**Intro To Exploitation - Pyjails Solution**

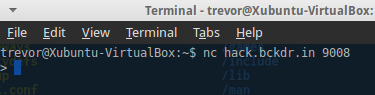
**Introduction:** Pyjails is a medium level exploitation challenge intended to teach students about the potential dangers of providing users access to unsecure services through a real world challenge. Additionally this challenge provides students with some knowledge of deducing what services may be running in an unknown environment. Pyjails real name is [worst-pwn-ever](https://backdoor.sdslabs.co/challenges/WORST-PWN-EVER), a challenge written by Ashish Chaudhary as part of SDSLabs [Backdoor CTF](https://backdoor.sdslabs.co/) 2016.

**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?

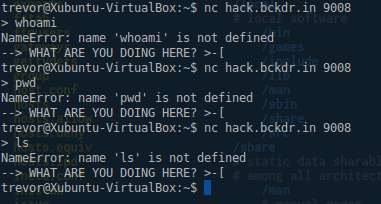
Tip: he might shut down the machine if he notices you - and he will (maybe in 45 seconds).

Access: nc hack.bckdr.in 9008

**Solving:** Begin by opening a terminal and connecting to the netcat credientials provided: hack.bckdr.in 9008. Once you connect the only indication you’ve connected to the service is that your shell will output ‘>’ a classic indicator of a command line interface of some form.

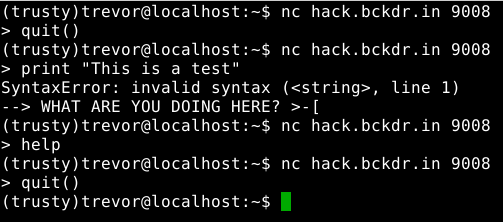


Before you can exploit any system you must first figure out what kind of environment or service is running on this remote machine. Begin by throwing some arbitrary commands at the service. I chose some common bash commands as a starting point.



Interesting, we can probably rule out the target environment being bash. Where do we go from here then? Notice that each time you execute a command two pieces of information are output by the system. The first line output is the most important “NameError: name ‘COMMAND’ is not defined”, the second output “--> WHAT ARE YOU DOING HERE? >-[“ is output when the system “notices you” and then kicks you out every time you run an unknown command.

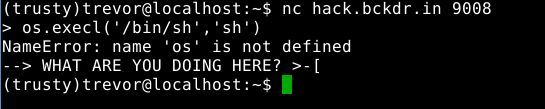
Let’s go to [Google](http://lmgtfy.com/?q=NameError%3A+name+is+not+defined) and see if we can’t dig up any information on this “NameError: name ‘COMMAND’ is not defined” nonsense. Well what do you know, the entire first page is full of Python based questions. This gives us a pretty strong hint that our target system is interpreting our commands through some sort of python script, quite possibly the python interpreter itself. Let’s test this theory out by trying to execute some very basic, python commands such as: “print”, “help”, and “quit()”.



Interesting! The commands “help” and “quit()” execute perfectly but we don’t see any output from the system. Our “print” statement gives us a SyntaxError: for some strange reason. Either way, it would be a good guess to say we’re stuck in some stripped version of the python interpreter, now it’s time to try and exploit it.

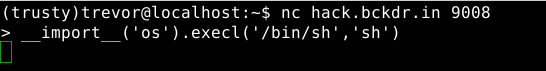
Python has a function known as eval() which will evaluate a string of Python code if passed to the function. If used improperly, this function can be rather dangerous. You can read more about exploiting Python’s eval() statement [here](http://nedbatchelder.com/blog/201206/eval_really_is_dangerous.html).

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

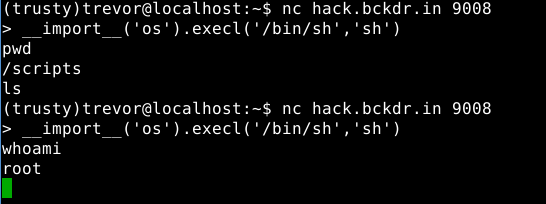


Well that’s unfortunate, it seems the OS module isn’t loaded. What if I told you there’s a way to force Python to import a module for you? You can read more about it [here](https://2013.picoctf.com/problems/pyeval/stage3.html).

Let’s try this piece of code now: ‘\_\_import\_\_('os').execl('/bin/sh','sh')’



We certainly didn’t get kicked out of the target system, that’s a pretty good sign right? Let’s try running those bash commands from before again.



Bingo! We’ve successfully launched a root level shell on the target system, we essentially own this system now. But we’re not done yet, we still need to find the flag and complete this challenge.

Feel free to dig around the system and look around if you like, you won’t find the flag though. The question says that “tocttou is an environmentalist” which is somewhat poor hint that breaks down like this: environmentalist, environment-alist. Bash environment variables! Let’s see if the flag is hidden in the environment variables!

You can list the bash environment variables with the command: ‘printenv’

