**CSCE 629 Lab 3**

**Winter 2019**

**Buffer Overflows / Exploitation**

**Assigned: Lesson 9, 17 Jan**

**Due: Lesson 15, 29 Jan, 1400**

You must include these questions in your submitted solution. In other words, your submission must include the question listed followed by your solution with the answer clearly indicated (e.g., put a box or circle around the final answer). You will work with your partner and submit one solution.

**Buffer Overflow**

**Use Kali-Linux-2016.2 for problems 1 and 2. Newer versions of Kali will not work.**

1. Consider the program *bo-problem1.c* on the file server. It is similar to programs we discussed in class. Your assignment is to crash the program using a buffer overflow technique.

1. Assuming no canary, draw a diagram (memory map) showing the contents of the stack just before the **gets** instruction is executed. This diagram should look very similar to those on the course slides.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Memory Bank | |  |  |  |
|  |  |  |  |  |  |
|  |  | 03 | 03 | Buffer |  |
| 03 | 03 | 03 | 03 | Buffer |  |
| 03 | 03 | 03 | 03 | Buffer |  |
| f8 | 04 | bd | bf | EBP |  |
| 1e | 85 | 04 | 08 | return pointer | |

1. Predict the minimum number of characters the user must enter in order to crash the program. Remember, there is always a null character (\x00) appended to the end of strings. In other words, when you enter six B’s, seven bytes are actually stored in memory: BBBBBB\x00.

* 14, because the return pointer starts 15 bytes from the beginning of the buffer. Thus, we need a total of 14 characters input, plus the null character byte to reach the start (in memory) of return pointer.

c. Compile the code in Linux using the **–fno-stack-protector** option to disable the canary (stack protection). Depending on the operating system (and version) you are using, this switch may not work and you’ll have to account for the canary in your answer. Also use **–mpreferred-stack-boundary=2** and **–-param ssp-buffer-size=2** to effectively turn off boundary alignment and set the minimum buffer size to be protected to 2 bytes.

d. Disassemble the executable (**objdump –d a.out**) to determine the return address that will be stored on the stack. What is the return address?

e. Execute your code and enter “**0123456**”. On your screenshot of the results, circle each field listed in part (a) above (e.g., buffer, canary if it exists, SFP, RP). Do you see the return pointer in the correct location?

f. Enter progressively longer input strings until the program “crashes”. That is, enter **12345678**, then **12345679**, then **123456789a**, then **123456789ab** etc. What is the minimum number of characters required to crash the program? Ensure your screenshot shows the crashed program with your input visible.

g. Explain why it takes that number of characters to crash the program. Explain how the program crashed; in other words, how did the program become unstable? **Be very specific.**

2. Consider the program *bo-problem2.c* on the file server. We will use it to investigate the behavior of the stack, crash the program, and actually change a variable value using a buffer overflow. The last of these is probably the most pernicious.

a. Compile the code in Linux using the **–fno-stack-protector** option to disable the canary (stack protection). Depending on the operating system (and version) you are using, this switch may not work and you’ll have to account for the canary in your answer. Also use **–mpreferred-stack-boundary=2** and **–-param ssp-buffer-size=2** to effectively turn off boundary alignment and set the minimum buffer size to be protected to 2 bytes.

b. Execute the program and enter the letter B when prompted. Record the addresses of **x**, **user\_input** and **buffer** on the lines below.

**buffer \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**user\_input ­ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**x \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

c. Draw a memory map similar to the following example illustrating where each byte of the variables is stored in memory. You may shorten your addresses as shown below in red. Remember to include the SFP and return pointer.

|  |  |
| --- | --- |
| Memory Location (one byte) | Variable stored at that location |
| BF800D7C | Buffer[0] |
| 7D | Buffer[1] |
| 7E | Buffer[2] |
| 7F | Buffer[3] |
| 80 | Buffer[4] |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

d. Execute the program several more times in order to complete the following table. Stop executing the program once you see a segmentation fault. Record the contents (not the addresses) of the three variables. The input column (first column) indicates how many B’s to enter when prompted.

|  |  |  |  |
| --- | --- | --- | --- |
| **Input  (# of B’s)** | **buffer** | **user\_input** | **x (in hex)** |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| 11 |  |  |  |
| 12 |  |  |  |
| 13 |  |  |  |
| 14 |  |  |  |
| 15 |  |  |  |

e. Comment on the behavior of the three variables after you enter the B’s. That is, how are the three variables affected? I’m looking for a deep understanding of how the program is affecting memory. **Be very specific.**

f. Why does the program generate a Segmentation fault? Recall that **main()** is actually a function called by the operating system.

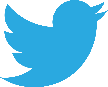
g. Assuming this program is used by an e-commerce site and x represents the cost of a hub in dollars, your mission is to pay exactly $33 (in decimal) instead of $100. Discuss how to accomplish this diabolical feat and then do it!!!!!!!!! Ensure your screenshot is legible.

**Exploitation**

**You may not use Armitage for question 3. You may use Armitage for question 4.**

During this course (including the remaining labs and final project), you may never change permissions on files or folders. This includes sharing a drive/folder such that anyone can gain access. Also, you may never start services that provide access to the target such as FTP, HTTP, RDP, etc. This includes creating a service that is password protected.

3. Using techniques you’ve seen, you will attempt to learn the contents of a flag file on a computer owned by Mullins Movies, Music, and Machines Inc. (M4I). Your reconnaissance indicates this computer is on the CDN network. The following questions will help guide your exploitation. Besides describing how you completed a task, provide the exact commands you used as well as screenshots of your results for each step. Be sure to only attack your target machine; verify by checking the computer name. You may not use Armitage for this question. Remember your target machine name ends with your team number (e.g., Target3). The following question will help guide your quest…

[](https://twitter.com/DrEvilM4I)

a. How did you learn the target computer name?

b. How did you identify the IP addresses of your target and the attacker (you)?

c. What is the target operating system?

d. How did you exploit the machine? Describe exactly how your exploited the machine. What vulnerability did you use? For example, the exploit uses a buffer overflow in application XYZ.

e. How did you establish a command shell from the target back to the attacker?

f. How did you search a computer for a specific file name?

g. How did you display the contents of a file?

h. Display the hostname and IP address within your metasploit console.

i. If you have made it this far, you can now answer the burning question… what is the message in the file?

4. Your target is a machine on the CDN that is listening on port 6667. What are the contents of the two flag files? What is the operating system? Verify you are attacking your team’s computer. If you exploit the machine, describe how the vulnerability is exploited. For example, the exploit uses a buffer overflow in application XYZ. You must demonstrate how to gain access to the target in two ways: one may be with Metasploit/Armitage but the second may not use Metasploit/Armitage. You may not use the same exploit for the second access.

**General Observations**

How long did it take you to complete this lab?

Was it an appropriate length lab?

What corrections and or improvements do you suggest for this lab? Please be very specific, and if you add new material, provide the exact wording and instructions you would give to future students in the new lab handout. You may cross out and edit the text of the lab on previous pages to make minor corrections/suggestions.