SI110: Introduction to Cyber Security, Technical Foundations

Fall AY2013 – 12-Week Exam

Individual work.
Closed book. Closed notes.
You may not use any electronic device.

Your answers must be legible to receive credit.

Each of the 30 problems is worth 5 points.

On the front of every sheet, legibly write your

Name: _____, Alpha: _____, Section Number: _____

ASCII Table for Printable Characters

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
32	20		43	2b	+	54	36	6	65	41	A	76	4c	L	87	57	W	98	62	b	109	6d	m	120	78	x
33	21	!	44	2c	,	55	37	7	66	42	B	77	4d	M	88	58	X	99	63	c	110	6e	n	121	79	y
34	22	"	45	2d	-	56	38	8	67	43	C	78	4e	N	89	59	Y	100	64	d	111	6f	o	122	7a	z
35	23	#	46	2e	.	57	39	9	68	44	D	79	4f	O	90	5a	Z	101	65	e	112	70	p	123	7b	{
36	24	$	47	2f	/	58	3a	:	69	45	E	80	50	P	91	5b	[	102	66	f	113	71	q	124	7c	|
37	25	%	48	30	0	59	3b	;	70	46	F	81	51	Q	92	5c	\	103	67	g	114	72	r	125	7d	}
38	26	&	49	31	1	60	3c	<	71	47	G	82	52	R	93	5d	]	104	68	h	115	73	s	126	7e	~
39	27	'	50	32	2	61	3d	=	72	48	H	83	53	S	94	5e	^	105	69	i	116	74	t			
40	28	(	51	33	3	62	3e	>	73	49	I	84	54	T	95	5f	_	106	6a	j	117	75	u			
41	29	)	52	34	4	63	3f	?	74	4a	J	85	55	U	96	60	`	107	6b	k	118	76	v			
42	2a	*	53	35	5	64	40	@	75	4b	K	86	56	V	97	61	a	108	6c	l	119	77	w			

hex digit	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
4-bit pattern	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

File Type	Header (Hex)	Header (ASCII)
png	89 50 4e 47	.PNG
jpg	FF D8 FF E0	ÿØÿà
bmp	42 4D	BM
avi	52 49 46 46 xx xx xx xx 41 56 49 20 4C 49 53 54	RIFF.... AVI LIST
mpg (video)	00 00 01 Bx	....
wav	52 49 46 46 xx xx xx xx 57 41 56 45 66 6D 74 20	RIFF.... WAVEfmt
xls	D0 CF 11 E0 A1 B1 1A E1	ÐÏ.à¡±.á
mp3	FF Fx	ÿ.
pdf	25 50 44 46	%PDF
zip	50 4B 03 04	PK..

⊕ Consider the following HTML document:

```
<html>
  <body>
    The <u id="foo"
           onclick="document.getElementById('bar').innerHTML='mountains'"
           style="color: green">rain</u>
    in Spain falls mainly on the <b id="bar">plain</b>.
    </body>
</html>
```

1. What is the value of document.getElementById('foo').innerHTML?

2. How does the appearance of the webpage change when the user clicks on the word 'rain'?

3. In the above HTML code, circle the names (only names!) of all the attributes defined for the u element.

4. Box the the entire b element in the above HTML.

---

5. Suppose Midn Jones has an amazon.com account (with username smurfdog86), which he has only ever accessed from his own laptop. One day he borrows his roommate's laptop and pulls up http://amazon.com in a browser window and, before he even has a chance to log in, sees near the top "Welcome back smurfdog86". Explain why he is surprised ... and angry.

6. Suppose an e-mail is sent to all Midshipman at USNA that includes an attachment that the e-mail asks them to open. The attachment contains the following piece of embedded Javascript:

```
<script type="text/javascript">
   document.location="http://rona.cs.usna.edu/~stahl/msg/mb.cgi?msg=GOARMY";
   </script>
```

Under exactly what circumstances will a midshipman post the message GOARMY to Dr. Stahl's message board as a result of this e-mail?

⊕ Consider the following HTML document:

```
<html>
    <body>
      <form name="time" action="http://bruise.usna.edu/proc.jsx">
        I spend
        <input type="text" name="perc" value="50">
        % of my day on SI110 homework.
        <input type="button" value="submit it"
                onclick="var x = Number(document.forms.time.perc.value);
                         if (0 <= x  && x <= 100)
                           submit();
                         else
                           return false;
                        "
                >
      </form>
    </body>
  </html>
```

7. Draw what this page looks like when it is first loaded.

8. If the user enters 83 in the input box and clicks submit, what is the URL that gets pulled up by the browser?

9. This form does client-side validation. Give an example of a value the user could enter in the input box that would not pass the client side validation, i.e. would not be submitted?

