

CICLO FORMATIVO DE GRADO SUPERIOR - TÉCNICO  
EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED  
ES

**SEGURIDAD Y ALTA DISPONIBILIDAD**

TEMA 4



**Nombre y apellidos:**  
**- Diego Pastrana Monzón**

**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

```
diego@neon:~$ sudo freshclam
[sudo] contraseña para diego:
ClamAV update process started at Wed Jan  8 08:58:02 2025
Wed Jan  8 08:58:03 2025 -> daily database available for update (local version: 27491, remote version: 27511)
Current database is 20 versions behind.
Downloading database patch # 27492...
Time: 0.65s, ETA: 0.0s [=====] 5.16KiB/5.16KiB
Downloading database patch # 27493...
Time: 0.35s, ETA: 0.0s [=====] 8.29KiB/8.29KiB
Downloading database patch # 27494...
Time: 0.35s, ETA: 0.0s [=====] 24.59KiB/24.59KiB
Downloading database patch # 27495...
Time: 0.25s, ETA: 0.0s [=====] 3.47KiB/3.47KiB
Downloading database patch # 27496...
Time: 0.35s, ETA: 0.0s [=====] 10.41KiB/10.41KiB
Downloading database patch # 27497...
Time: 0.25s, ETA: 0.0s [=====] 7.38KiB/7.38KiB
Downloading database patch # 27498...
Time: 0.25s, ETA: 0.0s [=====] 9.89KiB/9.89KiB
Downloading database patch # 27499...
Time: 0.25s, ETA: 0.0s [=====] 5.57KiB/5.57KiB
Downloading database patch # 27500...
Time: 0.25s, ETA: 0.0s [=====] 6.34KiB/6.34KiB
Downloading database patch # 27501...
Time: 0.25s, ETA: 0.0s [=====] 5.88KiB/5.88KiB
Downloading database patch # 27502...
Time: 0.25s, ETA: 0.0s [=====] 5.84KiB/5.84KiB
Downloading database patch # 27503...
Time: 0.25s, ETA: 0.0s [=====] 5.65KiB/5.65KiB
Downloading database patch # 27504...
Time: 0.25s, ETA: 0.0s [=====] 780B/780B
Downloading database patch # 27505...
Time: 0.25s, ETA: 0.0s [=====] 1.78KiB/1.78KiB
Downloading database patch # 27506...
Time: 0.25s, ETA: 0.0s [=====] 1.43KiB/1.43KiB
Downloading database patch # 27507...
Time: 0.25s, ETA: 0.0s [=====] 2.36KiB/2.36KiB
Downloading database patch # 27508...
Time: 0.35s, ETA: 0.0s [=====] 3.47KiB/3.47KiB
Downloading database patch # 27509...
Time: 0.25s, ETA: 0.0s [=====] 1.19KiB/1.19KiB
Downloading database patch # 27510...
Time: 0.25s, ETA: 0.0s [=====] 3.61KiB/3.61KiB
Downloading database patch # 27511...
Time: 0.25s, ETA: 0.0s [=====] 5.73KiB/5.73KiB
Testing database: /var/lib/clamav/tmp.3e1189ebid/clamav-c60diab4780ce9d50675a76272de3c5.tmp-daily.cld: ...
Database test passed.
Wed Jan  8 08:58:11 2025 -> daily.cld updated (version: 27511, sigs: 2071876, f-level: 90, builder: raynman)
Wed Jan  8 08:58:11 2025 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Wed Jan  8 08:58:11 2025 -> bytecode.cvd database is up-to-date (version: 335, sigs: 86, f-level: 90, builder: raynman)
ERROR: NotifyClamd: Can't find or parse configuration file /etc/clamav/clamd.conf
diego@neon:~$
```

