

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

Verde:17:Júpiter:1968:Sebastian

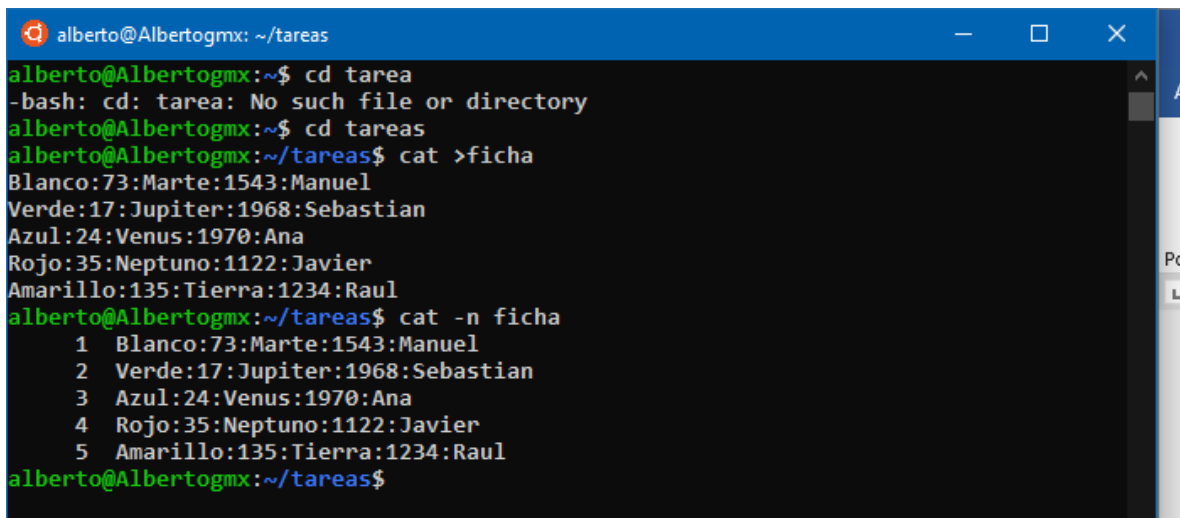
Azul:24:Venus:1970:Ana

Rojo:35:Neptuno:1122:Javier

Amarillo:135:Tierra:1234:Raul

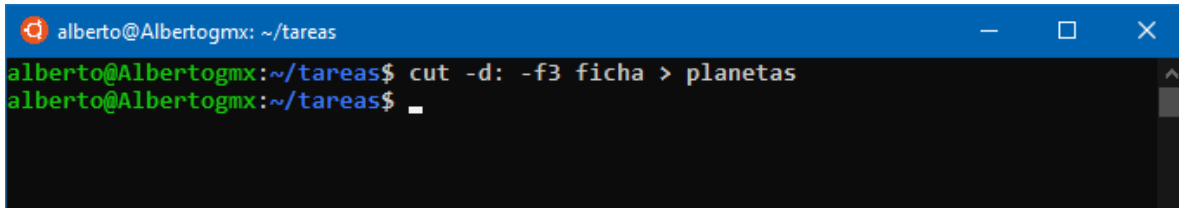
Ctrl d

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



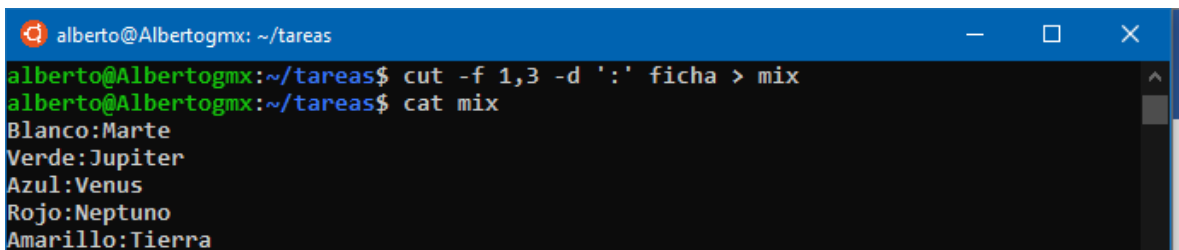
```
alberto@Albertogmx: ~/tareas
alberto@Albertogmx:~$ cd tarea
-bash: cd: tarea: No such file or directory
alberto@Albertogmx:~$ cd tareas
alberto@Albertogmx:~/tareas$ cat >ficha
Blanco:73:Marte:1543:Manuel
Verde:17:Jupiter:1968:Sebastian
Azul:24:Venus:1970:Ana
Rojo:35:Neptuno:1122:Javier
Amarillo:135:Tierra:1234:Raul
alberto@Albertogmx:~/tareas$ cat -n ficha
 1 Blanco:73:Marte:1543:Manuel
 2 Verde:17:Jupiter:1968:Sebastian
 3 Azul:24:Venus:1970:Ana
 4 Rojo:35:Neptuno:1122:Javier
 5 Amarillo:135:Tierra:1234:Raul
alberto@Albertogmx:~/tareas$
```

