Assignment Questions – Cyber Security

Unit-1

Submission Deadline: 29/09/2025

Question 1

Define cybercrime. Explain its nature, scope, and why it has become a major concern in today's digital era. Give suitable examples.

Answer

Definition: Cybercrime refers to any criminal activity that involves a computer, networked device, or a network. In these crimes, the computer may be used as a tool to commit the crime (e.g., cyberstalking, phishing) or it may be the target of the crime (e.g., hacking, denial of service attacks).

Nature of Cybercrime:

- **Intangible:** Unlike physical crime, cybercrime often leaves no physical evidence, making it harder to trace.
- **Borderless:** Cybercriminals can operate from anywhere in the world, crossing international jurisdictions effortlessly.
- **Speed and Scale:** Crimes can be committed in milliseconds and affect millions of victims simultaneously (e.g., a virus spread).

Scope: The scope of cybercrime is vast, ranging from individual offenses (harassment) to property offenses (intellectual property theft) and government offenses (cyberterrorism).

Why it is a Major Concern:

- **Digital Dependency:** Critical infrastructure (banking, healthcare, power grids) relies heavily on interconnected networks.
- **Financial Loss:** It causes trillions of dollars in damages globally through fraud and ransomware.
- **Privacy Erosion:** Massive data breaches compromise the personal identity of millions.

Examples:

1. **Phishing:** Sending fraudulent emails resembling reputable sources to steal sensitive data.
2. **Ransomware:** Malicious software that encrypts a victim's files until a ransom is paid.

Question 2

Discuss the major challenges faced by law enforcement agencies in tackling cybercrimes. How do anonymity, jurisdiction, and technology advancement affect cybercrime investigation?

Answer

Law enforcement agencies (LEAs) face significant hurdles in investigating and prosecuting cybercrimes due to the unique structure of the internet.

1. Anonymity: Cybercriminals use tools like VPNs (Virtual Private Networks), Proxy Servers, and the Tor network (The Onion Router) to mask their IP addresses. This makes it incredibly difficult for LEAs to attribute a crime to a specific individual or physical location.

2. Jurisdiction Issues: The internet has no borders, but laws do. A hacker in Country A can attack a server in Country B while routing traffic through Country C.

- LEAs must navigate complex Mutual Legal Assistance Treaties (MLATs) to get data from foreign ISPs.
- Laws regarding what constitutes a crime vary significantly between nations.

3. Technological Advancement: Criminals often adopt new technologies faster than law enforcement.

- **Encryption:** End-to-end encryption prevents authorities from accessing evidence even if they seize the device.
- **Anti-Forensics:** Attackers use tools to wipe logs and hide their tracks, leaving little evidence for forensic analysts.

Question 3

What is email spoofing? Explain its working mechanism with an example and suggest preventive measures. How could better cybersecurity policies or user awareness have prevented it?

Answer

Definition: Email spoofing is the creation of email messages with a forged sender address. The goal is to mislead the recipient about the origin of the message, often to gain trust for phishing attacks.

Working Mechanism: Email protocols (like SMTP - Simple Mail Transfer Protocol) do not inherently authenticate the sender. An attacker can modify the email header fields, specifically the `From:` field, to display any name or address they choose.

Example: An attacker sends an email to an employee that appears to come from `ceo@company.com`. The email requests an urgent wire transfer to a vendor. The employee, seeing the CEO's name, complies without verifying.

Preventive Measures:

- **SPF (Sender Policy Framework):** An email authentication method that specifies which mail servers are authorized to send email on behalf of a domain.
- **DKIM (DomainKeys Identified Mail):** Adds a digital signature to emails so the receiver can verify that the email was not altered in transit.
- **DMARC:** Uses SPF and DKIM to provide instructions to the receiving mail server on how to handle emails that fail authentication.

Role of Awareness: Better policies could prevent this by mandating multi-factor verification for financial transfers. User awareness training teaches employees to check the `Reply-To` address and verify urgent requests via a secondary communication channel (e.g., a phone call).

Question 4

Differentiate between spamming and internet time theft. Explain how each affects individuals and organizations. Compare and contrast their technical mechanisms, economic impact, and detection challenges.

Answer

Spamming	**Internet Time Theft**
Sending unsolicited bulk messages to a large number of recipients.	Unauthorized use of an organization's internet bandwidth or computing resources by employees for personal use.
Mechanism: Uses Botnets and automated scripts to harvest emails and blast messages via open SMTP relays.	**Mechanism:** Involves personal browsing, streaming, or social media usage during work hours using company networks.
Impact: Clogs network bandwidth, fills storage servers, and increases phishing risks.	**Impact:** Reduces productivity, wastes bandwidth, and exposes the internal network to malware sites.
Detection: Spam filters, keyword analysis, and IP blacklisting.	**Detection:** Traffic analysis, proxy logs, and employee monitoring software.

Comparison: While spam is an external attack meant to advertise or defraud, internet time theft is an internal threat related to productivity and resource misuse. Economically, spam costs organizations in security infrastructure and cleanup, whereas time theft costs organizations in lost man-hours and salary paid for non-work activities.

Question 5

Explain the concept of a salami attack with a real-life example. Why is it difficult to detect such cybercrimes?

Answer

Concept: A Salami Attack (or Salami Slicing) is a technique where an attacker commits a financial crime by stealing very small amounts of money from a large number of accounts. The

amounts are so small (like thin slices of salami) that they are individually unnoticeable, but cumulatively amount to a large sum.

Real-Life Example: Consider a bank that calculates interest on savings accounts. The interest might be \$15.3456. The bank normally rounds this to \$15.35 or \$15.34. In a salami attack, a programmer modifies the system to truncate the value to \$15.34 and moves the remaining fraction (\$0.0056) to their own secret account. When applied to millions of transactions daily, this generates significant profit.

Why it is Difficult to Detect:

- **Sub-threshold Nature:** The stolen amount from each individual is negligible (often fractions of a cent), so customers rarely notice or complain.
- **Internal Integrity:** Standard accounting audits often ignore rounding errors or consider them statistically insignificant.
- **Logic Bomb:** The code performing the theft is often hidden deep within legitimate banking software and may only run under specific conditions.