Lab - Protección del sistema Linux

Objetivos

- Utilice una herramienta de auditoría de seguridad para detectar vulnerabilidades del sistema.
- Implementar soluciones recomendadas para fortalecer el sistema.

Aspectos básicos/situación

La auditoría de un sistema para detectar posibles configuraciones incorrectas o servicios sin protección es un aspecto importante del fortalecimiento del sistema. Lynis es una herramienta de auditoría de seguridad de código abierto con un conjunto automatizado de scripts desarrollados para probar un sistema Linux. Lynis realiza un exhaustivo análisis del estado de su sistema. Incluye un informe detallado de las vulnerabilidades y las acciones recomendadas. En esta práctica de laboratorio, utilizará Lynis para analizar su VM y luego implementar soluciones para fortalecer su sistema.

Recursos necesarios

PC con **CSE-LABVM** instalada en VirtualBox

Instrucciones

Parte 1: Instale y actualice Lynis.

Paso 1: Determine la versión instalada de Lynis.

a. Inicie **CSE-LABVM**.

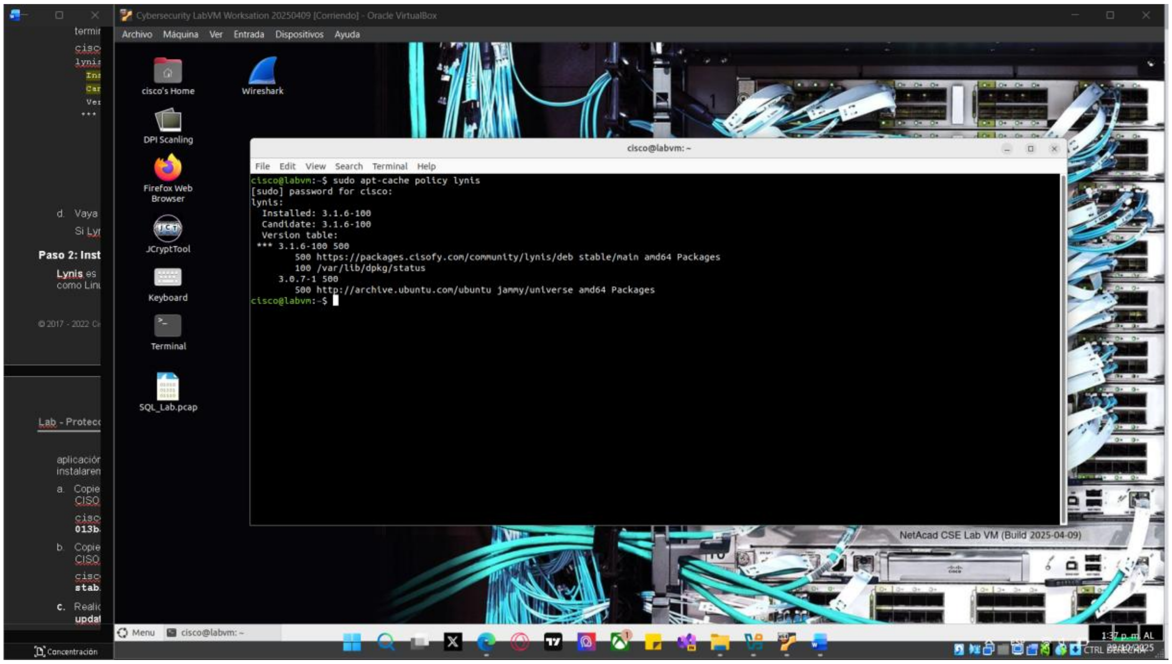
b. Haga doble clic en el icono de **Terminal** para abrir un terminal.

c. Para determinar la última versión proporcionada por CISOfy, introduzca el siguiente comando en el terminal.

```
cisco@labvm:~$ sudo apt-cache policy lynis
lynis:
  Installed: 3.0.6-100
  Candidate: 3.0.6-100
  Version table:
 *** 3.0.6-100 500
        500 https://packages.cisofy.com/community/lynis/deb stable/main amd64 Packages
        500 https://packages.cisofy.com/community/lynis/deb stable/main i386 Packages
        100 /var/lib/dpkg/status
     2.6.2-1 500
        500 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages
        500 http://archive.ubuntu.com/ubuntu focal/universe i386 Packages
```

d. Vaya a la siguiente parte si tiene la última versión de Lynis.

Si Lynis no está instalado o la última versión no está instalada, vaya al siguiente paso para instalar Lynis.



