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 sam

Sudo useradd joe

Sudo useradd amy

Sudo useradd sara

Sudo useradd 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 -p /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 chgrp engineers /home/engineers
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
Sudo apt install lynis
```

2. Command to view documentation and instructions:

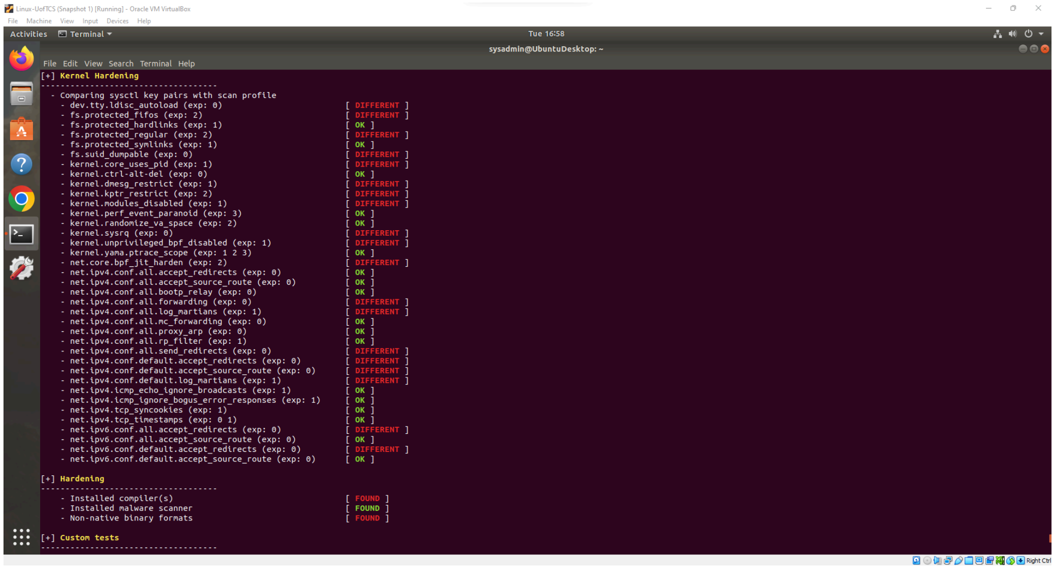
```
Lynis --help
Man lynis
```

3. Command to run an audit:

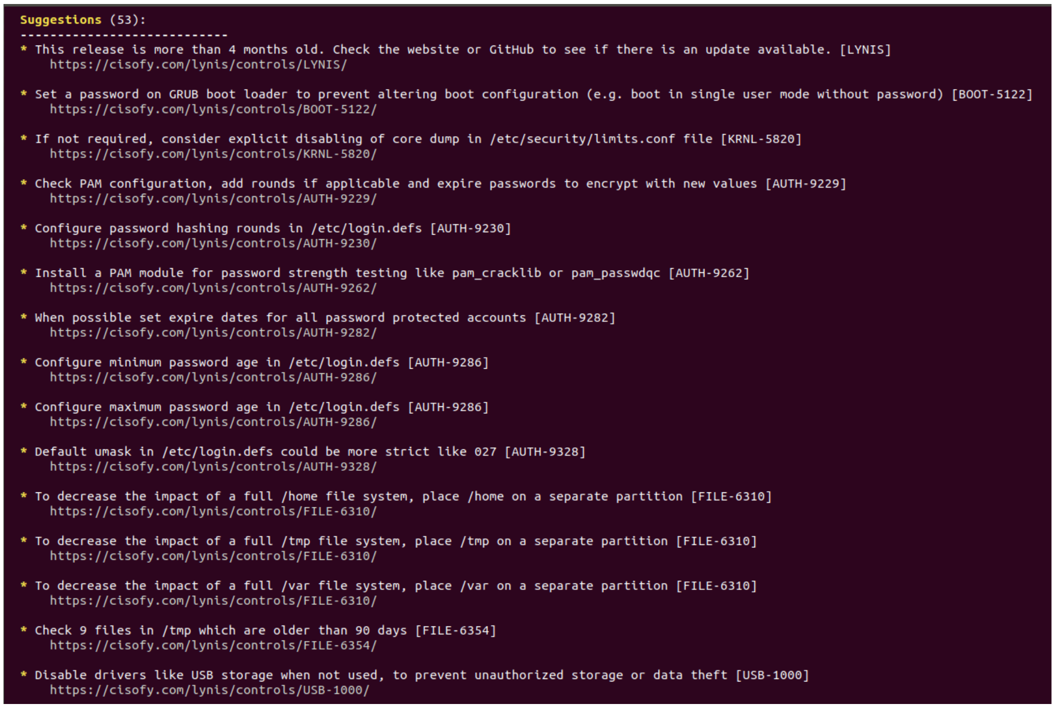
```
Sudo lynis audit system
```

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

