Lab - Configuración de funciones de seguridad en Windows y Linux

Objetivos

Parte 1: Actualizar Windows y Linux

Parte 2: Política de seguridad local de Windows

Parte 3: Configurar reglas de firewall

Parte 4: Instalar y ejecutar aplicaciones

Recursos necesarios

- 1 PC con Windows 10
- Esta máquina virtual CSE-LABVM
- Acceso a Internet

Aspectos básicos/Situación

En esta práctica de laboratorio, actualizará los sistemas Windows y Linux. Configurará la política de seguridad local y las reglas de firewall en Windows. En Linux, instalará dos aplicaciones: chkrootkit y Lynis.

Instrucciones

Parte 1: Actualice Windows y Linux

Continuamente se descubren nuevas vulnerabilidades y métodos de ataque. Es una buena idea mantener su PC actualizada para mitigar el aprovechamiento de las vulnerabilidades conocidas.

Paso 1: Verifique la conectividad entre CSE-LABVM y la computadora host de Windows.

En este paso, verificará la conectividad a Internet para poder descargar actualizaciones. Además, verificará la conectividad entre **CSE-LABVM** y la PC con Windows para poder realizar tareas más adelante en esta práctica de laboratorio.

a. Antes de iniciar **CSE-LABVM**, selecciónelo y elija **Configuración> Red**. Para el **adaptador 1**, cambie la opción **Adjunto a**: a **Adaptador en puente**. Luego puede elegir el adaptador. Muchas computadoras tienen dos adaptadores: uno para redes inalámbricas y otro para redes cableadas. Elija el que usa su computadora para conectarse a Internet.

b. Inicie CSE-LABVM y espere a que arranque.

c. En CSE-LABVM, abra un terminal e introduzca **ip address** para determinar su dirección IP.

d. En la computadora host de Windows, abra un símbolo del sistema e introduzca **ipconfig** para determinar su dirección IP.

Registre la dirección IP para CSE-LABVM y PC con Windows.

CSE-LABVM: 192.168.0.107

Computadora con Windows: 192.168.0.112

e. Desde las solicitudes de comando respectivas, haga ping en un sitio web de su elección para verificar que el host de Windows y **CSE-LABVM** puedan conectarse a Internet.

f. Verifique que el host de Windows pueda hacer ping al **CSE-LABVM**.

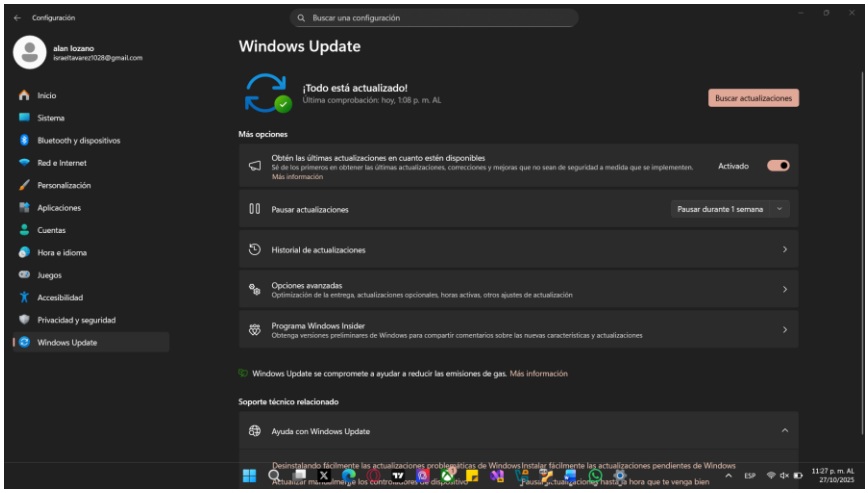
g. Desde **CSE-LABVM**, intente hacer ping al host de Windows. Es posible que **CSE-LABVM** no pueda hacer ping al host de Windows debido a la configuración de firewall predeterminada en Windows. Modificará la regla del firewall más adelante en esta práctica de laboratorio para permitir el ping a través del Firewall de Windows. Presione **CTRL-C** para detener los pings si es necesario.

Paso 2: Verificación de actualizaciones de Windows

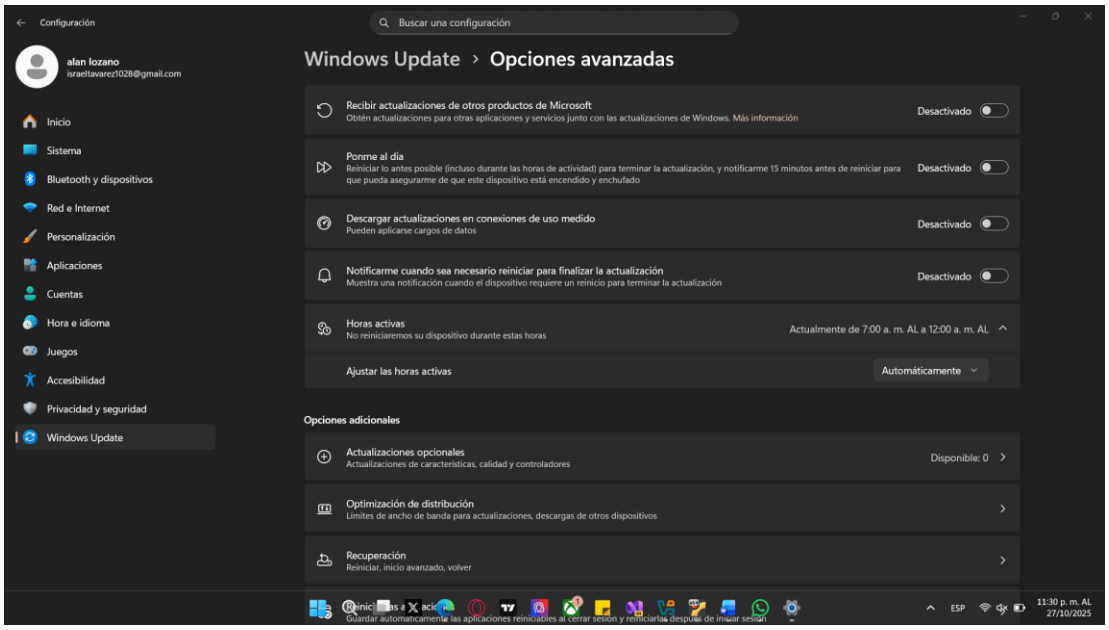
a. En el **menú Inicio de Windows**, busque **Buscar actualizaciones**.

