Juan Manuel Rodríguez Gómez **1º Curso DGIIM** **Fundamentos del Software**

Catástrofes con uso de comandos en Linux

- **rm -rf /**

Este comando que se utiliza para **borrar archivos o directorios en Linux**. Siempre hay que tener mucho cuidado al utilizarlo pues es uno de los más peligrosos de Linux.

El parámetro ***-r*** elimina el contenido de una carpeta **de forma recursiva** y el parámetro ***-f*** fuerza la eliminación **sin preguntar**. ***/*** indica que comience en el directorio raíz.

Tiene algunas variantes que solo borran algunos archivos, como los de solo lectura, de forma que a los demás archivos no les afecta. Sin embargo, salvo que seas un usuario experimentado con respecto a la terminal de Linux, no es nada recomendable introducir este código en la consola.

La utilización de *rm -rf /* ha dado lugar a **varios desastres en la comunidad Linux**. Veamos un gran desastre muy famoso que fue ocasionado por la ejecución de este comando:

Nos situamos en 1998, en los estudios de Pixar en Richmond, donde encontramos a unas 150 personas están trabajando en la animación, el modelado y el montaje de la película animada ***Toy Story 2***. Alguien de esas 150 personas ejecutó un ***rm –rf /*** en su ordenador, de forma que, sin saberlo, acababa de provocar la **pérdida del 90% de la producción de la película**

Los accidentes ocurren, son inevitables, pero también hay formas de prevenirlos o reducir el daño que puedan causar. En Pixar no se tomaron las precauciones necesarias para ello. Todo el equipo llevaba ya diez meses en la producción de *Toy Story 2*. Hoy en día a ningún equipo de trabajo se le ocurriría dar **permisos *root* a todos los miembros de trabajo**, ni tampoco fiarse de **una única copia de seguridad**. Estos fueron los **dos grandes errores** que cometió Pixar.

En el estudio de Pixar les gustaba trabajar como un equipo por igual. Todos los empleados que trabajaban en la edición de la película tenían los mismos permisos de acceso para trabajar en conjunto y de forma simultánea. De este modo cada uno avanzaba en cierto aspecto de la producción para ahorrar tiempo. No tener una jerarquía tiene sus ventajas, pero también desventajas.

Cuando **el miembro del equipo ejecutó el comando *rm –rf /*,** al ejecutarse dicho comando **con permisos *root***, se ordenó la **eliminación de todo el sistema compartido de archivos del proyecto de *Toy Story 2***.

Ante el caos que se venía encima y viendo en directo cómo **todo el trabajo de los últimos 10 meses se estaba borrando** decidieron desenchufar directamente todo el sistema para evitar que siga borrando archivos. Cuando unas horas más tarde decidieron restaurar la última copia de seguridad de los archivos se toparon con que **faltaba la mayor parte de la película en la copia de seguridad**. Al inicio de la producción y cuando se montó todo el sistema de trabajo **pensaron que con 4 GB de espacio tendrían suficiente para la copia de seguridad**, pero esto no fue así ya que con todo el trabajo que llevaban hecho **ya tenían más de 10 GB de película** cuando se borró.

Galyn Susman se podría decir que es **la heroína que salvó *Toy Story 2*.** Unos meses antes del desastre la empleada de Pixar dió a luz, Pixar decidió montarle un equipo de trabajo en su casa para que pudiese trabajar en remoto. Susman recibía periódicamente las actualizaciones de los archivos de la película.

Los directivos de la película decidieron ir rápidamente a la casa de Susman para ver si aún disponía de los ficheros. Se llevaron todo el ordenador y discos duros con el máximo cuidado posible. Al llevar el equipo a los estudios de Pixar y encenderlo vieron que el equipo tenía los archivos actualizados a la versión de hace dos semanas. Por lo **solo se había perdido el trabajo de las últimas dos semanas** y no de los últimos diez meses. Con eso y con algunos ficheros que aún no habían llegado a borrarse en los ordenadores del estudio pudieron recuperar casi toda la película. Finalmente, *Toy Story 2* se recuperó y la pesadilla terminó.

❖ EvilGnome

EvilGnome es un **malware** que se hace pasar por una extensión del famoso entorno gráfico para Linux llamado **Gnome** (de ahí el nombre EvilGnome). Los **descubridores** de este virus fueron los investigadores de **Intezer Labs** y escribieron un artículo sobre ello, el cual se encuentra en el siguiente enlace:

https://intezer.com/blog-evilgnome-rare-malware-spying-on-linux-desktop-users/

Según los investigadores de Palo Alto Networks, EvilGnome fue **desarrollado por Gamaredon Group**, un grupo ruso activo desde 2013. Los investigadores mencionan que fue **diseñado para capturar todo tipo de datos de nuestro equipo**, como capturas de pantalla del escritorio, robar archivos, grabar audio o incluso cargar y ejecutar otros módulos maliciosos, todo sin que nos demos cuenta de qué está pasando.

Este software malicioso se presenta como un **script** creado con *makeself*, un pequeño script Shell que genera un archivo TAR comprimido y autoextraíble desde el escritorio.

Para comprobar si estamos afectados tenemos que buscar el archivo ejecutable **"gnome-shel-ext"** en la **ruta *~/.cache/gnome-software/gnome-shell-extensions***.

¿Por qué he elegido estos ejemplos?

En primer lugar, he elegido como primer ejemplo el comando ***rm -rf /*** porque pienso que todo el mundo que tenga Linux como sistema operativo debería conocer ese comando al menos. Hasta las empresas más importantes pueden cometer un error al ejecutar dicho comando, como ocurrió con Pixar. Tras la ejecución de ese comando perderás todo lo que tengas y sé que a nadie le gustaría perder las cosas que tiene en el ordenador ya que todos guardamos cosas importantes en ellos: fotos de años anteriores, documentos de nuestro trabajo, etc.

En segundo lugar, he elegido el malware EvilGnome para hacer ver que los problemas de seguridad y virus también existen en Linux aunque sea más seguro que Windows. Aún teniendo Linux como sistema operativo existe el riesgo estar siendo espiado por otra persona debido a un malware y es por ello que siempre hay que tener mucha precaución, mantener siempre actualizado el software de tu ordenador y descargar cualquier archivo o software solo de fuentes oficiales.

Bibliografía

- https://computerhoy.com/listas/software/comandos-linux-que-pueden-destruir-tu-ordenador-53598
- https://www.howtogeek.com/125157/8-deadly-commands-you-should-never-run-on-linux/
- https://www.xataka.com/cine-y-tv/como-pixar-recupero-toy-story-2-borrar-toda-pelicula-error-copia-seguridad
- https://ayudalinux.com/evilgnome-nuevo-malware-de-linux-espia-a-los-usuarios-de-linux-y-roba-sus-archivos/
- https://blog.tqvcancun.org/post/186378427222/evilgnome-nuevo-y-raro-malware-que-afecta-a