# Práctica de laboratorio: fortalecimiento de un sistema Linux

## Objetivos

Demostrar el uso de la herramienta de auditoría seguridad para reforzar un sistema Linux.

## 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.

## Recursos necesarios

- Computadora con sistema Ubuntu 16.04.4 Desktop LTS instalado en una máquina virtual de VirtualBox o VMware.

### Paso 1: Abra una ventana del terminal en Ubuntu.

a. Inicie sesión en Ubuntu con las siguientes credenciales:

Usuario: **cisco**

Contraseña: **password**


b. Haga clic en el icono de terminal para abrir una ventana de terminal.

### Paso 2: La herramienta Lynis

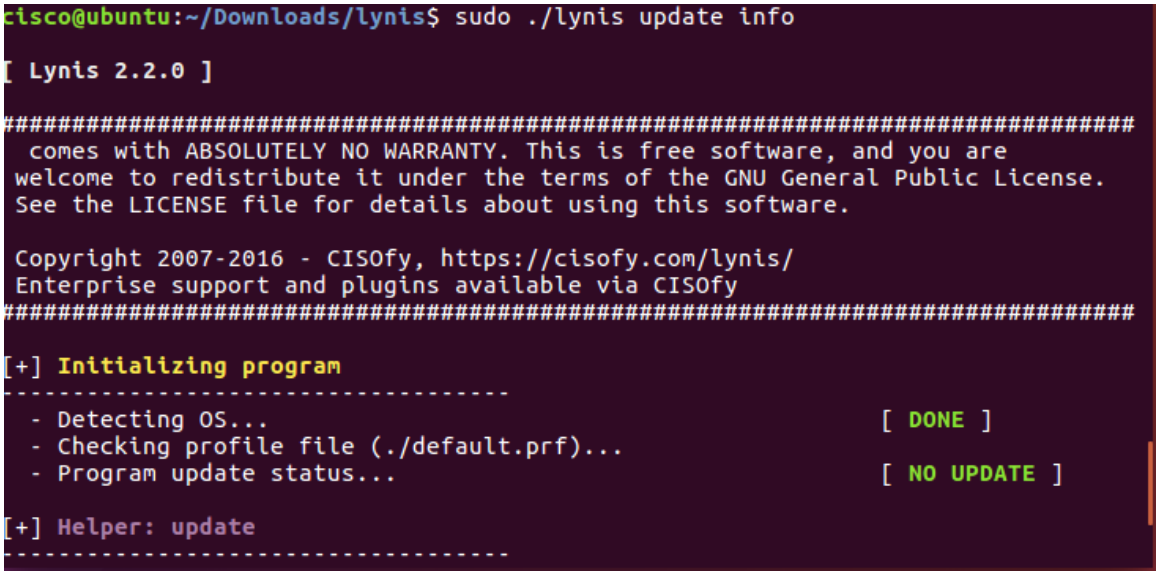
a. En la petición de ingreso de comando, ingrese el siguiente comando para cambiar el directorio de lynis:

```
cisco@ubuntu:~$ cd Downloads/lynis/
```

```
cisco@ubuntu:~$ cd Downloads/lynis/
cisco@ubuntu:~/Downloads/lynis$
```

b. En la petición de ingreso de comandos, introduzca el siguiente comando y la contraseña **password** cuando se le solicite:

```
cisco@ubuntu:~/Dowloads/lynis$ sudo ./lynis update info
```

