



Cybersecurity

Module 4 Challenge Submission File

Linux Systems Administration

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.
 - a. Command to inspect permissions:

```
ls -l /etc/shadow
```

- b. Command to set permissions (if needed):

```
sudo chmod 600 /etc/shadow
```

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
 - a. Command to inspect permissions:

```
ls -l /etc/gshadow
```

- b. Command to set permissions (if needed):

```
sudo chmod 600 /etc/gshadow
```

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

- a. Command to inspect permissions:

```
ls -l /etc/group
```

- b. Command to set permissions (if needed):

```
sudo chmod 644 /etc/group
```

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

- a. Command to inspect permissions:

```
ls -l /etc/passwd
```

- b. Command to set permissions (if needed):

```
sudo chmod 644 /etc/passwd
```

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin` with the `useradd` command.

- a. Command to add each user account (include all five users):

```
sudo useradd -m sam
sudo useradd -m joe
sudo useradd -m amy
sudo useradd -m sara
sudo useradd -m admin
```

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

- a. Command to add `admin` to the sudo group:

```
sudo usermod -aG sudo admin
```

Step 3: Create User Group and Collaborative Folder

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

- a. Command to add group:

```
sudo addgroup engineers
```

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

- a. Command to add users to `engineers` group (include all four users):

```
sudo usermod -G engineers sam
sudo usermod -G engineers joe
sudo usermod -G engineers amy
sudo usermod -G engineers sara
```

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

- a. Command to create the shared folder:

```
mkdir /home/engineers
```

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

- a. Command to change ownership of engineers' shared folder to `engineers` group:

```
sudo chown :engineers /home/engineers
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
sudo apt -y install lynis
```

2. Command to view documentation and instructions:

```
man lynis
```

3. Command to run an audit:

```
sudo lynis audit system
```

4. Provide a report from the Lynis output with recommendations for hardening the system.
 - a. Screenshot of report output:

Linux-Module_default_1666218692505_39787 (lynis output) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 21:46 sysadmin@UbuntuDesktop: ~

File Edit View Search Terminal Help

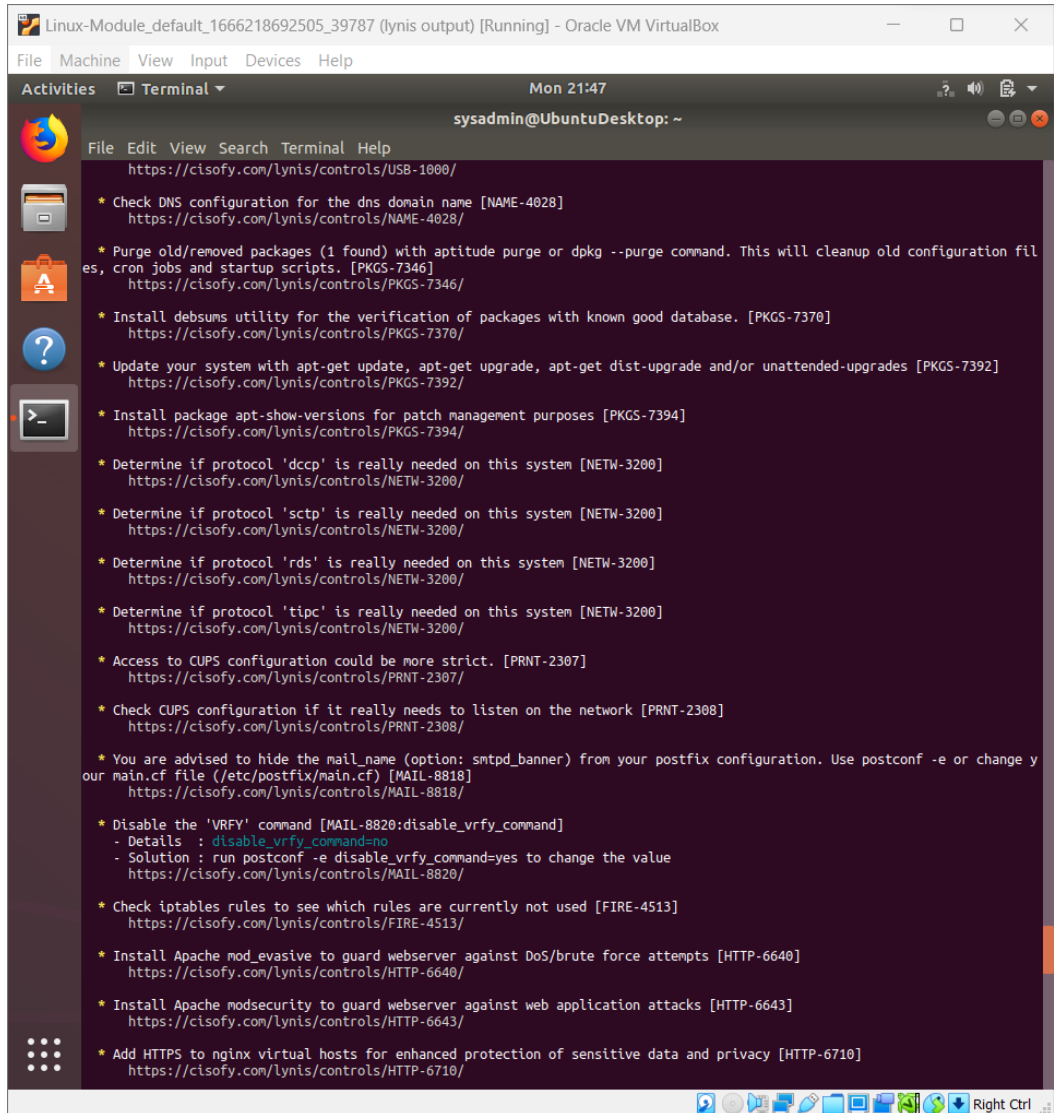
<https://cisofy.com/lynis/controls/MAIL-8818/>

