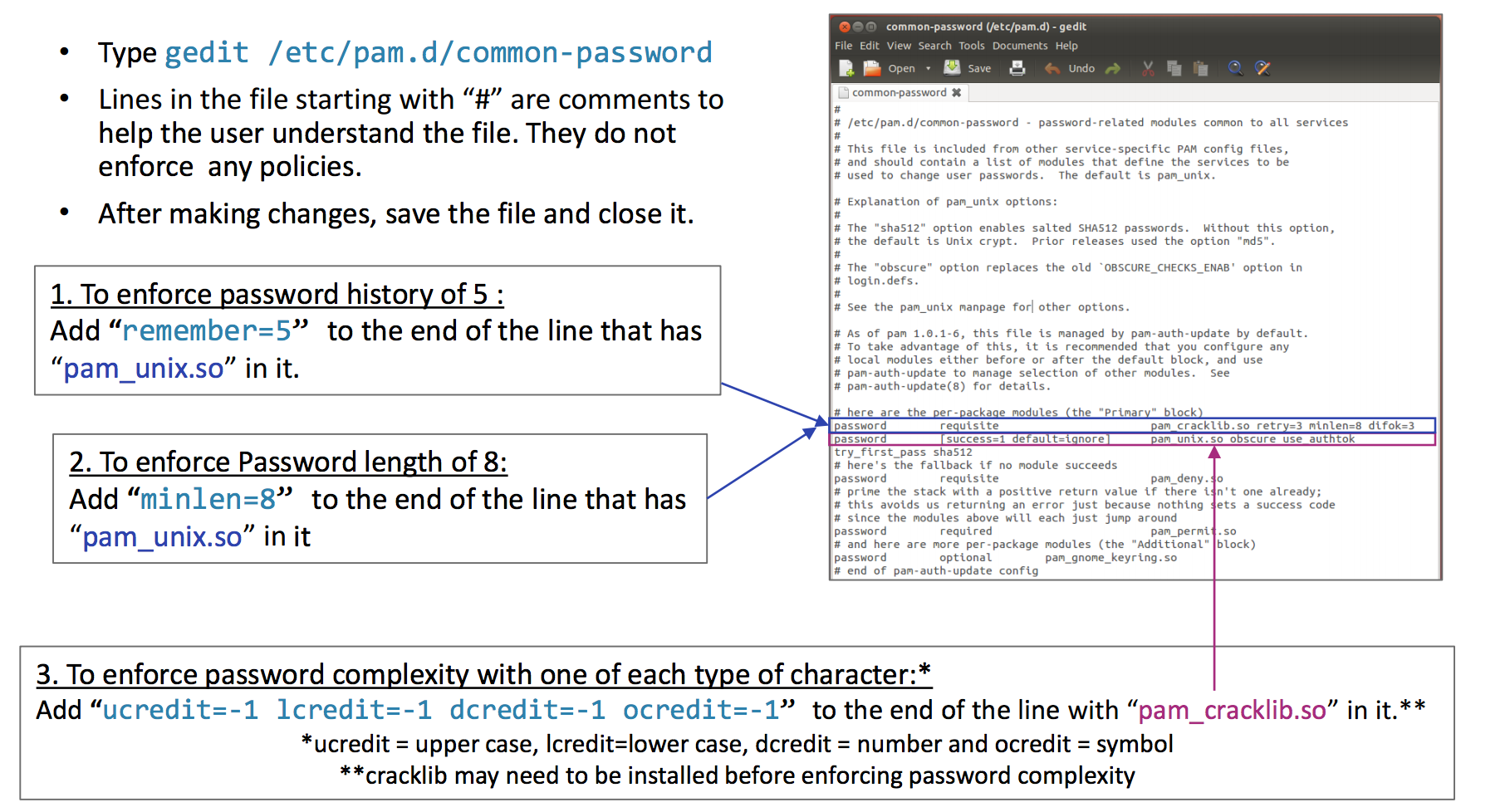
**Firewall**

* In Ubuntu all ports are blocked by default
* Default firewall - ufw(turned off by default)
  + Sudo ufw status
  + Sudo ufw enable/disable
* Firestarter for graphical interface(recommended)
  + Sudo apt-get install firestarter
  + Preferences
* You can download Gufw, a graphical firewall interface, from the Software Center and use it to make changes to the UFW in the GUI

