**Breaking Out of a Jail Shell**

**System based**

* Groups are access restricted by iptables or permissions etc.

**Application based**

* **Kshell/Lshell**

Normally done by restricting cmds that you can use

Sometimes a jail shell will disconnect you from cmds by removing the file paths from the shell

* This doesn’t mean that cmds aren’t there, you just have to find and navigate to the file path manually e.g., /usr/bin/ls

Env – shows environmental variables specific to current environment

* SPATH will show you what paths you have present

Python interactive shell

* Python -c import ‘os; os.system(‘/bin/sh’)’
* [Or] vi
  + :sh
* [OR] /bin/sh
* Creates and drops you into shell
* Can do this with man, less and more pages
  + Page has to be bigger than screen: scrollable
* Awk ‘BEGIN {system(“/bin/sh”)}’

Or import the paths so that you can use them (as long as there’s no group permission restrictions etc.)

* Export PATH=[whatever]

HW: break out of a jail shell with a history file