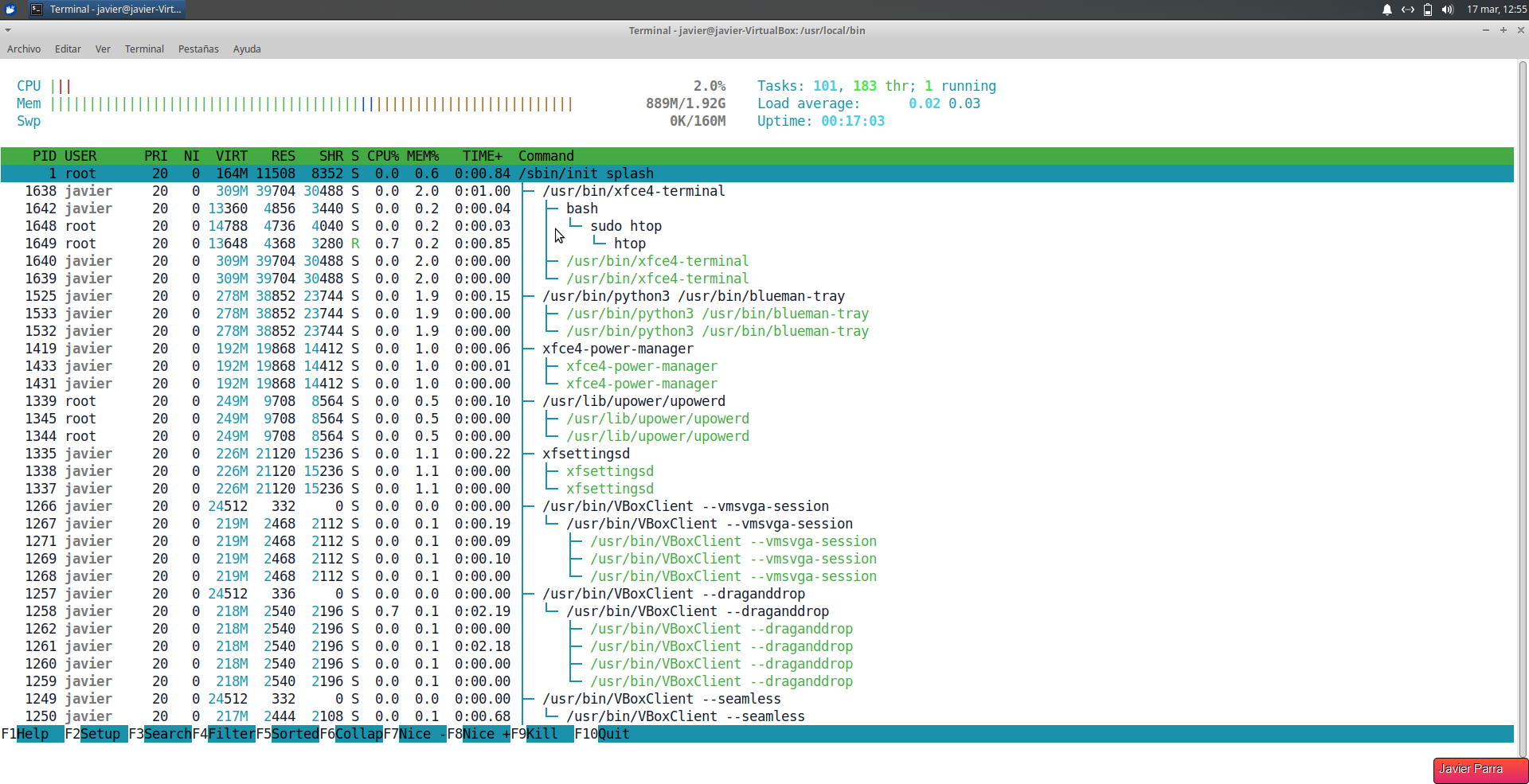
En la UD 07 hay un criterio de evaluación que dice lo siguiente: “**Se han tomado medidas de seguridad ante la aparición de procesos no identificados**”

