Week 4 Homework Submission File: Linux Systems Administration

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:
    - Command to set permissions (if needed):

```
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow
-rw------- 1 root shadow 3477 Dec 15 14:18 /etc/shadow
sysadmin@UbuntuDesktop:~$
```

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
    - Command to inspect permissions:
    - Command to set permissions (if needed):

```
sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow
-rw------- 1 root shadow 1135 Dec 15 14:21 /etc/gshadow
```

3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.
    - Command to inspect permissions:
    - Command to set permissions (if needed):

```
sysadmin@UbuntuDesktop:~$ ls -l /etc/group
-rw----r-- 1 root root 1380 Dec 15 14:21 /etc/group

sysadmin@UbuntuDesktop:~$ sudo chmod 644 /etc/group
sysadmin@UbuntuDesktop:~$ ls -l /etc/group
-rw-r--r-- 1 root root 1380 Dec 15 14:21 /etc/group
```

4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.
    - Command to inspect permissions:
    - Command to set permissions (if needed):

```
sysadmin@UbuntuDesktop:~$ sudo chmod 644 /etc/passwd
sysadmin@UbuntuDesktop:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 3358 Dec 15 14:18 /etc/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):

```
sysadmin@UbuntuDesktop:/home$ sudo adduser sam
Adding user `sam' ...
Adding new group `sam' (1014) ...
Adding new user `sam' (1007) with group `sam' ...
Creating home directory `/home/sam' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sam
Enter the new value, or press ENTER for the default
        Full Name []: Sam
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

```
sysadmin@UbuntuDesktop:/home$ sudo adduser joe
Adding user `joe' ...
Adding new group `joe' (1015) ...
Adding new user `joe' (1013) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for joe
Enter the new value, or press ENTER for the default
```

```
        Full Name []: Joe
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

```
sysadmin@UbuntuDesktop:/home$ sudo adduser amy
Adding user `amy' ...
Adding new group `amy' (1016) ...
Adding new user `amy' (1014) with group `amy' ...
Creating home directory `/home/amy' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for amy
Enter the new value, or press ENTER for the default
        Full Name []: Amy
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y

sysadmin@UbuntuDesktop:/home$ sudo adduser sara
Adding user `sara' ...
Adding new group `sara' (1017) ...
Adding new user `sara' (1015) with group `sara' ...
Creating home directory `/home/sara' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sara
Enter the new value, or press ENTER for the default
        Full Name []: Sara
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

```
sysadmin@UbuntuDesktop:/home$ sudo adduser admin
Adding user `admin' ...
Adding new group `admin' (1018) ...
Adding new user `admin' (1016) with group `admin' ...
Creating home directory `/home/admin' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
        Full Name []: admin
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

2. Ensure that only the `admin` has general sudo access.
    - Command to add `admin` to the `sudo` group:

```
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG sudo admin
sysadmin@UbuntuDesktop:~$ sudo groups admin
admin : admin sudo
```

Step 3: Create User Group and Collaborative Folder

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

```
sysadmin@UbuntuDesktop:/home$ sudo addgroup engineers

Adding group `engineers' (GID 1019) ...

Done.
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers sam
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers joe
```

```
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers amy
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers sara
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG sudo admin
```

```
sysadmin@UbuntuDesktop:/home$ groups sam
sam : sam engineers
sysadmin@UbuntuDesktop:/home$ groups joe
joe : joe engineers
sysadmin@UbuntuDesktop:/home$ groups amy
amy : amy engineers
sysadmin@UbuntuDesktop:/home$ groups sara
sara : sara engineers
sysadmin@UbuntuDesktop:/home$ groups admin
admin : admin sudo

sysadmin@UbuntuDesktop:/home$ sudo mkdir engineers

sysadmin@UbuntuDesktop:/home$ sudo chmod 777 engineers

sysadmin@UbuntuDesktop:/home/engineers$ ls -la
drwxrwxrwx  2 root root 4096 Dec 15 14:26