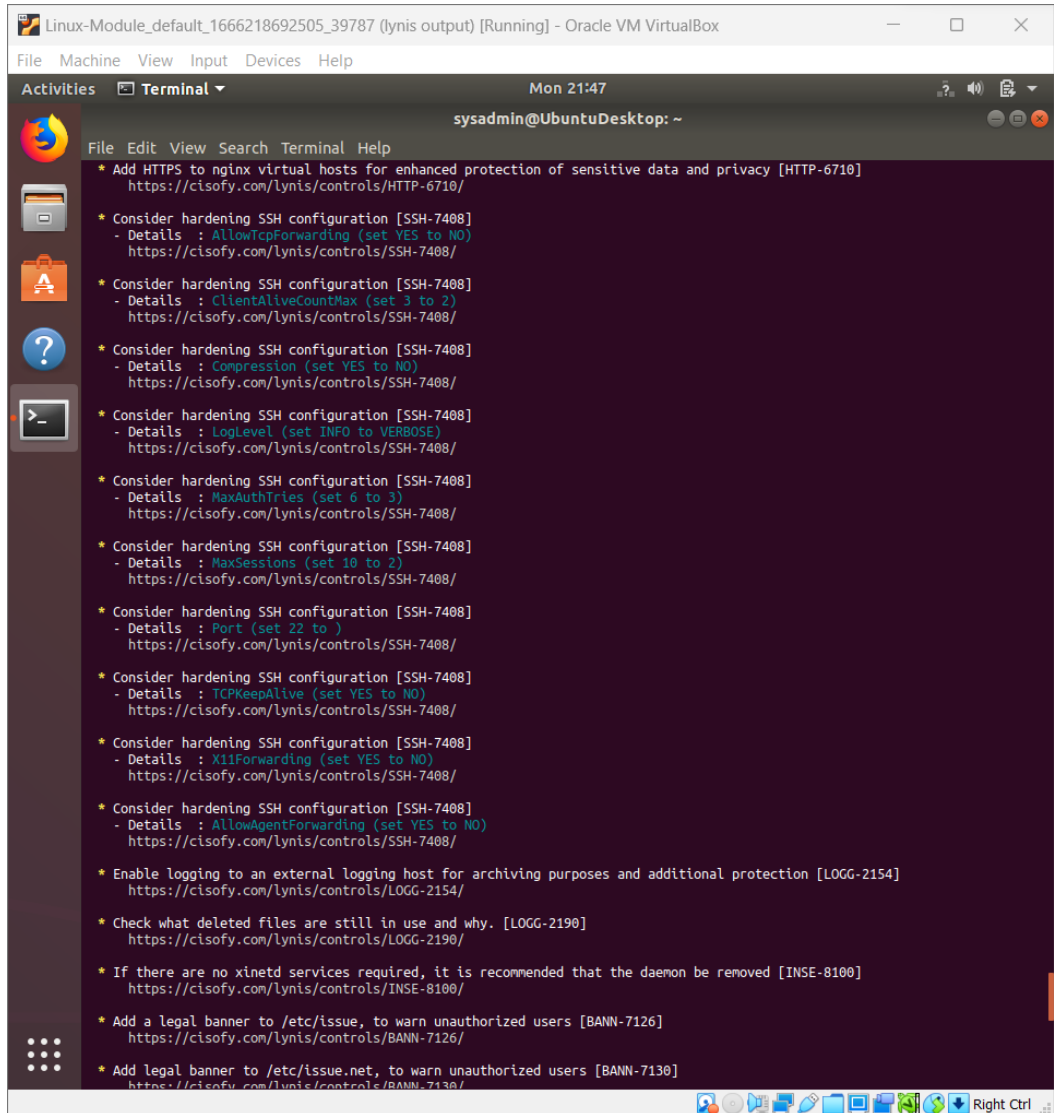
! Found one or more cronjob files with incorrect ownership (see log for details) [SCHD-7704]
<https://cisofy.com/lynis/controls/SCHD-7704/>

