SI110: Introduction to Cyber Security, Technical Foundations

Spring AY2013 – 12-Week Exam

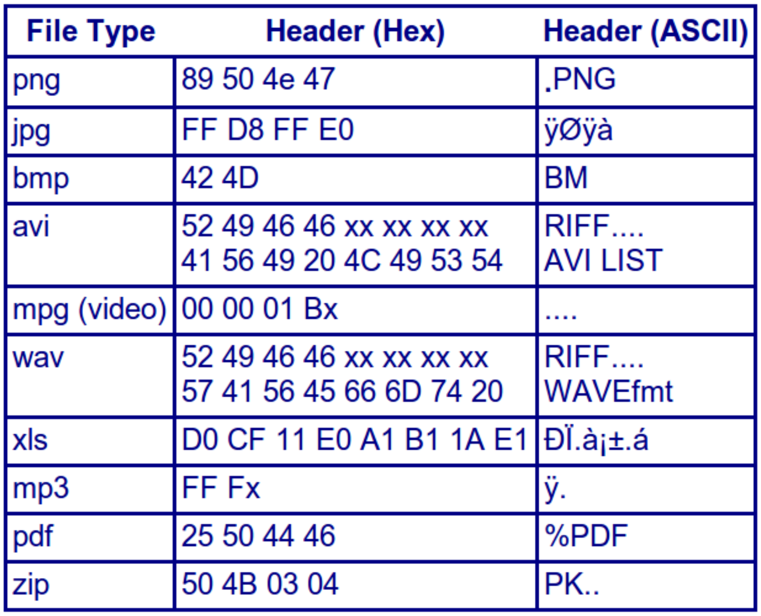
Individual work.
Closed book. Closed notes.
You may not use any electronic device.
Your answers must be legible to receive credit.
Each of the 22 problems is worth 5 points.
On the front of every sheet, legibly write your

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..

1. 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 harddrive 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.

2. Suppose you have an account at midblog.net, which you use to post your musings on life, the universe and everything. An evildoer wants to plant an embarrassing post on your account. So he tricks you into clicking on a link that sends your browser to:

   http://midblog.net/pst.jsx?newpost=GO_ARMY_BEAT_NAVY

   Explain why it is that the terribly embarrassing message will only actually be posted if you are logged into your midblog account at the point in time at which you click on the link.

3. 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 ___________.

4. For each blank below, write the number of the description that best matches.

   a. ____ Application Layer

   b. ____ Transport Layer

   c. ____ Internet Layer

   d. ____ Link Layer

   e. ____ Physical Layer

   1. moves bytes from a process running on one host to a process running on another host.
   2. services for users
   3. moves bytes from a file on the harddrive into RAM
   4. moves packets from one host to another host.
   5. moves bits over wires or through radio waves, etc.
   6. moves MAC-addressed data from one device to another within the same network
   7. responsible for deciding which process gets to use the CPU.

5. Which of the five network stack layers change when moving from a wired ethernet network to a wireless WiFi network?

6. You and your friends set up a network by plugging into a switch, and then connecting the switch to a router with ethernet cables. Then you all configure your hosts (no DHCP for you!). You try pinging one of your friends on the network using the IP address 85.170.15.3 he was supposed to use, and it works (as does pinging your other friends on the network). You remember that www.usna.edu's IP address is 136.160.88.128, so you try **ping 136.160.88.128** and it fails. Given all this, for each of the following network configuration tasks circle the most likely answer:

a. set my host's MAC address : not my job I probably did it I probably didn't do it

b. set my host's IP address : not my job I probably did it I probably didn't do it

c. set my host's subnet mask : not my job I probably did it I probably didn't do it

d. set my host's Gateway IP : not my job I probably did it I probably didn't do it

e. filled in my host's ARP table: not my job I probably did it I probably didn't do it