grep -i "sam\|joe\|amy\|sara\|admin" /etc/passwd
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
sysadmin:x:1000:1000:sysadmin,,,:/home/sysadmin:/bin/bash
sam:x:1007:1014:Sam,,,:/home/sam:/bin/bash
joe:x:1013:1015:Joe,,,:/home/joe:/bin/bash
amy:x:1014:1016:Amy,,,:/home/amy:/bin/bash
sara:x:1015:1017:Sara,,,:/home/sara:/bin/bash
admin:x:1016:1018:admin,,,:/home/admin:/bin/bash
```

Step 4: Lynis Auditing

1. Command to install Lynis:

   sudo apt install lynis

2. Command to see documentation and instructions:
   - man lynis
   - DOCUMENTATION :Supporting documentation can be found via https://cisofy.com/support/

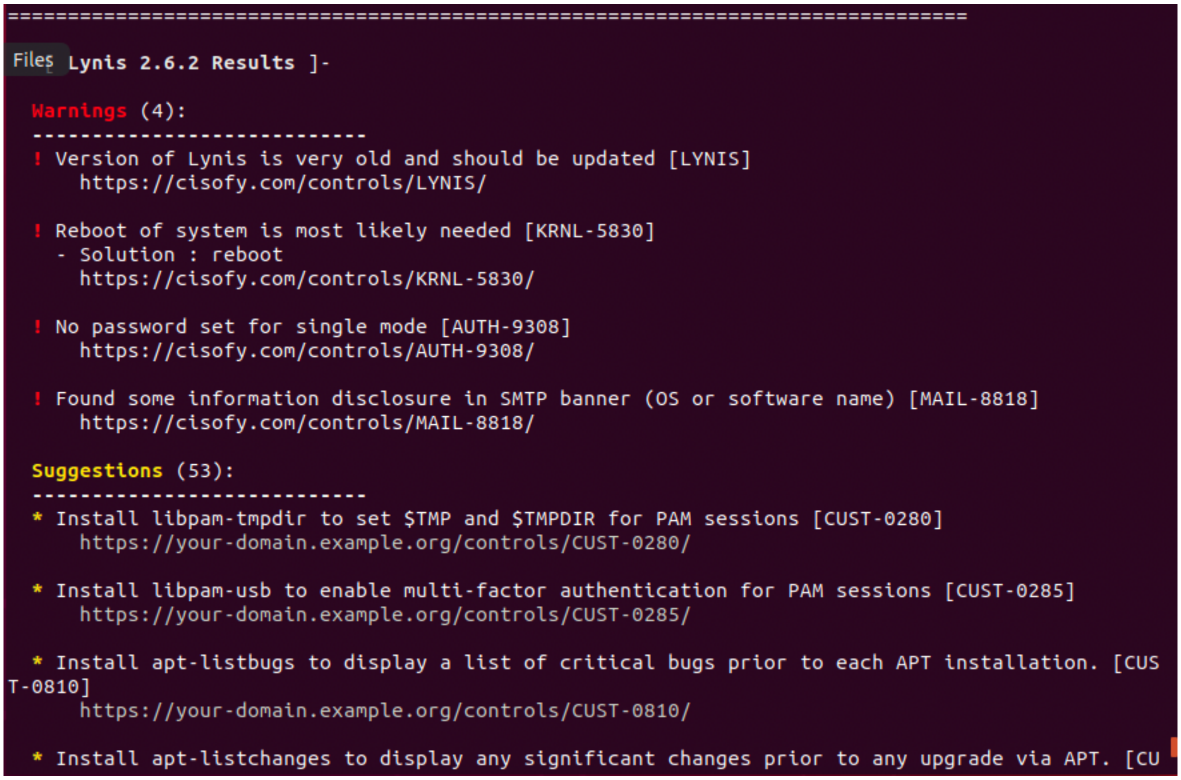
3. Command to run an audit:

   - **sudo lynis audit system**

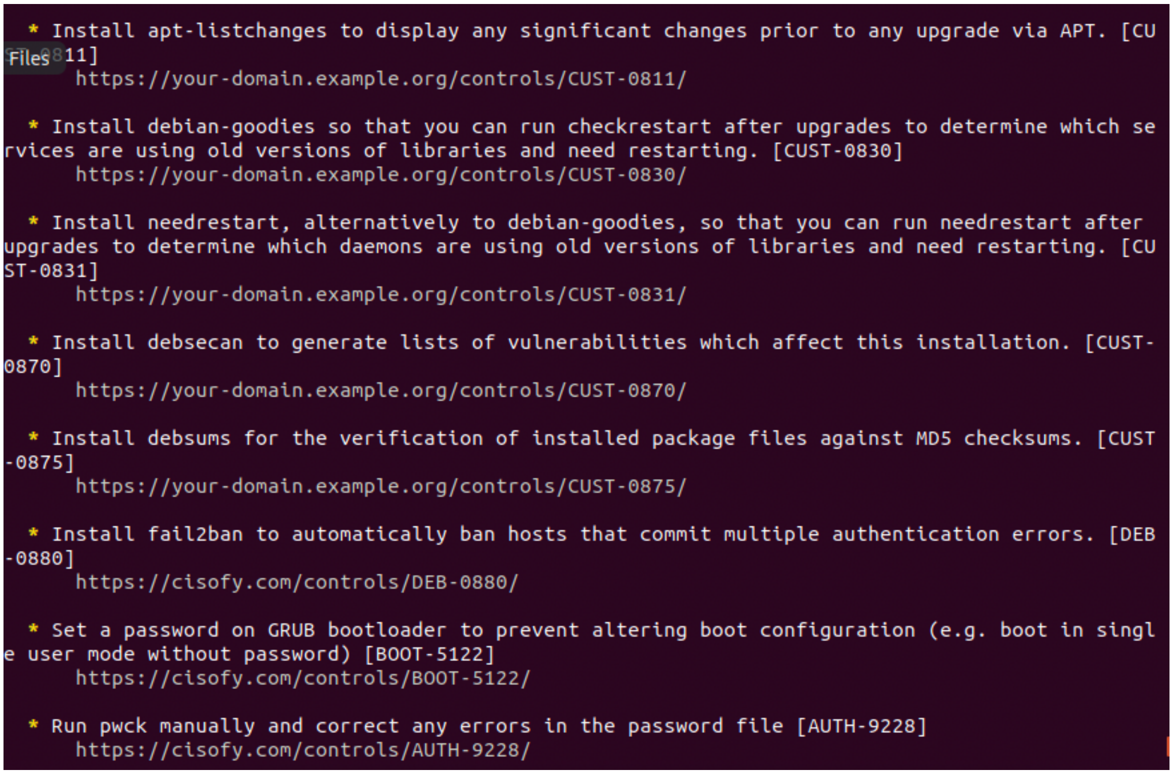
4. Provide a report from the Lynis output on what can be done to harden the system.

Screenshot of report output:

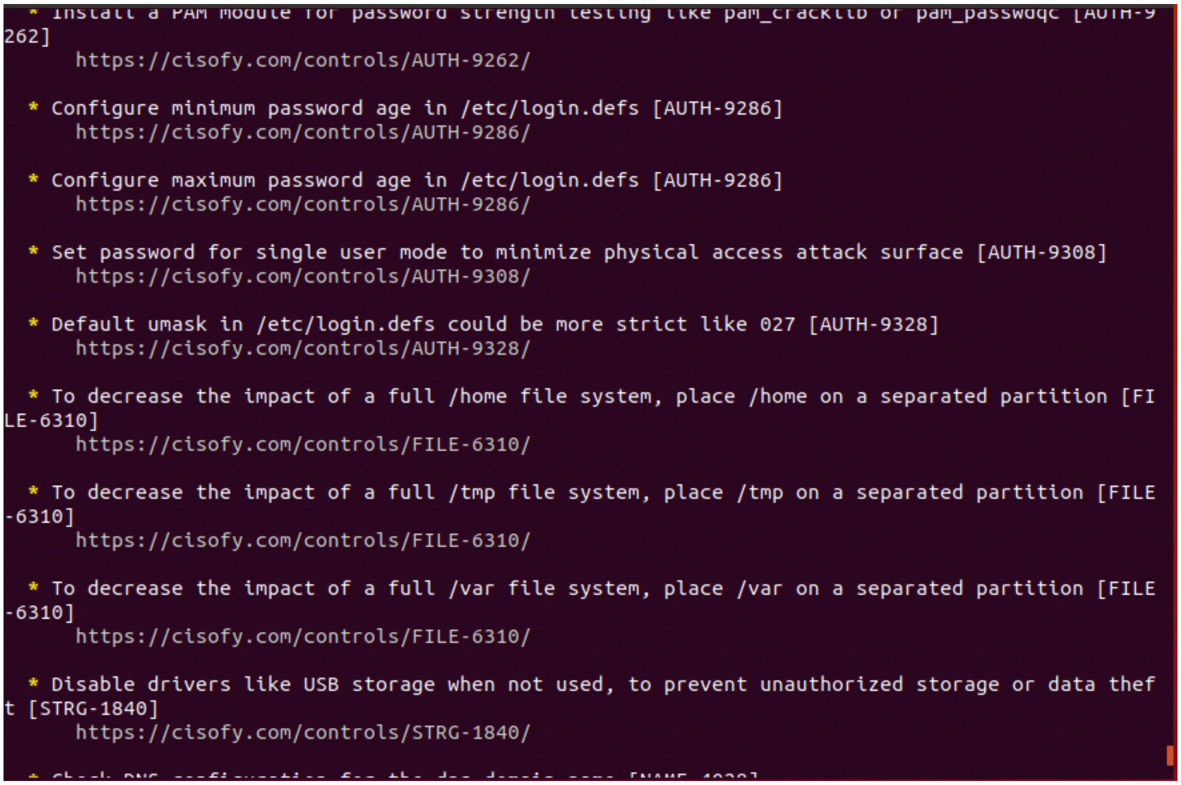
```
root@UbuntuDesktop:/# sudo apt install lynis
Reading package lists... Done
Building dependency tree
Reading state information... Done
lynis is already the newest version (2.6.2-1).
The following packages were automatically installed and are no longer required:
```



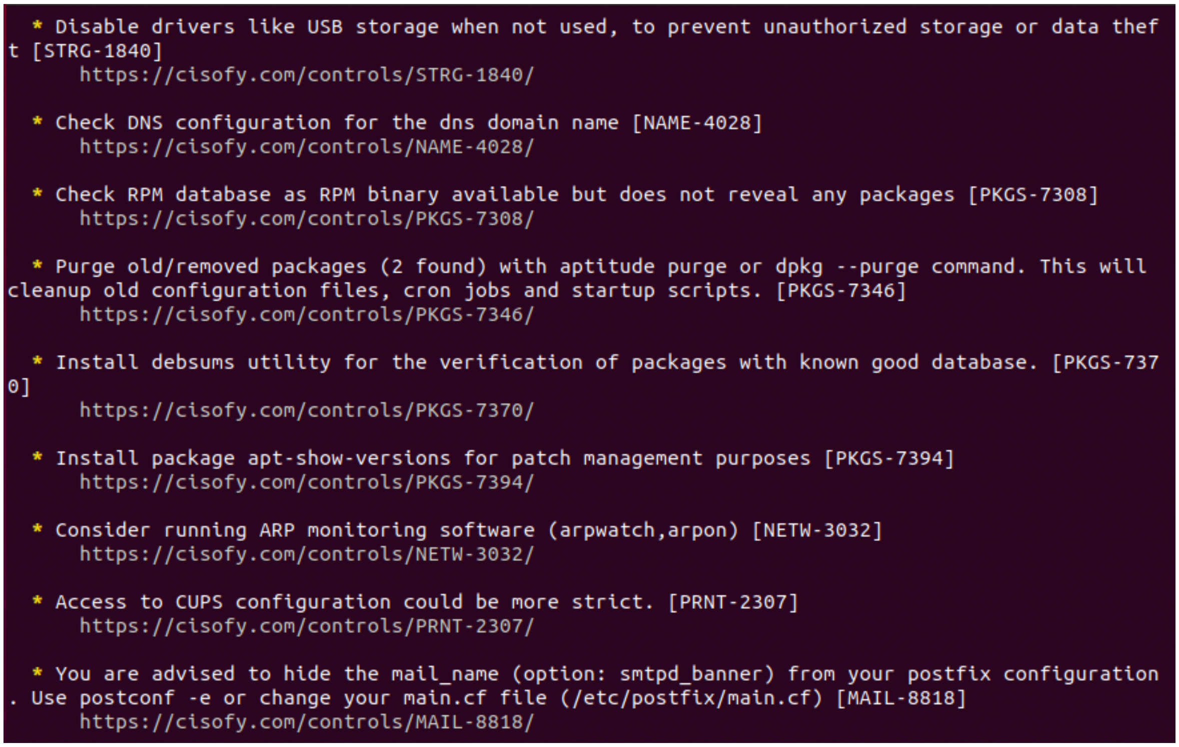
```
================================================================================

