Assignment: DEP/NX

Description:

Please complete the following lab CTF challenges, preferably in Python 3, using the “pwntools” library:

- Lab 4-1
- Lab 4-2
- Lab 4-3

Labs 4-1 and 4-2 should be relatively simple, as they are very similar to the problems shown in the lecture. I expect everyone to be able to solve these.

Lab 4-3 is similar in concept to 4-2 (i.e. you will use ROP), but more difficult because you’ll need to bypass stack cookies *and* DEP/NX! Additionally, the convenient “/bin/sh” string isn’t present, meaning you’ll need to find another way to recreate it in memory yourself. Please give this challenge your best effort, but rest assured I will still grade generously for a strong attempt, even if you do not achieve a working exploit. This challenge is a stretch goal.

Remember to please document your solutions. As previously stated, “documentation” may be as simple as code comments throughout your script, explaining what each part does, or as fancy as a separate write-up with screenshots, diagrams, and full explanation. Up to you, I’d just like to see your thought process.

Don’t forget to submit the flags! :)

Deliverables:

- For each of the labs listed above, please turn in to the dropbox…
  - Your well documented script which solves the challenge
  - A screenshot of it running, showing that it works.