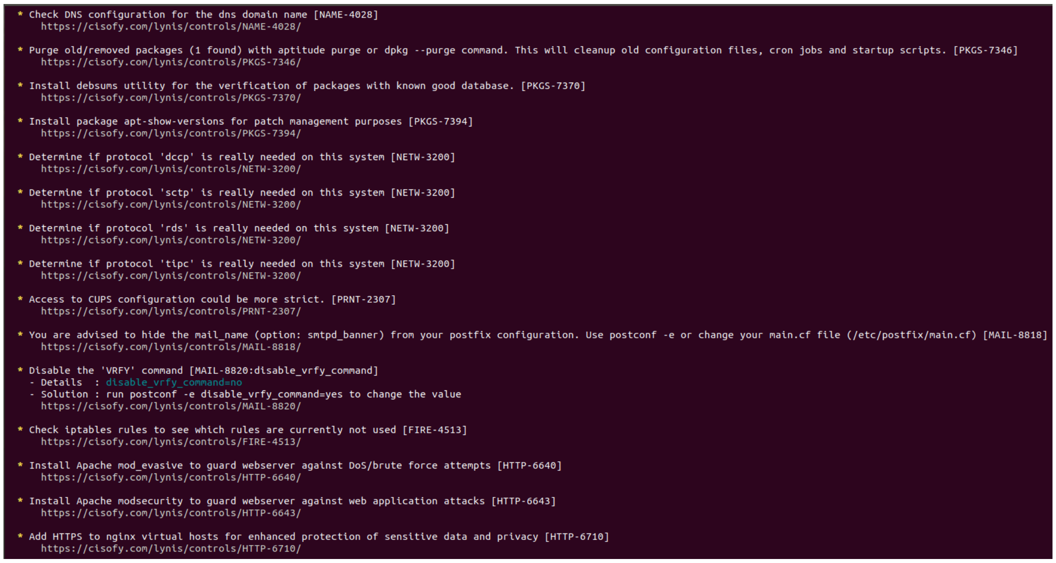
   a. Screenshot of report output:


Linux-UofTCS (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 16:58
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

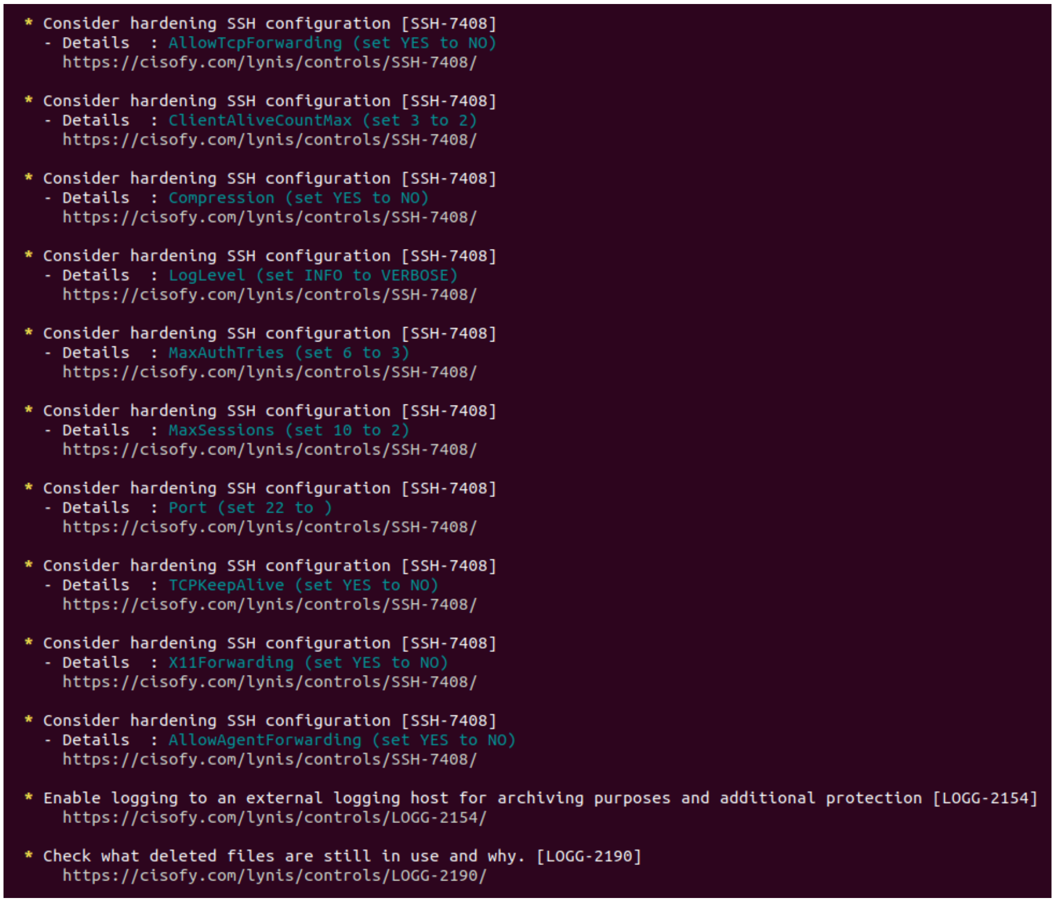
```
[+] Kernel Hardening
------------------------------------
  - Comparing sysctl key pairs with scan profile
    - dev.tty.ldisc_autoload (exp: 0)                           [ DIFFERENT ]
    - fs.protected_fifos (exp: 2)                               [ DIFFERENT ]
    - fs.protected_hardlinks (exp: 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 ]

