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 chown root:root /etcgshadow
```

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 chown root:root /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 chown root:root /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 adduser sam
sudo adduser amy
sudo adduser sara
sudo adduser 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 -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`.

    a. Command to create the shared folder:

```
sudo 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 -R /home/engineers
```

Step 4: Lynis Auditing

Source: 4.1 Linux SysAdmin notes on GitLab

1. Command to install Lynis:

```
sudo apt install lynis
```

2. Command to view documentation and instructions:

```
 man lynis
```

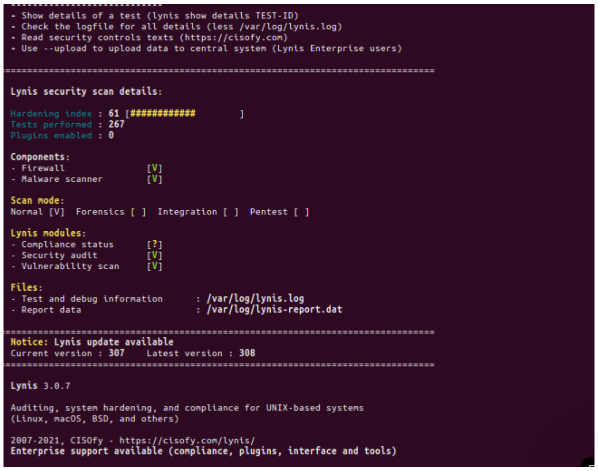
3. Command to run an audit:

```
sudo lynis audit system
```

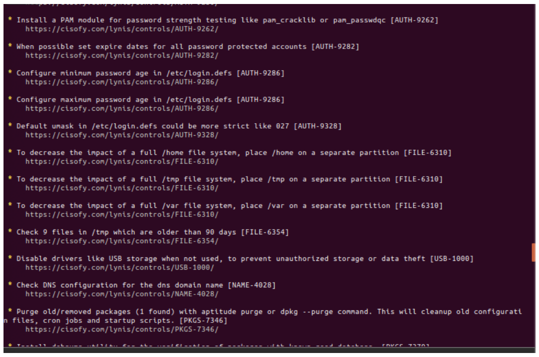
Source: https://adamtheautomator.com/lynis/

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

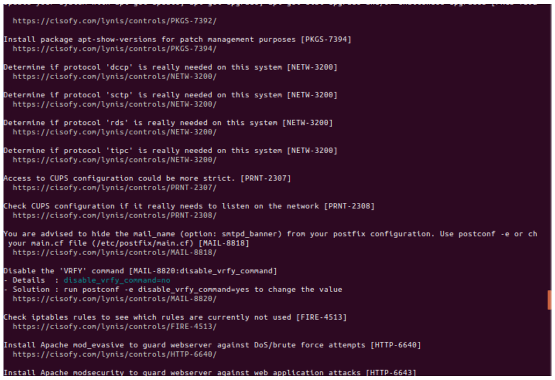
   a. Screenshot of report output:



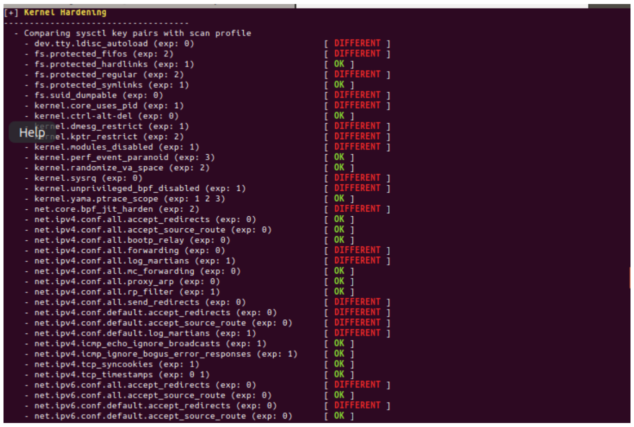
```
  - Show details of a test (lynis show details TEST-ID)
  - Check the logfile for all details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data to central system (Lynis Enterprise users)

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

  Lynis security scan details:

  Hardening index : 61 [############        ]
  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]

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

================================================================================
  Notice: Lynis update available
  Current version : 307    Latest version : 308
================================================================================

  Lynis 3.0.7

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

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
```



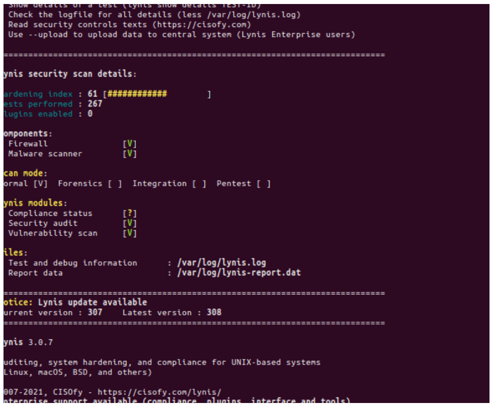
```
  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
      https://cisofy.com/lynis/controls/AUTH-9262/

  * 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/

  * 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]
      https://cisofy.com/lynis/controls/NAME-4028/

  * Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configurati
n 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]
```



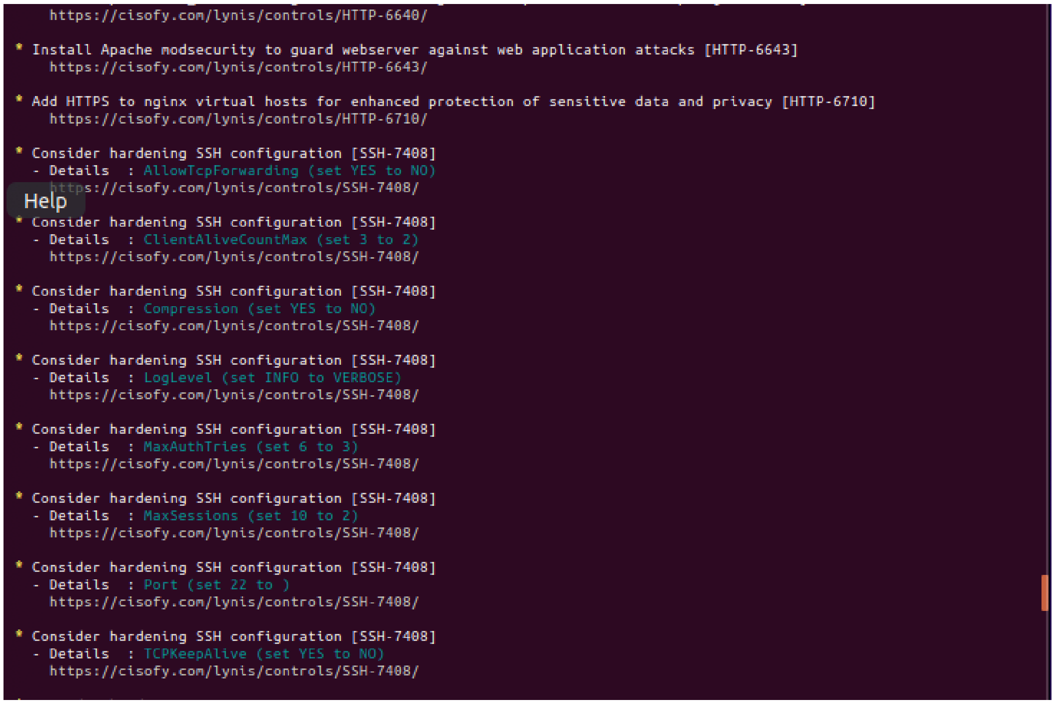
```
  https://cisofy.com/lynis/controls/PKGS-7392/

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 ch
 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]
```



```
[+] Kernel Hardening
------------------------------------
  - Comparing sysctl key pairs with scan profile
    - dev.tty.ldisc_autoload (exp: 0)                         [ DIFFERENT ]
    - fs.protected_fifos (exp: 2)                             [ DIFFERENT ]
    - fs.protected_hardlinks (exp: 1)                         [ OK ]
    - fs.protected_regular (exp: 2)                           [ DIFFERENT ]
    - fs.protected_symlinks (exp: 1)                          [ OK ]
    - fs.suid_dumpable (exp: 0)                               [ DIFFERENT ]
    - kernel.core_uses_pid (exp: 1)                           [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                            [ OK ]
    - kernel.dmesg_restrict (exp: 1)                          [ DIFFERENT ]
    - kernel.kptr_restrict (exp: 2)                           [ DIFFERENT ]
    - kernel.modules_disabled (exp: 1)                        [ DIFFERENT ]
    - kernel.perf_event_paranoid (exp: 3)                     [ OK ]
    - kernel.randomize_va_space (exp: 2)                      [ OK ]
    - kernel.sysrq (exp: 0)                                   [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)               [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                   [ OK ]
    - net.core.bpf_jit_harden (exp: 2)                        [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)             [ OK ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)          [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)                  [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)                   [ DIFFERENT ]
    - net.ipv4.conf.all.log_martians (exp: 1)                 [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)                [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                    [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                    [ OK ]
    - net.ipv4.conf.all.send_redirects (exp: 0)               [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)         [ DIFFERENT ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)      [ DIFFERENT ]
    - net.ipv4.conf.default.log_martians (exp: 1)             [ DIFFERENT ]
    - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)           [ OK ]
    - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)     [ OK ]
    - net.ipv4.tcp_syncookies (exp: 1)                        [ OK ]
    - net.ipv4.tcp_timestamps (exp: 0 1)                      [ OK ]
    - net.ipv6.conf.all.accept_redirects (exp: 0)             [ DIFFERENT ]
    - net.ipv6.conf.all.accept_source_route (exp: 0)          [ OK ]
    - net.ipv6.conf.default.accept_redirects (exp: 0)         [ DIFFERENT ]
    - net.ipv6.conf.default.accept_source_route (exp: 0)      [ OK ]
```



```
 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)

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

ynis security scan details:

ardening index : 61 [############        ]
ests performed : 267
lugins enabled : 0

omponents:
 Firewall               [V]
 Malware scanner        [V]

can mode:
ormal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

ynis modules:
 Compliance status      [?]
 Security audit         [V]
 Vulnerability scan     [V]

