Case Studies [Assignments]

Q Assess the impact of Active and Passive Attacks on the security of Banking System.

SBI's 12000 Employee data leaked (Active attack)

In July 2023, a Telegram channel leaked the data of over 12,000 SBI employees and account holders. The data included acc.no., photo IDs, work IDs, phone numbers, addresses, names, PAN no, etc.

The leak was caused due to a misconfiguration in a database that was used to store the personal information of SBI employees and account holders. The database was not password protected, which allowed anyone to access the data on internet.

The database was hosted on a cloud server that was not properly configured. The server was not perotected by firewall.

Cyber Attack on "Secure Bank" (Passive Attack)

Let's say there is a bank "Secure Bank" which offers a wide range of banking facilities.

There is a cybercrime group "CyberSec" which does cyber-crimes.

CyberSec sends spear-phishing emails to bank employees which has an attachement. On opening the attachement & or downloading the attachement an infected file is entered into the system.

The attackers can gain access to bank's network. They ~~a~~ employee a malware (Trojan) which can open network for them.

These leads to passive attack, where the cyber criminals can use techniques like Screen-capture tools, traffic sniffers, etc. These can help them to know activities like data transfers, transaction flows, etc.

Q. Importance of CIA triad for a large university. Additionally outline some specific security mechanisms to safeguard critical data, systems and resources effectively.

The CIA triad is a fundamental concept in information security. It stands for confidentiality, Integrity, Availabil

- Confidentiality: It ensures that only authorized individual or entities have access to sensitive information. For a university, this could include student records, research data, financial information, etc.

- Integrity: It ensures that information is accurate, complete, unaltered. Data Integrity is crucial for a university's research findings, administrative records, and other critical information.

- Availability: It ensures that information and resourc are accessible and usable when needed. In context of university, this includes access to educational resources online systems, research databases.

Specific security services and mechanisms that the university can implement to safeguard critical data, systems and resources include:

i) Access controls
ii) Encryption
iii) Intrusion detection and prevention systems
iv) Regular security Audits and penetration testing
v) security awareness training
vi) Data Backup & Disaster Recovery
vii) Incident Response Plan
viii) Using SIEM tools.