Basic Linux Round 1 Checklist

Tips:

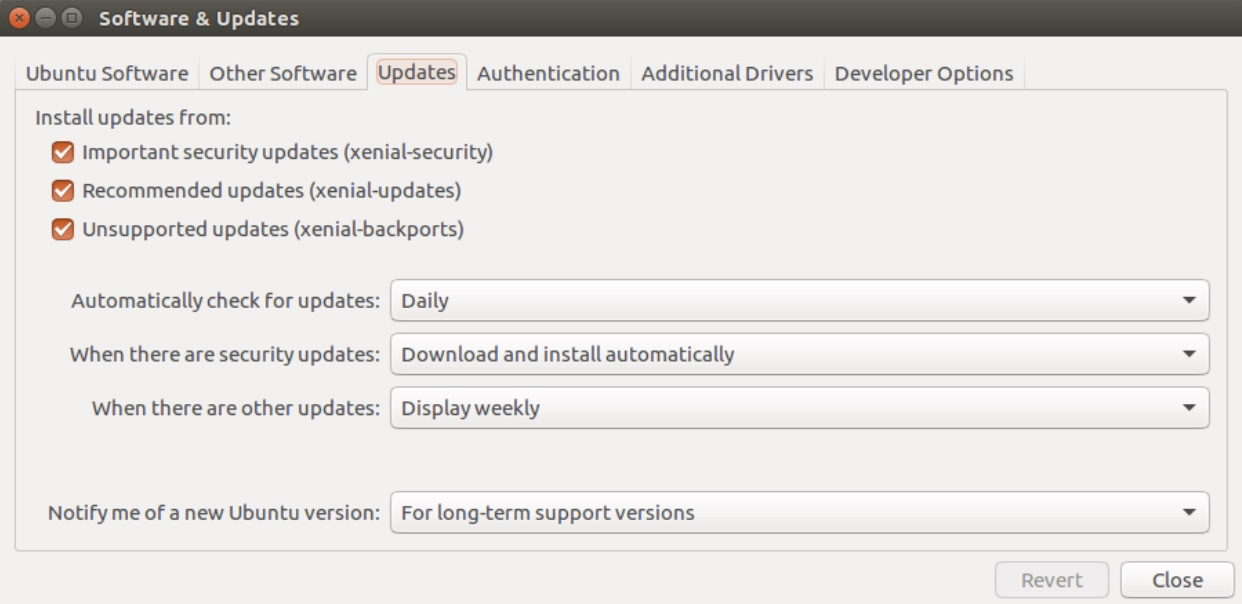
- Google is your friend (especially for forensics questions)

- If you don't have permission to run a command, use *sudo*

- Google services/packages before you remove them

- Don't rely solely on this checklist (Google "Linux security hardening checklist")!

1. Read the README thoroughly!
2. Perform updates (let them run in background)
   1. *sudo apt-get update; sudo apt-get upgrade*
3. Enable automatic updates
   1. **Settings -> Software & Updates -> Updates**

****

1. Users
   1. Use README for list of authorized users and administrators
   2. Delete a user: *sudo userdel [username]*
   3. Demote an unauthorized administrator: *sudo deluser [username] sudo; sudo deluser [username] adm*
   4. Change insecure passwords: *sudo passwd [username]*
2. Firewall
   1. *sudo ufw enable*
   2. *sudo ufw default deny incoming*
   3. *sudo ufw default allow outgoing*
3. PAM
   1. *sudo apt-get install libpam-cracklib*
   2. sudo gedit /etc/pam.d/common-password
      * At the end of the line with "pam\_cracklib.so": *retry=3 minlen=8 difok=8 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1*
   3. sudo gedit /etc/pam.d/common-auth
      * End of the file: *auth required pam\_tally2.so deny=5 onerr=fail unlock\_time=1800*
   4. sudo gedit /etc/login.defs
      * *PASS\_MAX\_DAYS 30*
      * *PASS\_MIN\_DAYS 10*
      * *PASS\_WARN\_AGE 7*
4. List services: *sudo service --status-all*
   1. Disable service: *sudo service [name] stop*
5. List packages: *sudo dpkg --get-selections*
   1. Remove package: *sudo apt-get remove [package]*
6. Remove suspicious files: *sudo rm -f [filename]*
   1. List of passwords, credit cards, other sensitive information
7. Configure critical services (ONLY if they're specified in the README)
   1. Use Google! (e.g. search "OpenSSH security hardening guide")
      * <https://www.tecmint.com/secure-openssh-server/>