Ubuntu/Linux Checklist

- ❏ **Take notes on the README file**
- ❏ **Answer the Forensics Questions (Look at how-to’s section on end of document)**
- ❏ **Install Antivirus & Anti Malware Applications**
  - ❏ Install Linux Malware Detect (LMD):
    - ❏ Open this link: https://www.rfxn.com/projects/linux-malware-detect/
    - ❏ Click on the first embedded link under “Current Release:”.
  - ❏ Install AVG Anti-Virus:
    - ❏ Open this link: https://www.avg.com/en-us/homepage
    - ❏ Click on the “FREE Download” button.

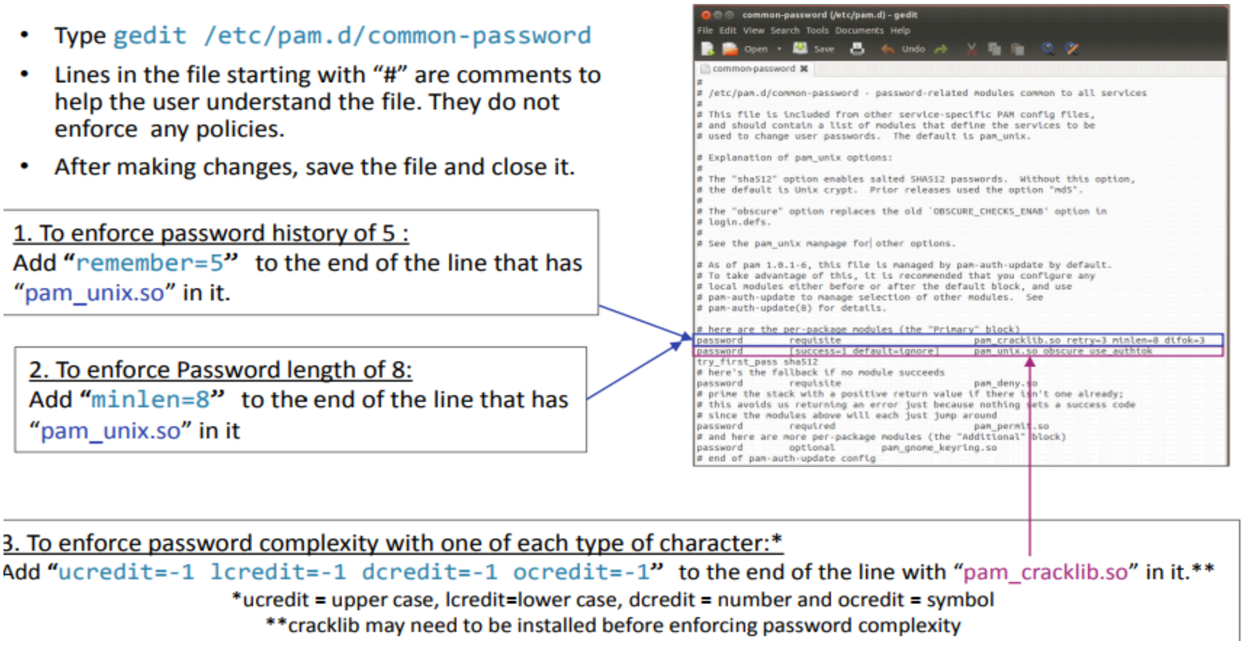
- ❏ **Change Root Password**
  - ❏ Click the Ubuntu button, type in “Terminal”, & press enter. Terminal should open.
  - ❏ Type in “sudo -i passwd”, & follow the directions to change the password for root.

- ❏ **Check for Scheduled Malicious Software**
  - ❏ Click the Ubuntu button, type in “Terminal”, & press enter. Terminal should open.
  - ❏ Type in “gedit /var/spool/cron/crontabs”

- ❏ **Check System Logs (Similar to Event Viewer in Windows 10 & Server 2016)**
  - ❏ Click the Ubuntu button, type in “System Logs”, & press enter. Logs should open.
  - ❏ Check each of the 4 logs: Auth.log (Tracks authentication events that prompt for user passwords), Dpkg.log (Tracks software events), Syslog (Tracks operating system events - Can mostly be ignored), & Xorg.0.log (Tracks desktop events).

