UNIT-1

Cyber Forensics Fundamentals

- computer forensics
    - set of methodological procedures and techniques to help identify, preserve, extract, interpret, document adnf preserve evidence from computing equipment that is accepatble in a legal/administrative proceeding
    - objectives
        - identify, gather, preserve evidence
        - gather evidence in a forensically sound manner
        - assess the intent of the perpetrator
        - minimize losses to org
        - protect org from future incidents
    - need
        1. protect integirty and existence of IT infra in orgs
        2. collect evidence that proves attacker's actions in court
        3. efficiently track down perpetrators from different parts of the world
        4. protect org's financial resources and time
    - when is it used
        - prepare for incident by strengthening defense mech and closing loopholes in security
        - identify actions needed for incident response
        - act against copyright and IP theft/misuse
        - estimate and minimize damages to corporate resources
        - set up security paramter/norms to ensure readiness
- cybercrimes
    - an illegal act involving a computing device, network, its sys or apps
    - types(based on the line of attack)
        - internal/insider
            - by an entrusted person with authorized access to the network
        - external
            - attacker from outside the org gains unauthorized access to comp sys or assets
    - examples
        - espionage
        - IP theft
        - trojan horse attack
        - SQL attack
        - brute force attack
        - DoS attack
        - cyber defamation
    - impact(at organizational level)
        - loss of CIA in organizational sys
        - theft of sensitive data
        - huge financial losses

            - reputational damage
- digital evidence
    - any info of probative value either stored or transmitted in digital form
    - is fragile by nature
    - Locard's Exchange principle
    - types
        - volatile data
            - data that is lost as soon as device is powered off
        - invoaltile data
            - permanent data stored on secondary storage
    - where it might help
        - identity theft
        - info leakage
        - abuse of Internet
        - false docs and accounts
    - sources
        - user created files
        - user protected files
        - computer created files
    - rules of evidence
        - understandable
        - admissible
        - authentic
        - reliable
        - complete
    - best evidence rule
        - court allows originals of docs, photo or recordings
        - copy only allowed after finding reasons for submission to be genuine
    - # SWGDE(scientific working group on digital evidence)
    - ACPO(association of chief police officers) principles of digital evidence
        - 4 principles
- forensic readiness
    - org's ability to optimally use digital evidence in a limited period of time wih minimal investigation costs
    - helps maintain business continuity by helping businesses iddentify what's missing and replace them in a timely manner
    - forensics reediness planning
        - a set of processes to be followed to achieve and maintain forensics readiness
- forensics investigator
    - need
        - cybercrime investigation
        - sound evidence handling
        - incident handling and response
    - roles + responsibilites
        - dtermiens extent of damage done

        - recovers data of investigative value
        - creates image of original evidence without rtamepring for integrity
        - guides investigating officals
    - features of a good investigator
        - good writing skills
        - strong analytical skills
        - has knowledge of laws with relevance to the case
        - knowledge of various tech, S/W and H/W
- computer forensics + legal compliance
    - legal compliance ensures that any evidence collected and analyzed is admissible in court

---

- forensic investigation
    - methodological approach to investigate, seize and analyze digital evidence and manage teh case from search to reporting the investigation result
    - importance
        - must ensure integrity
        - must compyly with local laws and established precedents
        - must follow a repeatable and well-docuemnted set of steps such taht every iteration provides the same findings
    - phases
        - pre-investigation
            - tasks to be performed prior to be commencement of the investigation
            - stages
                - setting up computer forensics lab
                    - CFL(computer forensics lab) is a location that houses S/W and H/W tools and forensic workstations required for conducting a computer-based investigation with regard to the collected evidence
                    - considerations
                        - planning and budgeting
                        - physical and structural design
                        - work area
                        - phy security
                        - human resource
                        - forensic lab
                - buliding the team
                    - keep it small to protect confidentiality
                    - ensure everyone has necessary clearance and authorization
                    - some people involved
                        - photograpehr
                        - incident responder
                        - incident analyzer
                        - evidence examiner
                        - attorney
            - understanding the H/W and S/W requirements of a forensic lab
                - H/W
                    - 2+ workstations with good RAM and CPU

      - archive + restore devices
      - media sterilization sys
    - S/W
      - OSes
      - password-cracking tools
      - data analyzers
      - data recovery tools
      - file viewers
      - file type conversion tools
- investigation
  - main phase
  - methodology
    - documenting the e-crime scene
      - to maintain a record of all forensic investigation processes
    - search and seizure
      - planning the search and seizure; it msut cotnain
        - description of incident
        - case name of incident
        - location of incident
        - etc.
      - initial search of the scene
      - securing and evaluating the crime scene
      - seizing the evidence
    - evidence preservation
      - proper hnadling + documentation of evidence to ensure that it is free from contamination
    - data acquisition
      - collecting evidence from the location of the incident
    - data analsis
      - examining, identifying, converting and modeling data to isolate useful information
    - case analysis
- post-investigation
  - includes docs of all actions undertaken and all findings uncovered during the investigation
  - ensures that the report is easily explicable to the target audience and provides adequate and acceptable evidence
  - stages
    - gathering and organizing info
      - identify facts
      - gather evidence
      - list conclusions
    - writing the investigation report
    - testifying as an expert witness