7. Suppose you have the following **netstat -an** output (line numbers added):

```
0: Proto Local Address      Foreign Address    State
1: TCP   0.0.0.0:20         0.0.0.0:0          LISTENING
2: TCP   0.0.0.0:22         0.0.0.0:0          LISTENING
3: TCP   0.0.0.0:80         0.0.0.0:0          LISTENING
4: TCP   10.53.33.223:139   0.0.0.0:0          LISTENING
5: TCP   10.53.33.223:49227 10.53.16.44:22     ESTABLISHED
6: TCP   10.53.33.223:49229 10.53.53.15:80     ESTABLISHED
7: TCP   10.53.33.223:49230 199.204.165.47:443 ESTABLISHED
8: UDP   0.0.0.0:53         0.0.0.0:0          LISTENING
9: UDP   0.0.0.0:64         0.0.0.0:0          LISTENING
```

a. Line ___ shows that I'm running a DNS server

b. Line ___ shows that I'm running an http server

c. Line ___ shows that I'm running an https client

d. Line ___ shows that I'm running an ssh client

e. Given that you were doing some online banking when this
netstat output was captured, navyfederal.org's IP address is ___________________________.

8. The following describes a scenario in which Host A sends data to Host B. Fill in the blanks.

Host A wants to send a packet to Host B. Host A computes the network addresses for itself and Host B based on the two IP Addresses and its own _________________________. It discovers that the two network addresses are different. So it sends the packet to the MAC address of its ____________________________.

9. The five pillars of IA are: __________________________ __________________________

__________________________ __________________________ __________________________

10. Midn Truss has an English professor who keeps his grades using an on-line gradebook at www.toughgrader.net. Though he's a world-renowned expert on the use of commas in late 18th Century Scottish poetry, he's not well-versed in cyber security. So an unscrupulous classmate, Midn Noone, who keeps trying to login to the prof's account with different password guesses eventually gets in with the password "monkey". Once in, Midn Noone changes all her C's and D's to A's, and also changes Midn Truss's A's to F's. Match each blank with one letter.

_____ Threat

_____ Vulnerability

_____ Exploit

_____ Impact

a. Midn Truss
b. English Professor
c. Midn Noone
d. Truss's grade is too low, Noone's grade too high
e. password guessing
f. weak password
g. not using salting and hashing
h. improper use of commas

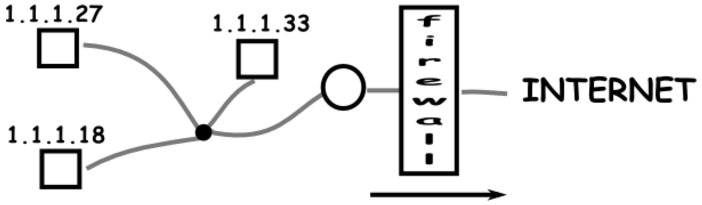
11. Continuing in the scenario from the previous example, circle all of the measures in the list below that would have helped thwart this particular attack.

a. salting passwords
b. two-factor authentication
c. hashing passwords
d. using https
e. password throttling

12. 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 the English prof having a toughgrader.net account*.

action	threats	vulnerability	likelihood	impact	risk
the prof goes back to a paper gradebook for himself, using the website only to make grades available for students to look at	______	______	______	______	______
the prof chooses a new super-secure password	______	______	______	______	______
the prof gives all of his sections a good tongue-lashing accusing them all of being no good hackers who wouldn't know a properly used comma if it bit 'em in the backside ... and lowers all their grades 10 points just because he can	______	______	______	______	______

13. Consider the following network diagram & firewall, along with an ACL for outgoing packets. (Assume default ports for services!)