**Install Required**

* apt-get install packageName (read the readme to check if the company wants any specific packages)

**Configure Pam.d**

* Install cracklib
  + sudo apt-get install libpam-cracklib
* 4 Types of PAM files:
  + Account – control account conditions (e.g. not expired, etc.)
  + Authentication – verify user identities
  + Password – control some password policies
  + Session – define actions performed at the beginning and end of user sessions.
* gedit /etc/pam.d/common-password
  + Lines that have a “#” are comments to help uspam
* 
* CAUTION: Last time we worked on a PAM file, our passwords wouldn’t work and because of this we had to restart the entire image.
  + For more info go to: <http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html>
  + This site helps you with password stuff too

**Start Services**

* service packageName start / stop

**Check administrators/users by using**

* sudo gedit /etc/groups/ on terminal.

**Check passwords/cancel all unauthorized users by using**

* sudo gedit /etc/passwd/ on terminal

**Seeing and Uninstalling Applications**

* Applications → Ubuntu Software Center
* Installed Software section
* Select application and click Remove
* Or use the command:
  + sudo apt-get remove [packageName]

**Disable Root Login**

* sudo gedit /etc/ssh/sshd\_config
* Search for: “PermitRootLogin”
* Replace it with no

**Secure Home Directory**

The final critical change we recommend, is that you protect your personal documents by [securing your home directory](https://wiki.ubuntu.com/SecureHome). The easiest way to do this is by clicking "Applications" selecting "Accessories" and choosing "Terminal." From there enter the command:

chmod 0700 /home/username (replace username with the name you use to login to your computer).

Now that you've successfully made these basic system setting modifications, you're ready to move on and start installing software that protects your system from being compromised.

**Antivirus**

* [Clam AntiVirus](http://www.clamav.net/) - One of the most popular UNIX based antivirus solutions. Works well with email gateways.
  + Install: sudo apt-get install clamav
  + Update virus database: sudo freshclam
  + Run scan (do this in the background): sudo clamscan -i -r --remove=yes
  + CAREFUL, MIGHT NOT BE ALLOWED BY CYBERPATRIOT
* [AVG Anti-Virus](http://free.grisoft.com/freeweb.php/doc/5390/lng/us/tpl/v5#avg-anti-virus-free) - Free version of a popular commercial virus scanner.
* [BitDefender](https://help.ubuntu.com/community/BitDefender) - On demand command line/shell script scanner.
* [Panda Antivirus](http://www.pandasoftware.com/download/linux/linux.asp) - Uses sophisticated software to remove viruses from workstations connected to a Linux server.

**Disable Auto Login**

* Settings > User Accounts> Automatic Login
* sudo nano /etc/group
  + Remove the line: nopasswdlogin:x:119:{{username}}