[+] Hardening
------------------------------------
    - Installed compiler(s)                                     [ FOUND ]
    - Installed malware scanner                                 [ FOUND ]
    - Non-native binary formats                                 [ FOUND ]

[+] Custom tests
------------------------------------
```



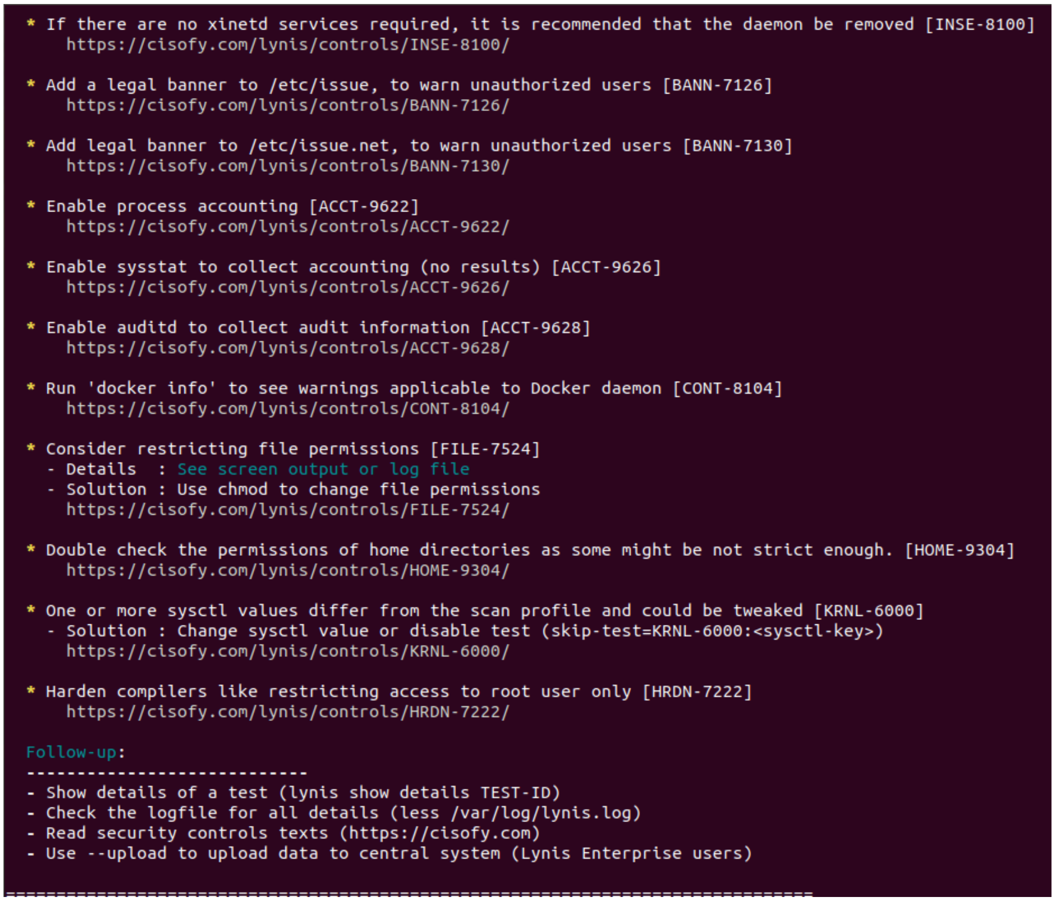
```
Suggestions (53):
----------------------------
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
    https://cisofy.com/lynis/controls/LYNIS/

