Ajay Kumar Garg Engineering College, Ghaziabad

Department of MCA

Model Solution- Sessional Test-2

Course:	MCA	Semester:	III
Session:	2017-18	Section:	MCA-1 & 2
Subject:	Cyber Security	Sub Code:	RCA-305
Max Marks:	50	Time:	2 hour

Section-A **(5 X 2 = 10)**

Q1. What is need of Electronic Cash?

Ans. Electronic cash refers to electronic transfer of money in the form of a block of data representing money that is transferred online.

Q2. What do you mean by Application Security?

Ans. Application security is the use of software, hardware and procedural methods to protect applications from external threats.

Q3. What do you understand by Spoofing?

Ans. Spoofing means to provide false information about your identity to gain unauthorized access of other computers.

Q4. What is Closed Circuit Television Surveillance (CCTV)?

Ans. CCTV cameras are also called the third eye because if human being missed noticing some people entering a restricted zone, these camaras could capture the event or photos.

Q5. Define IT asset.

Ans. An asset is a resource with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit. Physical security of our asset, especially the IT asset is also very important.

Section-B (5 X 5 = 25)

Q6. What is Firewall? Explain its various types in detail.

Ans. Firewall is a network security system that controls the incoming and outgoing network traffic based on an applied rule set.

→ Hardware firewall is physical piece of equipment that is kept between the internet and your LAN network.

→ Software firewall is a software program i.e. installed on your computer.

Types of Firewall

1) Packet filter: Inspects all packets.
2) Application level gateway: FTP & Telnet.
3) Circuit level gateway: TCP & UDP connection.
4) Proxy server: Check all messages that enter or leave a network.

Q7: What is e-payment? Discuss requirements for E-Payment through Credit-card.

Ans: There are several organizations that provids services for online payment, call e-payment.

Requirements for e-payments

1) Privacy: Details about any transaction must be kept secretly away from unauthorized parties. Privacy is usually ensured by using encryption techniques.
2) Integrity: Data cannot be altered or tamper while in transit. Integrity can be ensured using digital signatures and certificates.
3) Authentication: Authentication is vital to prevent fraud.
4) No-Repudiation: No one cannot deny their services.
5) Atomicity: Money is not lost or created during a transfer.

Q8: Discuss the various types of malicious Software.

Ans: Malicious Software (malware) is any Software that gives partial to full control of your computer to do whatever the malware creator wants.

There are Three types of Malicious Software:

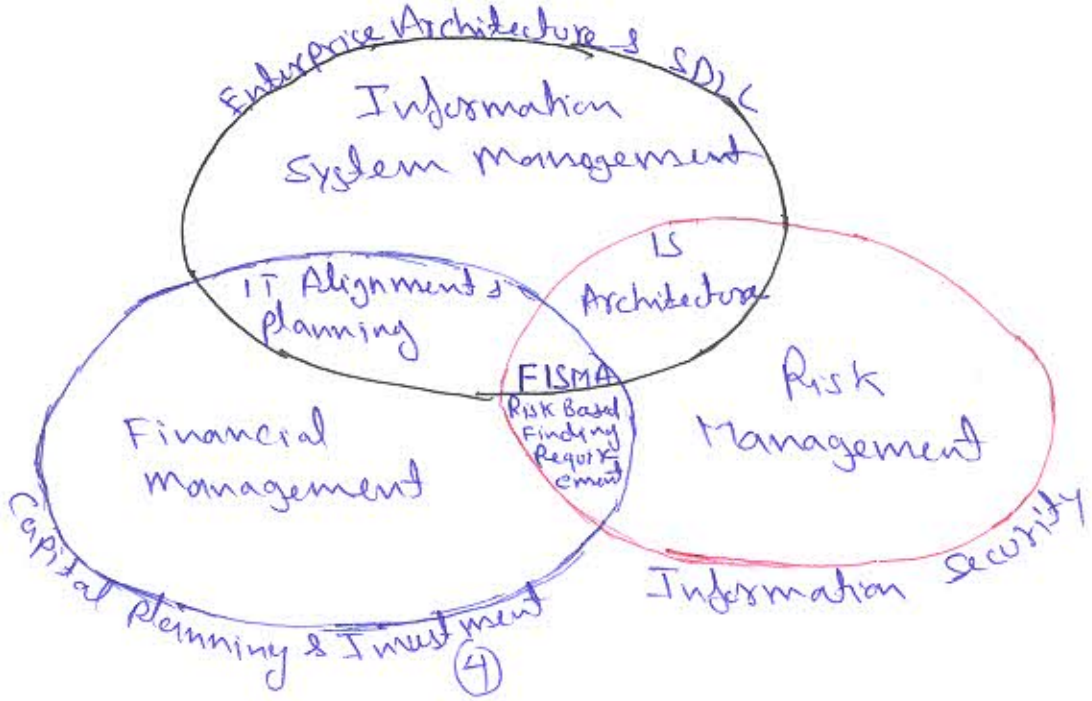
1) Malware: Software which is specifically designed to disturb, damage, or gain authorized access to a computer system.

