

293 - LINUX Y UBUNTU

Busca rootkits en Ubuntu con rkhunter y chkrootkit

Revisa tu propio equipo con dos herramientas gratuitas que detectan rootkits y cambios sospechosos en archivos del sistema.



NIVEL
Medio

TIEMPO
30 min

CATEGORÍA
Linux y Ubuntu

WEB
soporteinformatico360.com

Un rootkit es un programa malicioso que se esconde dentro del sistema. rkhunter y chkrootkit revisan tu Ubuntu en busca de señales típicas. Es una auditoría sencilla que puedes repetir cada cierto tiempo.

■ Qué necesitas

- ✓ Ubuntu en la última versión LTS
- ✓ Un usuario con permisos sudo
- ✓ Conexión a Internet
- ✓ El sistema recién actualizado

■ Paso a paso

01

Actualiza el sistema

Antes de nada, pon Ubuntu al día. Así evitas avisos por programas antiguos.

Terminal

```
$ sudo apt update
$ sudo apt upgrade -y
$
```

02

Instala las dos herramientas

Ambas están en los repositorios oficiales. Si durante la instalación aparece una pantalla de configuración de correo, elige «Sin configuración».

Terminal

```
$ sudo apt install rkhunter chkrootkit
$
```

03

Guarda la foto inicial

Con el sistema limpio y actualizado, rkhunter guarda cómo son tus archivos del sistema. Después compara contra esa foto.

Terminal

```
$ sudo rkhunter --propupd
$
```

04

Lanza la revisión de rkhunter

La opción --sk evita que te pida pulsar Intro en cada bloque. Al final verás un resumen con los avisos encontrados.

Terminal

```
$ sudo rkhunter --check --sk
$ sudo grep Warning /var/log/rkhunter.log
$
```

05

Pasa también chkrootkit

Ejecútalo y fíjate solo en las líneas que digan «INFECTED». Lo normal es que salga «not found» o «nothing found».

Terminal

```
$ sudo chkrootkit | grep INFECTED
$
```

06

Interpreta los avisos con calma

Muchos avisos son falsos positivos, por ejemplo tras actualizar paquetes. Busca el aviso concreto y, si el cambio lo hiciste tú, vuelve a ejecutar --propupd.



■ Consejos

CONSEJO 1

Ejecuta --propupd solo justo después de actualizar, nunca si sospechas que ya hay una infección.

CONSEJO 2

Repite la revisión una vez al mes o tras instalar software nuevo.

CONSEJO 3

Combina esta revisión con el cortafuegos activo y las actualizaciones automáticas.



Importante: Estas herramientas dan pistas, no certezas. Si confirmas una infección real, lo más seguro es copiar tus datos, reinstalar el sistema y cambiar tus contraseñas. Si no lo tienes claro, pide ayuda a un técnico.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar. soporte@soporteinformatico360.com
En taller, a domicilio en Madrid o por asistencia remota. soporteinformatico360.com

910 117 112