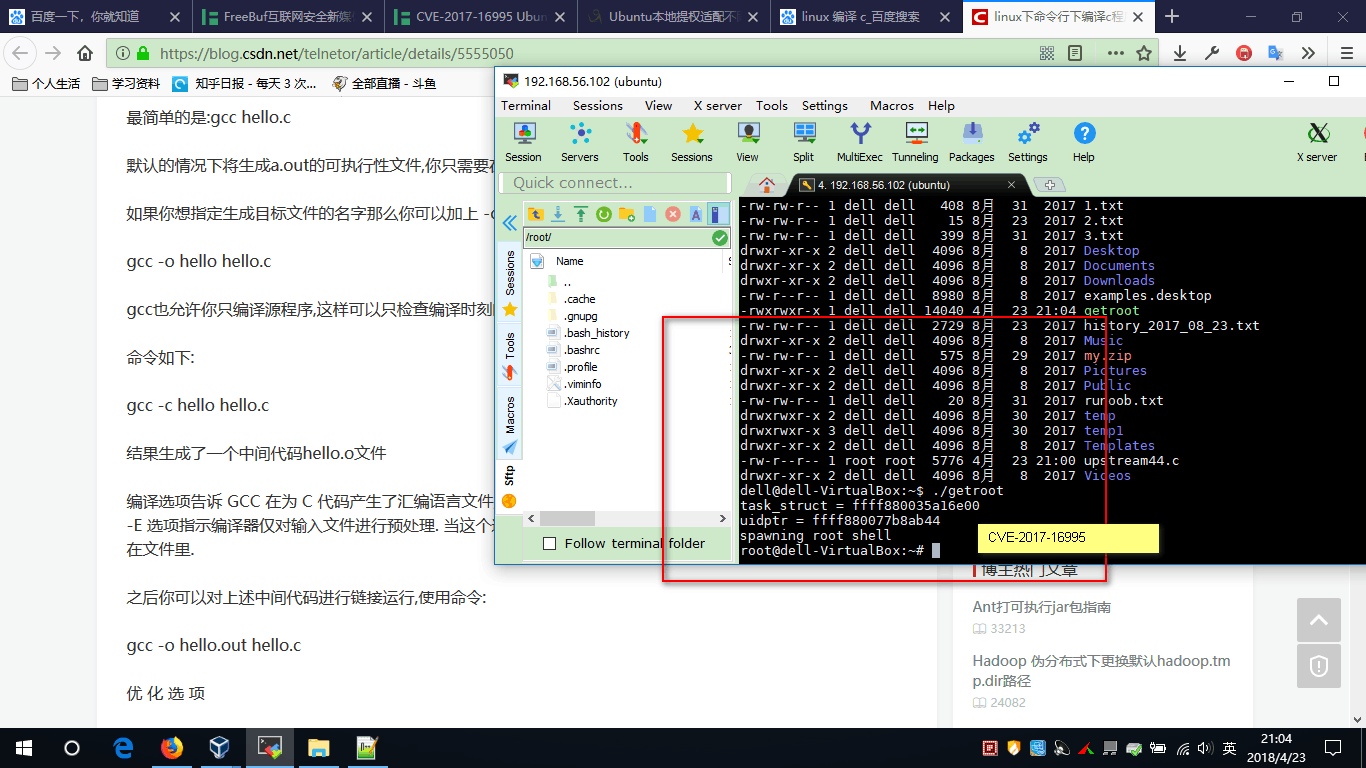
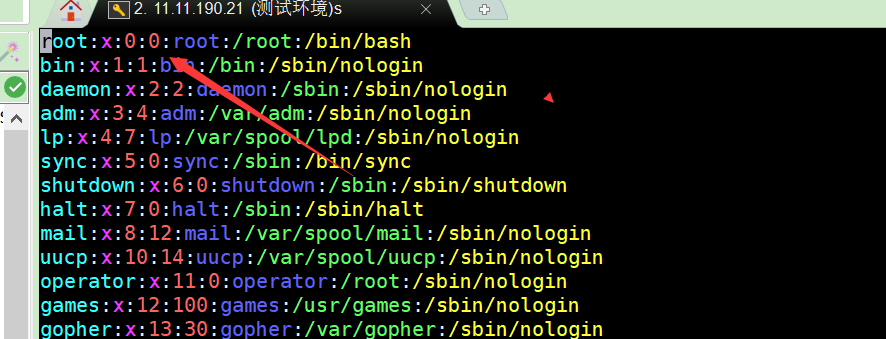
## CVE-2017-16995 任意读写漏洞的说明



