Solución 1.4: Creación de un Shell Restringido

Comandos Utilizados

Creacción del usuario `carmela`.

```
┌──(kali㉿kali)-[~]
└─$ sudo useradd -m -d /home/carmela -s /bin/bash -p $(mkpasswd 'abc123.') carmela
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ tail -n 1 /etc/passwd
carmela:x:1002:1002::/home/carmela:/bin/bash
```

1. En la terminal de administrador, edita `/etc/passwd` para que el shell por defecto de `carmela` sea `/bin/rbash` en lugar de `/bin/bash`.

```
grep carmela /etc/passwd | sed 's/\/bin\/bash/\/bin\/rbash/' /etc/passwd | tail -n
1 /etc/passwd
```

```
┌──(root㉿kali)-[~]
└─# grep carmela /etc/passwd | sed 's/\/bin\/bash/\/bin\/rbash/' /etc/passwd |
tail -n 1 /etc/passwd
carmela:x:1002:1002::/home/carmela:/bin/rbash
```

Nota: Diferencia entre shell `bash` y `rbash`. `rbash` (restricted bash) es una versión limitada de `bash` que restringe ciertas acciones para el usuario. Algunas de las limitaciones más comunes son:

1. No permite cambiar de directorio con el comando `cd`.
2. No permite ejecutar comandos fuera de un conjunto específico, como los que están en el `PATH` o en una lista permitida.
3. Desactiva el uso de ciertos comandos (como `exec`, `source` y otros).
4. Puede restringir el acceso a variables de entorno y a otros archivos del sistema.

En resumen, `rbash` limita la capacidad del usuario para interactuar con el sistema de manera más libre que `bash`. Esto se usa generalmente para proporcionar un entorno más controlado.

2. En la terminal de `carmela`, inicia sesión como `carmela` ejecutando:

```
sudo -u carmela -i
```

```
┌──(kali㉿kali)-[~]
└─$ sudo -u carmela -i
```

Nota: El comando `sudo -u carmela -i` realiza lo siguiente:

- **`sudo`** → Ejecuta un comando como otro usuario con privilegios.
- **`-u carmela`** → Especifica que el comando se ejecutará como el usuario `carmela`.
- **`-i`** → Inicia una sesión interactiva de login shell, lo que significa que:
  - Se carga el entorno del usuario (`~/.bashrc`, `~/.profile`, etc.).
  - Cambia al directorio personal del usuario (`/home/carmela`).
  - Se establece el shell por defecto del usuario.
    Es equivalente a `su - carmela`

3. En la terminal de `carmela`, verifica que:

- Eres `carmela` con `whoami`.
- Estás en `/home/carmela` con `pwd`.
- Usas un bash restringido con `ps`.
- El autocompletado con la tecla tabulador ya no funciona y no puedes cambiar de directorio con `cd`.
- Comandos como `ps` y `ls` siguen funcionando.
- `echo $PATH` muestra rutas como `/usr/bin`, `/bin`, etc. Esto debe corregirse en el siguiente paso.

```
whoami
pwd
ps
cd #Error
ps/ls
echo $PATH
```

```
┌──(carmela㉿kali)-[~]
└─$ whoami
carmela

┌──(carmela㉿kali)-[~]
└─$ pwd
/home/carmela

┌──(carmela㉿kali)-[~]
└─$ ps
    PID TTY          TIME CMD
  11408 pts/4    00:00:00 rbash
  16127 pts/4    00:00:00 ps

┌──(carmela㉿kali)-[~]
└─$ cd
-rbash: cd: restricted
```

```
┌──(carmela㉿kali)-[~]
└─$ ls

┌──(carmela㉿kali)-[~]
└─$ echo $PATH
/home/carmela/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/
bin:/usr/local/games:/usr/games:/home/carmela/.dotnet/tools
```

4. En la terminal de administrador, ubícate en `/home/carmela` y crea un directorio `bin`:

```
cd /home/carmela
sudo mkdir bin
```

```
┌──(root㉿kali)-[~]
└─# cd /home/carmela && mkdir bin

┌──(root㉿kali)-[/home/carmela]
└─# ls -l /home/carmela
total 4
drwxrwxr-x 2 root root 4096 Feb 26 07:17 bin
```

5. En la terminal de administrador, edita el archivo `.profile` con permisos de `sudo`:

```
sudo nano .profile
```

Añade al final la línea:

```
PATH="$HOME/bin"
```

```
┌──(root㉿kali)-[/home/carmela]
└─# tail -n 1 .profile
PATH="$HOME/bin"
```

