ISCC2014 Basic（基础关）Writeup

原创

RickGray 于 2014-06-14 23:55:38 发布 3432 收藏
分类专栏： CTF纪实 文章标签： 技术

第一次参加ISCC（泪奔），整个过程下来还是学到了不少，接触了不少以前没有遇到过的技术。

下面给出Basic的简要题解，若有不对，还望大牛们指出 :-)

0x00 兵者诡道 Score：50

兵者，诡道也。故能而世之不能，用而示之不用，近而示之远，远而示之近。孙子在下命令中为防敌军窃取情报玩了一个小把戏。你能找出隐藏在这个文件中的密码么？

思路：进入关卡页面后什么都没有，只有个Tips：”hello,guess where is the key???”，果断在firebug里一阵狂搜，在Http响应头中找到flag。

flag：Welcome-to-ISCC

0x01 知己知彼 Score：50

知彼知己者，百战不殆；不知彼而知己，一胜一负；不知彼不知己，每战必殆。孙子手下将士截获了敌军命令密文4545 424545454542 454542 42 424542 424545，你能解密成明文，做到知己知彼吗？

思路：根据密文格式，可以看出整体就两个数45和42，对应ascii字符为”-“和”*”，顿时想到摩斯密码，将对应的摩斯密码”-- .-- --. --. ..-. .--“解密为” MWGGERK”，提交答案，提示错误，再解密，经过简单处理，通过移位得到明文”ISCCANS”，改为小写提交，成功。

flag：isccans

0x02 正则指令 Score：50

不知军之不可以进而为之进，不知军之不可以退而谓之退，是谓縻军。

正则表达式是“行军作战指挥命令”的一项“准则”，可帮助将领减少错误的下达指令的概率。请分析这段正则表达式，看看它透露了什么信息？正则表达式如下

\bw{3}(?<x>\.)[xyz](?<3>o)(?<2>u)t\k<2>[bc][de]\k<x>c\3m\/watch\?v\=5x1vNTjbwcs\&list\=PL3ZQ5CpNulQm1cXMJ5M6tX3O5vyXnCYFd\b

提示:标题即flag

思路：作为小菜的我，这么复杂的正则表示看着就头大，但是明显可以看出是个url，通过google正则关键部分（PL3ZQ5CpNulQm1cXMJ5M6tX3O5vyXnCYFd）可以知道该正则是一个Youtube视频的地址-http://www.youtube.com/watch?v=5x1vNTjbwcs&list=PL3ZQ5CpNulQm1cXMJ5M6tX3O5vyXnCYFd，于是打开该地址，提交视频标题即可。（ps：小菜我开始做此题的时候，没有提示，在提交标题时多了个空格，搞得半天不懂这题要提交什么---，甚是郁闷）

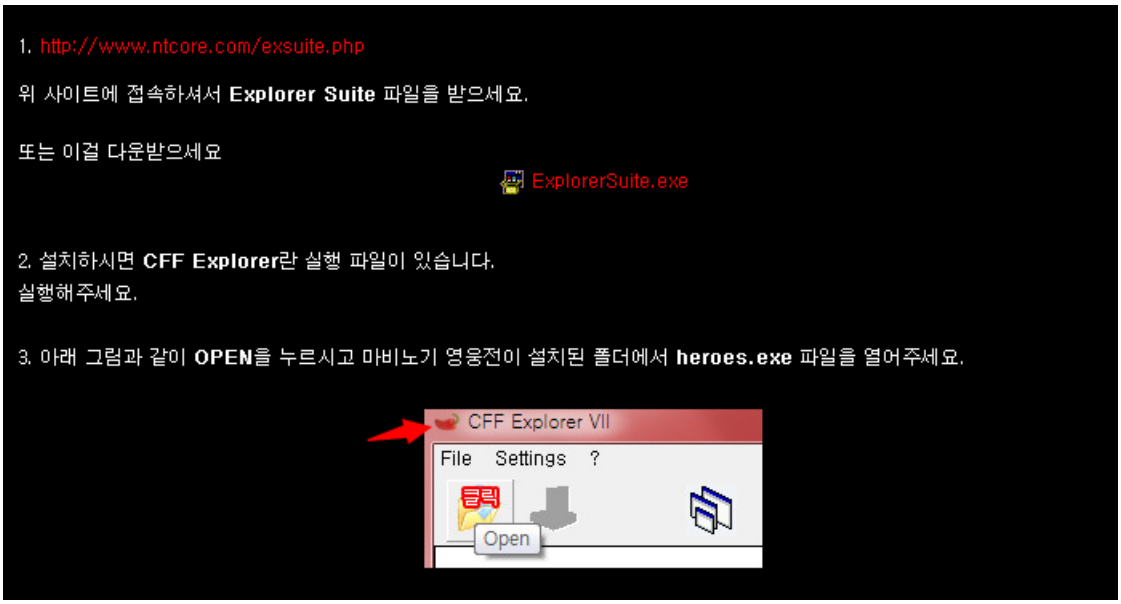
flag：Chilehit by an 8.2 magnitude earthquake

