Experiment no.: 11

Title: Case study of cyber-crime, where the attacker has performed any kind of cyber-attack. Prepare a report and also list the laws that will be implemented on attacker.

Theory:

Case Study Report: The Sony Sambandh Case (CBI v. Arif Azim)

1. Case Background

The **Sony Sambhand Case** stands as a significant milestone as it was India's first case where a conviction for cybercrime was achieved. Sony India Private Ltd. operated a website, www.sony-sambandh.com, which allowed Non-Resident Indians (NRIs) to purchase Sony products online and have them delivered to their friends and family in India.

2. The Attack

In May 2002, an individual placed an order on the Sony website for a television and cordless headphones using the stolen credit card details of an American national. The delivery was requested for Arif Azim in Noida, India. After verification, Sony India delivered the products and took photographs of Azim receiving them.

3. Discovery of the Crime

Approximately six weeks later, Sony India was notified by the credit card agency that the transaction was fraudulent as the card's owner had not authorized the purchase. Sony India then filed a complaint with the Central Bureau of Investigation (CBI).

4. Investigation and Verdict

The CBI's investigation revealed that Arif Azim, an employee at a Noida call center, had illegally obtained and used the American customer's credit card information. Azim was arrested, and the items were recovered. Faced with strong evidence, Azim confessed to the crime. The court found him guilty but, recognizing he was a young, first-time offender, sentenced him to one year of probation.

5. Significance

This case was notable for successfully applying traditional Indian Penal Code (IPC) provisions alongside the newer Information Technology (IT) Act of 2000 to address cybercrimes.

Laws Implemented on the Attacker

Arif Azim was convicted under sections of both the Indian Penal Code (IPC) and the Information Technology (IT) Act, 2000.

Under the Indian Penal Code (IPC)

- Section 418 (Cheating with knowledge that wrongful loss may ensue)
- Section 419 (Punishment for cheating by personation)
- Section 420 (Cheating and dishonestly inducing delivery of property)
- Other potentially applicable sections for similar cyber fraud cases include "conspiracy" and "breach of trust".

Under the Information Technology (IT) Act, 2000

- Section 66 (Computer-related offences), which criminalizes acts done dishonestly or fraudulently as described in Section 43.
- Section 43 (Penalty and compensation for damage to computer system, etc.), while primarily addressing civil liability and compensation, outlines actions such as unauthorized access and data downloading that can form the basis for charges under Section 66.

These legal provisions were used to address the unauthorized access, identity theft, and financial fraud committed in this case.

Conclusion:

I have successfully done a case study of cyber-crime, prepared a report and also listed the laws that were implemented on attacker.