- ❏ **Change Security Policies**
  - ❏ Install Cracklib:
    - ❏ Click the Ubuntu button, type “Terminal”, & press enter. Terminal should open.
    - ❏ In Terminal, type in “sudo apt-get install libpam-cracklib --force-yes -y”.
  - ❏ Change Password Policies:
    - ❏ Change Password Aging Controls:
      - ❏ Type in “gedit /etc/login.defs”.
      - ❏ Press CTRL+F and type “Password Aging Controls” in the find box.
      - ❏ Change “PASS_MAX_DAYS” to 90.
      - ❏ Change “PASS_MIN_DAYS” to 10.
      - ❏ Change “PASS_WARN_AGE” to 7.
      - ❏ Finally, click the “Save” button to save changes.
    - ❏ Change Password Criteria:
      - ❏ Type in “gedit /etc/pam.d/common-password” (Must be root to edit).
      - ❏ To enforce a password history of 5: Add “remember=5” to the end of the line that has pam_cracklib.so

- ❑ To enforce Password length of 8: Add minlen=8 to the end of the line that has pam-cracklib.so
- ❑ To enforce password complexity with one of each type of character: Add “ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1” to the end of the line with pam_unix.so.
- ❑ Lastly, click the “Save” button to save changes.
- ❑ Here is a walkthrough image (Note: Refer to the arrows, not the text):



- Type gedit /etc/pam.d/common-password
- Lines in the file starting with “#” are comments to help the user understand the file. They do not enforce any policies.
- After making changes, save the file and close it.