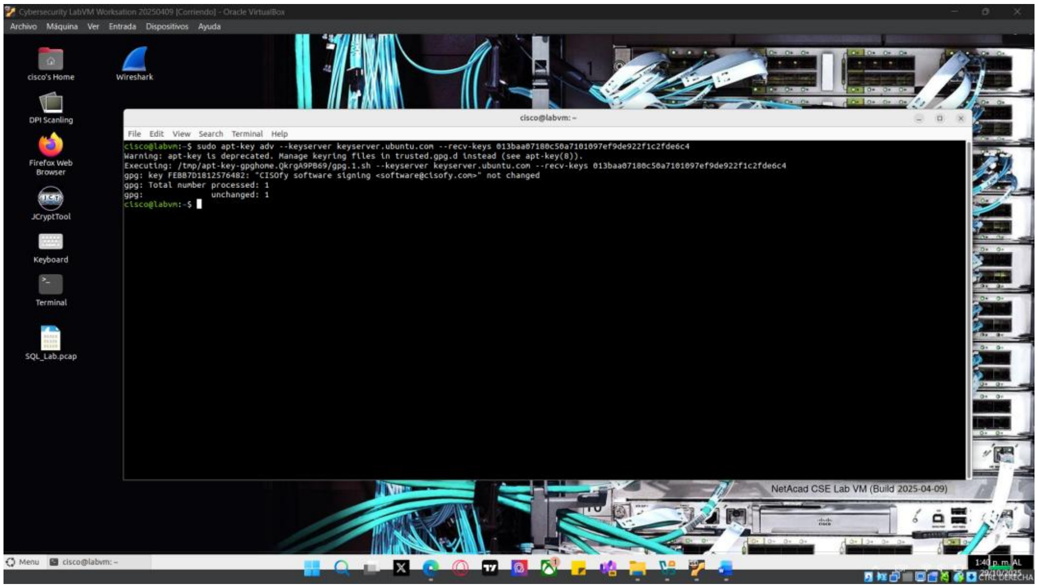
```
cisco@labvm:~$ sudo apt-cache policy lynis
[sudo] password for cisco:
lynis:
  Installed: 3.1.6-100
  Candidate: 3.1.6-100
  Version table:
 *** 3.1.6-100 500
        500 https://packages.cisofy.com/community/lynis/deb stable/main amd64 Packages
        100 /var/lib/dpkg/status
     3.0.7-1 500
        500 http://archive.ubuntu.com/ubuntu jammy/universe amd64 Packages
cisco@labvm:~$
```

Paso 2: Instale Lynis

Lynis es una herramienta de seguridad para sistemas que ejecutan sistemas operativos basados en Unix, como Linux y macOS. **lynis** se utilizará más adelante en otra actividad para fortalecer un sistema Linux. La aplicación **Lynis** es mantenida por CISOfy. En este paso, agregaremos el repositorio de software e instalaremos Lynis.

a. Copie y pegue el siguiente comando en una terminal para importar la clave del servidor de claves CISOfy. Esta clave es necesaria para verificar la integridad de su descarga cuando descarga **lynis**:

```
cisco@labvm:~$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4
```

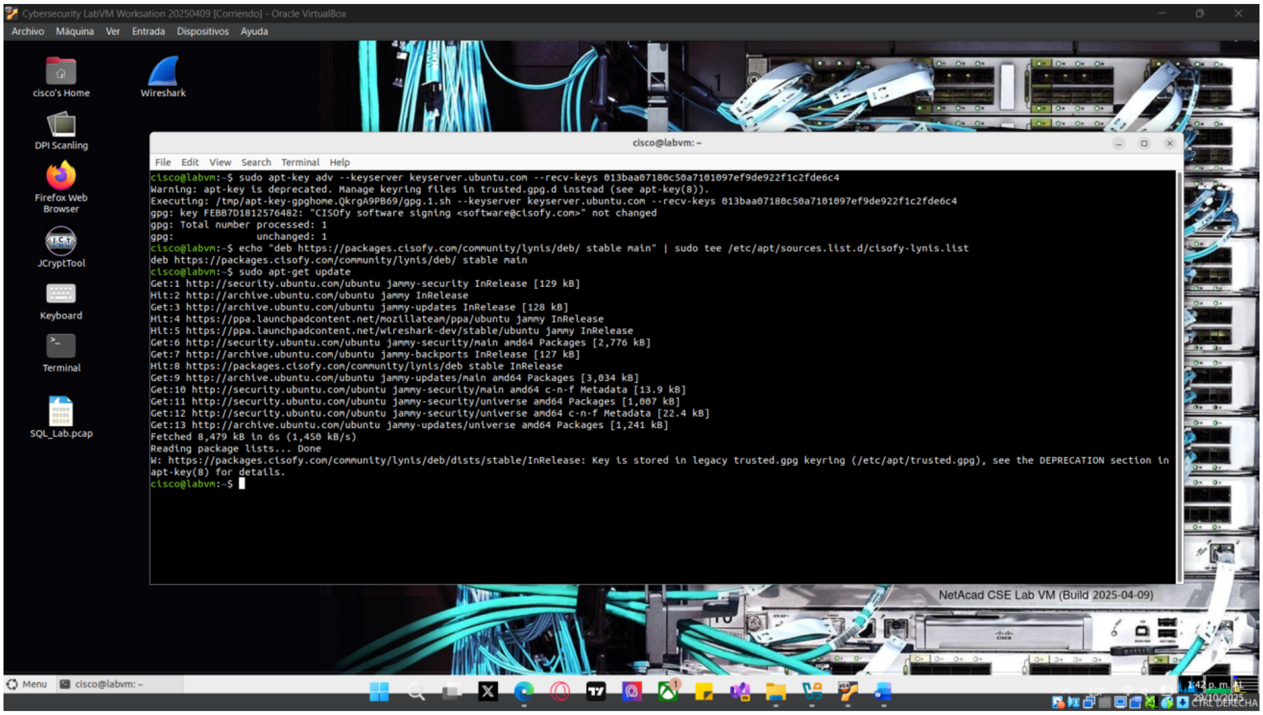


```
cisco@labvm:~$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
Executing: /tmp/apt-key-gpghome.QkrgA9PB69/gpg.1.sh --keyserver keyserver.ubuntu.com --recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4
gpg: key FEBB7D1812576482: "CISOfy software signing <software@cisofy.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
cisco@labvm:~$
```

b. Copie y pegue el siguiente comando en una terminal para agregar el repositorio **lynis** mantenido por CISOfy.

```
cisco@labvm:~$ echo "deb https://packages.cisofy.com/community/lynis/deb/
stable main" | sudo tee /etc/apt/sources.list.d/cisofy-lynis.list
```

c. Realice una actualización después de agregar un nuevo repositorio. En el prompt, ingrese **sudo apt-get update**.