b. En la ventana de **Windows Update**, puede revisar las actualizaciones opcionales y el historial de actualizaciones. Explore todas las opciones disponibles relacionadas con Windows Update y responda las siguientes preguntas.

¿Cuándo fue la última vez que el sistema buscó actualizaciones?



¿Cuáles son sus horas activas actuales? ¿Qué hará Windows fuera del horario de atención?



Paso 3: Actualización y actualización de Linux

a. En **CSE-LABVM**, introduzca el comando **apt-get** para ver la lista de comandos disponibles. El comando **apt-get update** siempre debe realizarse antes de una actualización.

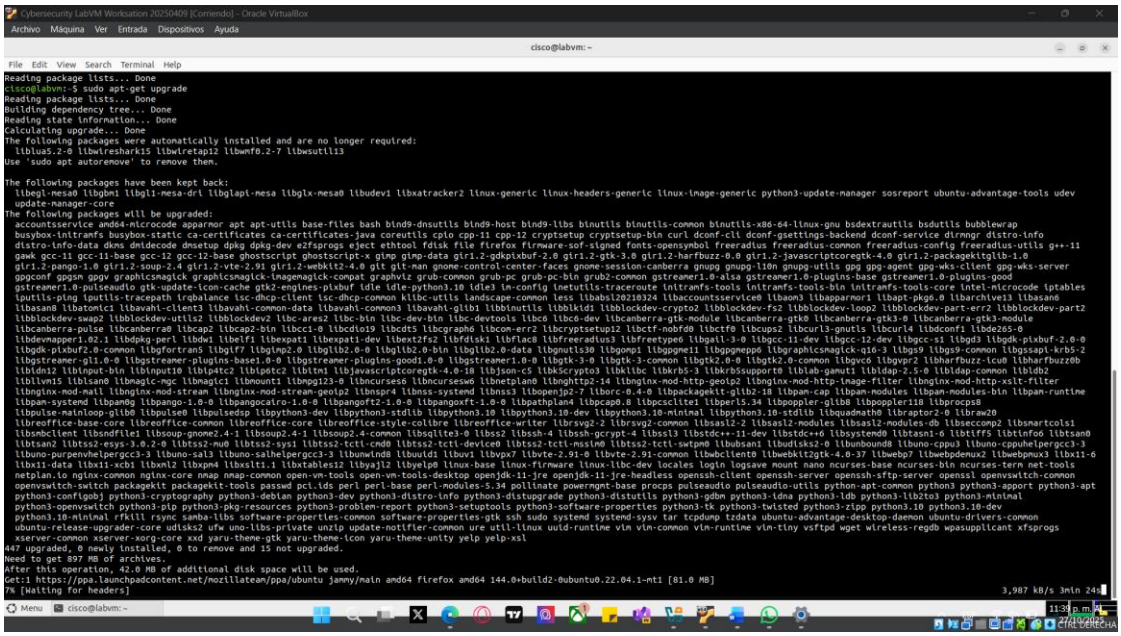
b. Ingrese el comando **sudo apt-get update** para volver a sincronizar los archivos de índice del paquete de sus fuentes. Introduzca la contraseña **password** cuando se le solicite.

```
cisco@labvm:~$ sudo apt-get update
[sudo] password for cisco:
```

c. En el terminal, ingrese el comando **sudo apt-get upgrade** para recuperar y actualizar los paquetes instalados actualmente con nuevas versiones disponibles. Este comando no eliminará los paquetes instalados actualmente. Si no se puede actualizar la versión más reciente, no se realizarán cambios en los paquetes.