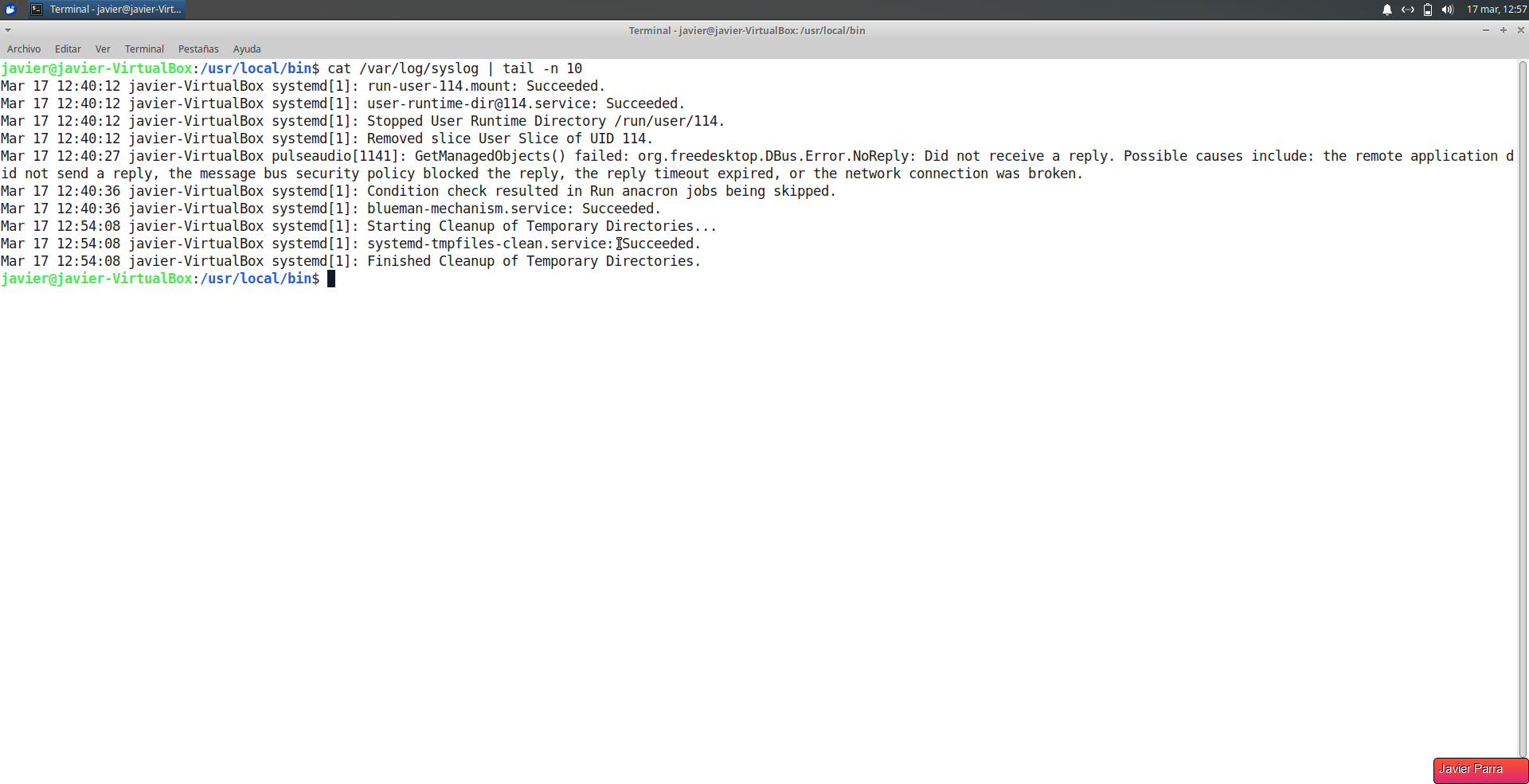
**¿Qué harías en tu servidor Linux?**

Ante la aparición de procesos no identificados es recomendable realizar las siguientes acciones:

1º Verificar la autenticidad de los procesos, utilizando herramientas como ps, top, htop o pstree, identificamos los procesos que están en ejecución en el sistema. De esta manera podremos identificar procesos que no reconozcamos o parezcan sospechosos.