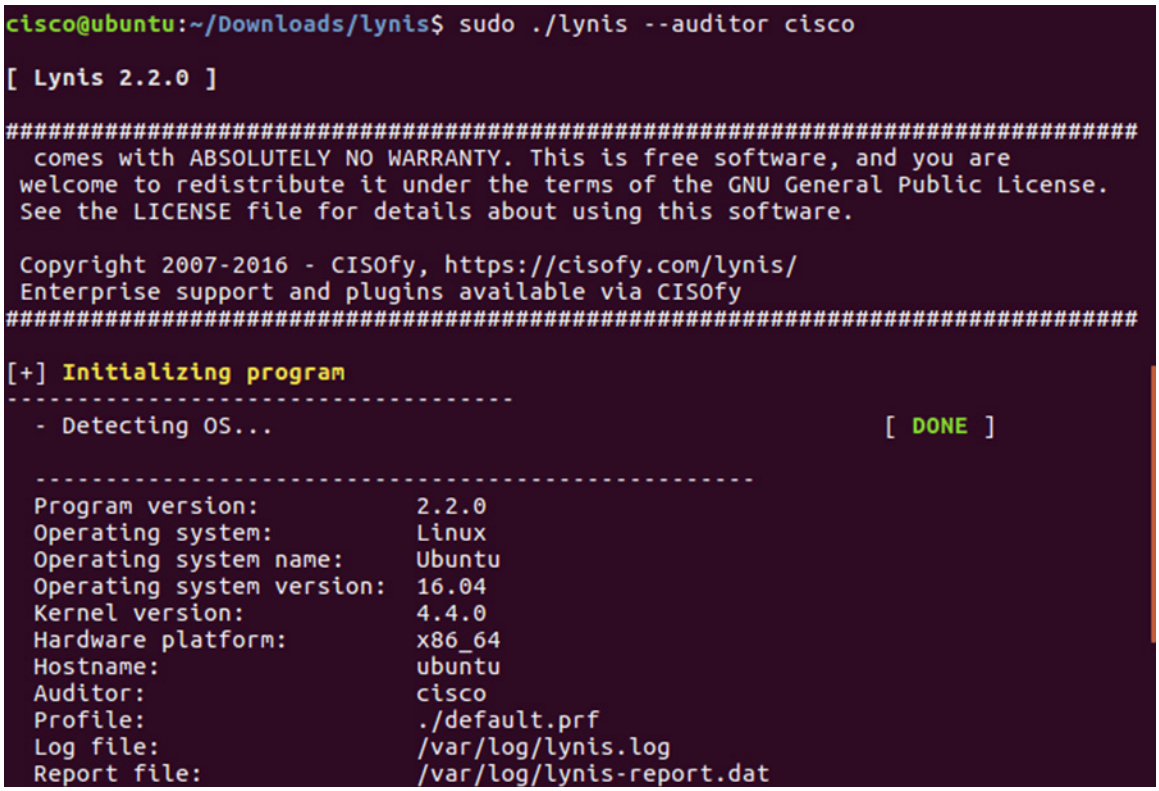



Este comando verifica que esta es la versión más recientes y actualiza la herramienta al momento de la redacción de esta práctica de laboratorio.

## Paso 3: Ejecute la herramienta

a. Escriba el siguiente comando en el terminal y presione **Intro**:

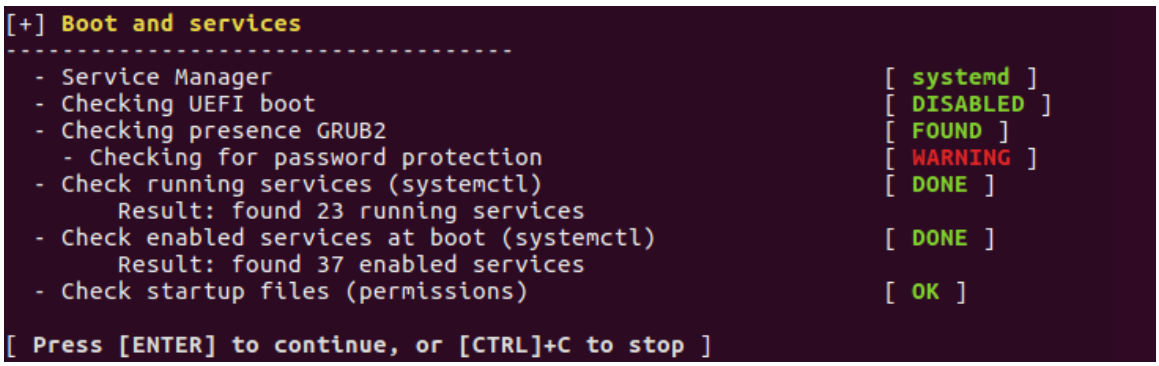
```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```




Como se muestra arriba, la herramienta comenzará a auditar mediante el usuario **cisco** como el auditor.

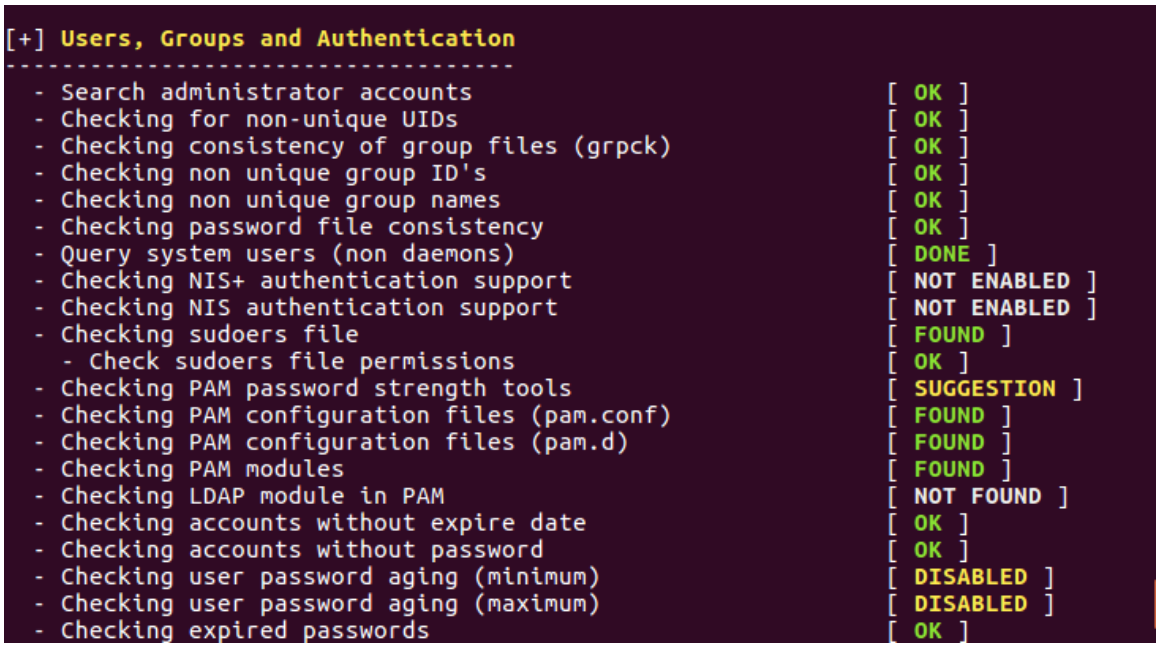
Aviso: recibirá **advertencias**.

b. Para continuar con cada etapa de la auditoría presione **Intro**. Recibirá advertencias como se muestra a continuación.

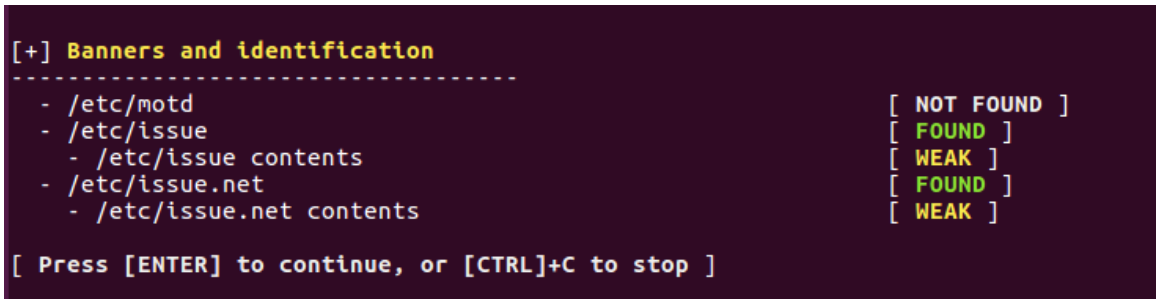


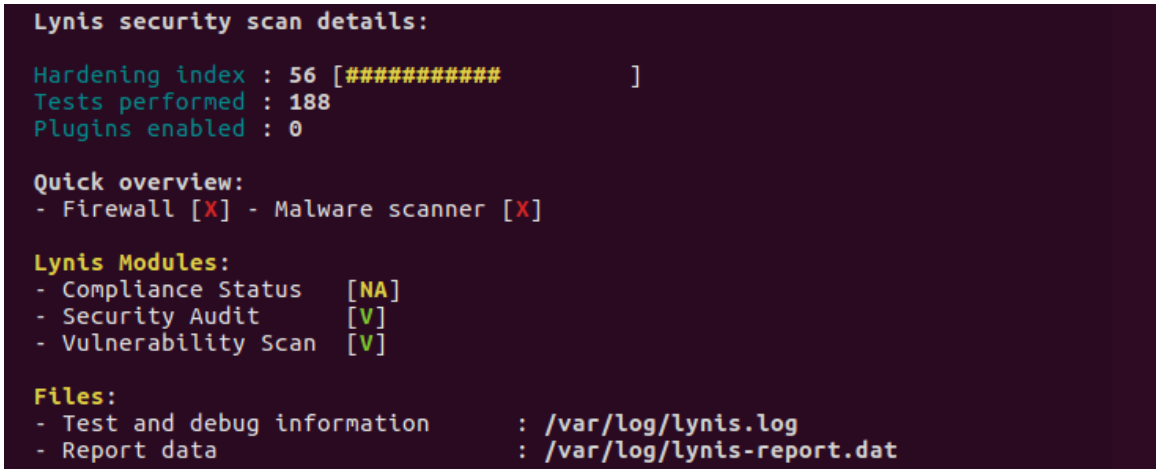
c. Recibirá advertencias como se muestra a continuación.




d. Recibirá una notificación para cada configuración que es débil como se muestra a continuación:




e. Recibirá sugerencias detalladas de mejora de la seguridad y también un resumen final que proporciona la ubicación donde puede encontrar el archivo de registro.



## Paso 4: Revise los resultados

a. Desplácese hasta la sección de resultados después de que la herramienta haya terminado de ejecutarse.

¿Cuántas advertencias recibió?

¿Cuántas sugerencias recibió?

b. Desplácese hasta las sugerencias y seleccione uno. Investigará una sugerencia que pueda implementar para resolver el problema.

¿Qué sugerencia considerará?

¿Cuál es la solución sugerida?

## Referencias

Lynis: https://cisofy.com/lynis/