Universidad Autónoma de Baja California

Facultad de Ciencias Químicas e Ingeniería



**Taller de Sistema Operativo UNIX**

**COMANDO TEE Y REDIRECCIONAMIENTO**

Docente: Dra. Pérez Ornelas Felicitas

Alumno: Gómez Cárdenas Emmanuel Alberto

Matrícula: 1261509

**Error en Sudo permitió a usuarios no autorizados de Linux ejecutar comandos root**

Una nueva vulnerabilidad ha sido descubierta, y parcheada, en Sudo -una de las utilidades más importantes y de uso común en UNIX y Linux.

La vulnerabilidad en cuestión es un problema de elusión de la política de seguridad de sudo que permitiría a un usuario no autorizado o a un programa ejecutar comandos como root en un sistema Linux atacado, incluso cuando la “configuración de sudoers” explícitamente inhabilita el acceso de root.

Dado que la separación de privilegios es uno de los paradigmas de seguridad fundamentales en Linux, los administradores pueden configurar un archivo de sudoers para definir qué usuarios pueden ejecutar qué comandos y a qué usuarios.

Por lo tanto, en un escenario específico en el que se le ha permitido ejecutar un comando específico, o cualquiera, como cualquier otro usuario excepto el root, la vulnerabilidad podría permitirle pasar por alto esta política de seguridad y tomar el control total del sistema como root. “Esto puede ser usado por un usuario con suficientes privilegios sudo para ejecutar comandos como root incluso si la especificación de Runas (ejecutar como) explícitamente no permite el acceso de root siempre y cuando la palabra clave ALL esté listada primero en la especificación de Runas,” dijeron los desarrolladores de Sudo a Hacker News.

**1. Ejecute el siguiente comando $ cat > ficha**

**Blanco:73:Marte:1543:Manuel**

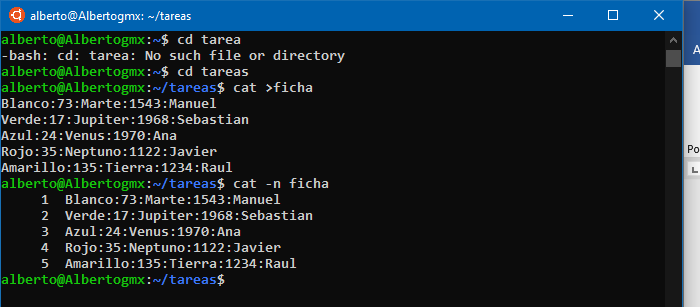
**Vede:17:Júpiter:1968:Sebastian**

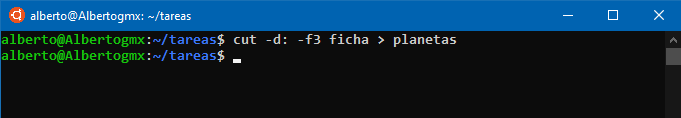
**Azul:24:Venus:1970:Ana**

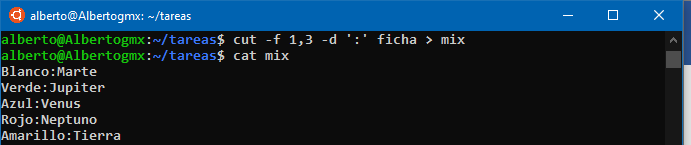
**Rojo:35:Netptuno:1122:Javier**

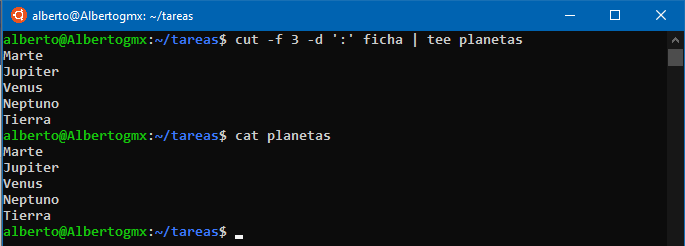
**Amarillo:135:Tierra:1234:Raul**

**Ctrl d**

**2. Muestre el archivo ficha con las líneas numeradas.** ****

**3. Muestre solamente a los planetas que están en el archivo ficha y redireccione la salida para generar un archivo llamado planetas.** 

**4. Muestre y genere un archivo solo con los colores y los planetas del archivo ficha, el nombre del archivo es opcional.**

**5. Repita el paso anterior pero ahora debe verse en pantalla el resultado al mismo tiempo que se genera el archivo.** ****