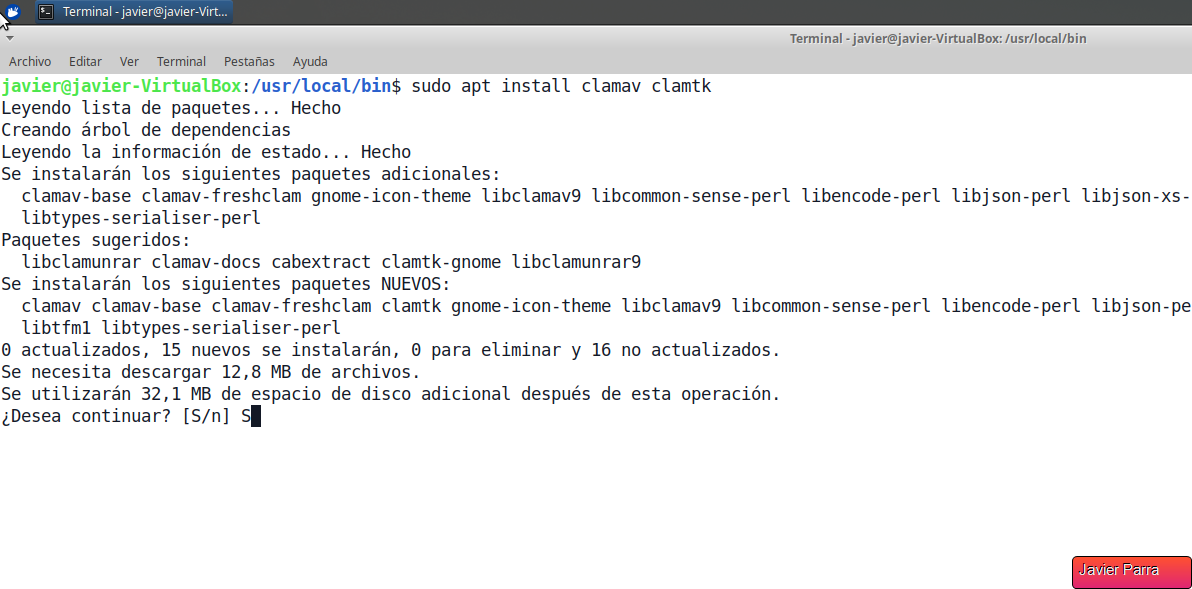
2º Realizar una investigación de la actividad del sistema, revisando los ficheros logs en las rutas /var/log/syslog, /var/log/auth.log o /var/log/messages, en busca de cualquier actividad que nos sea inusual. Estos logs nos pueden proporcionar pistas sobre que procesos se ejecutaron recientemente.



3º Realizar un análisis del sistema, utilizando herramientas de análisis de seguridad como rkhunter, chkrootkit o clamav para buscar signos de intrusiones de malware o rootkits escondidos en el sistema.

Podemos usar el antimalware clamav para analizar los procesos y ficheros del sistema.

