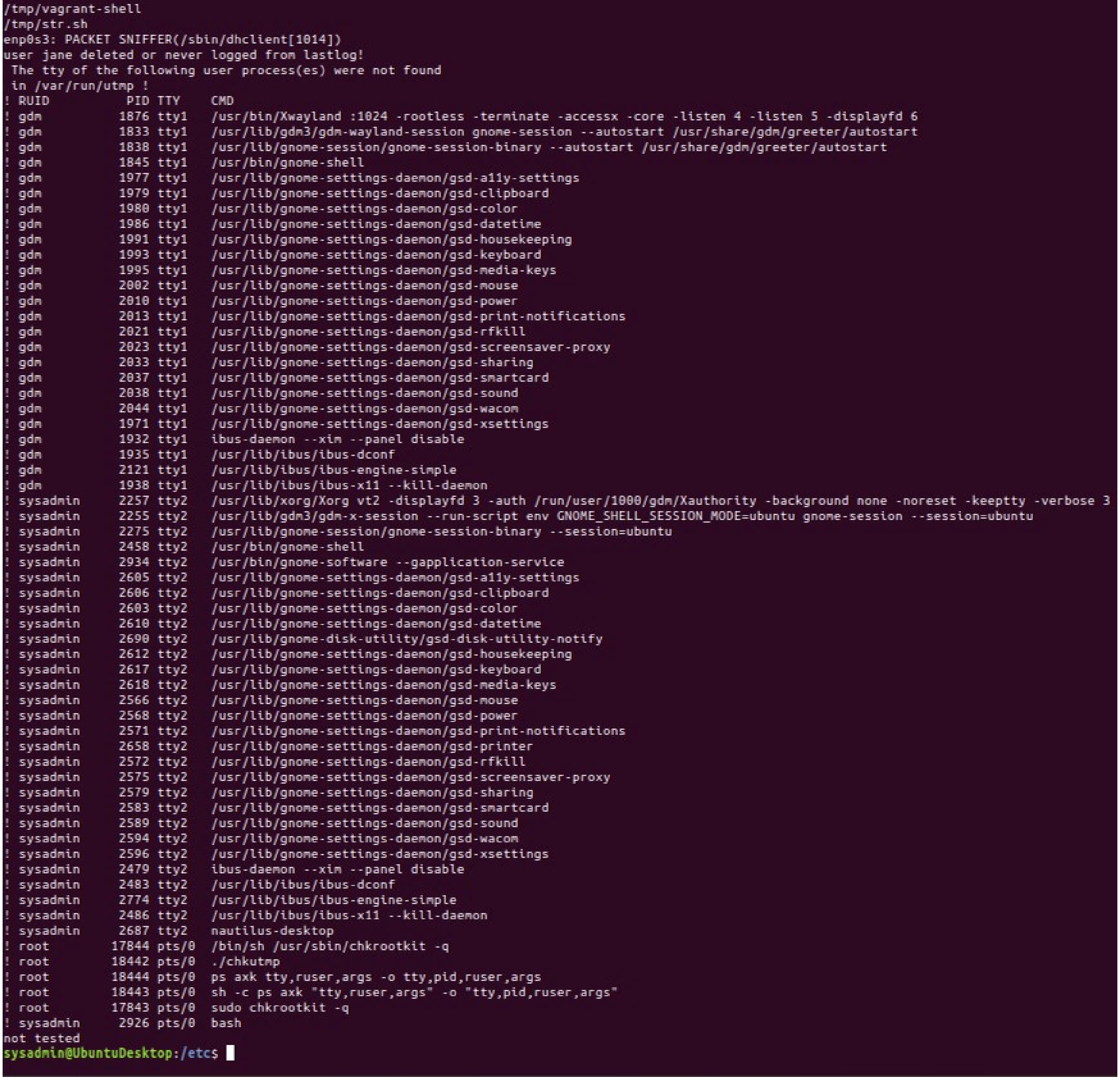
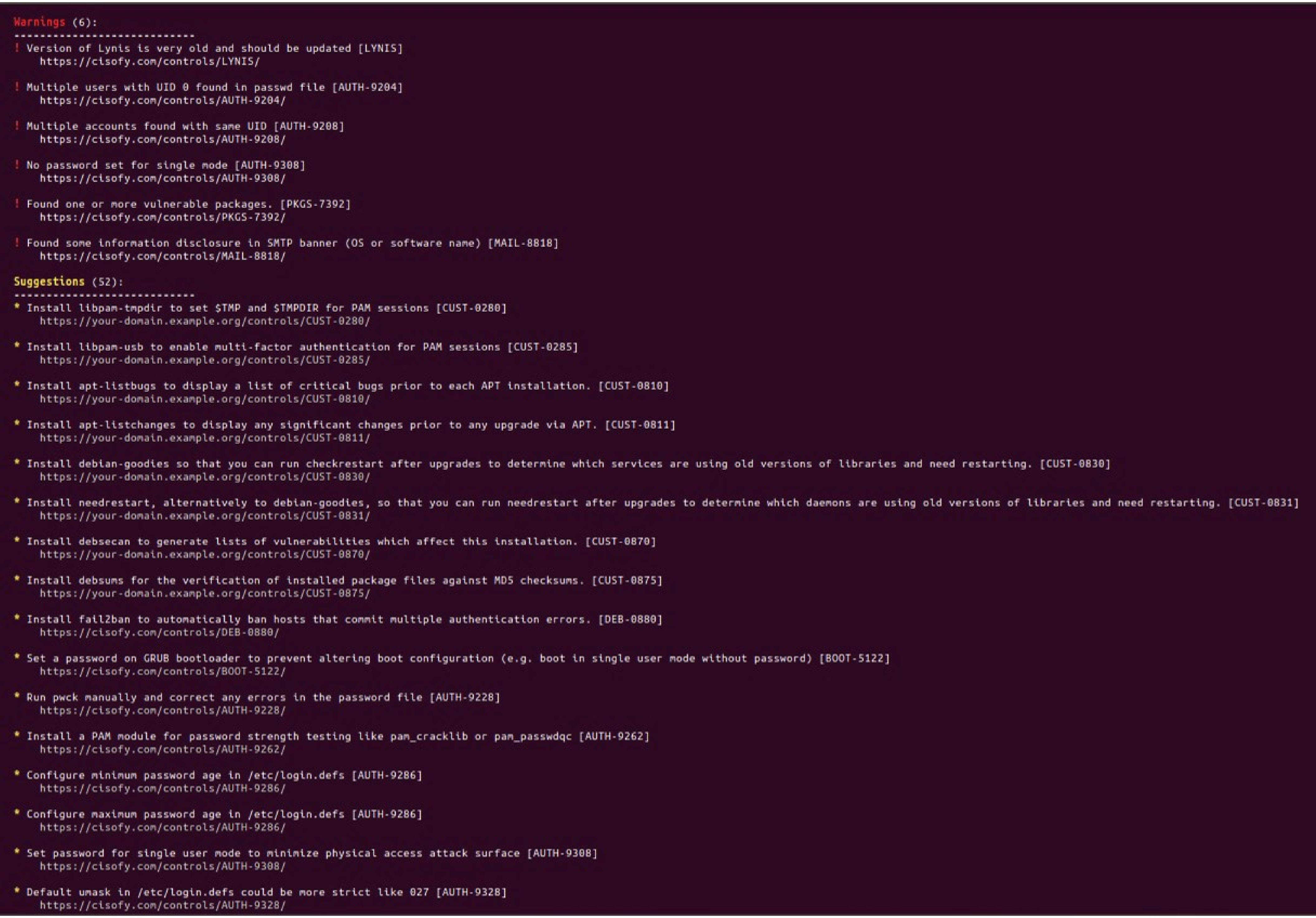
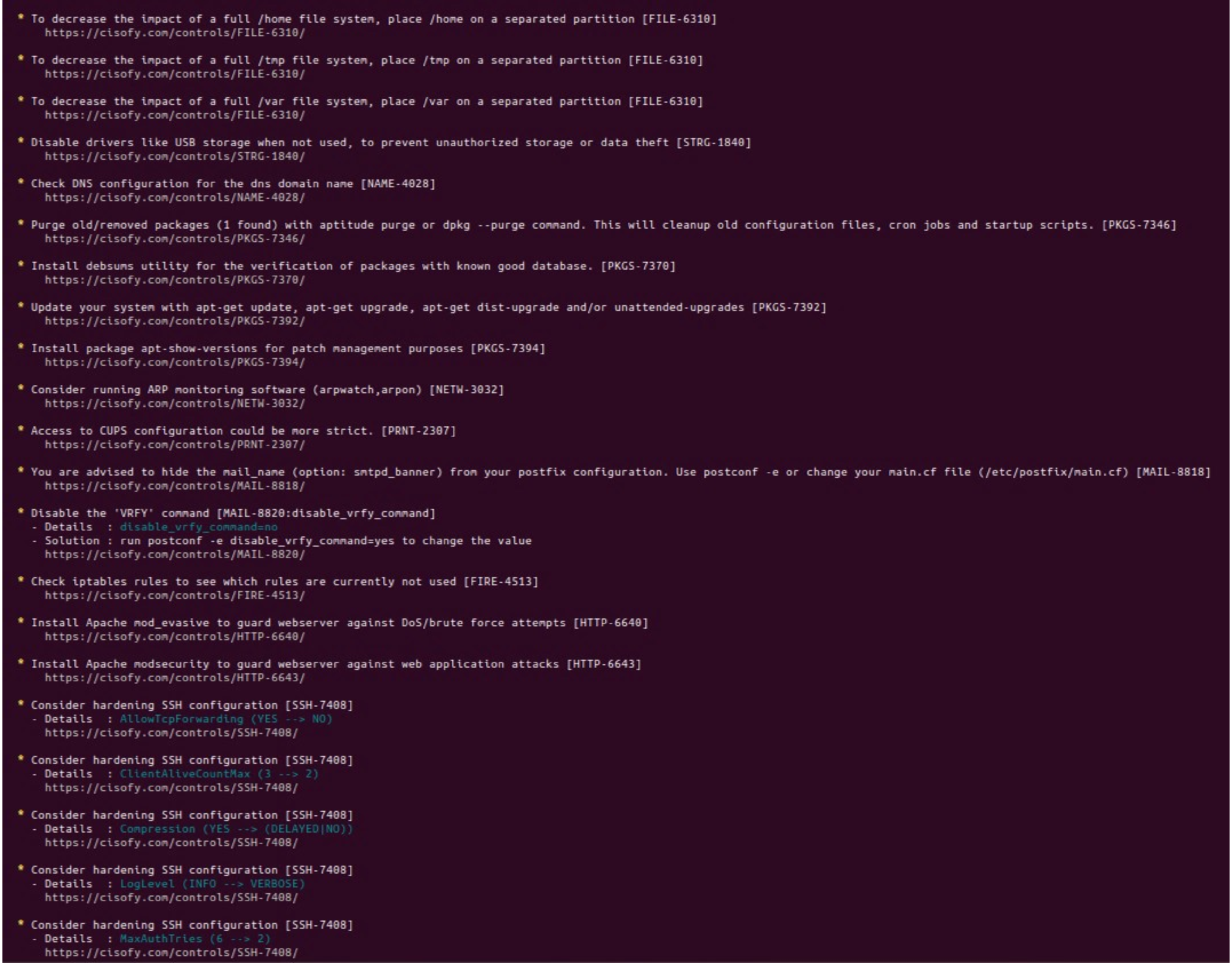


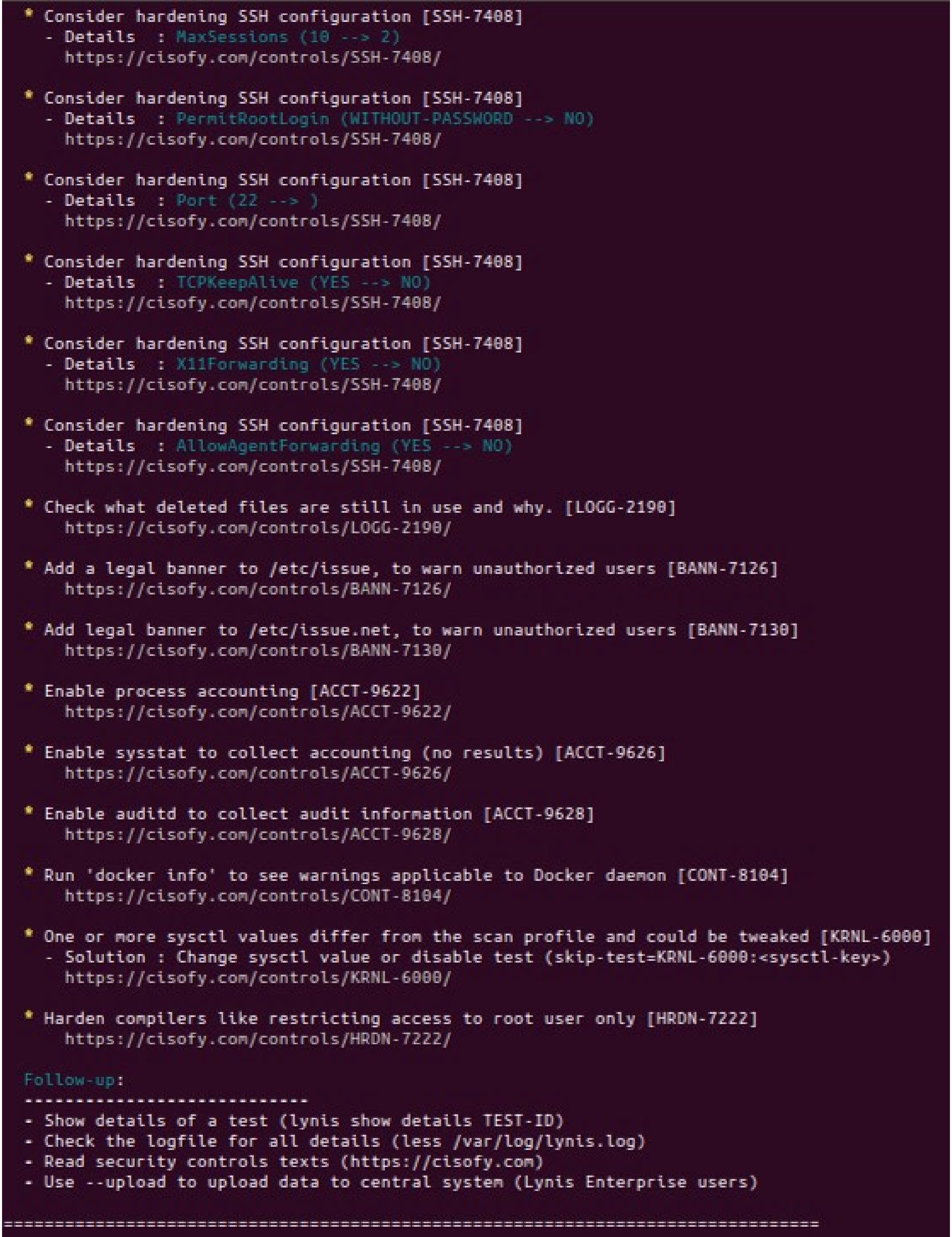
```
/tmp/vagrant-shell
/tmp/str.sh
enp0s3: PACKET SNIFFER(/sbin/dhclient[1014])
user jane deleted or never logged from lastlog!
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          1876 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm          1833 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1838 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm          1845 tty1   /usr/bin/gnome-shell
! gdm          1977 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          1979 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          1980 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          1986 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          1991 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          1993 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          1995 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2002 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2010 