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

================================================================================
otice: Lynis update available
urrent version : 307    Latest version : 308
================================================================================

ynis 3.0.7

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

007-2021, CISOfy - https://cisofy.com/lynis/
nterprise support available (compliance, plugins, interface and tools)
```



```
    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/
```

Bonus

1. Command to install chkrootkit:

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

2. Command to view documentation and instructions:

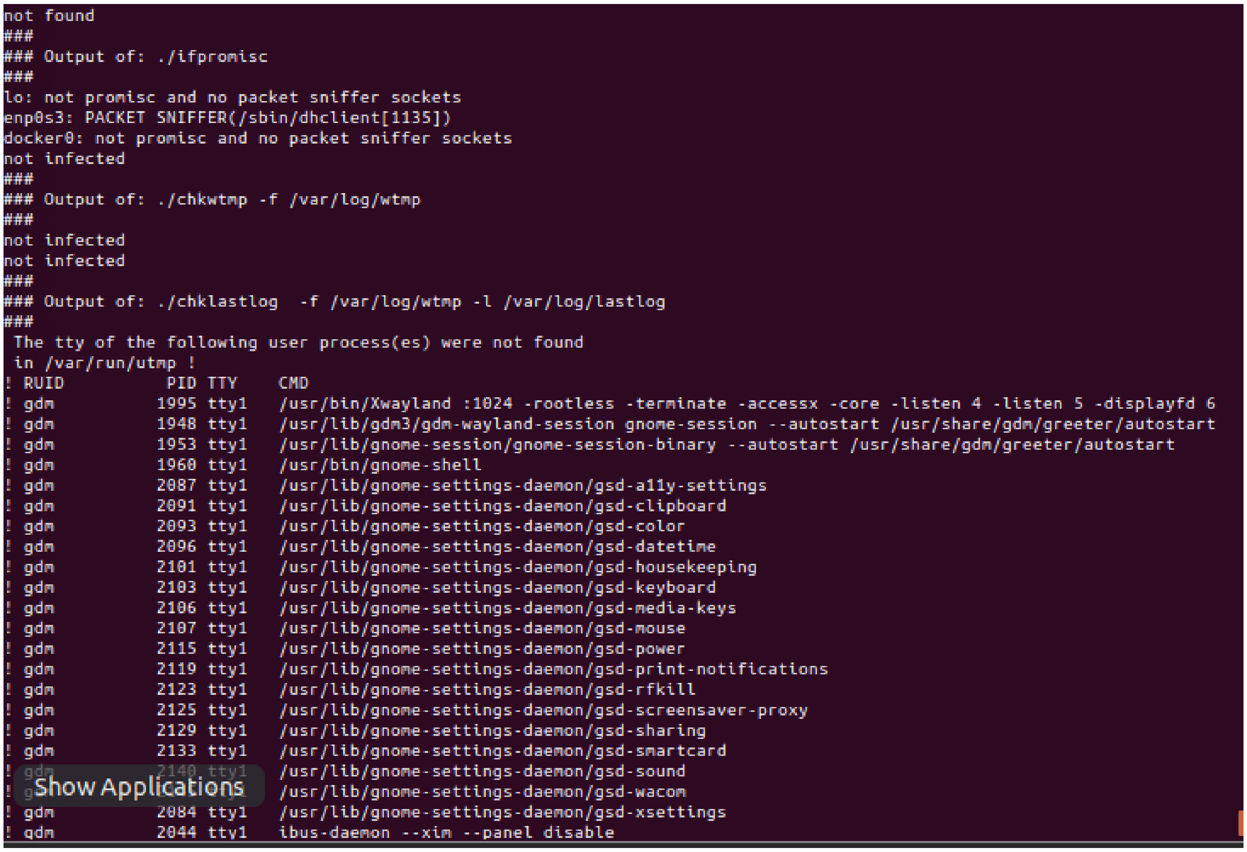
```
man chlrootkit
```

3. Command to run expert mode:

```
sudo chkrootkit -x
```

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

    a. Screenshot of end of sample output:



```
not found
###
### Output of: ./ifpromisc
###
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/sbin/dhclient[1135])
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          1995 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm          1948 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1953 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm          1960 tty1   /usr/bin/gnome-shell
! gdm          2087 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          2091 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          2093 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          2096 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          2101 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          2103 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          2106 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2107 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2115 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2119 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2123 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2125 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2129 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2133 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2140 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! g[illegible]             /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2084 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          2044 tty1   ibus-daemon --xim --panel disable
```

Sources

https://umn.bootcampcontent.com/University-of-Minnesota-Boot-Camp/UofM-VIRT-CYBER-PT-09-2022-U-LOLC/-/blob/main/04-Linux-SysAdmin-Fundamentals/1/StudentGuide.md

https://adamtheautomator.com/lynis/

https://umn.bootcampcontent.com/University-of-Minnesota-Boot-Camp/UofM-VIRT-CYBER-PT-09-2022-U-LOLC/-/blob/main/04-Linux-SysAdmin-Fundamentals/3/Activities/03_Permissions/Solved/README.md

I also rewatched recordings!