Outbound firewall rules

action	tcp/udp	sourceIP	destIP	port
drop	tcp	1.1.1.33	x.x.x.x	80
forward	udp	1.1.1.33	x.x.x.x	53
forward	tcp	1.1.1.x	x.x.x.x	80
drop	both	1.1.1.x	x.x.x.x	x

a. Can host 1.1.1.27 access a webserver at 22.105.7.88? yes / no

b. Can host 1.1.1.27 access a nameserver at 22.105.7.88? yes / no

c. Can host 1.1.1.27 access an ssh-server at 22.105.7.88? yes / no

d. Can host 1.1.1.33 access a webserver at 22.105.7.88? yes / no

e. Can host 1.1.1.33 access a nameserver at 22.105.7.88? yes / no

f. Can host 1.1.1.33 access an ssh-server at 22.105.7.88? yes / no

14. Use the Caesar Cipher to encrypt the plaintext **cat** with shift value 7. ______________________

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

15. You have an account at foobar.net. You forget your account password and call them up to ask for a password reset. After providing some reasonable evidence of your identity, they tell you that instead of resetting your password, they can tell you what your current password is. Explain why you are suddenly suspicious that foobar.net doesn't handle password authentication as securely as possible? Justify!

16. You have a friend "Joe" that you can only communicate with via e-mail. At some point, you both start to worry that your communication is being monitored, so you decide to start encrypting the text of your e-mail. Assuming that you can only communicate via e-mail, why would using AES (or any other symmetric encryption algorithm) for the encryption cause a problem?

17. Continuing from the previous problem. Suppose you decide to use RSA (and both have access to the SI110 RSA tool webpage). Explain briefly what you would do and what your friend Joe would do in order for you to send him the message "foobar" in such a way that only he could read it. Note: We're only worried about confidentiality for this problem!

a. He would ______________________________________ and send me ____________________________.

b. I would _______________________________________ and send him ____________________________.

c. He would ______________________________________ and then he'd have the message.

18. Match the following descriptions with the letter of the appropriate image:

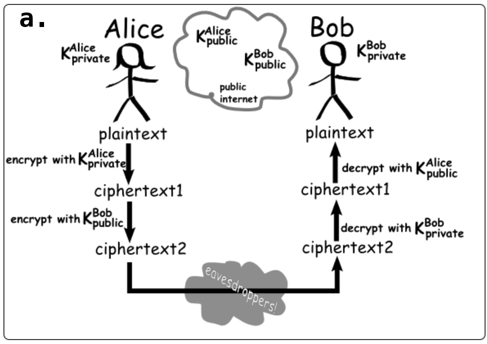
i. _____ Confidential communications with prior arrangements

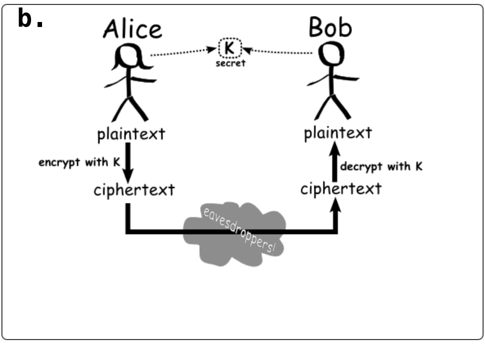
ii. _____ Confidential, authenticated & non-repudiation communications without prior arrangements

