2023-2024软件安全期末考试

选择题

1.5分一个，20个

主要考察雨课堂课后题和ppt上的一些加粗字体的内容

判断题

1分一个，20个

主要考察雨课堂课后题和ppt上的一些加粗字体的内容

简答题

7个，34分

1.有关于栈溢出

```
void why_here(void)
{    printf("why u r here?!\n");
      exit(0);
}
void f()
{     int buff; int * p = &buff;
       ________= (int)why_here;
}
int main(int argc, char * argv[])
{      f();
        return 0;
}
```

问你怎么写代码，然后让你画出对应的栈示意图，但是稍微做了改动

2.两种破解方法

```
#include <iostream>
using namespace std;
#define password "12345678"
bool verifyPwd(char * pwd)
{
    int flag;
    flag=strcmp(password, pwd);
    return flag==0;
}
void main()
{
    bool bFlag;
```

```
    char pwd[1024];
    printf("please input your password:\n");
    while (1)
    {
        scanf("%s",pwd);
        bFlag=verifyPwd(pwd);
        if (bFlag)
        {
            printf("passed\n");
            break;
        }else{
            printf("wrong password, please input again:\n");
        }
    }
}
```

3.写出符号执行的三步骤；写出静态和动态分别的优缺点

4.写出pintool的原理，和对应插桩的四种类型

5.

```
#include <stdio.h>
int main(int argc, char *argv[])
{
    char str[200];
    fgets(str,200,stdin);
    printf(str);
    return 0;
}
```

写出两种模式下的栈帧形态

6.

```
<h1 align=center>--Welcome To The Simple XSS Test--</h1>
<?php
ini_set("display_errors", 0);
$str =strtolower( $_GET["keyword"]);
$str2=str_replace("script","",$str);
$str3=str_replace("on","",$str2);
$str4=str_replace("src","",$str3);
echo "<h2 align=center>Hello ".htmlspecialchars($str).".</h2>".'<center>
<form action=xss_test.php method=GET>
<input type=submit name=submit value=Submit />
<input name=keyword  value="'.$str4.'">
</form>
</center>';
?>
```

```
</body>
</html>
```

此代码有什么漏洞?

分析对应的两种漏洞的利用方法：img和script

7.C++虚表指针，虚表，内存空间的关系？写出虚函数攻击的对应方法?

综合题

8分一个，一共16分

1.shellcode的编码：

为什么要编码?

说出一种编码类型

然后分析代码，填写代码

```
int main(){
   __asm  {
     call lable;
     lable: pop eax;
        add eax, 0x15             ;越过decoder记录shellcode起始地址
        xor ecx, ecx
    decode_loop:
        mov bl, [eax + ecx]
        xor bl, 0x44              ;用0x44作为key
        mov [eax + ecx], bl
        inc ecx
        cmp bl, 0x90              ;末尾放一个0x90作为结束符
        jne decode_loop
    }
    return 0;
}
```

需要填写　call lable; 和　　jne decode_loop

2.ROP返回导向编程

ROP基本思想?

```
ESP -> ???????? => POP EAX # RETN
            ffffffff => we put this value in EAX
            ???????? => INC EAX # RETN
            ???????? => XCHG EAX,EDX # RETN
```

分析EDX的值

然后是一个实践题，让你将EAX的值变为7，写ROP代码进行地址的调用