UBUNTU

|  |  |
| --- | --- |
| This disables guest accounts | sudo sh -c 'printf "[SeatDefaults]\nallow-guest=false\n" > /etc/lightdm/lightdm.conf.d/50-no-guest.conf' |
| Files and directories  Also has commands for viewing files in terminal | Use **synaptic** to get rid of hidden package files: *sudo apt-get install synaptic*  cd (directory name) this will move the user to the directory specified.  cd ~ this allows the user to go directly to the root directory  locate (filename) this will search the entire computer for the file specified and show you the directory or location of that file  mkdir (directory name) This allows you to make a subdirectory in the present directory  ls ~ this command shows all of the files and directories in the current directory.  ls -R ~ this command will allow you to see all of the files and directories in all of the directories including the sub directories  ls -a ~ this gives a list of all of the hidden files and folders |
| Installing packages | apt-get install packageName (read the readme to check if the company wants any specific packages) |
| Configuring pam.d | To configure the pam.d file, type  Sudo /etc/pam.d/common-password\  Into the terminal. In the file, find the line:  Password [success=1 default=ignore] pam\_unix.so obscure sha512  Add: “minlen=8” To the end of the line.  If current user’s password does not match the minimum requirements, lower the minimum. |
|  | |
| Password settings | Sudo gedit /etc/login.defs  Once you open the file, search for  “PASS\_MAX\_DAYS”   * 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 |
| User accounts | User Account Settings      *Go through the readme document to find the list of users that are allowed on the computer. Delete any unwanted users and check to be sure that administrators are set to be administrators and standard users are set to be standard users.*  Disable root login  sudo gedit /etc/ssh/sshd\_config  Once in that file search for “PermitRootLogin” add “no” to the end of the line.  Save the file and close. |
| Disable Samba service | Sudo service smbd stop  This should stop the samba service. To ensure that samba has been stopped type the following command  Sudo service smbd stop  Terminal window: |
| Updates | Update manager  Sudo apt-get update && sudo apt-get -y upgrade && sudo apt-get -y dist-upgrade && sudo apt-get -y autoremove  Applications > System Tools > Administration > Update Manager  nyb p-l87    *Set the update presets to the Automatically check for updates daily. Also ensure the boxes are checked that say, “important security updates (trusty-secure)” and “Recommended updates (trusty-updates)”*  Software updater    Open software updater and let the package scan the computer for updates. Let it run updates.  *(updates take a long time so try and time the updates with the rest of the images so they don’t get in the way of productivity of the team)* |
| Firewall | Sudo ufw status  This command will tell you if the firewall is on or off. It should say Status: *status* if it says active the firewall is on if it says firewall inactive the firewall is off  Sudo ufw enable  This command will enable the firewall. After you enable the firewall type sudo ufw status again to ensure it has been activated  Sudo apt-get install gufw  This will install a graphical firewall interface.  Sudo gufw  This command will run the graphical firewall interface. Once in there complete the following settings. |
| FIND | Command called find  Find / -type f -name “\_\_\_\_\_”  DELETE ALL: .mp3, .wav, .mp4 |
| Processes | To see processes  ps aux or top |
| 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/auth.log : User login and authentication logs  /var/log/daemon.log : Running services such as squid, ntpd and others log  message to this file  /var/log/kern.log : Kernel log file  Viewing Logs  tail, more, cat, less, grep  GNOME System Log Viewer |

<http://mixeduperic.com/ubuntu/how-to-set-the-root-password-in-ubuntu.html>

<https://www.effinghamschools.com/Page/19298>

Linux Checklist and Tools:

1. Run multiple tasks when not installing software

(Command Line Commands)

2. Users:

\* Change passwords → sudo passwd <USER>

\* Enable Account → sudo passwd -u <USER>

\* Disable Account → sudo passwd -l <USER>

\* Always disable root account

\* Change admin privileges → sudo visudo

\* Add a user → sudo adduser <USER>

\* Delete a user → sudo deluser

\* Check Groups → sudo cat /etc/group

\* Passwords are stored in → /etc/passwd abd /etc/shadow

3. Firewall (disabled by default)

\* Enable Firewall → sudo ufw enable

\* Disable Firewall → sudo ufw disable

\* Status → sudo ufw status

\* Allow a protocol through → sudo ufw allow <PORT>

\*Can use names too (ssh, ftp, telnet)

\* Deny protocols → sudo ufw deny <PORT>

\* Look at applications using firewall → sudo ufw app list

\* Activate TCP SYN Protection (Protects against some \*DOS attacks) → sudo nano /etc/sysctl.conf

4. Antivirus

\*Update database → sudo apt-get update

\*Install antivirus package → sudo apt-get install package

5. Rest on pdf

6. Make it so ROOT can only be accessed by ADMINS

7. Check for IcedTea

8. Make sure that needed services are allowed through the Firwall