Basic Security Checklist – Ubuntu Linux Focus

- Remember to run multiple tasks at once – except for installation of software!
- Antivirus (clamav)
    - Update database – sudo apt-get update
    - Install ClamAV – sudo apt-get install clamav
    - Update virus database – sudo freshclam
    - Check entire system for viruses – sudo clamscan –i –r --remove=yes /
        - Run this in a separate terminal as it will take a while
- Users
    - Change passwords - sudo passwd <USER>
    - Enable account – sudo passwd –u <USER>
    - Disable accounts – sudo passwd –l <USER>
        - Always disable root account after changing password
    - Change administrator privileges (sudo)
        - sudo visudo
    - Add a user – sudo adduser <USER>
    - Delete a user – sudo deluser --remove-home <USER>
    - Checking groups – sudo cat /etc/group
    - Where are passwords stored - /etc/passwd and /etc/shadow
- Firewall (ufw – disabled by default)
    - Enable firewall – sudo ufw enable
    - Disable firewall – sudo ufw disable
    - Status – sudo ufw status
        - Add verbose for more information (sudo ufw status verbose)
    - Allow protocol through – sudo ufw allow <PORT>
        - Can use name as well as number (ssh, ftp, telnet)
    - Deny a protocol – sudo ufw deny <PORT>
    - Look at applications available for rules – sudo ufw app list
    - Activate TCP SYN Cookie Protection (protects from some DOS attacks)
        - sudo nano /etc/sysctl.conf
        - change net.ipv4.tcp_syncookies entry from 0 to 1
- Removing applications
    - List installed applications – sudo dpkg --get –selections
    - Look for particular application - sudo dpkg --get –selections | grep <APP>
        - Common ones to look for: telnet; ftp; vnc; nfs, apache
    - Remove an application – sudo apt-get purge <APP>
        - Pay attention to daemon programs (ends in d)
        - Sometimes you have to remove more than one entry
    - Finding where a process is running from (replace pid with process number)
- sudo ls -l /proc/<pid>/exe

Update the system
    - Automatically check for updates
    - sudo nano /etc/apt/apt.conf.d/10periodic
        - Change to 1 – APT::Periodic::Update-Package-Lists
    - sudo apt-get dist-upgrade (typically requires a reboot)
    - Keep current version of configuration files unless scenario dictates otherwise if asked
- Find processes that are listening (sudo netstat –tulnp)
    - Use process identification number (PID)
    - Look for common programs (apache, ftp, telnet, nc)
    - Remove process – sudo kill <PID>
- Programs that start automatically (rc.local)
    - Edit the file – sudo nano /etc/init.d/rc.local
    - Another location – sudo crontab -e
    - Look in /etc/cron.d
    - You can also look to see what is automatically starting
        - Install chkconfig application (sudo apt-get install chkconfig)
        - sudo chkconfig --list | grep '3:on'
- Password settings (login.defs)
    - Edit the file – sudo nano /etc/login.defs
        - Key areas – PASS_MAX_DAYS, PASS_MIN_DAYS, PASS_WARN_AGE
    - Using libpam-cracklib
        - sudo apt-get install libpam-cracklib
        - sudo nano /etc/pam.d/common-password
            - Add at end of pam_unix.so line
                - remember=5
            - Add at end of pam_cracklib.so line
                - ucredit=1 lcredit=1 dcredit=1 ocredit=1
- Do not allow root account to login in using SSH! (sshd_config)
    - Edit the file – sudo nano /etc/ssh/sshd_config
        - Look for PermitRootLogin and set to no
- Do not allow automatic login
    - sudo nano /etc/lightdm/lightdm.conf
        - Remove line with autologin-user
        - Add the following line to disable guest account: allow_guest=false
- Services
    - List all services – sudo service --status-all
    - Remove service – sudo apt-get --purge <SERVICENAME>
- Finding Files – locate command
    - First update index – sudo updatedb
    - Search for a file name – locate <STRING>
        - Example: locate *.ogg