Universidad Francisco de Vitoria
*Centro de Documentación Europea*
UFV Madrid

# Bastionado Linux

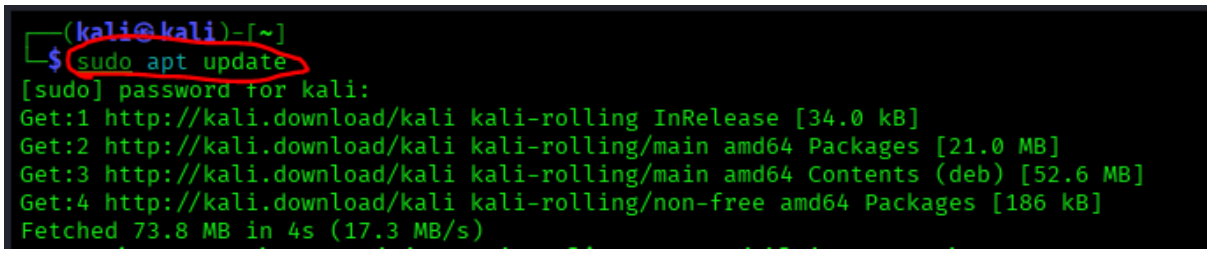
Héctor Ramírez López

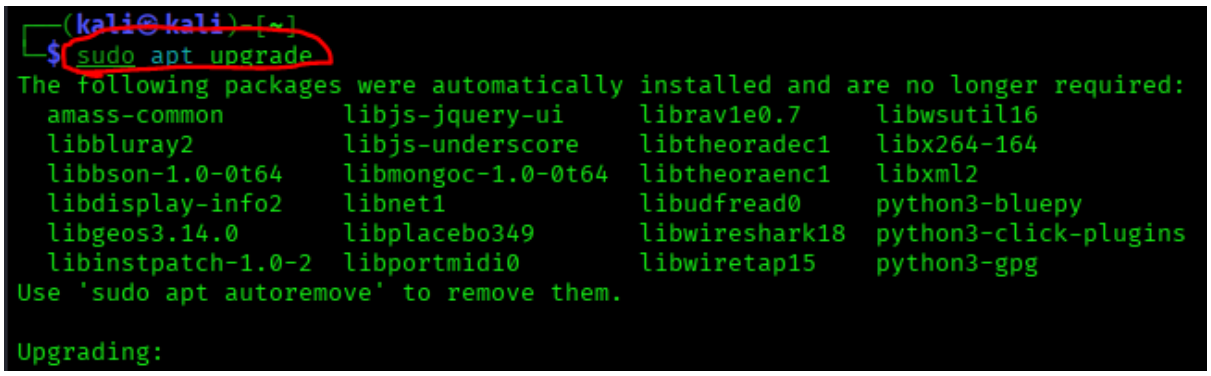
Índice

# 1. Configuración del sistema

## 1.1. Actualización y mantenimiento del sistema

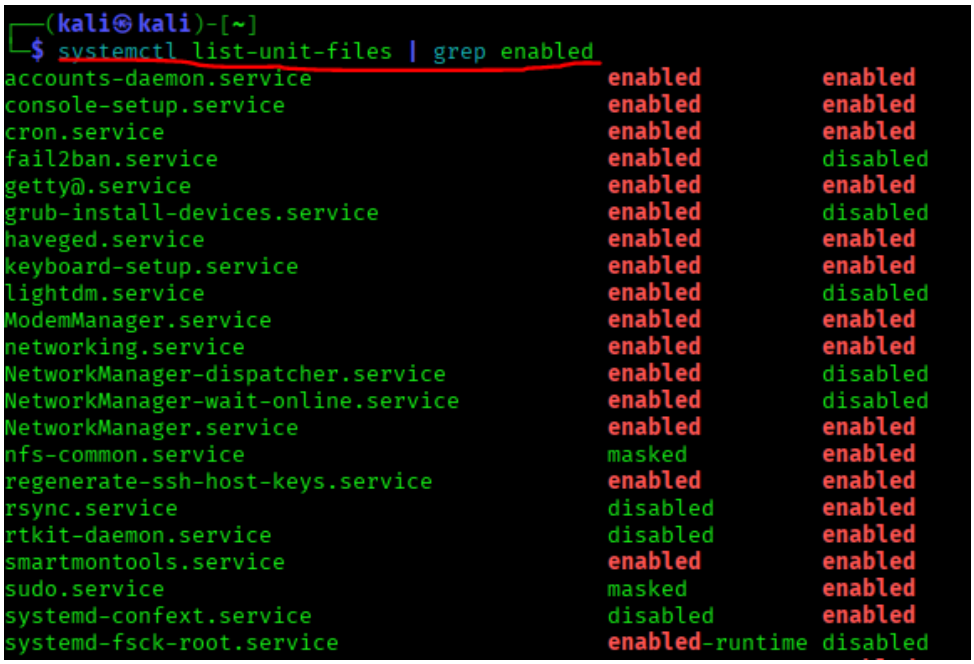
Lo primero que vamos a hacer es actualizar el sistema con los comandos (sudo apt update) y (sudo apt upgrade)