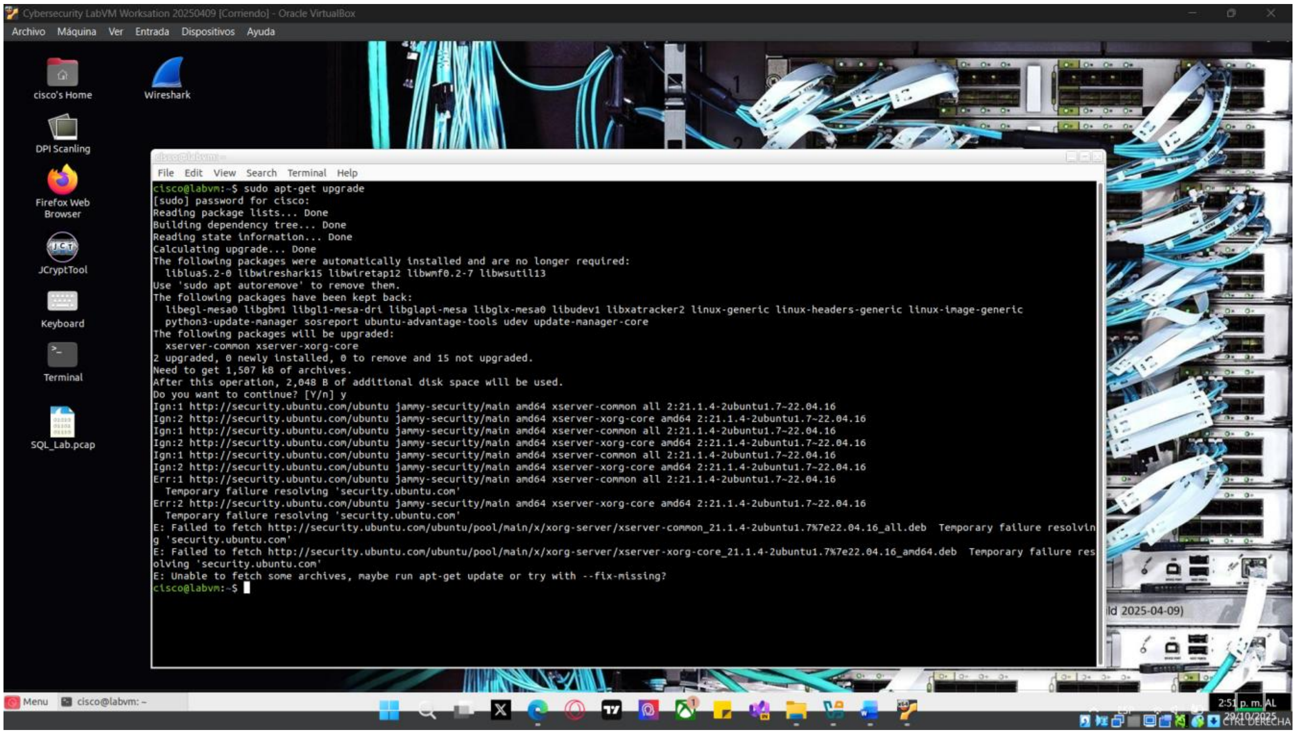


```
cisco@labvm:~$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
Executing: /tmp/apt-key-gpghome.QkrgA9PB69/gpg.1.sh --keyserver keyserver.ubuntu.com --recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4
gpg: key FEBB7D1812576482: "CISOfy software signing <software@cisofy.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
cisco@labvm:~$ echo "deb https://packages.cisofy.com/community/lynis/deb/ stable main" | sudo tee /etc/apt/sources.list.d/cisofy-lynis.list
deb https://packages.cisofy.com/community/lynis/deb/ stable main
cisco@labvm:~$ sudo apt-get update
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:4 https://ppa.launchpadcontent.net/mozillateam/ppa/ubuntu jammy InRelease
Hit:5 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy InRelease
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2,776 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Hit:8 https://packages.cisofy.com/community/lynis/deb stable InRelease
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [3,034 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [13.9 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [1,007 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [22.4 kB]
Get:13 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,241 kB]
Fetched 8,479 kB in 6s (1,450 kB/s)
Reading package lists... Done
W: https://packages.cisofy.com/community/lynis/deb/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in
apt-key(8) for details.
cisco@labvm:~$
```

d. Utilice el comando **apt install** para instalar Lynis si aún no está instalado.

```
cisco@labvm:~$ sudo apt install lynis
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  lynis
0 upgraded, 1 newly installed, 0 to remove and 17 not upgraded.
Need to get 0 B/262 kB of archives.
After this operation, 1,681 kB of additional disk space will be used.
Selecting previously unselected package lynis.
(Reading database ... 205787 files and directories currently installed.)
Preparing to unpack .../lynis_3.0.6-100_all.deb ...
Unpacking lynis (3.0.6-100) ...
Setting up lynis (3.0.6-100) ...
Processing triggers for man-db (2.9.1-1) ...
```

e. Realice una actualización después de la instalación para asegurarse de que la versión instalada de Lynis sea la última. Cuando se le solicite, ingrese **sudo apt-get upgrade**.