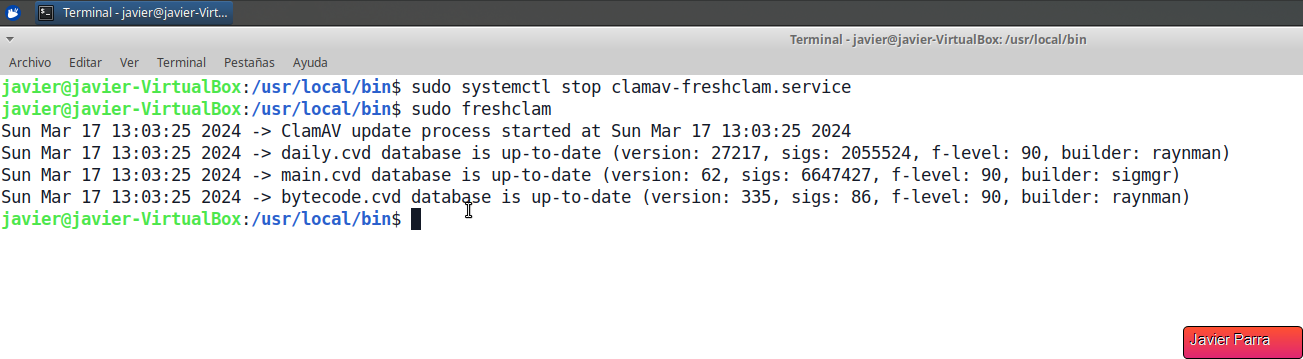
Instalamos clamav con su interfaz gráfica.



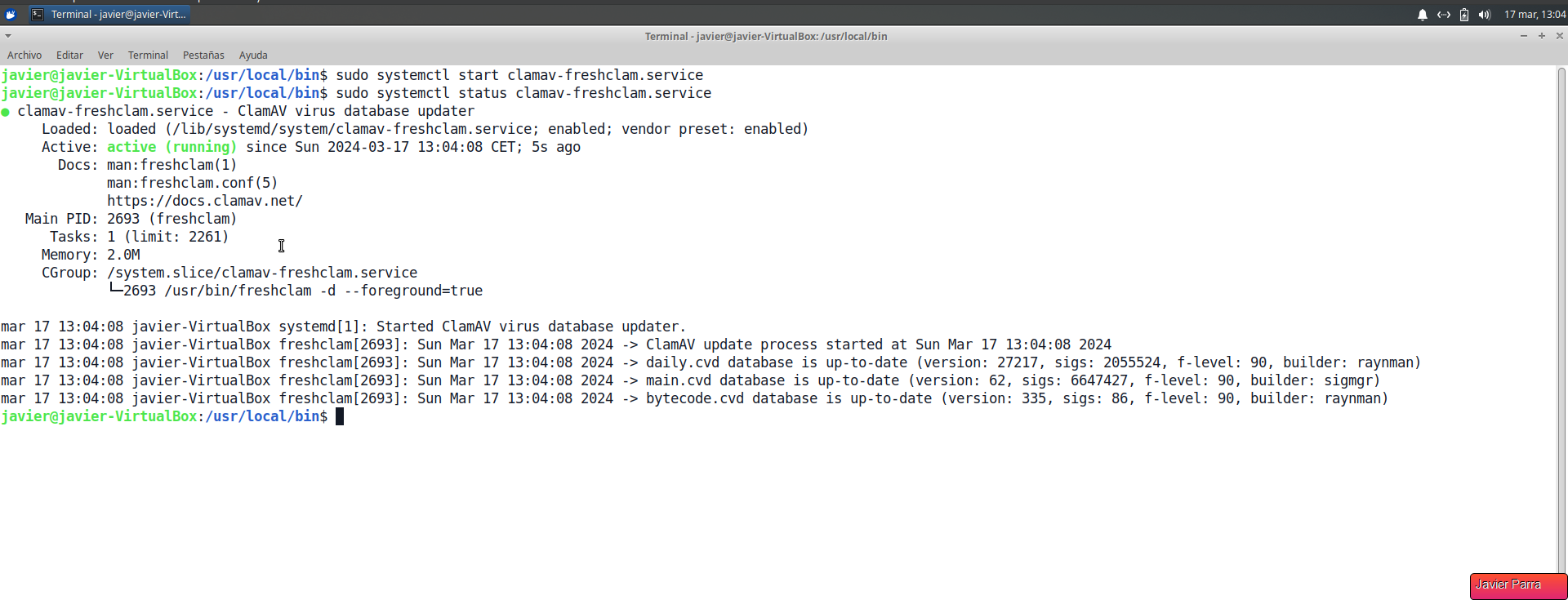
Paramos el servicio de clamav y actualizamos la base de datos de virus.