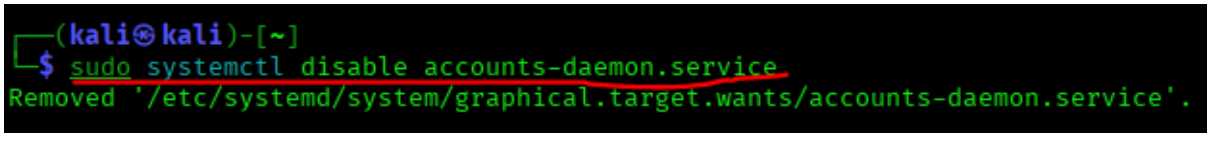
## 1.2. Eliminación de servicios

Ahora veremos como deshabilitar un servicio en caso de que no lo necesitemos, para ello ejecutaremos el comando de la imagen para ver qué servicios están habilitados.

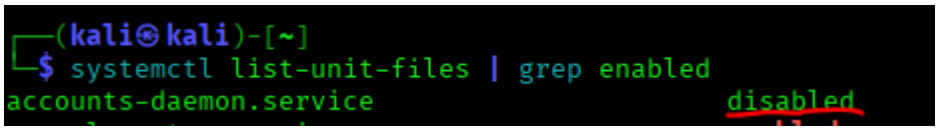



En este caso para ver como deshabilitarlo lo haremos con el servicio de la imagen.

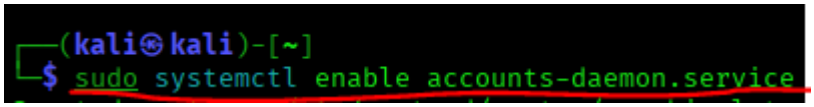

Para ello ejecutamos el siguiente comando .



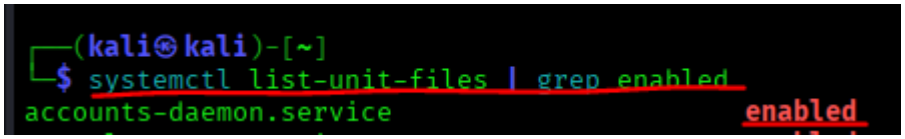
Y comprobamos con el comando anterior que se ha deshabilitado.




Ahora volveremos a habilitar el servicio con el comando siguiente .

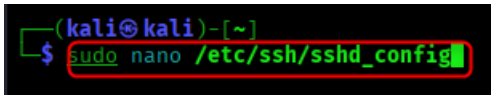



Volveremos a comprobar que se ha habilitado.