  Lynis 2.6.2 Results ]-

  Warnings (4):
  ----------------------------
  ! Version of Lynis is very old and should be updated [LYNIS]
      https://cisofy.com/controls/LYNIS/

  ! Reboot of system is most likely needed [KRNL-5830]
    - Solution : reboot
      https://cisofy.com/controls/KRNL-5830/

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

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

  Suggestions (53):
  ----------------------------
  * 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. [CUS
T-0810]
      https://your-domain.example.org/controls/CUST-0810/

  * Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CU
```



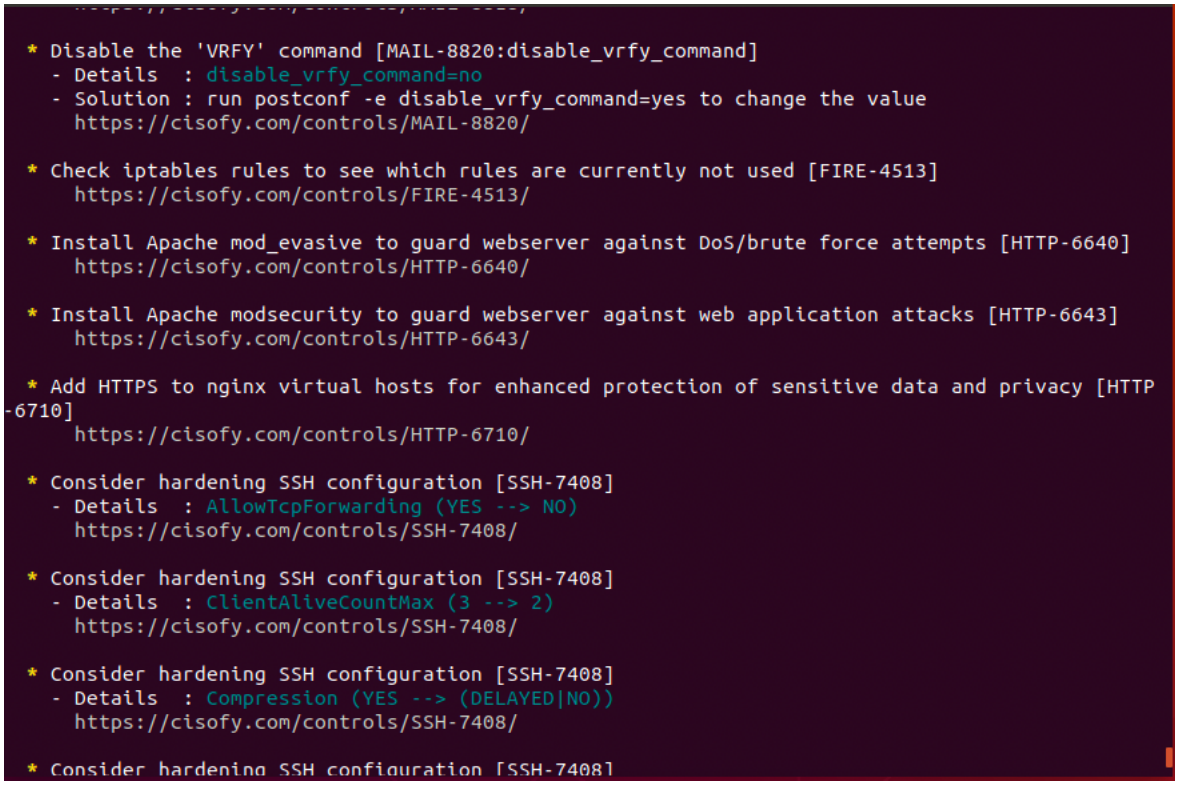
```
  * Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CU
ST-0811]
      https://your-domain.example.org/controls/CUST-0811/

