Exploit Education

Nebula – Level00

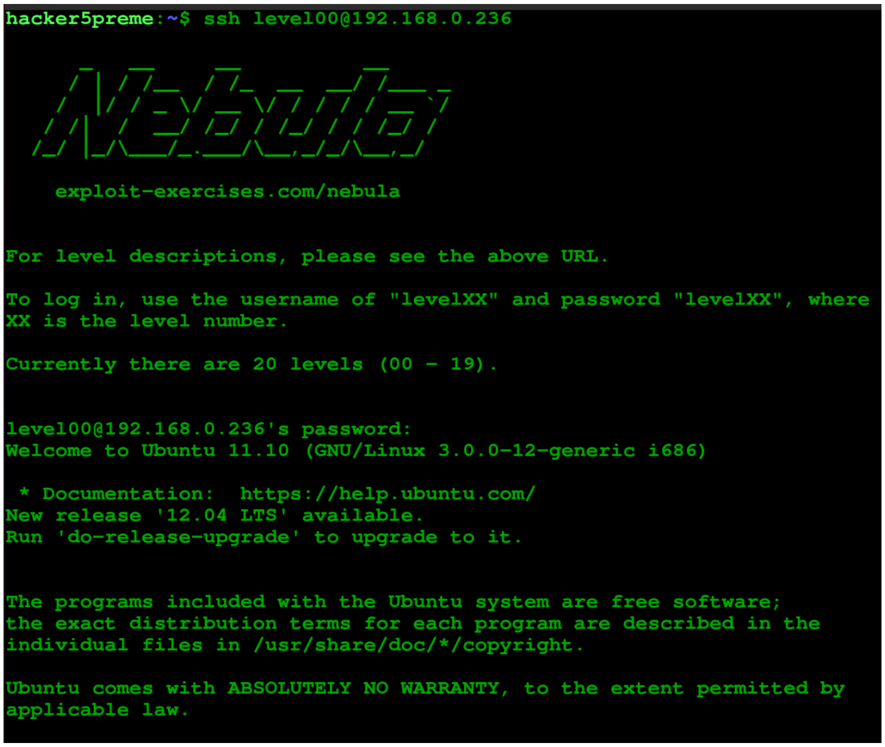
Description:

This level requires you to *find* a Set User ID program that will run as the “flag00” account. You could also find this by carefully looking in top level directories in / for suspicious looking directories. Alternatively, look at the find man page. To access this level, log in as level00 with the password of level00.

Solution:

Login:

First, login to Nebula via ssh: ssh level00@[your_IP_adress] . The password is level00.



```
hacker5preme:~$ ssh level00@192.168.0.236

      _   __     __          __
     / | / /__  / /_  __  __/ /___ _
    /  |/ / _ \/ __ \/ / / / / __ `/
   / /|  /  __/ /_/ / /_/ / / /_/ /
  /_/ |_/\___/_.___/\__,_/_/\__,_/

    exploit-exercises.com/nebula


For level descriptions, please see the above URL.

To log in, use the username of "levelXX" and password "levelXX", where
XX is the level number.

Currently there are 20 levels (00 - 19).


level00@192.168.0.236's password:
Welcome to Ubuntu 11.10 (GNU/Linux 3.0.0-12-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '12.04 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Research:

To solve level00 we are required to find Set User ID program that will run as the flag00 account.

What is a Set User ID programm:

First I looked up what Set User ID means: https://en.wikipedia.org/wiki/Setuid

> The Unix access rights flags **setuid** and **setgid** (short for "set user ID" and "set group ID") [1] allow users to run an executable with the file system permissions of the executable's owner or group respectively and to change behaviour in directories. They are often used to allow users on a computer system to run programs with temporarily elevated privileges in order to perform a specific task. While the assumed user id or group id privileges provided are not always elevated, at a minimum they are specific.

Then I went ahead and looked up how I can find programms with Set User ID permissions.

https://www.thegeekdiary.com/linux-unix-how-to-find-files-which-has-suid-sgid-set/

> find / -perm +4000

With this information I constructed the following find command:

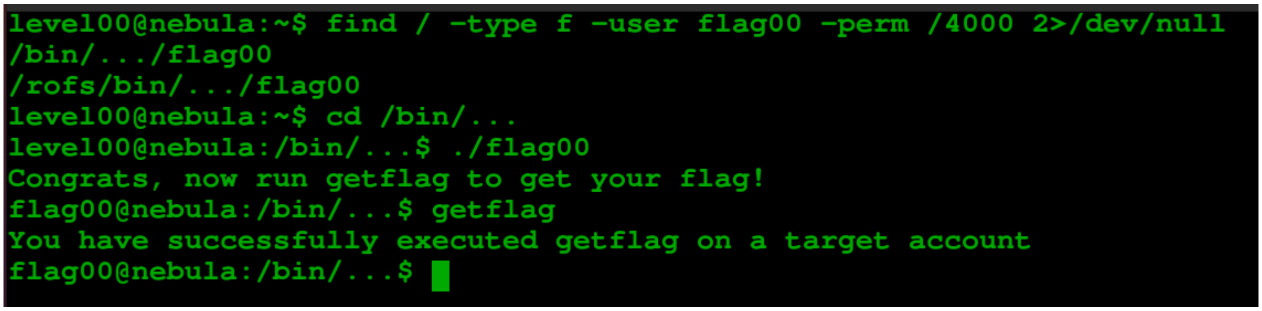
find / -type f -user flag00 -perm *4000 2*>/dev/null

-type: Defines the type which should be found (f for files)

- user: User, who owns the program (file)

- perm 4000: Find only programms with Set User ID permissions

-2>/dev/null: Don‘t display error messages



```
level00@nebula:~$ find / -type f -user flag00 -perm /4000 2>/dev/null
/bin/.../flag00
/rofs/bin/.../flag00
level00@nebula:~$ cd /bin/...
level00@nebula:/bin/...$ ./flag00
Congrats, now run getflag to get your flag!
flag00@nebula:/bin/...$ getflag
You have successfully executed getflag on a target account
flag00@nebula:/bin/...$ 
```