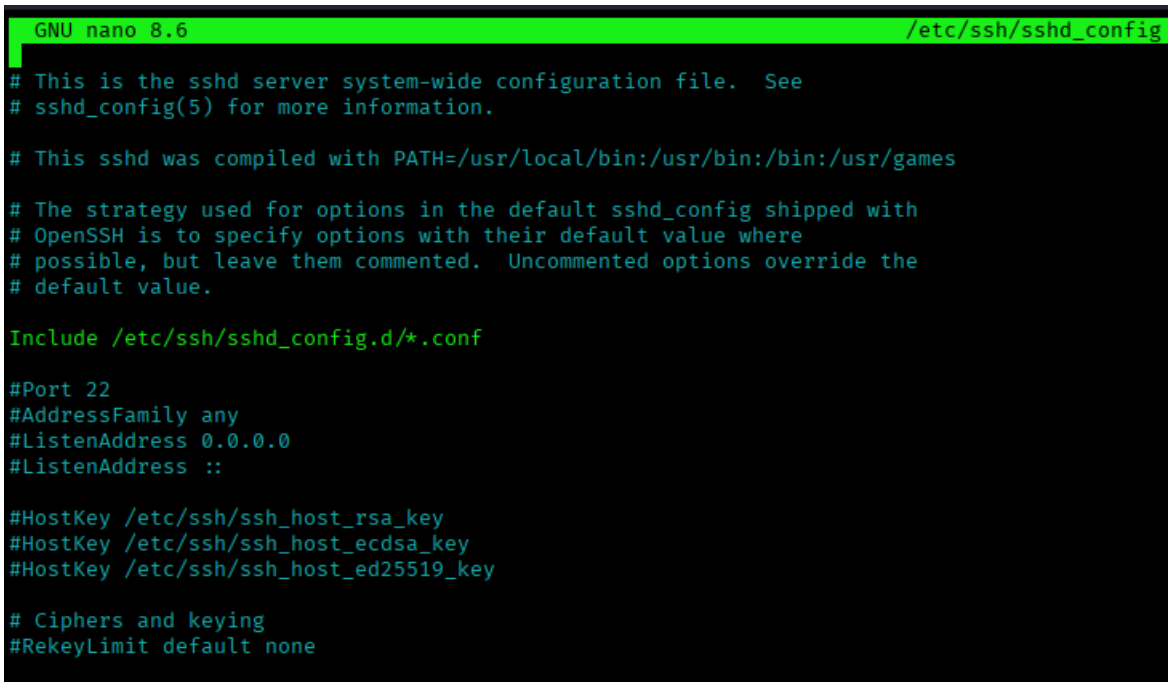


## 1.3. Configuración segura del servicio SSH

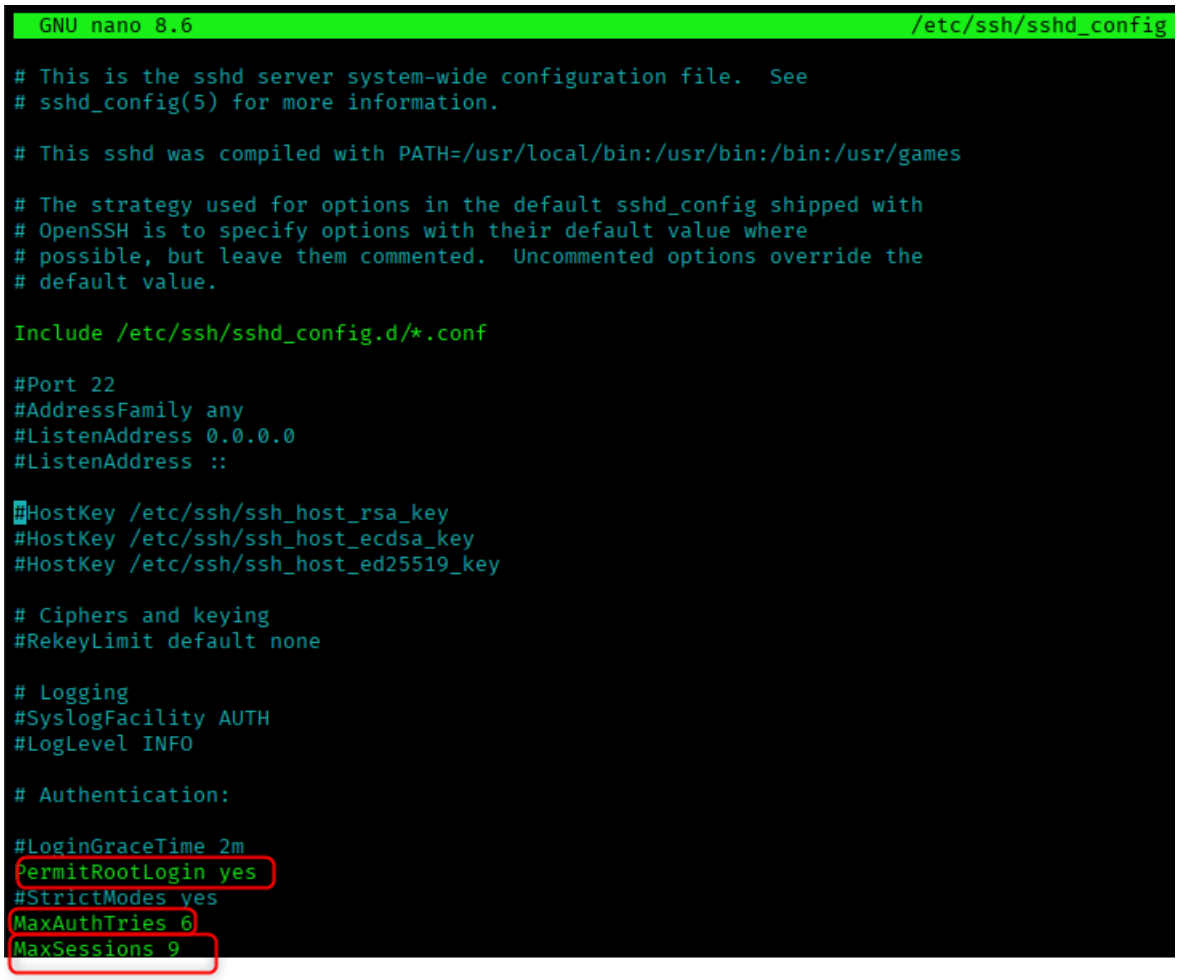
Ahora lo primero sera editar el fichero de configuración del SSH con el comando (sudo nano /etc/ssh/sshd_config) .




Una vez abierto el archivo para editarlo lo veremos así .

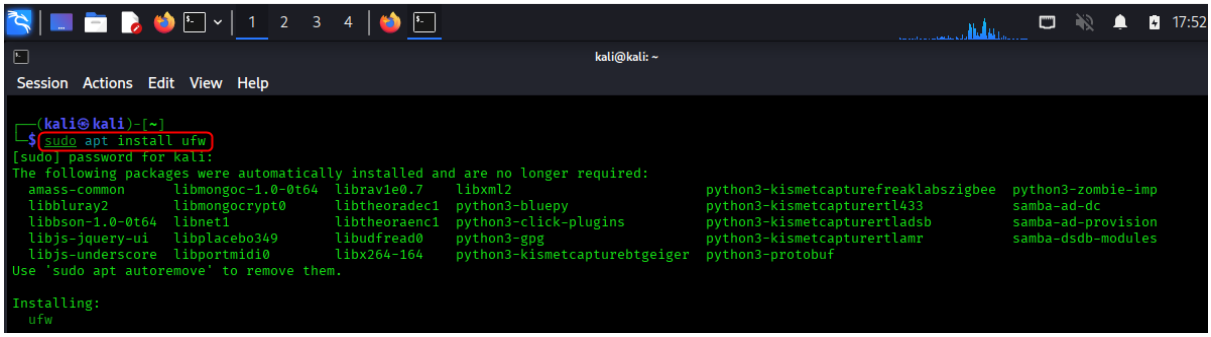


Ahora modificaremos algunos parámetros del archivo como (permitrootlogin yes) para permitir el acceso a root por SSH, (maxauthries) para establecer el maximo de intentos para autenticarse en este caso hemos puesto 6 y (maxsessions ) para limitar el número de sesiones simultaneas en este caso hemos puesto 9.