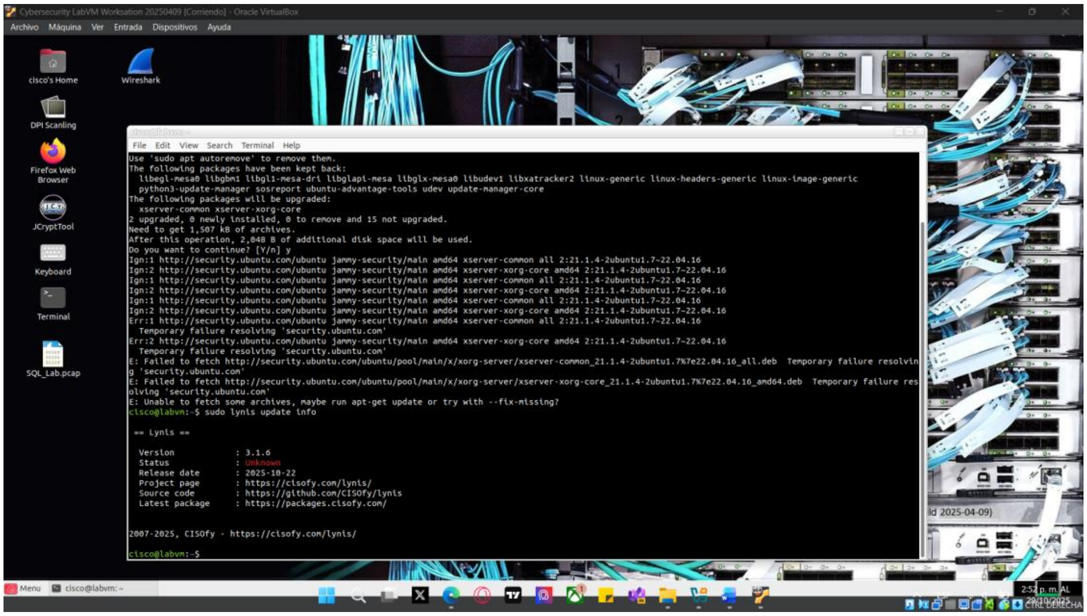


```
cisco@labvm:~$ sudo apt-get upgrade
[sudo] password for cisco:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  liblua5.2-0 libwireshark15 libwiretap12 libwmf0.2-7 libwsutil13
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  libegl-mesa0 libgbm1 libgl1-mesa-dri libglapi-mesa libglx-mesa0 libudev1 libxatracker2 linux-generic linux-headers-generic linux-image-generic
  python3-update-manager sosreport ubuntu-advantage-tools udev update-manager-core
The following packages will be upgraded:
  xserver-common xserver-xorg-core
2 upgraded, 0 newly installed, 0 to remove and 15 not upgraded.
Need to get 1,507 kB of archives.
After this operation, 2,048 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Ign:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
Ign:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
Ign:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
Ign:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
Ign:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
Ign:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
Err:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
  Temporary failure resolving 'security.ubuntu.com'
Err:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
  Temporary failure resolving 'security.ubuntu.com'
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/x/xorg-server/xserver-common_21.1.4-2ubuntu1.7%7e22.04.16_all.deb  Temporary failure resolvin
g 'security.ubuntu.com'
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/x/xorg-server/xserver-xorg-core_21.1.4-2ubuntu1.7%7e22.04.16_amd64.deb  Temporary failure res
olving 'security.ubuntu.com'
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
cisco@labvm:~$ 
```

Parte 2: Examinar la versión actual de Lynis.

Cambie al directorio de Lynis y luego introduzca el comando **sudo lynis update info** para verificar la información de actualización de Lynis. Introduzca la **password** para la contraseña de sudo. Este comando verifica que esta es la versión más reciente y actualiza la herramienta al momento de la redacción de esta práctica de laboratorio. Si la versión instalada de Lynis no está actualizada, ingrese **sudo apt-get upgrade** en el indicador.

```
cisco@labvm:~$ sudo lynis update info
[sudo] password for cisco: password

== Lynis ==

  Version            : 3.0.6
  Status             : Up-to-date
  Release date       : 2021-07-22
  Project page       : https://cisofy.com/lynis/
  Source code        : https://github.com/CISOfy/lynis
  Latest package     : https://packages.cisofy.com/


2007-2021, CISOfy - https://cisofy.com/lynis/
```



```
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  libegl-mesa0 libgbm1 libgl1-mesa-dri libglapi-mesa libglx-mesa0 libudev1 libxatracker2 linux-generic linux-headers-generic linux-image-generic
  python3-update-manager sosreport ubuntu-advantage-tools udev update-manager-core
The following packages will be upgraded:
  xserver-common xserver-xorg-core
2 upgraded, 0 newly installed, 0 to remove and 15 not upgraded.
Need to get 1,507 kB of archives.
After this operation, 2,048 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Ign:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
Ign:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
Ign:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
Ign:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
Ign:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
Ign:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
Err:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
  Temporary failure resolving 'security.ubuntu.com'
Err:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
  Temporary failure resolving 'security.ubuntu.com'
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/x/xorg-server/xserver-common_21.1.4-2ubuntu1.7%7e22.04.16_all.deb  Temporary failure resolvin
g 'security.ubuntu.com'
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/x/xorg-server/xserver-xorg-core_21.1.4-2ubuntu1.7%7e22.04.16_amd64.deb  Temporary failure res
olving 'security.ubuntu.com'
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
cisco@labvm:~$ sudo lynis update info

 == Lynis ==

  Version            : 3.1.6
  Status             : Unknown
  Release date       : 2025-10-22
  Project page       : https://cisofy.com/lynis/
  Source code        : https://github.com/CISOfy/lynis
  Latest package     : https://packages.cisofy.com/


2007-2025, CISOfy - https://cisofy.com/lynis/

cisco@labvm:~$
```

