HW4: 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): `Currently it is correct, but if not then:` **`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): `Currently it is correct, but if not then:` **`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  adduser  sam  # and answer the questions
sudo  adduser  joe  #  for each one
sudo  adduser  amy
sudo  adduser  sara
sudo  adduser  admin
```

2. Ensure that only the admin has general sudo access. **# What is "general"?**

```
sudo cat /etc/sudoers /etc/sudoers.d/* | \
          grep -v "^#\s" |grep -v "^Defaults" |sort

# My vm returns something like this:


     #
     #
     %admin ALL=(ALL) ALL
     #includedir /etc/sudoers.d
     max  ALL=(ALL:ALL) /usr/bin/less
     root  ALL=(ALL:ALL) ALL
     %sudo ALL=(ALL:ALL) ALL
     vagrant ALL=(ALL:ALL) NOPASSWD:ALL

sudo visudo  # use visudo to comment out the line for max
             # I choose to keep %admin, root, %sudo, vagrant
             # Rerun above sudo+cat command, ‘cuz might
             #  need to edit files in /etc/sudoers.d
sudo cat /etc/sudoers /etc/sudoers.d/* | \
          grep -v "^#\s" |grep -v "^Defaults" |sort
Result confirms max is gone
             # Now need to verify members of %admin, %sudo

sudo apt install members    # ‘members’ will id all members of
sudo members sudo           # a group either by numerics or text
My vm returns this:
     sysadmin instructor student     # I can accept this

sudo members admin
My vm returns this:
     admin admin    # means user admin is the only member of
          # group admin and is both a primary+secondary member
```

- Command to add admin to the sudo group:

  ```
  sudo usermod -aG sudo admin
       # now user admin has sudo capabilities through
       # two groups: admin and sudo
  ```

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 sam:engineers /home/engineers
sudo chmod  770  /home/engineers
sudo su - amy       # ----- NOW FOR SOME TESTS ----------
whoami   # answer is amy (as expected)
touch /home/engineers/AmysFile     # success
ls -l /home/engineers/A*     # shows file is 664 <that's OK
umask    # returns 0002, which is good for group sharing
```

Step 4: Lynis Auditing

1. Command to install Lynis: **In a time of software supply chain attacks, we need to be aware of tradeoffs as we select and enable software repositories. One could use the latest version of Lynis, as provided directly by CISOFY. The latest version probably includes additional tests to detect more or newer vulnerabilities. Or one could favor the Ubuntu Maintainer's repo, which is a version or two behind. Ubuntu applications have been used / tested by others, and more eyes have had an opportunity to review the code. Those steps would reduce the chance of a supply chain attack.**

    Since I'm working on throwaway VMs, I'll do both and compare.

    (A) CISOFY installation instructions are from
    https://packages.cisofy.com/community/#debian-ubuntu

```
sudo apt-key adv --keyserver keyserver.ubuntu.com \
   --recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4

# instructions suggest the next step is as shown below.
# but "apt show apt-transport-https" tells us this is a
# transitional package during apt 1.5. We are using apt 1.6,
# So I will SKIP this step.
sudo apt install apt-transport-https     ##SKIPPING
# Now continuing with setup of cisofy apt repository

echo 'Acquire::Languages "none";'    \
        | sudo tee /etc/apt/apt.conf.d/99disable-translations
WEBPAGE='https://packages.cisofy.com/community/lynis/deb/stable'
echo "deb ${WEBPAGE} main" | sudo tee         \
        /etc/apt/sources.list.d/cisofy-lynis.list

# Now install the latest and verify version number
sudo apt show -a lynis     # shows there are two packages in
           # the repos. Maintainer for 3.0.6 is CISOFY, for 2.6.2
           # it is Ubuntu Developers.  Here we try 3.0.6.
sudo apt install lynis
sudo lynis show version
# Answer is 3.0.2   that's the latest from CISOFY
sudo lynis show tests | grep -v '^#' | wc -l   # shows 440 tests
```

(B) UBUNTU REPO installation or update - on a different VM

```
sudo apt update; sudo apt upgrade
sudo lynis show version
# Answer is 2.6.2   that's the latest from Ubuntu Maintainers
sudo lynis show tests | grep -v '^#' | wc -l   # shows 382 tests
```

COMPARISON and RISK ACCEPTANCE

```
The changelog for Lynis shows:
  2.6.2 released 2018-02-13 = Over 4 years and 20 releases ago.
  3.0.6 released 2021-07-22 = Over 2 months old.
For this exercise, I accept risk for +58 tests, and use 3.0.6.
```

2. Command to see documentation and instructions:

```
# Full Documentation is at  https://cisofy.com/lynis/
# Also:
man lynis
```

3. Command to run an audit:

```
sudo lynis audit system --auditor "Ralph P" --no-color
```

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

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

  -[ Lynis 3.0.6 Results ]-  Recommended Actions to Harden

  Warnings (1):
  ----------------------------
  ! Found some information disclosure in SMTP banner (OS or software name)
[MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/


  Suggestions (52):
  ----------------------------
  * 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/