$ sudo systemctl stop clamav-freshclam.service

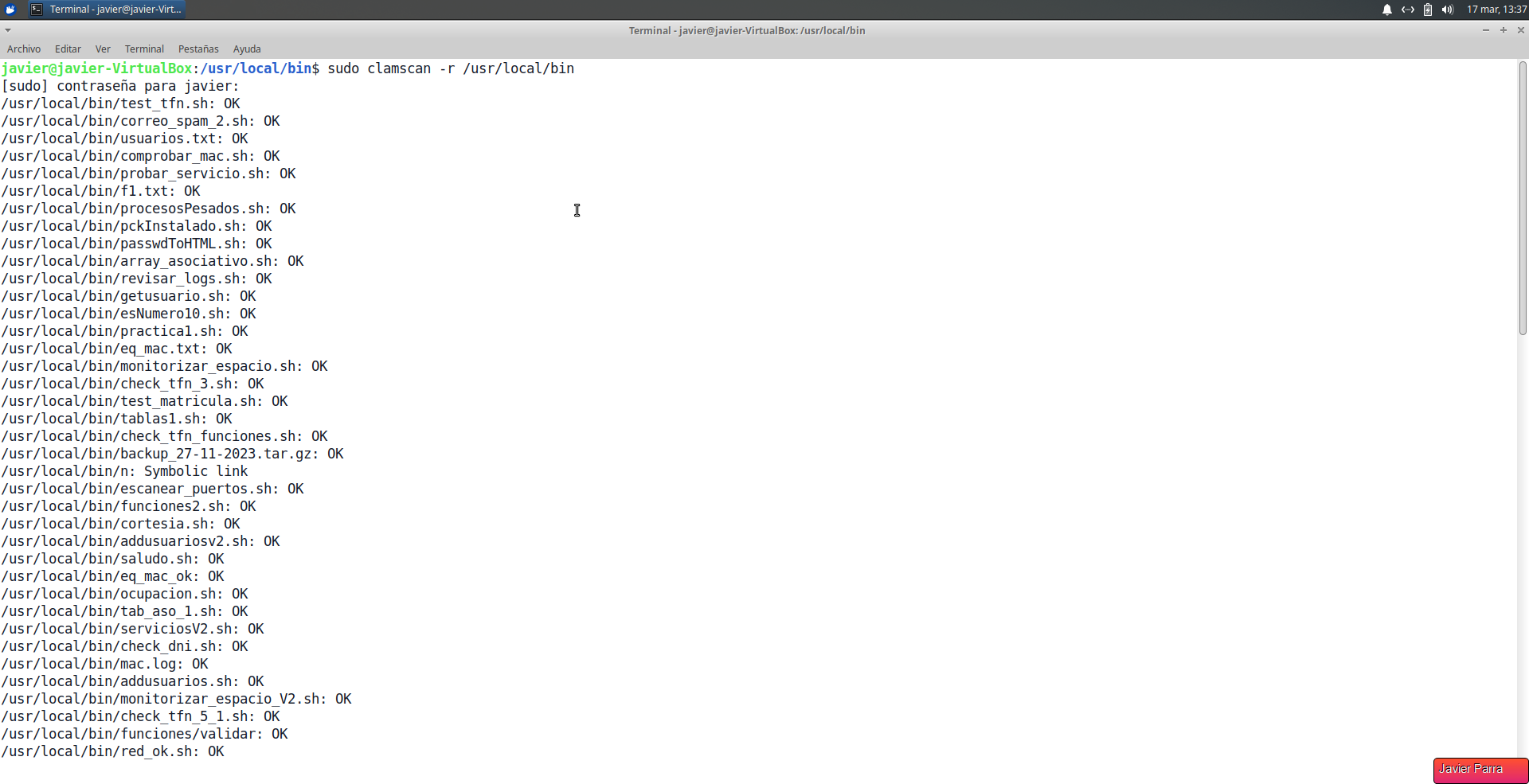
$ sudo freshclam

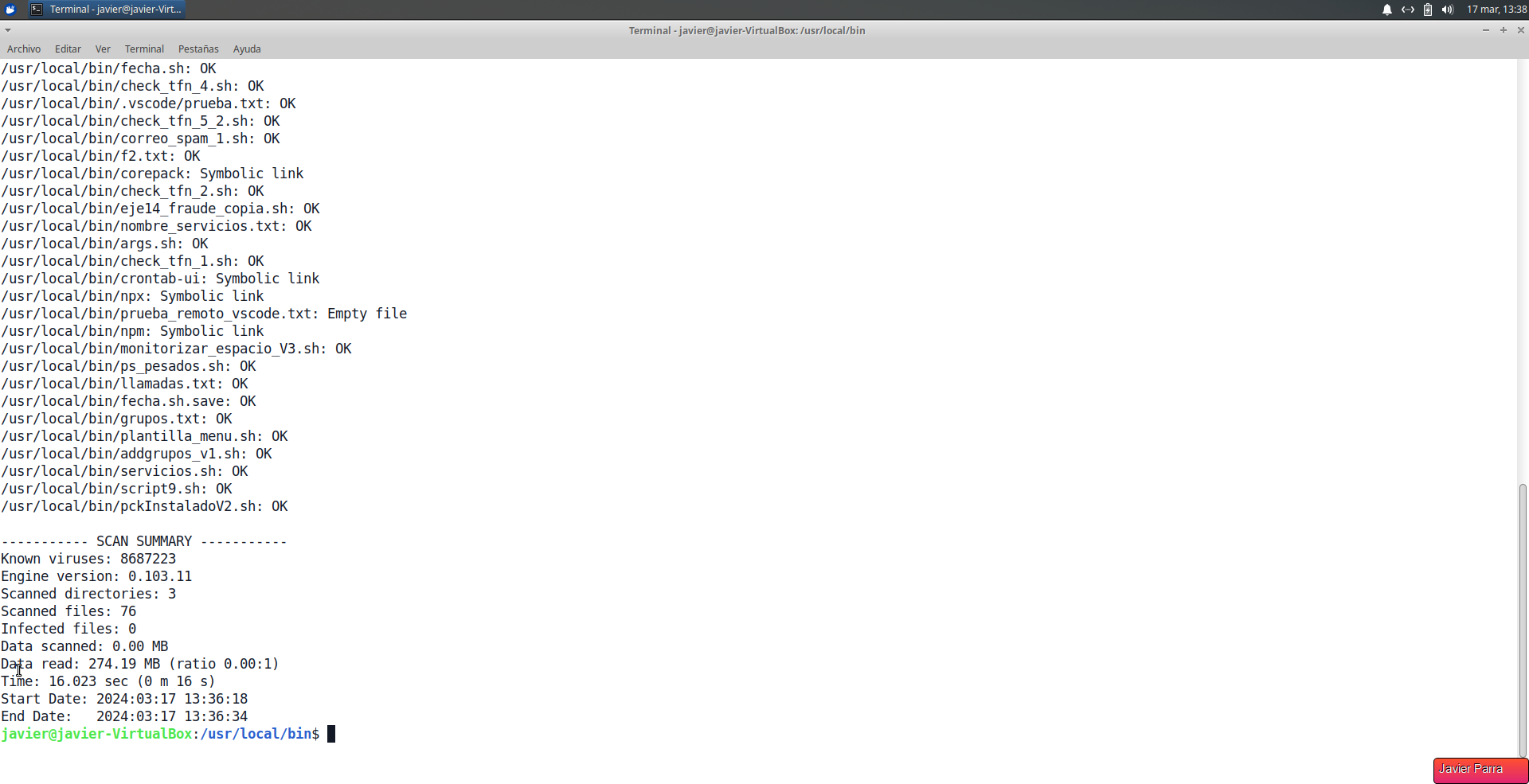


Volvemos a iniciar el servicio de ClamAV.

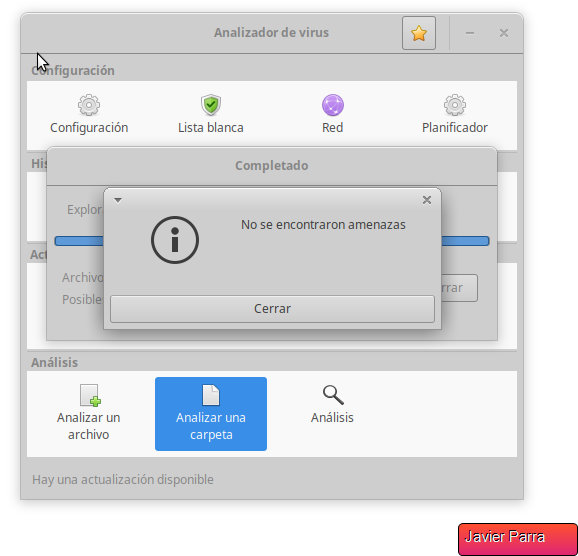


Analizamos un directorio en concreto para encontrar procesos o ficheros sospechosos.



