###FYI, SOME OF THESE COMMANDS I RAN USING ROOT --- SUDO SU ###

## Week 4 Homework Submission File: Linux Systems Administration

### Step 1: Ensure Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.

    - Command to inspect permissions: ls -l shadow

    - Command to set permissions (if needed): chmod 600 shadow

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.

    - Command to inspect permissions: ls -l gshadow

    - Command to set permissions (if needed):chmod 600 gshadow

3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.

    - Command to inspect permissions:ls -l group

    - Command to set permissions (if needed): chmod 644 group

4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.

    - Command to inspect permissions: ls -l passwd

    - Command to set permissions (if needed):chmod 644 passwd

### Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin`.

    - Command to add each user account (include all five users):adduser sam, adduser joe, adduser amy, adduser sara, adduser admin

2. Force users to create 16-character passwords incorporating numbers and symbols.

    - Command to edit `pwquality.conf` file: nano pwquality.conf (while in the dir)

    - Updates to configuration file: I set (difok = 2, minlen =16, dictcheck = 1, minclass = 4

3. Force passwords to expire every 90 days.

- Command to to set each new user's password to expire in 90 days (include all five users): sudo chage - M 90 sam/joe/amy/sara/admin (typed names separately)

4. Ensure that only the `admin` has general sudo access.

    - Command to add `admin` to the `sudo` group: usermod -G sudo admin

### Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.

    - Command to add group:addgroup engineers

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.

    - Command to add users to `engineers` group (include all four users):usermod -a -G engineers sam/joe/amy/sara (typed individually)

3. Create a shared folder for this group at `/home/engineers`.

    - Command to create the shared folder: while in /home/ typed "mkdir -p engineers"

4. Change ownership on the new engineers' shared folder to the `engineers` group.

    - Command to change ownership of engineer's shared folder to engineer group: sudo chown :engineers /home/engineers

5. Add the SGID bit and the sticky bit to allow collaboration between engineers in this directory.

    - Command to set SGID and sticky bit to shared folder: sudo chmod +s /home/engineers AND sudo chmod o+t engineers/

### Step 4: Lynis Auditing

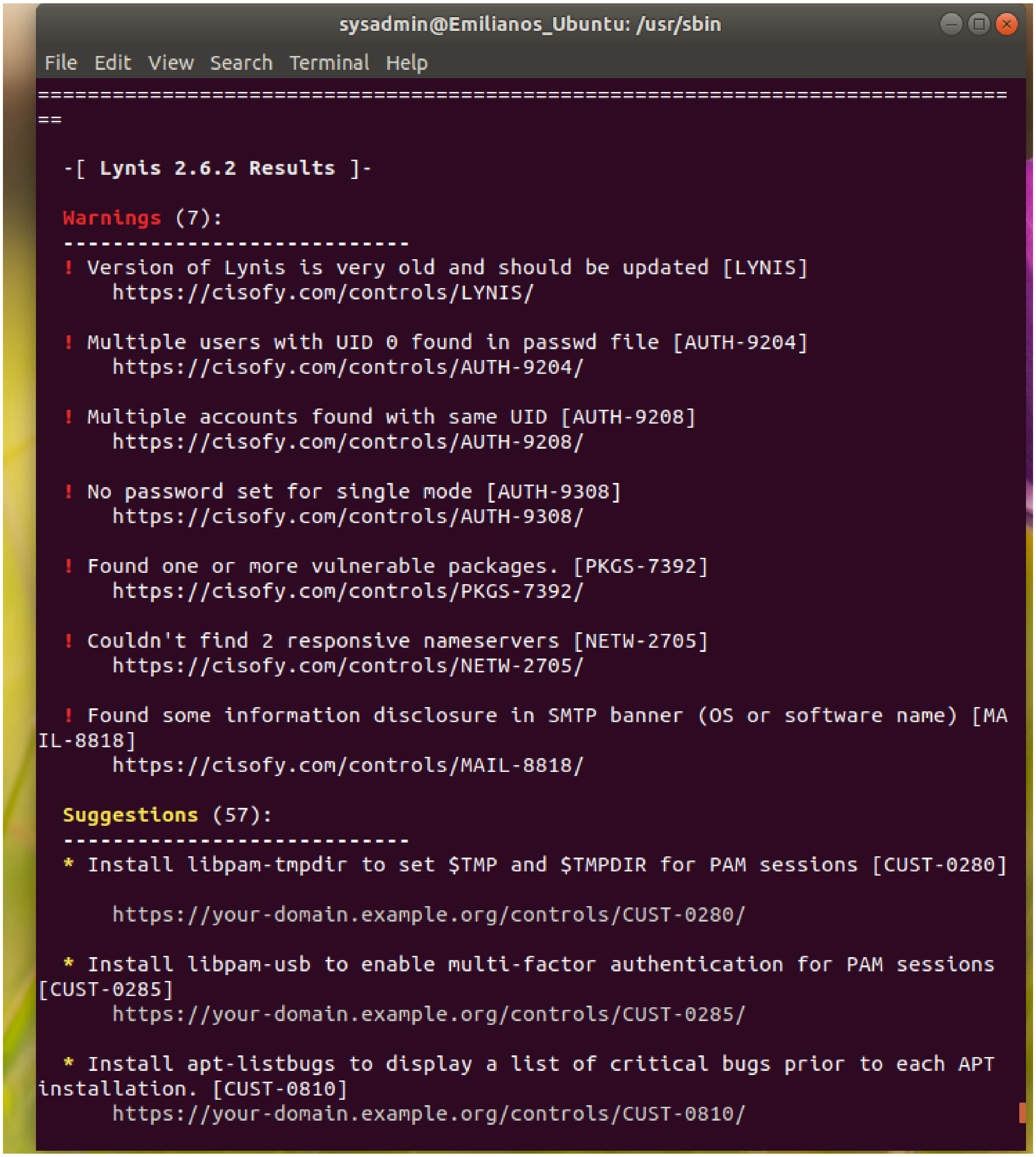
1. Command to install Lynis: apt-get install lynis