6. En la terminal de `carmela`, sal del shell con `exit` y vuelve a entrar con `sudo -u carmela -i`. Verifica que ya no puedes ejecutar ningún comando como `ls` o `ps`.

```
┌──(root㉿kali)-[/home/carmela]
└─# which ls
ls: aliased to ls --color=auto
```

```
┌──(root㉿kali)-[/home/carmela]
└─# whereis ls
ls: /usr/bin/ls /usr/share/man/man1/ls.1.gz

┌──(root㉿kali)-[/home/carmela]
└─# which ps
/usr/bin/ps
```

```
┌──(carmela㉿kali)-[~]
└─$ ls
-rbash: /usr/lib/command-not-found: restricted: cannot specify `/' in command
names

┌──(carmela㉿kali)-[~]
└─$ ps
-rbash: /usr/lib/command-not-found: restricted: cannot specify `/' in command
names
```

7. En la terminal de administrador, crea enlaces simbólicos para permitir que `carmela` use ciertos comandos:

```
sudo ln -s /bin/ls /home/carmela/bin/ls
sudo ln -s /bin/rm /home/carmela/bin/rm
sudo ln -s /bin/vi /home/carmela/bin/vi
sudo ln -s /bin/nano /home/carmela/bin/nano
```

```
┌──(root㉿kali)-[/home/kali]
└─# ln -s /bin/ls /home/carmela/bin/ls
┌──(root㉿kali)-[/home/kali]
└─# ln -s /bin/rm /home/carmela/bin/rm
┌──(root㉿kali)-[/home/kali]
└─# ln -s /bin/vi /home/carmela/bin/vi
┌──(root㉿kali)-[/home/kali]
└─# ln -s /bin/nano /home/carmela/bin/nano

┌──(root㉿kali)-[/home/kali]
└─# ls -la /home/carmela/bin
total 8
drwxrwxr-x 2 root    root    4096 Feb 26 17:47 .
drwx------ 6 carmela carmela 4096 Feb 26 07:23 ..
lrwxrwxrwx 1 root    root       7 Feb 26 17:46 ls -> /bin/ls
lrwxrwxrwx 1 root    root       9 Feb 26 17:47 nano -> /bin/nano
lrwxrwxrwx 1 root    root       7 Feb 26 17:46 rm -> /bin/rm
lrwxrwxrwx 1 root    root       7 Feb 26 17:46 vi -> /bin/vi
```

8. En la terminal de `carmela`, verifica que puedes ejecutar estos comandos, pero no `ps`.

```
echo "Hola" > /home/carmela/prueba.txt && chmod 777 /home/carmela/prueba.txt #como
root
ls
rm prueba.txt
ps # error
```

```
┌──(root㉿kali)-[/home/kali]
└─# echo "Hola" > /home/carmela/prueba.txt && chmod 777 /home/carmela/prueba.txt
```

```
┌──(carmela㉿kali)-[~]
└─$ ls
bin  prueba.txt

┌──(carmela㉿kali)-[~]
└─$ rm prueba.txt

┌──(carmela㉿kali)-[~]
└─$ ls
bin

┌──(carmela㉿kali)-[~]
└─$ ps
-rbash: /usr/lib/command-not-found: restricted: cannot specify `/' in command
names
```

9. En la terminal de `carmela`, ejecuta `ls -lisa` y verifica que los archivos de inicio (.profile, .bashrc, etc.) siguen siendo propiedad de `carmela`.

```
ls -lisa
```

```
┌──(carmela㉿kali)-[~]
└─$ ls -lisa
total 80
985932  4 drwx------ 6 carmela carmela  4096 Feb 26 17:51 .
913921  4 drwxr-xr-x 5 root    root     4096 Feb 26 06:51 ..
988004  4 -rw------- 1 carmela carmela   122 Feb 26 17:47 .bash_history
987998  4 -rw-r--r-- 1 carmela carmela   220 Oct 20 13:19 .bash_logout
987997  8 -rw-r--r-- 1 carmela carmela  5551 Nov 30 09:39 .bashrc
987996  4 -rw-r--r-- 1 carmela carmela  3526 Oct 20 13:19 .bashrc.original
987985  4 drwxr-xr-x 6 carmela carmela  4096 Feb 10 11:41 .config
987982 12 -rw-r--r-- 1 carmela carmela 11759 Oct 26 23:06 .face
987984  0 lrwxrwxrwx 1 carmela carmela     5 Feb 10 11:41 .face.icon -> .face
985973  4 drwxr-xr-x 3 carmela carmela  4096 Feb 10 11:41 .java
```

```
987976  4 drwxr-xr-x 5 carmela carmela  4096 Feb 26 07:05 .local
987999  4 -rw-r--r-- 1 carmela carmela   825 Feb 26 07:23 .profile
988011  4 -rw------- 1 carmela carmela   713 Feb 26 17:51 .viminfo
987995  4 -rw-r--r-- 1 carmela carmela   336 Nov 21 09:26 .zprofile
987983 12 -rw-r--r-- 1 carmela carmela 10868 Nov 21 09:26 .zshrc
988003  4 drwxrwxr-x 2 root    root     4096 Feb 26 17:47 bin
```

