[CTF]JTR没有ssh2john的解决办法

原创

jameskaron 于 2020-02-24 16:31:59 发布 694 收藏
分类专栏： CTF

本文链接：https://blog.csdn.net/jameskaron/article/details/104480052

1.JTR(John the ripper)是一个破解工具,其中ssh2john可以转化ssh私钥为john可以破解的格式.但是最新的JTR上没有发现ssh2joh

https://github.com/magnumripper/JohnTheRipper

可以看到src里面有很多*2john.c就是没有ssh2john,后来发现在run目录下有ssh2john.py

2.查了很多资料,很多资料都是旧的方法,都没有解决办法,于是想到直接touch一个文本,然后复制ssh2john的源码进去,使用python ssh

注意:刚复制进去的时候最后一行格式会有问题,只要加上TAB来给个空格就好

而且不能使用python3来运行

3.但是按照网上教程,这里使用命令破解:

```
zcat /usr/share/wordlists/rockyou.txt.gz |john --pipe --rules ssh_john.txt
```

然后报错:

```
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
mem_alloc(): ?????? trying to allocate 2147483648 bytes
```

百思不得其解,后来很偶尔情况下发现一篇文章:

https://l1cafe.blog/2019/03/03/kuya-1-writeup

里面不引用字典,而是直接使用john:

```
john ssh_john.txt
```

发现竟然可以破解成功了.最后按q退出即可