计算机安全导论实验

堆栈溢出攻击

16030130096 田宝林

babydragon.top

2019 年 4 月 5 日

Outline

Outline

```
1  #include <cstdio>
2  int add(int a, int b, int c){
3      return a+b+c;
4  }
5
6  int main(){
7      int a=2, b=3, c=3;
8      int ans = add(a, b, c);
9      printf("%d\n", ans);
10     return 0;
11 }
```

Listing 1: 函数的调用机制

内存示意图

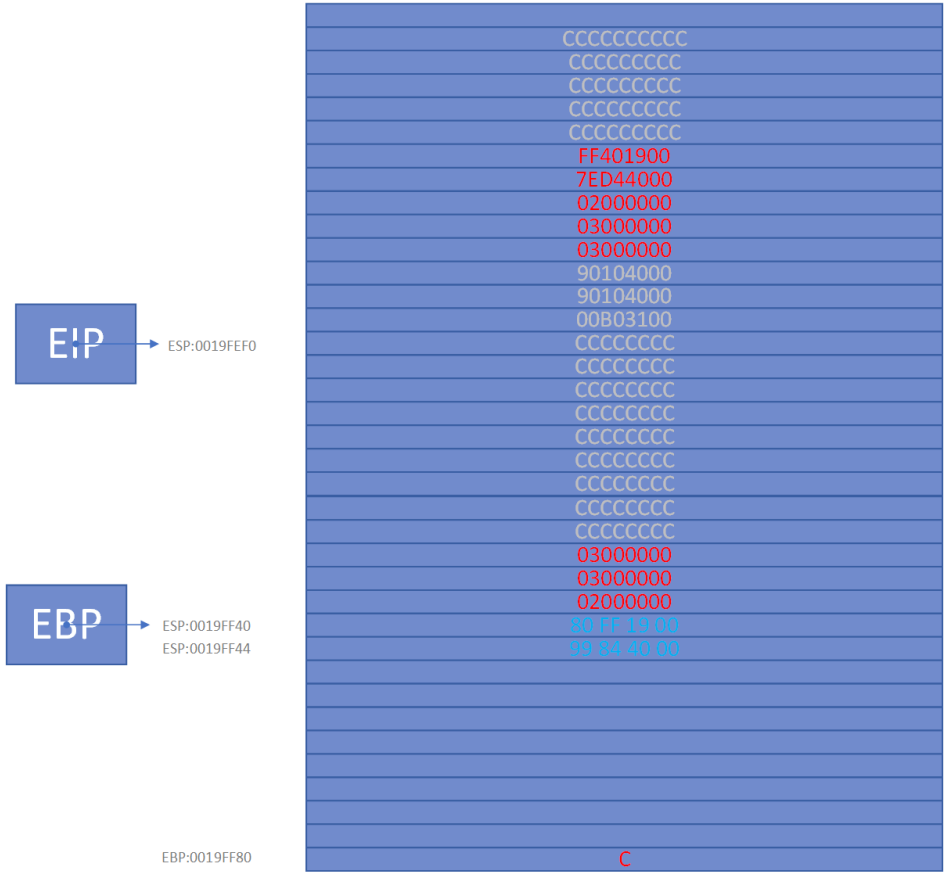

图: 内存示意图

简化图

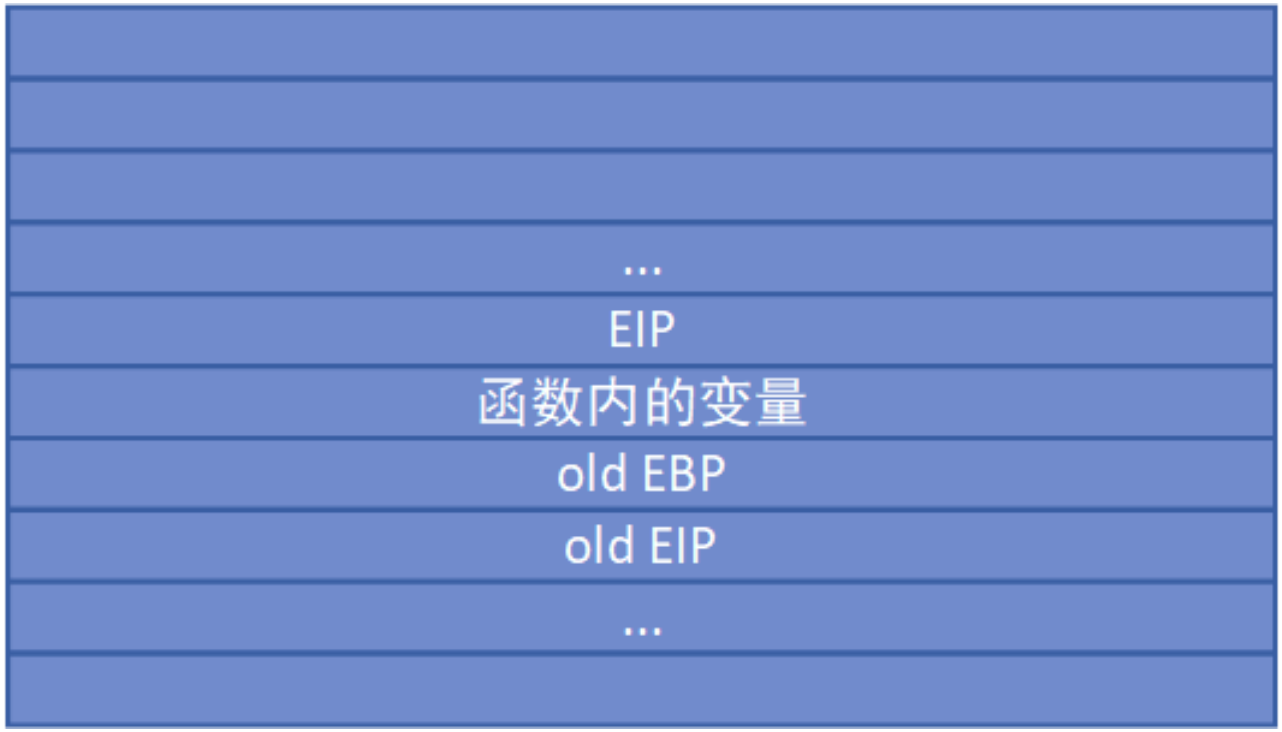

图: 简化图

Outline

Q:如何输出win?

