

实验吧 杂项

转载

[weixin_34087307](#) 于 2017-12-08 14:20:00 发布 774 收藏

文章标签: [php](#) [运维](#) [python](#)

原文链接: <https://yq.aliyun.com/articles/654417>

版权

1. xor解密:

lovelovelovelovelovelovelove

```
◆◆◆V◆◆◆
```

```
◆◆
```

```
◆0◆
```

```
◆0◆
```

```
◆0◆◆
```

```
◆◆◆◆◆◆
```

```
# -*- coding:utf-8 -*-  
a =open('1.txt','rb').read()  
b =open('2.txt','rb').read()  
lut = ''  
for i in range(0,len(a)):  
    res =ord(list(a)[i]) ^ord(list(b)[i])  
    lut=lut +chr(res)  
print lut
```

2.
竟然有个神奇的加密方式和蛇有关 <http://serpent.online-domain-tools.com/>, 记录下网址
- 3.

```

defrevStr(s):
    news=' '
    foriinrange(0,len(s),4):
        news += s[i+2:i+4]
        news += s[i:i+2]
    returnnews

deffoo():
    f=open('1')
    s='377a'
    forlineinf:
        s+=revStr(line.strip()[8:].replace(' ',''))
    fsave=open('1.txt','wb')
    fsave.write(s)
    fsave.close()
    pass

if__name__=='__main__':
    foo()

    print 'finished'

```

7z脚本，加上文件头，并把换行，序号去掉，每四个数前俩和后俩交换位置。但是最后储存的时候，还需16进制导入010再另存为.7z格式

4.

用processing将16进制转换为图片。

```

size(256,256);

String[] str = loadStrings("1.txt");

for(int i=0;i<65536;i++){

    if(str[0].charAt(i)=='1'){

        point(i/256,i%256);}

}

```

5. BAT公司信息查询系统

这个题怪扎心的，点进去是一个表单，无论提交什么都出现同样的东西。查看页面源代码，就两个可以点的一个css和一个php，php点开什么都没有，点开css找到了一个图片，加在url后面得到一张二维码的图片，扫描二维码得到一个txt，里面有个奇奇怪怪的东西，还有个php，加在后面，然后更奇怪的出来了：十攏數倉整燿煥敵嗟V灯捲≤-|>，据说这个是ansi编码，需要另存为unicode编码然后再用010导入的方式打开就行了。（不知道为什么我另存的时候需要换个名字，要不以16进制打开的方式还是会错。）

6. 抓到了你

打开wireshark，ping用的协议是icmp，所以过滤条件就写icmp，依次查看报文，发现第二条有data，而且是16字节，就是他。

7. 2015RCTF (misc50)

