Ques:

A. Explain three-pillar approach to cyber security? [1 + 1*4 = 5]

B .For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.
a. Facebook, managing public information on its Web server.Company ABC which manages law enforcement and takes care of extremely sensitive investigative information.
b. Company ABC which manages law enforcement and takes care of extremely sensitive investigative information
c. Institute web server which hosts department and course data.

Ans:

A) Three pillar approach to cyber security
Confidentiality
Integrity
Availability

- **Confidentiality** is roughly equivalent to Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.
- **Integrity** involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).
- **Availability** means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

B)

	Confidentiality	Integrity	Availability
Facebook	Moderate	High	Moderate
Company ABC	High	High	Moderate
Institute web server	Low	High	Moderate

Ques:

Consider you are an individual [1 + 2 + 2 = 5]
a. As an individual do I need to worry about cyber security, explain?
b. If you are a hacker, what you will do hack a system which is not connected to internet?
c. What are the sources of cyber-attacks? And how it can be prevented, explain with example?

a.

Cybersecurity is important because it **protects all categories of data from theft and damage**. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

Cyber threats are a big deal. Cyber-attacks **can cause electrical blackouts, failure of military equipment, and breaches of national security secrets**. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable.

b.

USB drives and social engineering

DiskFiltration Attacks

Analyzing Fans with Fansmitter

Changing temperature with BitWhisper

Wired and Laptop keyboards

c.

1. Vulnerability Exploits due to unpatched software or systems in the network - regular patching and periodic security review of the systems
2. DDoS Attacks - IDS/IPS, Firewall, DDoS prevention solutions
3. Malware - Anti-malware, network security solutions and user awareness
4. Social engineering attacks - Periodic simulations and user awareness
5. Sponsored attacks (state / competitor) - Defense in depth and periodic simulations to check readiness and effectiveness
6. Insider threat / Disgruntled employees - Separation of roles, stringent security policies for all operational procedures.

Hackers, Phishing emails**,** Malicious insiders**,** social engineering**,** Man in the middle attack, Malwares, Denial of service attack, MITM attack,

Ques:

a. In the Clark-Wilson model, must the TPs be executed serially, or can they be executed in parallel? If the former, why? If the latter, what constraints must be placed on their execution?
b. Company XYZ has been using the network of 193.56.7.0 /24. Requirement is to put each of the 6 floors in the building on a different subnet. How can we create subnets for this IP address? What is the range of host IDs for the 6th subnet after doing Subnetting? Explain. [3 x 2 = 6]

a. IN Clark-Wilson model; the TPs must be executed serially, as There's no way to *execute* in *parallel* in *Clark-Wilson* because there is no standardized rule for how to handle concurrent access to the same data.

b. Range of host IDs for 6^{th} subnet is 193.56.7.161 - 193.56.7.190

Explanation: For 6 Subnets, we need to borrow 3 bits, as $23 = 8 > 6$

Hence, now Network Bits will be: $24 + 3 = 27$ Hence Subnetting CIDR is: /27

Subnet Mask = 255.255.255.224

Therefore, Subnetwork Block Size = 256 – 224 = 32

Hence, Subnetworks are designed as bellow

NW Address	1st Host	Last Host	Broadcast Address
193.56.7.0	193.56.7.1	193.56.7.30	193.56.7.31
193.56.7.32	193.56.7.33	193.56.7.62	193.56.7.63
193.56.7.64	193.56.7.65	193.56.7.94	193.56.7.95
193.56.7.96	193.56.7.97	193.56.7.126	193.56.7.127
193.56.7.128	193.56.7.129	193.56.7.158	193.56.7.159
193.56.7.160	193.56.7.161	193.56.7.190	193.56.7.191

Ques:

Consider you are a Security Architect in your organization. A complex system has more changes of having security problems. In addition, too complex the system is, too many opportunities for something to go wrong. You would like to create small reusable components for repeated functionality. Which design principle is applicable in this scenario? Describe the design principle. Clearly explain the design principle with an example. [1 + 2 + 2 = 5]

Ans:

The design principle applicable to this scenario is - Economy of Mechanism (EoM) but for reusability some level of modular design principle also shall be used

EoM means that the design of SW and HW security measure should be as simple and small as possible.

This mechanism has fewer exploitable flaws and needs less maintenance. Easy configurations and testing are some of the features. Update and replacement is a simple mechanism

Modularity principle also may be put to good use to develop security mechanism which are frequently called. common modules will be easier to implement and integrate. Modularity also might provide good protection against tampering.

So one would prefer mix of EoM & Modularity to meet the needs of simple and reusable components.

Example - if we need to invoke a crypto check very often in some of the mechanisms.
A single mechanism with replacement parameters can be implemented and be made available to other interfacing security modules.
This will reduce the complexity of the system and allow easy configuration and maintenance according to principles of EoM with modularity

Ques:

Suppose you are a network admin, specify which protocols will be applied in below scenarios [1 X 5 = 5]

a. We want to assign IP addresses, subnet masks, default gateways, DNS servers, etc. to users when they login the network

b. To match domain names with IP addresses

c. When no handshaking between sender and receiver is required

d. To send email messages from clients to servers over the internet

e. We want to allow the download/upload of files between a client/server

Ans:

a. DHCP

b. DNS

c. UDP

d. SMTP

e. FTP

Ques:

Some Host H1 has IP address 192.168.1.97 and is connected through two routers ROU1 and ROU2 to another host H2 with IP address 192.168.1.80. Router ROU1 has IP addresses 192.168.1.135 and 192.168.1.110. ROU2 has IP addresses 192.168.1.67 and 192.168.1.155. The netmask used in the network is 255.255.255.224.

Which IP address should host H1 configure its gateway as? Explain it with proper steps [2 + 2 = 4]

Ans:

IP: 192.168.1.110

Router1 IP 192.168.1.135, 192.168.1.110
Router2 IP 192.168.1.67, 192.168.1.155

Host1 IP 192.168.1.97
Host2 IP 192.168.1.80, subnet mask is 255.255.255.224 which is /27

Number of address per subnet is 32 and hosts is 30
So subnet 1 is 0-31,
subnet 2 is 32-63,
subnet 3 is 64-95,
subnet 4 is 96-127

As the H1 IP is ending with .97, it is in the range of subnet 4 host addresses.

ROU1 has an IP address 192.168.1.110 which is in subnet 4.

Thus the H1 gateway is ROU1 192.168.1.110