Parte 3: Ejecute la herramienta Lynis.

a. Ingrese el comando **sudo lynis --auditor cisco**. Es posible que deba ingresar **password** como contraseña nuevamente. El análisis tardará aproximadamente un minuto en ejecutarse.

```
cisco@labvm:~$ sudo lynis --auditor cisco
```

b. Debería recibir la salida para una variedad de características del sistema que comienzan con **arranque y servicios**, y terminan con **refuerzo**, **pruebas personalizadas** y **complementos** (fase 2). La siguiente sección son los **resultados de Lynis 3.0.6**. Sus resultados probablemente incluyan las dos **advertencias** que se muestran a continuación. También puede recibir otras advertencias. Además, habrá una sección con una lista de **Sugerencias**, que enumera 49 en la salida de ejemplo a continuación. Solo se muestra la primera sugerencia.

```
[ Lynis 3.0.6 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

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


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

<output omitted>
[+] Boot and services
```

```
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB2                                   [ FOUND ]
<output omitted>
[+] Hardening
------------------------------------
    - Installed compiler(s)                                   [ FOUND ]
    - Installed malware scanner                               [ NOT FOUND ]
    - Non-native binary formats                               [ NOT FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                                   [ NONE ]

[+] Plugins (phase 2)
------------------------------------

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

  -[ Lynis 3.0.6 Results ]-

  Warnings (2):
  ----------------------------
  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (49):
  ----------------------------
  * 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/
<output omitted>
================================================================================

  Lynis 3.0.6

  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
/home/cisco/Downloads/lynis/default.prf for all settings)
```

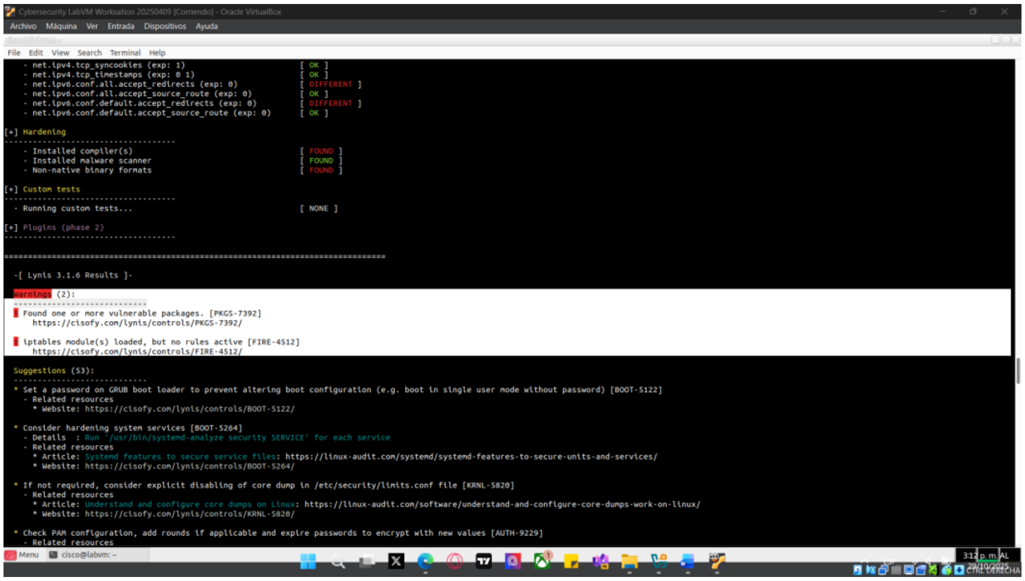
```
cisco@labvm:~$
```

```
cisco@labvm:~$ sudo lynis --auditor cisco

[ Lynis 3.1.6 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  22.04
  End-of-life:               NO
  Kernel version:            5.15.0
  Hardware platform:         x86_64
  Hostname:                  labvm
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /usr/share/lynis/plugins
  ---------------------------------------------------
  Auditor:                   cisco
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ UNKNOWN ]

[+] System tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete
```

Parte 4: Revise los resultados del análisis y aborde las advertencias.

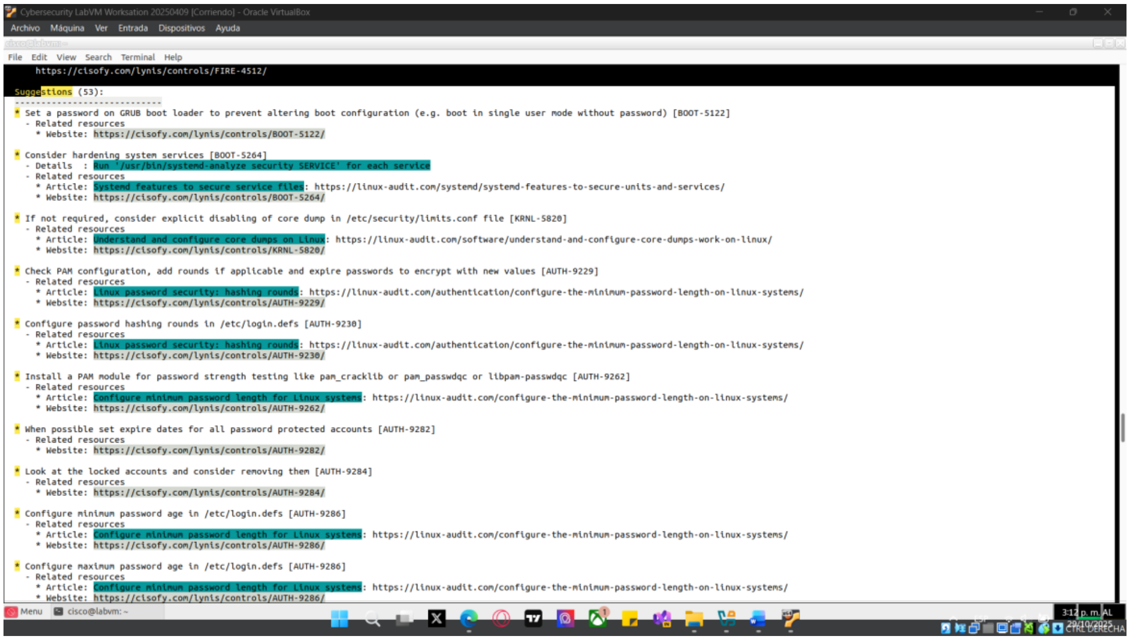
a. Desplácese hasta la sección **Resultados** en la salida para su análisis.

