Sasha Shahidi

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: ls -l /etc/shadow
   - Command to set permissions (if needed): sudo chmod 600 /etc/shadow
2. Permissions on /etc/gshadow should allow only root read and write access.
   - Command to inspect permissions: ls -l /etc/gshadow
   - 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.
   - Command to inspect permissions: ls -l /etc/group
   - 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.
   - Command to inspect permissions: ls -l /etc/passwd
   - 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.
   - Command to add each user account (include all five users):

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

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

   - 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.

   - 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 usermod -aG engineers sam
     sudo usermod -aG engineers joe
     sudo usermod -aG engineers amy
     sudo usermod -aG engineers 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 -R :engineers /home/engineers
     ```

Step 4: Lynis Auditing

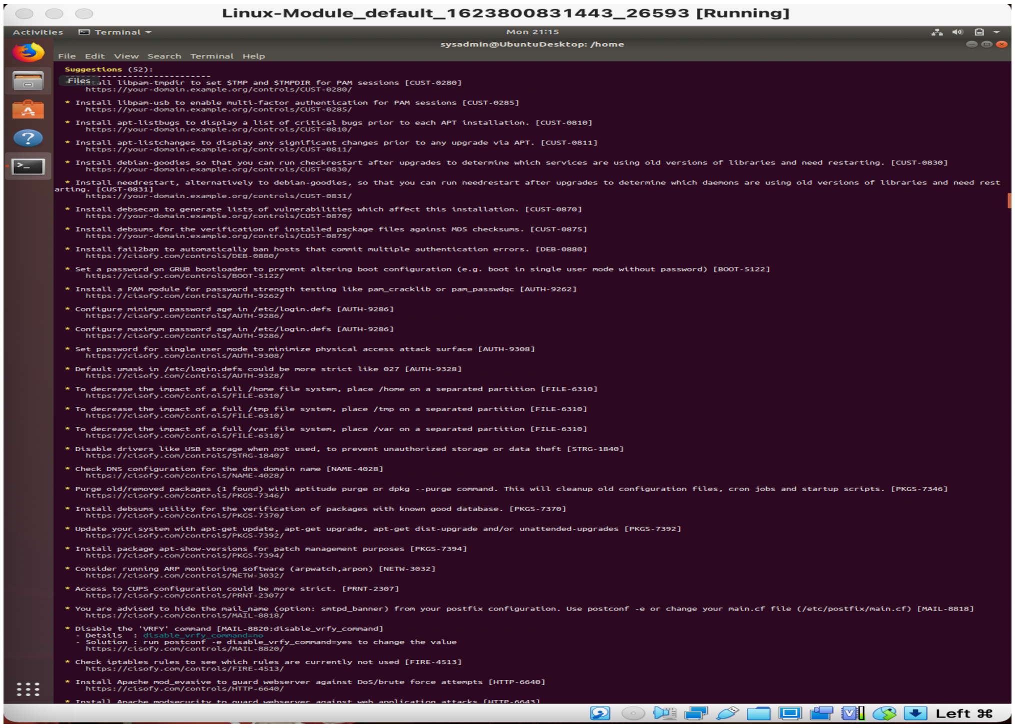
1. Command to install Lynis: `sudo apt-get install -y lynis`