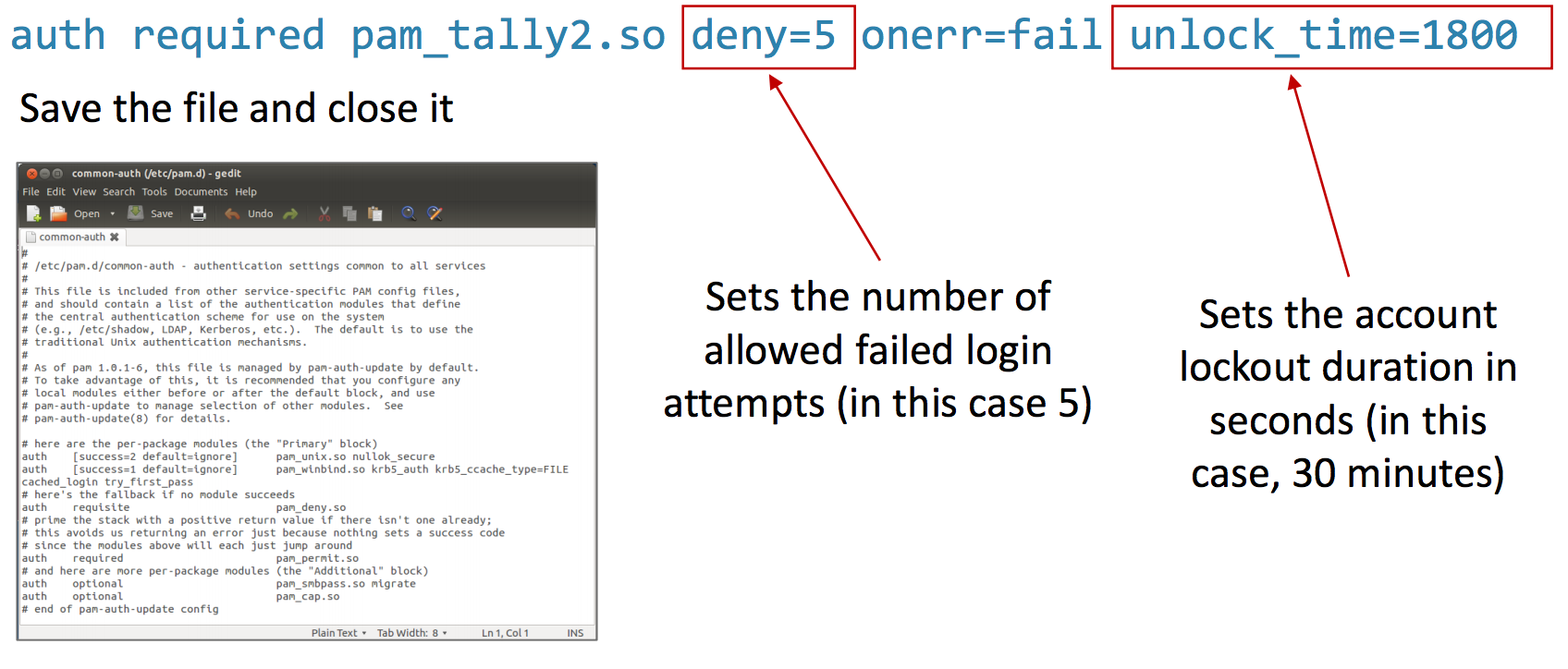
**Set Minimum Password Requirements**

* sudo gedit /etc/login.defs
* Search for: “PASS\_MAX\_DAYS”
  + Replace the values with the recommended values:
    - PASS\_MAX\_DAYS: 90
    - PASS\_MIN\_DAYS: 10
    - PASS\_WARN\_AGE: 7
* Save after editing the file.

**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 OR sudo gedit /etc/sudoers
  + James ALL=(ALL) ALL
  + Sudo adduser user\_name sudo
* Deleting standard users from being able to use root
  + Sudo deluser [username] sudo
* Adding users
  + Sudo adduser [username)]
* Deleting users
  + Sudo deluser [username]
  + Sudo deluser [username] --remove-home
* Removing world readable permission 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

**Set Account Policy**

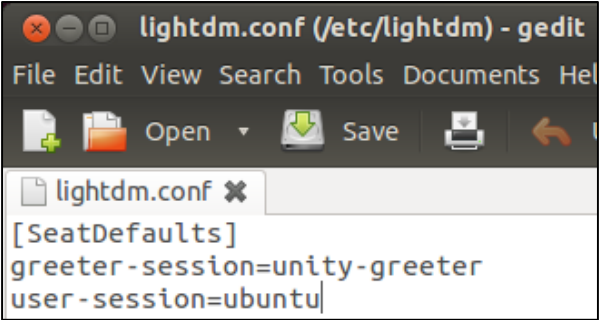
* sudo gedit /etc/pam.d/common-auth
* Add the following:
  + 

**Disable Guest Account**

**Ubuntu 16.04**

* -sudo sh -c 'printf "[SeatDefaults]\nallow-guest=false\n" > /etc/lightdm/lightdm.conf.d/50-no-guest.conf'