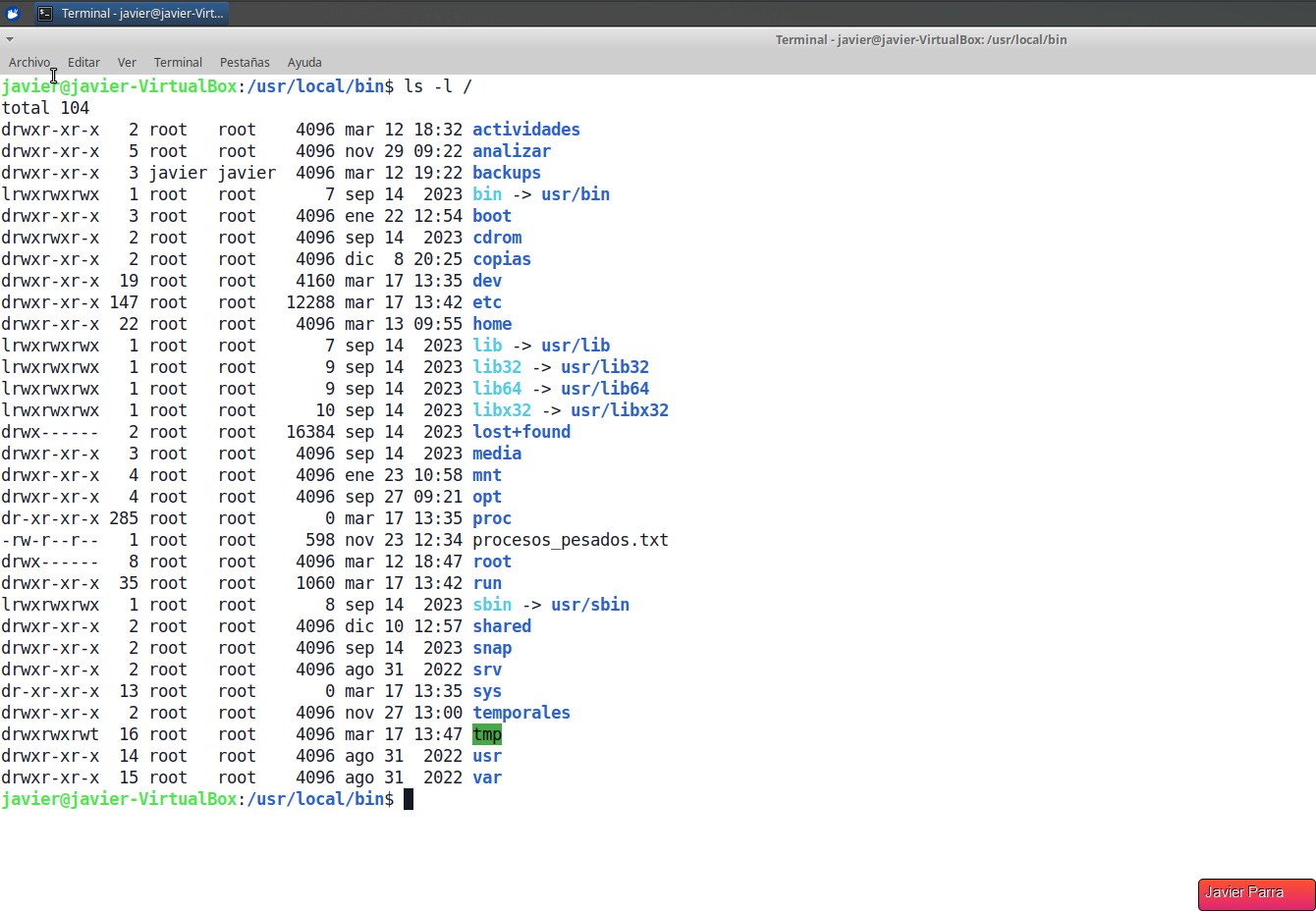


También podremos hacer uso de la interfaz gráfica ClamTK de ClamAV para analizar directorios.



4º Verificar la integridad del sistema, comprobando la integridad de los archivos que son críticos en el sistema, utilizando herramientas como tripwire, AIDE o ossec. Estas herramientas pueden detectar cambios no autorizados en archivos del sistema que pueden indicar una intrusión.

5º Revisar los permisos y accesos, verificando los permisos de los archivos y directorios más importantes del sistema, para asegurarse de que solo usuarios autorizados puedan acceder o modificarlos.



