Ultimate Linux Checklist

Make sure to write down your steps so you can backtrack/redo things if something goes wrong

Big thanks to Renee S. for the material this was based off.

1. Check system log files:
   a. Check /var/log/ logs
   b. Check /home/*/.bash_history and /home/*/.sh_history logs
2. See what software is installed
   a. Remove whatever is unnecessary
      i. Synaptic provides an in depth version, helpful for uninstalling programs you may not see in software center
         1. sudo apt-get install synaptic
         2. sudo synaptic
            a. Sort by installation type
   b. Check for common hacking tools
      i. Netcat, John the Ripper, Metasploit, Nmap, Nessus, Wireshark, etc.
3. Check cron for scheduled tasks in
   a. /var/spool/cron/crontabs
   b. /var/spool/anacron
4. Basic User Policy:
   a. Disable automatic logins (except for yourself, at least until you are done)
   b. Audit users and remove any unauthorized users, set strong passwd policy. NO GUEST!!!
      i. Check user privileges
         1. awk -F: ‘($3 == “0”{print}’ /etc/passwd
            a. Should only return root
         2. ls -l /etc/passwd
            a. Should only return root
      ii. Password Policy:
         1. Sudo apt-get install libpam -cracklib –force-yes -y
         2. Edit /etc/login.defs, change to
            a. PASS_MAX_DAYS 90
            b. PASS_MIN_DAYS 0
            c. PASS_WARN_AGE 7
         3. Edit /etc/pam.d/common-password
            a. In the line that contains “pam_unix.so”, add at the end:
               i. remember=5 minlen=8
            b. In the line that contains “pam_cracklib.so”, add at the end:
               i. ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
         4. Edit /etc/pam.d/common-auth
            a. At the end add:

i. auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800

c. Check the user groups
  i. In terminal, check: cat /etc/group
  ii. Sudo and admin groups should only contain admins/root
d. Remove root logon access
  i. Modify the /etc/securetty file
  ii. Edit root password
    1. sudo passwd root

5. Firewall
   a. If it is not installed:
     i. sudo apt-get install ufw
   b. Enable the Firewall:
     i. sudo ufw enable
   c. Check to ensure that it is running:
     i. sudo ufw status
   d. Modify permissions based on the services that you currently need
6. Anti-Malware/Rootkits
   a. Install Chkrootkit and Rkhunter
     i. sudo apt-get install rkhunter chkrootkit
   b. Run them:
     i. sudo chkrootkit
     ii. sudo rkhunter –check
     iii. If either come up with positives or warnings, research each thing that was flagged. Some things may be false positives
   c. Check /etc for suspicious/unusual programs
   d. Check for hidden files
   e. Check for prohibited media
     i. sudo find / -name “*.filetype” -type f
7. Auditing:
   a. Enable auditing:
     i. sudo apt-get install auditd
     ii. auditctl -e 1
   b. To view/edit policies go to:
     i. /etc/audit.d/auditd.conf
   c. If using SSH, you may want to check SSH failed attempts
     i. grep sshd.*Failed /var/log/auth.log | less
   d. HOSTS File:
     i. Check /etc/hosts file
     ii. Should only contain these lines:
       1. 127.0.0.1 localhost

            2. 127.0.1.1 ubuntu
            3. ::1 ip6-localhost ip6-loopback
            4. fe00::0 ip6-localnet
            5. ff00::0 ip6-mcastprefix
            6. ff02::1 ip6-allnodes
            7. ff02::2 ip6-allrouters

8. Services:
    - a. GUI:
        - i. Install Bum
            - 1. sudo apt-get install bum
            - 2. sudo bum
        - ii. Check the services that are running
    - b. Terminal:
        - i. Run:
            - 1. service –status-all
        - ii. To stop a service:
            - 1. service stop service
9. Ports
    - a. To see active ports:
        - i. sudo ss -ln
    - b. Necessary ports:
        - i. 80 & 443 (https, https)
    - c. Potential threats:
        - i. 20-21, 23, 135, 411-412 (ftp, telnet, remote desktop, peer-peer)
    - d. To close a port:
        - i. sudo lsof -I :$port
10. Server Configurations:
    - a. Apache 2
        - i. Edit apache2.conf
            - 1. TraceEnable off
            - 2. Leaving on could allow hacker to steal cookie info
            - 3. User apache
            - 4. Don’t let apache run as root
            - 5. Group apache
            - 6. Don’t let apache run as root
            - 7. ServerSignature Off
            - 8. ServerTokens Prod
            - 9. <Directory /var/www/html>
            - 10. Options -Indexes
            - 11. </Directory>
            - 12. Options -FollowSymLinks
            - 13. Options -Includes
            - 14. Options -ExecCGI

11. Directory Permissions:
    a. /tmp – World Writable
    b. /var/tmp – World Writable
    c. /boot/grub(2) – Read, write by root

Other things that you may want to do:

- Disable automounting (USBs, similar devices are physical threats)