

Checklist.

Área de Seguridad	Punto de Verificación
Autenticación y Contraseñas	Las contraseñas de usuario cumplen con los requisitos de complejidad del sistema.
Actualizaciones y Parches	seguridad.
Actualización del Kernel	parches de seguridad.
Servicios del Sistema	ejecución.
Firewall (UFW)	conexiones entrantes no solicitadas.
Permisos de Archivos	Los permisos de archivos y directorios críticos del sistema son restrictivos y correctos.
Auditoría y Monitoreo	del sistema.
Software Antimalware	actualizadas.
Acceso Remoto (SSH)	públicas).

Observación / Comando de Verificación
Revisar y configurar el archivo /etc/security/pwquality.conf. Se puede instalar con <code>sudo apt install libpam-pwquality</code> .
Ejecutar en la terminal: <code>sudo apt update && sudo apt full-upgrade</code> .
<code>upgrades</code> para automatizar.
<code>systemctl disable --now <servicio></code> .
<code>sudo ufw default deny incoming</code> .
Verificar con <code>ls -l /etc/shadow</code> y <code>ls -l /etc/sudoers</code> . Usar <code>sudo chmod</code> y <code>sudo chown</code> para corregir si es necesario.
Instalar con <code>sudo apt install auditd</code> . Revisar logs con <code>sudo ausearch -m USER_LOGIN -ts recent</code> .
Instalar: <code>sudo apt install clamav</code> . Actualizar firmas: <code>sudo freshclam</code> . Escanear directorio home: <code>sudo clamscan -r /home</code> .
<code>systemctl restart sshd</code> .