CSM4, CW-084/4 : Network and Systems Management.

Instructions to candidates:

1. All questions carry equal marks.
2. Question 1 **must** be attempted.
3. Answer any three other questions.
4. Start a new page in your answer booklet for each attempted question.

Question 1.

a. What does the `chkconfig` utility do? (1)

b. Identify the directory location for the UNIX/Linux configuration files used by `chkconfig`. (1)

c. What is the name of the configuration file used to initially configure networking (during boot-up) in Linux? (1)

d. Linux has two password files. Name both. (2)

e. Why does Linux maintain two password files? (2)

f. What are you likely to find in the `/proc` directory? (2)

g. Identify the two password cracking tools studied this year? (2)

h. Which service(s) provide firewall protection to Linux? (2)

i. What does `Nessus` do? (2)

j. What is port scanning? (1)

k. Identify the program that `Nessus` uses for port scanning? (1)

l. What is SSL and on which protocol port does it operate? (2)

m. How does the `tar` utility differ from the `gzip` utility? (2)

n. How does `ssh` differ from `telnet`? (1)

o. Does it ever make sense to operate telnet on a modern LAN? Justify your answer. (2)

p. What is the purpose of the "`-l`" parameter to the su command? (1)

Question 2.

a. List the four virtues of security. (4)

b. List of eight rules of security. (8)

c. Provide an example of a Network, Application and Social chokepoint. (3)

d. What is the advantage of "secretless security"? (2)

e. Describe what is meant by "failing securely". (2)

f. What is meant by "working in stillness"? (2)

g. Define the term "security zone". (1)

h. What is the difference between a ***trusted***, **untrusted** and **semi-trusted** security zone? (3)

Question 3.

a. Other than SNMP, what other protocol can be used for network management on the modern Internet? (1)

b. With reference to the protocol identified in part (a) of this question, identify the two types of network management service supported by this protocol. (2)

c. Identify two network management tools that use the protocol from part (a) of this question. (3)

d. Provide a one paragraph description for the four component parts of the SNMP Management Framework. (8)

e. How does SNMPv3 differ from, and relate to, SNMPv2 and SNMPv1? (4)

f. What is the significance of the "public" and "private" SNMP community strings? (2)

g. Describe the function of the following SNMP messages: (5)

i. `get-request`
ii. `get-next-request`
iii. `get-bulk-request`
iv. `inform-request`
v. `snmpV2-trap`

Question 4.

a. Consider this statement: "A firewall is all the network security an organisation will ever need". Do you agree with this statement? Why or why not? (3)

b. What do the letters VPN stand for? (1)

c. Describe how IPsec can be used to implement a VPN. (4)

d. Does IPsec have to execute on every device when being used to communicate over the public Internet? Illustrate your answer diagrammatically. (5)

e. How does an "extranet" differ from an "intranet"? (2)

f. Describe three advantages of packet-filtering routing technology. (6)

g. Describe two disadvantages of packet-filtering routing technology. (4)

Question 5.

a. Provide a one paragraph definition of the following computer virus terms: (10)

i. Trapdoor
ii. Logic Bomb
iii. Trojan Horse
iv. Bacteria
v. Worm

b. Identify and describe the four phases of a computer viruses lifespan. (8)

c. What is a “polymorphic virus”? (2)

d. Describe how data compression is used by some computer viruses. (2)

e. What is “heuristic antivirus scanning” and how does it work? (3)

Question 6.

a. Describe the basic characteristics of a public-key cryptosystem. (3)

b. Identify the four principals involved in any network communication. (4)

c. Describe how a public-key cryptosystem is used to authenticate the sender (Bob) of a message to a receiver (Alice). (3)

d. Describe how a public-key cryptosystem is used to ensure a message is kept confidential between the sender (Alice) and a receiver (Bob). (3)

e. What role does compression play in modern cryptosystems? Refer to PGP when illustrating your answer. (4)

f. How does a public-key cryptosystem differ from a conventional, symmetric cryptosystem? (3)

g. What is the single, largest problem associated with conventional, symmetric cryptosystems? (3)

h. Identify a technology that can be used to counteract the problem identified in your answer to part (g) of this question. (2)