¿Cuántas advertencias recibió?



```
    - 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
------------------------------------
  - Running custom tests...                                   [ NONE ]

[+] Plugins (phase 2)
------------------------------------

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

  -[ Lynis 3.1.6 Results ]-

  Warnings (2):
  ----------------------------
  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (53):
  ----------------------------
  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/BOOT-5122/

  * Consider hardening system services [BOOT-5264]
    - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
    - Related resources
      * Article: Systemd features to secure service files: https://linux-audit.com/systemd/systemd-features-to-secure-units-and-services/
      * Website: https://cisofy.com/lynis/controls/BOOT-5264/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
    - Related resources
      * Article: Understand and configure core dumps on Linux: https://linux-audit.com/software/understand-and-configure-core-dumps-work-on-linux/
      * Website: https://cisofy.com/lynis/controls/KRNL-5820/

  * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
    - Related resources
```

¿Cuántas sugerencias recibió?



```
    https://cisofy.com/lynis/controls/FIRE-4512/

Suggestions (53):
----------------------------
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/BOOT-5122/

* Consider hardening system services [BOOT-5264]
  - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
  - Related resources
    * Article: Systemd features to secure service files: https://linux-audit.com/systemd/systemd-features-to-secure-units-and-services/
    * Website: https://cisofy.com/lynis/controls/BOOT-5264/

* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
  - Related resources
    * Article: Understand and configure core dumps on Linux: https://linux-audit.com/software/understand-and-configure-core-dumps-work-on-linux/
    * Website: https://cisofy.com/lynis/controls/KRNL-5820/

* Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
  - Related resources
    * Article: Linux password security: hashing rounds: https://linux-audit.com/authentication/configure-the-minimum-password-length-on-linux-systems/
    * Website: https://cisofy.com/lynis/controls/AUTH-9229/

* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
  - Related resources
    * Article: Linux password security: hashing rounds: https://linux-audit.com/authentication/configure-the-minimum-password-length-on-linux-systems/
    * Website: https://cisofy.com/lynis/controls/AUTH-9230/

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc or libpam-passwdqc [AUTH-9262]
  - Related resources
    * Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-minimum-password-length-on-linux-systems/
    * Website: https://cisofy.com/lynis/controls/AUTH-9262/

* When possible set expire dates for all password protected accounts [AUTH-9282]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/AUTH-9282/

* Look at the locked accounts and consider removing them [AUTH-9284]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/AUTH-9284/

* Configure minimum password age in /etc/login.defs [AUTH-9286]
  - Related resources
    * Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-minimum-password-length-on-linux-systems/
    * Website: https://cisofy.com/lynis/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
  - Related resources
    * Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-minimum-password-length-on-linux-systems/
    * Website: https://cisofy.com/lynis/controls/AUTH-9286/
```

b. Debe abordar las advertencias. Elija al menos una advertencia e investigue cómo solucionar ese problema. Puede utilizar el enlace proporcionado en la salida de advertencia como punto de partida para abordar una advertencia. Pero también es posible que deba utilizar sus habilidades de investigación en Internet para localizar información adicional.

¿A qué advertencia se dirige?

Esta advertencia significa que **hay paquetes instalados en el sistema que no están actualizados** y podrían tener **vulnerabilidades conocidas**.
Lynis detecta esto al revisar la base de datos de seguridad de Ubuntu.

¿Cuál es su solución?

