TurnOut
(C version)

Overview

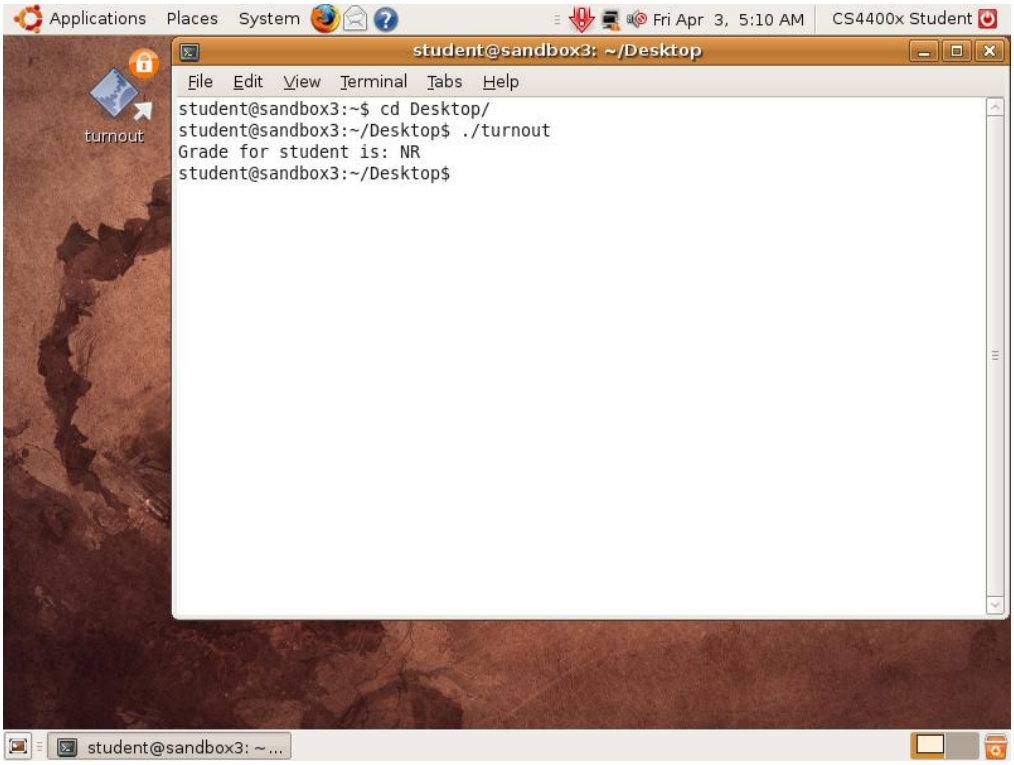
The TurnOut server that you will be analyzing is written in C and has a MySQL backend. Your initial focus should be to change your NR to a grade of your choosing, but the goal of this assignment is to gain an understanding of some of the different types of attacks that can occur in this realm. Once you are successful in changing your grade, continue to launch other types of attacks.

Setup

- You will need to download the latest version (sandbox3) of the TurnOut server from the Fossil Lab.
- It is available on the public drive (**P:/CS-440x/turnout3**). If you get the images mixed up or are unsure what version of the server you are running, check the lower right corner of the startup screen.

- Once you've gotten the server setup and running, you can log into the machine directly though the Ubuntu splash screen using "student" "Bending Unit 22" as the username and password respectively.

- On the desktop there is a linked binary named “turnout”. This is the application that you will be attacking.
- Open up a terminal inside the Ubuntu install (Applications > Accessories > Terminal), change the directory to the desktop and then you’re ready to go.



Task

Your task is to exploit this application to perform unintended operations on the system or application data. In order to get started, make your initial task to change your grade from a NR to a grade of your choosing, however once you’ve accomplished this; continue to explore the different aspects of this application to see how it may be vulnerable and, perhaps more importantly, what the “global” effect of attacking this application has on the system it is running on. Think of what other attacks could be launched as a result of this application’s poor security practices.

Security Block

At one point you may run into a security wall (ie, the OS’ security features prevent attacks that the application allows). If you’ve hit this point, the application will exit and there will be a decent amount of text explaining what occurred. Contact Bob Breznak (rbreznak@wpi.edu) with the output from the terminal, a quick description of the events that lead up to the attack and a short assessment of what underlying technology is at play. In return, you’ll receive instructions on how to “bypass” this and gain equivalent access to the system. Bonus points will be awarded if you are able to gain this access without using the “bypass.”