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2013 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2021 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2023 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2033 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2037 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2038 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2044 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          1971 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          1932 tty1   ibus-daemon --xim --panel disable
! gdm          1935 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2121 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          1938 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2257 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin     2255 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin     2275 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     2458 tty2   /usr/bin/gnome-shell
! sysadmin     2934 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     2605 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     2606 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     2603 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     2610 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     2690 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     2612 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     2617 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     2618 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     2566 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     2568 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     2571 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     2658 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     2572 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     2575 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     2579 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     2583 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2589 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2594 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2596 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2479 tty2   ibus-daemon --xim --panel disable
! sysadmin     2483 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2774 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2486 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2687 tty2   nautilus-desktop
! root        17844 pts/0  /bin/sh /usr/sbin/chkrootkit -q
! root        18442 pts/0  ./chkutmp
! root        18444 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        18443 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        17843 pts/0  sudo chkrootkit -q
! sysadmin     2926 pts/0  bash
not tested
sysadmin@UbuntuDesktop:/etc$ 
```



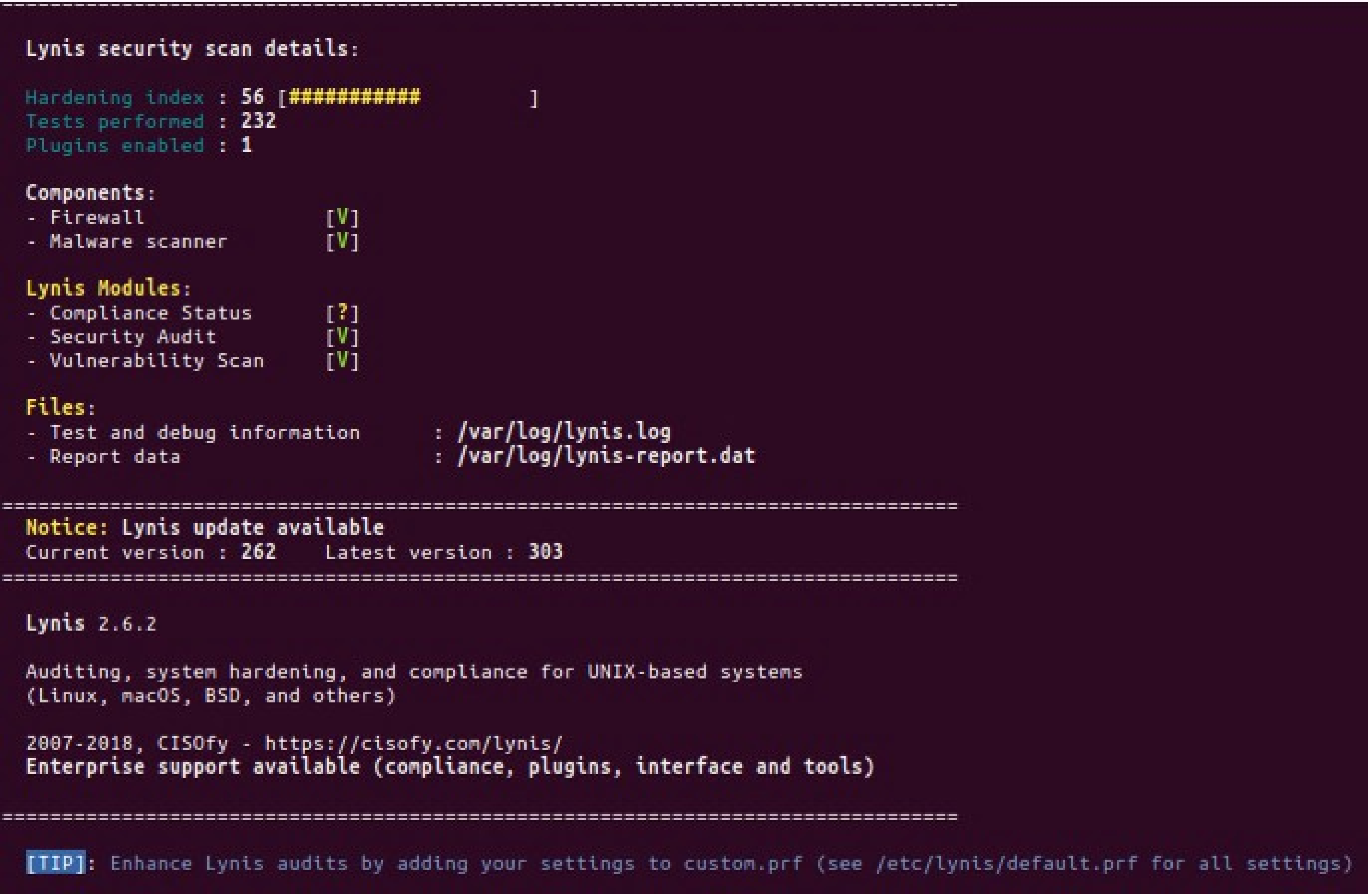
```
Warnings (6):
----------------------------
! Version of Lynis is very old and should be updated [LYNIS]
    https://cisofy.com/controls/LYNIS/

! Multiple users with UID 0 found in passwd file [AUTH-9204]
    https://cisofy.com/controls/AUTH-9204/

! Multiple accounts found with same UID [AUTH-9208]
    https://cisofy.com/controls/AUTH-9208/

! No password set for single mode [AUTH-9308]
    https://cisofy.com/controls/AUTH-9308/

! Found one or more vulnerable packages. [PKGS-7392]
    https://cisofy.com/controls/PKGS-7392/

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

Suggestions (52):
----------------------------
* Install 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 restarting. [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/

* Run pwck manually and correct any errors in the password file [AUTH-9228]
    https://cisofy.com/controls/AUTH-9228/

* 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]
    https://cisofy.com/controls/HTTP-6643/

* 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 : 56 [###########         ]
  Tests performed : 232
  Plugins enabled : 1

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

  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 : 262    Latest version : 303
================================================================================

  Lynis 2.6.2

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

  2007-2018, 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)
```