  * Install debian-goodies so that you can run checkrestart after upgrades to determine which se
rvices are using old versions of libraries and need restarting. [CUST-0830]
      https://your-domain.example.org/controls/CUST-0830/

  * Install needrestart, alternatively to debian-goodies, so that you can run needrestart after
upgrades to determine which daemons are using old versions of libraries and need restarting. [CU
ST-0831]
      https://your-domain.example.org/controls/CUST-0831/

  * Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-
0870]
      https://your-domain.example.org/controls/CUST-0870/

  * Install debsums for the verification of installed package files against MD5 checksums. [CUST
-0875]
      https://your-domain.example.org/controls/CUST-0875/

  * Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB
-0880]
      https://cisofy.com/controls/DEB-0880/

  * Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in singl
e user mode without password) [BOOT-5122]
      https://cisofy.com/controls/BOOT-5122/

  * Run pwck manually and correct any errors in the password file [AUTH-9228]
      https://cisofy.com/controls/AUTH-9228/
```



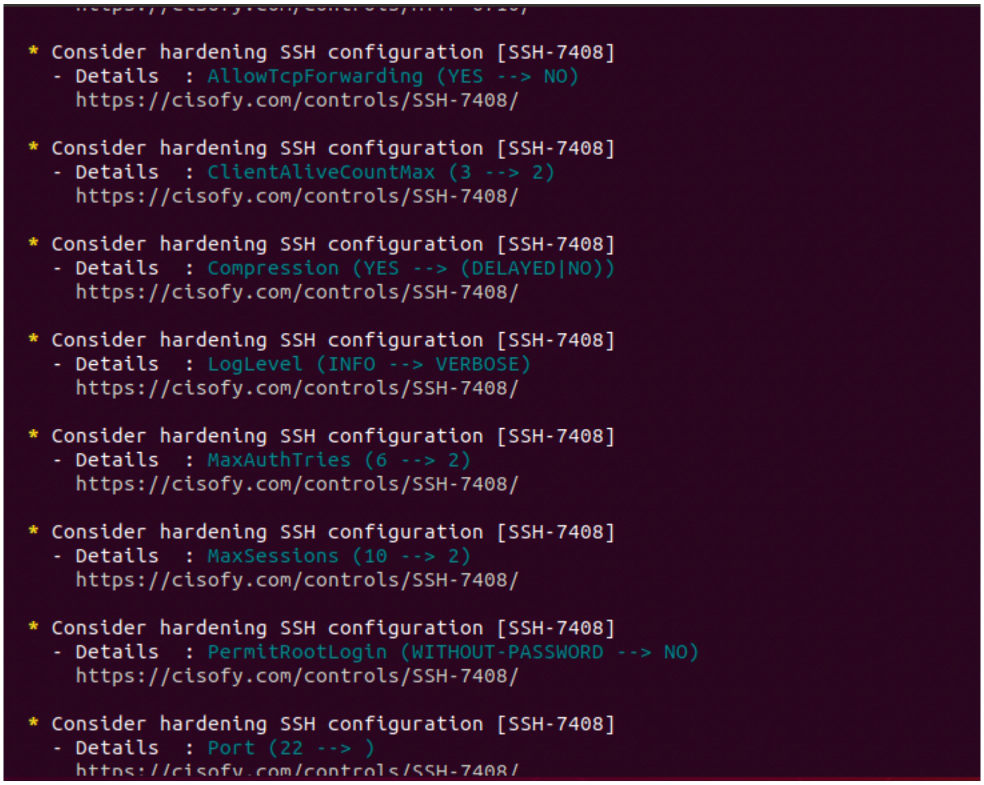
```
  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9
262]
      https://cisofy.com/controls/AUTH-9262/

  * Configure minimum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/controls/AUTH-9286/

  * Set password for single user mode to minimize physical access attack surface [AUTH-9308]
      https://cisofy.com/controls/AUTH-9308/

  * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
      https://cisofy.com/controls/AUTH-9328/

  * To decrease the impact of a full /home file system, place /home on a separated partition [FI
LE-6310]
      https://cisofy.com/controls/FILE-6310/

  * To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE
-6310]
      https://cisofy.com/controls/FILE-6310/

  * To decrease the impact of a full /var file system, place /var on a separated partition [FILE
-6310]
      https://cisofy.com/controls/FILE-6310/

  * Disable drivers like USB storage when not used, to prevent unauthorized storage or data thef
t [STRG-1840]
      https://cisofy.com/controls/STRG-1840/

