BugkuCTF-Crypto题Crack it

原创

彬彬有礼am_03 于 2021-08-24 21:32:33 发布 32 收藏

分类专栏： # BugkuCTF-Crypto 文章标签： linux 算法 安全

本文链接：https://blog.csdn.net/am_03/article/details/119899158

下载文件得到shadow文件

查看文件：cat shadow/more shadow

```
root@localhost:~/文档/CTF/CTF题目/CTF02/Crypto/Crack it# more shadow
root:$6$HRMJoyGA$26FIgg6CU0bGUOfqFB0Qo9AE2LRZxG8N3H.3BK8t49wGlYbkFbxVFtGOZqVIq3qQ6k0oetDbn2aVzdhuVQ6US.:17770:0:99999:7:::
root@localhost:~/文档/CTF/CTF题目/CTF02/Crypto/Crack it#
```

应该有工具可以爆破

Kali系统里的john工具可以用。

破解：john shadow

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]

```
root@localhost:~/文档/CTF/CTF题目/CTF02/Crypto/Crack it# john shadow
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 14 candidates buffered for the current salt, minimum 16 needed for performance.
Warning: Only 10 candidates buffered for the current salt, minimum 16 needed for performance.
Warning: Only 15 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 8 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
hellokitty       (root)
1g 0:00:00:02 DONE 2/3 (2021-06-06 12:21) 0.3367g/s 1855p/s 1855c/s 1855C/s ilovegod..ford
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Linuxshadow文件，还特意跟正常的对比了一下。现在想办法看shadow具体是怎么加密的。

linux /etc/shadow里hash算法包括缺省的DES经典算法、MD5哈希算法($1)、Blowfish加密算法($2或$2a)和SHA哈希算法($5或$6）。因此利用hashcat进行破解的参数也不同，比如MD5哈希算法($1)，使用hashcat -m 500参数；SHA哈希算法($5或$6），

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文件里，加密后的用户密码保存在了passwd文件的第二个字段里。各用户对于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。