SI110 – Introduction to Cyber Security
Technical Foundations

Spring AY2012 12-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

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..

Client-Side scripting (non-event driven)

1. (5 Pts) Draw what would appear in a browser if the following HTML file was loaded.

```
<html>
  <body>
    Testing
    <script type="text/Javascript">
      document.write("1");
      document.write("2");
      document.write("3");
    </script>
    <p>Testing completed!</p>
  </body>
</html>
```

Client-Side scripting (event driven)

2. Consider the following HTML.

```
<html>
  <body>
    Travelling through the
    <b onmouseover='document.location="http://www.usafa.af.mil"'
       style='color: red'
       id='surprise'
       >Bermuda Triangle</b>
    is dangerous.
  </body>
</html>
```

a) (5 Pts) Describe the dynamic/interactive behavior of this page.

b) (5 Pts) What are the names (not values) of the attributes defined for the "b" element in this page?

c) (5 Pts) What is the value of **document.getElementById("surprise").innerHTML** ?

Client-Side scripting (forms) & Server-Side scripting

3. Consider the following web page:

```
<html>
  <body>
    <form name="ineq"  action="http://frmgort.com/gawrp.jsx">
      Distance 1:
      <input type="text" name="d1" value="0">
      and Distance 2:
      <input type="text" name="d2" value="0">
      <p>
       <input type="button" value="send"
              onclick='var x = Number(document.forms.ineq.d1.value);
                       var y = Number(document.forms.ineq.d2.value);
                       if (y < 0)
                         return false;
                       else
                         submit();'>
      </p>
    </form>
  </body>
</html>
```

a. (5 Pts) Draw what this page looks like when it is first loaded.

b. (5 Pts) This page does input validation. Referring to your drawing, give an example of input the user could enter (show what values and where they would be entered) that would not pass the validation, i.e. would not be submitted.

c. (5 Pts) If the user entered 23 in the first box and 112 in the second box, then clicked submit, what URL would get visited as a result?

d. (5 Pts) Explain why the input validation on this page is not sufficient to ensure that the server-side script gawrp.jsx never gets executed with "bad" input?

Injection & XSS attacks

4 (5 Pts) Suppose you are looking at a blog that allows comments to be entered. You enter the following into the comment box:

```
one <script type="text/Javascript">two</script> three
```

Which one or more of the following rendered results would indicate that an injection attack on the blog probably will NOT work?

a. one three

b. one two three

c. one <script type="text/Javascript">two</script> three

5 (5 Pts) Suppose you have an account on a hot new social media site - faceboard.com. Your account name is "mid15". In a desperate attempt to get faceboard friends, you send phishing e-mails out that trick recipients into pointing their browsers at the URL

http://faceboard.com/sendFriendRequestTo.jsx?name=mid15

which is the mechanism faceboard uses to make friend requests. Explain why even if a person receiving the e-mail has a faceboard account, and even if they do open the e-mail and fall for the trick, a friend request still might not be sent from the account.

Networks and protocols 1

6. (5 Pts) 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 _____.

7. (5 Pts) Which of the hex strings could represent the bytes of an IPv4 or an IPv6 address?

a. 8e07 IPv4 / IPv6 / neither (circle one)

b. 8e07a1bf IPv4 / IPv6 / neither (circle one)

c. b3ff7842e92023b4 IPv4 / IPv6 / neither (circle one)

d. b3ff7842e92023b4b3ff7842e92023b4 IPv4 / IPv6 / neither (circle one)

8. (5 Pts) When you enter the URL **http://xkcd.com/326/index.html** into your browser's address bar, what server gets contacted before the browser sends a GET request to the web-server xkcd.com?

Networks and protocols 2

9. (5 Pts) 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 IP packets from one host to another host.

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

___ c. services for users

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

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

(1) Application Layer

(2) Transport Layer

(3) Internet Layer

(4) Link Layer

(5) Physical Layer

10. (5 Pts) Suppose Alice is on host 131.127.89.20 and gives the command **nc -l -p 18101** and that Bob is on host 131.127.89.58 and gives the command **nc -l -p 17123** . Finally, suppose that Eve is on host 131.127.89.66 and she wants to connect to Alice in order to carry on a netcat chat session. What Windows shell command should Eve give in order to do this?

_____

Networks and protocols 3 & 4

11. (5 Pts) rona has both a web-server and an ssh-server running. When data gets sent to rona over the internet, how does rona's operating system know whether that data is supposed to go to the web-server or the ssh-server?