### 2. Realiza un análisis con ClamAV de todos los archivos del sistema con las siguientes características:

- Incluyendo todos los archivos que se encuentran dentro del directorio.

```
diego@neon:~$ clamscan -r /
```

```
/var/cache/apt/archives/kde-style-breeze_4%3a6.2.5-0zneon+24.04+noble+release+build16_amd64.deb: OK
/var/cache/apt/archives/firefox_134.0~build1_amd64.deb: OK
/var/cache/apt/archives/libkipewire6_6.2.5-0zneon+24.04+noble+release+build12_amd64.deb: OK
/var/cache/apt/archives/gstreamer1.0-alsa_1.24.2-1ubuntu0.2_amd64.deb: OK
/var/cache/apt/archives/kf6-breeze-icon-theme_6.9.0-0zneon+24.04+noble+release+build9_amd64.deb: OK
/var/cache/apt/archives/kf6-kdnssd_6.9.0-0zneon+24.04+noble+release+build7_amd64.deb: OK
/var/cache/apt/archives/powerdevil_4%3a6.2.5-0zneon+24.04+noble+release+build18_amd64.deb: OK
/var/cache/apt/archives/kf6-kcrash_6.9.0-0zneon+24.04+noble+release+build7_amd64.deb: OK
/var/cache/apt/archives/libpam-kwallet5_4%3a6.2.5-0zneon+24.04+noble+release+build9_all.deb: OK
/var/cache/apt/archives/breeze5_4%3a6.2.5-0zneon+24.04+noble+release+build16_amd64.deb: OK
/var/cache/apt/archives/kf6-kactivities_6.2.5-0zneon+24.04+noble+release+build12_all.deb: OK
/var/cache/apt/archives/kf6-qqc2-desktop-style_6.9.0-0zneon+24.04+noble+release+build12_amd64.deb: OK
/var/cache/apt/archives/flatpak-kcm_6.2.5-0zneon+24.04+noble+release+build10_amd64.deb: OK
/var/cache/apt/archives/plasma-activities_6.2.5-0zneon+24.04+noble+release+build12_amd64.deb: OK
/var/cache/apt/archives/okular_4%3a24.12.0-0zneon+24.04+noble+release+build15_amd64.deb: OK
/var/cache/apt/archives/linux-tools-6.8.0-51-generic_6.8.0-51.52_amd64.deb: OK
/var/cache/apt/archives/kf6-kdoctools_6.9.0-0zneon+24.04+noble+release+build11_amd64.deb: OK
/var/cache/apt/archives/plymouth-theme-breeze_6.2.5-0zneon+24.04+noble+release+build12_amd64.deb: OK
/var/cache/apt/archives/libkf5waylandclient5_4%3a5.115.0+p24.04+vrelease+git20241227.2103-0_amd64.deb: OK
/var/cache/apt/archives/libcurl4t64_8.5.0-2ubuntu10.6_amd64.deb: OK
/var/cache/apt/archives/plasma-runners-addons_4%3a6.2.5-0zneon+24.04+noble+release+build18_amd64.deb: OK
/var/cache/apt/archives/plasma-firewall_6.2.5-0zneon+24.04+noble+release+build13_amd64.deb: OK
/var/cache/apt/archives/breeze-gtk-theme_6.2.5-0zneon+24.04+noble+release+build10_amd64.deb: OK
/var/cache/apt/archives/kf6-kirigami2_6.9.0-0zneon+24.04+noble+release+build13_all.deb: OK
/var/cache/apt/archives/partial: Can't open directory.
/var/cache/apt/archives/libnova-0.16-0t64_0.16-5.1build1_amd64.deb: OK
/var/cache/apt/archives/kf6-kcontacts_6.9.0-0zneon+24.04+noble+release+build6_amd64.deb: OK
/var/cache/apt/archives/libkf5coreaddons5_5.116.0-1zneon+24.04+noble+release+build4_amd64.deb: OK
/var/cache/apt/archives/kf6-ksvg_6.9.0-0zneon+24.04+noble+release+build7_amd64.deb: OK
/var/cache/apt/archives/kf6-kpeople_6.9.0-0zneon+24.04+noble+release+build7_amd64.deb: OK
/var/cache/apt/archives/linux-headers-generic_6.8.0-51.52_amd64.deb: OK
/var/cache/apt/archives/kf6-threadweaver_6.9.0-0zneon+24.04+noble+release+build8_amd64.deb: OK
```

- b. Excluyendo las líneas de todos los archivos que están ok.

```
diego@neon:~$ clamscan -ri /
```

### 3. Analiza con ClamAV el directorio /home:

- a. Incluyendo todos los archivos.

```
diego@neon:~$ clamscan -r
Loading: 5s, ETA: 0s [=====>] 8.70M/8.70M sigs
Compiling: 2s, ETA: 0s [=====>] 41/41 tasks

/home/diego/Capturas de pantalla/Captura de pantalla_20250102_041032.png: OK
/home/diego/Capturas de pantalla/Captura de pantalla_20250102_040417.png: OK
/home/diego/.stellarium/landscapes/azotea_stellarium/landscape.ini: OK
/home/diego/.stellarium/landscapes/azotea_stellarium/azotea.png: OK
/home/diego/.stellarium/landscapes/azotea_stellarium/Thumbs.db: OK
/home/diego/.stellarium/output.txt: Empty file
/home/diego/.stellarium/data/ssystem_minor.ini: OK
/home/diego/.stellarium/stars/default/starsConfig.json: OK
/home/diego/.stellarium/log.txt: OK
/home/diego/.stellarium/modules/Exoplanets/exoplanets.json: OK
/home/diego/.stellarium/modules/MeteorShowers/MeteorShowers.json: OK
/home/diego/.stellarium/modules/Satellites/tle14.txt: OK
/home/diego/.stellarium/modules/Satellites/tle19.txt: OK
/home/diego/.stellarium/modules/Satellites/tle33.txt: OK
/home/diego/.stellarium/modules/Satellites/tle45.txt: OK
/home/diego/.stellarium/modules/Satellites/tle38.txt: OK
/home/diego/.stellarium/modules/Satellites/tle28.txt: OK
/home/diego/.stellarium/modules/Satellites/tle40.txt: OK
/home/diego/.stellarium/modules/Satellites/tle17.txt: OK
/home/diego/.stellarium/modules/Satellites/tle42.txt: OK
/home/diego/.stellarium/modules/Satellites/tle31.txt: OK
/home/diego/.stellarium/modules/Satellites/tle37.txt: OK
```