0x03 搜索情报 Score：50

孙子曰：“是故智者之虑，必杂于利害。杂于利而务可信也，杂于害而患可解也。”

现在有《Windows exploitation in 2013》，文章里面的一款PE工具貌似挺强大的，你能收集到情报，找到这款软件的名字吗？

http://www.welivesecurity.com/2014/02/11/windows-exploitation-in-2013/
思路：题目给了网址，果断打开，发现是英文（--我等屌丝怎么看得懂），泛读一顿后，发现文章底部有个Process Explorer Tool，提交之，错误。然后发现文章中有张图片中有个软件很可疑没有名字，于是各种google、baidu中，发现了下面这个思密达网址-http://sekainonaka.tistory.com/167，果断入之，发现里面讲的就是那软件-CFF Explorer，成功过之。



flag：CFFExplorer

0x04 指令暗战 Score：50

孙子曰：“凡军之所欲击，城之所与攻，人之所欲杀，必先知其守将，左右，谒者，门者，舍人之姓名，令吾间必索知之。”我们派到敌方内部间谍拿到了敌军作战的指令，但是还不够明确，请你将消息确切转化为细致的机器码，并提交（不需空格）。

MOV AX,CS

MOV DS,AX

MOV ES,AX

MOV CX,0020H

MOV DX,1004H

MOV BX,000CH

MOV AX,2300H

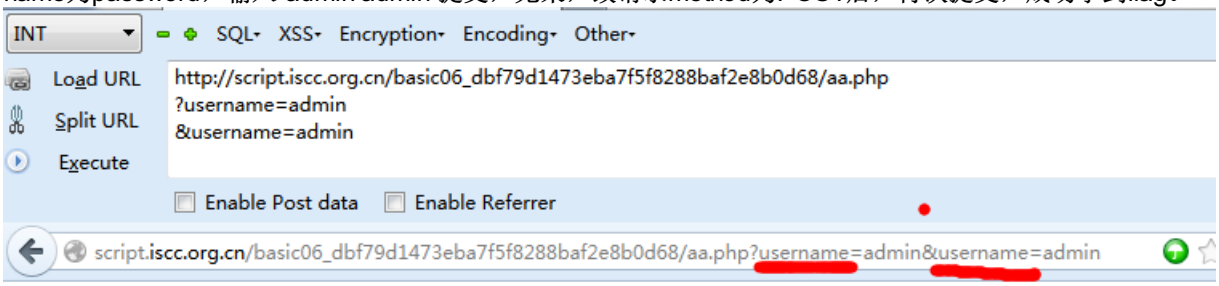
提示:提交时用大写即可

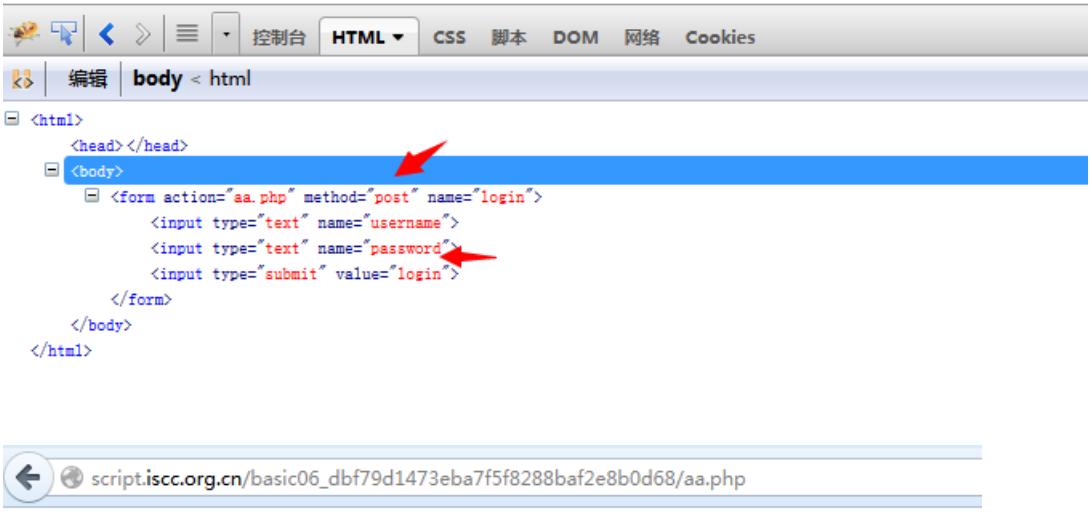
思路：此题一个基本的shellcode转换问题，直接将汇编代码对应的机器码（十六进制表示）写出即可，通过任何方式都可，小菜我是通过直接在debug里面-a输入汇编代码看的- -|，大牛勿喷。（ps：此题一开始无提示，看到题目中都全大写，我们答案肯定也得大写啦）
flag：8CC88ED88EC0B92000BA0410BB0C00B80023