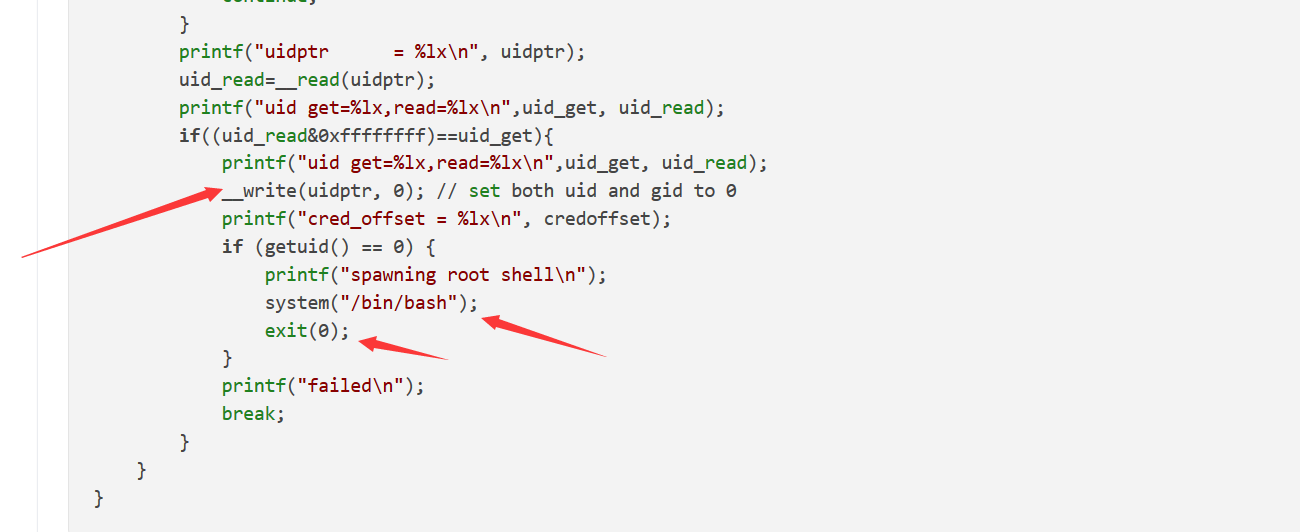
说明

漏洞利用的基础

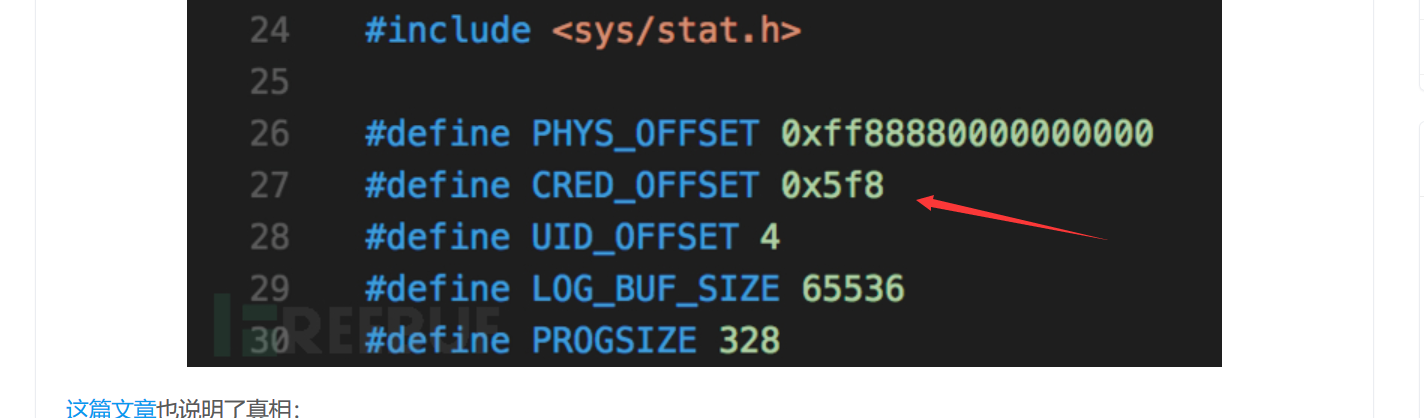
1. linux 的身份机制 是根据 这个shell的 uid中的值确定的,uid为 0 表示以root身份运行, uid查询可以在 /etc/passwd 进行查看



