Bugku CTF 杂项（13-20） Writeup

原创

KRDecad3 于 2018-06-22 11:48:19 发布 1944 收藏 8

分类专栏： writeup 文章标签： writeup Bugku CTF

本文链接：https://blog.csdn.net/KRDecad3/article/details/80771729

Bugku CTF 杂项（13-20） Writeup

0x13这么多数据包

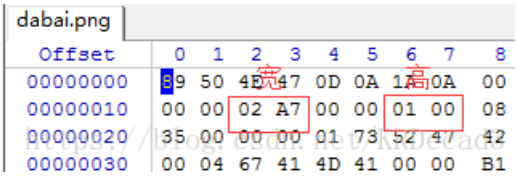
用wireshark打开，浏览一下从第104个包开始有TCP协议，那么就是从第104个包开始就是攻击机（192.168.116.138）向目标机（192.168.116.159）进行端口扫描，后面找到攻击机远程连接目标机的包（通过3389端口），网上说从第5542个包已经getshell，追踪TCP流就可以看到一串base64（但不知道原理，请赐教）。

普及一下：

> 3389端口是Windows 2000(2003) Server远程桌面的服务端口，可以通过这个端口，用”远程桌面”等连接工具来连接到远程的服务器，如果连接上了，输入系统管理员的用户名和密码后，将变得可以像操作本机一样操作远程的电脑，因此远程服务器一般都将这个端口修改数值或者关闭。

0x14隐写3

下载下来是一个大白的图片，猜测是图片长度被更改了，那么用winhex打开，更改高度的“01”为“11”，保存，flag显现。



0x15做个游戏(08067CTF)

下载下来是一个Java写的小游戏，通过Java反编译工具查看源码，在PlaneGameFrame.java中找到一串base64，解码得到flag。（具体原理本人也不清楚）

Java在线反编译工具

0x16想蹭网先解开密码

题目提示密码是电话号码并且给出了前七位，需要写个密码本遍历出后四位。
在其他前辈的wp上看到这么一句话：“WiFi认证过程重点在WPA的四次握手包，找到EAPOL握手协议”，过滤一下可以另存为一个文件，好像不这么做也没什么影响。

eapol

No.	Time	Source	Destination	Protocol	Length	Info
3066	45.138762	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	155	Key (Message 1 of 4)
3068	45.154148	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	155	Key (Message 2 of 4)
3070	45.168458	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	213	Key (Message 3 of 4)
3072	45.195620	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	133	Key (Message 4 of 4)

附上一个python脚本，本人暂时不会python（滑稽）

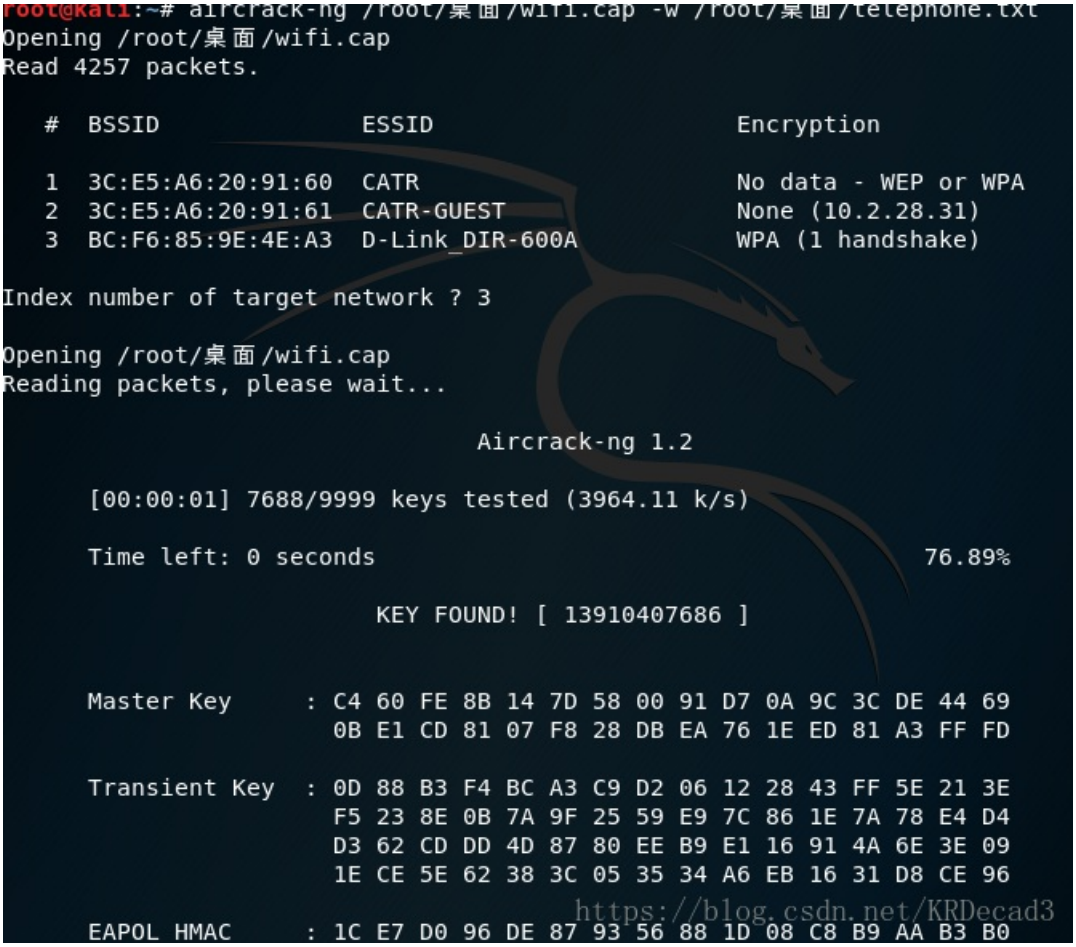
```python
#encoding:utf-8
import string
attendNum = string.digits
str1 = '1391040'
f = open('telephone.txt','w')
for i in attendNum:
    for j in attendNum:
        for k in attendNum:
            for l in attendNum:
                f.write(str1+i+j+k+l+'\n')
f.close()
```

