南京邮电大学网络攻防平台writeup ————密码学

原创

FLy_鹏程万里 于 2018-02-28 11:43:15 发布 1878 收藏 2
分类专栏： #南京邮电大学CTFwriteup 【CTF】
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/Fly_hps/article/details/79397949
版权

南京邮电大学CTFwriteup 同时被 2 个专栏收录
5 篇文章 0 订阅
订阅专栏

【CTF】
30 篇文章 26 订阅
订阅专栏

1、easy

题目提示：

/blog.csdn.net/Fly_hps

思路：

这是一个加密解密型试题，根据其特点可知是采用base64加密的，所以可以直接使用base64在线解密即可。

1. 在线搜索一个base64在线解密网站。

   推荐链接：http://base64.xpcha.com/

2、KeyBoard

题目提示：

思路：

题目中多次强调“看键盘，看键盘，看键盘”，所以可以确定题目中给定的字母序列的编写与键盘密切相关，根据给定的字母序列于空格可以依次在键盘上找到相应的解密“字母”

解题步骤：

Ytfvbhn　　对应“a”

Tgbgy　　对应“r”

Hjuygbn　　对应“e”

Yhnmki　　对应“u”

Tgvhn　　对应“h”

Uygbnjm　　对应“a”

Uygbn　　对应“c”

Yhnijm　　对应“k”

从上至下依次连接起来可以得到答案：“areuhack”

提交(注意格式：nctf{areuhack}　)即可！

3、base64 全家桶

题目提示：

可知需要经过base64 、base32、base16解密才行，所以我们直接使用Python跑一下就OK：

代码如下：

```
>>> import base64
>>> print base64.b16decode(base64.b32decode(base64.b64decode('R1pDVE1NWlhHUTNETU
4yQ0dZWkRNTUpYR00zREtNWldHTTJES1JSV0dJM0RDTlpUR1kyVEdNWlRHSTJVTU5SUkdaQ1RNTkJWSV
kzREVOUlJHNFpUTU5KVEdFWlRNTjJF')))
netf{base64_base32_and_base16}
>>>
```

4、n次base64

题目提示：

打开链接：

```
Vm0wd2QyUX1VWGxWV0d4V1YwZDRWMV13WkRSWFJteFZVMjA1VjAxV2JETlhhMk0xVmpKS1NHVkVRbUZ
VmxsM1ZtcEJlRll5U2tWVWJHaG9UV1Z3VlZacVFtRlRNbEpJVm10a1dHSkdjSEJXYTFwaFpWWmFkRTF
VWxSTmF6RTFWa2QwYzJGc1NuUnhSemxWVmpOT0xcFZXbUZrUjA1R1drWlNUbUpGY0VwV2JURXdZVEZ
U0ZOclpHcFNWR3hoV1d4U1IyUnNXbGRYY1hSWFRWaENSbFpYZUhkV01ERkZVbFJDVjAxdVVuWldha3B
VmpGT2RWVnNXbWhsYlhob1ZtMXdUMk15UmtkalJtUllZbGhIV0ZSV2FFTlNiRnBZWlVoa1YwMUVSalp
YkZKRFZqSkdjbUV6YUZaaGExcG9WakJhVDJOdFJrZFhiV2hzWWxob2IxWnRNWGRVTVZWNVVtdGtWMVR
YUZsWmJGWmhZMVphZEd0NlJteFNiSEJaV2xWb2ExWXdNVVZTYTFwV1lrWktSRlpxU2tabFZsSlpZVVp
VTFKV2NIbFdWRUpoVkRKT2MyTkZhR3BTYkVwVVZteG9RMWRzV25KWGJHUmFWakZHTkZaSGRHdFdiVXB
VjJ4U1dtSkhhRlJXTUZwVFZqRmtkRkp0ZUZkaVZrbzFWbXBLTkZReFdsaFRiRnBxVWxkU1lWU1ZXbmR
YkZweFVtMUdUMkpGV2xwWlZWcHJWVEZLVjJOSWJGZFdSVXBvVmtSS1QyUkdTbkphUmlocFZqTm9WVmR
VWs5Uk1XUkhWMjVTVGxaRlNsaFVWbVEwVjBaYVdHUkhkRmhTTUhCS1ZsZDRjMWROU2toaFJsSlhUVVp
VkZacVNrZFNiRkp6V1cxc1UwMHhSalpXYWtvd1ZUR1ZlRmR1U2s1WFJYQnhWVzB4YjFZeFVsaE9Wenx
WWtad2VGVnRNVWRVTWtwR1YyeHdXbFpXY0hKV1ZFWkxWMVpHY21KR1pHbFhSVXBKVm10U1MxVXhXWGh
YmxaV1lsaENWRmxyVm5kV1ZscDBaVWM1VWsxWFVucFdNV2h2VjBkS1JrNVdVbFZXTTJoSVZHdGFjMk5
WkhSa1IyaHBVbGhCZDFkV1ZtOVVNVnAwVTJ4V1YyRXhTbUZhVjNSaFYwWndSbFpZYUZkTlZrcDVWR3h
VDJGV1NuUlBWRTVYVFc1b1dGbHFTalpsUm1SWldrVTFWMVpzYOZWWFZsSkhaREZrUjJKSVRtaFNlbXh
VkZaYWQyVkdWblJsU0dScFVqQndWMV15ZEhkVO1ERnhVbXRvVjFaRldreFdNVnBIWTIxS1IxcEdaRTV
UlhCS1ZtMTBVMU14VlhoWFdHaGhVMFphVmxscldrdGpSbHB4VkcwNWEySkhVbnBYYTFKVFYyeFpkMkp
```

