

SI110 – Introduction to Cyber Security
Technical Foundations

Fall AY2012 – Twelve Week Exam

Individual work.

Closed book. Closed notes.

You may not use any electronic device.

Your answers must be legible to receive credit.

On the front of every sheet, legibly write your

_____, _____, _____
Name Alpha code Section Number

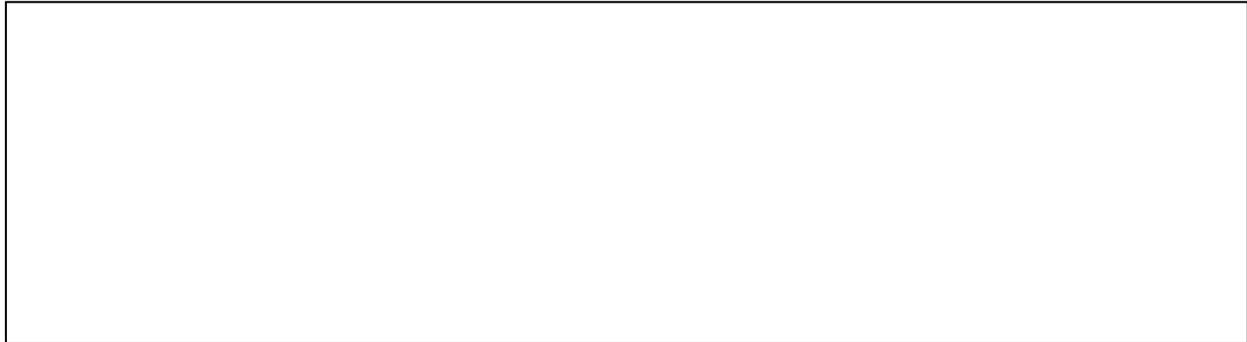
There are 25 questions on 8 pages.
Each problem is worth 5 points (125 total points).

A. Client-Side Scripting: Forms

1. Draw what appears when a file containing the following HTML is loaded by a browser:

```
<html>
  <head></head>
  <body>
    <form name="data" onsubmit="return false">
      <p>Name</p>
      First: <input type="text" name="first">
      Last: <input type="text" name="last">
    </form>
  </body>
</html>
```

Answer:



B. Server-Side Scripting

2. A file containing the following HTML is loaded by a browser:

```
<html>
  <head></head>
  <body>
    <form action="http://rona.cs.usna.edu/frt.jsx"
      name="FruitData" onsubmit="return false"
      method="get">
      Fruit: <input type="text" name="ft">
      Quantity: <input type="text" name="qy">
      <input type="button" onclick="submit()" value="send">
    </form>
  </body>
</html>
```

A user enters **"pear"** in the first input box, **"24"** in the other, then presses the send button. What URL is constructed by the browser? **Circle** your answer.

- a. `http://rona.cs.usna.edu/frt.jsxft=pear&qy=24`
- b. `http://rona.cs.usna.edu/frt.jsxFruit=pear&Quantity=24`
- c. `http://rona.cs.usna.edu/frt.jsx?Fruit=pear&Quantity=24`
- d. `http://rona.cs.usna.edu/frt.jsx?ft=pear&qy=24`
- e. `http://rona.cs.usna.edu/frt.jsx`

3. Suppose that, in the previous example, when the amount in the second input box is zero or negative, the server-side script `frt.jsx` crashes, in turn causing the whole webserver to crash. Why is client-side input validation (i.e. checking from within a script embedded in the HTML form that the value for the quantity is in fact greater than zero) not sufficient to stop an evil user from crashing the server?

C. Injection Attacks, XSS

4. Circle the correct word "client" or "server" in each underlined section below so that the text is accurate:

A "cookie" is a small piece of data stored on the hard-drive of the web
client / server. For a given site, the client / server asks the
client / server to store the cookie, and to then send it when any
"GET" requests are made by the client / server for files at the site.

5. Suppose you have an account at an auction website called `rockauction.com`. You receive an e-mail that tricks you into pointing your browser at the URL:

`http://rockauction.com/process.cgi?bidAmt=3000.00&bidItemNum=7826001`

"process.cgi" is a server-side script that places bids on items. Explain why a bid for \$3000 on item 7826001 will be registered in your name only if you happen to be logged into your `rockauction.com` account in your browser at the time you open your e-mail.

6. You input the following into a text input box labeled "Comments:" in a form on someone's blog web site:

What a <u>great</u> post! Funny!

After posting, your comment might render as one of the following

(A)

What a great post! Funny!

(B)

What a <u>great</u> post! Funny!

a. Which of these two possibilities would indicate that the site is protecting itself against injection attacks? Circle one: A / B

b. Justify your answer!

D. Networks & Protocols 1

7. Fill in the blanks:

A computer (in the most general sense) connected to the Internet is called a _____. When communicating on the internet (without DNS name resolution), the _____ to which data is to be sent is identified by its _____. Data to be sent across the Internet is broken up into small chunks which, together with the address of the recipient, forms what is called a _____.

8. When your browser visits the American Accordionists' Association (AAA) website

<http://www.ameraccord.com/newsletter.html>

... what server gets contacted *before* the browser sends a GET request to the AAA's webserver?