0x05 巧入军营 Score：50

故曰：“知己知彼，胜乃不殆；知天知地，胜乃不穷。”请运用基础的“技巧”登陆此敌军页面，拿到flag。

思路：进入关卡页面后，发现是个畸形的登陆页面，随便输入后，发现两个input框变量名一样-同为username，So，改一个name为password，输入”admin admin”提交，无果，改请求method为POST后，再次提交，成功拿到flag。





key: 4qrPccxPe9

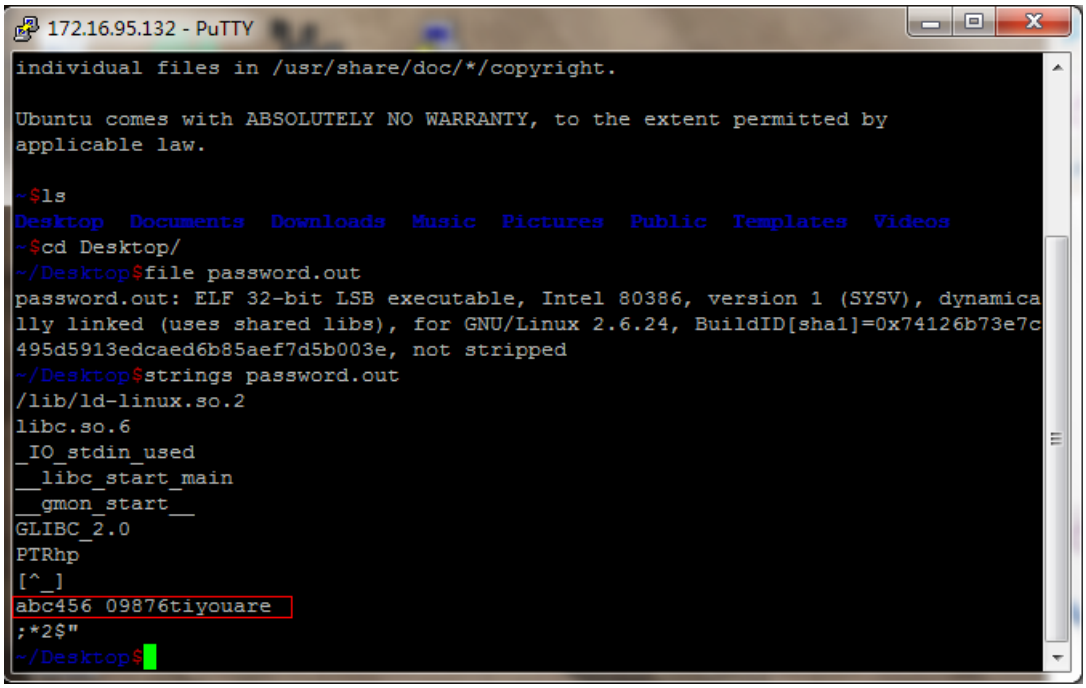
flag：4qrPccxPe9

0x06 知兵之将 Score：50

孙子曰；“故知兵之将，生民之司命，国家安危之主也。”

行军打仗最基础的是令行禁止，但知兵之将却要下达最正确的指令给他所带领的军队。请用最基础的linux命令，获得flag，证明你是知兵之将。

思路：down下文件后，二话不说，用file命令查一下，发现是elf文件-32位（ps：.out文件一般为*unix系统下由gcc/g++自动编译连接生成的可执行文件），运行一下发现没有输出，于是用strings命令搜索下该程序中有没有什么字符串，果然！让我发现了秘密。

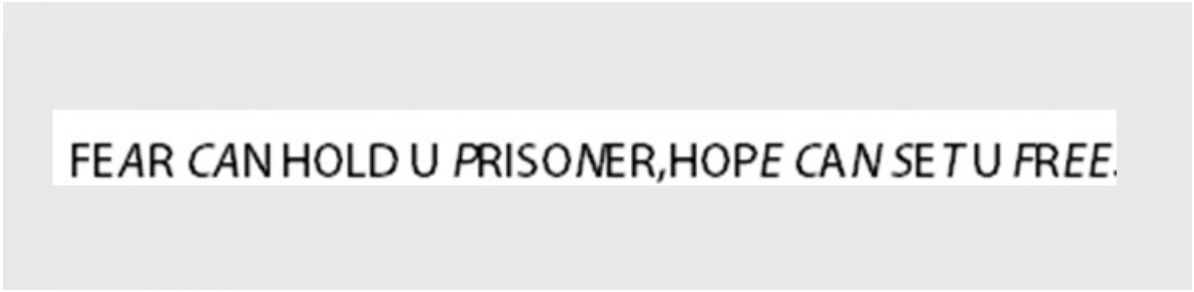


flag：abc456_09876tiyouare

0x07 虚实密文 Score：50

孙子曰：“故策之而知得失之计，作之而知动静之理，行之而知死生之地，角之而知有余不足之处。”

