BUUCTF Reverse reverse2 WriteUp

原创

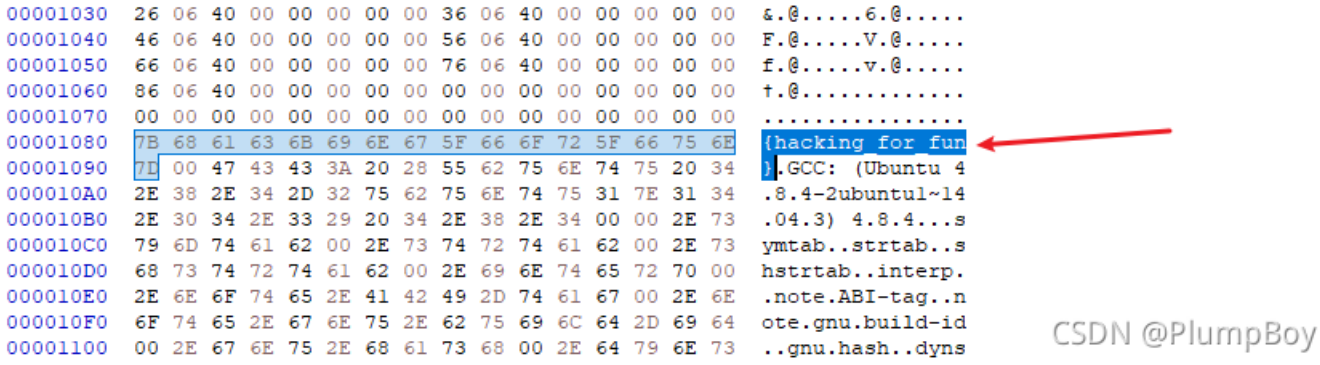
PlumpBoy 于 2021-09-10 18:35:53 发布 24 收藏

分类专栏： BUUCTF 逆向题解 文章标签： linux 系统安全 安全 经验分享

本文链接：https://blog.csdn.net/weixin_45723661/article/details/120227810

reverse_2

拖入HxD中看见ELF，linux平台的程序，但是懒得开虚拟机了，顺手搜索了一下，看见了一个很像flag的字符串，结果提交试了下，错误的，**那么应该是程序对这个字符串做了一些操作。**



拖入IDA

```
v8 = __readfsqword(0x28u);
  pid = fork();
  if ( pid )
  {
    waitpid(pid, &stat_loc, 0);
  }
  else
  {
    for ( i = 0; i <= strlen(&flag); ++i )
    {
      if ( *(&flag + i) == 'i' || *(&flag + i) == 'r' )
        *(&flag + i) = '1';
    }
  }
  printf("input the flag:");
  __isoc99_scanf("%20s", s2);
  if ( !strcmp(&flag, s2) )
    result = puts("this is the right flag!");
  else
    result = puts("wrong flag!");
  return result;
}
```

核心就是for循环，它对flag字符串进行了转换，再与输入进行比较。通过查询发现flag就是我们上面找到的字符串。写个程序将其输出就可以了。

```
#include<iostream>
#include<stdio.h>
using namespace std;

int main()
{
 char a[] = "hacking_for_fun";
    for (int i = 0; i <= 15; ++i)
    {
        if ( a[i] == 'i' || a[i] == 'r')
                a[i] = '1';
        cout << a[i];
    }
 return 0;
}
```

```
hack1ng_fo1_fun
D:\C++\20210522\Project1\Debug\Project1.exe (进程 16136)已退出，代码为 0。
按任意键关闭此窗口. . .
```