6º Realizar una actualización del sistema para parchear errores y vulnerabilidades de los que los que los ciberdelincuentes se puedan aprovechar utilizando diferentes exploits conocidos.

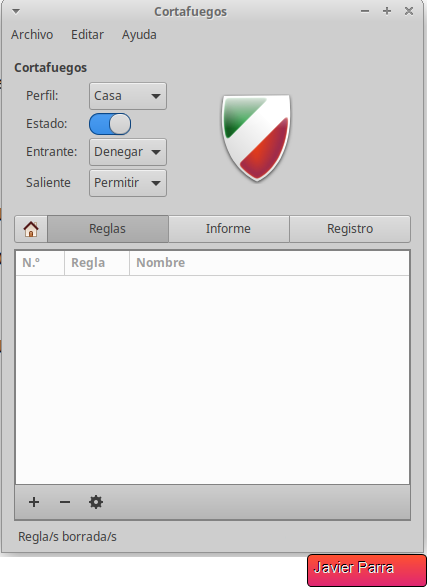


7º Aplicación de medidas de seguridad para la red, utilizando cortafuegos para realizar un filtrado de paquetes, utilizar sistemas de identificación de intrusos (IDS) o sistemas para la prevención de intrusiones basados en firmas (IPS).

Nos podemos instalar un cortafuegos, para crear reglas y protegernos ante conexiones maliciosas que provoquen la entrada de procesos sospechosos.

$ sudo apt install gufw





Podemos crear una regla, por ejemplo voy a crear una para no permitir el acceso mediante HTTP, para conexiones no seguras.