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



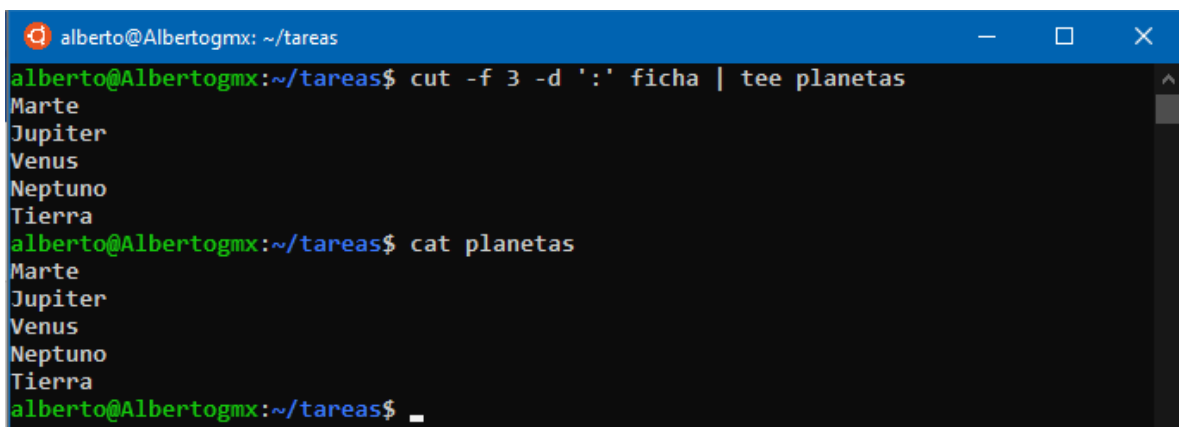
```
alberto@Albertogmx: ~/tareas
alberto@Albertogmx:~/tareas$ cut -d: -f3 ficha > planetas
alberto@Albertogmx:~/tareas$ _
```

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



```
alberto@Albertogmx: ~/tareas
alberto@Albertogmx:~/tareas$ cut -f 1,3 -d ':' ficha > mix
alberto@Albertogmx:~/tareas$ cat mix
Blanco:Marte
Verde:Jupiter
Azul:Venus
Rojo:Neptuno
Amarillo:Tierra
```

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



```
alberto@Albertogmx: ~/tareas
alberto@Albertogmx:~/tareas$ cut -f 3 -d ':' ficha | tee planetas
Marte
Jupiter
Venus
Neptuno
Tierra
alberto@Albertogmx:~/tareas$ cat planetas
Marte
Jupiter
Venus
Neptuno
Tierra
alberto@Albertogmx:~/tareas$ _
```