Introduzca la contraseña **password** cuando se le solicite. Responda **y** cuando se le pregunte si desea continuar. Este proceso puede demorar algunos minutos.

```
cisco@labvm:~$ sudo apt-get upgrade
[sudo] password for cisco:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
<output omitted>
Need to get 479 MB of archives.
After this operation, 53.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```



Parte 2: Política de seguridad local de Windows (opcional)

La Política de seguridad local de Windows de un sistema es un conjunto de información sobre la seguridad de su computadora. En esta parte, configurará la política de contraseña local, la configuración de bloqueo de cuenta y la política de auditoría.

Nota: La política de seguridad local solo viene con las ediciones Windows Pro o Enterprise. Si tiene la edición Home, puede buscar en Internet tutoriales sobre "Cómo habilitar la política de seguridad local (secpol.msc)". Por ejemplo, el sitio web majorgeeks.com tiene un excelente tutorial. Si no se le permite o prefiere no cambiar la política de seguridad local en su host de Windows, lea esta parte y pase a la siguiente.

Paso 1: Configurar la política de contraseña local en Windows

Ha determinado que la política de seguridad para la contraseña es la siguiente:

- Un usuario debe utilizar una contraseña única al menos en 2 cambios de contraseña.
- Las contraseñas deben tener al menos 8 caracteres.
- Las contraseñas deben cambiar cada 90 días.
- Can only change the password once a day.
- Una contraseña debe constar de tres de los siguientes cuatro elementos:
  - Al menos un carácter alfabético en minúsculas.
  - Al menos un carácter alfabético en mayúsculas.
  - Al menos un carácter numérico.
  - Al menos un carácter de símbolo.

a. Desplácese hasta la **Política de seguridad local** buscando primero y abriendo el **Panel de control**.

b. Haga clic en **Herramientas administrativas** > Buscar **política de seguridad local**.

c. Abra **Políticade seguridad local**.

Enumere algunas configuraciones de políticas de seguridad:

Vigencia máxima y mínima de contraseñas.

Longitud mínima de contraseñas.

Historial de contraseñas requeridas.

Complejidad de contraseñas.

Almacenamiento de contraseñas cifradas.

d. Expanda **Políticas de cuenta** y haga clic en **Políticade contraseñas**. Se muestran seis políticas en el panel derecho con sus configuraciones de seguridad predeterminadas asociadas.

e. La primera política, **Exigir historial de contraseñas**, se utiliza para establecer la cantidad de contraseñas únicas que el usuario debe introducir antes de permitirle reutilizar una contraseña. Haga doble clic en **Exigir historial de contraseñas** para abrir la ventana **Exigir propiedades del historial de contraseñas**. Set the value to **2**.

f. Mediante los requisitos de la política de seguridad del Paso 1, llene los valores que debe establecer en **Política de seguridad local** para las configuraciones de seguridad de **Política de contraseñas** restantes.

Política	Configuración de seguridad
Exigir el historial de contraseñas	2 contraseñas recordadas
Vigencia máxima de la contraseña	42 días
Antigüedad mínima de contraseña	0 días
Longitud mínima de la contraseña	0 caracteres
La contraseña debe cumplir con los requisitos de complejidad	deshabilitada
Guarde las contraseñas mediante cifrado reversible	deshabilitada

Nota: La **configuración de seguridad Almacenar contraseñas con cifrado reversible** debe estar desactivada en todo momento. Almacenar contraseñas mediante cifrado reversible es esencialmente lo mismo que almacenar las versiones de texto no cifrado de las contraseñas. Por este motivo, esta política nunca debe activarse a menos que los requisitos de aplicaciones sobrepasen la necesidad de proteger la contraseña.

