CECS 478 Assignment 3 - Exploitation

20 points

Assignment Description. Answer the following questions from the Chapter `0x300` reading from your textbook. Be through and complete with your answers. You *may* work on these questions with a partner (no more than two working together), but **both** students must submit the document individually on Beachboard Dropbox along with both students' names on each submission.

1. Describe what the following shell commands will do:
   (a) `env`
   (b) `su`
   (c) `echo $SHELL (additionally, where does this command get its output from?)`
   (d) `cat /etc/passwd >> ~/pfl`
   (e) `perl -e 'print "1\n5\nn\n5\n" . "A"x100 . "\x70\ x8d\x04\x08\n" . "1\nn\n" . "7\n"'`
2. What types of files are contained within the following Linux directories:
   (a) /root
   (b) /sbin
   (c) /etc
   (d) /var
   (e) /usr
3. Explain what the following entry in /etc/passwd means:

   ```
   myroot:XXq2wKiyI43A2:0:0:me:/root:/bin/bash
   ```

4. Section `0x321` in your textbook discusses debuggers applied to code vulnerability examination. How might you use a debugger to prepare for an exploitation?
5. How can the shell environment be useful for performing an exploitation attack?
6. How might I exploit a heap? A stack? What Linux tools would you use for conducting each?
7. What is the `%s` format parameter used for? Give an example. How might I use it to write out an exploit?
8. Big-endian and little-endian are two ways that computer architectures deal with numbers. What are they? Which one does the Intel `x86_64` architecture use?
9. How do exploits take advantage of direct parameter access? Give an example.
10. Define a *short write*. Give an example of using one in an exploit.

Deliverables. Submit the answers to the questions on **Beachboard Dropbox** by the indicated due date and time. Acceptable file submission formats are: .txt, .rtf, .odt, .doc, .docx, or .pdf.