ERSS
Midterm

Name: NetID:

There are 5 questions, with the point values as shown below. You have 75 minutes with a total of 75 points. Pace yourself accordingly.

This exam must be individual work. You may not collaborate with your fellow students. However, this exam is open notes, so you may use your class notes.

I certify that the work shown on this exam is my own work, and that I have neither given nor received improper assistance of any form in the completion of this work.

Signature:

#	Question	Points Earned	Points Possible
1	Performance		9
2	HTTP		16
3	Daemons		14
4	Security		20
5	Resilience		16
	Total		75
	Percent		100

Question 1 Performance [9 pts]

1. What is the difference between latency and throughput?

2. Why is latency important in server software?

3. Why is throughput important in server software?

Question 2 HTTP [16 pts]

Suppose you type `http://awesome.com/l33t/hacker.html` into your browser.

1. To what server does your browser send an HTTP request?

2. What is the contents of the HTTP request that your browser sends (be as completed as possible)?

3. Suppose the requested page contains the bold face text **hello**. What is the contents of the entire response from the server (again, be as completed as possible)?

Question 3 Daemons [14 pts]

1. When a process wants to become a daemon, one of the first thing it does is fork, then the parent exits. Why does it fork and run as the child?

2. The daemon does some other things, then forks another time. What does this second fork accomplish?

3. Name one advantage of using multiple threads (as opposed to processes) for parallelism .

4. Name one advantage of using multiple processes (as opposed to threads) for parallelism .

5. Name one advantage of pre-creating threads or processes.

6. Name one advantage of creating a thread or process per request.

Question 4 Security [20 pts]

1. We discussed 4 important major aspects of security. Name each of them.

   (a)

   (b)

   (c)

   (d)

2. What is the proper way to store password information?

3. A _____ (fill in the blank) allows space-efficient pre-computation of hashes for password cracking if you do not correctly store the password information.

4. What is "key stretching" and why do you want it?

5. For each of the below scenarios, describe how an adversary could carry out an attack, and then identify the category your attack falls into (from the ones that Tara, Tami, and/or I discussed in class).

   (a) An important/sensitive website does not use https. Instead, the website uses a homemade encryption system which exchanges un-signed keys using Diffie Hellman. The attacker sits in a position where she can view/alter the network traffic between a victim and the vulnerable site (*e.g.*, an evil network administrator, or an attacker who has already compromised the network administration). Describe an attack where the attacker can obtain the victim's login credentials without the victim being aware of it.

   Category of attack:

   (b) You order crab in a restaurant, and the waiter brings it to your table to show you that it is alive right before it is cooked. The waiter then takes the crab back into the kitchen, then after a while, returns with your cooked crab. Describe an attack where a dishonest restaurant could serve you crab that was long dead.

   Category of attack:

Question 5 Resilience [16 pts]

1. Explain the concept of RAII.

2. Show an example of code which *does not* use RAII, and does not make exception guarantees.

3. Alter your example code above to use RAII.

4. What is the "universal HA topology" (which Tyler Bletsch mentioned repeatedly in his guest lecture)?

5. Why is mirroring not an adequate backup solution?