* 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/

* 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/
```



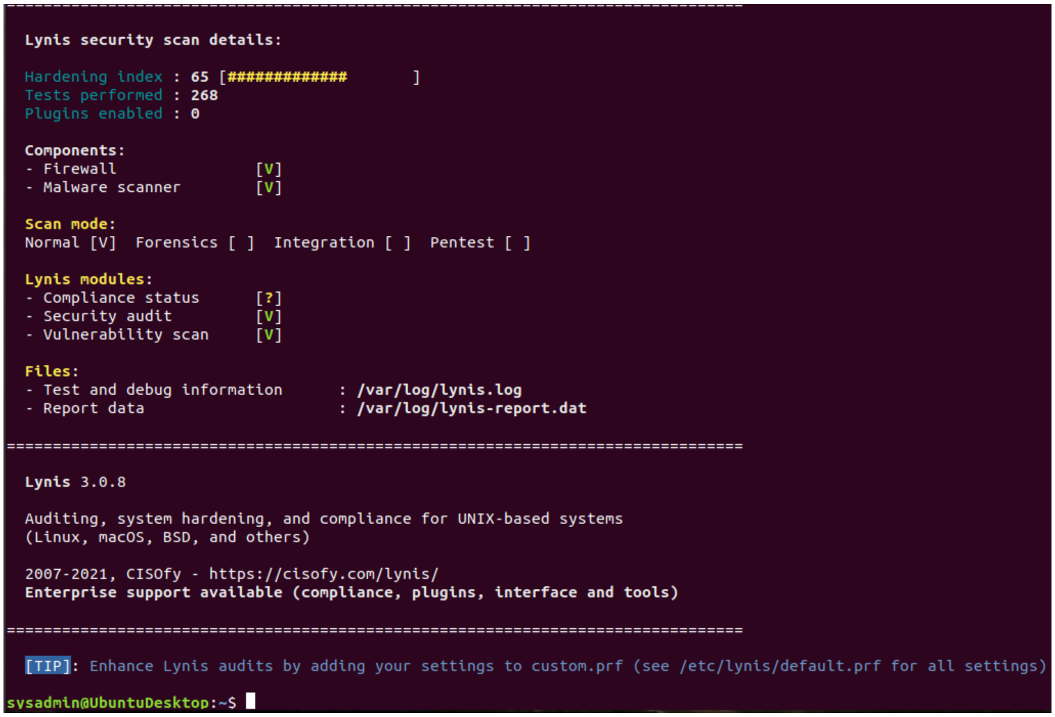
```
* Check DNS configuration for the dns domain name [NAME-4028]
    https://cisofy.com/lynis/controls/NAME-4028/

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

* 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)

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



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

  Lynis security scan details:

  Hardening index : 65 [#############       ]
  Tests performed : 268
  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

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

  Lynis 3.0.8

  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)

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

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

sysadmin@UbuntuDesktop:~$ █
```

Bonus

1. Command to install chkrootkit:

