Ubuntu Checklist

- Read the read-me CAREFULLY!
  - Almost always asks you to add a group, add users to group, etc.
  - Take pictures of Users
  - Remember admins and passwords!
    - Usually, at least one Admin who needs their password changed
    - Change passwords to similar iterations of the same word
  - Write down all relevant information, including ports to enable/disable and users
  - Don't do anything until later but make sure to take good notes!
- Read the first forensics question!
  - Commonly "Find absolute path of…"
    - Use "Find -type f -name "*.txt"'"
  - Commonly "This file is encrypted…"
    - Just google a decoder
  - Commonly "Find all files of this type and list their directories…"
    - Use "Find /home '*.type'"
- Once you finish the forensics, you can delete any data associated with them
- Securing users/user settings
  - Secure root
    - /etc/ssh/sshd_config
      - PermitRootLogin no
    - DON'T PULL A GIDEON!!
  - Disable guest user
    - /etc/lightdm/lightdm.conf and add the line allow-guest=false
    - sudo restart lightdm
  - Password Security
    - Open up /etc/passwd and check which users
      - Are uid 0
      - Can login
      - Are allowed in the readme
    - Add or change password expiration requirements to /etc/login.defs.
      - PASS_MIN_DAYS 7
      - PASS_MAX_DAYS 90
      - PASS_WARN_AGE 14
    - Null passwords do not authenticate
      - Sudo gedit /etc/pam.d/common_auth
        - Delete Nullok
        - Change unlock time to equal 1200
        - Change deny to equal 5
    - Min length, Pass history and complexity requirements

- Sudo gedit /etc/pam.d/common-password
    - Add minlen=8 and remember=5 to pam_unix.so
    - Add ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 to pam.cracklib.so
        - If libpam.cracklib doesn't exist, sudo apt-get install libpam-cracklib
- Go to /etc/pam.d/common-auth
    - Add deny=5 unlock_time=1800 to pam_tally2.so
- Go into users in settings
- Look for and delete all users not supposed to be there (not on your list)
- Change insecure passwords (will be on admin list)
    - Chpasswd!!
- Go to /etc/pam.d/common-account
- Add "account required pam-tally2.so" (without the quotation marks)

- Updates settings
    - Enable automatic updates
        - Go to update manager
        - Settings
        - Updates
        - Check for Updates
            - Daily
- Securing Network
    - Enable firewall
        - Sudo ufw enable
        - Configure firewall
        - (Most of this is done in the script)
    - Enable syncookies
        - sysctl -n net.ipv4.tcp_syncookies
    - Disable IPv6
        - echo "net.ipv6.conf.all.disable_ipv6 = 1" | sudo tee -a /etc/sysctl.conf
    - Disable IP forwarding
        - echo 0 | sudo tee /proc/sys/net/ipv4/ip_forward
    - Prevent IP Spoofing
        - echo "nospoof on" | sudo tee -a /etc/host.conf
    - Check for hacking tools
        - Installed Packages
- Configure Services
    - Check service config files
        - SQL, Apache, Daemon, etc.
    - Check service legitimacy
        - Service —status-all
- Updates

- Do this last to ensure that if it absolutely wrecks your machine, you're ok to submit if needed
  - sudo apt update
  - sudo apt upgrade
  - sudo reboot

Other

- System logs
  - Different logs
    - /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
- Uninstalling Software
  - Applications → Ubuntu Software Center
    - Installed Software section
      - Select application and click Remove
- Antivirus
  - sudo dpkg -i Downloads/clamtk_VERSION.deb
  - To use type Clamtk
- Deleting all files of a certain type
  - find /home -name '*.mov' -type f -delete
- Listing all active services
  - systemctl list-units --type=service --state=active
- Start SSH at boot
  - sudo update-rc.d ssh enable