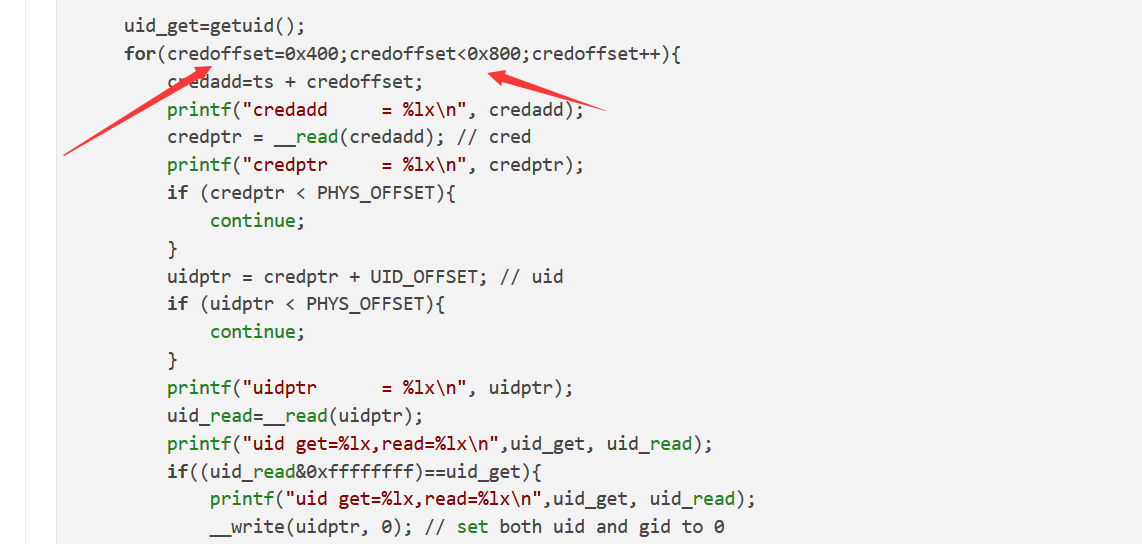
1. linux 允许用户bpf 与内核进行通讯,也就是说,利用bpf 这个机制 查找到uid的位置,将uid修改为 0,则用户就以root身份运行了



1. 如果要 修改uid的值,我们首先要知道他在哪里,
   1. 通过 cred结构体,则可以获取到uid的内存地址



* 1. 或者是进行内存遍历,通过某一个特征值,查找这个cred\_offset的位置,前提是 cred\_offset的值是固定的几个,cred\_offset的值是和 linux内核版本有关



由于 系统的运行内存是在低地址处,所以搜索的范围是在低地址出

4.漏洞的操作步骤,是 利用bpf漏洞,获取内核权限,然后进行内存查找,确定uid的内存地址,修改的uid的值为0, 设置 用户运行的shell /bin/bash,提权结束

参考文档

<https://www.cnblogs.com/rebeyond/p/8921307.html>

<http://www.freebuf.com/vuls/168980.html>