2. Command to see documentation and instructions: man lynis

3. Command to run an audit: sudo lynis audit system

4. Provide a report from the Lynis output on what can be done to harden the system.

    - Screenshot of report output:


sysadmin@Emilianos_Ubuntu: /usr/sbin
File Edit View Search Terminal Help

```
================================================================================
==

  -[ Lynis 2.6.2 Results ]-

  Warnings (7):
  ----------------------------
  ! Version of Lynis is very old and should be updated [LYNIS]
      https://cisofy.com/controls/LYNIS/

  ! Multiple users with UID 0 found in passwd file [AUTH-9204]
      https://cisofy.com/controls/AUTH-9204/

  ! Multiple accounts found with same UID [AUTH-9208]
      https://cisofy.com/controls/AUTH-9208/

  ! No password set for single mode [AUTH-9308]
      https://cisofy.com/controls/AUTH-9308/

  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/controls/PKGS-7392/

  ! Couldn't find 2 responsive nameservers [NETW-2705]
      https://cisofy.com/controls/NETW-2705/

  ! Found some information disclosure in SMTP banner (OS or software name) [MA
IL-8818]
      https://cisofy.com/controls/MAIL-8818/

  Suggestions (57):
  ----------------------------
  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]

      https://your-domain.example.org/controls/CUST-0280/

  * Install libpam-usb to enable multi-factor authentication for PAM sessions
[CUST-0285]
      https://your-domain.example.org/controls/CUST-0285/

  * Install apt-listbugs to display a list of critical bugs prior to each APT
installation. [CUST-0810]
      https://your-domain.example.org/controls/CUST-0810/
```