  * Check DNS configuration for the dns domain name [NAME-4028]
```



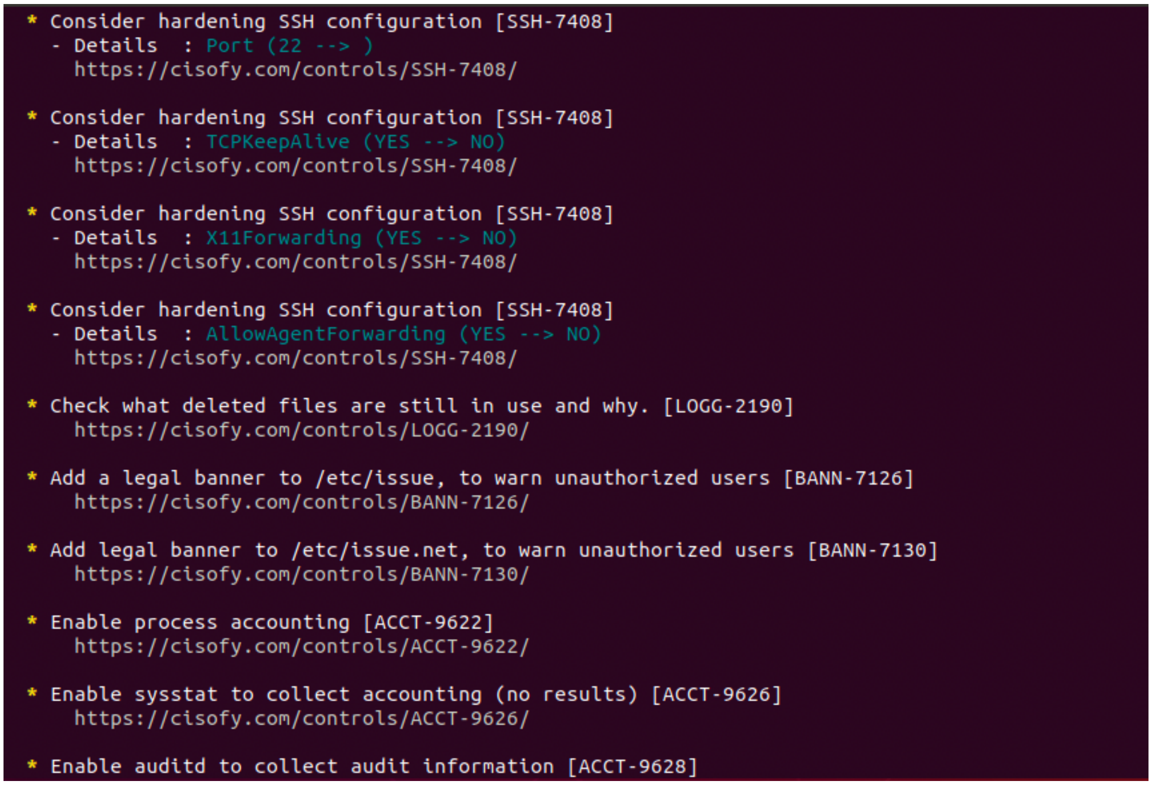
```
  * Disable drivers like USB storage when not used, to prevent unauthorized storage or data thef
t [STRG-1840]
      https://cisofy.com/controls/STRG-1840/

  * Check DNS configuration for the dns domain name [NAME-4028]
      https://cisofy.com/controls/NAME-4028/

  * Check RPM database as RPM binary available but does not reveal any packages [PKGS-7308]
      https://cisofy.com/controls/PKGS-7308/

  * Purge old/removed packages (2 found) with aptitude purge or dpkg --purge command. This will
cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]
      https://cisofy.com/controls/PKGS-7346/

  * Install debsums utility for the verification of packages with known good database. [PKGS-737
0]
      https://cisofy.com/controls/PKGS-7370/

  * Install package apt-show-versions for patch management purposes [PKGS-7394]
      https://cisofy.com/controls/PKGS-7394/

  * Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]
      https://cisofy.com/controls/NETW-3032/

  * Access to CUPS configuration could be more strict. [PRNT-2307]
      https://cisofy.com/controls/PRNT-2307/

  * You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration
. Use postconf -e or change your main.cf file (/etc/postfix/main.cf) [MAIL-8818]
      https://cisofy.com/controls/MAIL-8818/
```



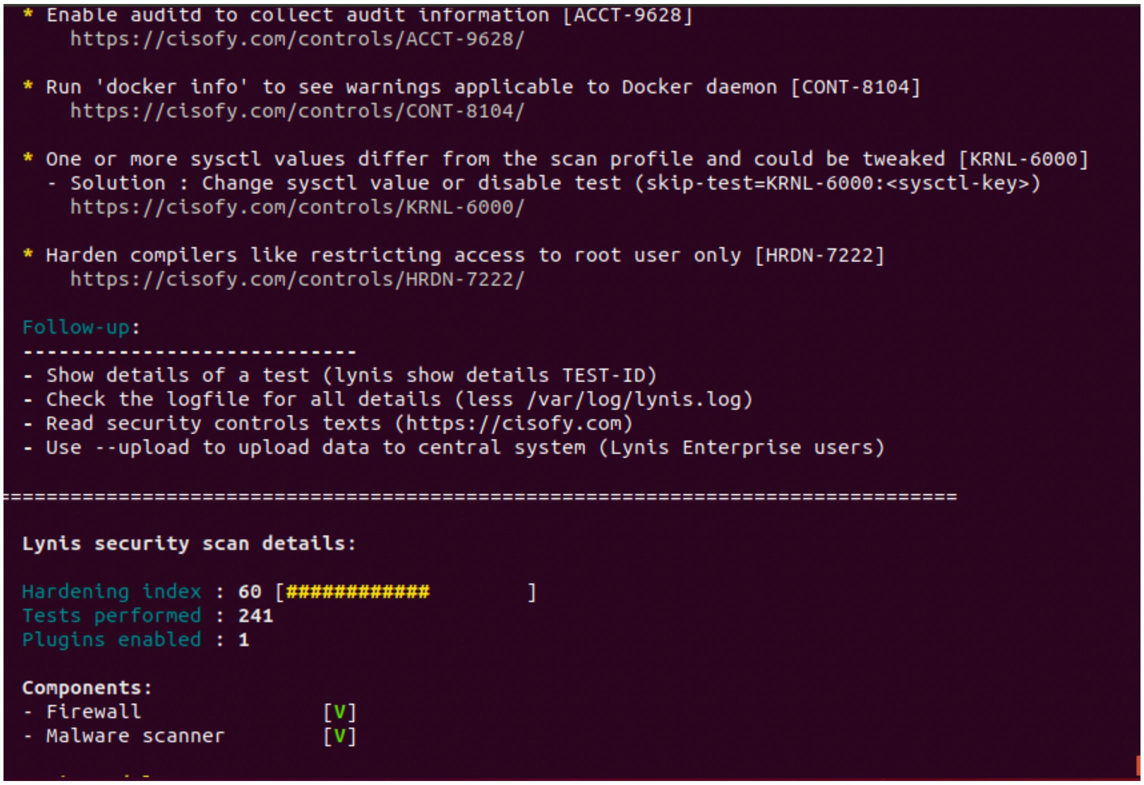
```
  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
    - Details  : disable_vrfy_command=no
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
      https://cisofy.com/controls/MAIL-8820/

  * Check iptables rules to see which rules are currently not used [FIRE-4513]
      https://cisofy.com/controls/FIRE-4513/

  * Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
      https://cisofy.com/controls/HTTP-6640/

  * Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
      https://cisofy.com/controls/HTTP-6643/