10. Even though this page has input validation, it is possible for a user to submit invalid input to the script proc.jsx. Describe what the user would do to accomplish this.

11. Suppose you enter the URL http://www.islesurfboards.com/index.html into your browser's address bar and press enter. What server gets contacted before your browser attempts to send a GET request to islesurfboards.com's webserver?

12. 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 are called _____.

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

___ a. moves MAC-addressed data from one device to another within the same network

___ b. moves bits over wires or through radio waves, etc.

___ c. moves packets from one host to another host.

___ d. moves bytes from a process running on one host to a process running on another host.

___ e. services for users

(1) Application Layer

(2) Transport Layer

(3) Internet Layer

(4) Link Layer

(5) Physical Layer

14. Fill in the following table:

Service	**Protocol**	**Port**	**TCP/UDP**	**Tool**
secure remote shell			TCP	
name resolution			UDP	
world wide web			TCP	
secure web		443	TCP	

15. Suppose you have the following output from netstat -an

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:20	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	10.17.3.88:51654	10.53.43.80:22	ESTABLISHED
TCP	10.17.3.88:48771	10.1.122.97:80	ESTABLISHED

Based on the netstat output:

a. This host is running an SSH server: T / F
b. This host is running an SSH client: T / F
c. This host is running a DNS server: T / F
d. This host is running an HTTP server: T / F
e. This host is running an HTTP client: T / F

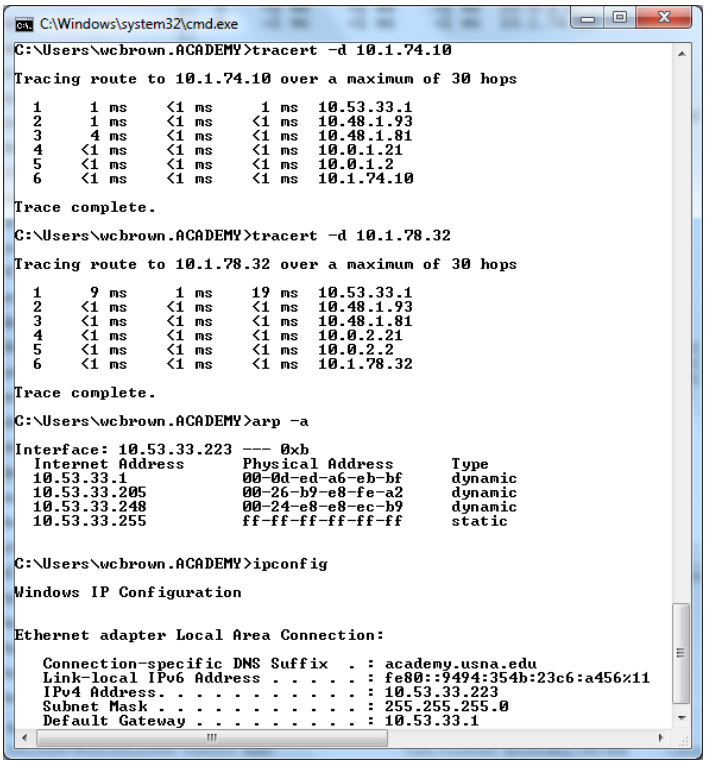
16. We built Ethernet networks and 802.11 (WiFi) networks in the two networking labs.

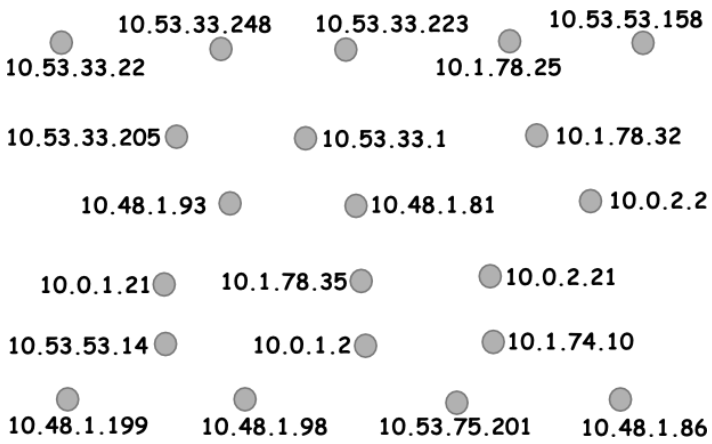
T / F : Ethernet & 802.11 involve the Application Layer
T / F : Ethernet & 802.11 involve the Transport Layer
T / F : Ethernet & 802.11 involve the Internet Layer
T / F : Ethernet & 802.11 involve the Link Layer
T / F : Ethernet & 802.11 involve the Physical Layer