1. To enforce password history of 5 :
Add “remember=5” to the end of the line that has “pam_unix.so” in it.

2. To enforce Password length of 8:
Add “minlen=8” to the end of the line that has “pam_unix.so” in it

common-password (/etc/pam.d) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
common-password

```
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords.  Without this option,
# the default is Unix crypt.  Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_cracklib.so retry=3 minlen=8 difok=3
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok
try_first_pass sha512
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

3. To enforce password complexity with one of each type of character:*
Add “ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1” to the end of the line with “pam_cracklib.so” in it.**

*ucredit = upper case, lcredit=lower case, dcredit = number and ocredit = symbol

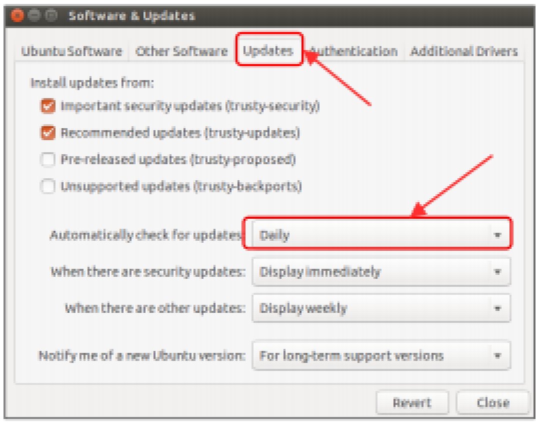
**cracklib may need to be installed before enforcing password complexity

- ❑ Change Account Lockout Policies:
  - ❑ Type in “gedit /etc/pam.d/common-auth”
  - ❑ At the end of the file, add the line “auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800”.
  - ❑ Finally, click the “Save” button to save changes.

- ❑ **Change Audit Policies**
  - ❑ Click the Ubuntu button, type in “Terminal”, & press enter. Terminal should open.
  - ❑ In Terminal, type in “sudo apt-get install auditd”.
  - ❑ Then, type in “auditctl -a exit,always -S open”. Auditing should begin.

- ❑ **Enable Firewall**
  - ❑ Click on this link: http://www.gufw.org
  - ❑ Click on “Ubuntu Installer”. GUFW (Graphical Uncomplicated Firewall) should open.
  - ❑ Click the Ubuntu button, type in “gufw”, & press enter. Firewall Config should open.
  - ❑ Click the button that says “Status:” to turn on firewall.
  - ❑ Make sure “Incoming” is set to “Deny” & “Outgoing” is set to “Allow”.

- ❑ **Install & Configure Updates**
    - ❑ <u>Install Updates:</u>
        - ❑ Click the Ubuntu button, type in “Update Manager”, & press enter. Update manager should open & start checking for updates.
    - ❑ <u>Configure Updates:</u>
        - ❑ Next, click the Ubuntu button, type in “Software & Updates”, & press enter. Update Settings should open.
        - ❑ Under “Ubuntu Software”, check “Canonical-supported free and open-source software” & “Community-maintained free and open-source software”, & if not mentioned about in the README, also check “Proprietary drivers for devices” & “Software restricted by copyright or legal issues”.
        - ❑ Under “Other Software”, check “Canonical Partners” & “Canonical Partners (Source Code)”, & if not mentioned in the README, also check “Independent” & “Independent (Source Code)” if available.
        - ❑ Under “Updates”, edit it so that the screen looks like the picture below:



Install updates from:

☑ Important security updates (trusty-security)
☑ Recommended updates (trusty-updates)
☐ Pre-released updates (trusty-proposed)
☐ Unsupported updates (trusty-backports)

Automatically check for updates: Daily
When there are security updates: Display immediately
When there are other updates: Display weekly
Notify me of a new Ubuntu version: For long-term support versions

- ❑ **Disable Guest Account**
    - ❑ Click the Ubuntu button, type in “Terminal”, & press enter. Terminal should open.
        - ❑ In Terminal, type in “gedit /etc/lightdm/lightdm.conf”.
        - ❑ Add the line “allow-guest=false” to the end of the file, & click the “Save” button.

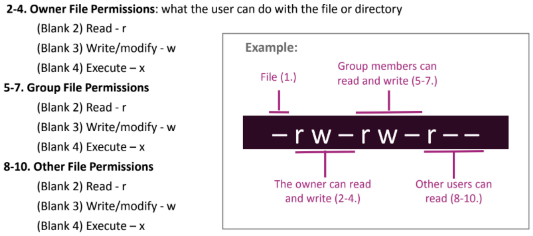
- ❑ **Update/Upgrade Image: (Only after everything else is done)**
    - ❑ Click the Ubuntu button, type in “Terminal”, & press enter. Terminal should open.
    - ❑ In Terminal, type in “sudo apt-get update” & “sudo apt-get upgrade”.

- ❑ **Find & delete Prohibited Files**
    - ❑ Click the Ubuntu button, type in “Terminal”, & press enter. Terminal should open.
    - ❑ Type in “sudo find / -name “*.[file extension]” -type f”. Extensions worth searching for are: mp3, wav, wmv, mp4, mpeg, & mep.
    - ❑ Then type in “sudo find /home -name “*.[file extension]” -type f”. Extensions worth searching for are: jpeg, jpg, png, gif, tif, and tiff.
    - ❑ To delete a file, type in “sudo rm -f [file with path]”.

Ubuntu/Linux How-To’s

- ❑ **How to add/remove a user/group:**
    - ❑ Add a user/group:
        - ❑ Click the Ubuntu button, type “Terminal”, & press enter. Terminal should open.
        - ❑ Add user:
            - ❑ Type in “sudo userdel [name of user] [group name - optional]”
        - ❑ Add group:
            - ❑ Type in “sudo addgroup [name of group]”
    - ❑ Remove a user or group:
        - ❑ Click the Ubuntu button, type “Terminal”, & press enter. Terminal should open.
        - ❑ Remove user:
            - ❑ Type in “sudo adduser [name of user]”
        - ❑ Remove group:
            - ❑ Type in “sudo groupdel [name of group]”

- ❑ **How to change/view file permissions**
    - ❑ View Permissions:
        - ❑ Click the Ubuntu button, type “Terminal”, & press enter. Terminal should open.
        - ❑ Type “ls -l [file with path]” to see file permissions for that file. This is how the output should look like & how to understand the output:



2-4. Owner File Permissions: what the user can do with the file or directory

(Blank 2) Read - r

(Blank 3) Write/modify - w

(Blank 4) Execute – x

5-7. Group File Permissions

(Blank 2) Read - r

(Blank 3) Write/modify - w

(Blank 4) Execute – x

8-10. Other File Permissions

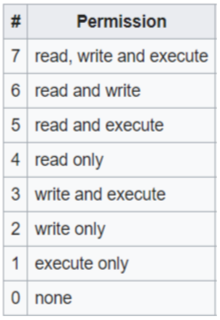
(Blank 2) Read - r

(Blank 3) Write/modify - w

(Blank 4) Execute – x

Example:
File (1.)
Group members can read and write (5-7.)
–rw–rw–r––
The owner can read and write (2-4.)
Other users can read (8-10.)

- ❑ Edit Permissions (CHMOD):
    - ❑ Click the Ubuntu button, type “Terminal”, & press enter. Terminal should open.
    - ❑ Type “chmod [permissions] [file name]”, where file name is the name of the file & permissions is either a 3 digit number or some text representing the permissions. Using text, you would write “u=”, “,g=”, & “,o=” with a combination of r, w, & x after each equal sign. Example: “chmod u=rwx, g=rwx, o=r file_name.extension”. Using numbers, the first number is the permissions of the user, the second is for the group, & the third is for others. Each number from 1 - 7 represents a permission, as per the table on the right. Example: “chmod 774 file_name.extension”. If, for a file named myfile.txt, the user can read, write, & execute, the group can read & execute, & others can only read the file, then the code can be “chmod u=rwx,g=rx,o=r myfile.txt” or “chmod 754 myfile.txt”.



#	Permission
7	read, write and execute
6	read and write
5	read and execute
4	read only
3	write and execute
2	write only
1	execute only
0	none