

Nombre de la práctica	ANTIVIRUS CLLAMAV			No.	7
Asignatura:	REDES DE COMPUTADORAS	Carrera:	INGENIERÍA EN SISTEMAS COMPUTACIONALES	Duración de la práctica (Hrs)	5 horas

NOMBRE DEL ALUMNO: Jesus Navarrete Martinez

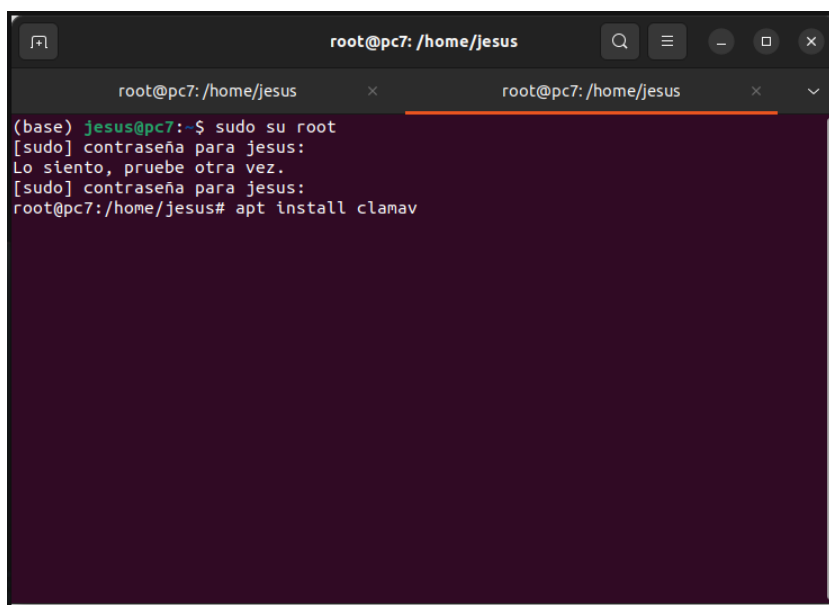
GRUPO: 3401

Encuadre con CACEI: Registra el (los) atributo(s) de egreso y los criterios de desempeño que se evaluarán en esta práctica.

No. atributo	Atributos de egreso del PE que impactan en la asignatura	Criterio de desempeño	Indicadores	
	El estudiante diseñará esquemas de trabajo y procesos, usando metodologías congruentes en la resolución de problemas de ingeniería en sistemas computacionales	CD1. IDENTIFICA METODOLOGÍAS Y PROCESOS EMPLEADOS EN LA RESOLUCIÓN DE PROBLEMAS	11	IDENTIFICACION Y RECONOCIMIENTO DE DISTINTAS METODOLOGÍAS PARA LA RESOLUCION DE PROBLEMAS
			12	MANEJO DE PROCESOS ESPECIFICOS EN LA SOLUCION DE PROBLEMAS Y/O DETECCION DE NECESIDADES
		CD2 DISEÑA SOLUCIONES A PROBLEMAS, EMPLEANDO METODOLOGÍAS APROPIADAS AL AREA	11	USO DE METODOLOGIAS PARA EL MODELADO DE LA SOLUCION DE SISTEMAS Y APLICACIONES
	El estudiante desarrolla proyectos y trabajos en equipo basándose en metodologías preestablecidas para lograr mayor calidad y eficiencia.	CD2. ASUME SU RESPONSABILIDAD EN EL DESARROLLO DE TRABAJOS Y/O PROYECTOS EN EQUIPO Y EN LA ENTREGA DE RESULTADOS	11	PARTICIPACIÓN ACTIVA EN EL DESARROLLO DE TRABAJOS Y PROYECTOS EN EQUIPO
			12	DIRIGIR Y ORGANIZAR TRABAJO EN EQUIPO
			13	PRESENTACION Y/O EXPOSICION DE TRABAJOS Y PROYECTOS EN EQUIPO

