Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.
    - Command to inspect permissions: sudo ls -la shadow
    - Command to set permissions (if needed): sudo chmod 600
2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
    - Command to inspect permissions: sudo ls -la gshadow
    - Command to set permissions (if needed): sudo chmod 600
3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.
    - Command to inspect permissions: sudo ls -la group
    - Command to set permissions (if needed): sudo 644
4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.
    - Command to inspect permissions: sudo ls -la passwd
    - Command to set permissions (if needed): sudo chmod 644

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):
    - Sudo adduser sam
    - Sudo adduser joe
    - Sudo adduser amy
    - Sudo adduser sara
    - Sudo adduser admin
2. Ensure that only the `admin` has general sudo access.
    - Command to add `admin` to the `sudo` group: sudo usermod -aG sudo admin
    - Sudo cat /etc/sudoers

Step 3: Create User Group and Collaborative Folder

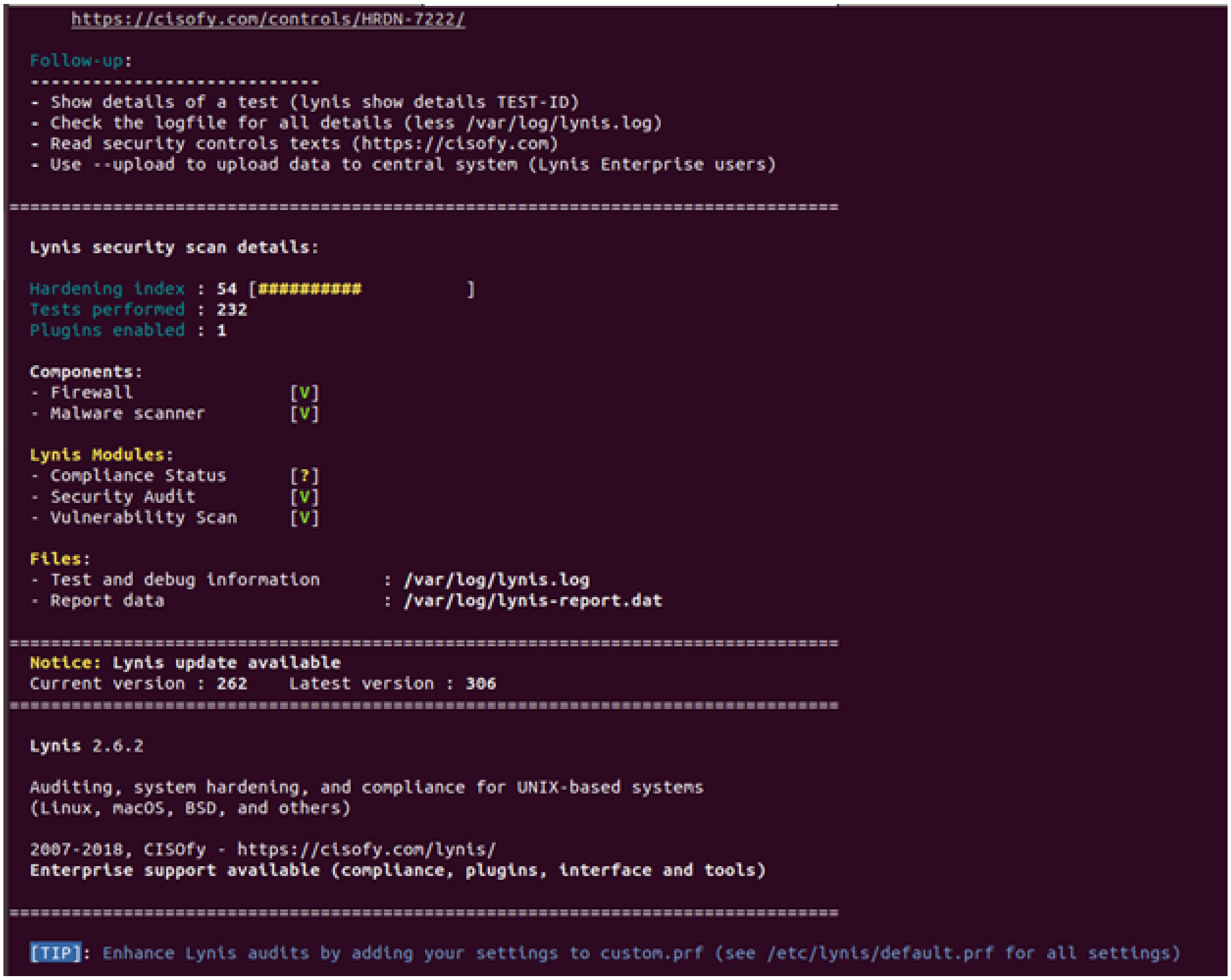
1. Add an `engineers` group to the system.
    - Command to add group: sudo addgroup engineers
2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.
    - Command to add users to `engineers` group (include all four users):
    - Sudo -a -G engineers sam joe amy sara
3. Create a shared folder for this group at `/home/engineers`.
    - Command to create the shared folder:
    - sudo mkdir /home/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

Step 4: Lynis Auditing

1. Command to install Lynis: sudo apt intall lynis
2. Command to see documentation and instructions: man lynis
3. Command to run an audit: lynis audit system
4. Provide a report from the Lynis output on what can be done to harden the system.
    - Screenshot of report output:

Based on the lynis report, we can update the current version installed to the latest version that is out.