2. Command to see documentation and instructions: `man lynis`

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

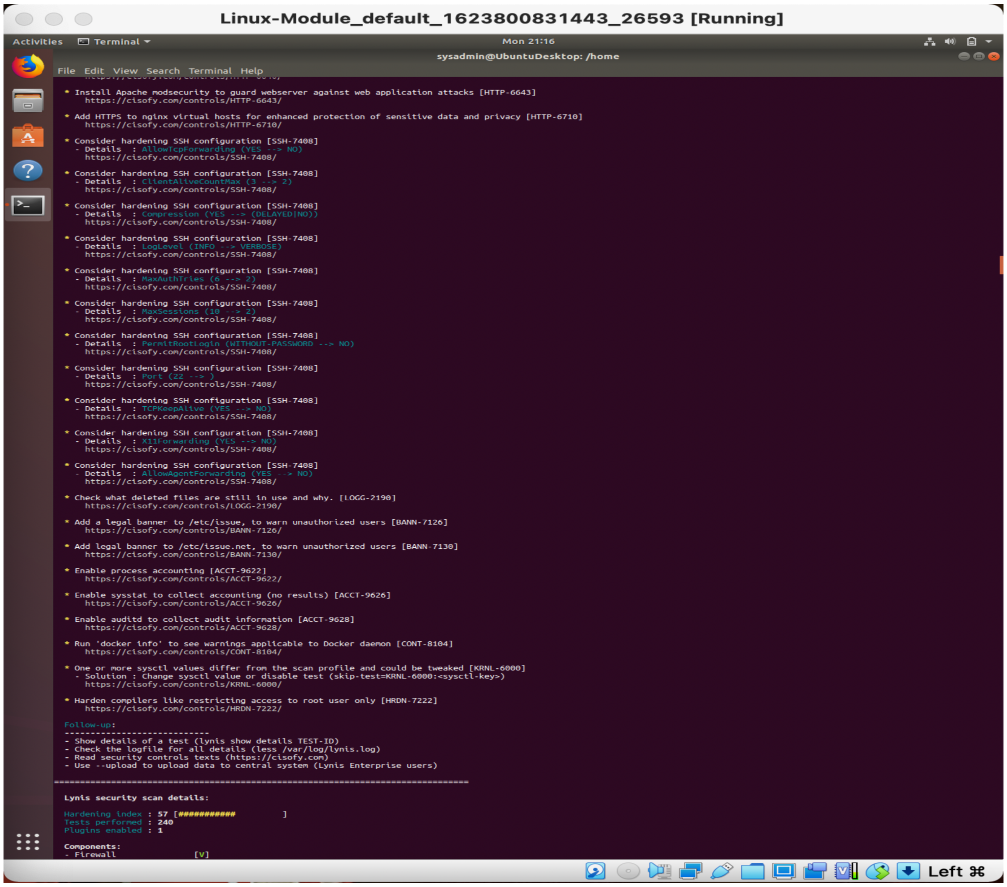
4. Provide a report from the Lynis output on what can be done to harden the system.

   - Screenshot of report output:



Linux-Module_default_1623800831443_26593 [Running]
Activities
Terminal
Mon 21:15
sysadmin@UbuntuDesktop: /home
File
Edit
View
Search
Terminal
Help
Files
Left ⌘

```
 Suggestions (52):
 ----------------------------
   Files all 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/

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

 * Install debian-goodies so that you can run checkrestart after upgrades to determine which services 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 rest
arting. [CUST-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 single user mode without password) [BOOT-5122]
     https://cisofy.com/controls/BOOT-5122/

 * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
     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 [FILE-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 theft [STRG-1840]
     https://cisofy.com/controls/STRG-1840/

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

 * Purge old/removed packages (1 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-7370]
     https://cisofy.com/controls/PKGS-7370/

 * Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]
     https://cisofy.com/controls/PKGS-7392/

 * 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]
```



Linux-Module_default_1623800831443_26593 [Running]
Activities
Terminal
Mon 21:16
sysadmin@UbuntuDesktop: /home
File
Edit
View
Search
Terminal
Help
Left ⌘

```
     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]
   - 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  : 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]
     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 : 57 [###########         ]
 Tests performed : 240
 Plugins enabled : 1

 Components:
 - Firewall               [V]
```

