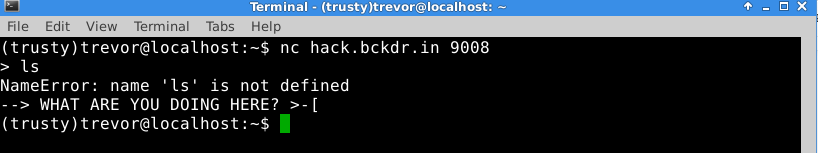
**Worst-pwn-ever writeup**

**Introduction:** Worst-pwn-ever was a 100 point challenge given during SDSLabs annual CTF challenge Backdoor CTF. During the CTF my teammates and I registered the team TXST-CS and ended up placing 24th out of ~270 teams. Since SDSLabs uses an ‘always-on’ system you can attempt to solve this challenege at backdoor.sdslabs.co while you read along. For that reason I will not be providing the final flag needed to collect the points.

**Task:** tocttou is an environmentalist. But some say he has a vicious motive and he uses nature to hide his dark side. We found a weird shell on his amazon (pun intended) web services. Can you tell us what is he upto? Tip: he might shut down the machine if he notices you - and he will (maybe in 45 seconds). Access: nc hack.bckdr.in 9008

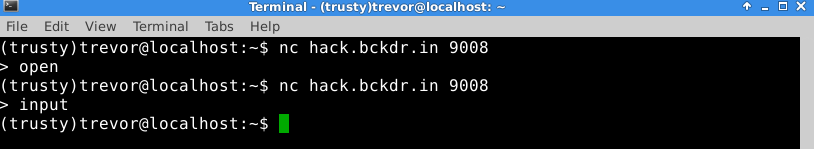
**Solving:** First thing’s first, connect to the address and see what we’re given. Then let’s try and run some commands if possible.



Upon connecting it seems like we’re given a shell, this should be pretty obvious, as you’re told this from the problem description. When we try and run basic commands such as ‘ls’ the system spits out “NameError: name ‘....’ is not defined” then kicks us out, interesting. Additionally, If you idle for more than 45 seconds you’re kicked out. Originally when this problem was posted the “NameError:....” output was hidden from us. Eventually the backdoor admins added the hint after much confusion from other competitors, including myself. If you idle for more than 45 seconds you’re also kicked out.

The “NameError: name ‘...’ is not defined” seems like as good a starting point as any, let's do some quick googling to figure out the meaning. After some quick skimming of [this](http://stackoverflow.com/questions/17413502/nameerror-name-n-is-not-defined-even-though-its-an-input-python) article on stack-overflow it seems the mysterious shell we’re connecting to is running in an eval() loop. If that’s the case let’s enter some basic python commands and see what happens.

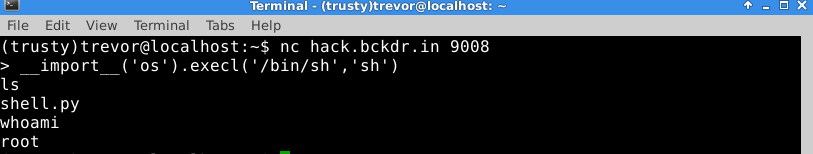
If you don’t know basic python keywords take a look at [this](http://www.tutorialspoint.com/python/python_basic_syntax.htm) page, it’ll give you some ideas. After various tests It seems like some basic keywords get evaluated but the output isn’t shown to us. For this example I used ‘open’ and ‘input’ there are other keywords that will produce the same output.



The next obvious step here is to try to gain access to a true shell by exploiting Python’s eval() function. If you’re unfamiliar with python eval() exploits I suggest having a look at [this](https://2013.picoctf.com//problems/pyeval/stage1.html) wonderful series of articles written by the PicoCTF team.

The magic piece of code we’ll be using today is : \_\_import\_\_('os').execl('/bin/sh','sh')

This line of code when interpreted will import Python’s OS library and allow us to use the execl function to launch a shell, let’s see if it works.



Uh Oh! I don’t think this is intended. Now let’s see if we can find the flag. For the purpose of this write up I’m going to outright tell you the flag isn’t stored anywhere ‘conventionally’ in the system. During the competition myself and others spent hours looking for the flag in the file system, after some complaining on IRC by other competitors the CTF admins posted a new hint.

“Who is Tocttou?”

Googling “tocttou” produces several pages of “TIme of check, to time of use” race condition exploits. After asking the CTF admin’s if there was a tocttou hole we needed to exploit to retrieve the flag, I was told no.

After some more thought about the hint we were given by the admins another hiding place revealed itself. If we re-read the question this line stands out “Tocttou is an environmentalist”. That doesn’t seem like much until you think about basic unix / linux. Environmentalist, environment-alist. Let’s take a look a the environment variables of the system and see what we get.

Use the command: printenv

To print the environment variables, you’ll find the flag there. SHA 256 the flag and submit it to backdoorctf to get credit.