中国电信线CTF线下选拔writeup

转载

weixin_30270561 于 2017-12-28 10:47:00 发布 278 收藏
原文链接：http://www.cnblogs.com/yubenliu/p/8134443.html

[盟军密码|30分]
二战时盟军截获德军一段密码，密文为：
00000110000000001010101101110000110001111000111100010011001110001111001（密钥：helloworld），你可能会解出一个keyxxxxx的答案，请在y后面加{，结尾加}，答案的格式是key{xxxxx}，所以答案是

二战时德军使用过的一种密码，其实是利用了二进制的表示法来替代字母，也称为“费娜姆密码”

A 1000001	B 1000010	C 1000011	D 1000100
E 1000101	F 1000110	G 1000111	H 1001000
I 1001001	J 1001010	K 1001011	L 1001100
M 1001101	N 1001110	O 1001111	P 1010000
Q 1010001	R 1010010	S 1010011	T 1010100
U 1010101	V 1010110	W 1010111	X 1011000
Y 1011001	Z 1011010		

0000011 H1001000=1001011K
0000000 E1000101=1000101E
0010101 L1001100=1011001Y
0110111 L1001100=1111011{
0000110 O1001111=1001001I
0011110 W1010111=1001001I
0011110 O1001111=1010001Q
0010011 R1010010=1000001A
0011100 L1001100=1010000P
0111001 D1000100=1111101}

key{iiqap}

[我来征服|30分]
我来，我见，我征服，d5Y8h5Xz]ZH7\Wok\Z\8PmUkPJYlQ5lkQmf4P}n}]m\5P}EkiT@@，答案就在这个密文里，答案的格式是key{xxxxx}，所以答案是
key{e0ea8a9aaf924a0eb7aa675393f6630a}

```
import base64
import StringIO
lstr="d5Y8h5Xz]ZH7\Wok\Z\8PmUkPJYlQ5lkQmf4P}n}]m\5P}EkiT@@"
lstr="a2V5e2UwZWE4YTlhYWY5MjRhMGViN2FhNjc1MzkzZjY2MzBhfQ=="
str2=''
for i in lstr:
    temp=chr((ord(i)-3)%128)
    str2=str2+temp
print(lstr)
print(str2)
print base64.decodestring(str2)
```

[小明入侵|30分]
小明入侵网站后获得了管理员的密文，由于太高兴了手一抖把密文删除了一部分，只剩下前10位e5a14523c0，
小明根据社工知道管理员的密码习惯是key{4位的数字或字母}
，所以管理员的密码是
key{mnwt}

```
import base64
import StringIO
import hashlib

seed = "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"

def get_pwd(str, num):
    if(num == 1):
        for x in str:
            yield x
    else:
        for x in str:
            for y in get_pwd(str, num-1):
                yield x+y

strKey="1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
for x in get_pwd(strKey,4):
    stra="key{"+x+"}"
    m2 = hashlib.md5()
    m2.update(stra)
    stra2=m2.hexdigest()
    if (cmp(stra2[:10],'e5a14523c0')==0):
        print(stra)
        break
```

[这是什么|30分]
我是什么，答案就在这个图片里，
http://ncstatic.oss-cn-hangzhou.aliyuncs.com/dianxin/06/img/78/78.jpg

答案的格式是key{xxxxx}，所以答案是

```
print chr(107)+chr(101)+chr(121)+chr(123)+chr(99)+chr(108)+chr(108)+chr(98)+chr(111)+chr(74)+chr(55)+chr
```

key{cllboJ7hgj}

[海贼王|30分]
这里有很多海贼王的图片，挑一张吧，
http://ncstatic.oss-cn-hangzhou.aliyuncs.com/activity/0327dianxin/onepiece25.zip
点击下载海贼王，答案的格式是key{xxxxx}，所以答案是
binwalk foremost steghide stegdetect
find . -name "." | xargs grep "key{"

key{CU5e6arJ2q78eLgbOo9dhNSzxkWiQlWS}

[找鼹鼠|50分]
答案就在这个文件里，http://ncstatic.oss-cn-hangzhou.aliyuncs.com/dianxin/067/98207.zip
点击下载，答案的格式是key{xxxxx}，所以答案是

key{Hhe80fr80afevgfrvgr}

[我心依旧|50分]
答案就在这首歌里，href="http://ncstatic.oss-cn-hangzhou.aliyuncs.com/dianxin/05/1.mp3"点击下载我心依旧，答案格式为key{xxx}，所以答案是

二进制打开1.mp3，搜索pass，注意误区

key{efrgrh48q4g5gh44q4fhfgg}

[EXE逆向|50分]
答案就在这里，href="http://ncstatic.oss-cn-hangzhou.aliyuncs.com/dianxin/789/7abd.zip"点击下载，答案格式为

KEY:{ANYUN0_md57e0cad17016b0>?45?f7c>0>4a>1c3a0}

```
import os
bb={0x4e,0x74,0x57,0x47,0x79,0x3b,0x32}
for i in bb:
   sys.stdout.wtire(chr(i^7))
bb={0x63,0x58,0x6e,0x46,0x61,0x50}
for i in bb:
    sys.stdout.wtire(chr(i^0x33))
lsP@~<5Pk]uRc
```

s

[APK逆向|50分]
答案就在这里，http://ncstatic.oss-cn-hangzhou.aliyuncs.com/dianxin/789/8kfe.apk
点击下载，答案格式为KEY{xxx}，所以答案是

KEY{Q1ul3lsR0ghS1}

[EXE2逆向|50分]
答案就在这里，http://ncstatic.oss-cn-hangzhou.aliyuncs.com/dianxin/789/99dkae.zip
点击下载，答案格式为KEY{xxx}，所以答案是

对于byte_415768,指向

及取V27[0]=

```
import sys
code=(1,4,14,10,5,36,23,42,13,19,28,13,27,39,48,41,42)
str="KfxEeft}f{gyrYgthtyhifsjei53UUrrr_t2cdsef66246087138\0087138"
for i in range (0,17):
   sys.stdout.write(str[code[i]-1])
```

对于
查49,48,50,52,125对应的ASCII码为’1’,’0’,’2’,’4’,’}’，显然是字符串“1024}”

KEY{e2s6ry3r5s8f61024}

转载于:https://www.cnblogs.com/yubenliu/p/8134443.html