g. Haga doble clic en cada una de las políticas y establezca los valores según las entradas en la tabla anterior.

Paso 2: Pruebe las configuraciones de seguridad de políticas de contraseña.

Pruebe las configuraciones de seguridad de políticas de contraseña intentando cambiar la contraseña. Intente con una nueva contraseña que no cumpla con la longitud o los requisitos de complejidad.

a. En el menú Inicio, busque **Cambiar contraseña**.

b. Haga clic en **contraseña**. Haga clic en **Cambiar**.

c. Ingrese su contraseña actual. Haga clic en **Siguiente** para continuar.

d. Ingrese la contraseña actual y proporcione su contraseña nueva dos veces. Asegúrese de que su nueva contraseña no cumpla con los requisitos de longitud o complejidad que configuró en el paso anterior. Haga clic en **Siguiente** para continuar.

e. Haga clic en **Finalizar**. Se le debe indicar con un mensaje que su nueva contraseña no cumple con los requisitos de políticas de contraseña. Haga clic en **Cerrar** para continuar.

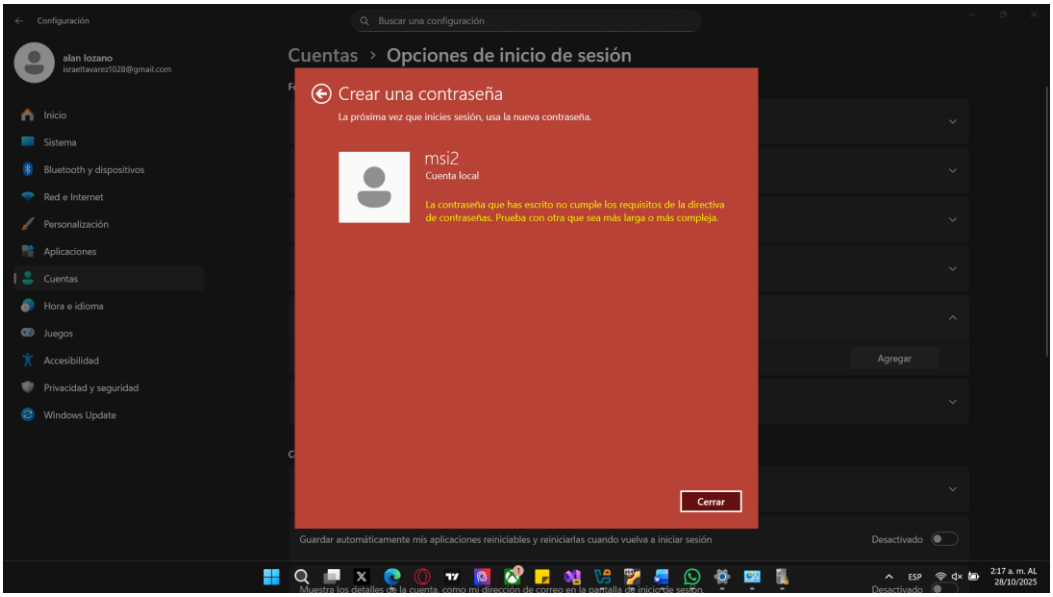
Paso 3: Configure las configuraciones seguridad de la política de bloqueo de cuentas.

a. Vuelva a la ventana Política de seguridad local.

b. En las **Políticas de cuenta** ampliadas y haga clic en **Política de bloqueo de cuenta**. Se muestran tres políticas en el panel derecho con sus configuraciones de seguridad predeterminadas asociadas.

c. Cambie la configuración predeterminada a lo siguiente:

- Un usuario debe esperar 10 minutos para que el contador se restablezca.
- Los usuarios son bloqueados de la computadora después de 5 intentos de ingresar la contraseña correcta.



¿Cuánto tiempo debe esperar el usuario antes de intentar volver a iniciar sesión?

10 minutos

¿Cuántas veces se le permite a un usuario intentar iniciar sesión antes de que se bloquee la cuenta?

5 minutos

Paso 4: Configure la seguridad de la política de auditoría.

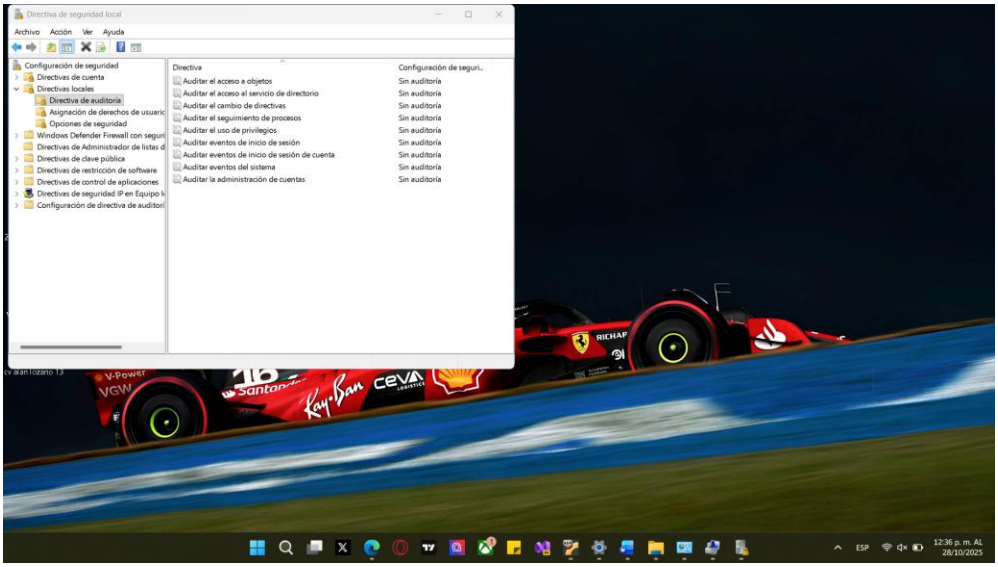
a. Expanda el menú **Políticas locales** y luego haga clic en **Políticade auditoría**.

b. Haga doble clic en **Auditar eventos de inicio de sesión de cuenta** para abrir laventana Propiedades.

c. En la pestaña **Configuración de seguridad local**, observe las casillas de verificación para **Éxito** y **Fallo**.

d. Haga clic en la pestaña **Explicar** para obtener sobre esta configuración de seguridad. Haga clic en **Aceptar** para cerrar la ventana **Propiedades**.

e. Continúe revisando cada configuración de seguridad. Haga clic en la pestaña **Explicar** para cada uno y lea lo que hace.



Parte 3: Configurar reglas de firewall

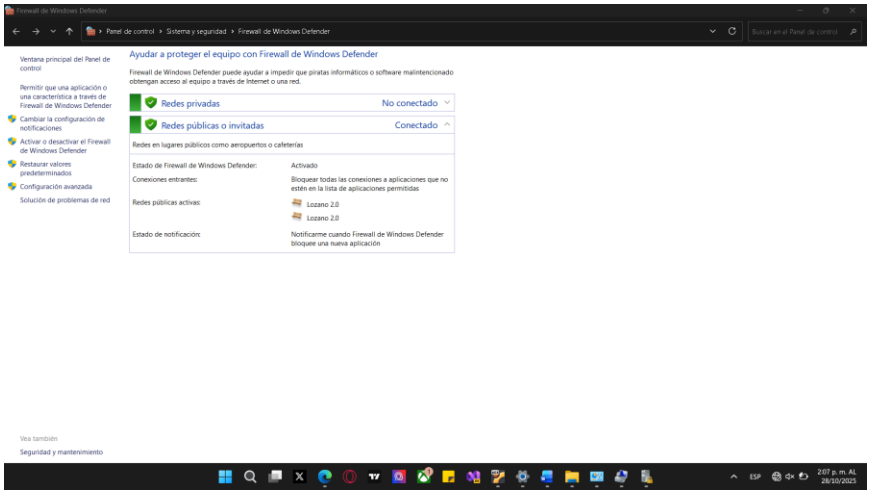
El tráfico ingresa y sale de los dispositivos mediante puertos. El firewall controla el flujo del tráfico. Piense en el firewall como un guardia de seguridad que controla el tráfico entrante y saliente según las reglas del firewall.

En esta parte, configurará el firewall de Windows Defender en Windows.

Paso 1: Investigar el firewall de Windows Defender

a. Desde el menú Inicio, busque y abra el **Firewall de Windows Defender**. El estado normal del Firewall de Windows es Activado.

Nota: Si utiliza una PC con Windows administrada por una organización, es posible que vea el mensaje: **Para su seguridad, el administrador del sistema administra algunas configuraciones.**



¿Cuáles son los beneficios del Firewall de Windows?

El Firewall de Windows protege el equipo al **bloquear conexiones no autorizadas** y **permitir solo el tráfico seguro**, ayudando a **prevenir ataques de red y accesos no deseados**.

b. En el panel izquierdo de la ventana, haga clic en **Permitir una aplicación o función a través de Firewall de Windows Defender**. En la ventana **Aplicaciones y funciones permitidas**, los programas y servicios que el Firewall de Windows no está bloqueando aparecerán con una marca de verificación.

