CICLO FORMATIVO DE GRADO SUPERIOR - TÉCNICO ENADMINISTRACIÓNDESISTEMASINFORMÁTICOSENR EDES

SEGURIDAD Y ALTA DISPONIBILIDAD

TEMA 4

Nombre y apellidos:
-Wuke Zhang

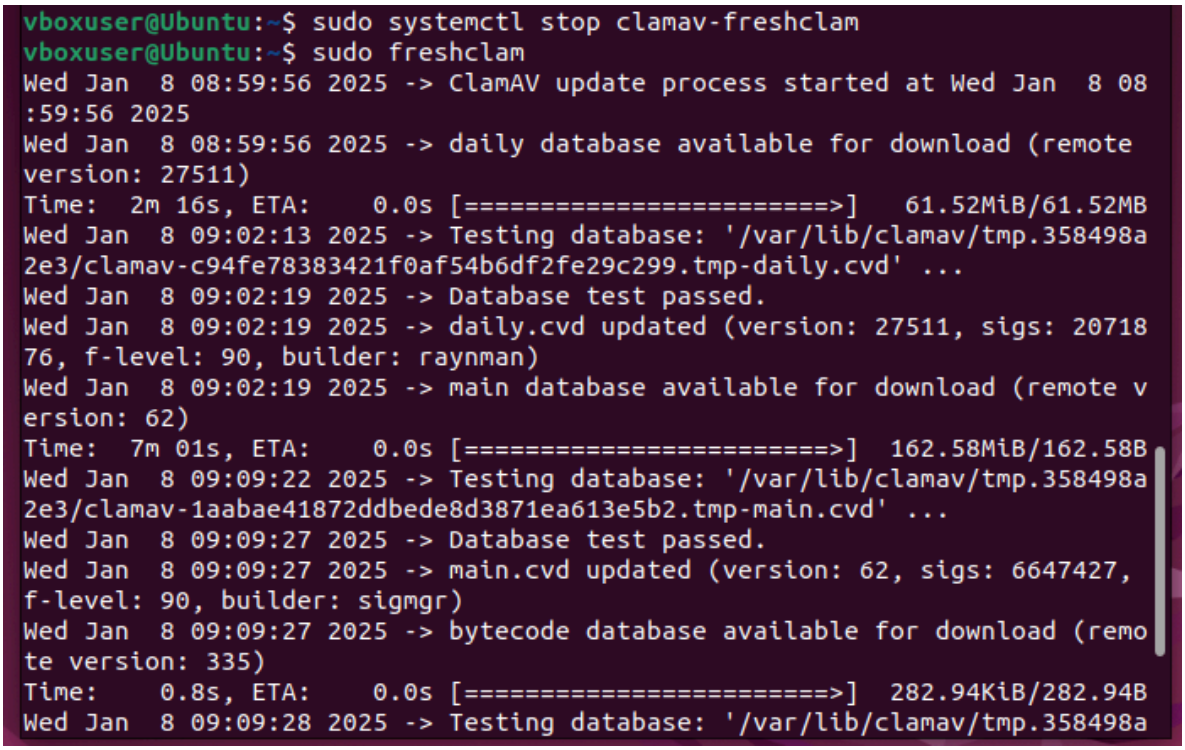
PRÁCTICA. Antivirus ClamAv en GNU/Linux

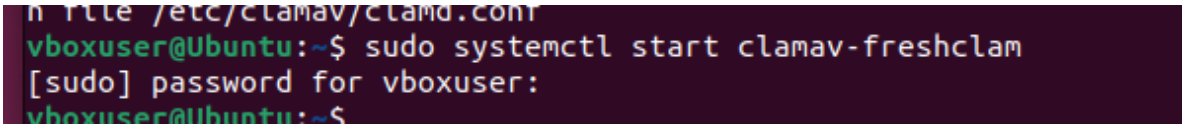
En esta actividad vamos a aprender a manejar el antivirus ClamAv para la búsqueda de virus en nuestro PC.

Añade capturas de pantalla de toda la ventana de la terminal en las preguntas en las que haya que ejecutar comandos. Se comprobará que el nombre del usuario sea el tuyo.