```
Sudo apt install chkrootkit
```

2. Command to view documentation and instructions:

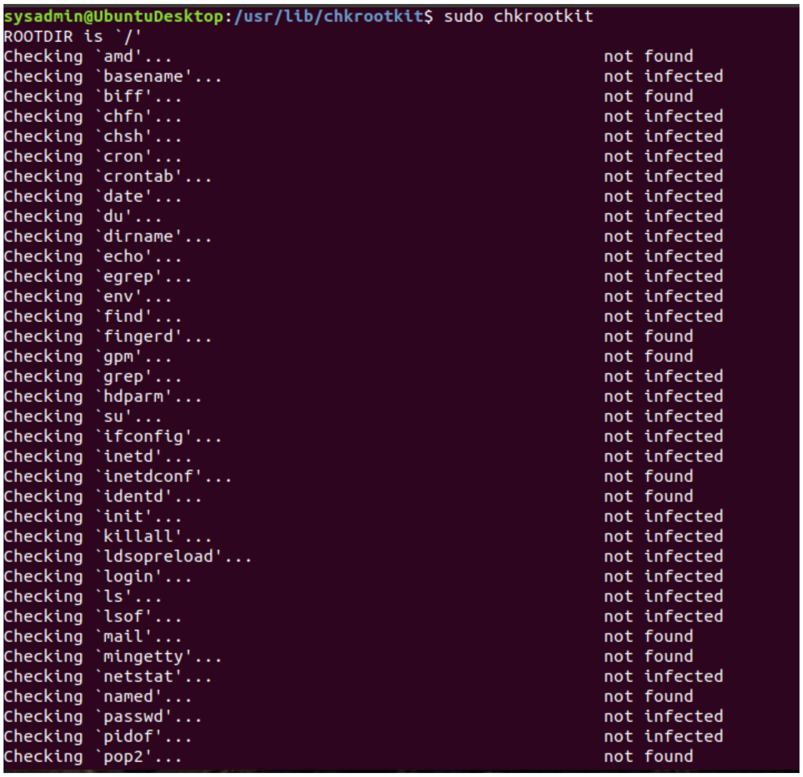
```
Man chkrootkit
Chkrootkit --help
```

3. Command to run expert mode:

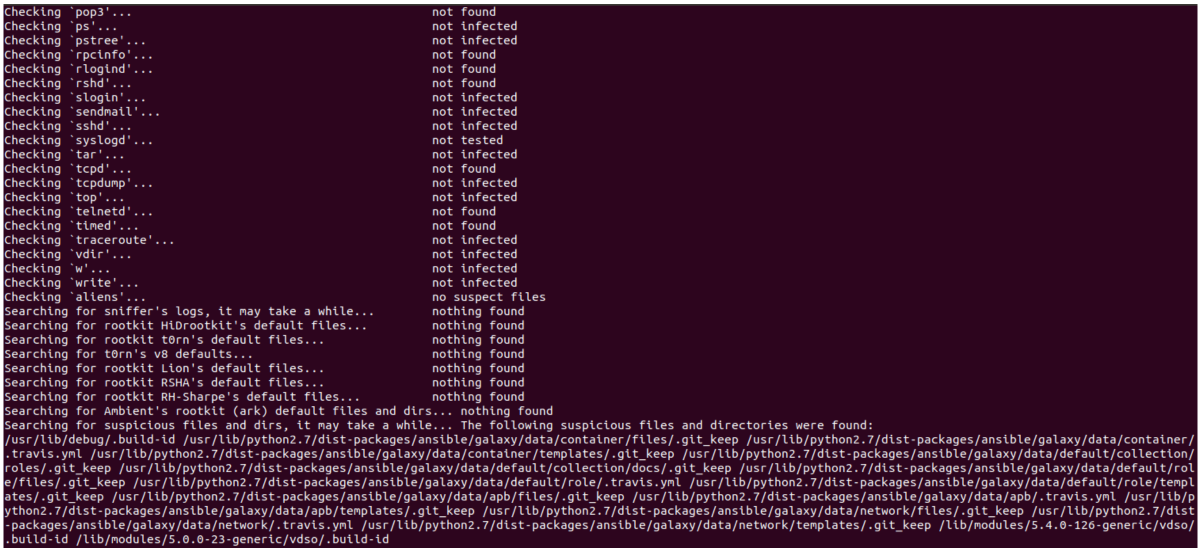
```
Sudo chkrootkit -x
```

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

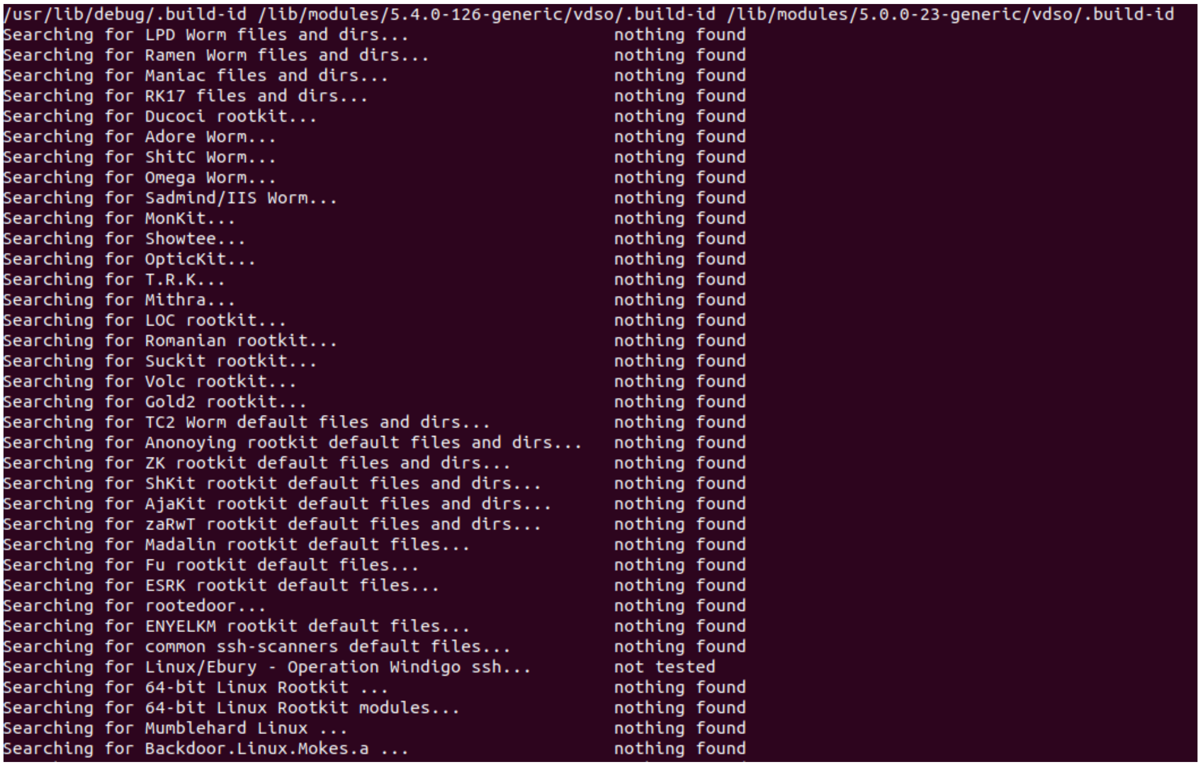
    a. Screenshot of end of sample output:



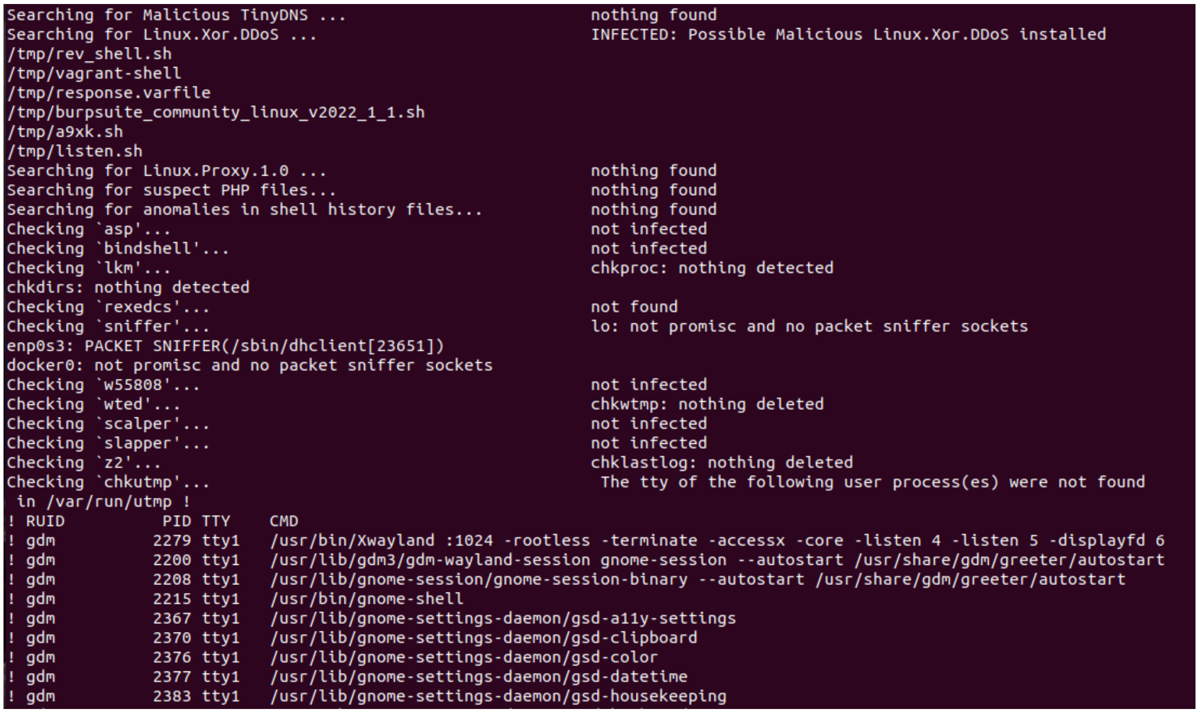
```
sysadmin@UbuntuDesktop:/usr/lib/chkrootkit$ sudo chkrootkit
ROOTDIR is `/'
Checking `amd'...                                           not found
Checking `basename'...                                      not infected
Checking `biff'...                                          not found
Checking `chfn'...                                          not infected
Checking `chsh'...                                          not infected
Checking `cron'...                                          not infected
Checking `crontab'...                                       not infected
Checking `date'...                                          not infected
Checking `du'...                                            not infected
Checking `dirname'...                                       not infected
Checking `echo'...                                          not infected
Checking `egrep'...                                         not infected
Checking `env'...                                           not infected
Checking `find'...                                          not infected
Checking `fingerd'...                                       not found
Checking `gpm'...                                           not found
Checking `grep'...                                          not infected
Checking `hdparm'...                                        not infected
Checking `su'...                                            not infected
Checking `ifconfig'...                                      not infected
Checking `inetd'...                                         not infected
Checking `inetdconf'...                                     not found
Checking `identd'...                                        not found
Checking `init'...                                          not infected
Checking `killall'...                                       not infected
Checking `ldsopreload'...                                   not infected
Checking `login'...                                         not infected
Checking `ls'...                                            not infected
Checking `lsof'...                                          not infected
Checking `mail'...                                          not found
Checking `mingetty'...                                      not found
Checking `netstat'...                                       not infected
Checking `named'...                                         not found
