

[Linux] Checklist

1. Read the ReadMe carefully
 - a. Make notes of the important specifics
 - b. Copy the users and passwords on a spreadsheet on the separate computer
2. Read and do the forensic questions first in case you delete something important later on
3. Firewall **Done**
 - a. Open terminal
 - i. `sudo apt install gufw`
 1. Type in the password for your user
 - ii. `gufw`
 1. Type in the password again
 - b. On the **firewall software**
 - i. Profile: Home
 - ii. Status: On
 - iii. Incoming: Reject
 - iv. Outgoing: Allow
4. Antivirus
 - a. Open **terminal**
 - i. `sudo apt install clamav -y`
 - ii. `clamav` (if this doesn't work, try `clamscan` or `man clamav`)
 - iii. If infected files: delete them
5. Users **Done**
 - a. In the upper right corner, click the down arrow and click **Settings**. Go into **Details** and then click **Users**
 - b. Unlock using admin username and password (found in ReadMe) located in the upper right corner of **Settings** window
 - c. Go down the spreadsheet of allowed users
 - i. If a user is not listed then delete:
 1. Select the user
 2. Click **Remove User**
 3. Click **Delete Files**
 - ii. Change account type for those who are listed differently (ex: listed as admin but should not be admin). This can be found in the ReadMe/spreadsheet
 1. Select the user
 2. Click **Standard** if they should not be an admin
 - iii. Change password for those with weak passwords (check that all passwords have upper and lowercase letters and include numbers):

1. Select the appropriate user
 2. Click the box next to the password and **choose a secure password** and type it into the **new password box**, verify this password and click **change**.
 3. Record new passwords in the spreadsheet as a precautionary
- iv. Create users for the ones listed in the ReadMe or spreadsheet
 1. Click **Add User**
 2. In the textbox labeled **Full Name**, type the name of the user account
 3. Set a secure password for them and click **Confirm**
 - a. Record this password in the spreadsheet as a precautionary
 4. Click **Add**
6. Stop or disable FTP service
 - a. Open **terminal**
 - i. `sudo systemctl stop pure-ftpd`
 1. Type user password if prompted
 - ii. `sudo systemctl disable pure-ftpd`
7. Install Updates from important security updates
 - a. Click **Software & Updates**
 - b. In the **Updates** tab, check the checkbox labeled Important security updates
 - c. Type user password if prompted
 - d. Click **Close** and then **Reload**
8. Set automatic updates
 - a. Open **Update Manager**
 - b. Go to **Settings**
 - c. Set **Check for Updates: Daily**
9. Update **OpenSSH** and **Firefox**
 - a. Click **Show Applications** on the bottom of the **Launcher** and click **Software Updater**
 - b. Click **Install Now**
10. Firefox Settings **Done**
 - a. Open **Firefox**
 - b. In the top right, click the 3 bars icon and then click **Preferences**
 - c. Go to **Privacy & Security**
 - i. Turn off "Ask to save logins and passwords for websites"
 1. Do "Show alerts about passwords for breached websites"
 - ii. Do "Block pop-up windows"

- iii. Do “Warn you when websites try to install add-ons”
- iv. Do “Block dangerous and deceptive content”
 - 1. Do “Block dangerous downloads”
- v. Do “delete cookies and site data when Firefox is closed”

11. Prohibited MP3 files are removed

- a. Open **terminal**
 - i. locate ‘*.mp3’
 - 1. This outputs the file system locations of the mp3 files
 - ii. `sudo rm “(folder)”*.mp3`
 - 1. In this scenario with esbern, we type `sudo rm "/home/esbern/Downloads/Damiano Baldoni/Lost Dynasty/"*.mp3`
 - iii. Repeat for ‘*.jpg’

12. Prohibited software **ManaPlus** and **Game Conqueror** removed (software installed must be limited to the ones listed in the ReadMe, if it’s not on the ReadMe then delete it)

- a. Click the **Ubuntu Software** icon on the left side of the image
- b. Then go to installed tab, read description
- c. Scroll down to **ManaPlus** and click **Remove**
- d. Scroll down to **Game Conqueror** and click **Remove**

