Question 1

1 Point

Denial of service (DoS) and distributed denial of service (DDoS) attacks have the same effect; however, a distributed denial of service (DDos) attack

(A) is launched from large numbers of hosts that have been compromised and act after receiving a particular command.

(B) involves intentional deception designed to produce illegal financial gain or to damage another party.

(C) is software written with the deliberate purpose of causing damage, destruction, or disruption

(D) involves accessing a system of computers without authorization.

Continue

Question 2

1 Point

Alice and Bob would like to communicate securely. Alice aims to provide a mechanism to ensure the confidentiality of data during transmission, and Bob aims to have a mechanism to confirm that it is coming from Alice. Alice needs to encrypt the message with_____

(A) the public key of Alice and the public key of Bob

(B) the public key of Bob and the private key of Alice

(C) the private key of Bob and the private key of Alice

(D) the private key of Bob and the public key of Alice

Continue

Question 3

1 Point

Which of the following refers to an intrusion detection system (IDS) programmed to identify known attacks occurring in an information system or network by comparing sniffed traffic or other activity with that stored in a database?

(A) Misuse detection

(B) Anomaly detection

(C) Behavioural analysis

(D) Signature analysis

Continue

Question 4

1 Point

What is the main difference between a low-interaction honeypot and a high-interaction honeypot?

(A) A low-interaction honeypot is a real system with full services and applications, while a high-interaction honeypot emulates IT services or systems.

(B) A low-interaction honeypot provides a realistic target, while a high-interaction honeypot provides a less realistic target.

(C) A low-interaction honeypot provides an initial interaction with specific components in a system, while a high-interaction honeypot may occupy an attacker for an extended period.

(D) A low-interaction honeypot is sufficient for use as a component or application of a distributed IDS, while a high-interaction honeypot is not.

Question 5

1 Point

Passing structured query language commands to a web application and getting the website to execute it is called SQL _____.

(A) Processing

(B) Injection

(C) Attacking

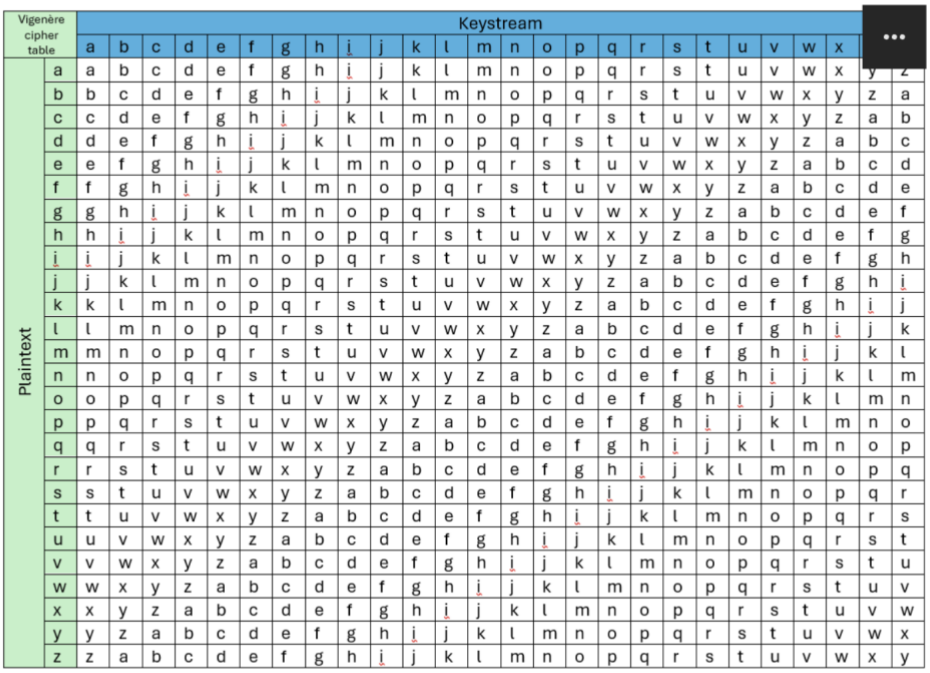
(D) Execution

Continue

Question 6

1 Point

Decrypt the ciphertext "FWF STJXQOJWX" using the provided Vigenère Polyalphabetic Substitution table and the keystream "SIMPLE". The plaintext is **Blank 1**



Vigenère cipher table	Keystream																									
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Blank 1 Add your answer

Question 7

1 Point

A company decided to use a symmetric encryption algorithm for various reasons. Which of the reasons given below is not valid and is considered a weakness of symmetric encryption?