- b. Mostrando la lista de infecciones.

```
diego@neon:~$ clamscan -i

----- SCAN SUMMARY -----
Known viruses: 8703665
Engine version: 1.0.7
Scanned directories: 1
Scanned files: 13
Infected files: 0
Data scanned: 0.31 MB
Data read: 0.15 MB (ratio 2.11:1)
Time: 7.347 sec (0 m 7 s)
Start Date: 2025:01:08 10:00:24
End Date: 2025:01:08 10:00:31
```

- c. Solicitando un reporte completo en un archivo de texto llamado "análisis.txt"

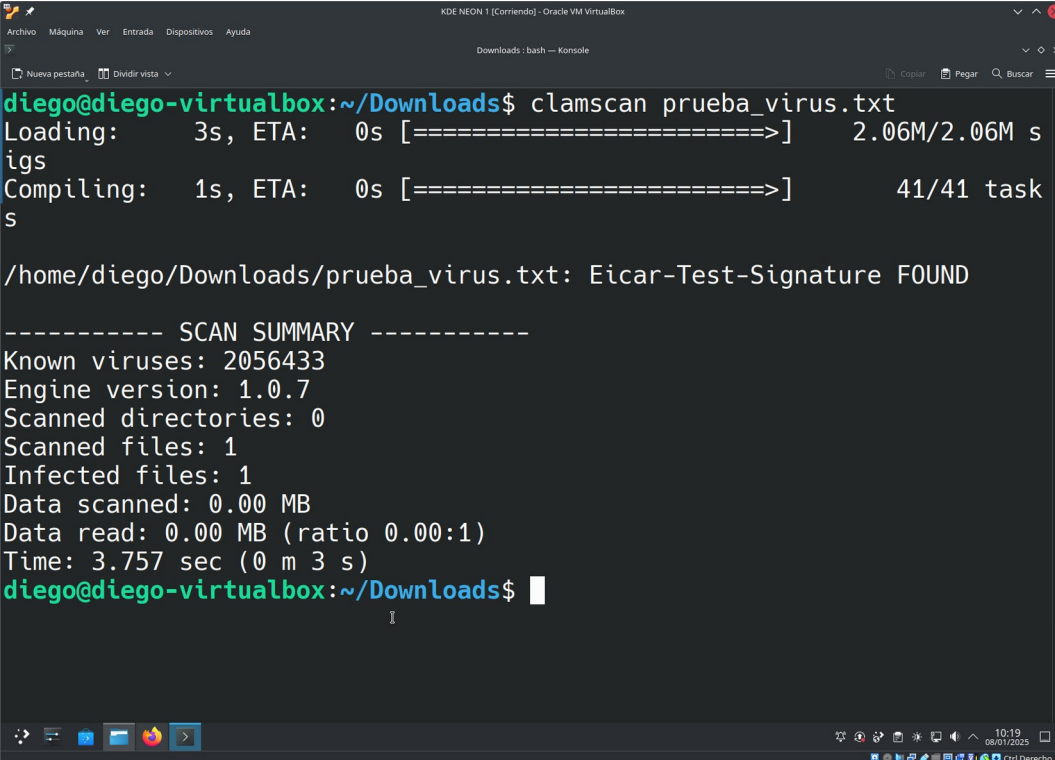
```
diego@neon:~$ clamscan > analisis.txt
diego@neon:~$ ls
analisis.txt                Orcaslicer
backup-neon.sh              Public
'Capturas de pantalla'    snap
curseforge.sh               Templates
Documents                   'Videocapturas de pantalla'
Downloads                   xampp.sh
'Fondos de pantalla'

diego@neon:~$ cat analisis.txt
/home/diego/analisis.txt: Empty file
/home/diego/xampp.sh: OK
/home/diego/.bashrc: OK
/home/diego/Orcaslicer: Symbolic link
/home/diego/.xsession-errors: OK
/home/diego/.gtk-bookmarks: OK
/home/diego/.gtkrc-2.0: OK
/home/diego/.sudo_as_admin_successful: Empty file
/home/diego/curseforge.sh: OK
/home/diego/.bash_history: OK
/home/diego/.profile: OK
/home/diego/backup-neon.sh: OK
/home/diego/.recently-used: OK
/home/diego/.bash_logout: OK
/home/diego/.nvidia-settings-rc: OK
/home/diego/.ImmersedConf: OK

----- SCAN SUMMARY -----
Known viruses: 8703665
Engine version: 1.0.7
Scanned directories: 1
Scanned files: 13
Infected files: 0
Data scanned: 0.31 MB
Data read: 0.15 MB (ratio 2.11:1)
Time: 6.811 sec (0 m 6 s)
Start Date: 2025:01:08 10:07:02
End Date: 2025:01:08 10:07:09
```