Checking `passwd'...                                        not infected
Checking `pidof'...                                         not infected
Checking `pop2'...                                          not found
```



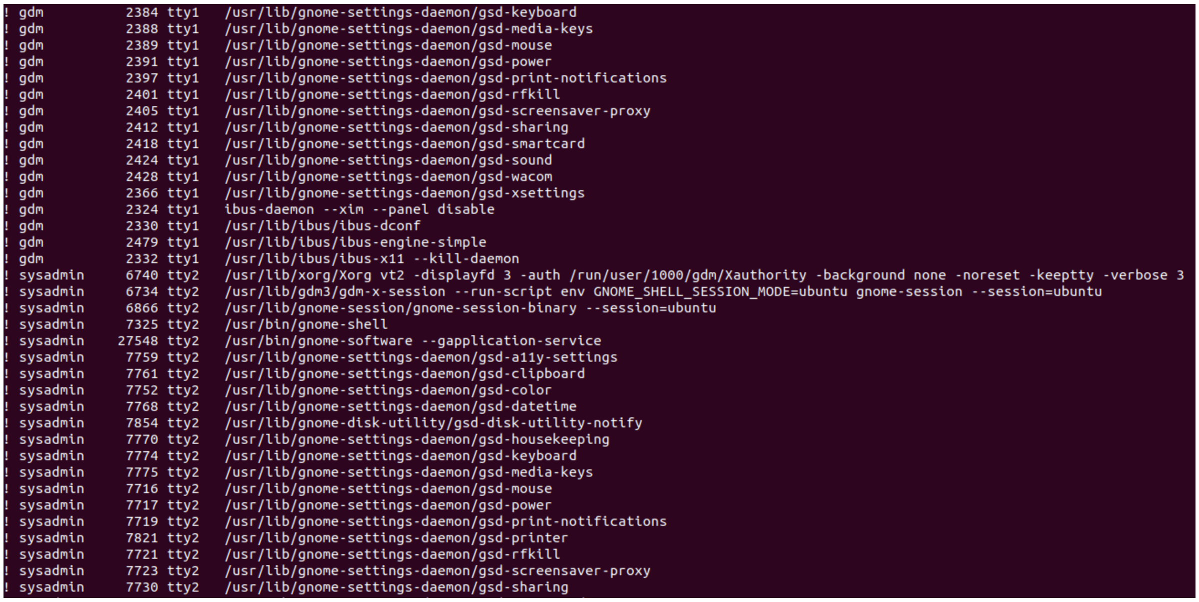
```
Checking `pop3'...                                          not found
Checking `ps'...                                            not infected
Checking `pstree'...                                        not infected
Checking `rpcinfo'...                                       not found
Checking `rlogind'...                                       not found
Checking `rshd'...                                          not found
Checking `slogin'...                                        not infected
Checking `sendmail'...                                      not infected
Checking `sshd'...                                          not infected
Checking `syslogd'...                                       not tested
Checking `tar'...                                           not infected
Checking `tcpd'...                                          not found
Checking `tcpdump'...                                       not infected
Checking `top'...                                           not infected
Checking `telnetd'...                                       not found
Checking `timed'...                                         not found
Checking `traceroute'...                                    not infected
Checking `vdir'...                                          not infected
Checking `w'...                                             not infected
Checking `write'...                                         not infected
Checking `aliens'...                                        no suspect files
Searching for sniffer's logs, it may take a while...        nothing found
Searching for rootkit HiDrootkit's default files...         nothing found
Searching for rootkit t0rn's default files...               nothing found
Searching for t0rn's v8 defaults...                         nothing found
Searching for rootkit Lion's default files...               nothing found
Searching for rootkit RSHA's default files...               nothing found
Searching for rootkit RH-Sharpe's default files...          nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
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/files/.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/lib/python2.7/dist-packages/ansible/galaxy/data/default/collection/docs/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/rol
e/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/templ
ates/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/.travis.yml /usr/lib/p
ython2.7/dist-packages/ansible/galaxy/data/apb/templates/.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/5.4.0-126-generic/vdso/
