CSM4, CW-084/4 : Network and Systems Management – 2004/2005.

Instructions to candidates:

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

Question 1.

a. Consider this Linux command line:

```
                                                               tar
zxvf   openssl-0.9.7e.tar.gz
```

What does the above command do? (1)

b. What do the “z”, “x”, “v” and “f” options do to the command shown in part (a) of this question? (2)

c. Assuming the file referred to in part (a) of this question is a software package, detail the commands used to install the software on Linux. (2)

d. What does the following command do:

```
chkconfig --list | grep ':on' | sort | less
```

(2)

e. Provide a one-line description of the functionality provided by each of the following Linux system services:

```
iptables apmd
named anacron
cups xfs
portmap http
squid vncserver
```

(5)

f. What is the function of the Linux `inittab` configuration file? (1)

g. Three source code files are required when installing a secure **Apache** web-server. One is the file of source code to **Apache**, identify the other two. (2)

h. What is the name of the protocol used to provide a secure web service? What port does this protocol/service typically operate on? (2)

i Name and explain the reasoning for the existence of two separate password files in Linux. (2)

j. Identify two tools routinely used to configure a firewall on Linux. (2)

k. How do **SSH** and **SSL** differ? (2)

l. What is the **NetSNMP** project? (1)

m. How do the **nessus** and **nmap** tools relate to each other? (1)

Question 2.

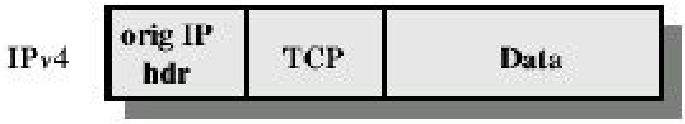
a. Identify and expand the two acronyms used to describe the authentication and encryption services provided by IPsec. (2)

b. Why does IPsec provide both authentication and encryption services? (2)

c. Is it always necessary to authenticate and encrypt with IPsec? (2)

d. How do the "Transport" and "Tunnel" modes of IPsec differ? (4)

e. Describe, with the aid of two diagrams, what happens to this IPv4 datagram whenever is it processed by IPsec within its Transport and Tunnel modes. You are to assume that IPsec is providing both authentication and encryption services: (8)



f. When does it make sense to use Tunnel mode over Transport mode? (4)

g. What changes need to be made to applications running on an IPsec-enabled network? (3)

Question 3.

Consider the following:

A medium-sized business has three sites, all connected to the Internet by high-speed digital links. At each site, a firewall monitors access to/from the Internet. A different vendor's firewall operates at each of the sites (including one built locally with Linux). Local configuration is the responsibility of a designated expert employee. These employees meet on a monthly basis to swap "horror stories" and set-up changes. Only one of the three sites enforces a regular password change policy. The other two claim that such a policy is inflexible and annoying to their users, who have "no interest in systems security anyway, so why annoy them needlessly?". Web access is restricted at one site, but provided "in total" at the other two. [Note that the site which enforces a password policy provides unrestricted access to the Web]. A central site maintains a test and production system. New changes to the in-house, corporate applications are tested on the central site's test system, then moved to production and tested again. If all is well, the new changes are "rolled-out" to the other two sites' production systems. When a security breach is detected at any one site, it is dealt with as quickly and quietly as possible, without informing the other two sites or "the powers that be". Virus protection software does exist at all sites, but it is left up to the end-users to update their virus definition file whenever they suspect a virus is on their system. When a virus is suspected, a machine is wiped clean by the local expert employee and a fresh *operating system installed from CD. The corporate applications are then reinstalled, as required. A report of the incident is sent to the end-users' immediate supervisor.*

Identify and expand upon any Security Virtues and Security Rules ignored and/or broken by this medium-sized business. (25)

Question 4.

a. Identify the three zones of trust. (3)

b. For each of the zones identified in part (a) of this question, provide an example Network, Application and Physical resource associated with each zone. (9)

c. Provide a definition to the term “chokepoint”. (1)

d. Identify and briefly describe three chokepoint advantages. (6)

e. Identify and briefly describe two chokepoint disadvantages. (4)

f. Identify two technologies used to implement a chokepoint on modern networked systems. (2)

Question 5.

a. The year is 1969 and computer user Alice and computer user Bob wish to communicate electronically over an non-secure communications channel. Assuming the use of some conventional cryptographic technology, what options do Alice and Bob have when it comes to exchanging their shared key? (4)

b. Referring to part (a) of this question, what is stopping Alice and Bob from using a public-key cryptographic technology? (2)

c. The year is 1979, and Alice and Bob wish to once again communicate securely over a non-secure communications channel. Have the cryptographic options for exchanging a shared key improved? And if so, how? (2)

d. What is the main difference between secure systems based on conventional cryptographic technologies and those based on public-key technologies. (1)

e. Identify two technologies used to secure modern e-mail systems. (2)

f. Assume Alice and Bob are communicating by e-mail over a non-secure channel using one of the technologies you identified in part (e) of this question. Provide generic answers to the following questions:

1. How can Alice be sure that only Bob reads her email? (2)
2. How can Bob be sure that the email he received is actually coming from Alice? (2)

g. What is a one-way function? (2)

h. How does a one-way function relate to digital signature technology? (2)

i. How does a digital signature differ from a message digest? (2)

j. What is the advantage of employing compression within a cryptographic process? If used, when should compression be applied? Be sure to justify your answer. (4)

Question 6.

a. Identify the three design goals of modern firewall systems. (3)

b. Identify the three main types of modern firewall system. (3)

c. Provide a short description for each of the three firewall systems identified in part (b) of this question. (Note: limit your answer to no more than one or two paragraphs per firewall type). (9)

d. What would you expect the following firewall “rules” to do: (6)

i. `block;payroll;*;www.hotmail.com;*;`
ii. `allow;mailsys;25;*;*;`
iii. `block;*;*;*;>1023;`

e. What is a bastion host, and how does it relate to a firewall? (2)

f. If a router has the ability to filter packets, does it then follow that the router is a firewall? Justify your answer. (2)