截获敌军情报是掌握敌军动向的一个好方法，也许这种加密方法可能不多见，但是只要能看破密文中的虚虚实实的消息，就能拿到我们所希望的信息。



思路：文件down下来之后，发现是一张png，于是各种分析无果后，发现图片中的那句话穿插着字母正体和斜体，网上搜索一下，发现是培根密码（ps：大家自行搜索普及一下），于是根据培根密码的加密方法，正体为a，斜体为b，转化成如下编码：aaba bba aaaa a baaaabaa, aaab bab bab a babb，再将其每5个分为一组：aabab|baaaa|aabaa|aabaa|aaabb|abbab|ababb，通过查培根编码表可以得到明文：freedom。

flag：freedom

0x08 经之五事索其情 Score：50

孙子曰：“故经之以五事，校之以计而索其情：一曰道，二曰天，三曰地，四曰将，五曰法。”

你是否熟悉RSA算法？敌军正在用RSA算法加密，但是防范不周，被我军获取了部分信息。请解密密文是981，w = 13，n = 2537，分解式的一个因子是43的明文。

思路：题目说了是RSA加密（ps：大二学了密码学，当时做题的时候哈都不知道- -|），对着加解密公式，将变量带入即可，此题难道较低，最后算得结果-702。（参考文章：http://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html）

flag：704

0x09 趁虚而入 Score：100

孙子曰：“攻其不备，出其不意。此兵家之胜，不可先传也。”我方能不能借助敌人的指挥系统来获得信息，混入敌方内部绝对是一个不错的方法。现在由于对方的疏忽，我们可以现在已有“握手口令”（握手包），请你帮助我方统帅搞定密码吧！

思路：根据题目描述，down下来的附件中包含有一个handshake，利用软件EWSA进行跑包即可（ps：此题密码较弱，不需要自行添加字典，使用软件默认即可），跑出密码：zzzzzzzz。