.build-id /lib/modules/5.0.0-23-generic/vdso/.build-id
```



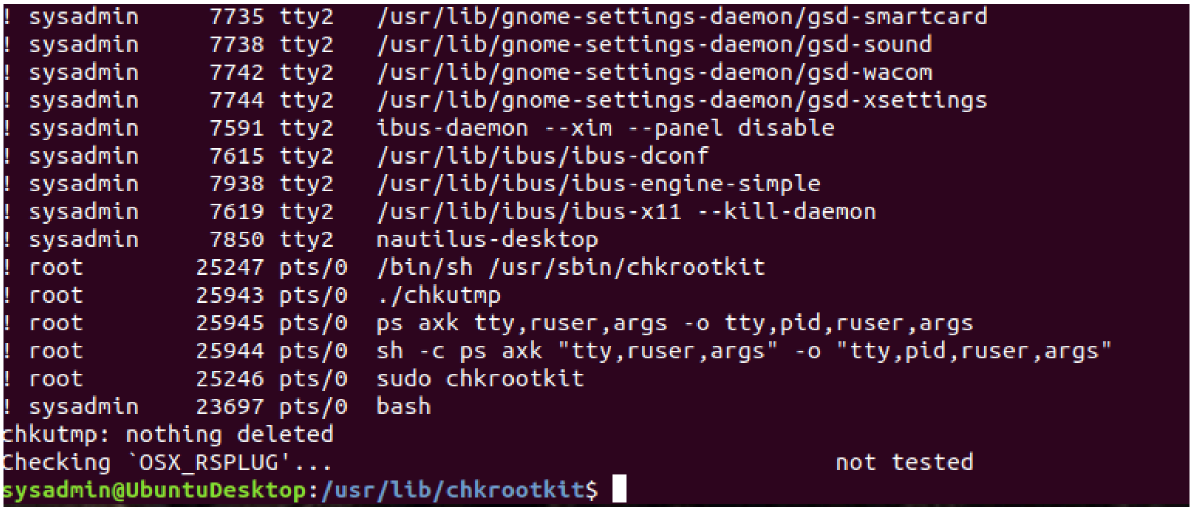
```
/usr/lib/debug/.build-id /lib/modules/5.4.0-126-generic/vdso/.build-id /lib/modules/5.0.0-23-generic/vdso/.build-id
Searching for LPD Worm files and dirs...                    nothing found
Searching for Ramen Worm files and dirs...                  nothing found
Searching for Maniac files and dirs...                      nothing found
Searching for RK17 files and dirs...                        nothing found
Searching for Ducoci rootkit...                             nothing found
Searching for Adore Worm...                                 nothing found
Searching for ShitC Worm...                                 nothing found
Searching for Omega Worm...                                 nothing found
Searching for Sadmind/IIS Worm...                           nothing found
Searching for MonKit...                                     nothing found
Searching for Showtee...                                    nothing found
Searching for OpticKit...                                   nothing found
Searching for T.R.K...                                      nothing found
Searching for Mithra...                                     nothing found
Searching for LOC rootkit...                                nothing found
Searching for Romanian rootkit...                           nothing found
Searching for Suckit rootkit...                             nothing found
Searching for Volc rootkit...                               nothing found
Searching for Gold2 rootkit...                              nothing found
Searching for TC2 Worm default files and dirs...            nothing found
Searching for Anonoying rootkit default files and dirs...   nothing found
Searching for ZK rootkit default files and dirs...          nothing found
Searching for ShKit rootkit default files and dirs...       nothing found
Searching for AjaKit rootkit default files and dirs...      nothing found
Searching for zaRwT rootkit default files and dirs...       nothing found
Searching for Madalin rootkit default files...              nothing found
Searching for Fu rootkit default files...                   nothing found
Searching for ESRK rootkit default files...                 nothing found
Searching for rootedoor...                                  nothing found
Searching for ENYELKM rootkit default files...              nothing found
Searching for common ssh-scanners default files...          nothing found
Searching for Linux/Ebury - Operation Windigo ssh...        not tested
Searching for 64-bit Linux Rootkit ...                      nothing found
Searching for 64-bit Linux Rootkit modules...               nothing found
Searching for Mumblehard Linux ...                          nothing found
Searching for Backdoor.Linux.Mokes.a ...                    nothing found
```



