Assignment :: Common Vulnerabilities

Computer & Network Security
Cameron Reeves *cameron.reeves@uts.edu.au*

October 9, 2017

Due: 27/10/2017 at 23:59

Marking

- You are to work on this assignment individually.
- Answer the questions below in no more than three pages.
- Concise answers are good answers. Don't try and pad with generic information.
- Do not refer to code using screenshots. Format it neatly within your document if required.
- Ensure you read comments in included files for compilation and usage instructions.

1 Low Level Exploits (21 marks)

1.1 Savegames [10 marks]

Jimmy is becoming increasingly frustrated at the computer game hes playing. He has a save right before the levels boss but he needs either more health or more gold in order to win. The game is loaded from a normal file on disk but the health and gold are encrypted in some complicated fashion. The characters name is not, however.

Read and compile the C code in *savegame.c* using the command on line two and run *a.out* using the command line to answer the following questions.

1. Set the characters gold or health to a number greater than 9000 by utilising a buffer overflow. How did you achieve this? Explain using reference to bytes and ASCII as to what the exact value was that you achieved. [4 marks]
2. How could this exploit be prevented? [2 marks]
3. Could this exploit be useful for more than just the game? Could it be used to gain access to a system? If not, why not? If so, where might it be used? [4 marks]

1.2 General Questions [11 marks]

1. Why is it necessary for us to provide the flag *-fno-stack-protector* to GCC? What is a canary in terms of a buffer overflow and how can a canary prevent a buffer overflow exploit? [4 marks]
2. If the game above was written in Java instead of C, would the savegame still be exploitable? [2 marks]
3. Imagine you were exploiting a program that was running with escalated privileges (i.e. could read sensitive files, modify other users settings and so on) is it possible to obtain a BASH shell using buffer overflows? Be sure to explain what shellcode is and how the shellcode is executed[1]. [5 marks]

2 SQL Exploits (10 marks)

Read and run the Python code in *injection.py* using the command on line one to answer the following questions.

1. Show how it is possible to log in as any user by performing an SQL injection attack on the username/password login page. [2 marks]
2. The website has been clued in on their major security problem and pre-

[1] The traditional introduction to this topic is Smashing The Stack For Fun And Profit: *http://www.phrack.com/issues.html?issue=49&id=14*

vented the previous attack. Is it possible to use the status query to work out the password of one of the administrators *Bobby*[2]? [4 marks]

3. How can these attacks be prevented? Is it a difficult security problem to fix? Why is it so common? [4 marks]

[2] SQLite (the database in use here) doesnt allow multiple SQL statements to be executed in a single execute query consider using *substr* and subqueries