

Nombre de la práctica	PRACTICA ANTIVIRUS CLAMAV			No.	4
Asignatura:	REDES DE COMPUTADORAS	Carrera:	INGENIERÍA EN SISTEMAS COMPUTACIONALES	Duración de la práctica (Hrs)	5 horas

NOMBRE DEL ALUMNO: Vanesa Hernández Martínez

GRUPO: 3501

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	
A2	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	I1	IDENTIFICACION Y RECONOCIMIENTO DE DISTINTAS METODOLOGIAS PARA LA RESOLUCION DE PROBLEMAS
			I2	MANEJO DE PROCESOS ESPECIFICOS EN LA SOLUCION DE PROBLEMAS Y/O DETECCION DE NECESIDADES
		CD2 DISEÑA SOLUCIONES A PROBLEMAS, EMPLEANDO METODOLOGÍAS APROPIADAS AL AREA	I1	USO DE METODOLOGIAS PARA EL MODELADO DE LA SOLUCION DE SISTEMAS Y APLICACIONES
A7	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	I1	PARTICIPACIÓN ACTIVA EN EL DESARROLLO DE TRABAJOS Y PROYECTOS EN EQUIPO
			I2	DIRIGIR Y ORGANIZAR TRABAJO EN EQUIPO
			I3	PRESENTACION Y/O EXPOSICION DE TRABAJOS Y PROYECTOS EN EQUIPO

PRACTICA ANTIVIRUS CLAMAV

1. Lo primero que tenemos que hacer es instalar **Clamav**, para ello nos dirigimos a nuestra terminal en Linux y colocamos primero nos entramos con el usuario estándar, y una vez dentro colocamos el comando **apt install clamav**.

```
(base) vane@pc6:~$ sudo su root
[sudo] contraseña para vane:
root@pc6:/home/vane# apt install clamav
```

2. Después detenemos el clamav-freshclam, mediante el comando: **systemctl stop clamav-freshclam**

```
root@pc6:/home/vane# systemctl stop clamav-freshclam
```

3. Posteriormente actualizamos la base de datos del antivirus mediante el comando **freshclam**

```
root@pc6:/home/vane# freshclam
Wed Oct 9 16:45:10 2024 -> ClamAV update process started at Wed Oct 9 16:45:10 2024
Wed Oct 9 16:45:10 2024 -> daily database available for download (remote version: 27422)
Time: 4m 05s, ETA: 0.0s [=====] 61.20MiB/61.20MiB
Wed Oct 9 16:49:18 2024 -> Testing database: '/var/lib/clamav/tmp.b6807dfd56/clamav-1b1e5648b751710a4815a967daedb1db.tmp-d
Wed Oct 9 16:49:24 2024 -> Database test passed.
Wed Oct 9 16:49:24 2024 -> daily.cvd updated (version: 27422, sigs: 2067201, f-level: 90, builder: raynman)
Wed Oct 9 16:49:24 2024 -> main database available for download (remote version: 62)
Time: 15m 25s, ETA: 0.0s [=====] 162.58MiB/162.58MiB
Wed Oct 9 17:04:52 2024 -> Testing database: '/var/lib/clamav/tmp.b6807dfd56/clamav-7b4cf3d36539425e82370f81d638fc.tmp-m
Wed Oct 9 17:04:59 2024 -> Database test passed.
Wed Oct 9 17:04:59 2024 -> main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Wed Oct 9 17:04:59 2024 -> bytecode database available for download (remote version: 335)
Time: 1.9s, ETA: 0.0s [=====] 282.94KiB/282.94KiB
Wed Oct 9 17:05:01 2024 -> Testing database: '/var/lib/clamav/tmp.b6807dfd56/clamav-d1e4cb011d2eaa5fbf6ee22cc039bd59.tmp-b
Wed Oct 9 17:05:01 2024 -> Database test passed.
Wed Oct 9 17:05:01 2024 -> bytecode.cvd updated (version: 335, sigs: 86, f-level: 90, builder: raynman)
Wed Oct 9 17:05:01 2024 -> !NotifyClamd: Can't find or parse configuration file /etc/clamav/clamd.conf
```

4. Una vez que ya se actualizo la base de datos del antivirus, vamos a permitir que el servicio inicie nuevamente.

```
Executing: /lib/systemd/systemd-sysv-install enable clamav-freshclam
root@pc6:/home/vane#
```

5. Inicializamos el servicio de clamav con el siguiente comando: **systemctl status clamav-freshclam**

```
root@pc6:/home/vane# systemctl start clamav-freshclam
```