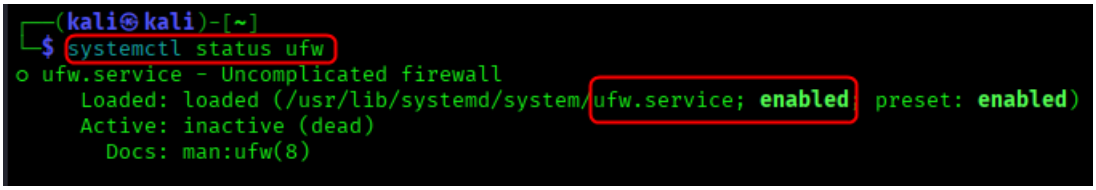


## 1.4. Configuración de firewall

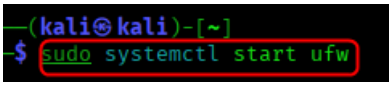
Lo primero que haremos en este punto será instalar el firewall con el comando (sudo apt install ufw).



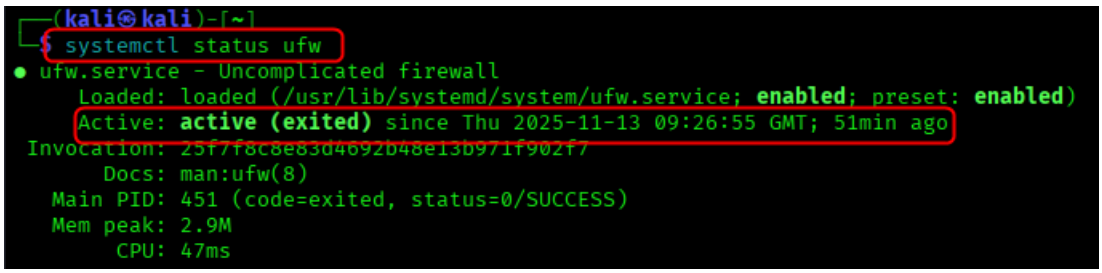

Una vez instalado nos aseguramos de que el servicio UFW este habilitado lo vemos con el comando (systemctl status ufw) como se observa en la imagen está habilitado.



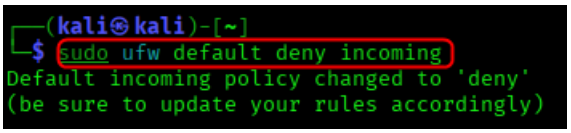

El siguiente paso es activar el servicio con el comando (sudo systemctl start ufw).



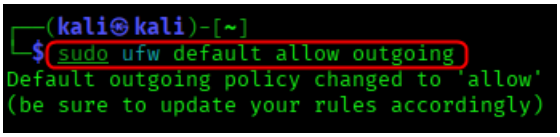

Comprobaremos que está activo con el comando anterior.



Ahora procederemos a aplicar una regla al firewall para que rechace las conexiones entrantes lo haremos con el comando (sudo ufw default deny incoming).



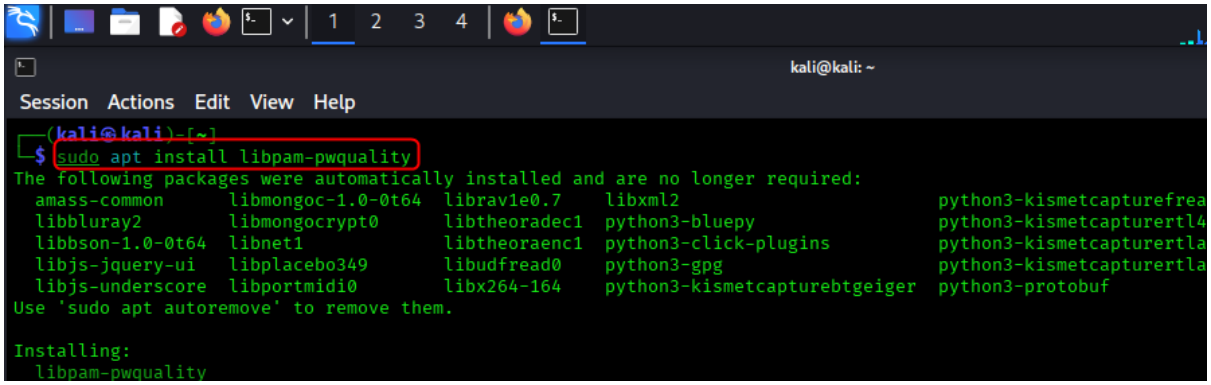

Realizaremos lo mismo, pero para que permita las conexiones salientes, esto se hace con el comando (sudo ufw default allow outgoing).