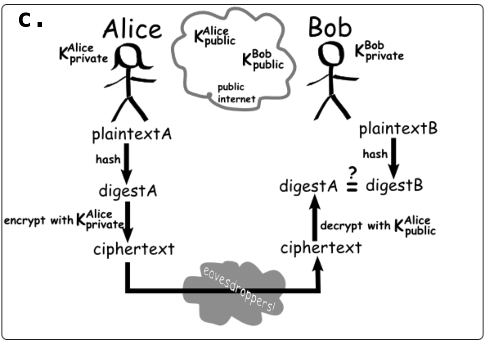
iii. _____ Verifying a password

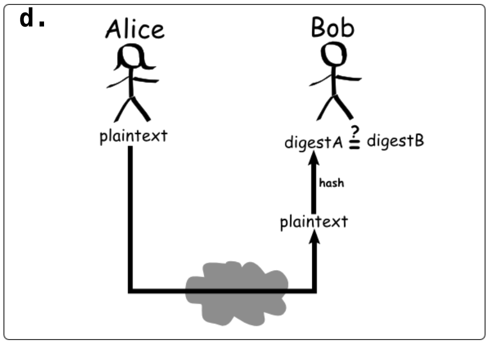
iv. _____ Digital signature

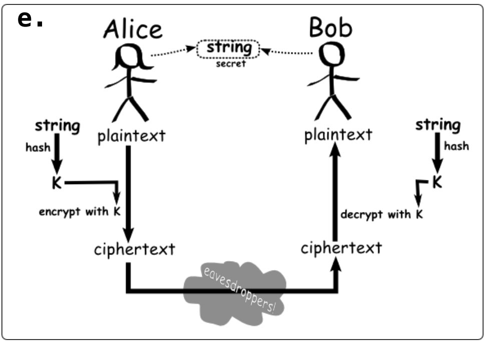
v. _____ password/passphrase encryption

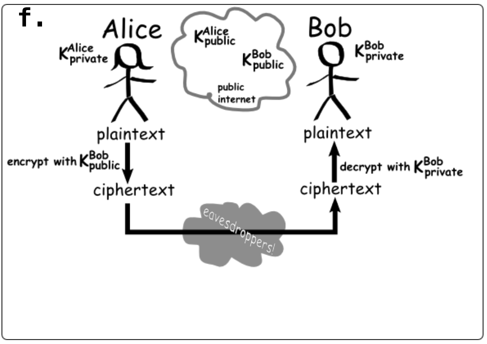


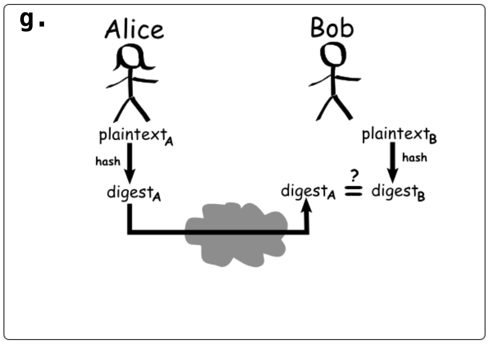












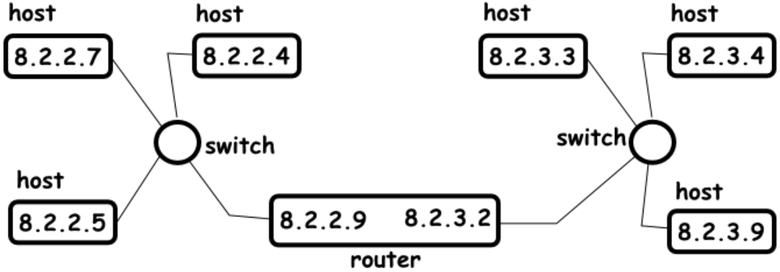
19. You like to shop at The GAP, but now find it hard to get out to a store. So you decide to try buying something off their website, and therefore enter **https://www.thegap.com** into your browser's URL bar. Circle true or false for each of the scenarios described in the following table.

	given that the certificate is trusted by my browser	given that the certificate is not trusted, but I tell my browser to "proceed anyway"
I can be certain that the server I'm connected with is really www.thegap.com	true / false	true / false
I can be certain that the domain thegap.com really belongs to the clothing company "The Gap"	true / false	true / false
I can be certain I am secure against someone snooping on my network traffic	true / false	true / false

20. Encryption and Steganography both offer ways to provide confidential communications. What's the difference in what's confidential when you use steganography versus what's confidential when you use encryption?

21. What Windows shell command tells you your IP Address, subnet mask, and default gateway router?

22. Consider the diagram below:



If the command **tracert 8.2.2.5** is given on host 8.2.3.9, which of the below is the output you will see: (circle your choice)

```
a. 8.2.3.2     b. 8.2.2.5      c. 8.2.2.9      d. 8.2.3.2      e. 8.2.3.9     f. 8.2.3.2
   8.2.2.5                        8.2.2.5         8.2.2.9         8.2.2.9
                                                  8.2.2.5         8.2.2.5
```