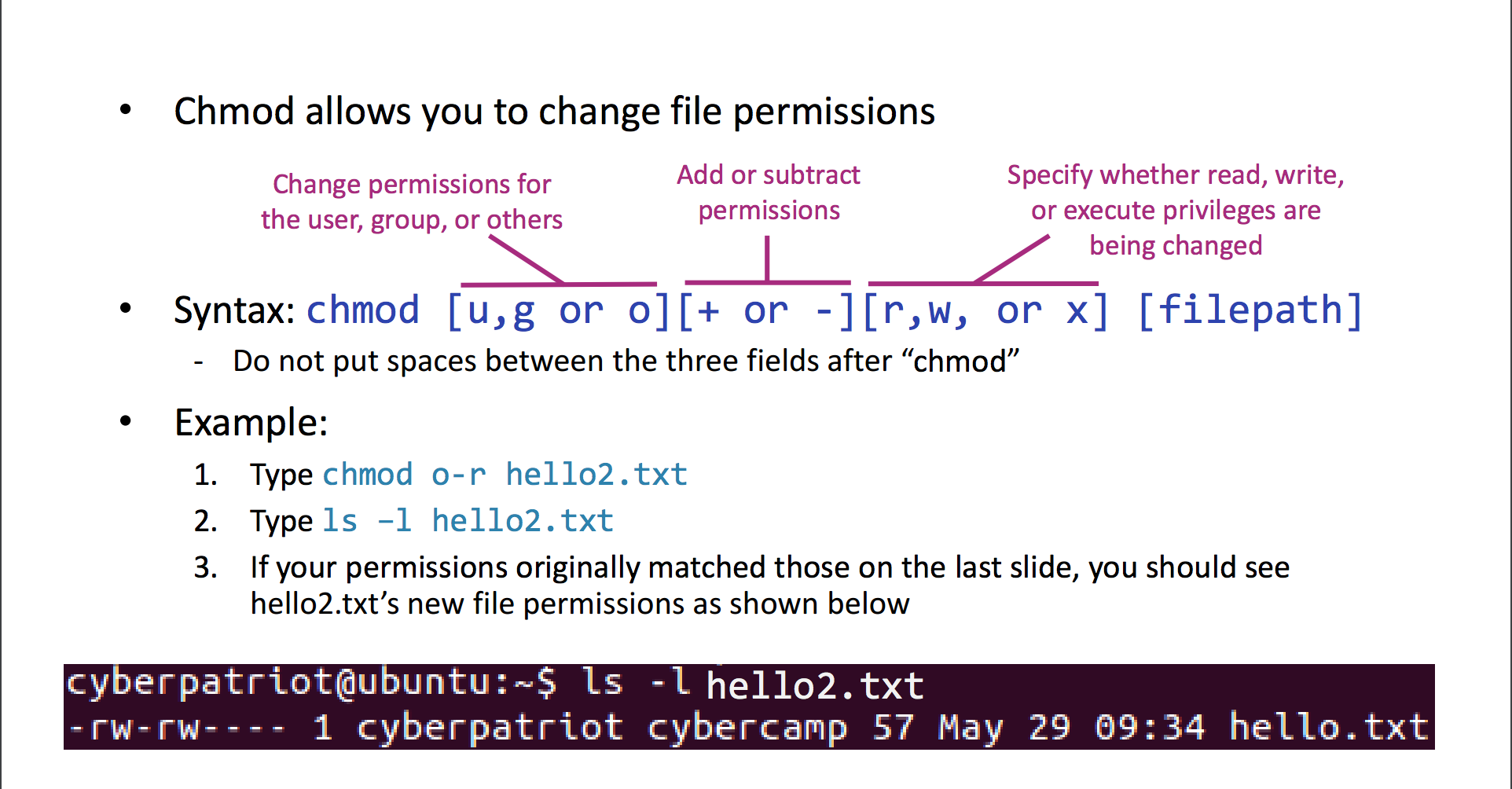
Ubuntu 14.04

* cd /usr/share/lightdm/lightdm.conf.d/
* Edit it by typing:
  + sudo gedit 50-ubuntu.conf
* Add:
  + Allow-guest=false
* Restart the computer to have the changes take effect:
  + sudo service lightdm restart
* 
  + ADD GREETER-SESSION=UNITY-GREETER
* You have to restart Ubuntu after doing this!!