Nota: Puede agregar aplicaciones a esta lista. Esto puede ser necesario si tiene una aplicación que requiere comunicaciones externas pero, por alguna razón, el Firewall de Windows no puede realizar la configuración automáticamente.

La creación de demasiadas excepciones en el archivo Programas y servicios puede tener consecuencias negativas.

Describa una consecuencia negativa de tener demasiadas excepciones.

Tener demasiadas excepciones puede **debilitar la seguridad** del sistema, permitiendo que programas maliciosos se conecten a Internet o que **usuarios no autorizados accedan al equipo.**

c. Haga clic en **Cancelar** para salir de la ventana Permitir aplicaciones.

Paso 2: configure las funciones de seguridad avanzada en el Firewall de Windows para permitir solicitudes de eco.

Nota: Este paso puede no estar permitido por la política de seguridad de su organización.

En este paso, creará una regla de entrada que permitirá los paquetes de solicitud de eco a través del firewall.

a. En el panel izquierdo de la ventana Windows Firewall (Firewall de Windows), haga clic en **Advanced settings** (Configuración avanzada).

b. En el **Firewall de Windows Defender con seguridad avanzada en la computadora local**, puede configurar reglas de entrada, reglas de salida o reglas de seguridad de conexión. También puede hacer clic en **Supervisar** para ver el estado de reglas configuradas.

c. Haga clic en **Reglas entrantes** y, en el panel **Acciones**, haga clic en **Nueva regla**.

d. En el **Asistente para nueva regla de entrada**, seleccione **Personalizado** y haga clic en **Siguiente** dos veces. Ahora debe estar en el paso de **protocolo y puertos**.

e. Para **Tipo de protocolo**, seleccione **ICMPv4** y haga clic en **Personalizar**.

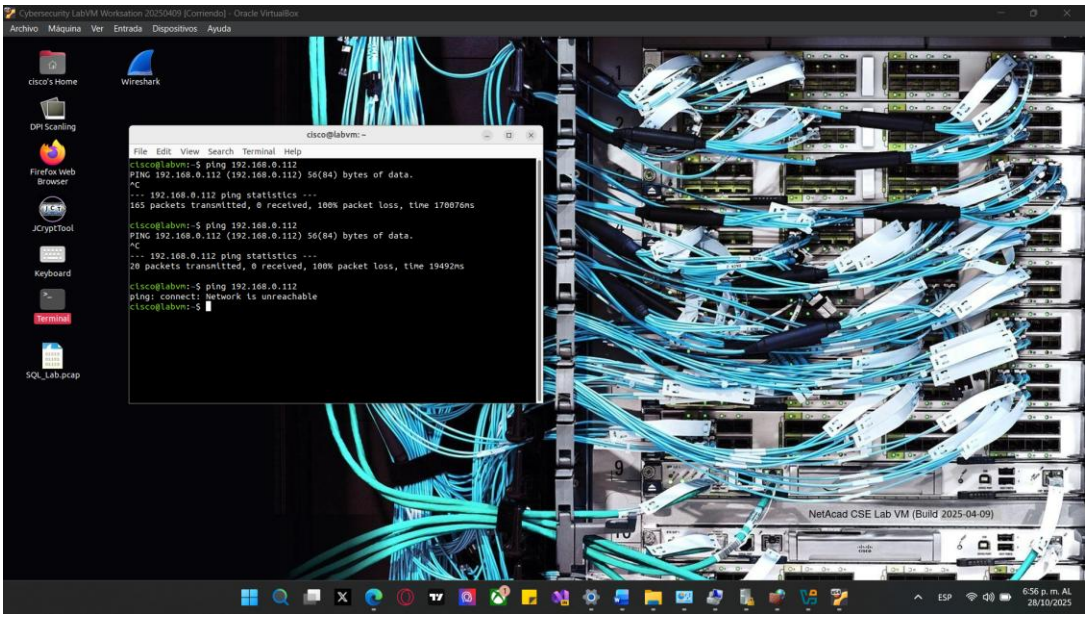
f. En la ventana **Personalizar configuración de ICMP**, seleccione **Tipos de ICMP específicos**, seleccione **Solicitud de eco** y haga clic en **Aceptar**.

g. Haga clic en **Next** (Siguiente) tres veces. Ahora debe estar en el paso **Perfil**.

h. Anule la selección de **Public** (Public) para que la PC con Windows no responda a una solicitud de eco en una ubicación de red pública, como un cibercafé. Haga clic en el botón **Siguiente** para continuar.

i. Proporcione un nombre para la nueva regla entrante que proporcione una buena descripción de la regla y haga clic en **Finalizar**. Ahora debería ver su regla en la parte superior de la lista de **Reglas de entrada** en el cuadro de diálogo **Firewall de Windows Defender con seguridad avanzada**.

j. Ahora la regla se ha creado y habilitado. Verifique que **CSE-LABVM** pueda hacer ping al host de Windows y recibir respuestas.



Parte 4: Instalar y ejecutar aplicaciones

En esta parte, instalará dos nuevas aplicaciones en **CSE-LABVM: chkrootkit y lynis**. La aplicación **chkrootkit** se descargará de un repositorio de software. Sin embargo, agregaremos un nuevo repositorio para poder instalar **lynis**, provisto por CISOfy.

Paso 1: Instale y ejecute chkrootkit

La herramienta **chkrootkit** se utiliza para verificar si hay signos de un rootkit en un sistema local. Rootkit es un tipo de malware que puede permanecer oculto en su computadora y puede ser utilizado para causar daños significativos a su dispositivo por hackers.

a. En una terminal, introduzca el comando **sudo apt install chkrootkit**. Introduzca la contraseña **password** cuando se le solicite.

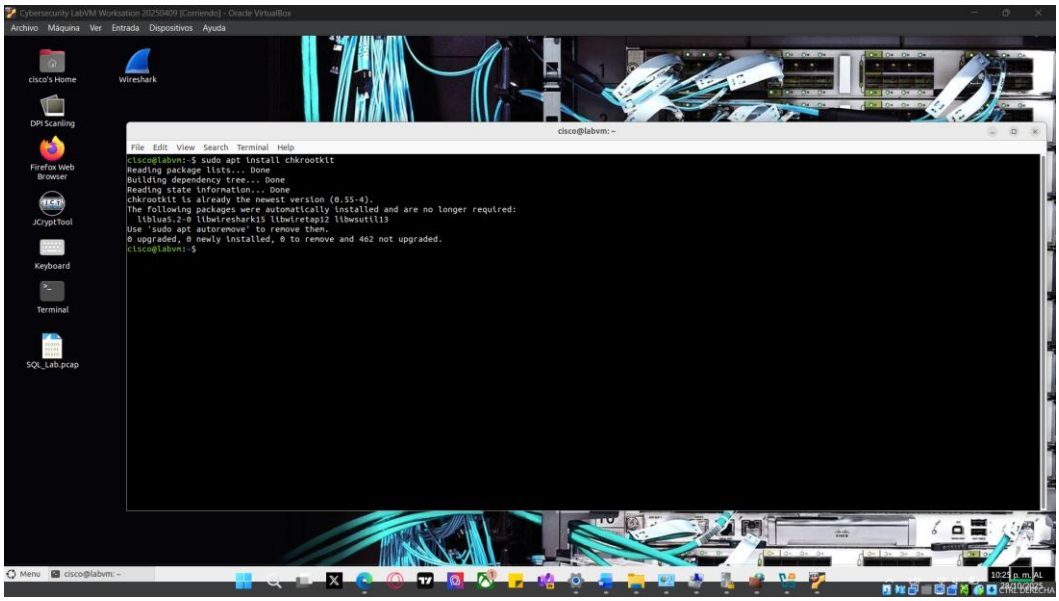
```
cisco@labvm:~$ sudo apt install chkrootkit
[sudo] password for cisco:
```

b. Ingrese el comando **sudo chkrootkit** para ejecutar una comprobación de rootkit.