flag：zzzzzzzz

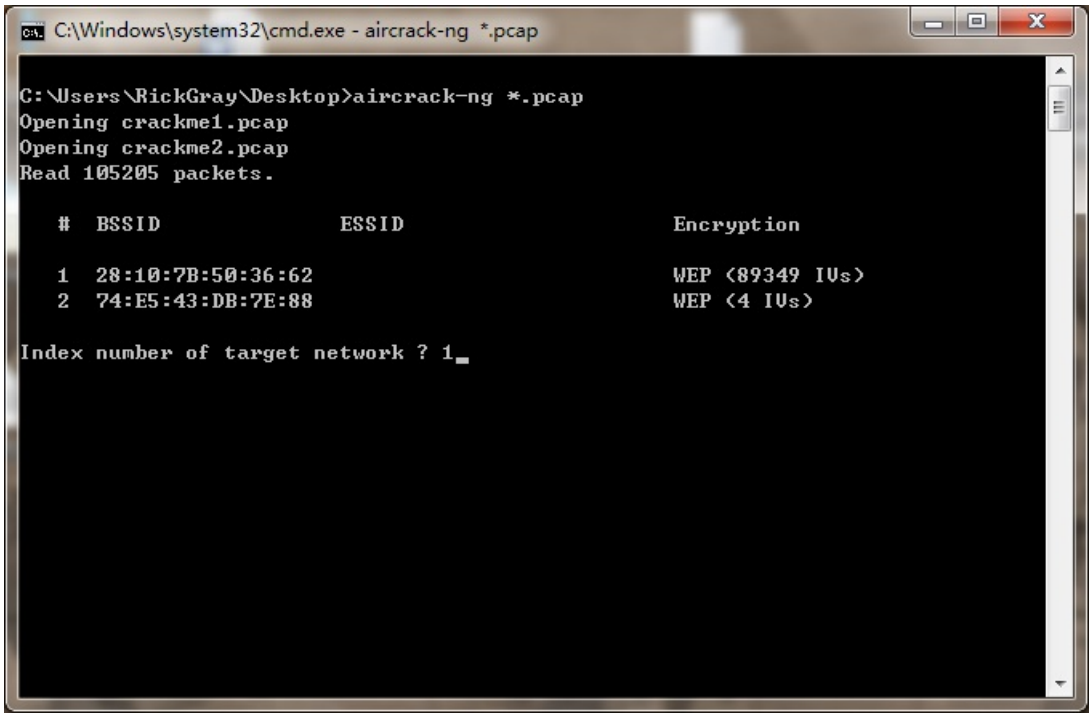
0x0a 出其不意 Score：100

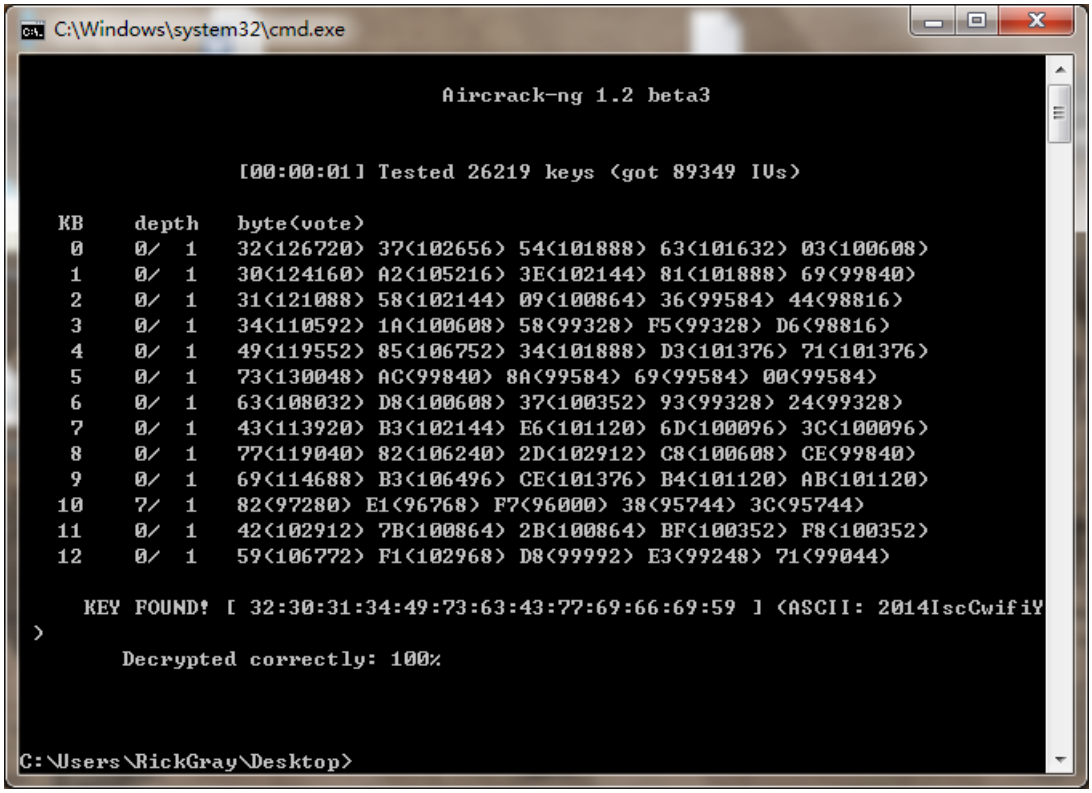
孙子曰：“出其所不趋，趁其所不意。”

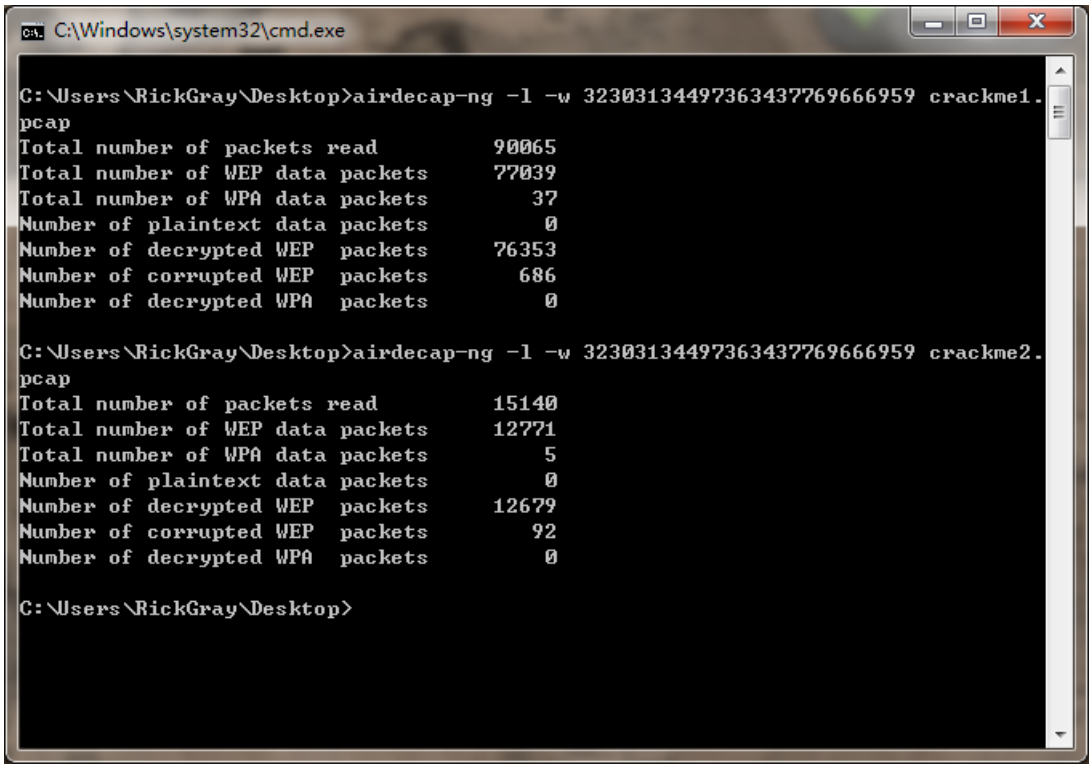
敌方居然把WIFI设成了ChinaUnicom，还真是出乎了我方的意料，但最终还是被我方发现了，并且我们发现他们用WEP加密,既然如此，那么就破解了他吧！从数据包中找到某人用ISCC账号通过该Wifi登录www.bitunion.org的密码。