Responde a las siguientes preguntas:

1. Actualiza la base de datos de ClamAv





2. Realiza un análisis con ClamAv de todos los archivos del sistema con las siguientes características:
    a. Incluyendo todos los archivos que se encuentran dentro del directorio.
    b. Excluyendo las líneas de todos los archivos que están ok.
    sudo clamscan -r --quiet /
3. Analiza con ClamAVel directorio /home:
    a. Incluyendo todos los archivos.
    b. Mostrando la lista de infecciones.
    c. Solicitando un reporte completo en un archivo de texto llamado “análisis.txt”

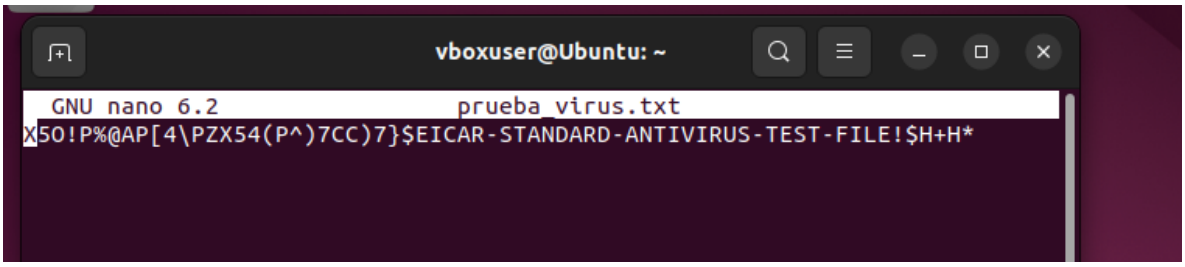
```
vboxuser@Ubuntu:~$ sudo clamscan -r /home --infected --log=analisis.txt

----------- SCAN SUMMARY -----------
Known viruses: 8703381
Engine version: 0.103.12
Scanned directories: 368
Scanned files: 419
Infected files: 0
Data scanned: 5.61 MB
Data read: 16.21 MB (ratio 0.35:1)
Time: 24.606 sec (0 m 24 s)
Start Date: 2025:01:08 09:24:02
End Date:   2025:01:08 09:24:26
vboxuser@Ubuntu:~$ cat analisis.txt
cat: analisis.txt: Permission denied
vboxuser@Ubuntu:~$ sudo cat analisis.txt
```

4. Crea desde el terminal un archivo llamado prueba_virus.txt.

   Añade con un editor de texto (por ejemplo, nano) la línea que aparece en la siguiente página: https://secure.eicar.org/eicar.com.txt

```
vboxuser@Ubuntu:~$ touch prueba_virus.txt
vboxuser@Ubuntu:~$ nano prueba_virus.txt
vboxuser@Ubuntu:~$
```



5. Realiza un análisis del fichero creado en el apartado 4:
   a. Incluyendo todos los parámetros vistos.
   b. Añade el pitido para que suene en caso de que detecte un virus.

```
vboxuser@Ubuntu:~$ clamscan prueba_virus.txt --bell
/home/vboxuser/prueba_virus.txt: Eicar-Signature FOUND

----------- SCAN SUMMARY -----------
Known viruses: 8703381
Engine version: 0.103.12
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 16.441 sec (0 m 16 s)
Start Date: 2025:01:08 09:29:40
End Date:   2025:01:08 09:29:57
```

¿Ha detectado un virus en el archivo?

Sí 1.

6. Realiza un análisis del mismo fichero anterior, pero incluye un parámetro para que elimine la infección automáticamente. Comprueba que el archivo se ha borrado.

```
vboxuser@Ubuntu:~$ clamscan prueba_virus.txt --remove
/home/vboxuser/prueba_virus.txt: Eicar-Signature FOUND
/home/vboxuser/prueba_virus.txt: Removed.

----------- SCAN SUMMARY -----------
Known viruses: 8703381
Engine version: 0.103.12
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 17.083 sec (0 m 17 s)
Start Date: 2025:01:08 09:36:48
End Date:   2025:01:08 09:37:05
vboxuser@Ubuntu:~$ ls -l prueba_virus.txt
ls: cannot access 'prueba_virus.txt': No such file or directory
```

Envía el documento en formato **.pdf** con el nombre '**Actividad4.1. NombreyApellidos**'.