10. En la terminal de administrador, cambia el dueño y grupo de estos archivos a `root`:

```
sudo chown root:root .profile
sudo chown root:root .bashrc
```

Verifica que `carmela` no puede modificarlos.

```
┌──(root㉿kali)-[/home/kali]
└─# chown root:root /home/carmela/.profile
┌──(root㉿kali)-[/home/kali]
└─# chown root:root /home/carmela/.bashrc
```

```
┌──(carmela㉿kali)-[~]
└─$ ls -lisa
total 80
985932  4 drwx------ 6 carmela carmela  4096 Feb 26 17:54 .
913921  4 drwxr-xr-x 5 root    root     4096 Feb 26 06:51 ..
988004  4 -rw------- 1 carmela carmela   122 Feb 26 17:47 .bash_history
987998  4 -rw-r--r-- 1 carmela carmela   220 Oct 20 13:19 .bash_logout
987997  8 -rw-r--r-- 1 root    root     5551 Nov 30 09:39 .bashrc
987996  4 -rw-r--r-- 1 carmela carmela  3526 Oct 20 13:19 .bashrc.original
987985  4 drwxr-xr-x 6 carmela carmela  4096 Feb 10 11:41 .config
987982 12 -rw-r--r-- 1 carmela carmela 11759 Oct 26 23:06 .face
987984  0 lrwxrwxrwx 1 carmela carmela     5 Feb 10 11:41 .face.icon -> .face
985973  4 drwxr-xr-x 3 carmela carmela  4096 Feb 10 11:41 .java
987976  4 drwxr-xr-x 5 carmela carmela  4096 Feb 26 07:05 .local
987999  4 -rw-r--r-- 1 root    root      825 Feb 26 17:54 .profile
988011  4 -rw------- 1 carmela carmela   713 Feb 26 17:51 .viminfo
987995  4 -rw-r--r-- 1 carmela carmela   336 Nov 21 09:26 .zprofile
987983 12 -rw-r--r-- 1 carmela carmela 10868 Nov 21 09:26 .zshrc
988003  4 drwxrwxr-x 2 root    root     4096 Feb 26 17:47 bin
```

11. En la terminal de `carmela`, intenta eliminar `.profile` con `rm .profile`. Si puedes hacerlo, sal y vuelve a entrar con `sudo -u carmela -i`, y comprueba que ahora `ps` vuelve a funcionar.

```
ln -s /bin/ps /home/carmela/bin/ps # como root
rm -r .profile # como carmela
ls -lisa # como carmela
```

```
┌──(root㉿kali)-[/home/kali]
└─# ln -s /bin/ps /home/carmela/bin/ps
```

```
┌──(carmela㉿kali)-[~]
└─$ rm -r .profile
rm: remove write-protected regular file '.profile'?

┌──(carmela㉿kali)-[~]
└─$ ls -lisa
total 80
985932  4 drwx------ 6 carmela carmela  4096 Feb 26 17:54 .
913921  4 drwxr-xr-x 5 root    root     4096 Feb 26 06:51 ..
988004  4 -rw------- 1 carmela carmela   290 Feb 26 17:57 .bash_history
987998  4 -rw-r--r-- 1 carmela carmela   220 Oct 20 13:19 .bash_logout
987997  8 -rw-r--r-- 1 root    root     5551 Nov 30 09:39 .bashrc
987996  4 -rw-r--r-- 1 carmela carmela  3526 Oct 20 13:19 .bashrc.original
987985  4 drwxr-xr-x 6 carmela carmela  4096 Feb 10 11:41 .config
987982 12 -rw-r--r-- 1 carmela carmela 11759 Oct 26 23:06 .face
987984  0 lrwxrwxrwx 1 carmela carmela     5 Feb 10 11:41 .face.icon -> .face
985973  4 drwxr-xr-x 3 carmela carmela  4096 Feb 10 11:41 .java
987976  4 drwxr-xr-x 5 carmela carmela  4096 Feb 26 07:05 .local
987999  4 -rw-r--r-- 1 root    root      825 Feb 26 17:54 .profile
988011  4 -rw------- 1 carmela carmela   713 Feb 26 17:51 .viminfo
987995  4 -rw-r--r-- 1 carmela carmela   336 Nov 21 09:26 .zprofile
987983 12 -rw-r--r-- 1 carmela carmela 10868 Nov 21 09:26 .zshrc
988003  4 drwxrwxr-x 2 root    root     4096 Feb 26 17:58 bin

┌──(carmela㉿kali)-[~]
└─$ ps
    PID TTY          TIME CMD
   1420 pts/4    00:00:00 rbash
   1552 pts/4    00:00:00 ps
```

