

Upgrading half shells to fully interactive TTYS

This document is how-to guide to upgrade your target machine's netcat reverse shell to a fully interactive TTY, that will allow things like auto-complete, command history, and Ctrl-C. Here's the steps:

- Once you've got your desired reverse shell go ahead and spawn bash using PTY

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

- Now background your reverse shell using Ctrl-Z
- While the shell is in the background examine the current terminal \$TERM and stty configuration:

```
root@kali:~# echo $TERM
xterm-256color
root@kali:~# stty -a
speed 38400 baud; rows 55; columns 205; line = 0;
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D; eol = <undef>; eol2
= <undef>; swtch = <undef>; start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R;
werase = ^W; lnext = ^V; discard = ^O; min = 1; time = 0;
-parenb -parodd -cmspar cs8 -hupcl -cstopb cread -clocal -crtscts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl ixon -
ixoff -iuclic -ixany -imaxbel iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0
ff0
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -echopr
echoctl echoke -flusho -extproc
root@kali:~#
```

The information needed is the TERM type ("*xterm-256color*") and the size of the current TTY ("*rows 55; columns 205*")

- With the shell still in the background set the current STTY to type raw and tell it to echo the input characters with the following command:

```
stty raw -echo
```

- Next foreground the shell with fg. It will re-open the reverse shell but formatting will be off. Finally, reinitialize the terminal with reset. Note: I did not type the nc command again (as it

might look above). I actually entered `fg`, but it was not echoed. The `nc` command is the job that is now in the foreground. The `reset` command was then entered into the netcat shell

- After reset the shell should look normal again. The last step is to set the shell, terminal type and `stty` size to match our current Kali window (from the info gathered earlier)

```
$ export SHELL=bash
$ export TERM=xterm256-color
$ stty rows 38 columns 116
```

The end result is a fully interactive TTY with all the features we'd expect (tab-complete, history, job control, etc) all over a netcat connection.

Reference:

<https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/>