- How to win?

```
1  #include <cstdio>
2  #include <iostream>
3  using namespace std;
4  int main()
5  {
6      int cookie;
7      char buf[8];
8      printf("%08x␣␣%08x\n", &cookie, &buf);
9      printf("%d\n", cookie);
10     gets(buf);
11     if(cookie == 0x41424344)
12         printf("win\n");
13     printf("%08x\n", cookie);
14     return 0;
15 }
```

Listing 2: How to win

Outline

Q：如何进入hacked函数

```
1  #include <stdio.h>
2  #include <string.h>
3  #include <stdlib.h>
4  void copy(char* input){
5      char var[20];
6      strcpy(var, input);
7  }
8  void hacked(){
9      printf("Can you see me now?\n");
10 }
11 int main(){
12     char n[100];
13     char source[] = "";
14     copy(source);
15     return 0;
16 }
```

Listing 3: How to win

Outline

Q：如何设置一段代码，使得我们能够打开一个计算器？

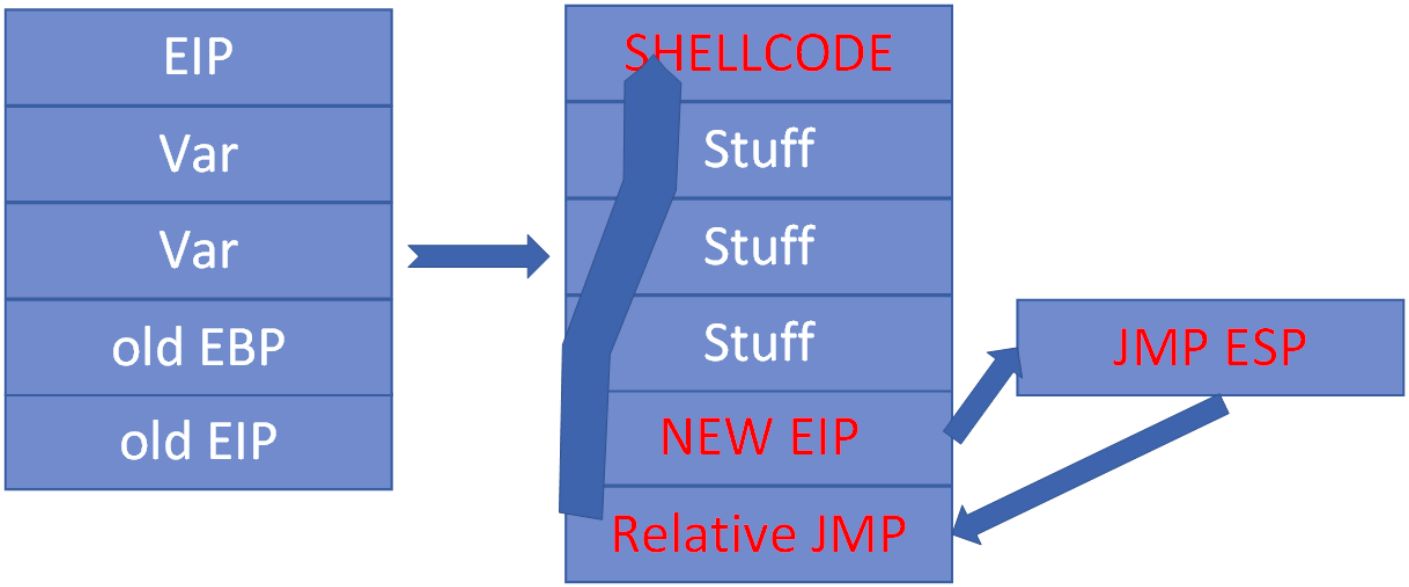

图: 逻辑转移示意

code

```
1  #include "stdio.h"
2  #include "stdlib.h"
3  #include "string.h"
4  int main() {
5      char name[512];
6      printf("Reading␣name␣from␣file...\n");
7      FILE *f = fopen("E:\\security␣test\\name.dat", "rb");
8      if (!f) return -1;
9      fseek(f, 0L, SEEK_END);
10     long bytes = ftell(f);
11     fseek(f, 0L, SEEK_SET);
12     fread(name, 1, bytes, f);
13     name[bytes] = '\0';
14     fclose(f);
15     printf("Hi,␣%s!\n", name);
16     //DWORD dwOld=0;
17     //VirtualProtect(name,516,PAGE_EXECUTE_READWRITE,&dwOld);
18     system("pause");
19     return 0;
20 }
```

- new EIP该怎么设置能够跳到shellcode呢？

- new EIP该怎么设置能够跳到shellcode呢？
- 编写shellcode

- new EIP该怎么设置能够跳到shellcode呢？
- 编写shellcode
- 汇编语言–机器代码

- new EIP该怎么设置能够跳到shellcode呢？
- 编写shellcode
- 汇编语言–机器代码
- python生成

提问时间

需要的软件

- *vc 6.0*
- *Ultraedit*
- *Spyder*
- *odllydbg*

参考链接

堆栈溢出攻击–弹出计算器堆栈溢出攻击–弹出计算器