腊鸡题看代码看的我眼疼，下载下来之后拖进010里面，发现是个rar，改后缀名，用sublime打开，是sqlmap跑出来的东西。ctrl+f搜索column_name爆字段名字的，这个的下面就是报flag的字段，

```
UNMS%29%HERE%20table_name%3D0x66c6167%20AND%20table_schema%3D0x6d697363%20AND%20%20column_name%3D0x66c6167%20LIMIT%20%2C1%29%2C5%2C1%29%29%3E1%29%2C5%2C150%29 HTTP/1.1" 200 5 "-" sqlmap/1.0-dev (
http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:05 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%203720%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%29%2C1%29%29%3E51%29%2C5%2C3720%29 HTTP/1.1" 200 5 "-"
"sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:06 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%203720%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%29%2C1%29%29%3E48%29%2C5%2C3720%29 HTTP/1.1" 200 5 "-"
"sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:06 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%203720%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%29%2C1%29%29%3E49%29%2C5%2C3720%29 HTTP/1.1" 200 5 "-"
"sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:06 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%203720%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%29%2C1%29%29%3E51%29%2C5%2C3720%29 HTTP/1.1" 200 5 "-"
"sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:06 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%203720%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%29%2C2%2C1%29%29%3E1%29%2C5%2C3720%29 HTTP/1.1" 200 5 "-"
"sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:07 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%207500%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28Flag%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%28ORDER%28BY%20Flag%20LIMIT%20%2C1%29%2C1%29%29%3E64%29%2C5%2C7500%29
HTTP/1.1" 200 5 "-" "sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:07 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%207500%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28Flag%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%28ORDER%28BY%20Flag%20LIMIT%20%2C1%29%2C1%29%29%3E64%29%2C5%2C7500%29
HTTP/1.1" 200 5 "-" "sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:08 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%207500%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28Flag%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%28ORDER%28BY%20Flag%20LIMIT%20%2C1%29%2C1%29%29%3E80%29%2C5%2C7500%29
HTTP/1.1" 200 5 "-" "sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:08 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%207500%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28Flag%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%28ORDER%28BY%20Flag%20LIMIT%20%2C1%29%2C1%29%29%3E88%29%2C5%2C7500%29
HTTP/1.1" 200 5 "-" "sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:08 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%207500%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28Flag%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%28ORDER%28BY%20Flag%20LIMIT%20%2C1%29%2C1%29%29%3E82%29%2C5%2C7500%29
HTTP/1.1" 200 5 "-" "sqlmap/1.0-dev (http://sqlmap.org) "-"
192.168.52.1 - - [06/Nov/2015:19:33:08 -0800] "GET /phpcode/rctf/misc/
index.php?id=1%20AND%207500%3DIF%28%28ORD%28MID%28285SELECT%20IFNULL%28CAST%28Flag%20AS%28CHAR%29%2C0x20%29%20FROM%20misc.flag%28ORDER%28BY%20Flag%20LIMIT%20%2C1%29%2C1%29%29%3E82%29%2C5%2C7500%29
HTTP/1.1" 200 5 "-" "sqlmap/1.0-dev (http://sqlmap.org) "-"
```

从第一个flag到最后一个flag，url解码，会出现二分法爆flag表的flag字段内容，代表着每一位爆出来的字符的ascii码，将！=后面的数字拿出来ascii解码即可。

8. NSCTF misc250

这个题看的writeup，下载来的pcapng用wireshark打开，然后在左上角点击，文件—导出对象—http—save all 得到两个文件，一个是%5c,一个是压缩文件，压缩文件需要密码

我们先看%5c，仍winhex，发现是html,改后缀打开，告诉我们密码是nsfocus+5位数字

这应该就是rar的密码，直接掩码破解，还是很快的。然后打开rar压缩包就可以了。

9. deeeeeeeeeaaaadbeeeeeeeeeef-200

腊鸡火狐，图片根本打不开，换到谷歌里面，将图片保存，然后托到010里面，画图打开，根本看不懂啊，这个字怪酷的，看了下前面的信息图片是iPhone5拍摄的，查了下iphone5的分辨率，发现图片大小不一样，改一下就行了，然后就找到key了。

10.A记录

cap的数据包果断需要用wireshark分析.不过这里我们需要查询dns请求，所以需要解密cap（必须要有essid,password），甩到kali

```
root@kali:~# aircrack-ng '/root/Desktop/shipin.cap'
Opening /root/Desktop/shipin.cap
Read 16664 packets.

# BSSID          ESSID          Encryption
1 00:1D:0F:5D:D0:EE 0719          WPA (1 handshake)

Choosing first network as target.

Opening /root/Desktop/shipin.cap
Please specify a dictionary (option -w).

Quitting aircrack-ng

root@kali:~# aircrack-ng -w '/root/Desktop/lpass00.txt' '/root/Desktop/shipin.cap'
Opening /root/Desktop/shipin.cap
Read 16664 packets.

# BSSID          ESSID          Encryption
1 00:1D:0F:5D:D0:EE 0719          WPA (1 handshake)

Choosing first network as target.

Opening /root/Desktop/shipin.cap
Reading packets, please wait...

Aircrack-ng 1.2 rc4

[00:00:00] 12/22860 keys tested (262.14 k/s)

Time left: 1 minute, 27 seconds          0.05%

KEY FOUND! [ 88888888 ]

root@kali:~# airdecap-ng "/root/Desktop/shipin.cap" -p 88888888 -e 0719
Total number of packets read          16664
Total number of WEP data packets       0
Total number of WPA data packets      27
Number of plaintext data packets       0
Number of decrypted WEP packets        0
Number of corrupted WEP packets        0
Number of decrypted WPA packets        16
root@kali:~#
```

