Linux Checklist

Read the scenario document **FIRST**

Read the forensic questions **SECOND and work to complete**

User Administration (add /remove/ modify)

Make sure to strengthen weak passwords

Remove any un-needed packages/apps

Remove any files described as (usually media files) undesired

Check for any ports that are listening that seem suspicious
netstat -atulpn. (review the man page for what these options do)
This must be run as root. Pay attention to the Program Name listed.

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Disable the guest account
* Edit the lighted.conf (in etc/lightdm/lightdm.conf)
* Add the line : allow-guest=false

FireFox update
* sudo apt-get update && sudo apt-get install firefox

Review Firefox security settings

Disable Root Login vis SSH
* Edit the file vi **/etc/ssh/sshd_config**
  Update the Line: PermitRootLogin no

Review these other settings:

- PermitRootLogin no # disallows root access via SSH
- AllowUsers [username] # limits SSH access to the stated users

- IgnoreRhosts yes # disallows SSH from trusting a host based only on its IP
- HostbasedAuthentication no # as above
- PermitEmptyPasswords no # prevents users from logging into SSH with an empty password, if set as such
- X11Forwarding no # stops the possiblity of the server sending commands back to the client
- MaxAuthTries 5 # drops the SSH connection after 5 failed authorization attempts
- Ciphers aes128-ctr,aes192-ctr,aes256-ctr # disable weak ciphers
- UsePAM yes # disables password authentication and defers authorization to the key-based PAM
- ClientAliveInterval 900 # logs out idle users after 15 minutes
- ClientAliveCountMax 0 # how many times the server checks whether the session is active before dropping

To only allow certain users: add **AllowUsers** username

Enable the Firewall
* Sudo enable **ufw**
* Review the default policy and modify as needed

Check that the rc.local in (/etc) is empty

Update the /etc/login.defs
* PASS_MAX_DAYS
* PASS_MIN_DAYS
* PASS_WARN_DAYS

Remove Samba File Share
* sudo apt-get purge samba

Remove Telnet
apt-get remove telnet

Disable ftp (insecure)

- Install **vsftp** and start up vsftpd

Verify the nonsecure protocol apps aren’t running:

- ftpd

Check the sudoers file using **visudo**

Check the /etc/group file and make sure that the only users listed as part of the sudo group are admins

Check the crontab to verify that there is no rogue jobs running
Crontab -e (to edit the crontab)

This might or might not have points: echo ALL >>/etc/cron.deny (excluded everyone from running cron jobs)

Lock a users account

```
passwd -l accountName
```

System update

```
apt-get update && apt-get upgrade
```

Restrict users password use

```
# vi /etc/pam.d/common-password
```

Add this auth section : auth   sufficient   pam_unix.so likeauth nullok
Add this to the password section : password   sufficient   pam_unix.so nullok use_authtok md5 shadow remember=5

Enforce strong passwords

```
# vi /etc/pam.d/system-auth
/lib/security/$ISA/pam_cracklib.so retry=3 minlen=8 lcredit=-1
ucredit=-2 dcredit=-2 ocredit=-1
```

Need to have pam_cracklib.so on the system to make this work

Check for empty password

```
# cat /etc/shadow | awk -F: '($2==""){print $1}'
```

Ignore ICMP / Broadcast requests

Add following line in “/etc/sysctl.conf” file to ignore ping or broadcast request.

Ignore ICMP request:
net.ipv4.icmp_echo_ignore_all = 1

Ignore Broadcast request:
net.ipv4.icmp_echo_ignore_broadcasts = 1

Then execute: **sysctl -p**

Check the running processes: .. trying to spot something unusual

- ps -fe (can used with less) .. so: **ps -fe | less**

Enable auditd
apt-get install auditd … Start the service with /etc/init.d/auditd start

Scan for RootKits on the system
apt-get install chkrootkit
Run **chkrootkit** as root.

Make sure apparmor is installed.

Securing Ubuntu 14 - https://www.maketecheasier.com/hardening-ubuntu-server/

Other links Linux Security links :
https://www.process.st/server-security/
https://www.cyberciti.biz/tips/linux-security.html