Advertencia elegida:
PKGS-7392 – Found one or more vulnerable packages

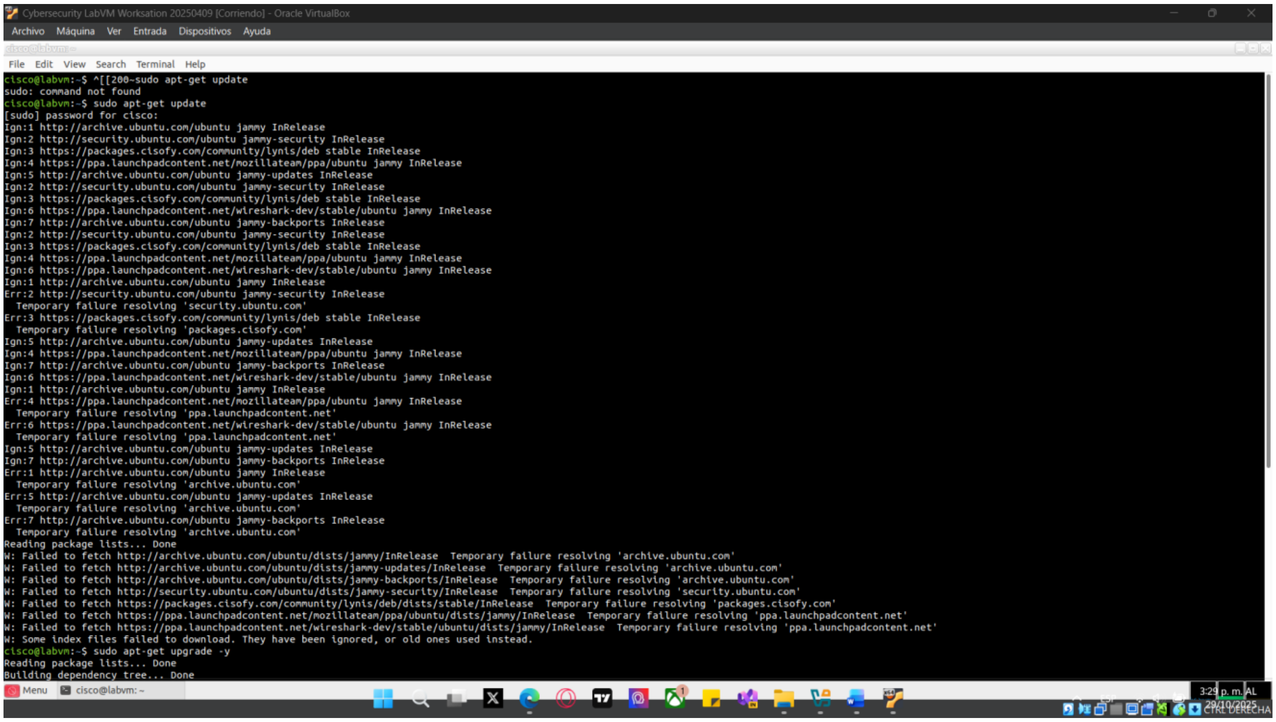
Solución aplicada:
Actualizar todos los paquetes del sistema para eliminar vulnerabilidades conocidas.
Los comandos ejecutados fueron:

```
sudo apt-get update

sudo apt-get upgrade -y

sudo apt-get dist-upgrade -y

sudo apt-get autoremove -y

sudo apt-get autoclean

sudo dpkg --configure -a
```

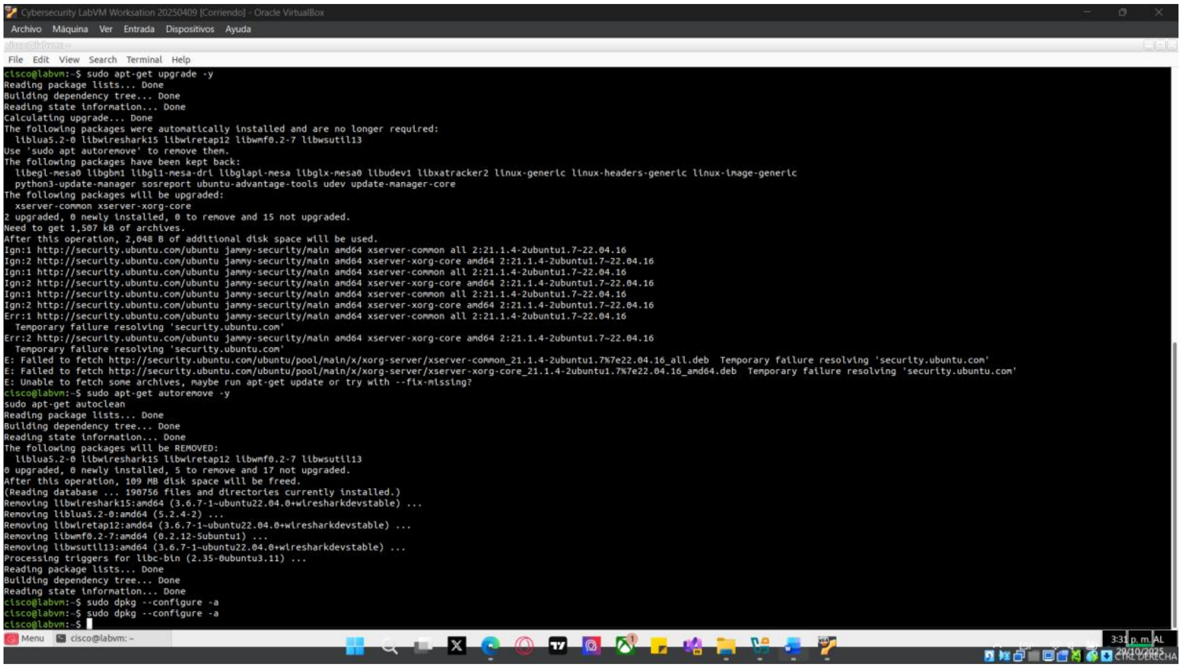
Explicación:
Estos comandos actualizan la lista de paquetes, instalan las versiones más recientes (incluyendo parches de seguridad), eliminan paquetes innecesarios y corrigen configuraciones pendientes.