aircrack-ng这个命令挺强的，百度的时候看到了好多可以用来破解wlan的教程，本来想试下的，但是我没有无线网卡啊，这就很尴尬了。

解完有个新的cap，打开搜索dns就能看到了。

11.绕

打开题目链接是个表单，先查看页面源代码，发现了下面这一段

```
_=function $(){e=getEleByld("c").value;length==16^22a60b0b310e5ece$0ebe5)
{tU2FsdGS481hY7loIBh2Waw==nVkX1829IDS37Dtcv78qFewr eA/kNjZ1UZ6LuMTMoP2
[t,n,r,i];for(o=0;o<13;++o){[0];.splice(0,1)}}}'< onclick=$(>Ok!);delete _
",".docu.match(/"/);/)!=null=[" write(s[o%4]button if(e. ment';for(Y in
$=' with(_.split($[Y]))_ =join(pop());eval(_)
```

我是用谷歌做的，直接f12有个console模块，将eval改成console.log,出来的内容，看下这一块

```
if(e.length==16)if(e.match(/^22a60b/) != null)if(e.match(/0b310/) != null)if(e.match(/e5ece$/)!= null)if(e.match(/0ebe5/) != null)
```

拼接下得到22a60b310ebe5ece，提交到表单中，得到

U2FsdGVkX182eA/8U/2KZS481hY9IDS37kNjZ1UZtCckgQoGA7lo/Dtcv78qFew6LuMTMoP2mEapD0YIBh2Wa
又是aes对称加密，名字MD5加密，解密得到ctf%7BConsole.log%28shiyandar%29%7D，再url解码就行了

12.雌黄出其唇吻

访问网页，只有一串字符串，而且刷新后还会变，F12查看页面源代码，什么也没有发现，网

址<http://ctf5.shiyandar.com/misc/10/>，加个爬虫的文件试试，于是访

问<http://ctf5.shiyandar.com/misc/10/robots.txt>，发现都是disallow，不能访问，但是右面进度条还没到底，拉到

最下面是一个xml，于是访问<http://ctf5.shiyandar.com/misc/10//sitemap87591u096080.xml>，看到两个

php，/flag1241098092ewiuqu9t53.php 访问得到base加密的字符串，解密即可

13.女神

下载题目给的压缩包，解压有个txt还有一个文件夹，把文本里面的内容拿去base64解码，得到PNG开头的内容，我是将解码的内容存到txt里面又导入到010里面，但是图片就是不能打开，看了下wp，直接在python里面，open('nvshen.png','wb').write(open('C:\\Users\\cws6\\Desktop\\nvshen.txt','rb').read().decode('base64'))，一个命令就搞定了，图片去百度识图就行了，对名字是中文不要符号。

14.XDCTF misc100

下载出来是两张一模一样的图片，原以为是得用steglove分析，但是看到题目提示说是brainfuck，就直接用bftools就行了，和隐写里面的brainfuck一样的操作方式。

```
G:\tools\信息隐藏\bftools>bftools.exe decode braincopter C:\Users\cws6\Desktop\zzzzzyu.png --output --out.png
```

```
G:\tools\信息隐藏\bftools>bftools.exe run --out.png
```