12. En la terminal de administrador, restaura `.profile` con la copia de seguridad que hayas hecho previamente.

```
cp -pv /home/carmela/.profile /home/carmela/.profile_VIEJO # como root
rm /home/carmela/.profile # como root
```

```
┌──(root㉿kali)-[/home/kali]
└─# cp -pv /home/carmela/.profile /home/carmela/.profile_VIEJO
'/home/carmela/.profile' -> '/home/carmela/.profile_VIEJO'
```

```
┌──(root㉿kali)-[/home/kali]
└─# rm /home/carmela/.profile
```

13. Como `carmela` tiene permisos de escritura en `/home/carmela`, puede eliminar archivos. Para corregir esto, en la terminal de administrador ejecuta:

```
sudo chown root:root /home/carmela
sudo chmod +t /home/carmela
```

Verifica con `ls -lisa /home` que los permisos sean `drwxr-xr-t` y el dueño `root:root`.

```
┌──(root㉿kali)-[/home/kali]
└─# chown root:root /home/carmela

┌──(root㉿kali)-[/home/kali]
└─# chmod +t /home/carmela

┌──(root㉿kali)-[/home/kali]
└─# ls -lisa /home
total 20
913921 4 drwxr-xr-x  5 root root 4096 Feb 26 06:51 .
     2 4 drwxr-xr-x 18 root root 4096 Feb 10 11:50 ..
985932 4 drwx-----T  6 root root 4096 Feb 26 18:02 carmela
985707 4 drwx------ 17 kali kali 4096 Feb 26 17:46 kali
985927 4 drwx------  5 pepe pepe 4096 Feb 25 09:28 pepe
```

14. En la terminal de `carmela`, intenta borrar `.profile`. Verás que ahora no puedes.

```
sudo -u carmela -i # error al intentar acceder
```

```
┌──(kali㉿kali)-[~]
└─$ sudo -u carmela -i
sudo: unable to change directory to /home/carmela: Permission denied
-rbash: /home/carmela/.bash_profile: Permission denied
carmela@kali:/home/kali$
```

15. En la terminal de `carmela`, intenta crear un archivo (`nano prueba`). Verás que tampoco puedes porque no tienes permisos de escritura en tu directorio.

```
nano /home/carmela/prueba
```

```
carmela@kali:/home/kali$ nano /home/carmela/prueba
Unable to create directory /home/carmela/.local/share/nano/: Permission denied
It is required for saving/loading search history or cursor positions.
```

16. Para solucionar esto, hay dos alternativas:

- Opción 1:

```
sudo chown root:carmela /home/carmela
sudo chmod 1775 /home/carmela
```

Si `carmela` aún puede borrar `.profile`, esta opción no es válida y deberás restaurar la copia de seguridad.

- Opción 2:

```
sudo chown root:root /home/carmela
sudo chmod 1755 /home/carmela
sudo setfacl -m "u:carmela:rwx" /home/carmela
```

Verifica con `getfacl /home/carmela` que la ACL está activa y con `ls -lisa /home` que hay un `+` al final de los permisos.

Opción 1

```
┌──(root㉿kali)-[/home/kali]
└─# cp -pv /home/carmela/.profile_VIEJO /home/carmela/.profile

┌──(root㉿kali)-[/home/kali]
└─# chown root:carmela /home/carmela

┌──(root㉿kali)-[/home/kali]
└─# chmod 1775 /home/carmela

┌──(root㉿kali)-[/home/kali]
└─# ls -ld /home/carmela
drwxrwxr-t 6 root carmela 4096 Feb 26 18:08 /home/carmela
```

```
┌──(carmela㉿kali)-[~]
└─$ rm .profile
rm: remove write-protected regular file '.profile'?
```

Opción 2

```
┌──(root㉿kali)-[/home/kali]
└─# ls -ld /home/carmela
drwxrwxr-t+ 6 root root 4096 Feb 26 18:08 /home/carmela

┌──(root㉿kali)-[/home/kali]
└─# getfacl /home/carmela
getfacl: Removing leading '/' from absolute path names
# file: home/carmela
# owner: root
# group: root
# flags: --t
user::rwx
user:carmela:rwx
group::r-x
mask::rwx
other::r-x
```

17. En la terminal de `carmela`, prueba que puedes crear archivos pero no modificar ni eliminar `.profile`.

```
┌──(carmela㉿kali)-[~]
└─$ rm .profile
rm: remove write-protected regular file '.profile'?

┌──(carmela㉿kali)-[~]
└─$ echo "Modificar" >> .profile
-rbash: .profile: restricted: cannot redirect output

┌──(carmela㉿kali)-[~]
└─$ nano prueba

┌──(carmela㉿kali)-[~]
└─$ ls -l
total 8
drwxrwxr-x 2 root    root    4096 Feb 26 17:58 bin
-rw-rw-r-- 1 carmela carmela    4 Feb 26 18:24 prueba
```