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>

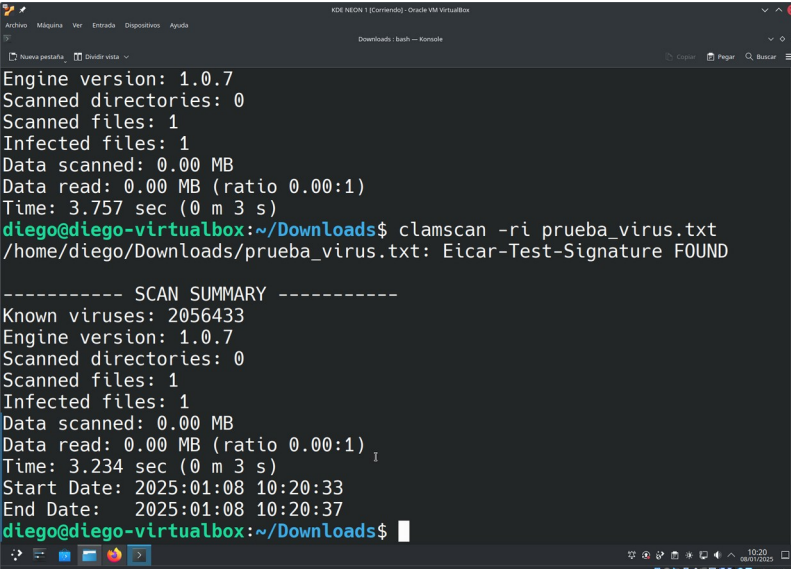


```
diego@diego-virtualbox:~/Downloads$ clamscan prueba_virus.txt
Loading:      3s, ETA:   0s [=====>]      2.06M/2.06M s
igs
Compiling:    1s, ETA:   0s [=====>]      41/41 task
s

/home/diego/Downloads/prueba_virus.txt: Eicar-Test-Signature FOUND

----- SCAN SUMMARY -----
Known viruses: 2056433
Engine version: 1.0.7
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 3.757 sec (0 m 3 s)
diego@diego-virtualbox:~/Downloads$
```

5. Realiza un análisis del fichero creado en el apartado 4:  
a. Incluyendo todos los parámetros vistos.



```
diego@diego-virtualbox:~/Downloads$ clamscan -ri prueba_virus.txt
/home/diego/Downloads/prueba_virus.txt: Eicar-Test-Signature FOUND

----- SCAN SUMMARY -----
Known viruses: 2056433
Engine version: 1.0.7
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 3.234 sec (0 m 3 s)
Start Date: 2025:01:08 10:20:33
End Date: 2025:01:08 10:20:37
diego@diego-virtualbox:~/Downloads$
```

- b. Añade el pitido para que suene en caso de que detecte un virus.

```
diego@diego-virtualbox:~/Downloads$ clamscan -ri --bell prueba_virus.txt
/home/diego/Downloads/prueba_virus.txt: Eicar-Test-Signature FOUND

----- SCAN SUMMARY -----
Known viruses: 2056433
Engine version: 1.0.7
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 3.256 sec (0 m 3 s)
Start Date: 2025:01:08 10:30:42
End Date: 2025:01:08 10:30:45
```

¿Ha detectado un virus en el archivo?

Si

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.

```
diego@diego-virtualbox:~/Downloads$ clamscan --remove prueba_virus.txt
Loading: 3s, ETA: 0s [=====>] 2.06M/2.06M sigs
Compiling: 1s, ETA: 0s [=====>] 41/41 tasks

/home/diego/Downloads/prueba_virus.txt: Eicar-Test-Signature FOUND
/home/diego/Downloads/prueba_virus.txt: Removed.

----- SCAN SUMMARY -----
Known viruses: 2056433
Engine version: 1.0.7
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 4.237 sec (0 m 4 s)
Start Date: 2025:01:08 10:42:30
End Date: 2025:01:08 10:42:34
diego@diego-virtualbox:~/Downloads$ ls
thunderbird.tmp xampp-linux-x64-8.2.12-0-installer.run
```