



Ejercicio 42.2 Más de setuid y scripts

Supongamos que tenemos el siguiente programa en **C** (`./writeit.c`), el cual intenta sobrescribir un archivo llamado `afile` en el directorio actual:

```
#include <stdio.h>
#include <unistd.h>
#include <fcntl.h>
#include <stdlib.h>
#include <string.h>
#include <stdlib.h>
#include <sys/stat.h>

int main(int argc, char *argv[])
{
    int fd, rc;
    char *buffer = "TESTING A WRITE";
    fd = open("./afile", O_RDWR | O_CREAT | O_TRUNC, S_IRUSR | S_IWUSR);
    rc = write(fd, buffer, strlen(buffer));
    printf("wrote %d bytes\n", rc);
    close(fd);
    exit(EXIT_SUCCESS);
}
```

Si está tomando la versión de autoaprendizaje de este curso, el código fuente está disponible para su descarga desde la pantalla **Laboratorio**.

Si el programa se llama `writeit.c`, puede ser compilado haciendo:

```
$ make writeit
```

o de forma equivalente:

```
$ gcc -o writeit writeit.c
```

Si intenta ejecutar este programa como un usuario normal sobre un archivo del cual `root` es el dueño, obtendrá lo siguiente:

```
$ sudo touch afile
$ ./writeit
wrote -1 bytes
```

pero si lo ejecuta como `root`:

```
$ sudo ./writeit
wrote 15 bytes
```

Por lo tanto, el usuario `root` fue capaz de sobrescribir el archivo del cual es dueño, pero un usuario normal no podría.

Tenga en cuenta que no ayudará cambiar el dueño de `writeit` a `root`:

```
$ sudo chown root.root writeit
$ ./writeit
wrote -1 bytes
```

porque todavía no le permitirá sobrescribir `afile`.

Al configurar el bit **setuid** usted puede habilitar a cualquier usuario normal para que lo haga:

```
$ sudo chmod +s writeit
$ ./writeit

wrote 15 bytes
```

Usted se podría preguntar por qué simplemente no escribimos un script que realice la operación, en vez de escribir y compilar un programa ejecutable.

Bajo **Linux**, si se cambia el **setuid** en un script ejecutable, no hará nada a menos que usted cambie el bit setuid en la shell (tal como bash), lo cual sería un gran error; cualquier cosa que se corra desde ahí podría escalar privilegios.