6. Posteriormente a la nacionalización del sistema debemos de comprobar que el estado del servicio este corriendo para ello utilizamos el comando: **systemctl start clamav-freshclam**

```
root@pc6: /home/vane

● 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 11:12:58 CST; 1h 13min ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://docs.clamav.net/
   Main PID: 1472 (freshclam)
     Tasks: 1 (limit: 38031)
    Memory: 207.2M
       CPU: 7.720s
    CGroup: /system.slice/clamav-freshclam.service
           └─1472 /usr/bin/freshclam -d --foreground=true

oct 10 11:12:58 pc6 freshclam[1472]: Thu Oct 10 11:12:58 2024 -> ClamAV update >
oct 10 11:12:58 pc6 freshclam[1472]: Thu Oct 10 11:12:58 2024 -> daily database>
oct 10 11:13:00 pc6 freshclam[1472]: Thu Oct 10 11:13:00 2024 -> Testing databa>
oct 10 11:13:05 pc6 systemd[1]: /lib/systemd/system/clamav-freshclam.service:11>
oct 10 11:13:07 pc6 freshclam[1472]: Thu Oct 10 11:13:07 2024 -> Database test >
oct 10 11:13:07 pc6 freshclam[1472]: Thu Oct 10 11:13:07 2024 -> daily.cld upda>
oct 10 11:13:07 pc6 freshclam[1472]: Thu Oct 10 11:13:07 2024 -> main.cvd datab>
oct 10 11:13:07 pc6 freshclam[1472]: Thu Oct 10 11:13:07 2024 -> bytecode.cvd d>
oct 10 11:13:07 pc6 freshclam[1472]: Thu Oct 10 11:13:07 2024 -> !NotifyClamd: >
oct 10 11:13:07 pc6 systemd[1]: /lib/systemd/system/clamav-freshclam.service:11>
lines 1-23
```

Una vez que el servicio esta corriendo correctamente terminamos el proceso de instalación comenzamos el proceso para el escaneo.

Escaneo de un directorio principal

6. Colocamos el siguiente comando en donde especificaremos la ruta del directorio principal que queremos escanear: **clamscan -r /directorioprincipal**

En nuestro caso escanearemos home, así que nuestro comando quedaría de la siguiente manera: **clamscan -r /home**

```
root@pc6: /home/vane
res/extra/tricky_list.text: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/gfm_links.html: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/footnotes.text: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/gfm_del.html: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/same_bullet.text: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/list_item_text.text: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/gfm_tables.html: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/gfm_tables_uneven.text: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/hetero_list.text: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/lazy_blockquotes.text: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/nested_square_link.html: OK
/home/vane/anaconda3/pkgs/mistune-0.8.4-py311h5eee18b_1000/info/test/tests/fixtures/extra/nested_square_link.text: OK
```

Resultados del escaneo

```
root@pc6: /home/vane
(base) vane@pc6:~$ sudo su root
[sudo] contraseña para vane:
root@pc6:/home/vane# clamscan -r media/vane/ADATA HD710 PRO
media/vane/ADATA: No such file or directory
WARNING: media/vane/ADATA: Can't access file
HD710: No such file or directory
WARNING: HD710: Can't access file
PRO: No such file or directory
WARNING: PRO: Can't access file

----- SCAN SUMMARY -----
Known viruses: 8698711
Engine version: 0.103.12
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 17.466 sec (0 m 17 s)
Start Date: 2024:10:10 12:43:16
End Date: 2024:10:10 12:43:34
root@pc6:/home/vane#
```

known viruses, va a identificar los virus conocidos

engine clamov, es el motor o la versión de clamov

scanned directories son los directorios escaneados

infected files, son los archivos infectados

data scanned son los datos escaneados

data read son los datos leídos

time scanned, es el tiempo de escaneo

start date, es el inicio de escaneo

end date es la finalización del escaneo

Conclusión

Al llevar a cabo un escaneo con ClamAV en Linux sobre un directorio principal, se puede concluir que esta herramienta proporciona una solución efectiva y de código abierto para la detección y eliminación de malware en sistemas basados en Linux. Durante el escaneo, ClamAV analiza de manera exhaustiva los archivos del directorio seleccionado, identificando posibles amenazas, como virus, troyanos o software malicioso.

El resultado del escaneo, mostrado en un resumen, incluye la cantidad de archivos analizados, el número de amenazas detectadas y, en caso de haberlas, el nombre del malware encontrado. Este resumen permite evaluar el estado de seguridad del directorio y tomar acciones correctivas como la eliminación o cuarentena de los archivos infectados.