10908662

1. Spyware is an application used to monitor another person’s computer usage legally or illegally.
2. Investment offer fraud: this is a type of computer fraud where attackers lure their victims to make some investment decisions by misleading them with false investment opportunities in hopes of making very large returns. e.g., Ponzi schemes, whiles Data Piracy is the illegal copying of protected data for financial gains. e.g., pirated software, digital music, etc.
3. Physical layer

Eavesdropping: when there’s an unauthorized monitoring and interception of electronic communication between two or more parties.

Data link layer

MAC spoofing involves changing the Media Access Control (MAC) address, enabling attackers to impersonate a trusted device within the network and gain unauthorized access.

VLAN Hopping: VLAN Hopping: In situations with switched networks, attackers might take advantage of security flaws to move between virtual LANs (VLANs) and access private network segments without authorization.

Network layer

IP spoofing is where the attacker creates fake IP packets with false source address to hide the sender’s identity.

Routing Attacks: These comprise attacks on routing protocols that can reroute traffic to unauthorized locations.

Transport layer

Man-in-the-Middle: it occurs when data transmission between two parties is interrupted between two parties making them believe they are directly communicating with each other.

Session layer

Session hijacking: Through the theft of cookies or session tokens, an attacker can gain control of an established session between two parties and pretend to be a genuine user.

Attacks known as denial of service (DoS) can interfere with session layer protocols, preventing communication and rendering services unusable.

Presentation layer

Malware Payloads: When processing data, attackers can insert malicious code that takes advantage of holes in the application layer.

Application layer

SQL Injection: Via the manipulation of input into web applications, attackers can run unauthorized SQL queries against the database and perhaps obtain sensitive data.

Cross-Site Scripting (XSS): When malicious scripts are injected into websites that other users visit, there is a chance that their accounts may be compromised, and their data will be stolen.

Phishing: this is where attackers deceive victims into revealing sensitive information. It can be done also buy installing malware.