This question paper consists of 5 printed pages, each of which is identified by the Code Number COMP391101.

This is an open book examination.
Any written or printed material is permitted.

School of Computing

January 2018

COMP3911

Secure Computing

Answer all three questions

Time allowed: 2 hours

TURN OVER FOR QUESTIONS

Question 1

(a) Consider the following quote, from Niels Ferguson and Bruce Schneier's book *Practical Cryptography*:

> "You have probably seen the door to a bank vault: 10-inch thick, hardened steel, with large bolts.
>
> We often find the digital equivalent of such a vault door installed in a tent. The people standing around it are arguing over how thick the door should be, rather than spending their time looking at the tent."

Explain the point that Ferguson and Schneier have tried to make here, referencing in your answer the cryptographic techniques typically in use today and the security risks generally faced by computer systems. **[6 marks]**

(b) An attacker captures the ciphertext generated from a known piece of plaintext by a symmetric cipher. He considers trying to brute-force the 48-bit key used by this cipher. He has at his disposal a system that can perform 250 million decryptions per second. This system is able to perform 750 million comparisons per second of the resulting bytes with the plaintext. How practical is brute-forcing in this case? Show a calculation that supports your answer. **[4 marks]**

(c) What if the attacker didn't have known plaintext for the ciphertext that he intercepted? Explain why this is likely to have significant implications for a brute-force attack. **[3 marks]**

(d) One of the lectures considered the case of TinKode, a Romanian hacker who illegally accessed numerous computer systems, including government and military web sites. TinKode was quoted as saying

> "I don't do bad things. I only find and make public the info. Afterwards I send an email to them to fix the holes. It's like a security audit, but for free."

Comment on the ethics of TinKode's actions. Contrast this case with the approach typically used when researching vulnerabilities responsibly. **[7 marks]**

[Question 1 total: 20 marks]

Question 2

(a) Draw an attack tree showing some of the ways in which a mail server might be attacked. Your attack tree should have two levels below the root and should have at least three attack paths representing different types of attack. **[4 marks]**

(b) Many e-Commerce web sites allow their customers to post feedback about products purchased from the site. What are the precise conditions required for a cross-site scripting attack involving such a web site to succeed? **[5 marks]**

(c) A system adminstrator is managing a web application for her employer. The application is database-driven and runs on a Unix system. She runs intrusion detection software to scan the web server logs for suspicious activity. This software highlights the following pair of URLs:

```
http://foo.com/%2e%2e%2f%2e%2e%2fetc%2fpasswd

http://foo.com/login?username=aaa%27+OR+1%3d1+--+
```

You may wish to use information from Figure 1 on page 4 to help you interpret these URLs when answering the questions below.

(i) Consider the first of these URLs. What type of attack does this indicate? What is the attacker attempting to achieve? **[3 marks]**

(ii) Describe a technique that the web server could use to defend itself against the attack indicated by the first URL. **[2 marks]**

(iii) Consider the second URL. What type of attack does this indicate? What is the attacker attempting to achieve? **[3 marks]**

(iv) The attack indicated by the second URL is unsuccessful. What does this suggest about how the web application has been implemented? **[3 marks]**

[Question 2 total: 20 marks]

Dec	Bin	Hex	Char	Dec	Bin	Hex	Char
32	0010 0000	20	space	64	0100 0000	40	@
33	0010 0001	21	!	65	0100 0001	41	A
34	0010 0010	22	"	66	0100 0010	42	B
35	0010 0011	23	#	67	0100 0011	43	C
36	0010 0100	24	$	68	0100 0100	44	D
37	0010 0101	25	%	69	0100 0101	45	E
38	0010 0110	26	&	70	0100 0110	46	F
39	0010 0111	27	'	71	0100 0111	47	G
40	0010 1000	28	(	72	0100 1000	48	H
41	0010 1001	29	)	73	0100 1001	49	I
42	0010 1010	2A	*	74	0100 1010	4A	J
43	0010 1011	2B	+	75	0100 1011	4B	K
44	0010 1100	2C	,	76	0100 1100	4C	L
45	0010 1101	2D	-	77	0100 1101	4D	M
46	0010 1110	2E	.	78	0100 1110	4E	N
47	0010 1111	2F	/	79	0100 1111	4F	O
48	0011 0000	30	0	80	0101 0000	50	P
49	0011 0001	31	1	81	0101 0001	51	Q
50	0011 0010	32	2	82	0101 0010	52	R
51	0011 0011	33	3	83	0101 0011	53	S
52	0011 0100	34	4	84	0101 0100	54	T
53	0011 0101	35	5	85	0101 0101	55	U
54	0011 0110	36	6	86	0101 0110	56	V
55	0011 0111	37	7	87	0101 0111	57	W
56	0011 1000	38	8	88	0101 1000	58	X
57	0011 1001	39	9	89	0101 1001	59	Y
58	0011 1010	3A	:	90	0101 1010	5A	Z
59	0011 1011	3B	;	91	0101 1011	5B	[
60	0011 1100	3C	<	92	0101 1100	5C	\
61	0011 1101	3D	=	93	0101 1101	5D	]
62	0011 1110	3E	>	94	0101 1110	5E	^
63	0011 1111	3F	?	95	0101 1111	5F	_

Figure 1: Selected ASCII characters and their numeric representations.

Question 3

(a) A report on a piece of malware notes that it “is able to attack vulnerable Windows machines and make them part of a botnet”.

Discuss two different approaches that this malware might use to recruit machines to the botnet. As part of your answer, indicate clearly the conditions necessary in case case for the recruitment to succeed, and give reasons why defensive measures such as firewalls or anti-virus software might be ineffective. **[8 marks]**

(b) A student researches botnets and writes up his findings as follows:

> “A botnet could be used to conduct a distributed denial-of-service attack. A program running on each bot could listen on a particular port for an incoming command from its controller. This command could include the IP address of the victim, the mode of attack—ICMP echo request or SYN flood—and the time at which to mount the attack. A network intrusion detection system would be a pretty effective tool for detecting such commands.”

Give three reasons why this might not be a sensible assessment of botnet attacks and defensive techniques. **[3 marks]**

(c) You are working on a large legacy client-server application, written in C. During a code review, you come across the following fragment of server code:

```
 1  void build_message(char* s1, int len1, char* s2, int len2)
 2  {
 3    char buf[128];
 4
 5    if (len1 + len2 < 128) {
 6      printf(s1);
 7      printf(s2);
 8      strncpy(buf, s1, len1);
 9      strncat(buf, s2, len2);
10      ...
11    }
12  }
```

(i) What security reason could there be for having the `if` statement in this code? Is it effective? Explain your reasoning. **[4 marks]**

(ii) Discuss two different potential security problems with the code in the body of the `if` statement (lines 6–9). Indicate the circumstances under which either problem might result in an exploitable vulnerability. **[5 marks]**

[Question 3 total: 20 marks]

[Grand total: 60 marks]