17. Suppose you are on an open (i.e. no WEP / WPA1 / WPA2) WiFi network at a coffee shop. A bad person is evesdropping on everyone's traffic, i.e. monitoring each packet that gets sent across a network. Explain (thoroughly!) why you would be in trouble logging into your account at http://tubaworld.com/login.html but not at https://piccoloplanet.org/login.html.

18. In the wireless lab, we saw that there are two things that must be done to secure a WiFi base station that is "just out of the box", i.e. has the factory default settings. What are they?

⊕ Consider the terminal window below, which shows output from an arp -a command, two tracert's and an ipconfig.





19. Next to the terminal image is a diagram in which dots represent hosts, each labeled by an IP address. Given the terminal output, draw lines between each pair of dots that you can tell have a direct connection from the Internet Layer's perspective. In other words, there may be switches or base stations or other link-layer devices in between, but from the Internet Layer's perspective they are directly connected because they can communicate without a router in between them.

20. Continuing from above: What is this host's IP address? _____

21. Continuing from above:
What is the MAC address of this host's Gateway Router? _____

22. Continuing from above:
Which host is 10.1.74.10's Gateway Router? _____

23. The five pillars of IA are: _____ _____

_____ _____ _____

⊕ Suppose Professor Doris Locket runs a small message-board style website for her English class. The message board is mostly for social chatting amongst her students, although she also uses it to post homework assignments for her class. Unfortunately, her message board doesn't do any input sanitization, and a disgruntled student named Isis Chut, whom Prof Locket rudely awakened too many times in class, carries out an injection attack so that anyone who views the message board is instantly redirected to www.maroon5.com.

24. Continuing from above:
Which pillar of IA is attacked? _____

25. Continuing from above, match:

____	threat	a. injection attack
		b. can't read/post to message board
____	vulnerability	c. Isis Chut
		d. Doris Locket
____	impact	e. Maroon5
		f. no input validation / sanitization
____	exploit	g. English class

26. Continuing from above:
Use labels ↑, ↓, — to show how the various factors in the risk equation go up, down or stay the same when the stated action is taken. Note: We are talking about *the risk involved with Prof Locket providing this message board service*.

	threat	vulnerability	liklihood	impact	risk
Use email instead of message board to send out HW assignments	_____	_____	_____	_____	_____
Be nicer to students, let them sleep, etc.	_____	_____	_____	_____	_____
Add server-side code that rejects any message board post that includes the characters < and >.	_____	_____	_____	_____	_____

27. Ceasar-Shift Cipher encrypt the following with shift value (secret key) 4:

    Plaintext : O G R E [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]

    Ciphertext: _____

28. Suppose your SI110 class is playing around on the SI110 message board while your professor drones on and on. You decide you'd like to have a secure conversation with user KoolKat99, although you don't know which of your classmates that might be. Assume you are both familiar with the Vigenere Cipher (as all SI110 students are!), what makes it difficult to carry out a Vigener-Cipher-encrypted, SI110-message-board conversation between you and KoolKat99 with any hope of keeping it secure?

29. If two hosts are on the same network then ... (circle all that *must* be true)

    a. they have the same MAC address

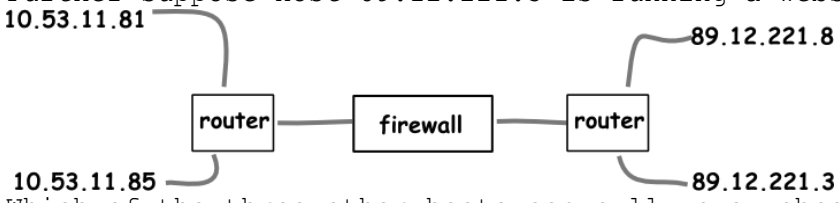
    b. they have the same IP address

    c. they have the same network address

    d. they have the same subnet mask

    e. they have the same ports open

30. Consider the following scenario, with several hosts and routers and a firewall. The firewall drops all traffic with destination port 80, in both directions. Further suppose host 89.12.221.3 is running a webserver.



Which of the three other hosts can pull up a webpage from the server running on 89.12.221.3. Justify your answer!