Name: _____

ECE568S: Final Exam

Examiner: C. Gibson

Duration: 2.5 hours
Exam Type: C (single reference sheet, both sides)
Calculator Type: 4 (none)

1. Please use a **pen** to complete all of your answers.
2. Do not turn this page over until you have received the signal to start.
3. This exam is closed book. One double-sided, letter-sized (8.5"x11") reference sheet may be used. Use of calculators, computing and/or communicating devices is not permitted. Work independently.
4. Do not remove any sheets from this test book. Answer all questions in the space provided, unless otherwise indicated. No additional sheets are permitted.
5. The value of each question or part-question is noted next to the question. The total of all marks is 100.
6. Please write your name and student number in the space below, and write your name on the top of each sheet.

First Name: _____

Last Name: _____

Student Number: _____

Q1. _____ / 20	Q4. _____ / 15
Q2. _____ / 25	Q5. _____ / 15
Q3. _____ / 15	Q6. _____ / 10
	Total: _____ / 100

Name: _____

1. Short-Answer Questions (20 marks)

Please *briefly* answer the following questions, in the space provided. If you require more space, please indicate that you are continuing your answer on the back of the sheet, and put the question number next to the continuation of your answer.

a) Briefly describe the difference between *access control lists* and *capability-based access control*. **(4 marks)**

b) IPSec is composed of two protocols. Name (or briefly describe) the two different protocols, and list one advantage of each. **(2 marks)**

c) The Bell-LaPadula security model defines an information flow that is sometimes referred to as "read down, write up". What security property Bell-LaPadula is trying to protect, and how might that property could be compromised if the information flow were reversed? **(3 marks)**

d) With respect to covert channels, what is the *Non-Interference* property? **(3 marks)**

e) A normal TCP exchange begins with the client and server exchanging a "three-way handshake", in order to avoid simple "spoofing" attacks. Briefly describe one method a spammer might use to successfully send "spoofed" packets, with someone else's IP address, by using a compromised machine to start the TCP handshake. **(3 marks)**

f) Explain, with reference to the messages exchanged, how a mail server typically identifies candidate IPs to place onto an anti-spam *graylist.* **(3 marks)**

g) From the standpoint of legitimate users, what is the biggest disadvantage of graylisting as an anti-spam measure? **(2 marks)**

2. Code Vulnerabilities (25 marks)

The following program compiles and runs as described, but has one or more security vulnerabilities that can be exploited using techniques we've discussed in class.

a) (9 marks) Consider the following program:

```
01 #include <stdio.h>
02 #include <string.h>
03
04 void
05 reverse ( char * source, char * dest )
06 {
07      int i, len;
08      char temp[80];
09
10      strcpy ( temp, source );
11      len = strlen ( temp );
12
13      for ( i = 0 ; i < len ; i++ )
14           dest[i] = temp[len - i - 1];
15
16      dest[i] = '\0';
17 }
18
19 int
20 main ( int argc, char * argv[] )
21 {
22      char buffer[80];
23
24      if ( argc != 2 ) return (-1);
25
26      printf ( "%s backwards is ", argv[1] );
27      reverse ( argv[1], buffer );
28      printf ( buffer );
29
30      return (0);
31 }
```

When executed, the program reverses the contents of the first command-line argument:

```
$ ./question2 Hello
Hello backwards is olleH
$ ./question2
$
```

Assuming the above code is running on an ECF lab workstation, what exploitable security vulnerabilities exist in the code, if any? Provide your answer in the table on the following page, with specific details of how the exploit would work (see the example provided in the first line of the table, below).

Name: _____

Line #	Type of Attack	What value(s) would the attack try to overwrite, and why?	When would the attack trigger?
Example	*Denial of Service*	*Overwrite the "examplePointer" pointer, located in foo's stack frame, in order to cause a segmentation fault that crashes the server and makes it unavailable to other users.*	*When examplePointer is dereferenced on line 63.*

b) **(8 marks)** The question is sometimes asked: can we prevent stack overflow attacks by simply reversing the direction that the stack grows? Assume that the above program is now running on a redesigned system, in which arrays and the stack both grow in the same direction (*i.e.*, from smaller to larger addresses). Reexamine the program, and complete the following table by listing all of the exploitable security vulnerabilities, if any, that now exist in the code. Where your answer differs from part (a), please be specific.

Line #	Type of Attack	What value(s) would the attack try to overwrite, and why?	When would the attack trigger?

c) **(3 marks)** The shellcode that we used in labs #1 and #2 did some setup of its variables, and then trapped into the kernel by calling:

```
int $0x80       // machine code: 0xcd0x80
```

Consider what would happen if the architecture and operating system of the victim machine were redesigned, so that trapping into the kernel required raising a different interrupt:

```
int $0x100      // machine code: 0xcd0x10x00
```

What problem would that create for injecting our shellcode?

d) **(5 marks)** If the `int` instruction can only take a constant (*i.e.*, a fixed value, rather than a register) as a parameter, how could you alter the shellcode to fix the problem?