2) Adware: Software that automatically displayed or downloads advertising material such as banners or pop-up when a user is online.

3) Spyware: Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Q9 what are Security Considerations during Information System development?

Ans:



Step1: Identification and planning: followed by improvement of risk are important Processes developing a secure information system.

Step2: Manage risk properly.

We have to find a balance between different Process that include Protecting organizations information and assets, cost incurred in applying security controls and in formulation strategies.

Finally: Secure IS developed by integrating risk analysis and management activities at the start of the system development and Continuing throughout.

Q10 what is Intrusion Detection System (IDS)? Explain HIDS and NIDS.

Ans: An IDS is a device or software application that monitors network or system activities for malicious activities or policy violations and Produces reports to a management Station.

NIDS: (Network Intrusion detection Systems) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network

→ HIDS, (Host Intrusion Detection System) are run on individual hosts or devices on the network.

- A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected.

Section C (2×7.5=15)

Q 11, What are data security considerations? Explain in this reference data backup, data archival security and data disposal consideration.

Ans: Data is any type of stored digital information and security is about the protection of assets.

Prevention: measures taken to protect your assets from being damaged.

Detection: measures taken to allow you to detect when an asset has been damaged, how it was damaged and who damaged it.

Reaction: measures that allow you to recover your assets.

1) Data Backup Security Considerations:

→ Backup of data is nothing but storage of snapshot of data at certain points and in case of data

is lass due to some reason, you could restore the most recent form of data.

→ you should backup your files incrementally or differentially.

→ Validate your backup copies.

→ frequently take backup of your data.

2) Data archival Security Consideration

→ The process separating older data from currently active, new, and fresh data is know as archival of data.

→ The separated old data is moved to a different storage device so that data can be retained for a long time and reference whenever required.

3) Data disposal Security consideration

→ Destruction of data means to completely wipe out the data from the storage media. This process is called data disposal.

→ Data disposal is an act of Permanently deleting or destroying the data stored in media.

→ Data disposal methods:

→ overwriting hard drives

→ Degaussing hard drives and backup tapes.

→ Destroying storage media.

Q 12 what are the security issues related to hardware, data storage and downloadable device?

Ans:-> Securing computer system means to Protect all of its components that includes:
- hardware, software, storage devices, operating system and peripheral devices.

-> Each component has own vulnerability such as
- Hardware parts can be stolen and destroyed.

-> Security of each component is equally important.

1) Security Issues in Hardware: Hardware mainly faces security issues related to stealing, destruction, gaining unauthorized access and breaking the security code of conduct.

Security measures:
-> Biometric access control
-> Use VPN
-> Use strong Passwords.
-> Provide limited access to the devices.

2) Security Issues with Storage Devices:

-> Data Storage devices are used to save information.
-> Divices such as compact disk (CD), digital versatile disk (DVD), memory cards, flash drive etc.

→ Can store information and be removed from the system to be kept on some other place.

→ The main issues are
  → Loss and theft of data.
  → Improper disposal of data
  → Introduction to malwares in your system.
  → Denial of data i.e. attack on availability of data.

3) Security Issues with downloadable devices

→ Peripheral Devices (PD): PDA, External Hard Drive
→ They are more vulnerable to attacks.

→ Issues related to them are -
  → Stealing of data.
  → Destruction of data.
  → External attacks (virus etc.)