Computer Security example exam.

PART A

Candidates should answer **ALL** of Question 1 in Part A.

Question 1

(a) Which of the following are examples of malicious software?
Select ALL that apply. [4]

i. Stuxnet
ii. Fireball
iii. Docker
iv. Wooden horse
v. Zeus
vi. DarkHotel

(b) Which of the following are true?
Select ALL statements that apply. [4]

i. CIA security objectives involve computers, the internet and access control.
ii. DoS attacks only attack Windows systems based on the Dos kernel.
iii. DDoS attacks can be used to break into secure databases.
iv. New wifi standards can only be met by upgrading the wifi hardware
v. WEP is considered to have strong encryption
vi. Firewalls check every packet passing through them, regardless of the type of firewall.

(c) Which are true about firewalls?

Select ALL statements that apply. [4]

i. Proxy firewalls access machines on the LAN on behalf of machines on the WAN

ii. Stateful firewalls do less packet checking than stateless firewalls

iii. Stateless firewalls can also be referred to as access control lists

iv. Statefull firewalls can allow for lower latency network access than stateless firewalls.

(d) Which of the following are examples of Microsoft Security features?

Select ALL statements that apply. [4]

i. Microsoft Defender

ii. Windows Hello

iii. Microsoft malware removal system (MMRS)

iv. Threat protection

v. Intrusion detection system

(e) Which of the following are examples of items that the Harbian Linux security auditing script can detect?

Select ALL statements that apply. [4]

i. User group assignments

ii. Suid files

iii. File permissions on configuration files

iv. Web server configuration

(f) Which of the following are true about the Ceasar cipher?

Select ALL statements that apply. [4]

i. It is a substitution cipher

ii. It is an example of symmetric encryption

iii. It is a shift cipher

iv. It can be cracked by trying 25 different shifts

v. It is an example of asymmetric encryption

(g) Which are true about public-private key encryption?

Select ALL statements that apply. [4]

i. If Alice is sending a message to Bob, Bob decrypts the message using Alice's public key

ii. If Bob is sending a message to Alice, Alice decrypts the message using Bob's private key

iii. If Bob is sending a message to Alice, Alice decrypts the message using Alice's private key

iv. If Bob is sending a message to Alice, Bob encrypts the message using Bob's private key

v. If Bob is sending a message to Alice, Bob encrypts the message using Alice's public key

(h) Which are true about bitcoin and finance?

Select ALL statements that apply. [4]

i. In traditional finance, if Bob sends a check to Alice and then sends another check to Sanjay, it is possible that there is a double spend problem

ii. Bitcoin transactions can map one input to many outputs

iii. Bitcoin transactions can map many inputs to one output

iv. Bitcoin transactions can map many inputs to many outputs

v. Bitcoin does not solve the solvency problem

vi. The public ledger is the blockchain

vii. Every block on the bitcoin blockchain contains a single transaction

(i) Which of the following are true about security policies?

Select ALL statements that apply. [4]

i. The Chinese Wall security policy considers four layers of abstraction: files, objects, companies groups and conflict classes

ii. Military security policy consists of the following sensitivity levels: top secret, secret, confidential, restricted and unclassified

iii. BellLa Padula, Biba and Graham Denning are all examples of firewall types

iv. Secrecy and integrity are different approaches to designing security models

(j) Which of the following are examples of ethical dilemmas in computer security?

Select ALL statements that apply. [4]

i. The right for anyone to encrypt data with hard encryption

ii. Providing backdoors to otherwise secure computer systems

iii. Deciding which software to use for intrusion detection

iv. Deciding which operating system to use

PART B

Candidates should answer any **TWO** questions from Part B.

Question 2

(a) Name two blockchain systems and state their purpose. [4]

(b) Draw out a feature comparison table comparing THREE features of the two blockchain systems you mentioned. [6]

(c) Name TWO problems that cryptocurrency technology solves. [2]

(d) Explain how cryptocurrency technology solves the TWO problems you named above. Provide details of how the transactions are stored on the blockchain. [4]

(e) Research online an example of a blockchain technology that you did not encounter in the course materials. Select one that has a data model and a programming model.

i. Name the technology and briefly describe what its purpose is. [4]

ii. Describe the data model underlying the technology [4]

iii. Describe the programming model underlying the technology, specifically:

What the the language used for operations on the blockchain? [2]

What kind of low level operations are possible? [2]

How does the programming part of the blockchain technology enable the functionality? [2]

Question 3

You are part of a team working on a patient information system for a local doctors' surgery.

(a) Your team is considering what kind of server operating system to deploy the back end of the software onto. One option is a containerised solution such as Docker, running GNU/Linux. Another is a Microsoft Windows system.

i. State TWO security points in favour of running the system in a Windows environment. [4]

ii. State TWO security points in favour of running the system in a containerised environment. [4]

(b) Your team is considering two options for a mobile application for Android. The application will be used by administrative and medical staff. One option is to create a fully native application which stores various patient data locally on the device. Storing data on the device means it will not need a constant internet connection. The other option is creating an application that runs in a web browser on the device, and it stores very limited data on the device. Compare these two options on THREE key security points. [6]

(c) You have been tasked with developing a security testing plan for the system.

i. Describe TWO specific static analyses you would do. [4]

ii. Describe TWO specific dynamic analyses you would do. [4]

(d) Your team needs to know how to use encryption in the patient information system. They have asked you to explain the various forms of encryption they have heard about. For each of the following, explain what it is and give an example of where it might be used in the patient information system.

i. Asymmetric encryption. [2]

ii. Symmetric encryption. [2]

iii. Public-private key cryptography. [2]

iv. HTTPS [2]

Question 4

The kid-RSA algorithm is a simplified version of the RSA algorithm. Kid-RSA takes as its input four numbers a, b, a1, b1. The four numbers are converted into four values M, e, d and n, according to the following equations:

M = a * b - 1
e = a1 * M + a
d = b1 * M + b
n = (e * d) / M

A plaintext message P can be encrypted to an encrypted message C with the public key (n,e) using:

C = e * P (mod n).

Once encrypted, C can be converted back to P using the private key 'd' as follows:

P = C * d (mod n)

(a) if a = 949, b = 112, a1 = 524 and b1 = 4266, calculate M, e, d and n. Show your working. [2]

(b) State the public key for these values of a,b,a1 and b1. [2]

(c) Encrypt the message 'Silver' using the public key. Show your working. [4]

(d) Decrypt the message. Show your working. [4]

(e) Name a simple shift cipher. [2]

(f) Explain how the shift cipher you mentioned works, with examples. [4]

(g) How would you go about cracking a shift cipher. [4]

(h) Research the enigma encryption that was used in the second world war.

i. What kind of cipher was this? [2]

ii. Compare it to the shift cipher you mentioned above [4]

iii. Which cipher is the most secure? Why? [2]

END OF PAPER

.