Session 2 Worksheet SOLUTIONS

Question One

Using the terminal find out what processes are running. Find out the command to search for a process based on its port number. If running the process on your own machine, open a program such as Firefox, find out its process name and end the process (you should see the window close).

There are many commands to see which processes are running. Here are some of them:
>   -> **ps -a** (the a command displays information about other users' processes as well as your own). You will usually see -aux where x shows processes without a controlling terminal and u narrows down the processes to your username)
>   -> **top** (this shows processes using the most memory)
>   -> **netstat** (this shows networking information and will give you the process id if you use the flag -p)

We can pipe the output from netstat into grep to look for a certain port number as so:
-> netstat -nlp | grep :80

There are multiple other options eg lsof -i :80. Port 80 is used as an example in both these answers.

To find firefox:
-> ps ax | grep firefox

To kill a process:
-> kill -9 3544 (where 3544 is an example of the pid you may find from the previous command)

Question Two

Explore Linux file permissions in a capture the flag scenario! You'll need Docker for this exercise, so either download Docker or use this website: https://labs.play-with-docker.com/#

For a video walkthrough of this challenge, [see this YouTube video](#) explaining the steps taken along the way and what leads to making those decisions.

Bandit Continued…

For a Bandit walkthrough, you can take a look at [this answer key](#) I prepared during my first run through. Keep in mind there are often several ways to do the same thing and the route I took might not be the best one!