还有一个用C写的：

```c
#include<stdio.h>

int main()
{
    int i,j,k,l;
    FILE *fp=NULL;
    fp=fopen("telephone.txt","w");
    for(i=0;i<=9;i++)
    {
        for(j=0;j<=9;j++)
        {
            for(k=0;k<=9;k++)
            {
                for(l=0;l<=9;l++)
                {
                    fprintf(fp,"1391040%d%d%d%d\n",i,j,k,l);
                }
            }
        }
    }
fclose(fp);
}
```

运行出来一个telephone.txt的密码本，把此txt文件和wifi.cap文件放到kalli里面，使用aircrack-ng工具。
终端输入命令：
aircrack-ng /root/桌面/wifi.cap -w /root/桌面/telephone.txt
然后选择参数3回车就能看到密码。



0x17Linux2

下载得到一个名为brave的文件，放入kali。
使用strings命令和grep命令查找key。
strings /root/桌面/brave | grep -i key
strings命令http://man.linuxde.net/strings
grep命令http://man.linuxde.net/grep

0x18账号被盗了

打开网页，用burp抓包，更改一下cookie，把isadmin改成true，在响应里找到一个exe文件，下载下来是一个CF刷枪的工具。

```
Content-Length: 0
Cookie: isadmin=false
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```



```
<!DOCTYPE html>
<html>
        <style>
                span {
                  display: block;
        margin: auto;
        height: 25px;
        text-align: center;
        font-size: 30px;
    }
        </style>
  <head>
    <title>bugku</title>
    <link href="style.css" rel="stylesheet" type="text/css">
  </head>
  <body>
    <span>http://120.24.86.145:9001/123.exe</span>
  </body>
</html>
```


用wireshark抓包，账号密码随便填，追踪TCP流，发现两串base64，解码是邮箱的账号和密码，登陆找到flag。

```
220 smtp.qq.com Esmtp QQ Mail Server
EHLO LAPTOP-7S7EQOKG
250-smtp.qq.com
250-PIPELINING
250-SIZE 73400320
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN
250-MAILCOMPRESS
250 8BITMIME
AUTH LOGIN
334 VXNlcm5hbWU6
YmtjdGZ0ZXN0QDE2My5jb20=
334 UGFzc3dvcmQ6
YTEyMzQ1Ng==
535 Error: ..........................: http://service.mail.qq.com/
cgi-bin/help?subtype=1&&id=28&&no=1001256
QUIT
221 Bye
```

0x19细心的大象

下载得到一张图片，打开属性发现备注里有一串base64，暂时不知道干嘛的。
kali里用binwalk查看里面还有一个压缩包，foremost分离，发现里面的压缩包需要密码，那么密码就可能是base64解码的那一串。解压得到和之前一样的图片隐写，更改高度得到flag。
还有另一个解法https://blog.csdn.net/sanky0u/article/details/77162806

0x20爆照

把图片用binwalk看一下，发现居然有辣么多东西，foremost提取，出现一堆图片，再挨个用binwalk分析，发现其中的88，888，8888是被修改过的。
（Linux不太会操作，又把文件移到Windows里的）
88里显示一张二维码，更改后缀名为jpg，扫描得到“bilibili”；
888里更改后缀名为jpg后，在属性里有base64编码，解码得“silisili”；
8888里还包含一个zip文件，foremost分离，解压得到一个二维码，扫描得“panama”。
题目提示为“xxx_xxx_xxx”，将以上三个字符串连起来就是flag了。