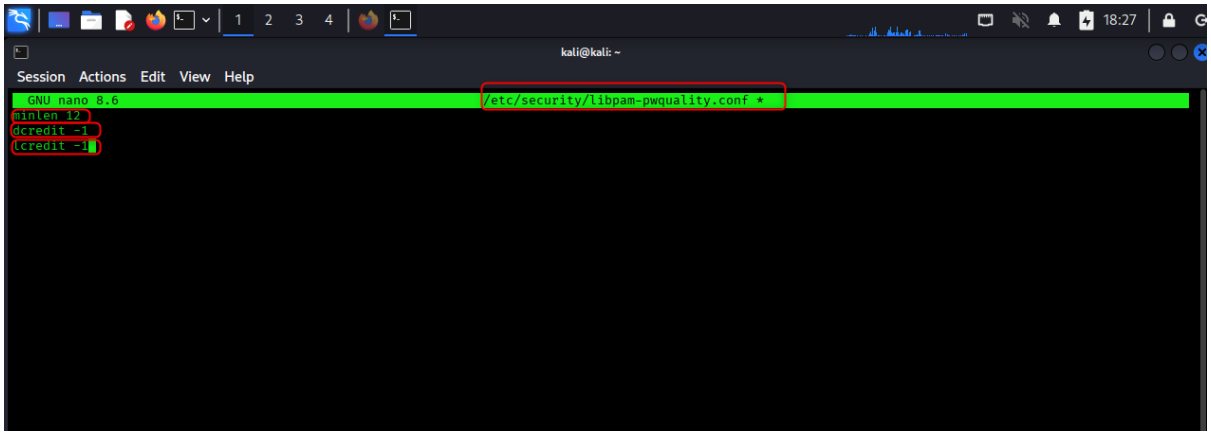
# 2. Seguridad de usuarios y contraseñas

## 1.1. Políticas de contraseñas

Para este punto instalaremos con (sudo apt install libpam_pwquality) para crear la política de contraseñas.



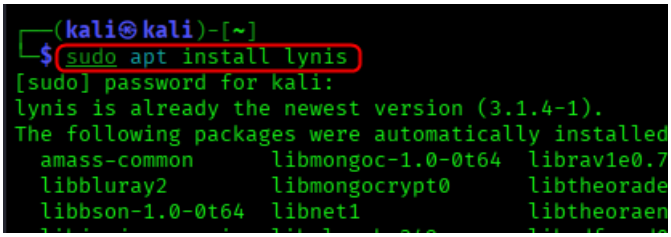

Tendremos que ajustar los criterios para establecer la complejidad de las contraseñas editaremos el fichero con (sudo nano /etc/security/libpam-pwquality.conf) y añadiríamos tres líneas (minlen 12) que sería el mínimo de caracteres que debe tener la contraseña, (dcredit –1) requiere al menos un numero en la contraseña y (lcredit –1) debe tener al menos 1 minúscula.



