Section 1 – Multiple Choice Questions.

1. In computer security, _____ means that computer system assets can be modified only by authorized parities.
    A) Confidentiality
    B) Availability
    C) Authenticity
    D) Integrity

2. Keyloggers are a form of _____.
    A) Spyware
    B) Shoulder surfing
    C) Trojan
    D) Social engineering
3. In Message Confidentiality, transmitted message must make sense to only intended_____
    A) Sender
    B) Receiver
    C) Modulor
    D) Translator

4. Which of the follow are correct about Bell-La Padula Model?
    A) This model provides Confidentiality
    B) Used to prevent simultaneous access to information of differing levels of sensitivity.
    C) Works according to “No Read up, No Write Down”
    D) All the above

5. What information you **cannot** extract from a X.509 Certificate?
    A) Operating System Version
    B) Version Number
    C) Subject name
    D) Issuer Name

6. Phishing is a form of_____.
    A) Spamming
    B) Impersonation
    C) Identify Theft
    D) Scanning

7. Which of the following are true about TLS (Transport layer security)?
    A) TLS can only be used with HTTP protocol
    B) TLS formally known as SSP (Secure Socket Protocol)
    C) TLS require reliable transport layer
    D) All the above

8. What key is used to encrypt a message which provides confidentiality in the asymmetric key encryption?
    A) Receivers private key
    B) Senders private key
    C) Receivers public key
    D) Same key used to encrypt the message

9. Which fields of information are used by a typical packet-filtering router in its security decisions?
    A) Digital certificates, IP addresses, and IP header checksums.
    B) Source and destination IP addresses, and TCP/UDP port numbers.
    C) URL addresses, IP addresses, and TCP/UDP port numbers.
    D) Usernames,IP addresses, Digital certificates and IP headers.

10. What does the digital signature provide?
    A) Signer Authentication
    B) Confidentiality
    C) Security
    D) Availability

11. Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?
    A) Web-based
    B) Human-based
    C) User-based
    D) Computer-based

12. What information you **cannot** extract from an email header?
    A) Senders email server details
    B) Receivers email address
    C) Email read status of the receiver
    D) Email subject

Section 2 – Structured Questions.

a) Define Confidentiality, Integrity and Availability.

Confidentiality

a. To ensure that unauthorized parties cannot access the data, message or information

Authenticity

b. To ensure that the source / sender of the data, message or information is identifiable

Integrity

c. To ensure that the data. Message or Information was not modified during transmission

Nonrepudiation

d. To ensure that either party cannot deny sending or receiving the data, message or information

b) What is SELinux?
Security-Enhanced Linux (SELinux) is a Linux kernel security module that provides a mechanism for supporting access control security policies

c) List two Categories of Threats and describe them using one sentence.
Phishing is an illegal activity that uses social engineering techniques to trick people into giving out personal information

Spam and viruses are ever-increasing security issue for anyone with an email account. Unsolicited junk mail steals system resources and leads to lost productivity, storage, and bandwidth. Spam can also be hostile and contain virus and Trojan horses.

d) Name four methods used by Operating Systems for enabling sharing of resources.
   a. Do not protect
   b. Isolate
   c. Share all or Share nothing
   d. Share via access limitations
   e. Share by capabilities

e) Draw an access control matrix for processes X and Y, and files file1 and file2 where;
   I. X can Write file1, and write file2
   II. Y can read file1, and no permission for file2.

	File 1	File 2
x	W	W

y	R	

f) Use the below command output in the Linux terminal to answer questions.

```
$ ls -l

-rw-r----x 1 test myteam 8214 Jan 21 12:47 test.txt
```

I. What is the group of this file? `myteam`

II. What permissions do the group members has on this file? `rw`

g) What is Authentication and Authorization?

Difference between **Authentication and Authorization**. ... **Authentication** means confirming your own identity, while **authorization** means granting access to the system. In simple terms, **authentication**is the process of verifying who you are, while**authorization** is the process of verifying what you have access to

Once your identity is verified by the system after successful authentication, you are then authorized to access the resources of the system

h) Name advantages and disadvantage of Stream Ciphers and Block Cipher.

Stream Ciphers

i) Advantage

a. Speed of transformation
b. Low error propagation

j) Disadvantage

a. Low diffusion-low spread capability
b. Susceptibility to malicious insertion and modifications-hard to acsess

k) What is Caesar Cipher and how does it work? Explain with an example.

Julius Caesar (“Caesar Cipher”)

a. Each plaintext letter is replaced by a letter some fixed number of positions further down the alphabet (e.g. hello (shift 5 positions) mjqqt)

l) What are advantages of Firewalls.

Auditing and logging.

a. By configuring a firewall to log and audit activity, information may be kept and analyzed at a later date.

Creating Virtual Private Networks

b. VPNs are communications sessions traversing public networks that have been made virtually private through the use of encryption technology. VPN sessions are defined by creating a firewall rule that requires encryption for any session that meets specific criteria.

User authentication.

c. Firewalls can be configured to require user authentication. This allows network administrators to control ,track specific user activity.

m) list web application vulnerabilities.

A1 Injection.
A2 Broken Authentication and Session Management.
A3 **Cross-Site Scripting** (**XSS**)

A4 Insecure Direct Object References.
A5 Security Misconfiguration.
A6 Sensitive Data Exposure.
A7 **Missing** Function Level Access Control.
Insufficient logging and monitoring
XML External Entities (XXE)

n) Does Email consider to be secure method of communication? Explain.

****