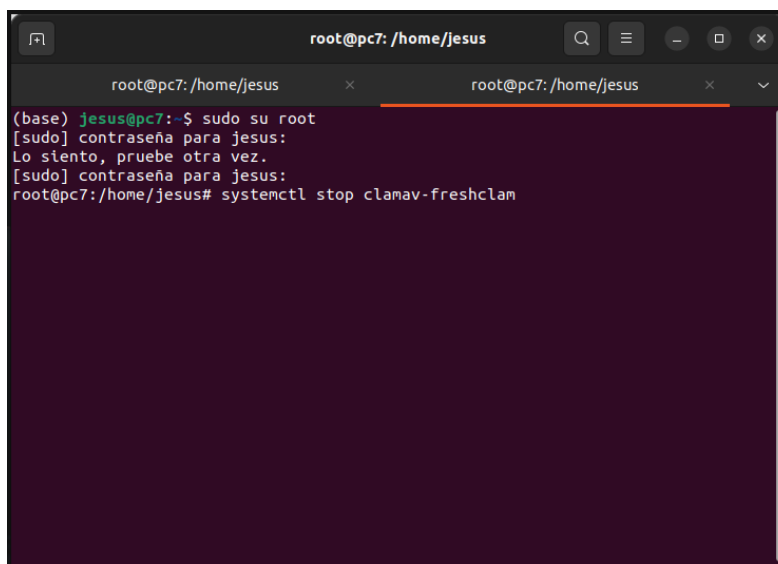
Instalación y uso de CLAMAV

1. Lo primero que vamos a realizar será la instalación del servicio de **clamav**, para ellos vamos a abrir nuestra terminal para posteriormente escribir **apt install clamav** al ejecutar este comando se iniciará de manera automática la descarga e instalación del servicio.



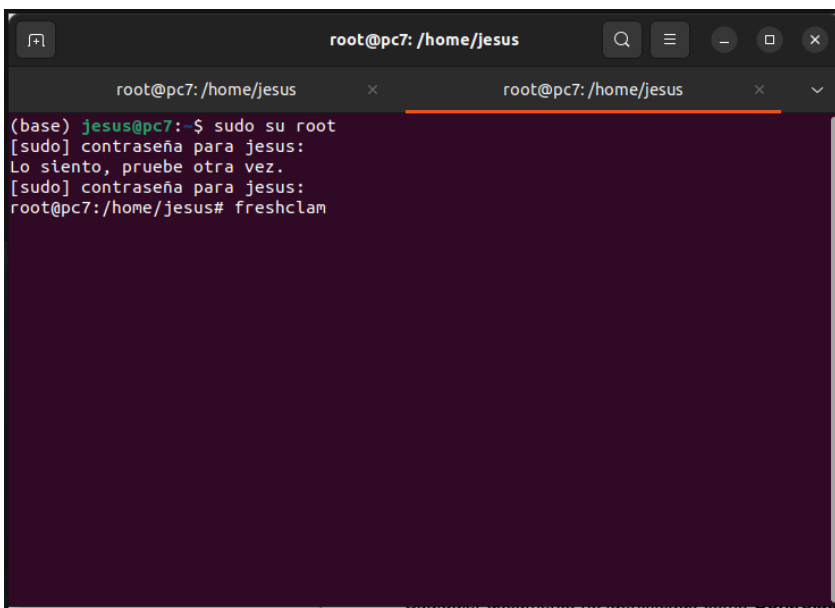
```
root@pc7: /home/jesus
(base) jesus@pc7:~$ sudo su root
[sudo] contraseña para jesus:
Lo siento, pruebe otra vez.
[sudo] contraseña para jesus:
root@pc7:/home/jesus# apt install clamav
```

2. Después de haber realizado la instalación debemos detener el servicio escribiendo en la terminal abierta anteriormente **systemctl stop clamav-freshclam**.