13. **SSH root login** has been disabled **Done**

- a. In the **terminal**, type `sudo gedit /etc/ssh/sshd_config`
- b. If prompted by sudo for a password, type the current user’s password.
- c. Change the line that says PermitRootLogin yes to **PermitRootLogin no**.
- d. Save file and exit

14. PAM Files (Pluggable Authentication Modules)

- a. Open **Terminal [9:12 in Video]**
 - i. `cd etc/pam.d/`
 - ii. `Then: cd ../../`
 - iii. `cd etc/pam.d/`
 - iv. `sudo apt install libpam-cracklib`
 - 1. Type password
 - v. `sudo nano common-password`
 - vi. Find the line that has pam_unix.so and add “remember=5” and “minlen=8” to that line **Done**
 - vii. Find the line that has pam_cracklib.so and add “ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1” to the end of that line
 - viii. [Ctrl O + Ctrl X] to save file and close it

15. Using gedit to Edit Password History **Done**

- a. Type *sudo nano ../login.defs*
- b. This is a much longer file so to easily find the section to edit, type Ctrl+F and then "PASS_MAX_AGE"
- c. Modify the following variables
 - i. PASS_MAX_DAYS = 90 [maximum password duration]
 - ii. PASS_MIN_DAYS = 10 [minimum password duration]
 - iii. PASS_WARN_AGE = 7 [days before expiration to warn users to change their password]
- d. Save the file and close it [Ctrl O + Ctrl X]

16. Using gedit to Set Account Policy **Done**

- a. *cd etc/pam.d/*
- b. Type *sudo nano common-auth*
- c. This file allows you to set an account lockout policy
- d. Add this line to the end of the file:
 - i. *auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800*

17. Watch for hacking software(s)


- a. Look for suspicious files wherever the programs are installed
- b. Open Terminal
 - i. *sudo apt-get install -y bum*
 - ii. Type *bum* to run the program
- c. Get rid of dangerous files such as:
 - i. nmap (used frequently)
 - ii. Metasploit
 - iii. armitrage
 - iv. aircrack-ng
 - v. Burpsuite
 - vi. ofe crack (used frequently)
 - vii. Wireshark
- d. *sudo apt install bum*
 - i. This gives you a list of all programs that start during boot-up

18. Turn off guest account

- a. *cd /etc/lightdm/*
- b. *sudo nano users.conf*
- c. Add "*allow-guest=false*" at the end of the file
- d. [Ctrl O + Ctrl X]

19.

Random Commands and Scripts For Linux Ubuntu (In Terminal)

- Forensics Question: Get the uid of a user
 - 2 different ways:
 - `id (name)`
 - `getent passwd (name)`
 - Ex: to get the uid of a user named paarthurnax
 - `id paarthurnax`
 - `getent passwd paarthurnax`
 - BEST Way:
 - First change directory of terminal *cd etc*
 - Then use *ls* or *dir* function to see what's in such directory
 - Lastly, *sudo gedit passwd* (passwd is one of the files in the directory etc)
- Forensics Question: Find the absolute path of the directory containing prohibited MP3 files
 - locate `'*.mp3'`
 - This outputs the file system location
- Remove mp3 files in a folder
 - `sudo rm "{folder}"*.mp3`
 - Ex: to remove mp3 files in esbern's downloads folder
 - `sudo rm "/home/esbern/Downloads/Damiano Baldoni/Lost Dynasty/"*.mp3`
- Get machine information
 - Type *hostnamectl* to get information like Machine ID
- Get Sha256 sum of file
 - Type `Sha256[path to file]` to get Sha256 sum
- To find a specific file
 - `sudo find / -iname "*.mp3" -print`
 - *find* is the syntax for finding things
 - `/` check the directory; in this case, it looks through the entire computer
 - *-iname* is the syntax to look for a file name
 - `"*.mp3"` looks for files with the extension .mp3
-  Linux: Command Line
- [Link to Linux script](#) (it might not work)