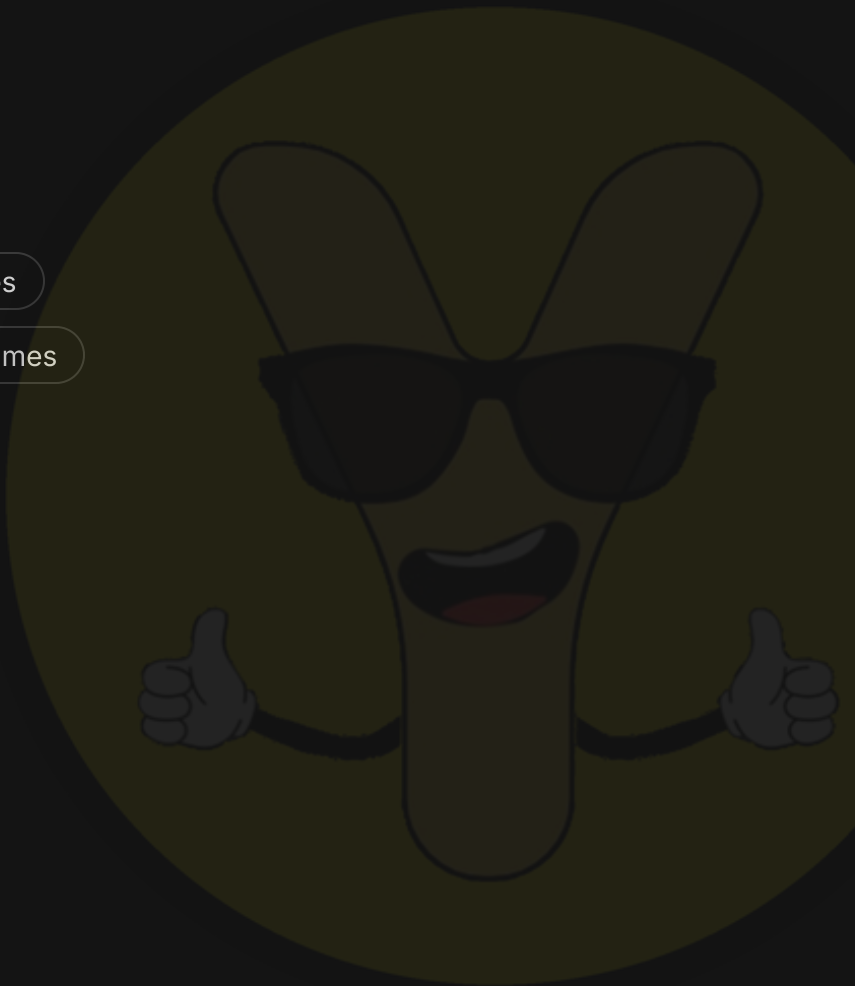
AKTU · 2ND YEAR · BCC301 / BCC401

Cyber Security

Unit 1 — Introduction to Cyber Security

- Introduction to Cybercrime
- Cybercrime and Information Security
- Classification of Cybercrimes
- Cybercrime: The Legal Perspectives
- Cybercrime and Indian ITA 2000
- Global Perspectives on Cybercrimes
- Cyber offenses: How Criminals Plan Them
- Social Engineering
- Cyberstalking
- Cybercafe and Cybercrimes
- Botnets: The Fuel for Cybercrime
- Attack Vector
- Cloud Computing



