

Discussion: According to the SANS Institute (one of the most highly respected organizations in the cyber industry and purveyor of cyber training and certifications) and MITRE Corp. (A Federally Funded Research and Development Corporation), the classic “buffer overflow” attack remains the #3 software vulnerability despite decades of awareness and response to the problem. It is therefore important to students to understand how they occur and how they are exploited.

Reading Assignment: Erickson, section 0x310-0x320, pp. 118-122.

1. Create a directory under your home folder named ‘SX7’. Copy the following files from the ‘booksrc’ folder to the ‘SX7’ folder:

hacking.h notetaker.c notesearch.c exploit_notesearch.c

Follow the author’s instructions on pp. 91-96 to compile the *notetaker* and *notesearch* programs and set permissions appropriately.

Remember to actually enter some notes!!!

2. Examine the *notesearch.c* source code in **nano**. Why is the resulting program vulnerable to a buffer overflow attack?

3. Why was it necessary to allow ‘setuid’ permission on these programs? Why is this particularly dangerous in this case?

4. Which user are you currently logged in as (**whoami**)?

5. Change back to your home directory(~).
 - a. Edit the file *unix_basics* with **nano**. Add a new line with your favorite command that isn't already on that list. Save the file and exit. Were you allowed to do this? Why?

- b. Navigate to the home directory for user **jose** (**/home/jose**). Create a file named 'virus'. (**touch virus**). What happened?

Why? What are your permissions on this directory? (**ls -la ..**)

- c. Try to delete some of the lines in a system configuration file that tells the computer how to boot up. (**nano /boot/grub/menu.lst**). What happened when you attempted to save this file? What permission do you have here?

- d. Attempt to modify system users. (**adduser bill**)
When prompted, enter password "goat14". Fill in anything you like for the remaining data.

Were you successful in doing this? Why/why not?

6. Now return to your 'SX7' directory, then compile and run *exploit_notesearch* **as shown** on pp. 121-122. Who are you now?

Run the following commands to restore your familiar *bash* shell.

➤ **export TERM=xterm**

➤ **su -**

7. What power do you now have?

How could this have been prevented?

8. Repeat the exercise in step 5 with your new-found power. Note the differences and implications in each step below.

a.

b.

c.

d.

Conclusion and Results:

Your typed lab report will consist of two paragraphs, in the first paragraph:

- Briefly describe what you did in the lab in your own words.
- Discuss something new that you learned.

In the second paragraph, answer the questions:

- How could an adversary use this knowledge or these tools for malicious purposes?
- How could you use your new understanding to protect your systems and personnel from attack?

Staple the completed report to the back of your original lab and turn it in to your instructor at the beginning of the next class.