```
cisco@labvm:~$ sudo chkrootkit
```

c. La salida se puede filtrar para buscar cadenas interesadas, como gusanos. El comando **chkrootkit** se puede canalizar junto con el comando **grep** con la opción **–i** para ignorar la distinción de mayúsculas y minúsculas en las cadenas de interés.

```
cisco@labvm:~$ sudo chkrootkit | grep -i worm
Searching for LPD Worm files and dirs...                   nothing found
Searching for Ramen Worm files and dirs...                 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 TC2 Worm default files and dirs...           nothing found
! cisco       32822 pts/0  grep --color=auto -i worm
```

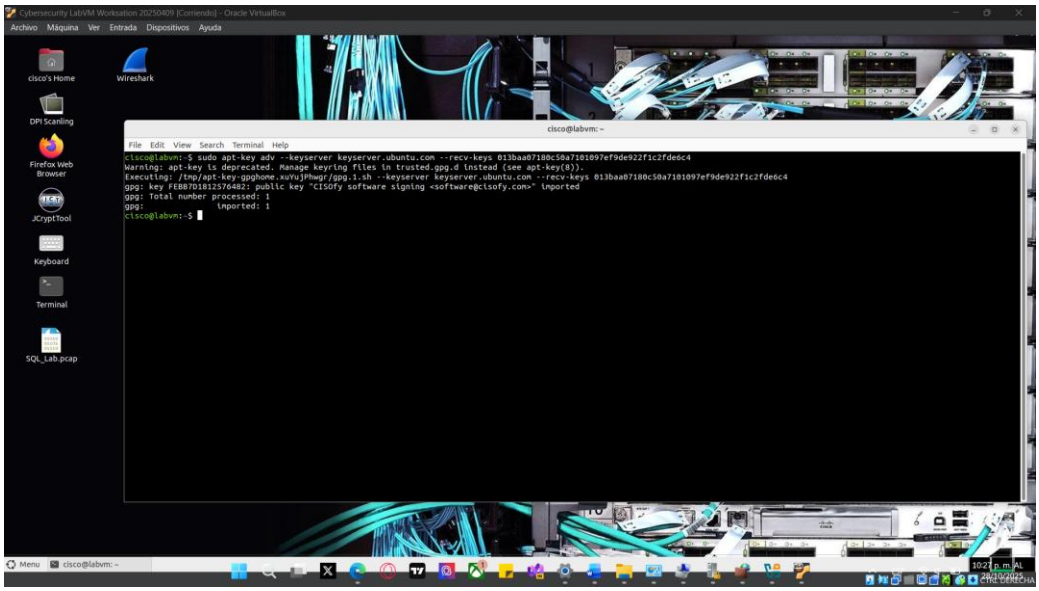


Paso 2: Instalar Lynis

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. CISOfy mantiene la aplicación **Lynis**. En este paso, agregaremos el repositorio de software e instalaremos Lynis.

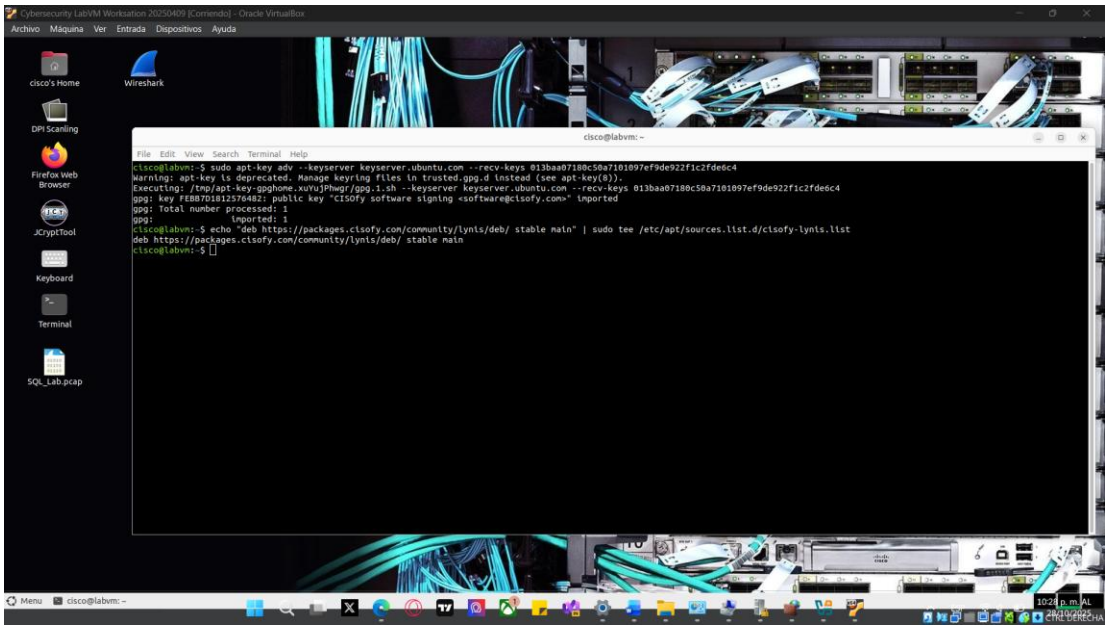
a. Copie y pegue el siguiente comando en un terminal para importar la clave del servidor de claves CISOfy. Esta clave es necesaria para verificar la integridad de la descarga cuando descarga **lynis**:

```
cisco@labvm:~$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys
013baa07180c50a7101097ef9de922f1c2fde6c4
Executing: /tmp/apt-key-gpghome.8C6X477onz/gpg.1.sh --keyserver keyserver.ubuntu.com -
--recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4
gpg: key FEBB7D1812576482: public key "CISOfy software signing <software@cisofy.com>"
imported
gpg: Total number processed: 1
gpg:               imported: 1
```



b. Copie y pegue el siguiente comando en una terminal para agregar el repositorio de **lynis** que mantiene CISOfy.

```
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/ estable main
```

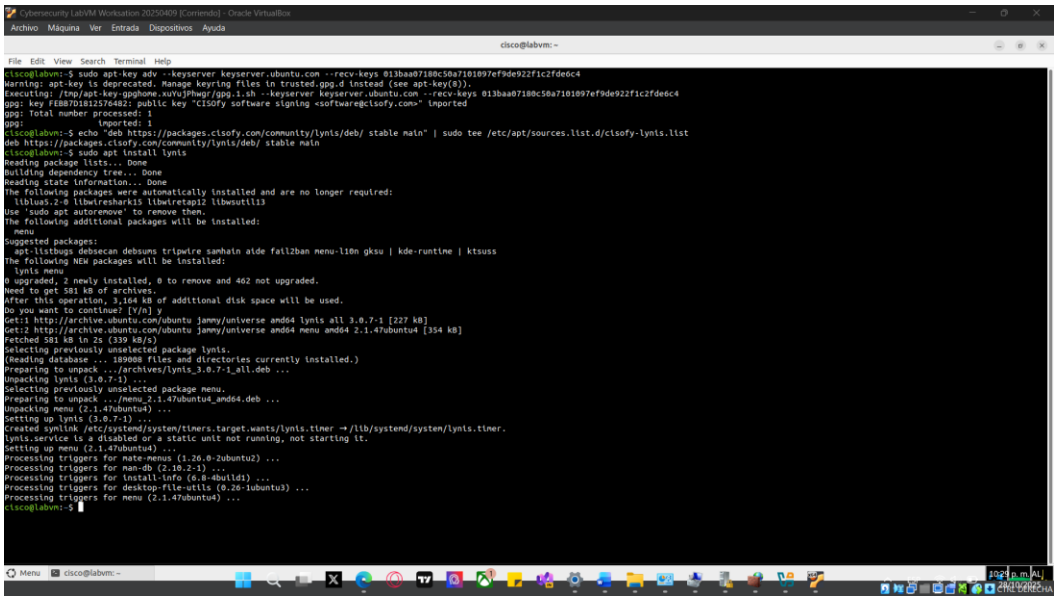


c. Realice una actualización después de agregar un nuevo repositorio. Cuando se le solicite, ingrese **sudo apt-get update**.

d. Utilice el comando **apt install** para instalar Lynis.