DECODED BY

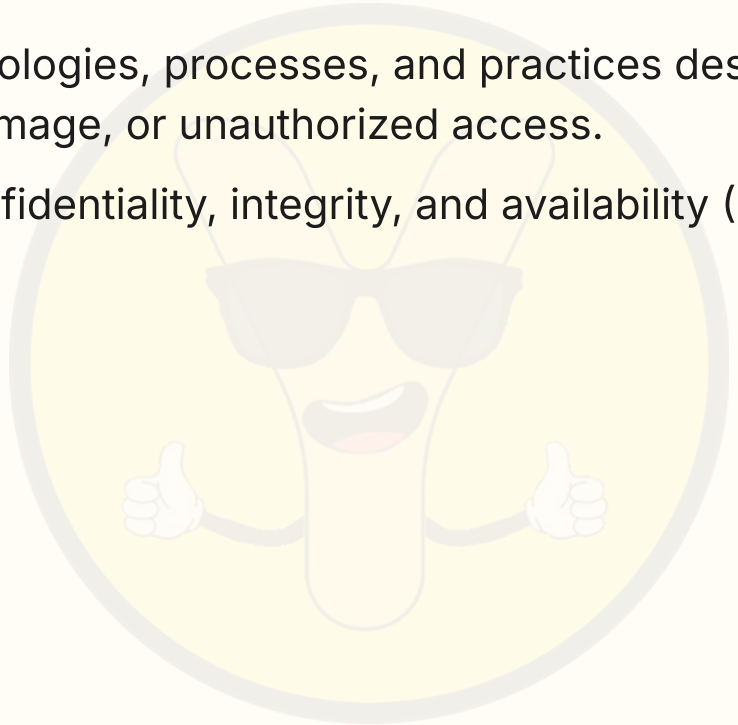
Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

Introduction to Cyber Security

Fundamental concepts of protecting digital assets and countering modern cyber threats.

- Cyber security encompasses technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.
- The primary goal is maintaining confidentiality, integrity, and availability (CIA Triad) of information across interconnected systems.

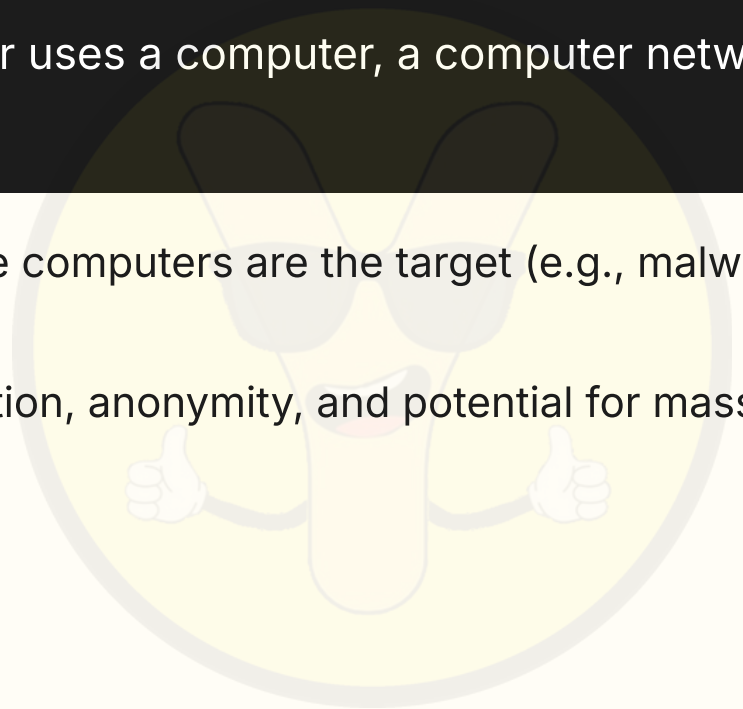


Introduction to Cybercrime

CYBERCRIME

Any criminal activity that targets or uses a computer, a computer network, or a networked device to commit offenses.