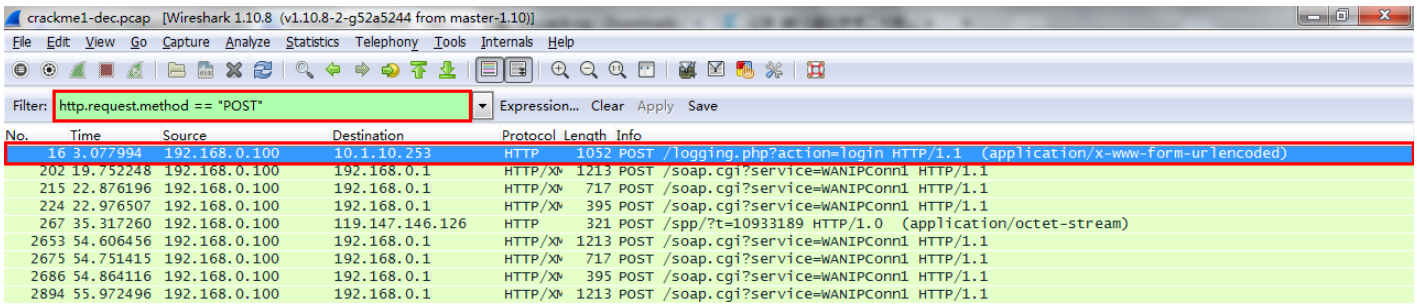
思路：题目给了两个.pkt的网络流量包，根据题意解题步骤应该是：首先破解wep的密码，然后从网络流量中找到该人用ISCC账号登陆www.bitunion.org的密码。

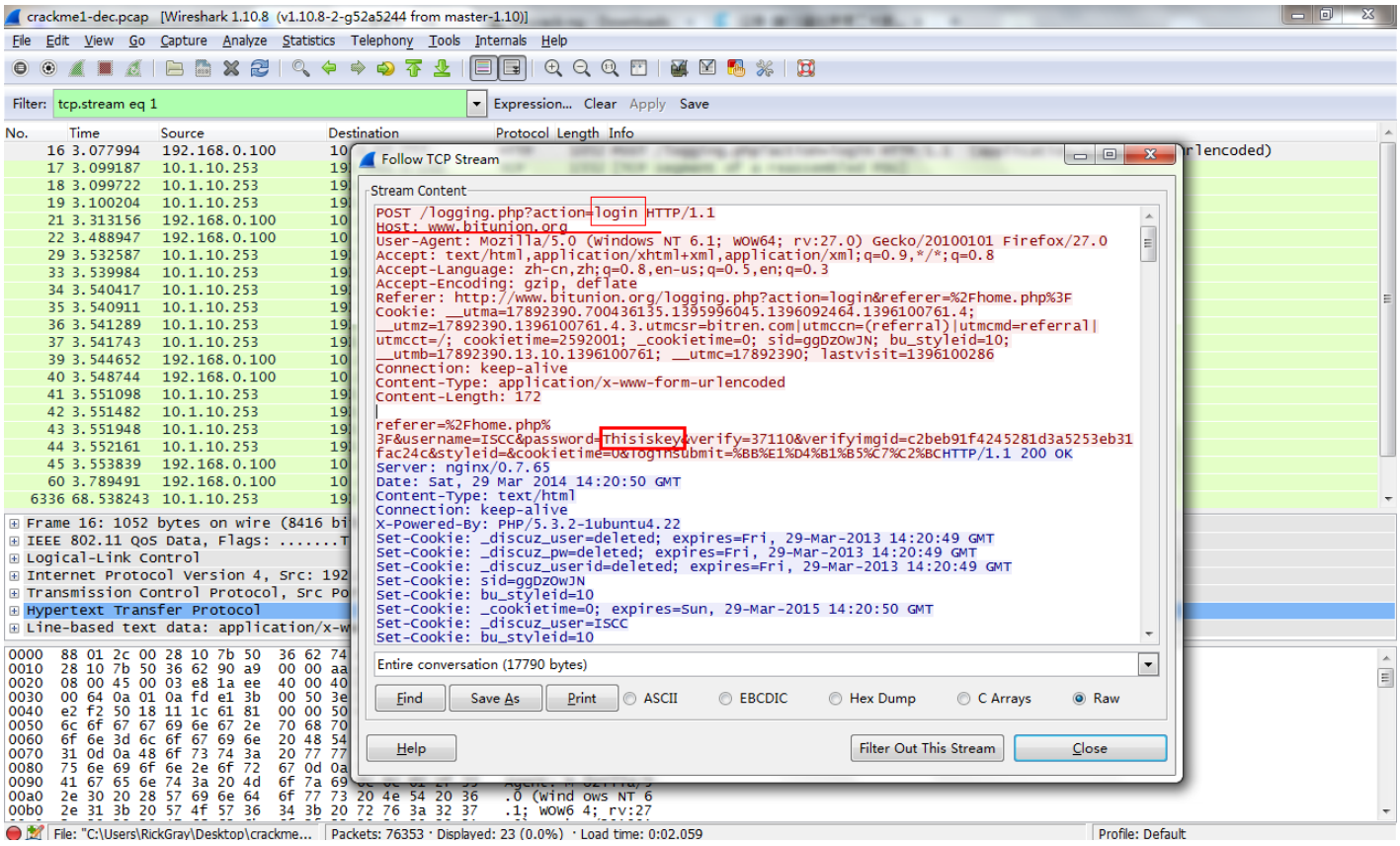
解题步骤，先将两个.pkt包转成.pcap格式，然后使用aircrack-ng 破解wep密码，再使用airdecap解密两个加密了的数据包，在里面搜索http协议的包，即可找到密码。