**Groups**

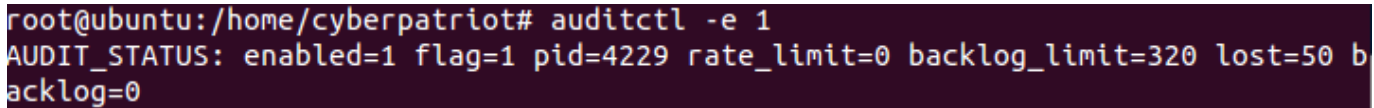
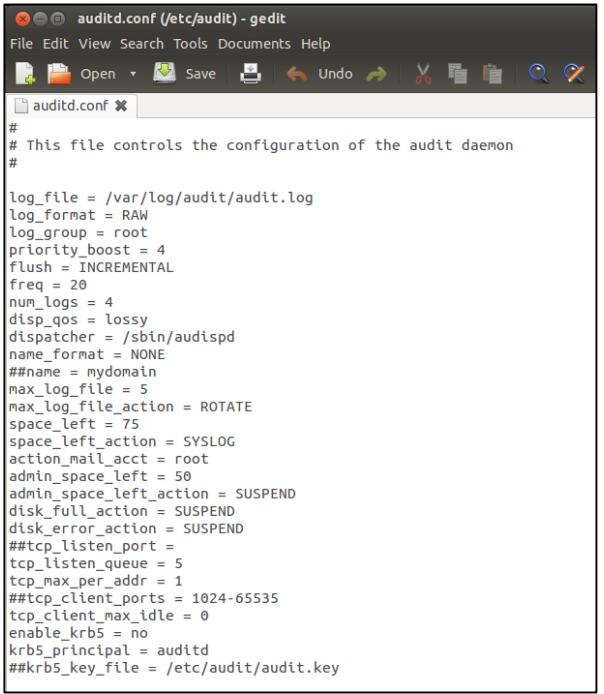
* To list all the groups use:
  + cat /etc/group
* Adding a group:
  + addgroup [groupname]
* Adding a user to a group:
  + adduser [username] [groupname]

**Changing File Permissions**

* Chmod command.
* 

**Setting Up Audit Policies**

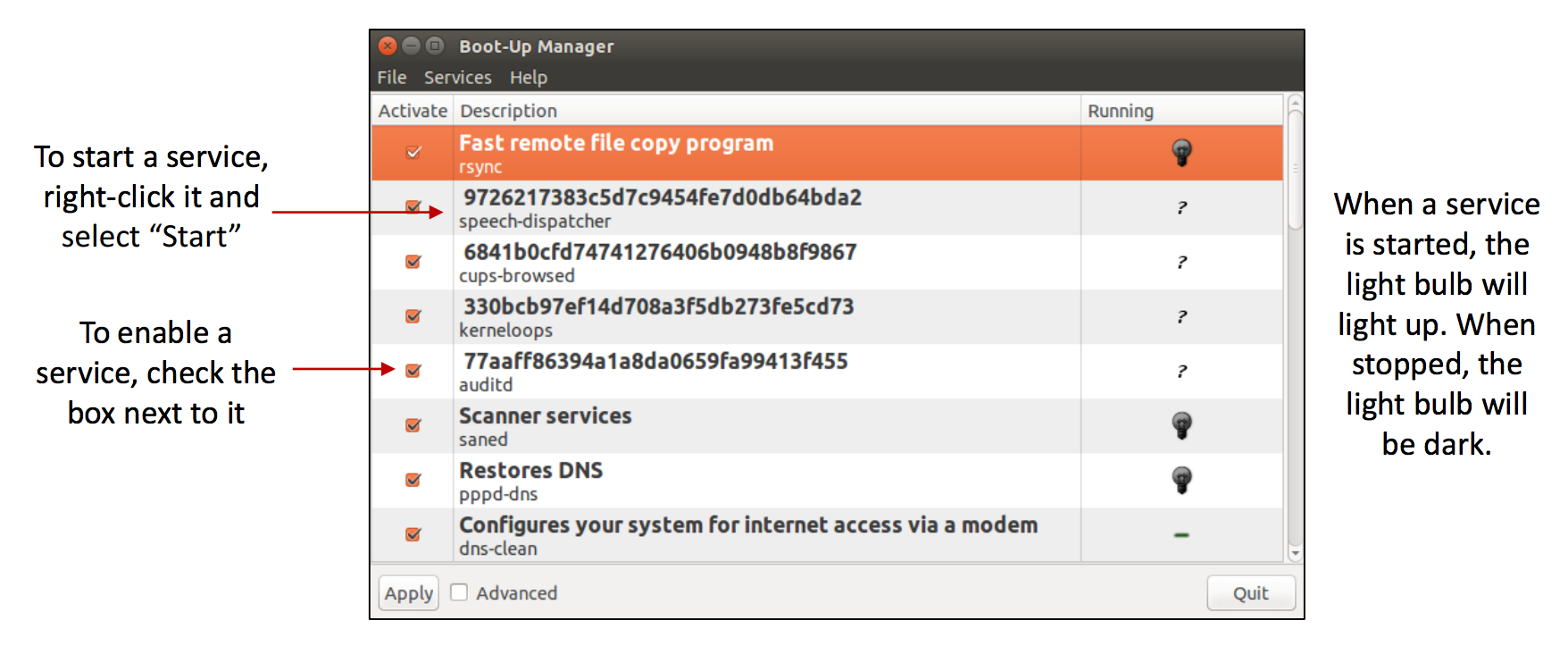
* Not setup by default on Ubuntu
* Steps of set a audit up:

1. Install the auditing program by typing apt-get install auditd
2. Enable audits by typing auditctl –e 1
   1. 
3. View and modify policies by typing gedit /etc/audit/auditd.conf
   1. 

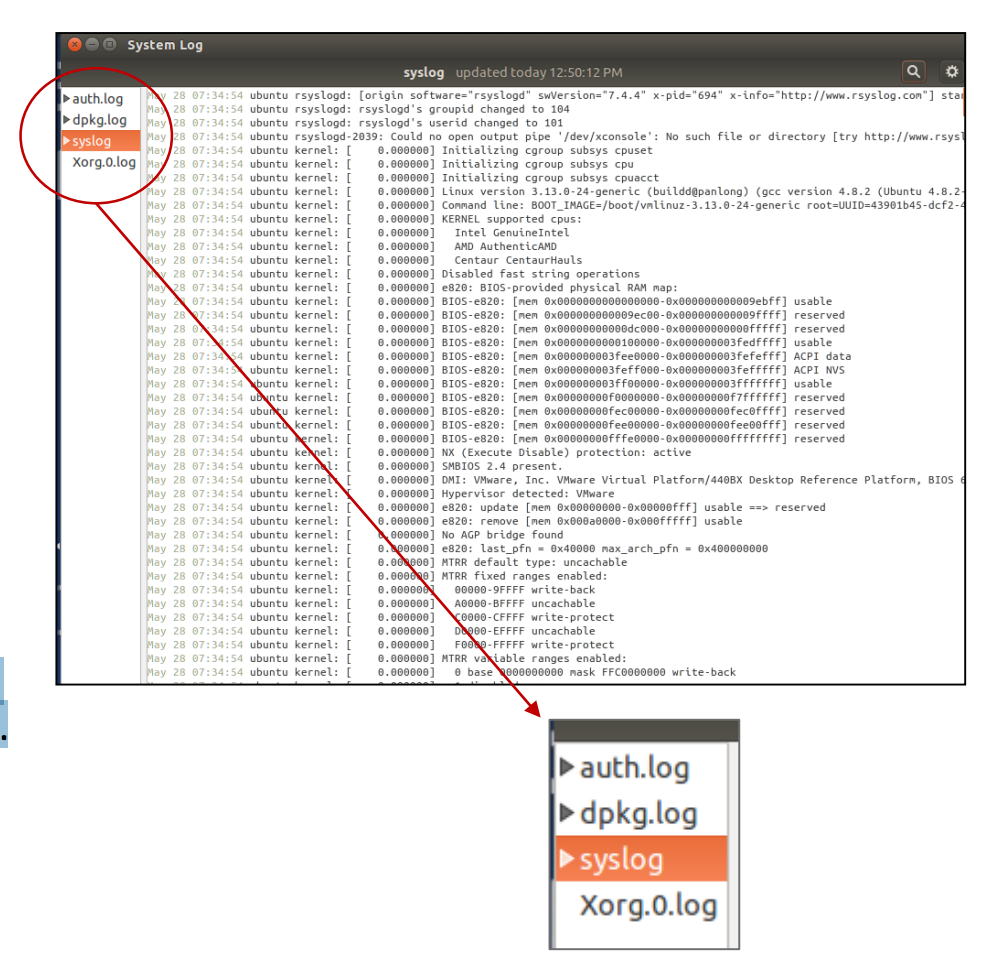
**Processes**

* To see processes
  + Ps aux OR top
  + System Monitor
* Know what default processare (screenshot/snip)

**Services**

* Managed through a GUI
* Install bum
  + sudo apt-get install bum
* Type in bum in terminal to run the application
* 

**System Logs**

* Use the search field in the Ubuntu menu that is on the top left of the desktop and search for system logs.
* Four different types of logs:
  + auth.log: Tracks authentication events that prompt for user passwords (e.g., uses of PAM files and sudo)
  + dpkg.log: Tracks software events (e.g., installations and updates)
  + syslog: Tracks operating system events (e.g. error messages)
  + Xorg.0.log: Tracks desktop events (e.g., service changes and graphic card errors.
* 

**Logs**

* Some of the logs
  + /var/log/messages : general log messages
  + /var/log/boot : System boot log
  + /var/log/debug : Debugging log messages
  + /var/log/daemon.log : Running services such as squid,ntpd and others log message to this file
* Viewing logs
  + Tail,more,cat,less,grep
  + GNOME System Log Viewer

**SSH:**

* Sudo apt-get install openssh-server
* Sudo service ssh status
* Sudo gedit /etc/ssh/sshd\_config
* Sudo service ssh restart
* Enabling SSH for specific users

**Bastille:**

* If bash file doesn’t work execute following commands below
  + sudo gedit /etc/apt/sources.list
  + Change DISTRIB\_CODENAME = xenial
  + aptitude upgrade
  + sudo bastille