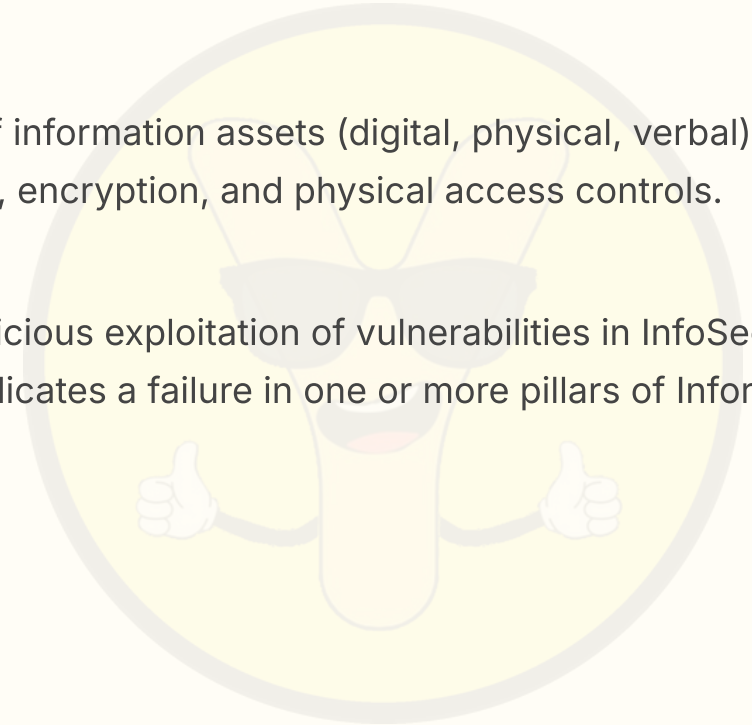
- Involves both illegal activities where computers are the target (e.g., malware infection) and where computers are the tool (e.g., online fraud).
- Characterized by borderless execution, anonymity, and potential for massive automated scale.



Cybercrime and Information Security

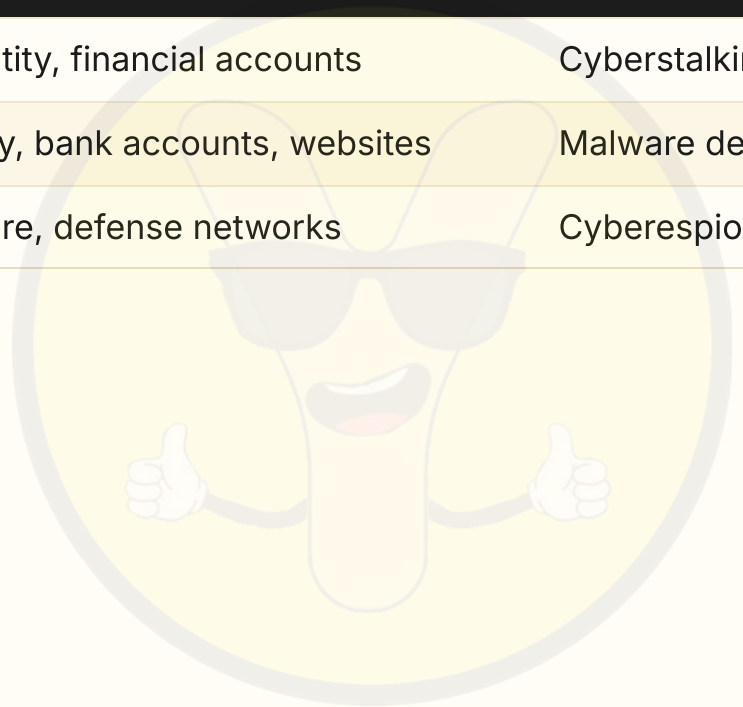
Understanding the interplay between securing information and combating cyber attacks.

- Information Security (InfoSec)
  - Broader domain protecting all forms of information assets (digital, physical, verbal).
  - Focuses on risk management, policies, encryption, and physical access controls.
- Intersection with Cybercrime
  - Cybercrime represents the active, malicious exploitation of vulnerabilities in InfoSec controls.
  - Every successful cybercrime event indicates a failure in one or more pillars of Information Security.