F. Networks & Protocols 2

9. Write the number of the protocol stack layer on the right that is associated with each of the service descriptions on the left:

- | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <p>___ a. moves bits over wires or through radio waves, etc.</p> <p>___ b. services for users</p> <p>___ c. moves IP packets from one host to another host.</p> <p>___ d. moves MAC-addressed data from one device to another within the same network.</p> <p>___ e. moves bytes from a process running on one host to a process running on another host.</p> | <p>(1) Application Layer</p> <p>(2) Transport Layer</p> <p>(3) Internet Layer</p> <p>(4) Link Layer</p> <p>(5) Physical Layer</p> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|

10. Circle the netcat (nc) command below that will connect to a webserver on host **131.122.88.22**

- | | |
|---------------------|------------------------|
| a. nc 131.122.88.22 | d. nc 131.122.88.22 53 |
| b. nc -l -p 53 | e. nc 131.122.88.22 80 |
| c. nc -l -p 80 | f. nc -l 131.122.88.22 |

G. Networks & Protocols 3 & 4

11. Fill in the following table

Protocol	Service	Tool
	world-wide web	
	secure remote shell	
	secure file transfer	
	secure web traffic	

12. Suppose you visit the index.html page at foo.bar.org, the content of which is:

```
<html><body>The coordinates are 38deg 59'N 76deg 30'W</body></html>
```

Describe the difference between what a bad guy snooping your network traffic would see if you pulled up the page as

http://foo.bar.org/index.html versus **https://foo.bar.org/index.html**

H. Networks & Protocols 5 & Build-a-LAN Lab

13. On the left are listed three ways of identifying computers for network communication. Match them to a correct description from the right:

- ___ a. MAC address 1. can be changed, used by the Internet Layer
- ___ b. IP address 2. easy for people to remember, but cannot be used directly to communicate between hosts
- ___ c. domain name 3. unchangeable, used by the Link Layer

14. **My** IP address is 131.122.88.132. I give the command **tracert 192.190.229.27** and get the following output:

```
1 131.122.88.250 0.620 ms 0.611 ms 0.613 ms
2 10.0.1.21      0.915 ms 0.907 ms 1.136 ms
3 10.0.1.6       2.045 ms 2.047 ms 2.428 ms
4 131.122.6.249 0.528 ms 0.521 ms 0.513 ms
5 192.190.229.27 0.798 ms 0.799 ms 0.791 ms
```

What is the IP Address of **my** gateway router? Answer:

15. My IP address is 131.122.88.132. If I give the command **tracert 131.122.88.120** (where 131.122.88.120 is a host on the same network), what will its output look like? (Ignore the timing data and just list IP Address information)

I. Wireless Networking & Build-a-WLAN Lab

16. Which of the five network protocol stack layers change when moving from wired to wireless networks?

17. Suppose you have a base station with five host-stations connected wirelessly and that's it. Explain why any one of the five host stations can ping any of the other four host-stations, but none of them can ping any other host? (like rona.cs.usna.edu, www.google.com, etc).

J. Information Assurance

18. List the "five pillars of IA":

19. Suppose you run a small company, whose business is conducted solely through its website, `www.foobars.com`. One of the pages on your website uses a server-side script `order.cgi`, which doesn't validate its input very well, so that if a user enters an unexpected value in the online form, it crashes your whole webserver, losing you business as customers go elsewhere. A hacker working for a rival firm figures this out and keeps sending bad input to the form, which keeps crashing your server and losing you business. Match the following:

- | | |
|----------------------------------------|--------------------------------------------------|
| <input type="checkbox"/> Threat | a. Server crashes on certain kinds of bad inputs |
| <input type="checkbox"/> Exploit | b. Hacker from other firm |
| <input type="checkbox"/> Vulnerability | c. Loss of customers and money |
| <input type="checkbox"/> Impact | d. Inputting bad value to form and submitting it |

20. In the scenario from the previous question, which one of the five pillars did you fail to maintain?

21. Suppose you administer a small network, connected via a router to the Internet. You require hosts on your network to be able to SSH to one another, but this is a security risk, so you install a firewall that drops all traffic coming into your network bound for SSH's port. What part(s) of the risk equation goes (go) down ?

K. Firewalls

22. Recall that SSH uses port 22 and DNS uses port 53. Suppose we have the following network configuration, in which the firewall forwards all traffic with destination port equal to 22, and drops everything else:



- a. Can host 3.3.3.8 access a DNS-server running on host 2.2.2.5? Explain!
- b. Can host 3.3.3.8 access a SSH-server running on host 2.2.2.5? Explain!

23. Previous problem scenario is repeated: Recall that SSH uses port 22 and DNS uses port 53. Suppose we have the following network configuration, in which the firewall forwards all traffic with destination port equal to 22, and drops everything else:



a. Can host 2.2.2.4 access a DNS-server running on host 2.2.2.5? Explain!

b. Suppose host 3.3.3.8 has running in its terminal window (command-shell window) an SSH connection to host 2.2.2.4

If the command `nslookup red.rider.org 2.2.2.5` were typed into that window, would the query be received by nameserver 2.2.2.5, or would the firewall prevent that? Explain!

L. Symmetric Cryptography

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

24. Decode the following message, which has been encrypted with Caesar Shift encryption using a shift of 2.

Cyphertext: NQQMUQM

Plaintext:

25. If you are setting up secret communication using a Vigenere Cipher, what kind of key will give you the strongest encryption?