Linux checklist:

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

Allow protocol through – sudo ufw allow <PORT>

Can use name as well as number (ssh, ftp, telnet)

Deny a protocol – sudo ufw deny <PORT>

Removing applications

List installed applications – sudo dpkg --get –selections

Look for particular application - sudo dpkg --get –selections | grep <APP>

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

o Finding where a process is running from (replace pid with process number)

sudo ls -l /proc/<pid>/exe

Update the system

Find processes that are listening (sudo netstat –tulnp)

Use process identification number (PID)

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

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>

Remove anonymous log-in on FTP

Change default passwords on FTP, SSH….