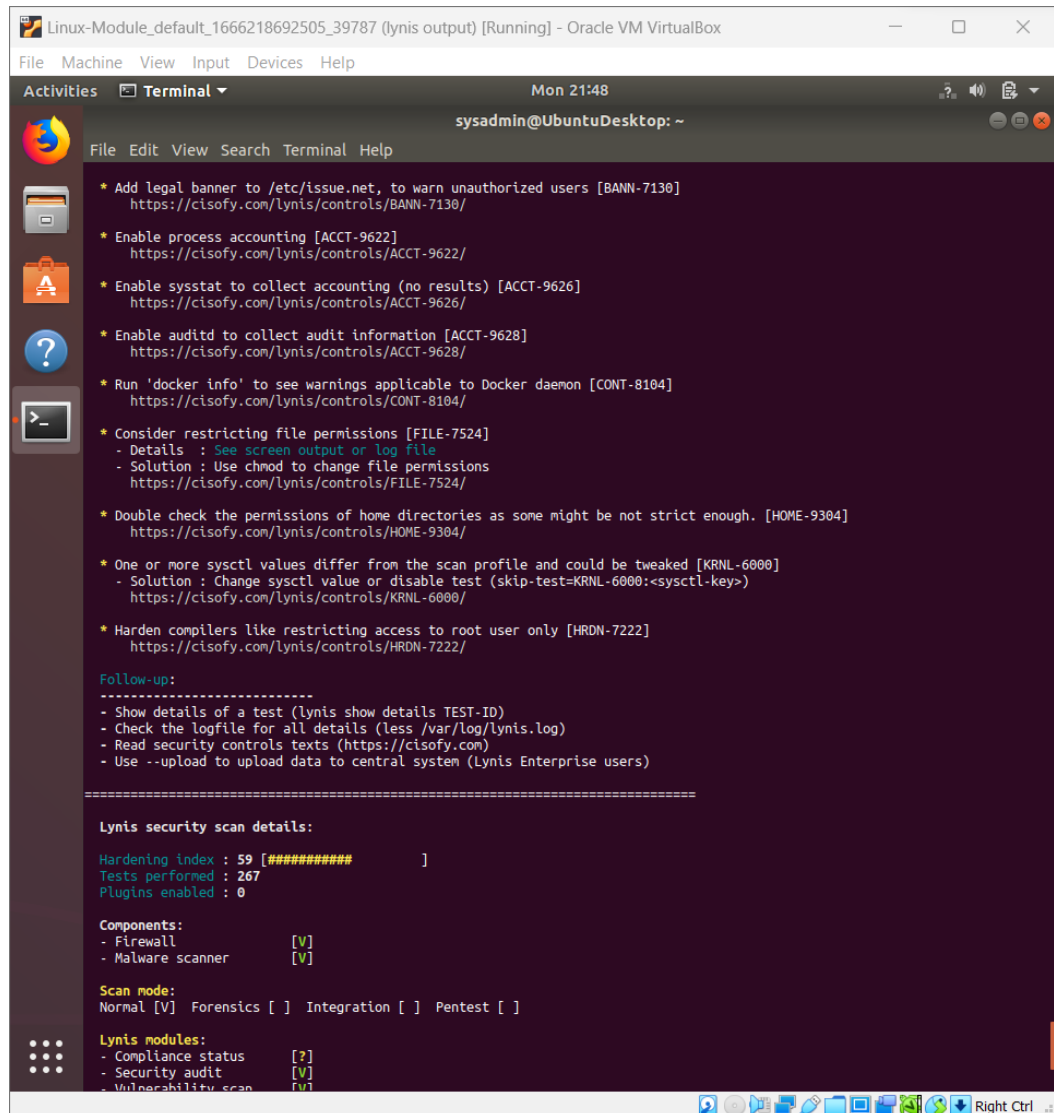
Suggestions (56):