  * 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/
  * 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]
      https://cisofy.com/lynis/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/lynis/controls/PKGS-7346/
  * Install debsums utility for the verification of packages with known good
database. [PKGS-7370]
      https://cisofy.com/lynis/controls/PKGS-7370/
  * Install package apt-show-versions for patch management purposes[PKGS-7394]
      https://cisofy.com/lynis/controls/PKGS-7394/
  * Determine if protocol 'dccp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/
  * Determine if protocol 'sctp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/
  * Determine if protocol 'rds' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/
  * Determine if protocol 'tipc' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/
  * Access to CUPS configuration could be more strict. [PRNT-2307]
      https://cisofy.com/lynis/controls/PRNT-2307/
  * Check CUPS configuration if it really needs to listen on the network
[PRNT-2308]
      https://cisofy.com/lynis/controls/PRNT-2308/
  * 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/lynis/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/lynis/controls/MAIL-8820/
  * Check iptables rules to see which rules are currently not used [FIRE-4513]
      https://cisofy.com/lynis/controls/FIRE-4513/
  * Install Apache mod_evasive to guard webserver against DoS/brute force
attempts [HTTP-6640]
      https://cisofy.com/lynis/controls/HTTP-6640/
  * Install Apache modsecurity to guard webserver against web application
attacks [HTTP-6643]
      https://cisofy.com/lynis/controls/HTTP-6643/
  * Add HTTPS to nginx virtual hosts for enhanced protection of sensitive data
and privacy [HTTP-6710]
      https://cisofy.com/lynis/controls/HTTP-6710/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
      https://cisofy.com/lynis/controls/SSH-7408/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Compression (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
      https://cisofy.com/lynis/controls/SSH-7408/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
      https://cisofy.com/lynis/controls/SSH-7408/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
      https://cisofy.com/lynis/controls/SSH-7408/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
      https://cisofy.com/lynis/controls/SSH-7408/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (set YES to NO)
```

```
      https://cisofy.com/lynis/controls/SSH-7408/

  * Enable logging to an external logging host for archiving purposes and
additional protection [LOGG-2154]

      https://cisofy.com/lynis/controls/LOGG-2154/

  * Check what deleted files are still in use and why. [LOGG-2190]

      https://cisofy.com/lynis/controls/LOGG-2190/

  * If there are no xinetd services required, it is recommended that the
daemon be removed [INSE-8100]

      https://cisofy.com/lynis/controls/INSE-8100/

  * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]

      https://cisofy.com/lynis/controls/BANN-7126/

  * 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)
================================================================================
```

Bonus

1. Command to install chkrootkit:

```
# Version 0.52 is available from the Ubuntu Developers.
sudo apt install chkrootkit

# Version 0.55 is available for download from chkrootkit.org
  mkdir ~/chkrootkit
  cd chkrootkit
  wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
  wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.md5
  #verify checksum matches
  cat chkrootkit.md5 ; md5sum chkrootkit.tar.gz
           # compare visually, proceed if the checksums match
  tar -xzvf chkrootkit.tar.gz
  cd ~chkrootkit/chkrootkit-0.55/   # cd here to run commands
  make sense
```

2. Command to see documentation and instructions:

```
# if you used ‘apt install’ you can view the man page
man chkrootkit
# if you installed from tarball, you need to be in this dir
cd ~/chkrootkit/chkrootkit-0.55 ; less README*