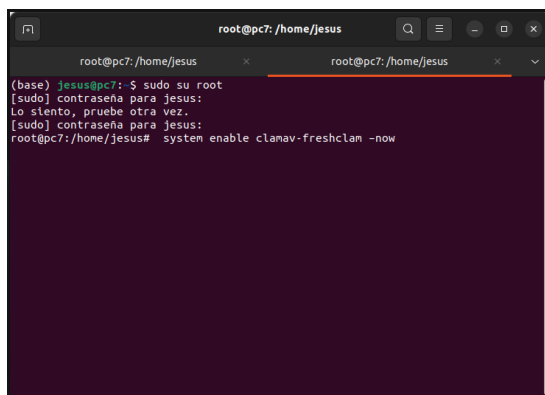
```
root@pc7: /home/jesus
(base) jesus@pc7:~$ sudo su root
[sudo] contraseña para jesus:
Lo siento, pruebe otra vez.
[sudo] contraseña para jesus:
root@pc7:/home/jesus# systemctl stop clamav-freshclam
```

3. Lo siguiente que debemos realizar es ejecutar la actualización de la base de datos de nuestro servicio clamav para ello escribiremos en la siguiente línea de la terminal **freshclam** al ejecutar este comando automaticamente se ira actualizando toda la base de datos para el correcto funcionamiento del servicio esto puede tardar algunos minutos.



```
root@pc7: /home/jesus
root@pc7: /home/jesus
(base) jesus@pc7:~$ sudo su root
[sudo] contraseña para jesus:
Lo siento, pruebe otra vez.
[sudo] contraseña para jesus:
root@pc7: /home/jesus# freshclam
```

4. Una vez que hemos realizado exitosamente la actualizacion de la base de datos de nuestro servicio , ahora debemos habilitarlo nuevamente ya que anteriormente lo habiamos detenido, para ello escribiremos en la terminal **system enable clamav-freshclam --now**.



```
root@pc7: /home/jesus
root@pc7: /home/jesus
(base) jesus@pc7:~$ sudo su root
[sudo] contraseña para jesus:
Lo siento, pruebe otra vez.
[sudo] contraseña para jesus:
root@pc7: /home/jesus# system enable clamav-freshclam --now
```

5. Ahora debemos corroborar que nuestro servicio ya esta corriendo correctamente para ello debemos escribir el siguiente comando **systemctl status clamav-freshclam**.

```
root@pc7: /home/jesus
root@pc7: /home/jesus
(base) jesus@pc7:~$ sudo su root
[sudo] contraseña para jesus:
Lo siento, pruebe otra vez.
[sudo] contraseña para jesus:
root@pc7: /home/jesus# systemctl status clamav-freshclam
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; ven
   Active: active (running) since Thu 2024-10-10 05:14:14 CST; 7h ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://docs.clamav.net/
   Main PID: 2417 (freshclam)
     Tasks: 1 (limit: 18684)
    Memory: 207.3M
       CPU: 4.473s
    CGroup: /system.slice/clamav-freshclam.service
            └─2417 /usr/bin/freshclam -d --foreground=true

oct 10 05:14:14 pc7 systemd[1]: Started ClamAV virus database updater.
oct 10 05:14:14 pc7 freshclam[2417]: Thu Oct 10 05:14:14 2024 -> ClamAV update
oct 10 05:14:14 pc7 freshclam[2417]: Thu Oct 10 05:14:14 2024 -> daily database
oct 10 05:14:22 pc7 freshclam[2417]: Thu Oct 10 05:14:22 2024 -> Testing databa
oct 10 05:14:25 pc7 freshclam[2417]: Thu Oct 10 05:14:25 2024 -> Database test
oct 10 05:14:25 pc7 freshclam[2417]: Thu Oct 10 05:14:25 2024 -> daily.cld upda
```