- * Version of Lynis outdated, consider upgrading to the latest version [LYNIS]
<https://cisofy.com/lynis/controls/LYNIS/>
- * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
<https://cisofy.com/lynis/controls/BOOT-5122/>
- * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
<https://cisofy.com/lynis/controls/KRNL-5820/>
- * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
<https://cisofy.com/lynis/controls/AUTH-9229/>
- * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
<https://cisofy.com/lynis/controls/AUTH-9230/>
- * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
<https://cisofy.com/lynis/controls/AUTH-9262/>
- * When possible set expire dates for all password protected accounts [AUTH-9282]
<https://cisofy.com/lynis/controls/AUTH-9282/>
- * Look at the locked accounts and consider removing them [AUTH-9284]
<https://cisofy.com/lynis/controls/AUTH-9284/>
- * Configure minimum password age in /etc/login.defs [AUTH-9286]
<https://cisofy.com/lynis/controls/AUTH-9286/>
- * Configure maximum password age in /etc/login.defs [AUTH-9286]
<https://cisofy.com/lynis/controls/AUTH-9286/>
- * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
<https://cisofy.com/lynis/controls/AUTH-9328/>
- * To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
<https://cisofy.com/lynis/controls/FILE-6310/>
- * To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
<https://cisofy.com/lynis/controls/FILE-6310/>
- * To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
<https://cisofy.com/lynis/controls/FILE-6310/>
- * Check 9 files in /tmp which are older than 90 days [FILE-6354]
<https://cisofy.com/lynis/controls/FILE-6354/>
- * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
<https://cisofy.com/lynis/controls/USB-1000/>
- * Check DNS configuration for the dns domain name [NAME-4028]

Right Ctrl







```
Linux-Module_default_1666218692505_39787 (lynis output) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 21:48 sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

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

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

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

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

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

* Consider restricting file permissions [FILE-7524]
  - Details : See screen output or log file
  - Solution : Use chmod to change file permissions
  https://cisofy.com/lynis/controls/FILE-7524/

* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
  https://cisofy.com/lynis/controls/HOME-9304/

* 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/lynis/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HRDN-7222]
  https://cisofy.com/lynis/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 : 59 [##### ]
Tests performed : 267
Plugins enabled : 0

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

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]
```

