Homework#3 [35/100 points]

Assigned: March 30, 2018
Due: April 15, 2018

In this task of the assignment, you will use VirtualBox as your virtual machine. Download and install on your computer. You will also need to download the virtual image, in OVF format, prepared for this task at https://www.dropbox.com/sh/l4w3p64yq6cxdmj/AACLuWgb6G_wdJgJSiZx-DOia?dl=0 (1.75GB) then import the image to VirtualBox (you can do so by double-clicking on the image). The virtual machine runs a version of Ubuntu Linux. The username is "pcs" and password is "practical".

All the C programs for this task are located in directory projects/hw3. Source codes are not provided for questions 1-3.

1) [4 points] The checkdate program asks for a date in DD/MM/YYYY format, then checks if the date entered is valid or not. Is checkdate program vulnerable to a buffer overflow or a format string attack or both? Explain why you believe so?

2) [5 points] For ./login, your task is to bypass the verification process and gain access to the system. Upon successful, you'll see the message 'Welcome admin! Congratulations! You are now authenticated.' Show the input that you need to use and explain in detail on how you can achieve this. Note that guessing or obtaining the correct password will not be considered as bypassing the verification process for this task.

3) A 10-digit alphanumeric code 'key0982341' (without quotes) is hidden in the mykey.exe program. Your task is to exploit a format string vulnerability to gain read and write memory access at a specific location that stores the program's key. Answer the following questions.

   3.1 [3 point] Using gdb, what is the memory address of the key? Show how the memory address can be obtained.

   3.2 [4 point] By exploiting the format string vulnerability, show two different inputs (by using different format specifier) that you can use to view the key in the program.

   3.3 [4 point] You next task is to tamper with the key. You need to change the key to 'key098234i' (replace '1' with 'i'). What is your crafted input? Demonstrate in detail how you can achieve this.

4) Given a vulnerable program vuln.c and a shellcode below, answer the following questions. (for the executable used in this question, use vuln **not** vuln.exe)

   Shellcode:

   "\xeb\x18\x5e\x31\xc0\x88\x46\x07\x89\x76\x08\x89\x46\x0c\xb0\x0b\x8d\x1e\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\xe8\xe3\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68"

   4.1 [2 points] Explain how this program "vuln" is vulnerable to buffer overflow attacks.

   4.2 [2 points] If the shellcode is successfully injected and run, give one possible harmful consequence that can occur to the victim's host?

   4.3 [3 points] For this task, you need to overwrite the return address and get it to point to the inserted shellcode. How can you determine where your new return address should be placed? Show where in the memory (i.e. the memory address) that you need to overwrite with the new return address for the shellcode. (Hint: you can determine the address by causing the program to get a segmentation fault.)

   4.4 [4 points] What is the input that you need to provide as an argument for this program in order to spawn a shell? Full points will only be given if the input provided can be used to spawn a shell. Explain in detail how you craft the input. For this task, demonstrate the approach with gdb.

5) [4 points] Stack canaries are used to detect buffer overflow before the malicious code can get executed. Explain how the use of stack canaries can detect buffer overflow. Aside from obtaining or guessing the values of the stack canaries, are there any other approaches that an attacker can use to bypass this countermeasure? Discuss one such approach. You may need to use code to explain your answers.

This homework is to be done individually. You must write your answer *independently*.

There is no page restriction for this assignment.

To submit an assignment, log into home.nyu.edu, go to Academic -> NYU Classes -> Special Topic: Practical Computer Security -> Assignments, and upload your answer in PDF format. Make sure that you 'submit' the assignment before the deadline.

Late homework will be marked down by 10% for every day of lateness.