6. Una vez que ya hemos realizado todo lo anterior de manera exitosa, podemos continuar con el escaneo de una unidad de almacenamiento o una ruta en especifico de nuestra computadora, para ello escribiremos **clamscan -r /home** al realizar esto se ejecutara automáticamente el escaneo a la ruta o unidad de almacenamiento especificada después de / , esto puede demorar poco o bastante tiempo dependiendo de lo que nosotros como usuario deseamos escanear.

```
root@pc7: /home/jesus
root@pc7: /home/jesus
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; ven
   Active: active (running) since Thu 2024-10-10 05:14:14 CST; 7h ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://docs.clamav.net/
   Main PID: 2417 (freshclam)
     Tasks: 1 (limit: 18684)
    Memory: 207.3M
       CPU: 4.473s
    CGroup: /system.slice/clamav-freshclam.service
            └─2417 /usr/bin/freshclam -d --foreground=true

oct 10 05:14:14 pc7 systemd[1]: Started ClamAV virus database updater.
oct 10 05:14:14 pc7 freshclam[2417]: Thu Oct 10 05:14:14 2024 -> ClamAV update
oct 10 05:14:14 pc7 freshclam[2417]: Thu Oct 10 05:14:14 2024 -> daily database
oct 10 05:14:22 pc7 freshclam[2417]: Thu Oct 10 05:14:22 2024 -> Testing databa
oct 10 05:14:25 pc7 freshclam[2417]: Thu Oct 10 05:14:25 2024 -> Database test
oct 10 05:14:25 pc7 freshclam[2417]: Thu Oct 10 05:14:25 2024 -> daily.cld upda
oct 10 05:14:25 pc7 freshclam[2417]: Thu Oct 10 05:14:25 2024 -> main.cvd datab
oct 10 05:14:25 pc7 freshclam[2417]: Thu Oct 10 05:14:25 2024 -> bytecode.cvd d
oct 10 05:14:25 pc7 freshclam[2417]: Thu Oct 10 05:14:25 2024 -> !NotifyClamd:

root@pc7: /home/jesus# clamscan -r /home
```

Nota: Una vez que se haya completado el escaneo correctamente se mostrara el siguiente resumen sobre los resultados que nuestro servicio ha obtenido, debemos prestar especial atención hacia **Infected files** ya que este apartado nos indicara cuantos archivos infectados fueron encontrados.

```
root@pc7: /home/jesus

/home/jesus/nltk_data/corpora/stopwords/hungarian: OK
/home/jesus/nltk_data/corpora/stopwords/french: OK
/home/jesus/nltk_data/corpora/stopwords/nepali: OK
/home/jesus/nltk_data/corpora/stopwords/portuguese: OK
/home/jesus/nltk_data/corpora/stopwords/russian: OK
/home/jesus/nltk_data/corpora/stopwords/README: OK
/home/jesus/nltk_data/corpora/stopwords/norwegian: OK
/home/jesus/nltk_data/corpora/stopwords/azerbaijani: OK
/home/jesus/nltk_data/corpora/stopwords/turkish: OK
/home/jesus/nltk_data/corpora/stopwords/english: OK
/home/jesus/.bashrc.save: OK

----- SCAN SUMMARY -----
Known viruses: 8698711
Engine version: 0.103.12
Scanned directories: 56291
Scanned files: 652004
Infected files: 3802
Data scanned: 20817.86 MB
Data read: 17471.78 MB (ratio 1.19:1)
Time: 2977.798 sec (49 m 37 s)
Start Date: 2024:10:10 11:40:33
End Date: 2024:10:10 12:30:10
root@pc7: /home/jesus#
```

Conclusiones:

ClamAV se posiciona como una solución sólida y confiable para la detección y eliminación de malware en entornos Linux. Aunque las amenazas de virus en Linux son menos comunes que en otros sistemas operativos, es crucial contar con una herramienta eficiente que permita identificar vulnerabilidades y prevenir infecciones.

Su facilidad de instalación y capacidad de realizar análisis exhaustivos lo convierten en una herramienta práctica para cualquier usuario de Linux que desee reforzar la seguridad de su equipo. A través de esta práctica, quedó claro que ClamAV es una opción eficiente para mantener los sistemas limpios de malware sin comprometer el rendimiento, proporcionando tranquilidad y control sobre la seguridad de los archivos y dispositivos.