Classification of Cybercrimes

Category	Target	Example Activity
Against Individuals	Personal data, identity, financial accounts	Cyberstalking, identity theft, phishing
Against Property	Intellectual property, bank accounts, websites	Malware deployment, carding, website defacement
Against Government	Critical infrastructure, defense networks	Cyberespionage, state-sponsored attacks, terrorism



Cybercrime: The Legal Perspectives

CYBER LAW

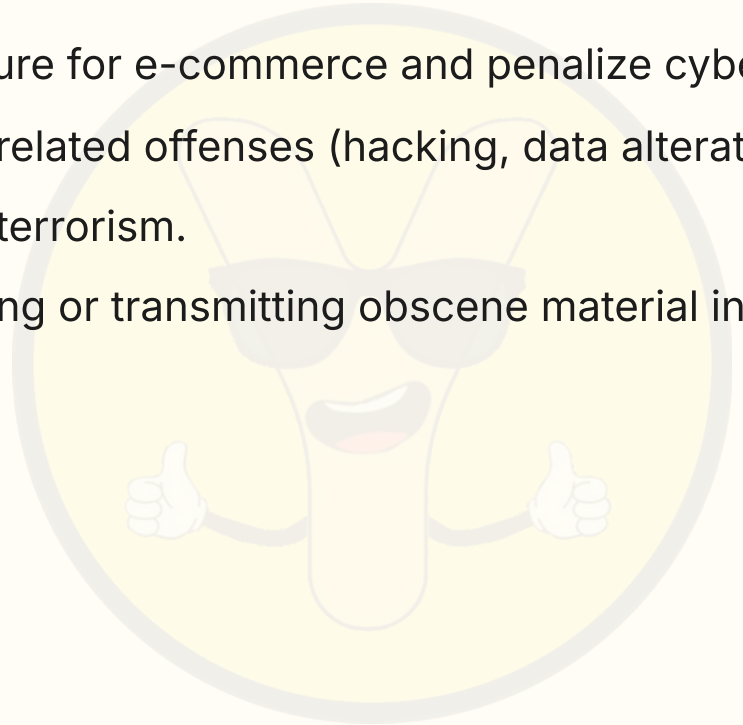
The legal framework that governs the digital sphere, covering cyberspace, electronic commerce, software, and information security.

- Establishes legal recognition for electronic records and digital signatures.
- Defines cyber offenses, establishes jurisdiction over cross-border crimes, and prescribes penalties for digital breaches.

Cybercrime and Indian IT Act 2000

The foundational legislation regulating cyber activities and electronic commerce in India.

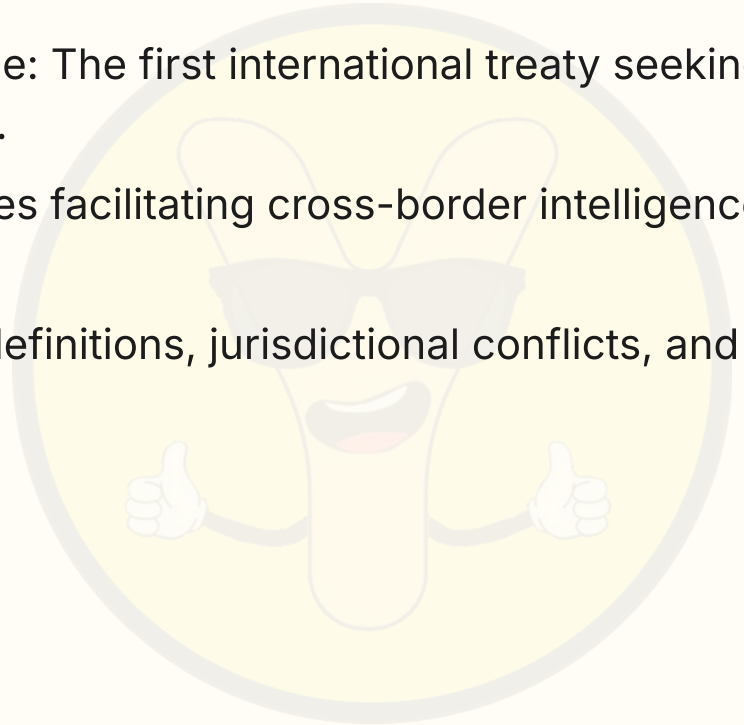
- Enacted to provide legal infrastructure for e-commerce and penalize cyber offenses.
- Section 66: Penalties for computer related offenses (hacking, data alteration).
- Section 66F: Punishment for cyber terrorism.
- Section 67: Punishment for publishing or transmitting obscene material in electronic form.