发现许许多多的base密文，而且提示要用n次base64，所以我们可以多次base64解密，直到得到flag：

5、骚年来一发吗？

题目提示：

可以获取的信息：

这是一个php加密函数

密文已知：密文：iEJqak3pjIaZ0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas

加密函数已知。

接下来我们要做的就是解密，那么根据加函数的功能我们进行逆向其过程就OK：

```php
<?php
    function decode($str){
        $string=base64_decode(strrev(str_rot13($string)));
        for($_0=0;$_0<strlen($str);$_0++){
            $_c=substr($str,$_0,1);
            $__=ord($_c)-1;
            $_c=chr($__);
            $_=$_.$_c;
        }
        $str=strrev($_);
        return $st;
    }
    $str='iEJqak3pjIaZ0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas';
    echo decode($string);
?>
```

之后在本地访问该php文件即可：

```
/* 错误hpinfo(); flag:nctf{gzip_base64_hhhhhh} */
Notice: Undefined variable: string in D:\phpStudy\WWW\project01\1.php on line 31

Notice: Undefined variable: string in D:\phpStudy\WWW\project01\1.php on line 19

Notice: Undefined variable: _ in D:\phpStudy\WWW\project01\1.php on line 26

Notice: Undefined variable: st in D:\phpStudy\WWW\project01\1.php on line 27
```

6、异性相吸

题目提示：

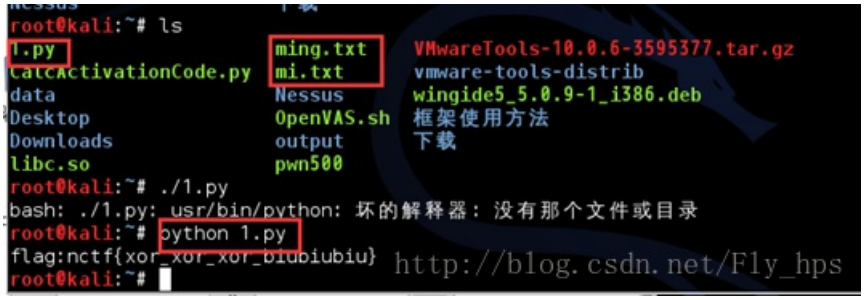
下载文件到本地，并且将解压之后的文件移至Kali中，之后编写脚本如下，根据给定的解密与加密关系进行解密：

```
f_a=open('mi.txt','rb')
f_b=open('ming.txt','rb')

a="".join(f_a.readlines())
b="".join(f_b.readlines())

s=''
for i,j in zip(a,b):
    s+=chr(ord(i)^ord(j))
print s
```

http://blog.csdn.net/Fly_hps



7、Md5

题目提示：

直接使用Python循环遍历进行查找即可！代码如下：

```
import md5
import string
for i in string.uppercase:
    for j in string.uppercase:
        for k in string.uppercase:
            a='TASC'+i+'O3RJMV'+j+'WDJKX'+k+'ZM'
            b=md5.md5(a).hexdigest()
            if(b[0:5]=='e9032'):
                print b
```

之后得到**flag:nctf{e9032994dabac08080091151380478a2}**