实验吧try them all

原创

Gunther17 于 2017-07-30 15:31:10 发布

http://www.shiyanbar.com/ctf/1981
try them all:
You have found a passwd file containing salted passwords.
An unprotected configuration file has revealed a salt of 5948.
The hashed password for the 'admin' user appears to be
81bdf501ef206ae7d3b92070196f7e98, try to brute force
this password.
解：别人思路：加盐+Md5+暴力

```
#-*- coding:utf -*-
__author__='xiaoyu'
__date__ ="$2017-7-30 9:47:51$"
from hashlib import md5
def bruteforce():
#rb以二进制读模式打开,file.readlines()返回一行
#另一方面，.readline() 每次只读取一行，通常比 .readlines() 慢得多。
#仅当没有足够内存可以一次读取整个文件时，才应该使用 .readline()
f=open('F:\p\webshellpassword.txt','rb').readlines()
salt='5948'.encode("utf-8")#盐值化成字节
m='81bdf501ef206ae7d3b92070196f7e98'#hash值
for line in f:
t=line.strip()+salt
#Python strip() 方法用于移除字符串头尾指定的字符（默认为空格）。
#md5.digest() 返回二进制的加密结果
#md5.hexdigest() 返回十六进制的机密结果
t=md5(t).hexdigest()
if(t==m):
print(line.strip())
break
pass
#用于在dos下直接运行.py文件
if __name__=='__main__':
bruteforce()
print('运行完成')
```

别人总结：这题只是考验md5加salt，明文找一份比较全的字典去跑即可，然而
我字典找的不好全扯淡。

最后我自己是用工具解决的，锻炼自己搜索能力。
这里说一下提交答案很重要,不然浪费老子松果，靠flag:sniper