C:\Windows\system32\cmd.exe - aircrack-ng *.pcap
C:\Users\RickGray\Desktop>aircrack-ng *.pcap
Opening crackme1.pcap
Opening crackme2.pcap
Read 105205 packets.
BSSID ESSID Encryption
1 28:10:7B:50:36:62 WEP (89349 IVs)
2 74:E5:43:DB:7E:88 WEP (4 IVs)
Index number of target network ? 1


C:\Windows\system32\cmd.exe
Aircrack-ng 1.2 beta3
[00:00:01] Tested 26219 keys (got 89349 IVs)
KB depth byte(vote)
0 0/ 1 32(126720) 37(102656) 54(101888) 63(101632) 03(100608)
1 0/ 1 30(124160) A2(105216) 3E(102144) 81(101888) 69(99840)
2 0/ 1 31(121088) 58(102144) 09(100864) 36(99584) 44(98816)
3 0/ 1 34(110592) 1A(100608) 58(99328) F5(99328) D6(98816)
4 0/ 1 49(119552) 85(106752) 34(101888) D3(101376) 71(101376)
5 0/ 1 73(130048) AC(99840) 8A(99584) 69(99584) 00(99584)
6 0/ 1 63(108032) D8(100608) 37(100352) 93(99328) 24(99328)
7 0/ 1 43(113920) B3(102144) E6(101120) 6D(100096) 3C(100096)
8 0/ 1 77(119040) 82(106240) 2D(102912) C8(100608) CE(99840)
9 0/ 1 69(114688) B3(106496) CE(101376) B4(101120) AB(101120)
10 7/ 1 82(97280) E1(96768) F7(96000) 38(95744) 3C(95744)
11 0/ 1 42(102912) 7B(100864) 2B(100864) BF(100352) F8(100352)
12 0/ 1 59(106772) F1(102968) D8(99992) E3(99248) 71(99044)
KEY FOUND! [32:30:31:34:49:73:63:43:77:69:66:69:59] (ASCII: 2014IscCwifiY
)
Decrypted correctly: 100%
C:\Users\RickGray\Desktop>







flag:Thisiskey

0x0b 择人任势 Score：100

孙子曰：“故善战者，求之于势，不责于人，故能择人而任势。”现有一vbs文件，你能从中找出理想的flag吗？

思路：down下题目附件，是一个vbs脚本（ps：vbs没有学过！！），用编辑器打开，发现格式非常糟糕，经过代码调整和分析，可以知道，他使用excute()函数执行了关键语句，将它的str逆序过来观察后，得到如下代码：

```
dim tbl,pwd,err,str,i,x
tbl=split("56|117|149|186|125|5|37|205|230|121|184|173|82|98|237|6|222|192|141|132|131|53|133|118|188|143|1
pwda=split("94|45|144|52|118|22|46|88|-39|-37|38|127|-11|-45", "|")
pwdb=split("157|24|6|107|251|35|94|67|136|199|12|34|97|202|188|31","|")

err="密码错误！"
ok="你输入的密码就是KEY！"
x=0:a=0:b=0
str=inputbox("查看KEY请输入密码","","")

if (len(str)=14) then
for i=0 to 13
if Int(asc(mid(str,14-i,1))+pwda(i))=Int(tbl(i+pwdb(i))) then
x=x+1
exit for
end if
next
if x=14 then
msgbox ok
end if
else
msgbox err
end if
```

可以看到，匹配部分在for循环那里，我们改一下程序，使它不进行比较，直接输出tbl(i+pwdb(i)))-pwda(i)即可，得到数据序列：xxx，将其逆序就是flag了。