Global Perspectives on Cybercrimes

International cooperation and treaties addressing borderless digital threats.

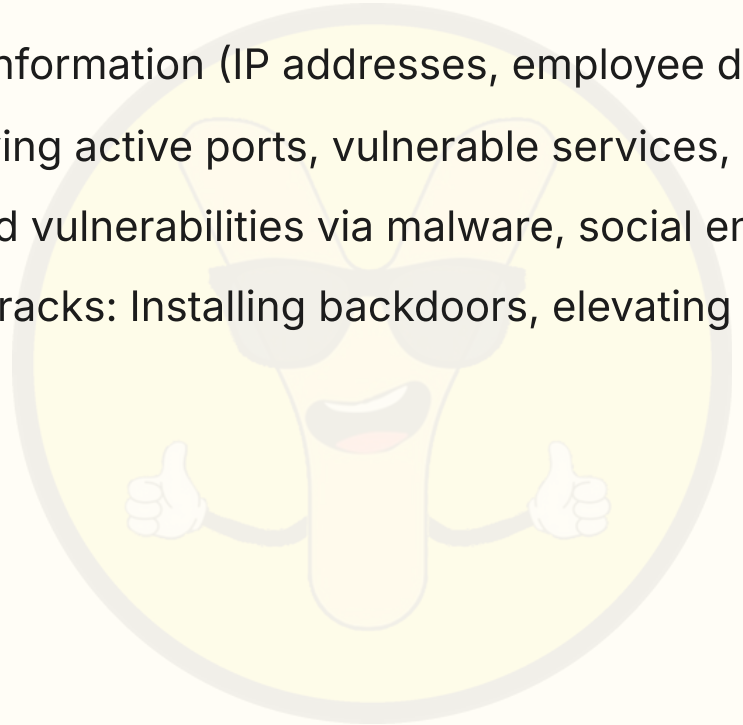
- Budapest Convention on Cybercrime: The first international treaty seeking to address Internet and computer crime by harmonizing national laws.
- Interpol and Europol: Global agencies facilitating cross-border intelligence sharing and joint cyber operations.
- Challenges: Varying national legal definitions, jurisdictional conflicts, and safe havens for hackers.



Cyber Offenses: How Criminals Plan Them

The structured lifecycle of executing a cyber attack.

- Reconnaissance: Gathering target information (IP addresses, employee details, tech stack).
- Scanning and Enumeration: Identifying active ports, vulnerable services, and network maps.
- Gaining Access: Exploiting identified vulnerabilities via malware, social engineering, or brute force.
- Maintaining Access and Covering Tracks: Installing backdoors, elevating privileges, and deleting logs.