**6. Genere un archivo con las últimas tres líneas del archivo ficha.**

**7. ejecute el siguiente comando**

**$ cat > números**

**101**

**112**

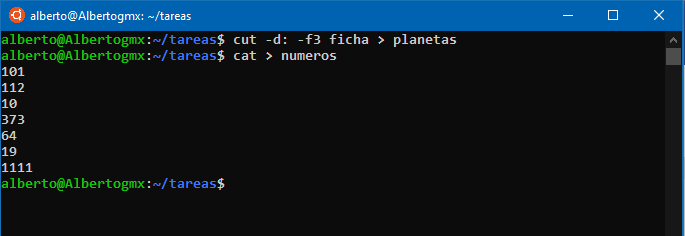
**10**

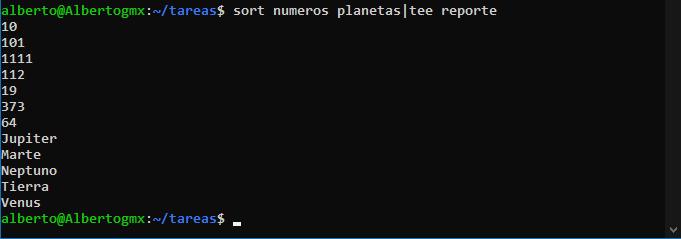
**373**

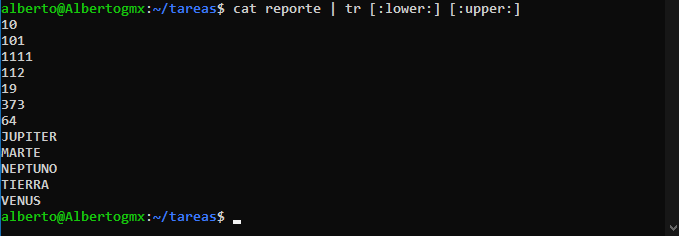
**64**

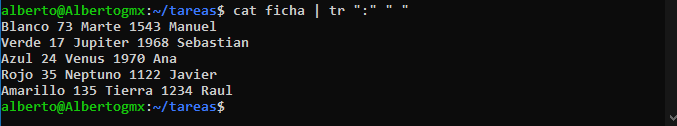
**19**

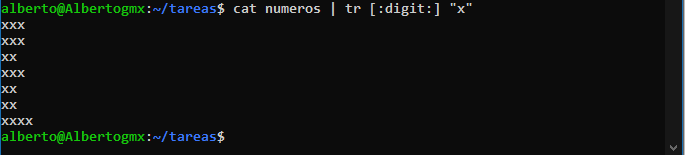
**1111**

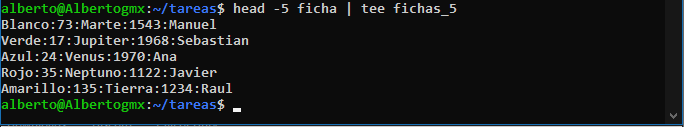
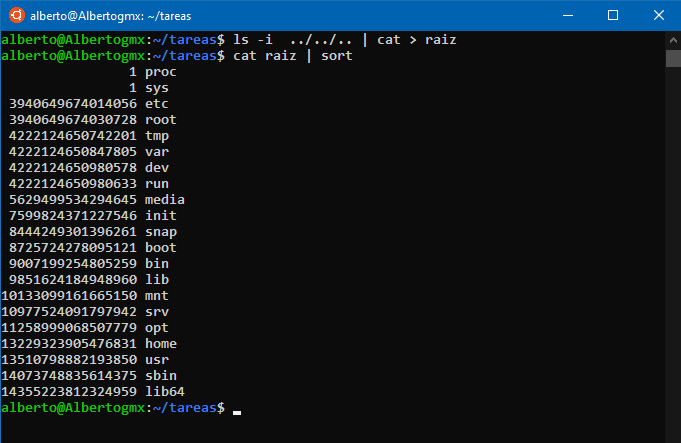
**Ctrl d**

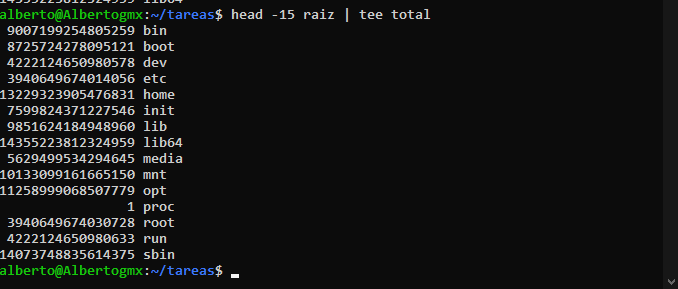
**8. Integre el archivo números y el archivo planetas en un archivo reporte.** ****

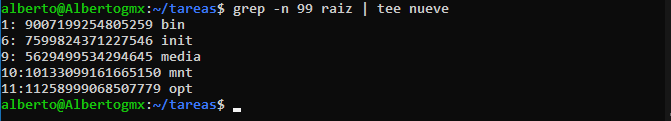
**9. El archivo reporte debe estar escrito todo en mayúsculas.** ****

**10. En el archivo de ficha sustituya todos los “:” por espacios.** ****

**11. En el archivo números sustituya todos los números por algún otro carácter.** ****

**12. Genere un archivo con las primeras 5 líneas del archivo ficha, el nombre del archivo es opcional.** **13. Genere un archivo del directorio / con detalles, ordenado por número de i-nodo. El resultado, además debe verse en pantalla. El nombre del archivo será raíz.** ****

**14. Genere un archivo llamado total con las primeras 15 líneas del archivo raíz, el resultado también debe verse en pantalla.** ****

**15. Genere un archivo nueves con las líneas que tengan dos nueves seguidos del archivo raíz.** ****

**Conclusiones**

Los comandos de redireccionamientos son bastante utiliza la hora de querer hacer respaldos, ya que te dejan redireccionar toda aquella información y guardarla en un archivo para respaldar los datos, sin embargo, también te permiten mandar esa información a otros comandos, por si lo que se desea es seguir manipulando esa información.

En cuanto a la vulnerabilidad descubierta, es un tema bastante grave, debido a que, poder saltarse ciertas restricciones, que, están ahí, porque son necesarias. Están creadas para restringir aquello que puede ser potencialmente peligroso ante el sistema operativo.

References

Error en Sudo permitió a usuarios no autorizados de Linux ejecutar comandos root. (2019). Retrieved 8 December 2019, from https://diarioti.com/error-en-sudo-permitio-a-usuarios-no-autorizados-de-linux-ejecutar-comandos-root/111013