Project 3 :: Common Vulnerabilities

Computer & Network Security (Sydney University)
Luke Anderson *luke@lukeanderson.com.au*

May 2, 2015

Due: Part 3 is to be marked in labs on the 19th of May

Marking

- You are to work on this assignment in groups of 1 or 2. These groups do not have to be the same as those for your previous project.
- Answer the questions below in no more than three pages - concise answers are good answers. Diagrams are welcome where appropriate.
- Typed assignment and any relevant code is to be emailed to your tutor by the end of the tutorial. Late assignments will **not** be accepted.
- You are expected to demo the practical component of **Savegames** (1,2) and **SQL Exploits** (1) during class to demonstrate your understanding.
- Ensure any code and/or solutions employed are included in a legible and well documented fashion.

1 Low Level Exploits (30 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.

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 iCubeKinect [9 marks]

1. Why does the iCubeKinect system use an asymmetric cipher to verify their DVD games? Would it be possible to use a symmetric cipher instead? [3 marks]
2. What problem exists in the iCubeKinect verification code? How could you make the machine execute any arbitrary DVD[1]? [4 marks]
3. How would you fix it? Would the security vulnerability be made less serious by using either a stronger hashing scheme (such as SHA-512) or a different asymmetric cipher? [2 marks]

1.3 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[2].

[1] You may assume there are thousands of legitimate game / cert pairs to use to assist you.

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

[5 marks]

2 SQL Exploits (10 marks)

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 prevented the previous attack. Is it possible to use the status query to work out the password of one of the administrators *Bobby*[3]? [4 marks]
3. How can these attacks be prevented? Is it a difficult security problem to fix? Why is it so common? [4 marks]

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