  * Add HTTPS to nginx virtual hosts for enhanced protection of sensitive data and privacy [HTTP
-6710]
      https://cisofy.com/controls/HTTP-6710/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (YES --> NO)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (3 --> 2)
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Compression (YES --> (DELAYED|NO))
      https://cisofy.com/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
```



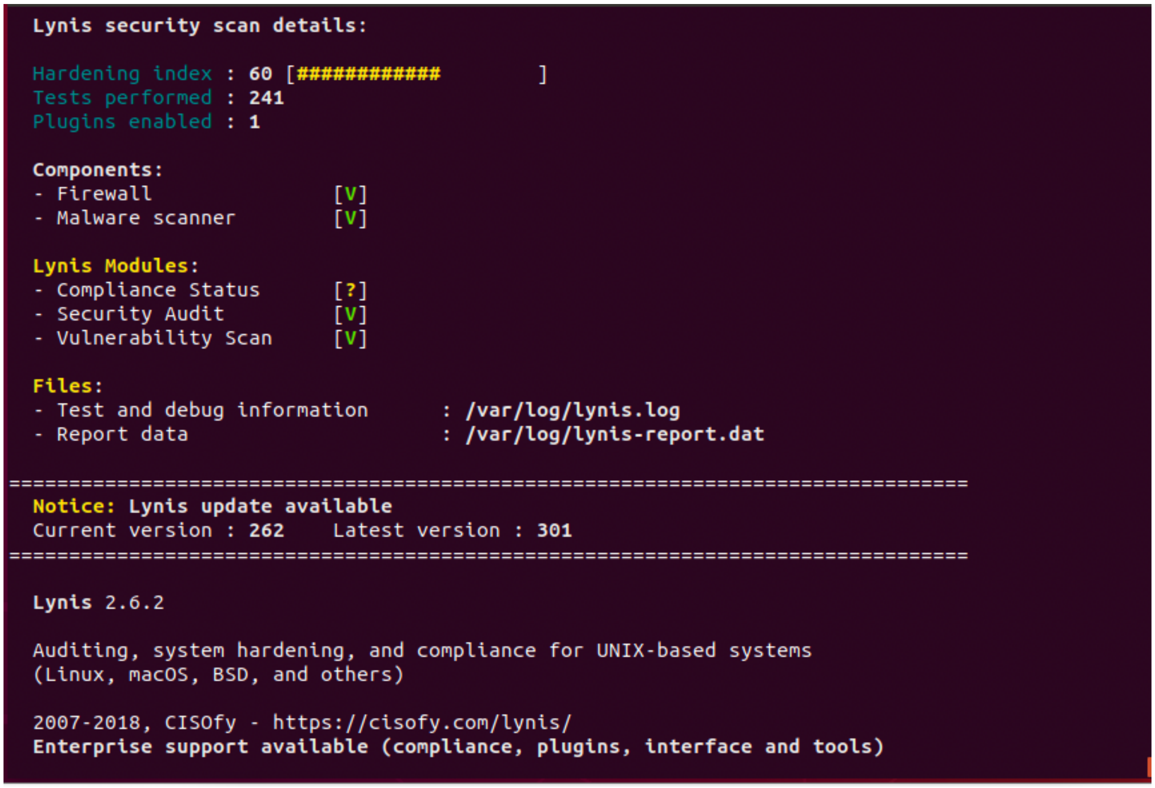
```
* Consider hardening SSH configuration [SSH-7408]
  - Details  : AllowTcpForwarding (YES --> NO)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : ClientAliveCountMax (3 --> 2)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : Compression (YES --> (DELAYED|NO))
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : LogLevel (INFO --> VERBOSE)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : MaxAuthTries (6 --> 2)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : MaxSessions (10 --> 2)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : PermitRootLogin (WITHOUT-PASSWORD --> NO)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : Port (22 --> )
    https://cisofy.com/controls/SSH-7408/
```



```
* Consider hardening SSH configuration [SSH-7408]
  - Details  : Port (22 --> )
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : TCPKeepAlive (YES --> NO)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : X11Forwarding (YES --> NO)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : AllowAgentForwarding (YES --> NO)
    https://cisofy.com/controls/SSH-7408/

* Check what deleted files are still in use and why. [LOGG-2190]
    https://cisofy.com/controls/LOGG-2190/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
    https://cisofy.com/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
    https://cisofy.com/controls/BANN-7130/

* Enable process accounting [ACCT-9622]
    https://cisofy.com/controls/ACCT-9622/

* Enable sysstat to collect accounting (no results) [ACCT-9626]
    https://cisofy.com/controls/ACCT-9626/

* Enable auditd to collect audit information [ACCT-9628]
```



```
 * Enable auditd to collect audit information [ACCT-9628]
     https://cisofy.com/controls/ACCT-9628/

 * Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
     https://cisofy.com/controls/CONT-8104/

 * One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
   - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
     https://cisofy.com/controls/KRNL-6000/

 * Harden compilers like restricting access to root user only [HRDN-7222]
     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 : 60 [############        ]
 Tests performed : 241
 Plugins enabled : 1

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



```
  Lynis security scan details:

  Hardening index : 60 [############        ]
  Tests performed : 241
  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 : 301
================================================================================

  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)
```

Bonus

1. Command to install chkrootkit:

```
root@UbuntuDesktop:/# sudo apt install chkrootkit
Reading package lists... Done
Building dependency tree
Reading state information... Done
chkrootkit is already the newest version (0.52-1ubuntu0.1).
The following packages were automatically installed and are no longer required:
```

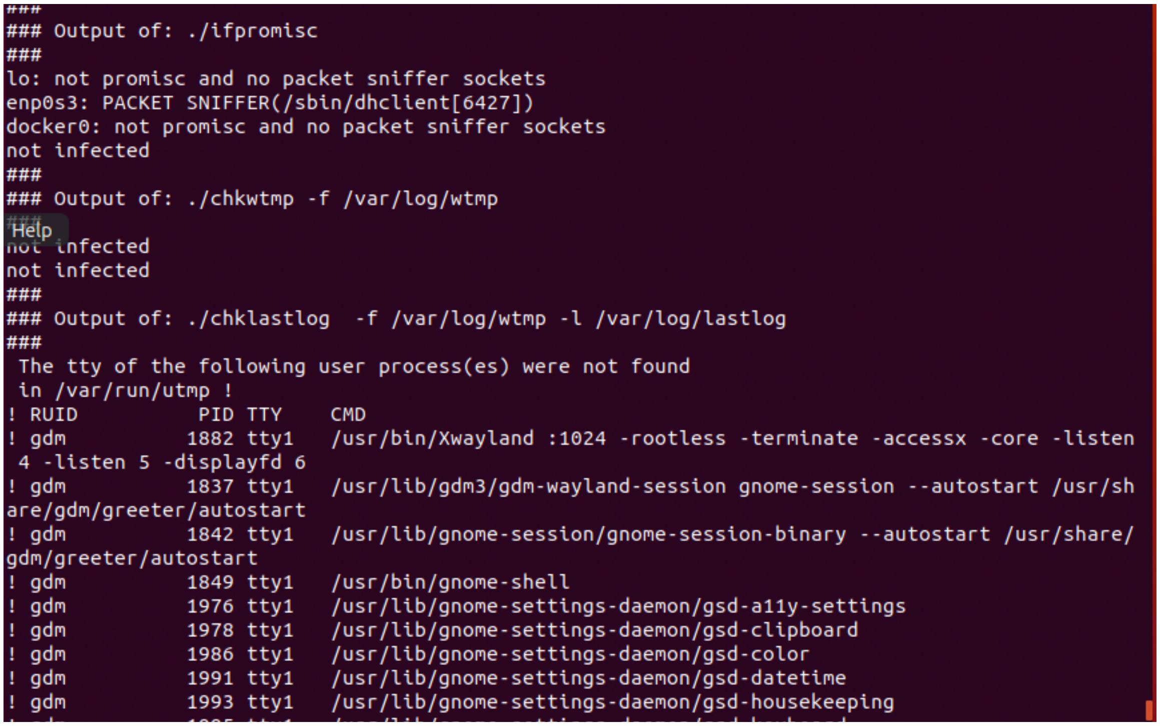
2. Command to see documentation and instructions:

- man chkrootkit
- Chkrootkit.org
- The Manual Documentation exists on the Home Page of chkrootkit.org

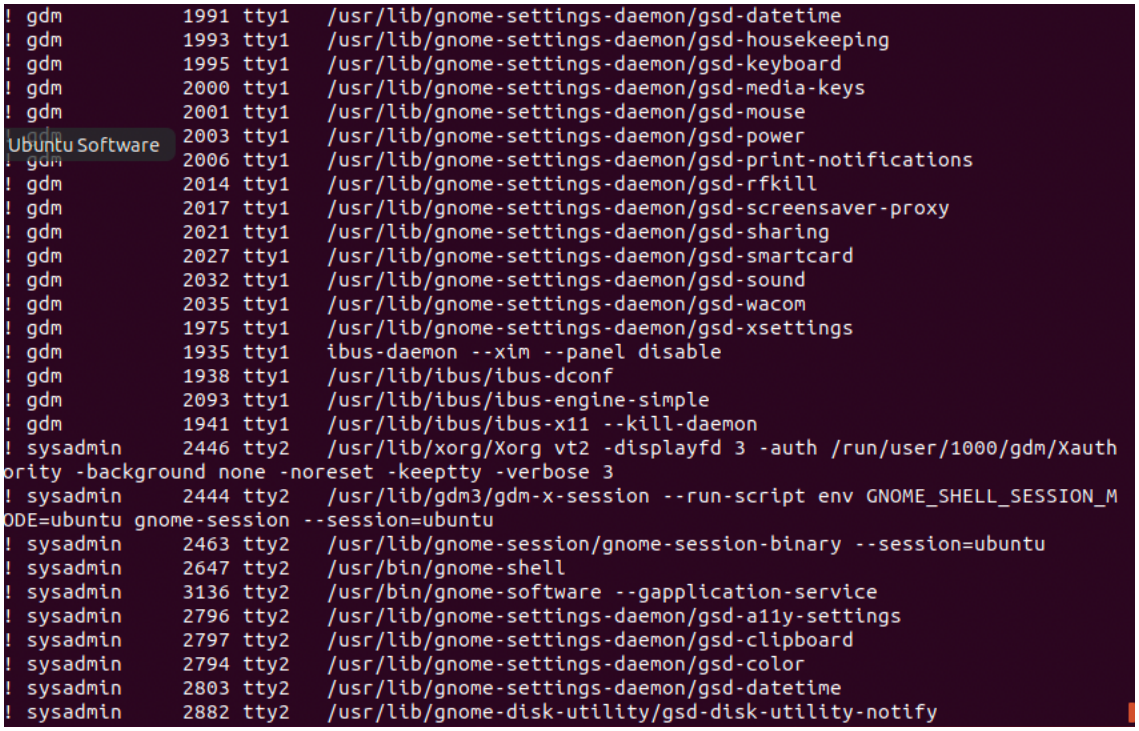
3. Command to run expert mode:

```
sudo chkrootkit -x > /usr/sbin/chkrootkit2.txt
```

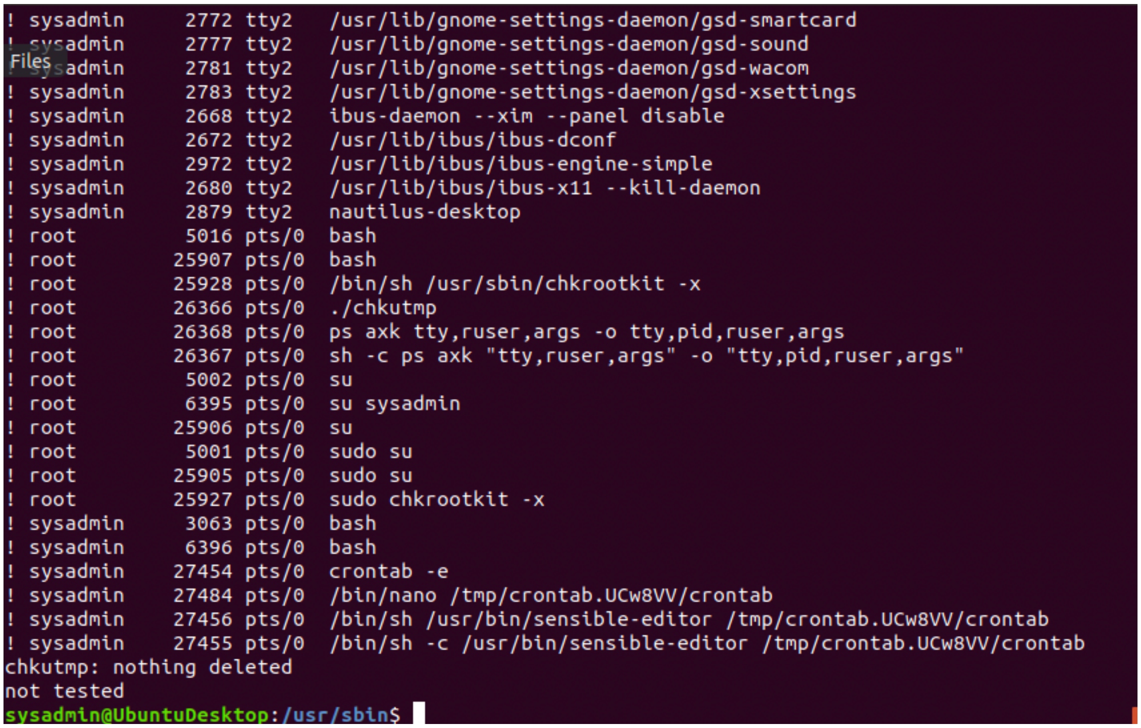
4. Provide a report from the chrootkit output on what can be done to harden the system.
    - Screenshot of end of sample output:



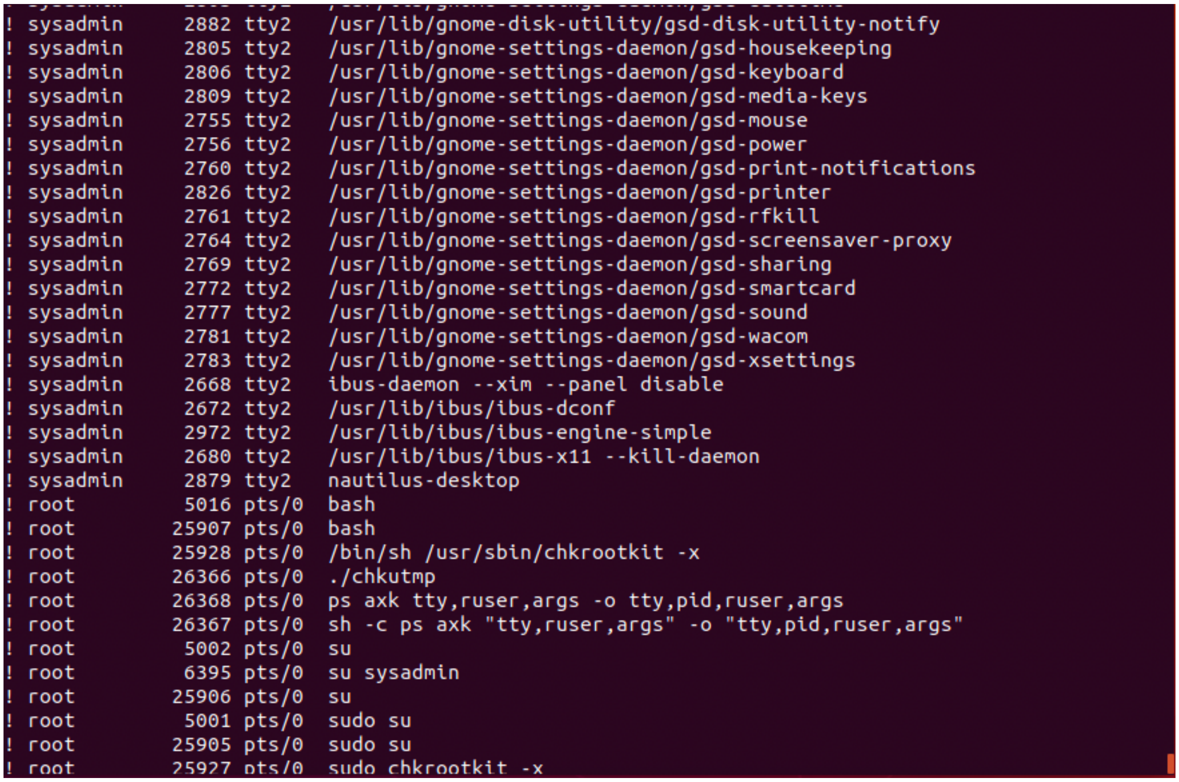
```
###
### Output of: ./ifpromisc
###
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/sbin/dhclient[6427])
docker0: not promisc and no packet sniffer sockets
not infected
###
### Output of: ./chkwtmp -f /var/log/wtmp
###
not infected
not infected
###
### Output of: ./chklastlog  -f /var/log/wtmp -l /var/log/lastlog
###
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          1882 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen
 4 -listen 5 -displayfd 6
! gdm          1837 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/sh
are/gdm/greeter/autostart
! gdm          1842 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/
gdm/greeter/autostart
! gdm          1849 tty1   /usr/bin/gnome-shell
! gdm          1976 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          1978 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          1986 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          1991 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          1993 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
```



```
! gdm          1991 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          1993 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          1995 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          2000 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2001 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2003 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2006 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2014 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2017 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2021 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2027 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2032 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2035 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          1975 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          1935 tty1   ibus-daemon --xim --panel disable
! gdm          1938 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2093 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          1941 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2446 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauth
ority -background none -noreset -keeptty -verbose 3
! sysadmin     2444 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_M
ODE=ubuntu gnome-session --session=ubuntu
! sysadmin     2463 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     2647 tty2   /usr/bin/gnome-shell
! sysadmin     3136 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     2796 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     2797 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     2794 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     2803 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     2882 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
```



```
! sysadmin     2772 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2777 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2781 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2783 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2668 tty2   ibus-daemon --xim --panel disable
! sysadmin     2672 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2972 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2680 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2879 tty2   nautilus-desktop
! root         5016 pts/0  bash
! root        25907 pts/0  bash
! root        25928 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root        26366 pts/0  ./chkutmp
! root        26368 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        26367 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root         5002 pts/0  su
! root         6395 pts/0  su sysadmin
! root        25906 pts/0  su
! root         5001 pts/0  sudo su
! root        25905 pts/0  sudo su
! root        25927 pts/0  sudo chkrootkit -x
! sysadmin     3063 pts/0  bash
! sysadmin     6396 pts/0  bash
! sysadmin    27454 pts/0  crontab -e
! sysadmin    27484 pts/0  /bin/nano /tmp/crontab.UCw8VV/crontab
! sysadmin    27456 pts/0  /bin/sh /usr/bin/sensible-editor /tmp/crontab.UCw8VV/crontab
! sysadmin    27455 pts/0  /bin/sh -c /usr/bin/sensible-editor /tmp/crontab.UCw8VV/crontab
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:/usr/sbin$
```



```
! sysadmin     2882 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     2805 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     2806 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     2809 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     2755 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     2756 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     2760 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     2826 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     2761 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     2764 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     2769 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     2772 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2777 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2781 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2783 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2668 tty2   ibus-daemon --xim --panel disable
! sysadmin     2672 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2972 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2680 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2879 tty2   nautilus-desktop
! root         5016 pts/0  bash
! root        25907 pts/0  bash
! root        25928 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root        26366 pts/0  ./chkutmp
! root        26368 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        26367 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root         5002 pts/0  su
! root         6395 pts/0  su sysadmin
! root        25906 pts/0  su
! root         5001 pts/0  sudo su
! root        25905 pts/0  sudo su
! root        25927 pts/0  sudo chkrootkit -x
```