```
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) ...
```

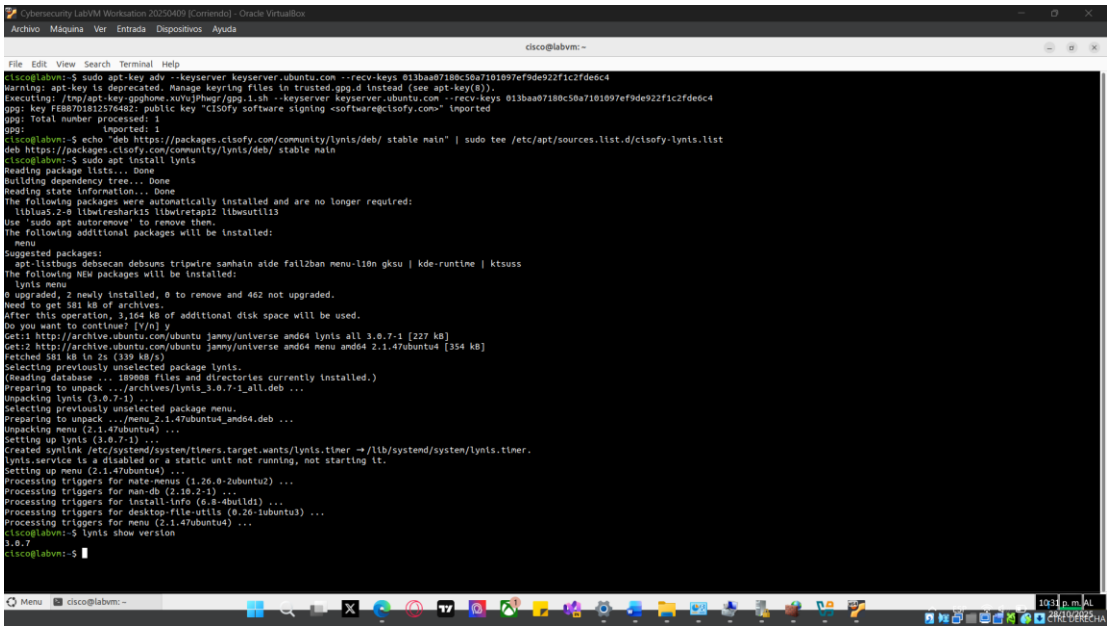
En la salida, ¿cuál es la versión instalada de Lynis?



Setting up lynis (3.0.7-1) ...

e. Para verificar la versión instalada, ingrese el comando **lynis show version** en la terminal.

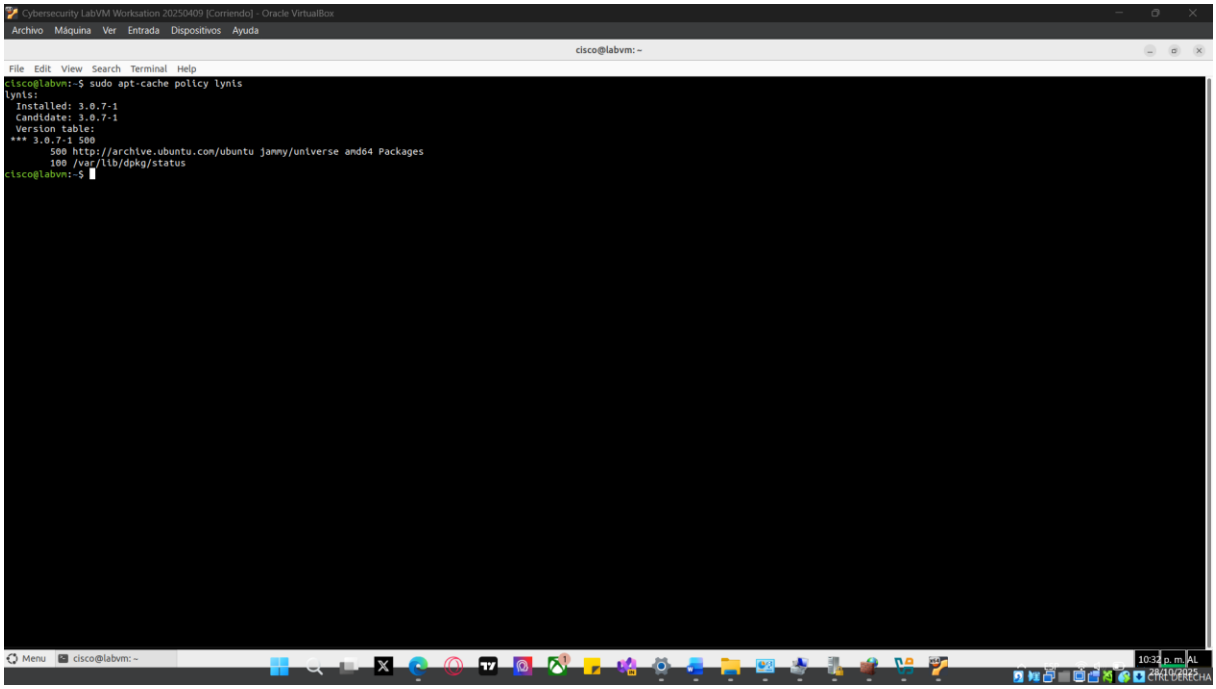
```
cisco@labvm:~$ lynis show version
3.0.6
```



f. Si desea 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
```



g. Puede ejecutar **sudo apt-get update** y **sudo apt-get upgrade** nuevamente para asegurarse de contar con las últimas actualizaciones de CISOfy