12. (5 PTs) Suppose ITSD monitors all of your outgoing network traffic. Would using HTTPS (as opposed to HTTP) to visit the website usma.edu mean that ITSD would know

a. both that you visited the usma.edu website, and which pages you looked at, or

b. that you visited the usma.edu website, but not which pages you looked at, or

c. which pages you looked at, but not that they were on the usma.edu website, or

d. nothing about which pages or which websites you visited.

Circle the letter that is your answer, and explain why you think it is correct.

13. (5 Pts) If you are logged into host foo.usna.edu and you give the command **netstat -a** and see that there is a process listening on port 80, what does that tell you?

14. (5 Pts) Fill in the following table:

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

Networks nuts and bolts / build-a-LAN

15. (5 Pts) Suppose your host has IP address 131.122.89.71. Here are two possible output of the command **tracert 131.122.89.25**

a. 1) 131.122.89.25

b. 1) 131.122.89.88
   2) 131.122.89.25

What would it mean if you got output (a) as opposed to output (b)?

16. (5 Pts) Suppose you have two hosts and you want to determine whether they are on the same network. Which piece(s) of information about these hosts would you need in order to determine whether or not they are on the same network (circle one or more):

a) MAC addresses c) subnet masks e) link-layer protocols (e.g. WiFi or Ethernet)

b) IP addresses d) port numbers

17. (5 Pts) Suppose **I** give a traceroute (tracert) command and get the following output:

```
 1  101.149.87.150  0.449 ms  0.430 ms  0.671 ms
 2  101.149.2.21  0.666 ms  0.662 ms  0.653 ms
 3  101.149.2.6  0.968 ms  1.265 ms *
 4  31.122.66.249  0.938 ms  1.215 ms  1.209 ms
 5  31.122.66.222  1.856 ms  1.852 ms  2.127 ms
```

What is the IP address of **my** gateway router? _____

Wireless Networks nuts and bolts / build-a-wireless-LAN

18. (5 Pts) Which of the five network protocol stack layers change when moving from wired to wireless networks?

19. (5 Pts) If you get a brand new WiFi base station straight out of the box, what two steps should you take to make using it more secure? Hint: "change the SSID" is not a good answer!

20. (5 Pts) A WiFi base station typically has one wired ethernet port on it. This is useful for configuring the base station, but why else is it needed?

Information Assurance

21. (5 Pts) What are the "five pillars of IA"?

_____ _____ _____

_____ _____

22. (5 Pts) Suppose you have a WEP-protected WiFi base station at home. Natasha Fatale sneaks within range and cracks your WEP key. She then sets up her laptop to send spam out through your WiFi network. Eventually, your ISP (Internet Service Provider) realizes that tens of thousands of spam e-mails are being sent from your network and not only turns off your internet access, but convinces the FBI to press charges against you for "spamming activities". Match the following:

____ a. threat	(1) weak encryption protocol in WEP
____ b. vulnerability	(2) cracking WEP
____ c. impact	(3) Natasha Fatale
____ d. exploit	(4) loss of internet access, and legal troubles

23. (5 Pts) Choose **two** pillars of IA and explain how they are violated in the previous example.

24. (5 Pts) FTP is an insecure file transfer protocol that uses port 21. Suppose USNA allows FTP to be used without any restriction. Later, suppose USNA adds a firewall that blocks all port 21 traffic from entering or leaving the USNA network. As a result of the firewall being added:

a) Do "vulnerabilities" increase / decrease / stay-unchanged ? Circle one and explain!

b) Do "threats" increase / decrease / stay-unchanged ? Circle one and explain!

Firewalls

25. (5 Pts) Suppose you have a firewall with just one host (10.1.1.42) behind it, and suppose host 10.1.1.42 runs a webserver. You want to allow access to the webserver from all hosts except 131.122.88.91, and you don't want any other services on 10.1.1.42 to be accessible to anyone. Place the following rules in the correct order to form an ACL for the firewall that achieves these goals.

a. **Drop** packets from IP **ANY** going to TCP port **ANY** on IP **10.1.1.42**

b. **Forward** packets from IP **ANY** going to TCP port **80** on IP **10.1.1.42**

c. **Drop** packets from IP **131.122.88.91** going to TCP port **ANY** on IP **10.1.1.42**

Rule 1. _____

Rule 2. _____

Rule 3. _____