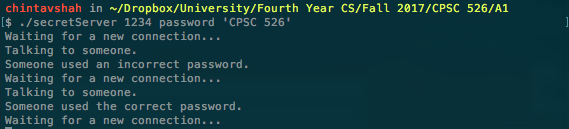
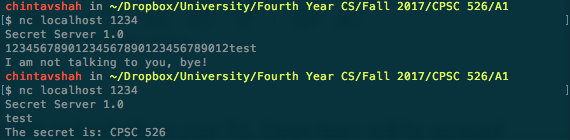
The exploit occurs when the password the client enters for the secret server is larger than the size of the buffer (32 bytes). This is because the 33rd byte overwrites the original password. So, anything that is entered after the 32nd byte becomes the new password. The exploit is fixed by enforcing the pointer to write a maximum of 32 bytes to the buffer.

**Sample exploit of original server**



**Figure 1: Starting the server with the original password**



**Figure 2: Revealing the secret with a different password (test)**