Name: _____

CPSC 310A Final Exam

Dec. 12th, 2013

This is an open book, open note, open computer take-home final.
It is due Thursday, Dec. 12th, 2013 by 11:30 am.
Please submit a tar file of your answers via email.
There are 9 questions for a total of 100 points. There is one bonus question.

---

1. The three pillars of Computer Security are *Confidentiality*, *Integrity*, and *Availability*. Describe attacks on each of these, using topics discussed in class. **(10 points)**

2. An **Affine** cipher is a cipher of the form:

$$C_n = A \times P_n + B \mod M \tag{1}$$

   Where the key is the integers A, B, and M.

   - Is this a symmetric key cipher? Why or why not?
   - As it turns out, the Caesar cipher is a specialized form of an Affine cipher. What values of A, B, and M define a Caesar cipher?
   - The equation above defines how to encrypt messages using the affine cipher. What is the equation for decryption?
   - Write a $C++$ program that encrypts text using an affine cipher, where $A = 7$, $B = 2$, and $M = 26$. Use this program to encrypt the following message. Only encrypt the alphabetic characters, and process the letters so that you always produce alphabetic characters.

     ```
     you wanted to know who i am, zero cool? well, let me explain the new
     world order. governments and corporations need people like you and
     me. we are samurai... the keyboard cowboys... and all those other
     people who have no idea what's going on are the cattle... moooo.
     ```

   (20 points)

3. What is the difference between a public-key cryptographic system, versus a symmetric key cryptographic system? What challenges are present in one versus the other? Why would a programmer choose one over the other in a given implementation? Are there any possible solutions to these problems?

   (10 points)

4. Let $n = 491 \times 397$. Generate an RSA public key for the chosen private key 47. **(10 points)**

5. Consider the following, very simplistic definition of a hash function:

   ```
   Read a string bit by bit, until 512 bits are read.  Convert this bit
   stream into 128 hex digits, and output the result.
   ```

   - Write a $C++$ program that produces hashes of the above defined form. Produce a hash of the following input string.

     ```
     Of all the things that I've lost, I think I miss my mind the most
     ```

   - Is this hash definition secure? If so, explain why. If not, describe an attack that can be performed on this hash function.

   (15 points)

6. Describe how are SSL and TLS able to authenticate web servers as trusted entities? What additional mechanisms must be in place? **(10 points)**

7. Write a valid reduction for the hash specified in Question 5. This function should output an 8 character, lowercase alphabetic password. **(15 points)**

8. Using the Nebula game, we explored *privilege escalation* attacks. What was the purpose of these attacks? What element was necessary to allow root privilege shells to be created, versus a new shell as the current user? **(5 points)**

9. Stack based Buffer-Overflow attacks are extremely common in C and $C++$. However, they are all but impossible in languages like Python and Java. What mechanisms prevent these issues? What is the expense of these mechanisms? **(5 points)**

10. **Bonus:** There is a $C++$ program uploaded to the course website, that is vulnerable to a stack based buffer-overflow attack. Generate an input that would cause the program to authenticate you, without using the correct password. Is it possible to generate an input that would spawn a shell? **(5 points)**