CICLO FORMATIVO DE GRADO SUPERIOR - TÉCNICO EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN REDES

Seguridad y Alta Disponibilidad

ClamAV. Guía de básica de uso.

Antivirus ClamAV:

Es un software antivirus open source (de licencia GPL) para las plataformas Windows, Linux y Otros sistemas operativos semejantes a Unix. El propósito principal de este software es la integración con los servidores de correo (escaneo de datos adjuntos). El paquete proporciona un servicio flexible y escalable, un analizador de línea de comandos y una utilidad para la actualización automática vía Internet. Los programas están basados en una librería distribuidacon el paquete Clam Antivirus, la cual puede ser usada por su propio software. Y lo más importante, la base de datos se mantiene actualizada constantemente.

Desarrollo y Estructura de ClamAV:

El objetivo primario de ClamAV es la consecución de un conjunto de herramientas que identifiquen y bloqueen el malware proveniente del correo electrónico. Uno de los puntos fundamentales en este tipo de software es la rápida localización e inclusión en la herramienta de los nuevos virus encontrados y escaneados. Esto se consigue gracias a la colaboración de losmiles de usuarios que usan ClamAV y a sitios como Virus Total.com que proporcionan los virusescaneados. Otra pieza clave de ClamAV es el soporte de desarrolladores que posee en todo el mundo, eta red de desarrolladores global, posibilita una rápida reacción ante cualquier evidencia de un nuevo virus.

Instalación:

Para instalar el software en distribuciones Linux, hay que ejecutar el siguiente comando:

- Sudo apt-get install clamav

Actualizar base de datos de antivirus:
1º Hay que detener el servicio de antivirus, de lo contrario no tendremos acceso a la base de datos de virus para actualizarla:
- Systemctl stop clamav-freshclam

2º Actualizamos la base de datos a través del comando:
- Freshclam

3º Hay que volver a iniciar el servicio de antivirus, ¡de que nos sirve un antivirus si no está en marcha!

Realizar una búsqueda de virus en el sistema:

Para realizar análisis de los directorios y ficheros del sistema, ClamAV incluye el comando “clamscan”, el cual permite:

- Escanear el directorio sobre el que se ejecuta. Ej:

  vboxuser@ASO:~/Desktop$ clamscan

- Escanear un directorio específico. Ej:

  vboxuser@ASO:~/Desktop$ clamscan /etc

- Escanear recursivamente

  vboxuser@ASO:~/Desktop$ clamscan -r

Gestión de los resultados de búsqueda

Por defecto, clamscan emite los resultados de la busqueda por la terminal en la que se ejecuta el comando. Sin embargo, podemos utilizar diferentes opciones del comando para añadir mayor utilidad a la herramienta.

- Guardar la información en archivos de log. Ej:

  vboxuser@ASO:/etc$ clamscan -r --log=/var/ReportClamAV/report.log (Guarda el informe en el archive report.log bajo el directorio /var/ReportClamAV).

*Recuerda crear los directorios si no existen previamente.

- Añadir señal sonora al terminar el proceso. Los procesos de escaneo recursivo suelen tardar bastante tiempo, por lo que se incluye la opción de hacer sonar un pitido al finalizar el escaneo. Ej:

  vboxuser@ASO:~/Desktop$ clamscan –bell

- Eliminar automáticamente los archivos infectados. Aunque por defecto lo ideal seria poder aislar y someter a inspección los archivos infectados por virus, en caso de no disponer de tiempo o carecer de los conocimientos necesarios es posible habilitar la herramienta para que elimine automáticamente los virus. Ej:

  vboxuser@ASO:~/Desktop$ clamscan –remove

Extras:

- Para realizar pruebas con el antivirus, puedes crear falsos archivos infectados insertando la siguiente línea:

  X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

- También dispones de una herramienta gráfica llamada *clamtk* que puedes instalar como un paruqte normal:

  apt-get install clamtk