**ANEXO V**

**Práctica 5: Uso de ClamAV como antivirus en Linux.**

**Informe**

* **Documentar las configuraciones aplicadas.**

Las configuraciones realizadas se encuentran en la parte procedimiento de la práctica.

* **Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados. Además, indicar el impacto en la seguridad.**

Los resultados obtenidos de la práctica con la debida explicación se muestran en la parte de resultados de la práctica. Y también el impacto que tiene en la seguridad de los dispositivos.

* **Configurar ClamAV con sistemas como SpamAssassin para escanear correos electrónicos.**

SpamAssassin es un filtro de spam que puede trabajar junto con ClamAV para analizar los archivos adjuntos de los correos electrónicos y detectar posibles amenazas de malware. Esta integración es especialmente útil en servidores de correo, ya que mejora la seguridad al combinar la detección de correo no deseado con la protección contra archivos maliciosos, reduciendo así el riesgo de infecciones.

De esta forma primero se instala SpamAssassin en el sistema con el comando sudo apt install spamassassin spamc -y. Se puede verificar versión con spamassassin –version.

Luego para que SpamAssassin trabaje junto a ClamAV es necesario editar ambos archivos de configuración y así tener la capacidad de analizar los archivos adjuntos en los correos electrónico. En consecuencia se edita SpamAssassin con el comando sudo nano /etc/mail/spamassassin/local.cf, y se configura de la siguiente forma.

A computer screen shot of a program

Description automatically generated

**Figura 5.24.** Configuración del archivo local.cf.

Por otra parte, con el comando sudo nano /etc/clamav/clamd.conf se configura ClamAV, para ellos se añade las siguientes líneas al final del archivo y se reinicia el servicio con sudo systemctl restart clamav-daemon.

A screenshot of a computer

Description automatically generated

**Figura 5.25.** Configuración del archivo clamd.conf

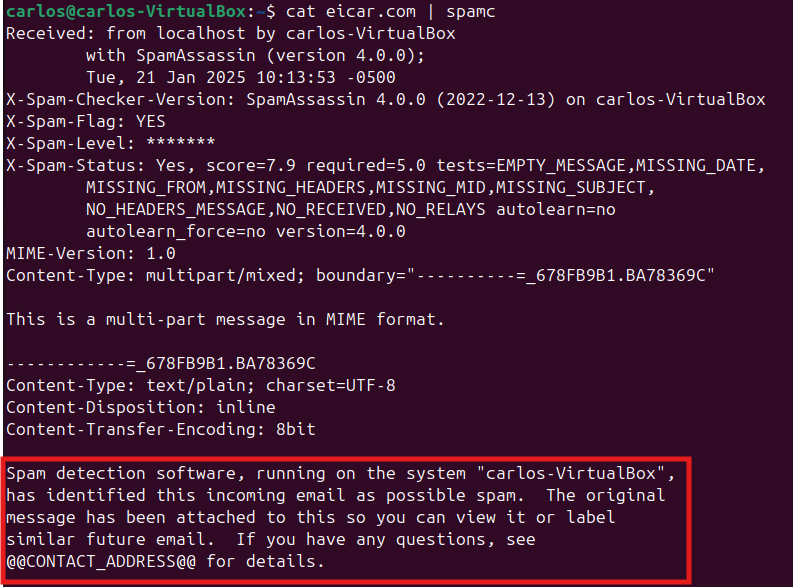
Luego para realizar el test correspondiente es necesario descarga un archivo de prueba EICAR (archivo inofensivo usado para probar antivirus). Esto se realiza con el comando wget -O eicar.com https://secure.eicar.org/eicar.com.txt

A computer screen shot of a computer code

Description automatically generated

**Figura 5.26.** Descarga del correo de prueba.

Una vez que se tiene el correo infectado de prueba se usa el siguiente comando cat eicar.com | spamc, para que ClamAV y SpamAssassin analicen los archivos que posee el correo, donde si ClamAV detecta el archivo como malicioso, SpamAssassin le asignará una puntuación alta y marcará el correo como spam.



**Figura 5.26.** Resultado de escanear el correo.

En consecuencia, la figura muestra que el archivo fue marcado como spam para ser revisado manualmente y bloquearlo si se necesario. Esto de como resultado una mejora en la seguridad de servidores de correo electrónico con sistema operativo Linux, dando una protección adecuada contra archivos peligrosos.