Resultado esperado:
Al volver a ejecutar sudo lynis audit system --auditor cisco, la advertencia **[PKGS-7392]** debería desaparecer del reporte, indicando que el sistema está actualizado y reforzado.

c. Implemente su solución y ejecute el comando **sudo lynis --auditor cisco** nuevamente. Si la advertencia que eligió ya no aparece en la sección **Resultados**, ¡felicitaciones! Usted acaba de aumentar el fortalecimiento de su VM de Ubuntu. Si la advertencia sigue apareciendo, vea si puede encontrar más información para ayudarlo a obtener un informe claro de Lynis en el que la advertencia ya no se informa.



```
cisco@labvm:~$ ^[[200~sudo apt-get update
sudo: command not found
cisco@labvm:~$ sudo apt-get update
[sudo] password for cisco:
Ign:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Ign:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Ign:3 https://packages.cisofy.com/community/lynis/deb stable InRelease
Ign:4 https://ppa.launchpadcontent.net/mozillateam/ppa/ubuntu jammy InRelease
Ign:5 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Ign:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Ign:3 https://packages.cisofy.com/community/lynis/deb stable InRelease
Ign:6 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy InRelease
Ign:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Ign:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Ign:3 https://packages.cisofy.com/community/lynis/deb stable InRelease
Ign:4 https://ppa.launchpadcontent.net/mozillateam/ppa/ubuntu jammy InRelease
Ign:6 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy InRelease
Ign:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Err:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
  Temporary failure resolving 'security.ubuntu.com'
Err:3 https://packages.cisofy.com/community/lynis/deb stable InRelease
  Temporary failure resolving 'packages.cisofy.com'
Ign:5 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Ign:4 https://ppa.launchpadcontent.net/mozillateam/ppa/ubuntu jammy InRelease
Ign:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Ign:6 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy InRelease
Ign:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Err:4 https://ppa.launchpadcontent.net/mozillateam/ppa/ubuntu jammy InRelease
  Temporary failure resolving 'ppa.launchpadcontent.net'
Err:6 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy InRelease
  Temporary failure resolving 'ppa.launchpadcontent.net'
Ign:5 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Ign:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Err:1 http://archive.ubuntu.com/ubuntu jammy InRelease
  Temporary failure resolving 'archive.ubuntu.com'
Err:5 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
  Temporary failure resolving 'archive.ubuntu.com'
Err:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
  Temporary failure resolving 'archive.ubuntu.com'
Reading package lists... Done
W: Failed to fetch http://archive.ubuntu.com/ubuntu/dists/jammy/InRelease  Temporary failure resolving 'archive.ubuntu.com'
W: Failed to fetch http://archive.ubuntu.com/ubuntu/dists/jammy-updates/InRelease  Temporary failure resolving 'archive.ubuntu.com'
W: Failed to fetch http://archive.ubuntu.com/ubuntu/dists/jammy-backports/InRelease  Temporary failure resolving 'archive.ubuntu.com'
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/jammy-security/InRelease  Temporary failure resolving 'security.ubuntu.com'
W: Failed to fetch https://packages.cisofy.com/community/lynis/deb/dists/stable/InRelease  Temporary failure resolving 'packages.cisofy.com'
W: Failed to fetch https://ppa.launchpadcontent.net/mozillateam/ppa/ubuntu/dists/jammy/InRelease  Temporary failure resolving 'ppa.launchpadcontent.net'
W: Failed to fetch https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu/dists/jammy/InRelease  Temporary failure resolving 'ppa.launchpadcontent.net'
W: Some index files failed to download. They have been ignored, or old ones used instead.
cisco@labvm:~$ sudo apt-get upgrade -y
Reading package lists... Done
Building dependency tree... Done
```



```
cisco@labvm:~$ sudo apt-get upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  liblua5.2-0 libwireshark15 libwiretap12 libwmf0.2-7 libwsutil13
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  libegl-mesa0 libgbm1 libgl1-mesa-dri libglapi-mesa libglx-mesa0 libudev1 libxatracker2 linux-generic linux-headers-generic linux-image-generic
  python3-update-manager sosreport ubuntu-advantage-tools udev update-manager-core
The following packages will be upgraded:
  xserver-common xserver-xorg-core
2 upgraded, 0 newly installed, 0 to remove and 15 not upgraded.
Need to get 1,507 kB of archives.
After this operation, 2,048 B of additional disk space will be used.
Ign:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
Ign:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
Ign:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
Ign:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
Ign:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
Ign:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
Err:1 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-common all 2:21.1.4-2ubuntu1.7~22.04.16
  Temporary failure resolving 'security.ubuntu.com'
Err:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 xserver-xorg-core amd64 2:21.1.4-2ubuntu1.7~22.04.16
  Temporary failure resolving 'security.ubuntu.com'
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/x/xorg-server/xserver-common_21.1.4-2ubuntu1.7%7e22.04.16_all.deb  Temporary failure resolving 'security.ubuntu.com'
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/x/xorg-server/xserver-xorg-core_21.1.4-2ubuntu1.7%7e22.04.16_amd64.deb  Temporary failure resolving 'security.ubuntu.com'
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
cisco@labvm:~$ sudo apt-get autoremove -y
sudo apt-get autoclean
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  liblua5.2-0 libwireshark15 libwiretap12 libwmf0.2-7 libwsutil13
0 upgraded, 0 newly installed, 5 to remove and 17 not upgraded.
After this operation, 109 MB disk space will be freed.
(Reading database ... 190756 files and directories currently installed.)
Removing libwireshark15:amd64 (3.6.7-1~ubuntu22.04.0+wiresharkdevstable) ...
Removing liblua5.2-0:amd64 (5.2.4-2) ...
Removing libwiretap12:amd64 (3.6.7-1~ubuntu22.04.0+wiresharkdevstable) ...
Removing libwmf0.2-7:amd64 (0.2.12-5ubuntu1) ...
Removing libwsutil13:amd64 (3.6.7-1~ubuntu22.04.0+wiresharkdevstable) ...
Processing triggers for libc-bin (2.35-0ubuntu3.11) ...
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
cisco@labvm:~$ sudo dpkg --configure -a
cisco@labvm:~$ sudo dpkg --configure -a
cisco@labvm:~$ 
```