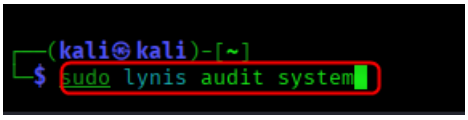
# 3. Validación y auditoria

## 3.1. Uso de herramientas de auditoría

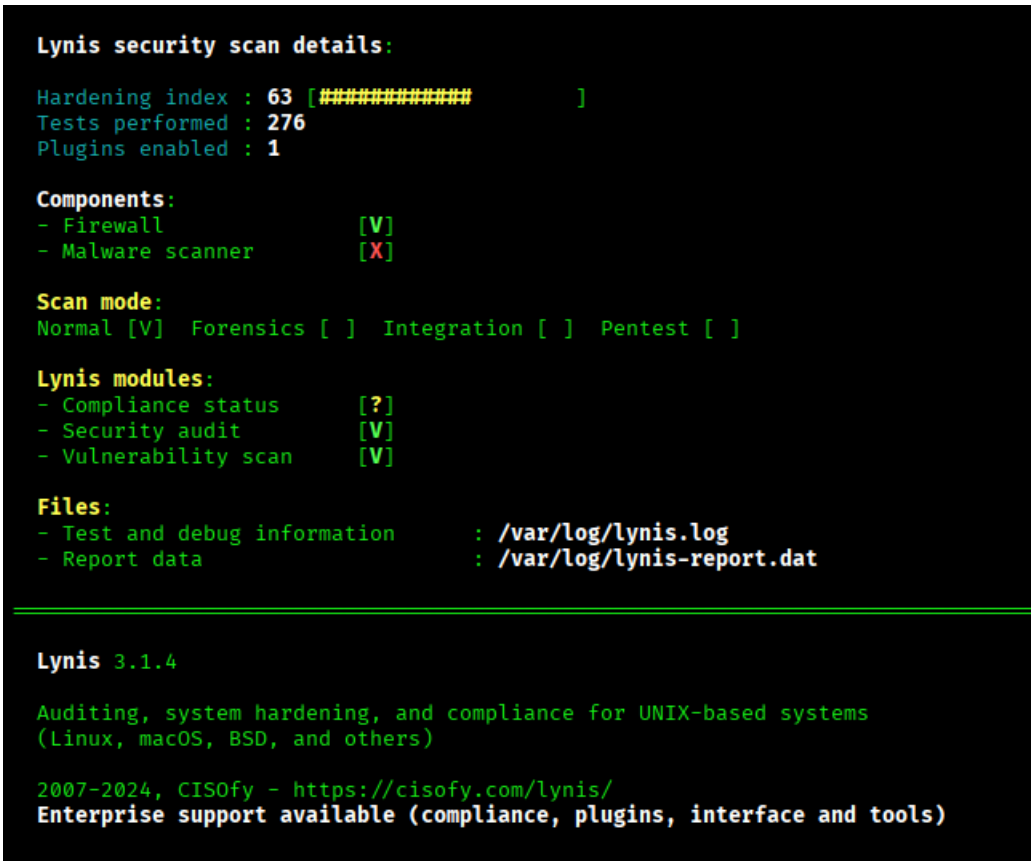
Instalaremos la herramienta de auditoria Lynis con (sudo apt intall lynis).




Ejecutaremos la herramienta con el comando (sudo lynis audit system).

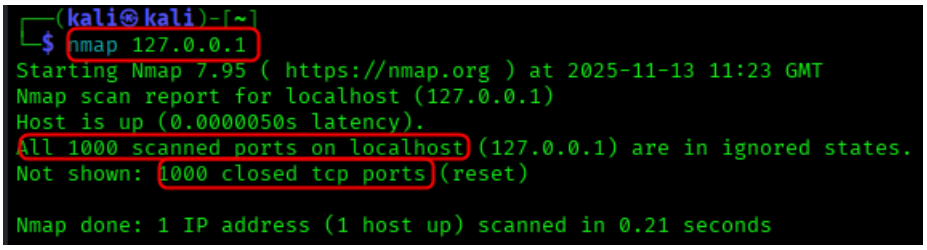


Tras ejecutar este comando nos realizará una auditoria y nos dará los resultados. Nos da un 63 de hardening index es decir una puntuación media y nos recomienda: Configurar políticas más estrictas de contraseñas y permisos, activar un antivirus o escáner de malware, fortalecer el firewall y asegurar servicios de red innecesarios.



## 3.2. Verificación mediante escaneo

Aquí mostramos el escaneo localhost realizado con nmap se ha realizado con el comando (nmap 127.0.0.1) nos dice que nmap ha escaneado 1000 puertos, pero no ha encontrado ninguno abierto.



Universidad Francisco de Vitoria
*Centro de Documentación Europea*
UFV Madrid

RAMIREZ LOPEZ HECTOR - 53858461M

Firmado digitalmente por RAMIREZ LOPEZ HECTOR - 53858461M
Fecha: 2025.11.13 12:36:25 +01'00'