- (A) It requires a secure mechanism to deliver keys properly
- (B) It is less complex
- (C) It is very fast.
- (D) It is very efficient when sending large amounts of data.

Question 8

1 Point

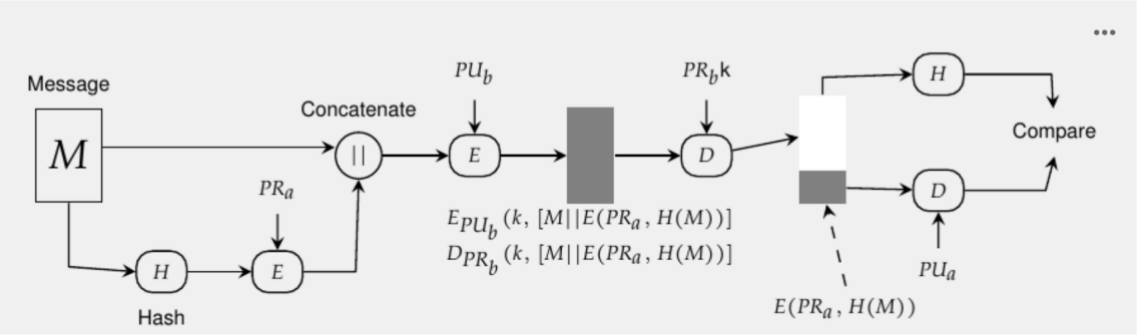
To prevent DNS hijacking DNS pharming, DNS secure (DNSSEC) should be deployed. Which from the list below is not a service DNSSec provides?

- (A) Authenticity of Denial of existence
- (B) Integrity of reply
- (C) Confidentiality of origin
- (D) Authenticity of DNS answer

Question 9

1 Point

What security principles are provided by the cryptographic process shown in the diagram?



- (A) In addition to digital signature, this method provides both confidentiality and authentication.
- (B) It uses public key encryption to protect the integrity and confidentiality of the hash but does not use a digital signature to verify the sender's identity
- (C) It encrypts the message but does not provide any form of authentication.
- (D) It guarantees confidentiality by hashing the message only.

Question 10

1 Point

An _____attack is a form of SQL Injection where data is retrieved using a different channel.

- (A) Internal
- (B) Inferential
- (C) Out-of-Band
- (D) In-Band

Question 11

1 Point

Which of the statements below is not an error caused by a buffer overflow?

- (A) Corruption of DLL files
- (B) Unexpected transfer of control in the program
- (C) Corruption of data used by the program
- (D) Possible memory access violation

Question 12

1 Point

What is the role of the Ticket Granting Server (TGS) in the Kerberos authentication process?

- (A) It decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested application server.
- (B) It encrypts the client's password to create a ticket.
- (C) It creates and sends a session key to the client for encryption.
- (D) It grants access to the application server by verifying the user's credentials.

Question 13

1 Point

Encrypt the plaintext message "SUCCEED IN FIRST ATTEMPT" using the transposition method and the secret key "HELLO". The ciphertext is ***Blank 1***

Blank 1 Add your answer

Continue

Question 14

1 Point

Which security principle does Sarah need to employ if she needs a security system that checks every user's access against the access control mechanism?

- (A) Fail-safe default
- (B) Economy of mechanism
- (C) Separation of Privilege
- (D) Complete mediation

Question 15

1 Point

Put the following phases of the Diffie Hellman key Exchange in the correct order:

1. Alice and Bob can the shared secret key for secure communication.
2. Alice and Bob agree on a public prime number and a base.
3. Alice and Bob exchange their public values.
4. Alice chooses a secret number and calculates her public value. Bob chooses his secret number and calculates his public value.
5. Each of them calculates the shared secret key using their private number and the other's public value.

(A) 2, 4, 3, 5, 1

(B) 5, 4, 2, 1, 3

(C) 3, 1, 4, 2, 5

(D) 1, 2, 3, 4, 5

Question 16

1 Point

Which access model is most appropriate for companies with high employee turnover?

(A) Mandatory access control (MAC)

(B) Role-based access control (RBAC)

(C) File access control (FAC)

(D) Discretionary access control (DAC)

Question 17

1 Point

Decrypt the ciphertext message "**AS AEO REWLG TE TUREDCOA**" using the transposition method and the secret key "**LEARNT**" . The plaintext is **Blank 1**

Blank 1 Add your answer

Continue

Question 18

1 Point

The _____ function consists of two phases of encryptions, one with a symmetric encryption key and one with a public key.

- (A) Clear-signed data
- (B) Enveloped data
- (C) Signed and enveloped data
- (D) Signed data

Question 19

1 Point

What type of encryption uses the same key to encrypt and to decrypt information?

