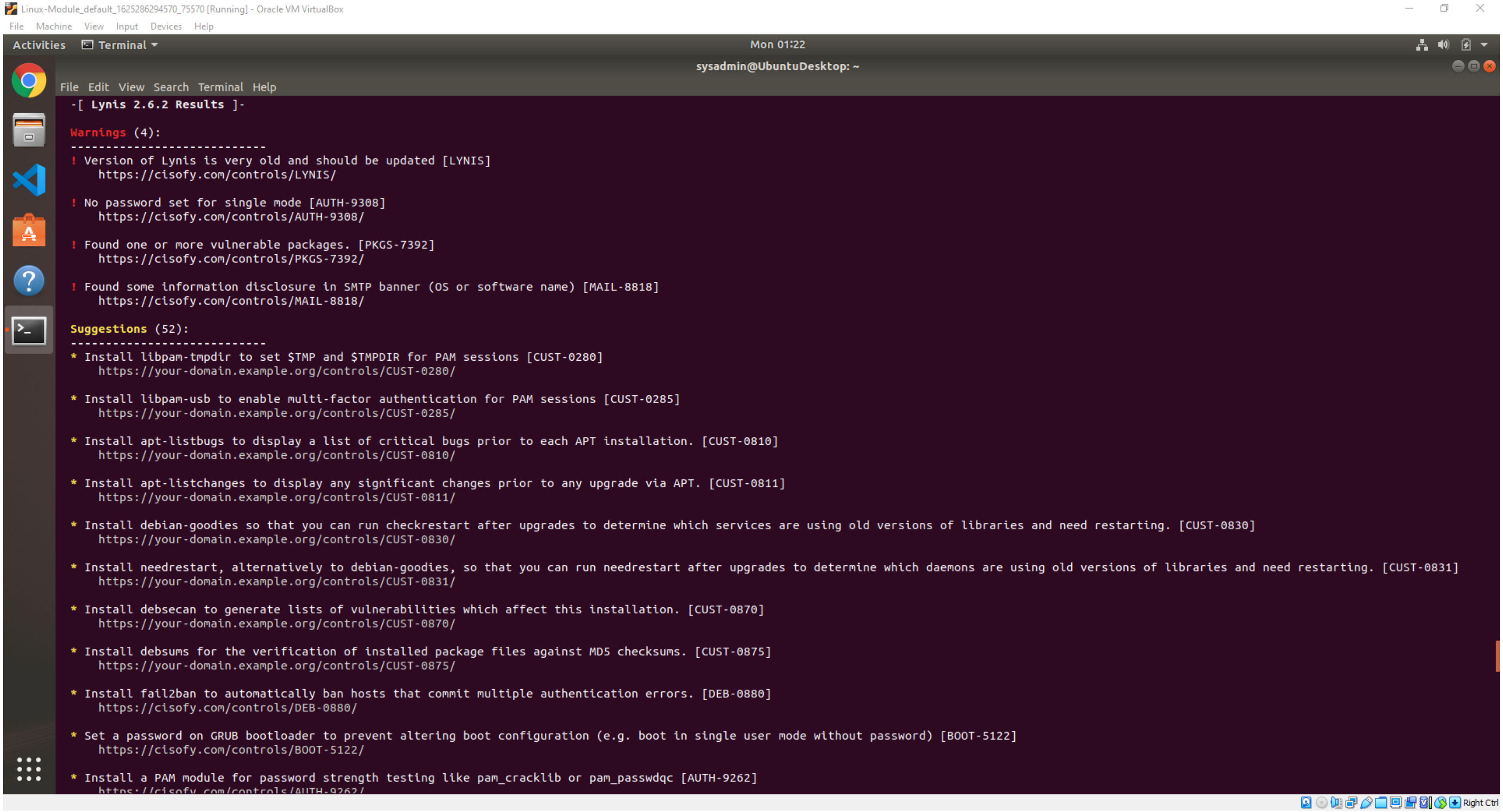
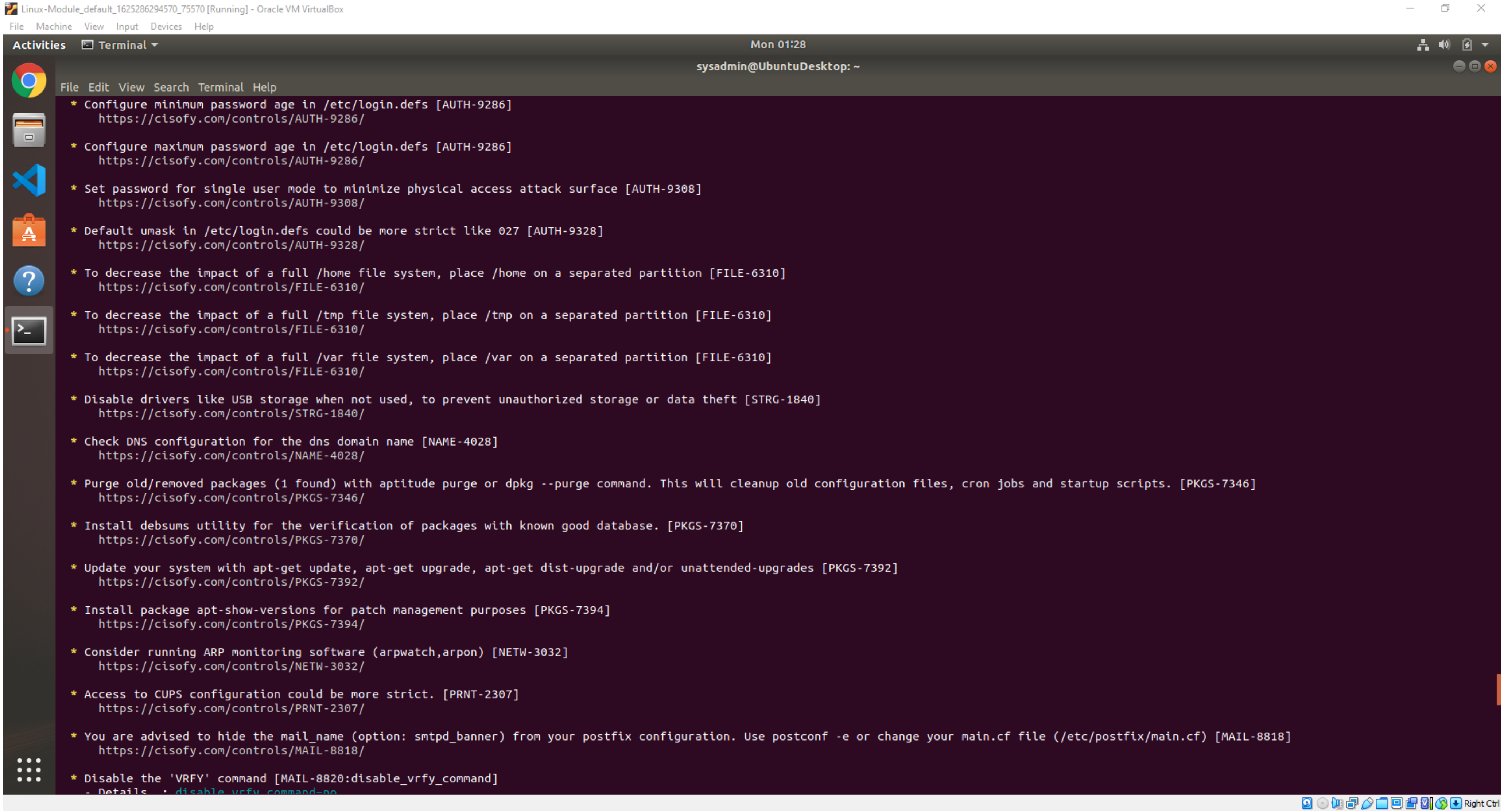
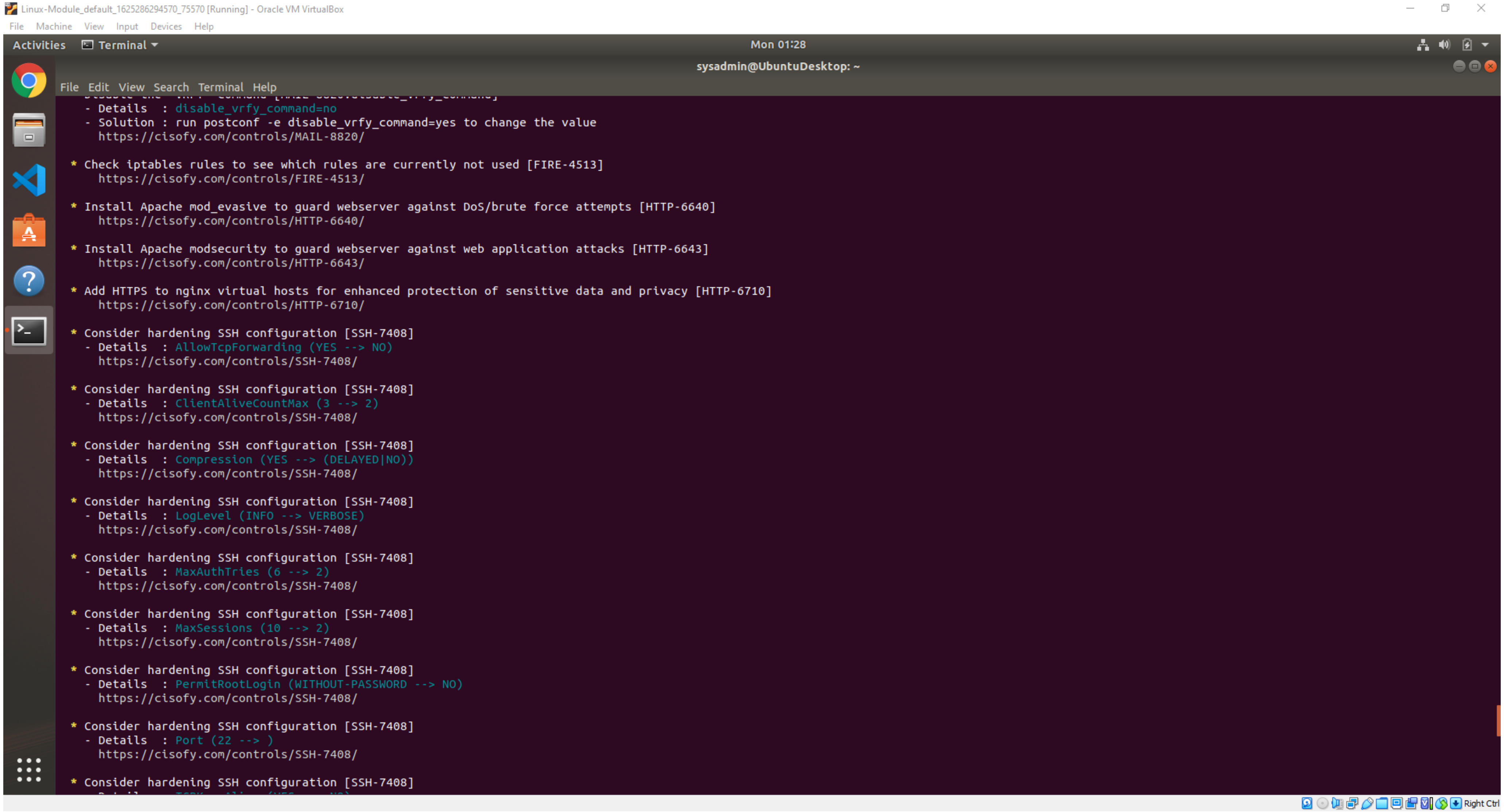

Linux-Module_default_1625286294570_75570 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 01:22
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

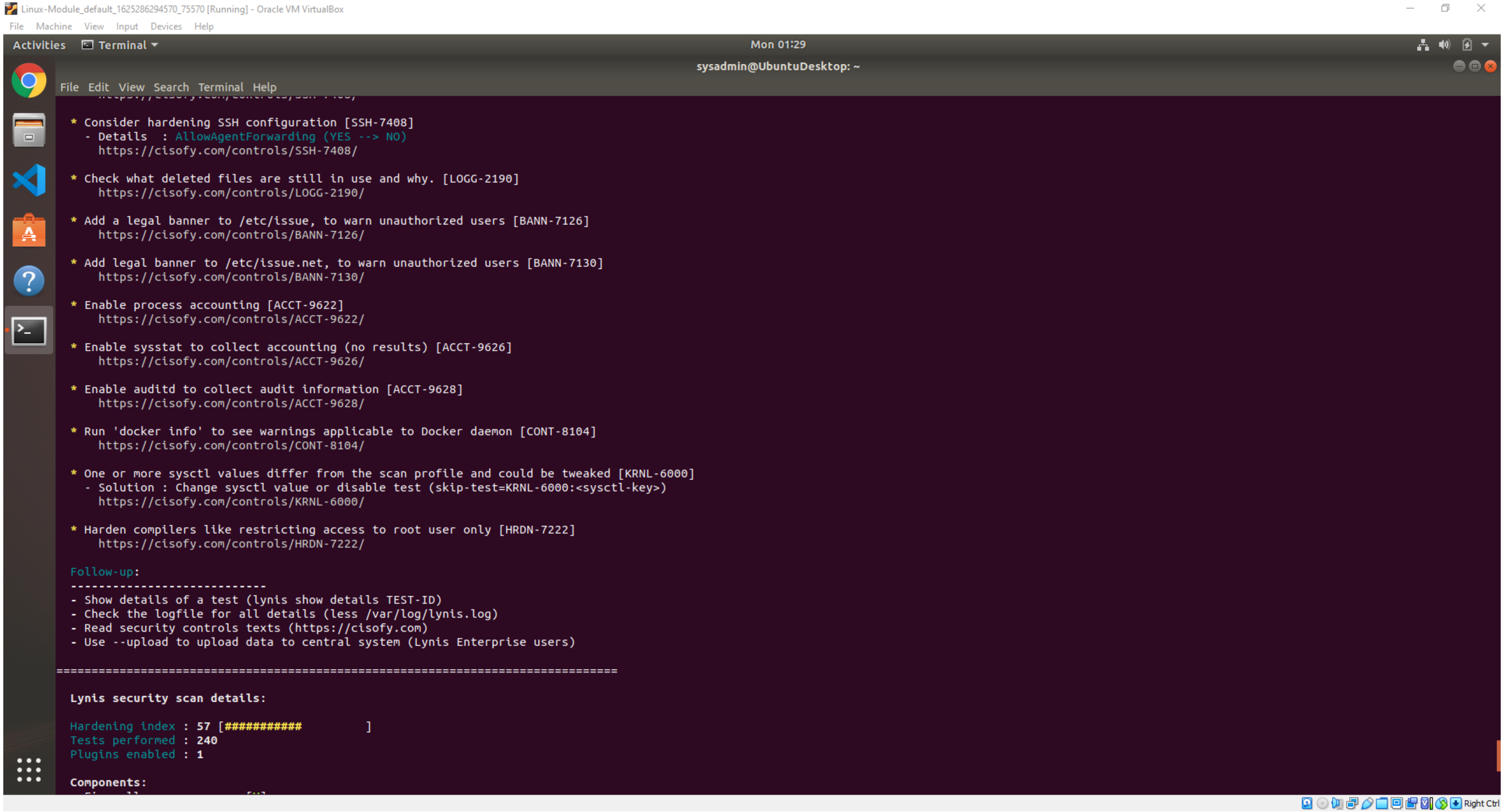
```
-[ Lynis 2.6.2 Results ]-

Warnings (4):
----------------------------