Bonus

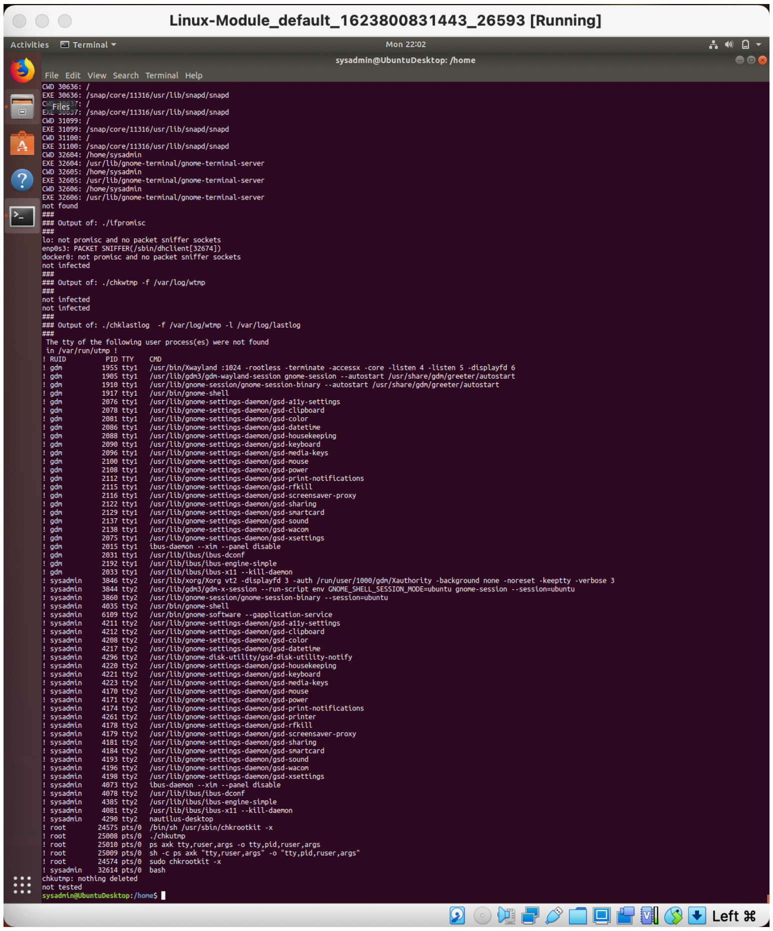
1. Command to install chkrootkit: sudo apt-get install chkrootkit -y

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:



Linux-Module_default_1623800831443_26593 [Running]
Activities
Terminal
Mon 22:02
sysadmin@UbuntuDesktop: /home
File Edit View Search Terminal Help
Files
Left ⌘

```
CWD 30636: /
EXE 30636: /snap/core/11316/usr/lib/snapd/snapd
CWD 30637: /
EXE 30637: /snap/core/11316/usr/lib/snapd/snapd
CWD 31099: /
EXE 31099: /snap/core/11316/usr/lib/snapd/snapd
CWD 31100: /
EXE 31100: /snap/core/11316/usr/lib/snapd/snapd
CWD 32604: /home/sysadmin
EXE 32604: /usr/lib/gnome-terminal/gnome-terminal-server
CWD 32605: /home/sysadmin
EXE 32605: /usr/lib/gnome-terminal/gnome-terminal-server
CWD 32606: /home/sysadmin
EXE 32606: /usr/lib/gnome-terminal/gnome-terminal-server
not found
###
### Output of: ./ifpromisc
###
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/sbin/dhclient[32674])
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          1955 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm          1905 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1910 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm          1917 tty1   /usr/bin/gnome-shell
! gdm          2076 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          2078 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          2081 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          2086 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          2088 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          2090 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          2096 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2100 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2108 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2112 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2115 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          2129 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2137 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2138 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2075 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          2015 tty1   ibus-daemon --xim --panel disable
! gdm          2031 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2192 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          2033 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     3846 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin     3844 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin     3860 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     4035 tty2   /usr/bin/gnome-shell
! sysadmin     6109 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     4211 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     4212 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     4208 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     4217 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     4296 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     4220 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     4221 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     4223 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     4170 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     4171 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     4174 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     4261 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     4178 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     4179 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     4181 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     4184 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     4193 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     4196 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     4198 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     4073 tty2   ibus-daemon --xim --panel disable
! sysadmin     4078 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     4385 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     4081 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     4290 tty2   nautilus-desktop
! root        24575 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root        25008 pts/0  ./chkutmp
! root        25010 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        25009 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        24574 pts/0  sudo chkrootkit -x
! sysadmin    32614 pts/0  bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:/home$ 
```