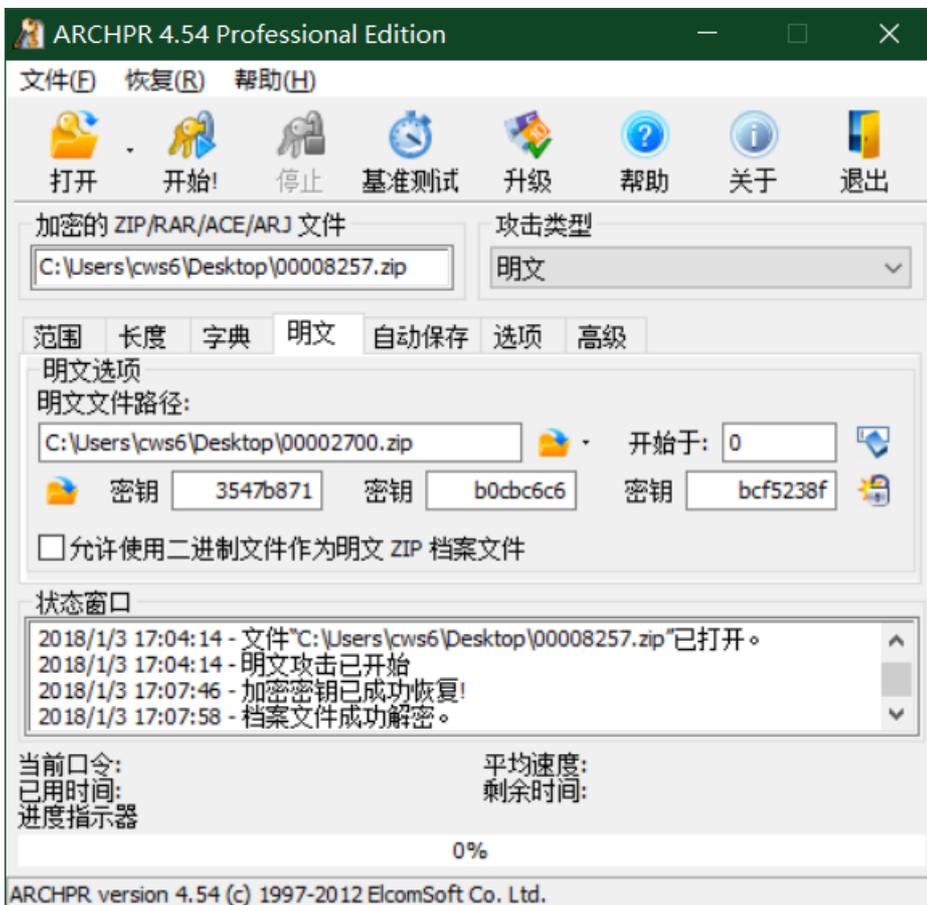
15.XDCTF misc200

密码分析中，已知明文攻击（Known plaintext attack）是一种攻击模式，指攻击者掌握了某段明文 x 和对应密文 y 。在所有密码分析中，均假设攻击者知道正在使用的密码体制，该假设称为Kerckhoff假设。而已知明文攻击也假设攻击者能够获取部分明文和相应密文，如截取信息前段，通过该类型攻击获取加密方式，从而便于破解后段密文。希尔密码依赖唯密文攻击较难破解，而通过已知明文攻击则容易攻破。(说了那么多，这道题其实就是知道了readme.txt的明文和密文，然后得到Encryption key

下载下来不知道是个什么格式的东西，拖到010里面，找打了五个zip压缩包，但是名字改成.zip解压需要密码，看wp说是有两个压缩包，但是我找到了五个啊。。本来想着直接010阶段分开的，但是不知道为什么只把后两个截出来的话前面就死了，然后就foremost分离了，得到两个压缩包

```
root@kali:~# foremost '/root/Desktop/areyoukidding'
```

两个readme.txt的CRC相同，所以这应该就是相应的明文和密文，使用ARCHPR



得到所示的三个密钥就可以解密了，解压后的文件夹中的flag.txt就是flag

16.你有记日志的习惯吗

不知道该怎么形容这个题，下载的时候那么大，其实是很懵的这要找到啥时候啊，然后默默翻了下评论，在 [www.lampplc.com](#) 这个文件下面有个my.cnf 搜索key得到password=YouGottIt!@#\$

17.这是捕获的黑客攻击数据包，Administrator用户的密码在此次攻击中泄露了，你能找到吗？

通过观察可以大概判断192.168.30.101 给服务器上了菜刀。因为菜刀是以POST方式发送数据的，我们过滤http,然后查看那些post,随便打开一条,在下面HTML里面可到BASE64加密后的Value值，通过解密就可以很显示的看到菜刀指令。可以将那些value值都base64解码一下，很快就能找到了。

18.Only one file

下载下来拖到binwalk里面

```
binwalk /root/Desktop/onlyOneFile
```

不知道为啥我没用-e直接解出来了。。然后将图片合成一张

```
cat /root/Desktop/onlyOneFile1/* > one.png
```

图片拖到010里面没找到什么有用的东西，又用steglove还是没找到什么东西，看下面评论说是adobe firework的，我们需要用firework打开，百度了下这个东西，就不想安装了，ps打开还不行就不做了。。据说是这个里面有个二维码反色下扫描就行了。