! Version of Lynis is very old and should be updated [LYNIS]
    https://cisofy.com/controls/LYNIS/

! 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/

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


Linux-Module_default_1625286294570_75570 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 01:28
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

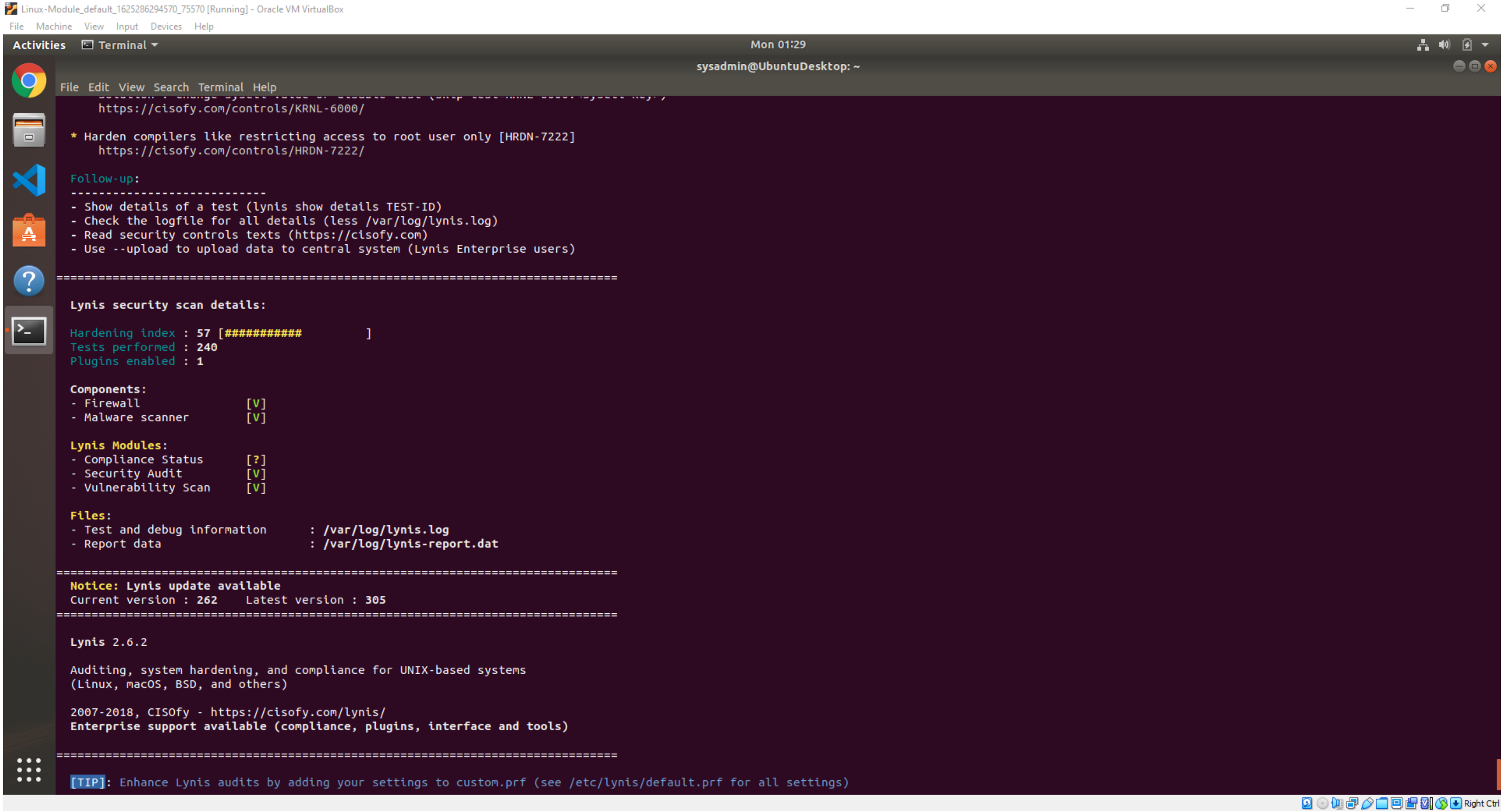
```
 * Configure minimum password age in /etc/login.defs [AUTH-9286]
     https://cisofy.com/controls/AUTH-9286/

 * 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
```


Linux-Module_default_1625286294570_75570 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 01:28
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

```
  - 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/

* 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]
```


Linux-Module_default_1625286294570_75570 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 01:29
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

```
  * 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:
```


Linux-Module_default_1625286294570_75570 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 01:29
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

```
      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]
  - 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 : 305
================================================================================

  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)
```