First Internal Examination

Q1. Fill in the blanks:

1. **Evidence** - Cyber crime investigation involves the identification, collection, and analysis of evidence to determine illegal activities.
2. **Warfare** - Cyber warfare refers to the use of internet-based attacks to target a nation's critical systems, like power grids or government databases.
3. **Integrity** - While gathering evidence during data recovery, it is crucial to maintain integrity to ensure the evidence remains admissible in court.
4. **Preserving** - The process of preserving original media ensures that no modifications occur, making the evidence admissible in legal proceedings.

Q2. Compare Information vs. Intelligence with respect to cyber threats.

Aspect	**Information**	**Intelligence**
Definition	Raw, unprocessed data collected from various sources.	Analyzed and processed information for decision-making.
Nature	Static and factual.	Dynamic and actionable.
Usage	Used to identify patterns or potential threats.	Used to make strategic decisions and respond to threats.
Examples	Logs of network activity, IP addresses.	Insights on potential attackers' methods, motives.

Q3. List the types of hackers and describe them in detail.

1. **White Hat Hackers**: Ethical hackers who use their skills to identify and fix vulnerabilities.
2. **Black Hat Hackers**: Malicious hackers who exploit vulnerabilities for illegal purposes.
3. **Gray Hat Hackers**: Operate in a gray area, sometimes violating laws but without malicious intent.
4. **Script Kiddies**: Inexperienced hackers using pre-written scripts or tools.
5. **Hacktivists**: Use hacking to promote political or social agendas.

Q4. Differentiate the following with appropriate tools and examples:

Aspect	Sniffing	Scanning
Definition	Capturing data packets in transit.	Probing systems or networks for vulnerabilities.
Tools	Wireshark, Tcpdump	Nmap, Nessus
Purpose	To analyze network traffic.	To identify weak points in a network.

Aspect	Authentication	Authorization
Definition	Verifying user identity.	Granting access to resources.
Tools	Passwords, biometrics	Role-based access control (RBAC) systems.
Purpose	To ensure only legitimate users access the system.	To control the level of access a user has.

Q5. Explain the following social engineering types:

1. **Shoulder Surfing**: Observing a person's screen or keyboard to obtain sensitive information, such as passwords or PINs.
2. **Water Holing**: Setting up fake websites to target specific groups and infect their systems.
3. **Dumpster Diving**: Retrieving confidential information from discarded items like papers or drives.
4. **Pharming**: Redirecting users to malicious websites to steal information.

Second Internal Examination

Q1. Discuss the guidelines of evidence collection.

- Ensure the evidence is collected legally and ethically.
- Maintain the integrity of evidence with proper documentation.
- Use tools like write blockers to prevent evidence tampering.
- Chain of custody must be established for admissibility in court.

Q2. State what potential evidence the devices might contain in case of any cyber crime.

1. **Digital Cameras**: Photos, videos, metadata (e.g., timestamps, GPS data).
2. **Hard Drives**: Logs, documents, applications, deleted files.
3. **Modem, Router, Hub, Switches**: Logs of internet activity, MAC addresses.
4. **Pagers**: Stored messages, timestamps, recipient information.

Q3. What is forensic duplication? Discuss it with all possible techniques.

Definition: Forensic duplication involves creating an exact, bit-by-bit copy of digital evidence for analysis without altering the original.

Techniques:

1. **Disk Imaging**: Creating a complete image of a drive (e.g., using FTK Imager).
2. **Logical Copying**: Extracting specific data such as files or directories.
3. **Live Acquisition**: Copying data from active systems in volatile memory.

Q4. Explain the Four principles for dealing with digital evidence in detail.

1. **Admissibility**: Ensure evidence is collected legally and ethically to be used in court.
2. **Authenticity**: Maintain the originality of the evidence without modification.
3. **Integrity**: Use cryptographic hashes to prove the evidence has not been altered.
4. **Chain of Custody**: Document every step in the handling process for accountability.

Q5. How email headers will help the investigation team to collect evidence?

- Email headers provide metadata like sender IP, recipient addresses, timestamps, and routing information.
- They help trace the originating IP address of the email, though IP spoofing or anonymizers may limit reliability.