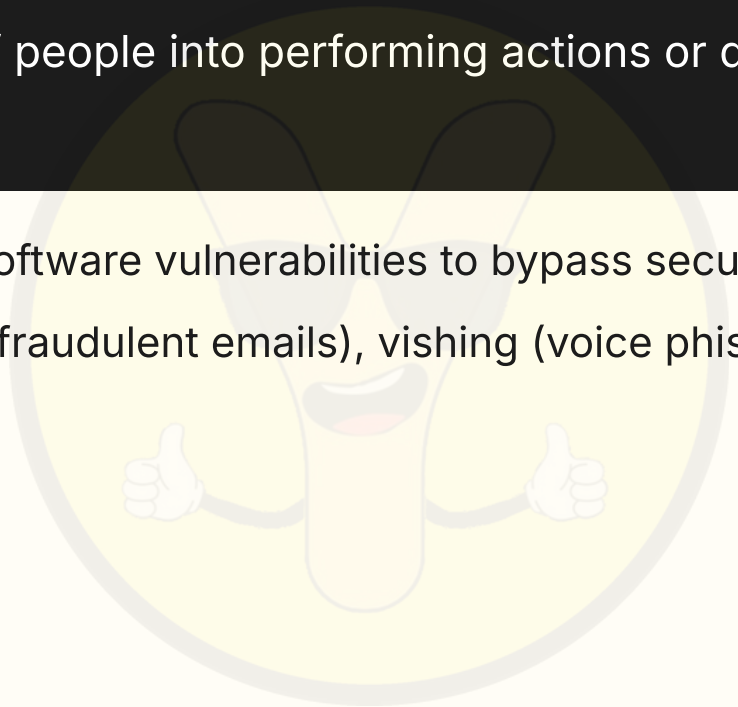


Social Engineering

SOCIAL ENGINEERING

The psychological manipulation of people into performing actions or divulging confidential information.

- Relies on human error rather than software vulnerabilities to bypass security controls.
- Common vectors include phishing (fraudulent emails), vishing (voice phishing), dumpster diving, and pretexting.



Cyberstalking

CYBERSTALKING

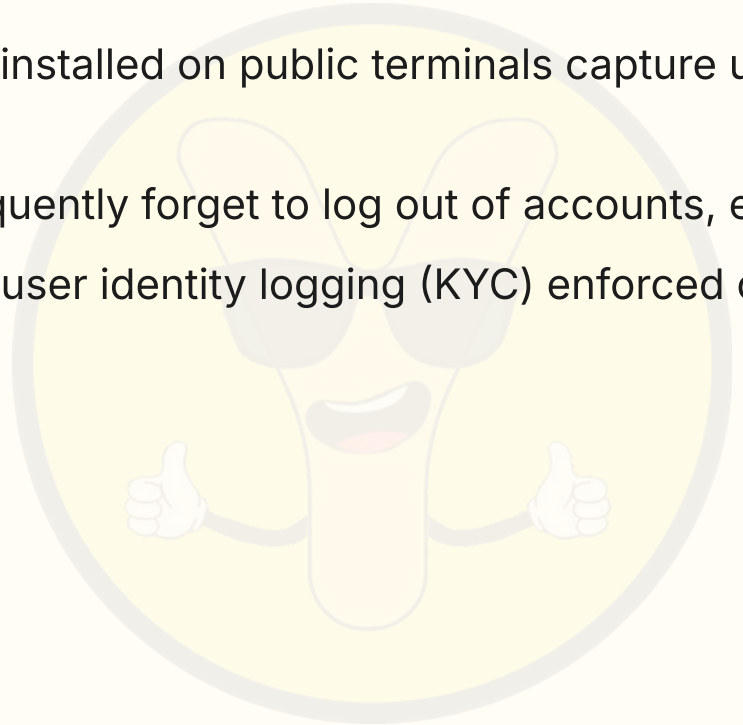
The use of the Internet or other electronic means to stalk or harass an individual, organization, or group.

- Involves persistent monitoring, false accusations, threats, gathering information, and sending damaging materials.
- Distinguished from physical stalking by its digital ubiquity, often leaving digital forensic trails like IP logs and message headers.

Cybercafe and Cybercrimes

Public internet access hubs as vulnerable points for illicit digital activities.

- Shared hardware risks: Keyloggers installed on public terminals capture user credentials and banking details.
- Lack of secure sessions: Users frequently forget to log out of accounts, enabling session hijacking.
- Regulatory compliance: Mandatory user identity logging (KYC) enforced on cybercafe owners to deter anonymous cybercrimes.