  + Follow this [link](https://www.digitalocean.com/community/tutorials/how-to-install-and-use-bastille-to-harden-an-ubuntu-12-04) for more information

**Shutdown unnecessary services:**

* netstat -anp | grep LISTEN | grep -v STREAM
  + Research these services because some of them can shutdown your computer (BEN)
* cd /etc find . -print | grep XXX (where XXX is part of the name of the program)

**Securing Terminals:**

* gedit /etc/securetty
* Check that the secure option is removed from any local entries that don't need root login capabilities.

**Secure shared memory:**

* sudo gedit /etc/fstab
* Add this line
  + tmpfs /run/shm tmpfs defaults,noexec,nosuid 0 0
* Must reboot server for it to actually work

**MISC**

**Helpful links**

* <https://github.com/Forty-Bot/linux-checklist>
* <https://www.reddit.com/r/cyberpatriot/comments/5k0jef/what_will_round_3_be_like_how_should_i_prepare/>

**Quotes from the https://www.reddit.com/r/cyberpatriot/**

* “The first thing I did for Ubuntu was watch this [video](https://www.youtube.com/watch?v=MI3FmecbZM8) and take notes on all the commands he did and what it accomplished. Then I went into each topic and did more research for possible vulnerabilities. I've done a lot of online research just by searching "Ubuntu security vulnerabilities", but that video will be the fastest way to gain points if you need to be introduced to the topics (though I guess this late in the season unless someone quit it probably won't help much).

**IMPORTANT IMPORTANT**

* Always edit /etc/passwd with sudo vipw
* Always edit /etc/shadow with sudo vipw -s
* Always edit /etc/group with sudo vigr
* Always edit /etc/gshadow with sudo vigr -s
* Always edit /etc/sudoers with sudo visudo