**UBUNTU**

**ReadMe/forensics first**

* Forensics Questions - You may destroy the requisite information if you work on the checklist!

1. Open terminal, type “mysql --version”, returns 14.14
2. 3306
   1. Ust netstat
      1. sudo apt install net-tools
      2. sudo netstat -ltnp
         1. Check ‘tcp
   2. sudo lsof -i -P -n

* Users - open System tools ⇒ System Settings ⇒ User Accounts
  + Remove elena and reno
    - Gui
    - Terminal
      * sudo deluser username
      * (optional) sudo deluser --remove-home username
  + Give passwords to all users (except current)
    - Good password:
      * Length 8+, uppercase, number, symbol
      * Change to smth like 1Cyberpatriots@$
    - Change bwallace password
    - Change ykisaragi to administrator
  + **User commands**:
    - Useradd username
    - Deluser username
    - Passwd username
    - Groupadd groupname
    - usermod username -a -G groupname
    - Grep gold /etc/group
* Turn on Firewall
  + open System tools ⇒ System Settings ⇒ Firewall Configuration
  + Switch to “on”
    - Use gufw
* Software updates
  + Automatic updates
    - open System tools ⇒ System Settings ⇒ Software Updates
    - Check ‘Important Security Updates’
    - Check ‘Recommended updates’
  + Update software
    - open System tools ⇒ Administration ⇒ Software Updater
    - Sudo apt-get update && apt-get upgrade
* Delete unwanted files
  + Accessories ⇒ Files
  + Open Music, delete “Shaolin Dub”
* Turn off unnecessary services
  + Use Bum (terminal)
    - Sudo apt-get install bum
    - Bum
    - Uncheck pure-ftp, hit apply
      * Some unnecessary services services: Telnet • Anonymous FTP • Remote processes (Rexec.Rlogin,Rsh) • Rstatd • Finger • Talk, Ntalk
* Secure Firefox
  + Check for updates
  + Check all security
    - No popups
    - Strict
    - Always to do not track
    - Warn when websites try to install add-ons
    - Block dangerous and deceptive content
* Remove insecure software (terminal)
  + Dpkg -l
  + sudo apt remove --purge kismet
    - Sus packages: pure-ftpd, john the ripper, hydra, nmap, metasploit, aircrack-ng, Netcat, Nessus, wireshark, snort

**DEBIAN**

* Forensics
  + 1. Ps -ef
    - /sbin/init
  + 2. find /home -name “Chocobo\_Gold.jpg”

-/home/cstrife/Pictures/

* Users
  + All Applications ⇒ Users (GUI)
    - Remove tseng
    - Remove rude
    - Make dyne standard
    - Change bwallace password
      * CyberPatriots123@
    - Add ykisaragi, change pass on next login
  + Add users to group (terminal)
    - Sudo -i
    - Groupadd gold
    - usermod bwallace -a -G gold
    - usermod ykisaragi -a -G gold
    - usermod tlockhart -a -G gold
    - usermod againsborough -a -G gold
    - grep gold /etc/group
* Firewall on
  + sudo apt-get install gufw (already installed)
  + Gufw, turn on
* Software
  + Search software and updates
    - Check security updates, recommended updates, change to daily
  + Update
    - Go to software center, hit reload (bad idea)
      * Hit restart and update when done
    - sudo apt-get update && sudo apt-get upgrade
    - Only openssh (is updated with the other packages, but in case u want to know):
      * sudo apt-get update
      * Sudo apt-get install ssh
* Firefox
  + Preferences
  + Check “block dangerous downloads”
* Services
  + Service --status-all
  + apt remove dovecot
    - Remove dovecot to remove pop3
  + Apt autoremove
* Packages
  + Open software center, remove
  + dpkg -l
  + apt-get --purge remove nmap
  + sudo apt remove --purge remove ettermap