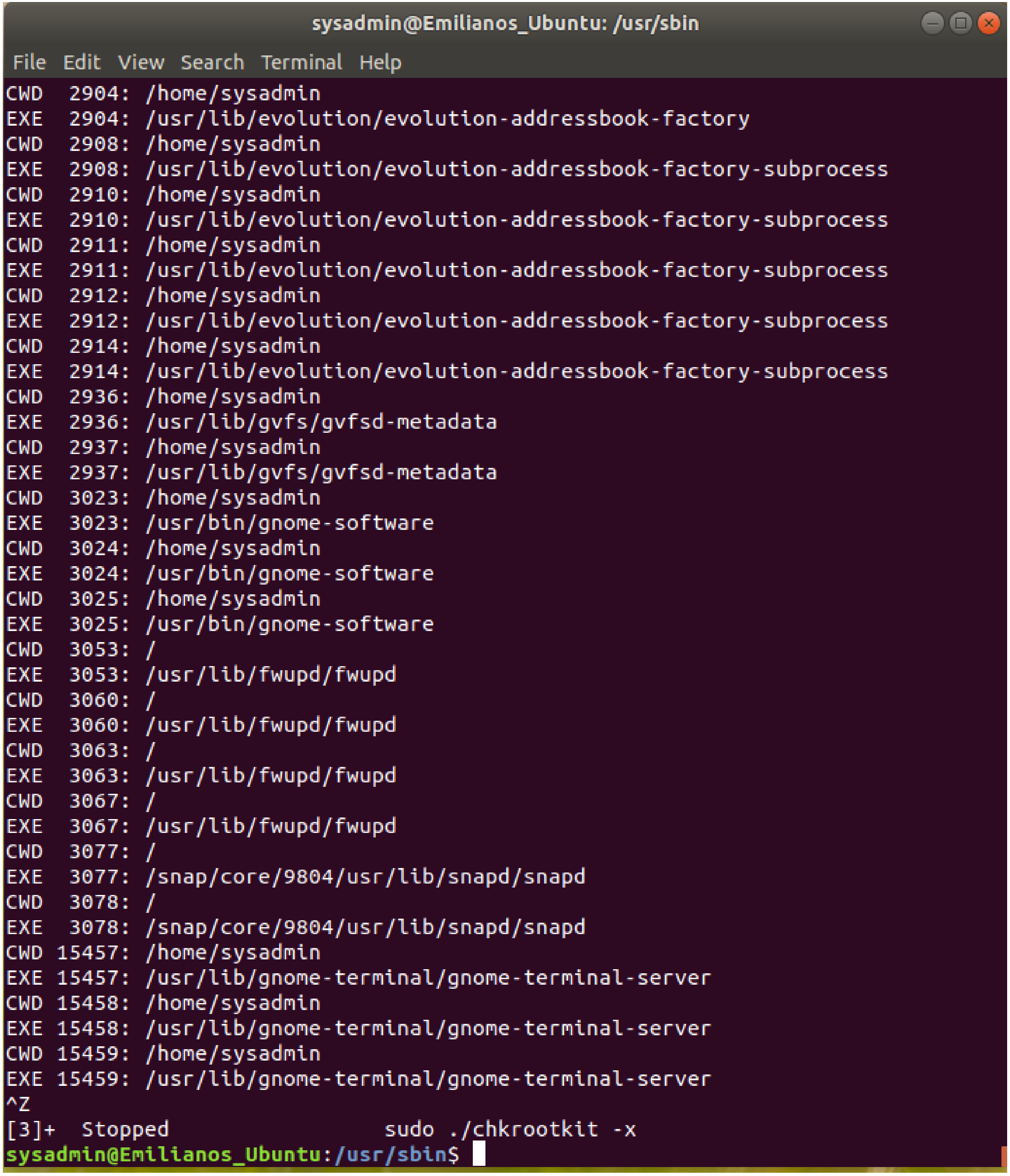
### Bonus
1. Command to install chkrootkit: sudo apt-get install chkrootkit

2. Command to see documentation and instructions: man chkrootkit

3. Command to run expert mode: sudo ./chkrootkit -x

4. Provide a report from the chrootkit output on what can be done to harden the system.

- Screenshot of end of sample output:



sysadmin@Emilianos_Ubuntu: /usr/sbin
File Edit View Search Terminal Help

```
CWD  2904: /home/sysadmin
EXE  2904: /usr/lib/evolution/evolution-addressbook-factory
CWD  2908: /home/sysadmin
EXE  2908: /usr/lib/evolution/evolution-addressbook-factory-subprocess
CWD  2910: /home/sysadmin
EXE  2910: /usr/lib/evolution/evolution-addressbook-factory-subprocess
CWD  2911: /home/sysadmin
EXE  2911: /usr/lib/evolution/evolution-addressbook-factory-subprocess
CWD  2912: /home/sysadmin
EXE  2912: /usr/lib/evolution/evolution-addressbook-factory-subprocess
CWD  2914: /home/sysadmin
EXE  2914: /usr/lib/evolution/evolution-addressbook-factory-subprocess
CWD  2936: /home/sysadmin
EXE  2936: /usr/lib/gvfs/gvfsd-metadata
CWD  2937: /home/sysadmin
EXE  2937: /usr/lib/gvfs/gvfsd-metadata
CWD  3023: /home/sysadmin
EXE  3023: /usr/bin/gnome-software
CWD  3024: /home/sysadmin
EXE  3024: /usr/bin/gnome-software
CWD  3025: /home/sysadmin
EXE  3025: /usr/bin/gnome-software
CWD  3053: /
EXE  3053: /usr/lib/fwupd/fwupd
CWD  3060: /
EXE  3060: /usr/lib/fwupd/fwupd
CWD  3063: /
EXE  3063: /usr/lib/fwupd/fwupd
CWD  3067: /
EXE  3067: /usr/lib/fwupd/fwupd
CWD  3077: /
EXE  3077: /snap/core/9804/usr/lib/snapd/snapd
CWD  3078: /
EXE  3078: /snap/core/9804/usr/lib/snapd/snapd
CWD 15457: /home/sysadmin
EXE 15457: /usr/lib/gnome-terminal/gnome-terminal-server
CWD 15458: /home/sysadmin
EXE 15458: /usr/lib/gnome-terminal/gnome-terminal-server
CWD 15459: /home/sysadmin
EXE 15459: /usr/lib/gnome-terminal/gnome-terminal-server
^Z
[3]+  Stopped                  sudo ./chkrootkit -x
sysadmin@Emilianos_Ubuntu:/usr/sbin$ 
```