```
Searching for Malicious TinyDNS ...                         nothing found
Searching for Linux.Xor.DDoS ...                            INFECTED: Possible Malicious Linux.Xor.DDoS installed
/tmp/rev_shell.sh
/tmp/vagrant-shell
/tmp/response.varfile
/tmp/burpsuite_community_linux_v2022_1_1.sh
/tmp/a9xk.sh
/tmp/listen.sh
Searching for Linux.Proxy.1.0 ...                           nothing found
Searching for suspect PHP files...                          nothing found
Searching for anomalies in shell history files...           nothing found
Checking `asp'...                                           not infected
Checking `bindshell'...                                     not infected
Checking `lkm'...                                           chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'...                                       not found
Checking `sniffer'...                                       lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/sbin/dhclient[23651])
docker0: not promisc and no packet sniffer sockets
Checking `w55808'...                                        not infected
Checking `wted'...                                          chkwtmp: nothing deleted
Checking `scalper'...                                       not infected
Checking `slapper'...                                       not infected
Checking `z2'...                                            chklastlog: nothing deleted
Checking `chkutmp'...                                        The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2279 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm          2200 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2208 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm          2215 tty1   /usr/bin/gnome-shell
! gdm          2367 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          2370 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          2376 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          2377 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          2383 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
```



```
! gdm          2384 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          2388 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2389 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2391 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2397 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2401 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2405 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2412 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2418 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2424 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2428 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2366 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          2324 tty1   ibus-daemon --xim --panel disable
! gdm          2330 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2479 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          2332 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     6740 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin     6734 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin     6866 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     7325 tty2   /usr/bin/gnome-shell
! sysadmin    27548 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     7759 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     7761 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     7752 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     7768 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     7854 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     7770 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     7774 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     7775 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     7716 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     7717 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     7719 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     7821 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     7721 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     7723 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     7730 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
```



```
! sysadmin     7735 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     7738 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     7742 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     7744 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     7591 tty2   ibus-daemon --xim --panel disable
! sysadmin     7615 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     7938 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     7619 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     7850 tty2   nautilus-desktop
! root        25247 pts/0  /bin/sh /usr/sbin/chkrootkit
! root        25943 pts/0  ./chkutmp
! root        25945 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        25944 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        25246 pts/0  sudo chkrootkit
! sysadmin    23697 pts/0  bash
chkutmp: nothing deleted
Checking `OSX_RSPLUG'...                                 not tested
sysadmin@UbuntuDesktop:/usr/lib/chkrootkit$
```