# With both installation methods, you can
# also visit http://www.chkrootkit.org/books/   and visit
https://www.alibabacloud.com/blog/how-to-install-chkrootkit-security-scanner-on-ubuntu-18-04_595711
sudo chkrootkit -l  # to see the available rootkits tests
sudo chkrootkit -h  # to see options
```

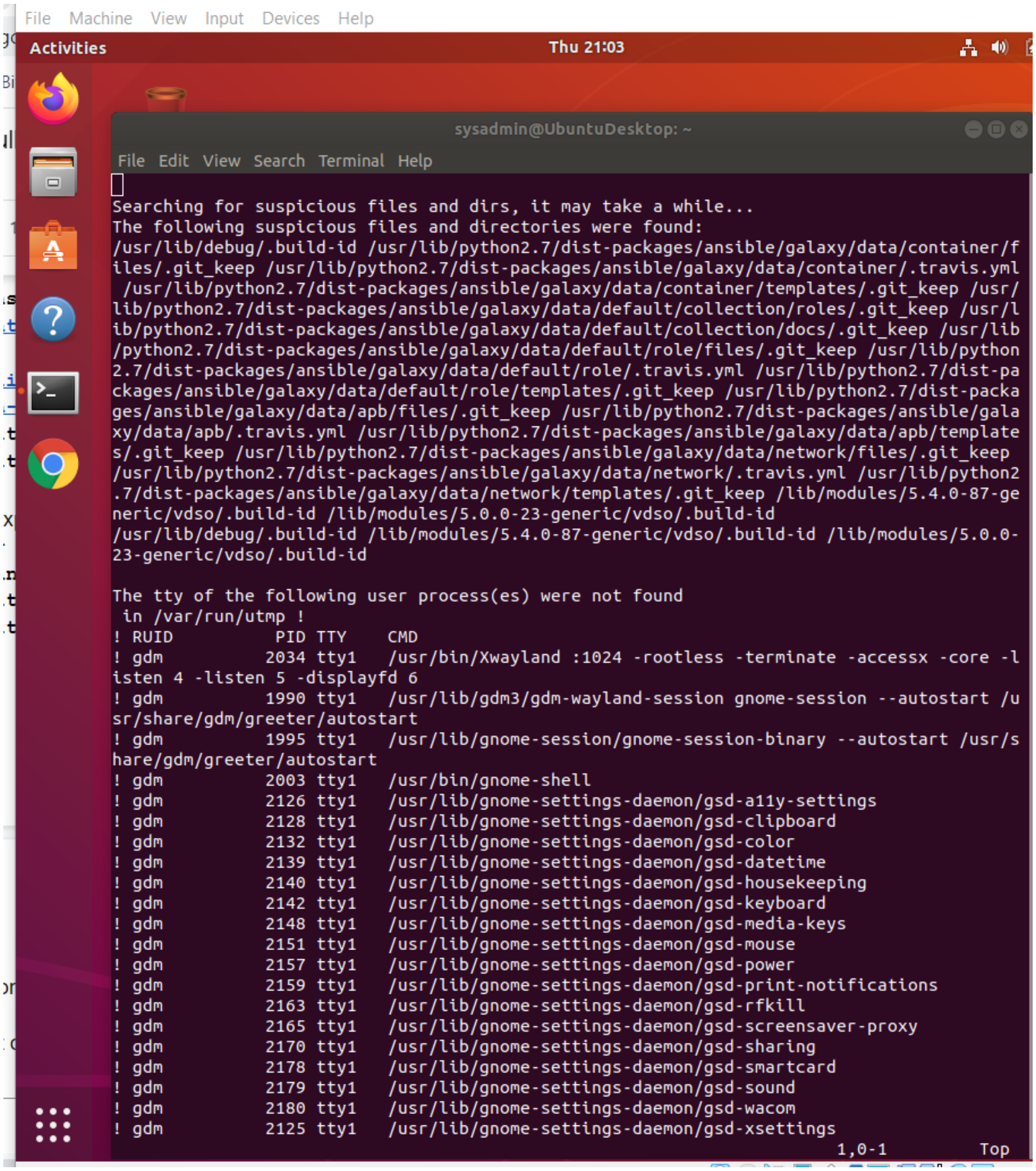
3. Command to run expert mode:

```
cd ~/chkrootkit/chkrootkit-0.55 # again, this is if from tarball
sudo ./chkrootkit -x | egrep '^/'
# and look for suspicious strings in binaries..
# These two commands can also be helpful
sudo ./chkrootkit -q  # quiet mode only reports issues + grep
sudo ./chkrootkit |egrep -C 5 'INFECTED|Vulnerable but disabled'
```

```
# Ignore the grep process itself. There are no other matches
```

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

Actions: Investigate these files and directories. Investigate the following list of processes.


File Machine View Input Devices Help
Activities
Thu 21:03
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
Searching for suspicious files and dirs, it may take a while...
The following suspicious files and directories were found:
/usr/lib/debug/.build-id /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/f
iles/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/.travis.yml
 /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/templates/.git_keep /usr/
lib/python2.7/dist-packages/ansible/galaxy/data/default/collection/roles/.git_keep /usr/l
ib/python2.7/dist-packages/ansible/galaxy/data/default/collection/docs/.git_keep /usr/lib
/python2.7/dist-packages/ansible/galaxy/data/default/role/files/.git_keep /usr/lib/python
2.7/dist-packages/ansible/galaxy/data/default/role/.travis.yml /usr/lib/python2.7/dist-pa
ckages/ansible/galaxy/data/default/role/templates/.git_keep /usr/lib/python2.7/dist-packa
ges/ansible/galaxy/data/apb/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/gala
xy/data/apb/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/template
s/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/files/.git_keep
/usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/.travis.yml /usr/lib/python2
.7/dist-packages/ansible/galaxy/data/network/templates/.git_keep /lib/modules/5.4.0-87-ge
neric/vdso/.build-id /lib/modules/5.0.0-23-generic/vdso/.build-id
/usr/lib/debug/.build-id /lib/modules/5.4.0-87-generic/vdso/.build-id /lib/modules/5.0.0-
23-generic/vdso/.build-id

The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2034 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -l
isten 4 -listen 5 -displayfd 6
! gdm          1990 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /u
sr/share/gdm/greeter/autostart
! gdm          1995 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/s
hare/gdm/greeter/autostart
! gdm          2003 tty1   /usr/bin/gnome-shell
! gdm          2126 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          2128 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          2132 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          2139 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          2140 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          2142 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          2148 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2151 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2157 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2159 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2163 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2165 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2170 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2178 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2179 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2180 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2125 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
                                                                 1,0-1         Top
```