Information Security (CP3404) — Sample Examination

This exam has 33 questions, for a total of 50 marks.

- This exam has two parts, i.e. **Part A** (questions 1 to 30), and **Part B** (questions 31 to 45).
- In **part A**, write your answers directly on to this exam paper; in the space provided after each question.
- In **part B**, write your answers on the exam booklet provided.

*************** **Part A** ***************

Question 1 [1 mark]

True or False: Today's software attack tools do not require any sophisticated knowledge on the part of the attacker.

Solution:

Question 2 [1 mark]

True or False: Spreading similarly to a virus, a worm inserts malicious code into a program or data file.

Solution:

Question 3 [1 mark]

True or False: Pharming is a type of phishing attack that automatically redirect the user to a fake web site.

Solution:

Question 4 [1 mark]

True or False: Steganography hides the existence of data within images by dividing and hiding portions of a file within the image.

Solution:

Question 5 [1 mark]

Digital signatures actually only show that the public key labeled as belonging to the person was used to encrypt the digital signature.

Solution:

Question 6 [1 mark]

True or False: Mobile devices such as laptops are stolen on average once every 20 seconds.

Solution:

Question 7 [1 mark]

True or False: The Discretionary Access Control model gives the user full control over any objects that he owns.

Solution:

Question 8 [1 mark]

True or False: Passwords provide strong protection.

Solution:

Question 9 [1 mark]

True or False: A subset of business continuity planning and testing is disaster recovery, also known as IT recovery planning.

Solution:

Question 10 [1 mark]

Audits serve to verify that the security protections enacted by an organization are being followed and that corrective actions can be swiftly implemented before an attacker exploits a vulnerability.

Solution:

Question 11 [1 mark]

True or False: In a white box test, the tester has no prior knowledge of the network infrastructure that is being tested.

Solution:

Question 12 [1 mark]

Each of the following is a goal in information security EXCEPT ______.

(a) avoid legal consequences
(b) foil cyberterrorism
(c) prevent data theft
(d) limit access control

Solution:

Question 13 [1 mark]

The motivation of ______ may be defined as ideology, or attacking for the sake of their principles or belief.

(a) brokers
(b) cyberterrorists
(c) hactivists
(d) cybercriminals

Solution:

Question 14 [1 mark]

What type of controls are the processes for developing and ensuring the policies and procedures are carried out?

(a) technical controls
(b) active controls
(c) administrative controls
(d) policy controls

Solution:

Question 15 [1 mark]

A(n) ______ is decrypted but is only used for comparison purposes.

(a) stream
(b) digest
(c) algorithm
(d) key

Solution:

Question 16 [1 mark]

A ______ is a specially formatted encrypted message that validates the information the CA (Certificate Authority) requires to issue a digital certificate.

(a) Certificate Signing request (CSR)
(b) digital digest
(c) FQDN form
(d) digital certificate

Solution:

Question 17 [1 mark]

What prevents a mobile device from being used until the user enters the correct passcode?

(a) swip identifier (SW-ID)
(b) keyboard
(c) touch pad
(d) lock screen

Solution:

Question 18 [1 mark]

What is the current version of TACACS (Terminal Access Control Access Control system)?

(a) XTACACS
(b) TACACS+
(c) TACACSv5
(d) TRACACS

Solution:

Question 19 [1 mark]

Which authentication factor is based on a unique talent that a user possesses?

(a) what you have

(b) what you are

(c) what you do

(d) what you know

Solution:

Question 20 [1 mark]

A(n) ______ is always running off its battery while the main power runs the battery charger.

(a) secure UPS (Uninterruptible Power supply)

(b) backup UPS

(c) off-line UPS

(d) on-line UPS

Solution:

Question 21 [1 mark]

Which statement is NOT a guideline for developing a security protocol?

(a) Notify users in advance that a new security policy is being developed and explain why the policy is needed.

(b) require all users to approve the policy before it is implemented.

(c) Provide a sample of people affected by the policy with an opportunity to review the policy and comment on it.

(d) Prior to development, give all users at least two weeks to review the policy and comment on it.

Solution:

Question 22 [1 mark]

Open Authorization (OAuth) is an open-source service that authenticates a user on multiple sites using ______ credentials.

(a) OpenID

(b) account lockup policy

(c) Federated Identity Management (FIM)

(d) token

Solution:

*************** **Part B** ***************

Question 23 [3 marks]
What is a hacker? Describe white hat and black hat hackers.

Question 24 [2 marks]
Describe adware.

Question 25 [2 marks]
How does an RFID (Radio Frequency IDentification) tag embedded into an ID badge function without a power supply?

Question 26 [2 marks]
Discuss how HMAC (Hashed Message Authentication Code) works.

Question 27 [6 marks]
Discuss the three areas of protection that are provided by IPsec (Internet Protocol Security).

Question 28 [2 marks]
What are the two TCP/IP (Transmission Control Protocol / Internet Protocol) protocols that are used by mail servers for clients accessing incoming mail?

Question 29 [2 marks]
List two major access control models.

Question 30 [3 marks]
What are the three broad categories on which authentication can be based?

Question 31 [2 marks]
Explain why the LAN Manager (LM) hash is vulnerable.

Question 32 [2 marks]
What are the four (4) duties of the Change management team (CMT)?

Question 33 [2 marks]
Describe the purpose of a honeypot.