Name: _____

3. Viruses and Worms (15 marks)

Please *briefly* answer the following questions, in the space provided. If you require more space, please indicate that you are continuing your answer on the back of the sheet, and put the question number next to the continuation of your answer.

a) What is the difference between a polymorphic virus and a metamorphic virus? **(5 marks)**

b) Consider a polymorphic virus that first checks the time, and only decrypts itself and runs if it is between noon and 1pm. Explain how this minor change creates a significant problem for an anti-virus scanner that uses a "generic decryption" (GD) algorithm. **(5 marks)**

c) The authors of worms often create a "hit list" of machines to help launch the initial wave of worm propagation, and these machines often have specific properties that help in quickly spreading the worm. From what we have been able to determine, the Stuxnet worm used a very different "hit list" of machines for its initial infection; briefly explain how it differed from the usual "hit list", and why its propagation goals were different than traditional worms. **(5 marks)**

4. Encryption (15 marks)

Please *briefly* answer the following questions, in the space provided. If you require more space, please indicate that you are continuing your answer on the back of the sheet, and put the question number next to the continuation of your answer.

a) **(5 marks)** You and a friend have previously exchanged a secret key (**k**), and you want to use it to exchange encrypted messages. You are worried about the possibility of replay attacks, and decide on the following handshake protocol when you want to start a conversation:

- You pick a random nonce value (**n**) that has the same number of bits as **k**
- You compute the XOR of **n** and **k**, and send the resulting value (**n** ⊕ **k**) to your friend
- Your friend XORs that value with **k**, and sends the result ((**n** ⊕ **k**) ⊕ **k**) back to you
- If this value you receive back from your friend is the same as your original value **n**, then you know that you and your partner have the same shared key (**k**)

You then reverse the process, and exchange a similar set of messages in the opposite direction, with your parter picking their own value **n**. At the end of the exchange you will have both verified that the other party knows the secret key (**k**), and that this isn't a replay of a previous handshake.

There is a flaw in this protocol that makes it very easy for an attacker to discover your secret key (**k**). Briefly explain how this attack could work. (There are several variations possible: just describe one.)

b) Continuing the question from above, if you had a pair of previously-exchanged keys ($\mathbf{k_1}$ and $\mathbf{k_2}$), could you alter the algorithm to make it significantly harder for the attacker to discover the key? If so, explain how you could alter the algorithm. If not, explain why the flaw still exists. **(5 marks)**

c) Why do RSA Public Keys have to be so much longer than the keys used in symmetric key encryption, for the same level of security? (*e.g.*, a 1024-bit RSA modulus versus a 128-bit AES key.) **(5 marks)**

5. Diffie-Hellman (15 marks)

You decide that you are going to start a file-hosting service, similar to "Dropbox", that allows users upload their files onto an Internet-based virtual disk. Consider the following scenario:

- Instead of using usernames and passwords, you decide to use public key cryptography to authenticate your users.
- In order to keep the file transfers confidential, you decide to use a Diffie-Hellman exchange to establish a secret encryption key for each login session.

To implement the above, the following exchange takes place between a User (U) and the Server (S):

U → S: { g^u, U's public key }
U ← S: { g^s, S's public key, {g^u,g^s} signed with S's private key }
U → S: { {g^u,g^s} signed with U's private key }

The Server then grants the User access, and they share a secret cryptographic key (g^{us}). The User can check the name in the Server's public key, and verify that she's talking to the correct server.

a) Show that it's possible for Attacker (A), another user of the service, to do a "man-in-the-middle" attack on this protocol, such that the User thinks that she's talking to the Server, and that the Server thinks that it's talking to the Attacker. (Note that the Attacker will <u>not</u> be able to decrypt the communication between the User and the Server.) **(10 marks)**

b) Explain how this attack would violate the confidentiality of the User's data if she uploaded a file, even though the Attacker can't read the messages between the User and the Server. **(5 marks)**

Name: _____

6. Web Security (10 marks)

Please *briefly* answer the following questions, in the space provided. If you require more space, please indicate that you are continuing your answer on the back of the sheet, and put the question number next to the continuation of your answer.

a) Consider a website that allows users to change their passwords, using a web form that performs an HTTPS GET request. For example:

```
https://ece568.com/newPassword.cgi?newPass=5678&user=jskule&oldPass=1234
```

The newPassword.cgi script then executes a SQL statement, constructed as follows:

```
sql = "UPDATE user SET password='" & Request.QueryString("newPass") &
      '" WHERE username='" & Request.QueryString("user") &
      "' AND password='" & Request.QueryString("oldPass") & "';"
```

In the case of this example, it would generate the following SQL statement:

```
UPDATE user SET password='5678' WHERE username='jskule' AND password='1234';
```

This example will only update the record in the database if both the username and the "old" password match.

How could you alter the above GET request, to attack the script and change the password for "jskule" to "5678" even if you didn't know his existing password? (Provide the specific GET request.) **(5 marks)**

b) **(5 marks)** Consider a bank website, hosted at https://bank.com/, that uses HTTPS for all communication. Suppose that, two seconds after the user logs in, the bank's webpage fetches and executes some JavaScript from:

```
https://bank.com/scripts/
```

Recall that whenever a browser connects to a server using HTTPS, the server sends an SSL certificate to the browser, and the browser then verifies that the server's certificate is valid. However, suppose the victim has a web browser with a bug in the way that it treats SSL certificates: once a page has been retrieved over HTTPS, it assumes that all subsequent HTTPS requests to the same domain are a continuation of the same session and, thus, do not require a certificate check.

Briefly explain how a remote attacker could exploit this bug using DNS cache poisoning, to read the cookie of the banking webpage from a victim user. For this question, you may assume that the victim's browser does not cache the DNS responses, and performs a separate DNS lookup for each HTTPS request. (You do not need to explain the contents of the individual DNS messages involved, but you do need to be specific about the actions the attacker is taking.)