- (A) Asymmetric encryption
- (B) No type of encryption uses the same key to encrypt and decrypt information
- (C) Symmetric encryption
- (D) Non-symmetric encryption

Question 20

1 Point

A network administrator has noticed that the central switch of their network is failing due to a malicious attack. They noticed that it looks like it is not able to accept any new device connection, although there are many ports available. Which attack do you think is happening here?

- (A) ARP poisoning
- (B) MAC flooding
- (C) ARP spoofing
- (D) MAC hijacking

Question 21

1 Point

How do metamorphic worms differ from polymorphic worms?

- (A) Metamorphic worms rewrite their own code entirely, making each version unique.
- (B) Metamorphic worms are always detectable by antivirus software.
- (C) Metamorphic worms infect only a specific operating system.
- (D) Metamorphic worms spread using a single method.

Question 22

1 Point

The security principle which states that individuals will be given only the level of access that is appropriate for their specific job role or function is called _____.

(A) job rotation

(B) separation of duties

(C) implicit deny

(D) least privilege

Question 23

1 Point

When an attacker injects client-side scripts into web pages viewed by other users so that those users interact with it, it is an example of _____ attack.

(A) Structured Query Language (SQL) injection

(B) Buffer overflows

(C) Cross-site scripting (XSS)

(D) Traversal attacks

Question 24

1 Point

When an attacker injects client-side scripts into web pages viewed by other users so that those users interact with it, it is an example of _____ attack.

(A) Cross-site scripting (XSS)

(B) SQL injection

(C) Command injection

(D) XML injection

Question 25

1 Point

Which encryption algorithm that uses block mode is considered not suitable for sending images?

(A) Cipher Block Chaining CBC

(B) Data Encryption Standard DES

(C) Rivest Cipher 4 (RC4)

(D) Electronic Code Book ECB

Question 26

1 Point

Which of the following is not a step in the TLS handshake process?

- (A) Certificate Verification
- (B) Server Hello
- (C) Application Data Transfer
- (D) Client Hello

Question 27

1 Point

An operating system received many ICMP packets of very large and odd sizes and crashed. Which Denial of Service attack type happened?

- (A) Ping of Death
- (B) Teardrop attack
- (C) ICMP flood
- (D) SYN Flood

Question 28

1 Point

Which of the following statements best describes the **Key Exchange** phase in the SSH message exchange process?

- (A) The client and server agree on the cryptographic algorithms to be used for the session.
- (B) The client formally begins secure communication by sending an encrypted message using the session key.
- (C) The client and server exchange their identification strings to initiate the handshake.
- (D) The client sends a randomly generated key, encrypted with the server's public key, and the server verifies and responds.

Question 29

1 Point

Decrypt the message "Kssh Pygo mr MGX" using the Caesar cipher substitution method and the rotation value of "4". The plaintext is ***Blank 1***

Blank 1 Add your answer

Continue

Question 30

1 Point

Which of the following statements best describes the role of **TLS in HTTPS communication**?

(A) TLS provides encryption, integrity, and authentication for HTTP communications.

(B) TLS operates at the network layer to provide security for IP packets.

(C) TLS ensures that HTTP requests and responses are compressed for faster transmission.

(D) TLS replaces HTTP as the primary protocol for web communication.

Question 31

1 Point

What type of attack can be prevented by using ESP in IPSec?

(A) Message replay

(B) Denial of service

(C) Man-in-the-middle

(D) Eavesdropping

Question 32

1 Point

Which of the following would be defined as an absence or weakness of a safeguard that could be exploited?

(A) A risk

(B) A vulnerability

(C) An exposure

(D) A threat

Question 33

1 Point

A hacker is attempting to decrypt an encrypted message by analysing the most commonly occurring characters and comparing them to typical letter distributions in the target language. Their aim is to reconstruct the original plaintext without knowing the encryption key. Which cryptanalysis technique is the hacker using in this scenario?

(A) Known Plaintext Attack

(B) Differential Cryptanalysis Attack

(C) Dictionary Attack

(D) Frequency and pattern analysis

Question 34

1 Point

Encrypt the message “It takes time” using the Caesar cipher substitution method and the rotation value of "3". The ciphertext is *Blank 1*

Blank 1 Add your answer

Continue

Question 35

1 Point

A hacker is conducting an information gathering assessment on a server they aim to exploit. Which of the scanning methods should the hacker avoid since it is considered too noisy and might be flagged as malicious; hence, they risk getting caught at this early stage?

A Connect scan

B Syn scan

C Ping scan

D Fin scan