Bonus

1. Command to install chkrootkit:

```
sudo apt -y install chkrootkit
```

2. Command to view documentation and instructions:

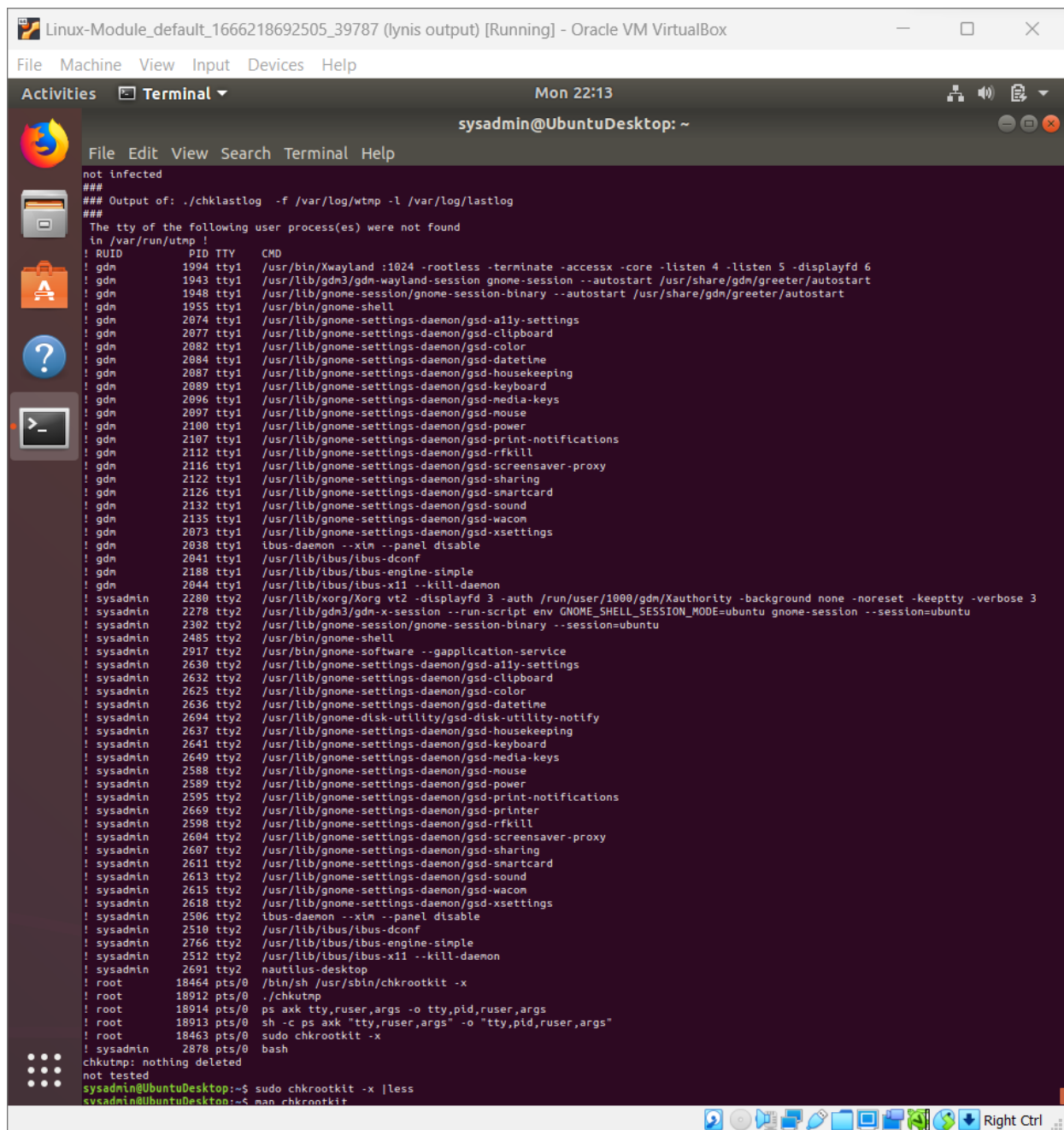
```
man chkrootkit
```

3. Command to run expert mode:


```
sudo chkrootkit -x
```

4. Provide a report from the chkrootkit output with recommendations for hardening the system.

- a. Screenshot of end of sample output:



```
Linux-Module_default_1666218692505_39787 (lynis output) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 22:13
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
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 1994 tty1 /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm 1943 tty1 /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm 1948 tty1 /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm 1955 tty1 /usr/bin/gnome-shell
! gdm 2074 tty1 /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm 2077 tty1 /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm 2082 tty1 /usr/lib/gnome-settings-daemon/gsd-color
! gdm 2084 tty1 /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm 2087 tty1 /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm 2089 tty1 /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm 2096 tty1 /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm 2097 tty1 /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm 2100 tty1 /usr/lib/gnome-settings-daemon/gsd-power
! gdm 2107 tty1 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm 2112 tty1 /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm 2116 tty1 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm 2122 tty1 /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm 2126 tty1 /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm 2132 tty1 /usr/lib/gnome-settings-daemon/gsd-sound
! gdm 2135 tty1 /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm 2073 tty1 /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm 2038 tty1 ibus-daemon --xin --panel disable
! gdm 2041 tty1 /usr/lib/ibus/ibus-dconf
! gdm 2188 tty1 /usr/lib/ibus/ibus-engine-simple
! gdm 2044 tty1 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 2280 tty2 /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin 2278 tty2 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin 2302 tty2 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin 2485 tty2 /usr/bin/gnome-shell
! sysadmin 2917 tty2 /usr/bin/gnome-software --gapplication-service
! sysadmin 2630 tty2 /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin 2632 tty2 /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin 2625 tty2 /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin 2636 tty2 /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin 2694 tty2 /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin 2637 tty2 /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin 2641 tty2 /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin 2649 tty2 /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin 2588 tty2 /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin 2589 tty2 /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin 2595 tty2 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin 2669 tty2 /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin 2598 tty2 /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin 2604 tty2 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin 2607 tty2 /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin 2611 tty2 /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin 2613 tty2 /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin 2615 tty2 /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin 2618 tty2 /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin 2506 tty2 ibus-daemon --xin --panel disable
! sysadmin 2510 tty2 /usr/lib/ibus/ibus-dconf
! sysadmin 2766 tty2 /usr/lib/ibus/ibus-engine-simple
! sysadmin 2512 tty2 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 2691 tty2 nautilus-desktop
! root 18464 pts/0 /bin/sh /usr/sbin/chkrootkit -x
! root 18912 pts/0 ./chkutmp
! root 18914 pts/0 ps axk tty,ruser,args -o tty,pid,ruser,args
! root 18913 pts/0 sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root 18463 pts/0 sudo chkrootkit -x
! sysadmin 2878 pts/0 bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:~$ sudo chkrootkit -x |less
sysadmin@UbuntuDesktop:~$ man chkrootkit
```

