Cybercrime :-

as any criminal misconduct carried using network, technical gadgets or the internet.

Types of cybercrime :-

i) crime against individual
  - Email spoofing
  - Spamming
  - Harrassment & cyber stalking

ii) crime against property
  - credit card frauds
  - Intellectual property
  - Internet time

iii) crime against organization
  - Unaccess of computer
  - DOS
  - Logic Bomb
  - Dindling
  - Virus
  - Salami
  - Email Bombing

iv) crime against society
  - Forgery
  - cyber Terrorism
  - web Jacking

Protection against cybercrime :-

- Use complex passwords
- keep online profiles secure
- safeguarding data
- Safeguard mobile devices
- secure online Identity
- safeguarding computers with security software

Types of cyber criminal :-

1. Hackers
   - a) white
   - b) Grey
   - c) Black
2. Internet stalkers
3. Disgruntled employees
4. Phreakers

Phases of Ethical Hacking

i) Reconnaissance

ii) Scanning

iii) Gaining Access

iv) Maintaining Access

v) Clearing tracks

vi) Reporting

vii) Post-Testing Actions.

Digital Forensics

→ process of investigating crimes committed using any type of computing device (such as computer, servers, lap top, cell phones).

→ The ultimate goal of Digital Forensics investigation is to preserve, identity, acquire, document digital evidence to be used in court of law.

Process of Digital Forensics:-

i) Identification

Identity purpose of investigation, resources required.

ii) Preservation:-

Data is isolated, secured and preserved.

iii) Analysis:-

Identity tool and techniques, process data, Interpret Analysis result.

iv) Documentation:-

Documentation of crime scene, along with photograph sketching and crime-mapping

v) Presentation:-

Process of summarization and explaination of conclusions done with help of gathered facts.

Types of Digital Forensics:-

- Disk Forensics.
- Network Forensics
- Wireless Forensics
- Database Forensics
- Malware Forensics
- Email Forensics
- Memory Forensics

Digital Evidences:-

1. Logs.
   - OS Logs
   - Database Logs
   - Email Logs
   - phone logs
   - Network logs
   - IP logs
   - server logs
   - Device fingerprints
2. Video Footage and Images
3. Archives
4. Active Data
5. Metadata
6. Residual data
7. Volatile Data.
8. Replicant Data.

Date

Chain of custody - Digital Evidences

Data collection → Examination → Analysis → Reporting

Media → Data → Information → Evidence

- Collection:-
  documenting the collection procedure
- Packaging and Labelling:-
- Sealing
- Documentation
- Storage
- Transfer
- Analysis
- Reporting

Anti forensics.

- Anti forensics, also known as counter-forensics, refers techniques and methods employed to deliberately thwart or undermine digital forensic investigation
- The goal is to disrupt or manipulate the collection, analysis, and preservation of digital evidence, making it more challenging for forensic investigator to uncover information or illicit activities.

common Anti-Forensic techniques:-

- Data Deletion
- Data Encryption
- Steganography
- Filesystem Manipulation
- Network Anonymization
- Memory Scrubbing
- File Deletion and Shredding
- Attack on Forensic Tool.
- Tampering with Timestamps
- Data Fragmentation
- Booby Trapping

Incident Response

→ IR is a systematic approach to managing and mitigating the impact of security incidents on an organization's IT infrastructure.

1. Preparation.
   - IRP
   - Training and Awareness
   - Tools and Resources
2. ~~Event Detection~~ (Identification:-
   - Event Detection
   - Incident Triage
3. Containment
   - Isolation
   - Remediation
4. Eradication
   - Identify and Remove
   - System Restoration
5. Recovery
   - Business continuity
   - Data Recovery
6. Lessons Learned
   - Post-Incident Analysis
   - Documentation
7. Communication
   - Internal communication
   - External communication

Roles of CSIRT in handling incident

- computer security Incident Response Team

1. Preparation
2. Detection and Analysis
3. containment and Eradication
4. Recovery
5. coordination and communication
6. Documentation and Reporting
7. continous Improvement
8. Threat Intelligence Integration.
9. Legal and Regulatory compliance.

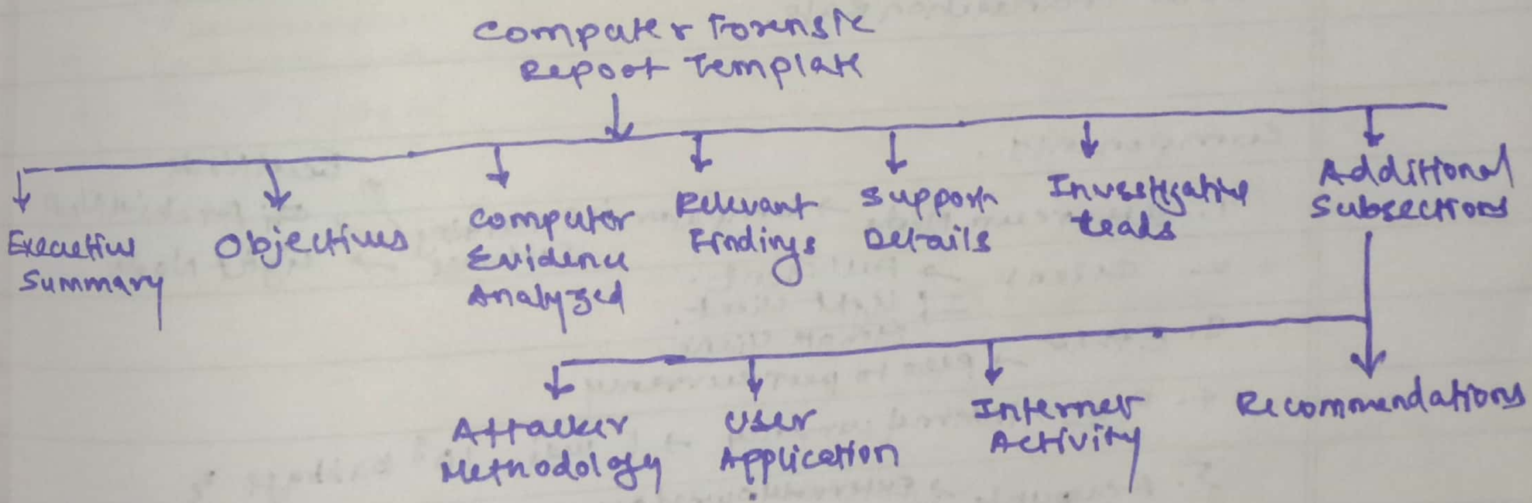
Mod 6:- Report Generation.

Forensic Report :-

Goals of Forensic Report:-

- Documentation of Evidence
- Analysis and Interpretation
- Clarity and Precision
- Objectivity and Impartiality
- Compliance and Standards
- Support for Legal Proceding.
- Transparency and Accountability
- Risk Mitigation

Layout of Forensic Report


Computer Forensic Report Template
Executive Summary
Objectives
Computer Evidence Analyzed
Relevant Findings
Support Details
Investigative Leads
Additional Subsections
Attacker Methodology
User Application
Internet Activity
Recommendations