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

7. ejecute el siguiente comando

\$ cat > números

101

112

10

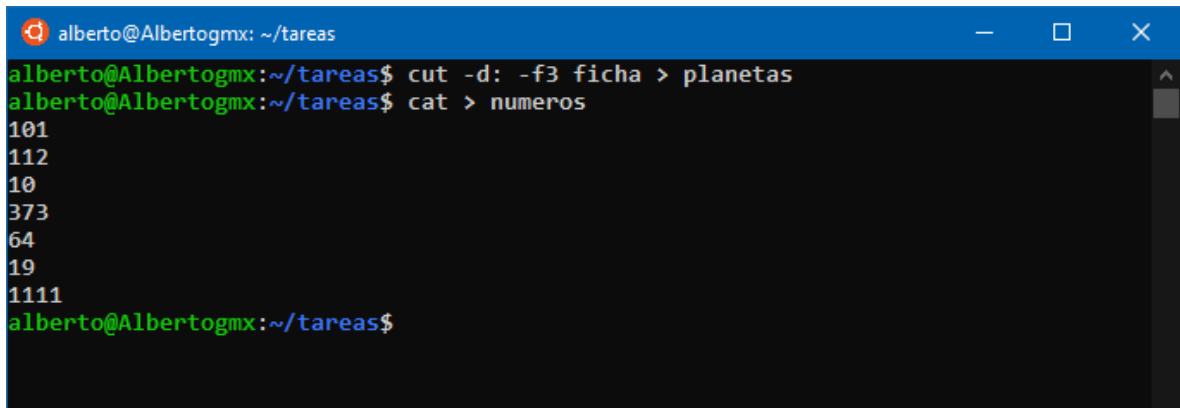
373

64

19

1111

Ctrl d



```
alberto@Albertogmx: ~/tareas
alberto@Albertogmx:~/tareas$ cut -d: -f3 ficha > planetas
alberto@Albertogmx:~/tareas$ cat > numeros
101
112
10
373
64
19
1111
alberto@Albertogmx:~/tareas$
```

A terminal window with a blue title bar showing the user 'alberto' at host 'Albertogmx' in the directory '~/tareas'. The terminal displays the execution of two commands: 'cut -d: -f3 ficha > planetas' and 'cat > numeros'. Following the second command, the numbers 101, 112, 10, 373, 64, 19, and 1111 are printed on separate lines. The prompt returns to 'alberto@Albertogmx:~/tareas\$' after the last line.

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

```
alberto@Albertogmx:~/tareas$ sort numeros planetas|tee reporte
10
101
1111
112
19
373
64
Jupiter
Marte
Neptuno
Tierra
Venus
alberto@Albertogmx:~/tareas$ _
```

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

```
alberto@Albertogmx:~/tareas$ cat reporte | tr [:lower:] [:upper:]
10
101
1111
112
19
373
64
JUPITER
MARTE
NEPTUNO
TIERRA
VENUS
alberto@Albertogmx:~/tareas$ _
```

10. En el archivo de ficha sustituya todos los ":" por espacios.

```
alberto@Albertogmx:~/tareas$ cat ficha | tr ":" " "
Blanco 73 Marte 1543 Manuel
Verde 17 Jupiter 1968 Sebastian
Azul 24 Venus 1970 Ana
Rojo 35 Neptuno 1122 Javier
Amarillo 135 Tierra 1234 Raul
alberto@Albertogmx:~/tareas$
```

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

```
alberto@Albertogmx:~/tareas$ cat numeros | tr [:digit:] "x"
xxx
xxx
xx
xxx
xx
xx
xxxx
alberto@Albertogmx:~/tareas$
```

12. Genere un archivo con las primeras 5 líneas del archivo ficha, el nombre del archivo es opcional.

```
alberto@Albertogmx:~/tareas$ head -5 ficha | tee fichas_5
Blanco:73:Marte:1543:Manuel
Verde:17:Jupiter:1968:Sebastian
Azul:24:Venus:1970:Ana
Rojo:35:Neptuno:1122:Javier
Amarillo:135:Tierra:1234:Raul
alberto@Albertogmx:~/tareas$
```

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.

```
alberto@Albertogmx: ~/tareas
alberto@Albertogmx:~/tareas$ ls -i ../../.. | cat > raiz
alberto@Albertogmx:~/tareas$ cat raiz | sort
      1 proc
      1 sys
3940649674014056 etc
3940649674030728 root
4222124650742201 tmp
4222124650847805 var
4222124650980578 dev
4222124650980633 run
5629499534294645 media
7599824371227546 init
8444249301396261 snap
8725724278095121 boot
9007199254805259 bin
9851624184948960 lib
10133099161665150 mnt
10977524091797942 srv
11258999068507779 opt
13229323905476831 home
13510798882193850 usr
14073748835614375 sbin
14355223812324959 lib64
alberto@Albertogmx:~/tareas$ _
```

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

```
alberto@Albertogmx:~/tareas$ head -15 raiz | tee total
9007199254805259 bin
8725724278095121 boot
4222124650980578 dev
3940649674014056 etc
13229323905476831 home
7599824371227546 init
9851624184948960 lib
14355223812324959 lib64
5629499534294645 media
10133099161665150 mnt
11258999068507779 opt
      1 proc
3940649674030728 root
4222124650980633 run
14073748835614375 sbin
alberto@Albertogmx:~/tareas$ _
```


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

```
alberto@Albertogmx:~/tareas$ grep -n 99 raiz | tee nueve
1: 9007199254805259 bin
6: 7599824371227546 init
9: 5629499534294645 media
10:10133099161665150 mnt
11:11258999068507779 opt
alberto@Albertogmx:~/tareas$ _
```

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>