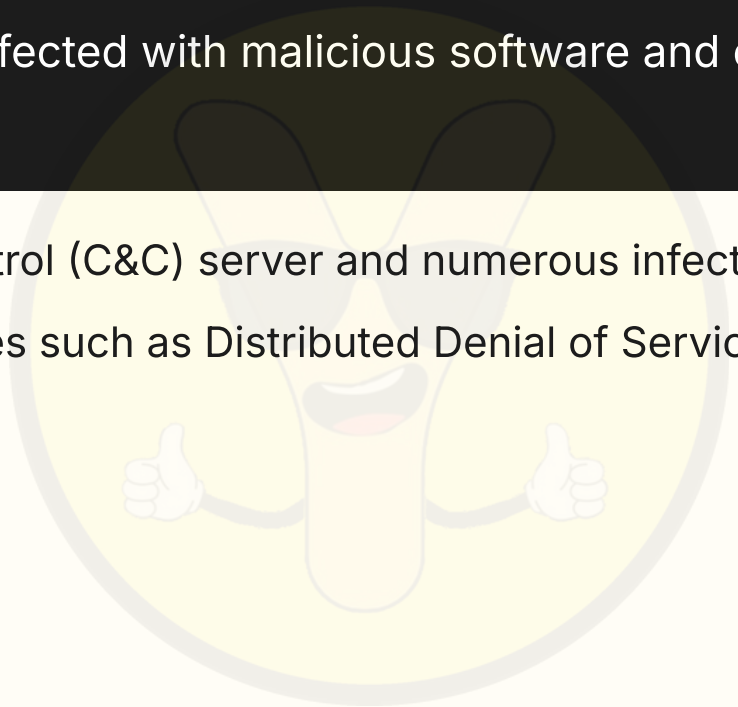


Botnets: The Fuel for Cybercrime

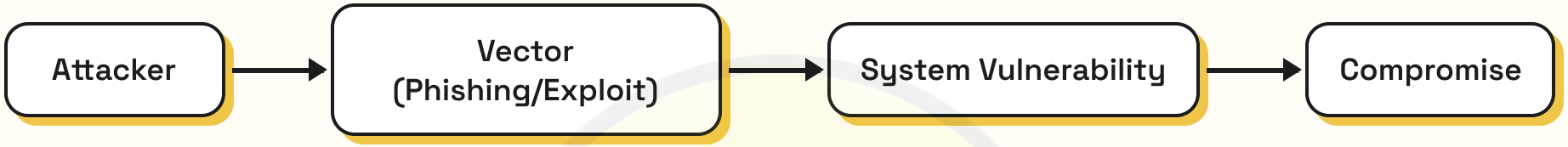
BOTNET

A network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

- Composed of a Command and Control (C&C) server and numerous infected client nodes (bots or zombies).
- Used extensively to fuel cybercrimes such as Distributed Denial of Service (DDoS) attacks, cryptojacking, and mass spam distribution.



Attack Vector Architecture



Pathways used by cybercriminals to breach target environments.

Attack Vector

ATTACK VECTOR

A path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome.

- Includes compromised credentials, unpatched software, malicious email attachments, and misconfigured cloud buckets.
- Identifying vectors allows security teams to prioritize hardening and defense mechanisms.

Cloud Computing and Security Risks

Examining security implications in distributed, on-demand computing environments.

- Cloud Computing Model: Delivers hosted services over the internet (IaaS, PaaS, SaaS) across public, private, and hybrid deployments.
- Shared Responsibility Model: Cloud provider secures the underlying infrastructure; the customer secures their data, configurations, and access management.
- Key Risks: Insecure APIs, misconfigurations, data breaches, and multi-tenancy vulnerabilities.

Exam corner

- **Q1** Define Cybercrime and distinguish it from traditional crimes with suitable examples.
- **Q2** Explain the key provisions and penalties under the Indian Information Technology (IT) Act, 2000.
- **Q3** What is Social Engineering? Discuss various techniques used by attackers to manipulate users.
- **Q4** Describe the concept of Botnets. How do they act as fuel for launching large-scale cyber attacks?
- **Q5** What is an Attack Vector? Discuss different vectors exploited by cybercriminals to compromise systems.
- **Q6** Explain the security challenges and vulnerabilities associated with Cloud Computing environments.

Unit 1 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 2 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

