

BugkuCTF crypto Crack it

原创

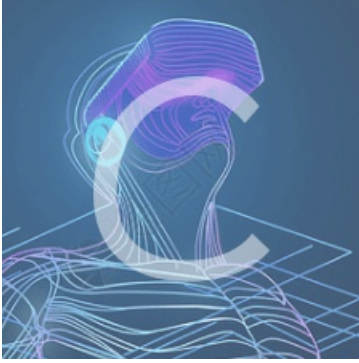
H4ppyD0g 于 2019-09-15 19:39:18 发布 669 收藏

分类专栏: [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/weixin_42172261/article/details/100861516

版权



[CTF 专栏收录该内容](#)

45 篇文章 0 订阅

订阅专栏

shadow密码文件

在unix早些时候是没有/etc/shadow这个文件的。一个用户的所有信息都只是保存在/etc/passwd文件中, 加密后的用户密码保存在了passwd文件的第二个字段中。每个用户对于password文件都是可读的。

后来出现了shadow文件, 把密码放在这个文件里面, 并且保证了只有root才能对shadow文件进行读写。

/etc/shadow中密码格式:

```
$id $salt $encrypted
```

id	算法
1	MD5
2a	Blowfish
5	SHA-256
6	SHA-512

使用 `more shadow` 命令查看shadow文件信息。

用到john工具。John the Ripper是一个快速的密码破解程序

`john --show[=LEFT]` 显示破解的密码[如果=左, 然后uncracked]

输入命令 `john --show shadow`