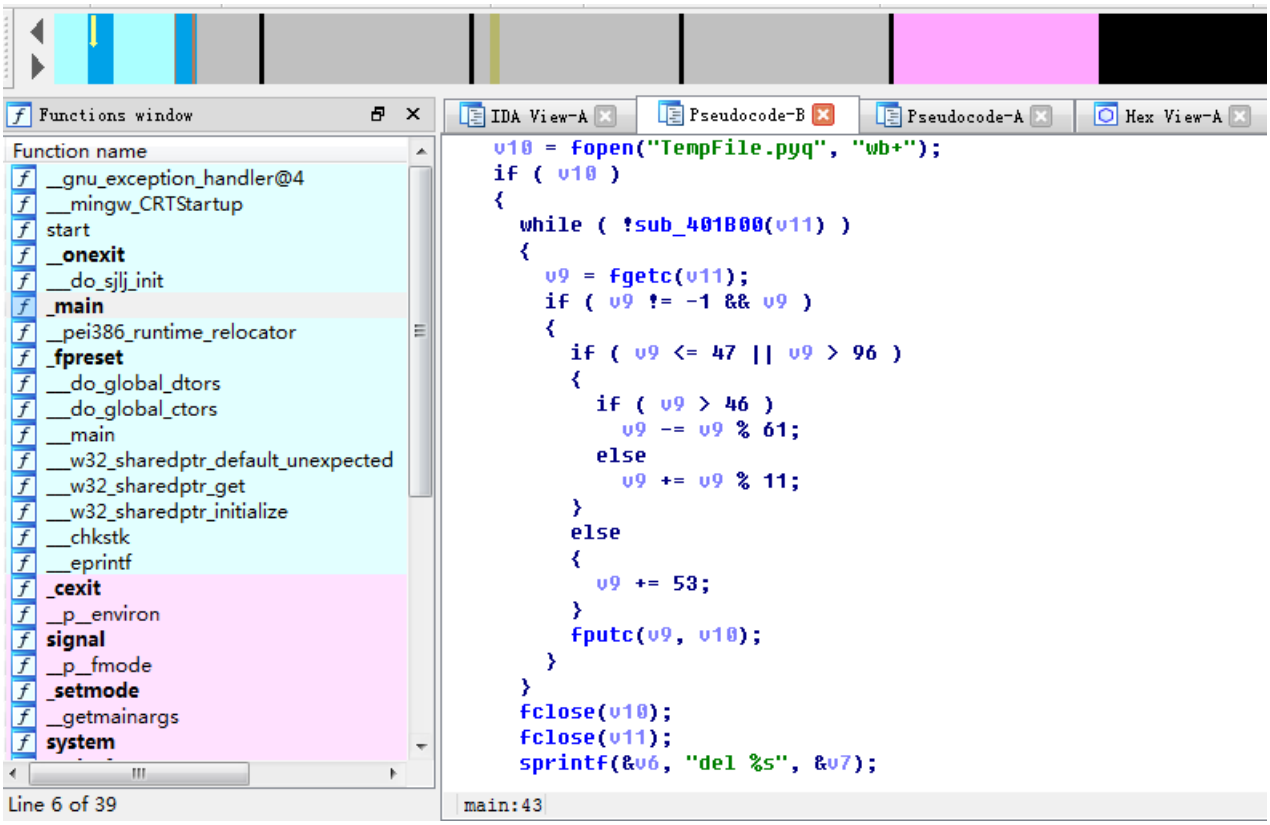
flag：vB5_5cR1pT.Vb$

0x0c 庙算多寡，胜负定矣 Score：100

孙子曰：“夫未战而庙算胜者，得算多也；未战而庙算不胜者，得算少也。”

在一次作战中，你获得了对方用于加密的文件，和密文“+%=keky+%=jjnx”这也许关系到敌人的下一步作战行动，你能否将此密文通过从加密文件中获得信息，把密文给解密出来？

思路：down下附件，是个exe程序，运行之，发现是个简单的加密程序，果断载进IDA分析。载入IDA后，发现该程序可以成功的F5，于是分析他的代码，发现了关键的加密部分（简单说明：每次读取待加密文件中的一个字符，经过处理，映射到另一个字符上），分析清楚后，小菜我用python写了个简单的爆破程序，去爆明文，得到明文”&#a606D&#a5579”，但是提交发现不对，仔细看了下明文发现606D是十六进制，于是把a改为x后，在html中可以成功显示-“恭喜”，但题目只需提交”&#x606D&#5579”即可。



爆破程序如下：

```
code = '+%=keky+%=jjnx'
codelist = []
for i in code:
    codelist.append(ord(i))

result = ''
offset = 0
codedic = []

for i in codelist:
    codedic.append({offset: []})
    for k in range(256):
        x = k
        if x <= 47 or x > 96:
            if x > 46:
                x -= x % 61
            else:
                x += x % 11
        else:
            x += 53

        if x == i:
            result += chr(k)
            #print 'Found the %s nume: %s' % (offset, k)
            codedic[offset][offset].append(chr(k))
            break
    offset += 1

print 'S: %s' % code
print 'M: %s' % result
```

flag：&#x606D&#5579