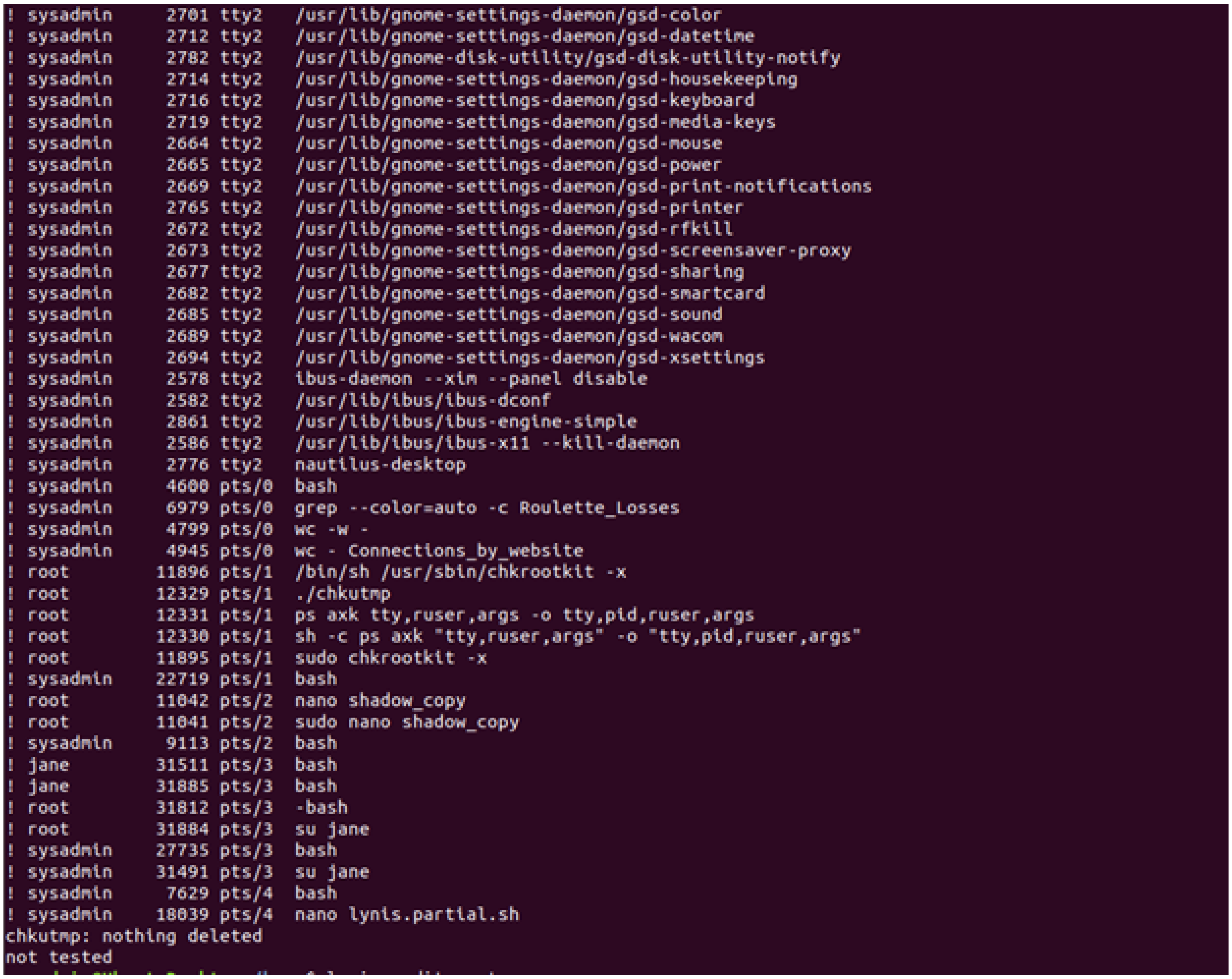


```
      https://cisofy.com/controls/HRDN-7222/

  Follow-up:
  ----------------------------
  - Show details of a test (lynis show details TEST-ID)
  - Check the logfile for all details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data to central system (Lynis Enterprise users)

================================================================================

  Lynis security scan details:

  Hardening index : 54 [##########          ]
  Tests performed : 232
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [V]

  Lynis Modules:
  - Compliance Status      [?]
  - Security Audit         [V]
  - Vulnerability Scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================
  Notice: Lynis update available
  Current version : 262    Latest version : 306
================================================================================

  Lynis 2.6.2

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
```

Bonus

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

Based on the chrootkit report, we can change permissions to some users.



```
! sysadmin     2701 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     2712 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     2782 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     2714 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     2716 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     2719 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     2664 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     2665 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     2669 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     2765 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     2672 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     2673 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     2677 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     2682 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2685 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2689 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2694 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2578 tty2   ibus-daemon --xim --panel disable
! sysadmin     2582 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2861 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2586 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2776 tty2   nautilus-desktop
! sysadmin     4600 pts/0  bash
! sysadmin     6979 pts/0  grep --color=auto -c Roulette_Losses
! sysadmin     4799 pts/0  wc -w -
! sysadmin     4945 pts/0  wc - Connections_by_website
! root        11896 pts/1  /bin/sh /usr/sbin/chkrootkit -x
! root        12329 pts/1  ./chkutmp
! root        12331 pts/1  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        12330 pts/1  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        11895 pts/1  sudo chkrootkit -x
! sysadmin    22719 pts/1  bash
! root        11042 pts/2  nano shadow_copy
! root        11041 pts/2  sudo nano shadow_copy
! sysadmin     9113 pts/2  bash
! jane        31511 pts/3  bash
! jane        31885 pts/3  bash
! root        31812 pts/3  -bash
! root        31884 pts/3  su jane
! sysadmin    27735 pts/3  bash
! sysadmin    31491 pts/3  su jane
! sysadmin     7629 pts/4  bash
! sysadmin    18039 pts/4  nano lynis.partial.sh
chkutmp: nothing deleted
not tested
```