NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF APPLIED SCIENCE

COMPUTER SCIENCE DEPARTMENT

Examinations – January 2013

SUBJECT: COMPUTER SECURITY
CODE: SCS 4107

Instructions to candidate:

1. Answer any four questions. Paper contains five questions.
2. All programming questions to be answered in the Java language
3. Each questions contains 25 marks

3 HOURS

QUESTION ONE

a) Online banking is a phenomenon that has brought much convenience to the way people do their financial transaction. Zimbabweans are embracing services that make it easier to transfer money and make payments online. The mobile is now as good as a bank account. However, the general client has not been informed about the threats that all the convenience brings. Prepare a document that explains **five** threats that this use of technology brings to these transactions. In the document, analyse the measures that can be taken to mitigate the impact or protect the user from the mentioned threats. [20]

b) Explain the two modes in which IPSec protocols operates [5]

QUESTION TWO

a) How could you use an IDS to detect attempted buffer overflow attacks on an Intel-based machine? State, and briefly explain, example snort rule(s) to do so. In your answer you may wish to make use of the fact that the NOP instruction for Intel-based machines is 0x90. [10]

b) Explain the security differences between Ipv4 and Ipv6 [5]

c) Evaluate User Datagram Protocol (UDP) as an alternative of Transmission Control Protocol (TCP) Internet Protocol. [10]

QUESTION THREE

a) Evaluate Kerberos as a network authentication protocol. Explain the implementation of the Kerberos Authentication Protocol on a windows-based system. [10]

b) What makes it unsafe to use peer-to-peer applications over the Internet? Use an example to explain. [5]

c) You receive an "I love you" text message on your mobile phone. You call the number to find out more, only to be answered by a very old voice. You suspect that there could be a younger person who might have sent the message (probably the grandchild). Explain how you would use social engineering to find information about the sender of the message. The information you want to get is the name, age and level of education. [6]

d) Compare and contract cyberterrorism and hacktivism [4]

QUESTION FOUR

a) This very simplistic RSA encryption uses public key (n=33,e=17) and encodes text one character at a time using the following numeric codes for each character:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	B	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t

21	22	23	24	25	26	27	28	29	30	31	32
u	V	w	x	y	z	.	,	;	!	?	-

Show enough working that we can verify your calculations.

i. Encrypt "edith" [6]
ii. What is the RSA private key? [4]
iii. Decrypt "ml.z" [5]

b) Explain what you could do to detect passive sniffing on your LAN. [10]

QUESTION FIVE

a) Describe three possible different attacks on firewalls. Analyse the merits of each, what weaknesses of firewalls they exploit, and discuss what could be done by a system administrator to either prevent the attacks or minimise their impact on the system.
Select which attack is the most effective against current firewall technology and briefly state why. [15]

b) Describe all the replication mechanisms used by the Internet Worm. You are a sysadmin for a medium sized company employing a mixture of Linux and Windows boxes. Briefly set out those parts of your security policy relating to the threat posed by malware. [10]

END OF QUESTION PAPER