Experiment 8

Chinmay Parikh A059

Questions

1. Explain various stages in computer forensics?
2. What is log analysis? How it is useful in cyber forensics?
3. Explain common log format?
4. What section of Indian IT act may be applicable in case of DoS attack, Virus dissemination?

Answers

1. Computer forensics is a meticulous practice. When a crime involving electronics is suspected, a computer forensics investigator takes each of the following steps to reach — hopefully — a successful conclusion:

    1. Obtain authorization to search and seize.
    2. Secure the area, which may be a crime scene.
    3. Document the chain of custody of every item that was seized.
    4. Bag, tag, and safely transport the equipment and e-evidence.
    5. Acquire the e-evidence from the equipment by using forensically sound methods and tools to create a forensic image of the e-evidence.
    6. Keep the original material in a safe, secured location.
    7. Design your review strategy of the e-evidence, including lists of keywords and search terms.
    8. Examine and analyze forensic images of the e-evidence (never the original!) according to your strategy.
    9. Interpret and draw inferences based on facts gathered from the e-evidence. Check your work.
    10. Describe your analysis and findings in an easy-to-understand and clearly written report.
    11. Give testimony under oath in a deposition or courtroom.

2. LOG File - Log files are considerable sources for determining the health status of a system and used to capture the events happened within a computer system and networks. Logs are collection of log entries and each entry contains information related to a specific event that has taken place within a system or network. Many logs within an association contain records associated with computer security which are generated by many sources, including operating systems on servers, workstations, networking equipment and other security software's, such as antivirus software, firewalls, intrusion detection and prevention systems and many other applications.

Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful for performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems. Cyber forensics is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of cyber evidence derived from cyber sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations [9].One important Element of cyber forensics is the credibility of the cyber evidence. In Cyber forensic, log files are like the black box on an airplane that records the events occurred within an organization's system and networks. Logs are composed of log entries that play a very important role in evidence gathering and each entry contains information related to a specific event that has occurred within a system or a network.

3. The Common Log Format, also known as the NCSA Common log format, is a standardized text file format used by web servers when generating server log files. Because the format is standardized, the files may be analyzed by a variety of web analysis programs. Each line in a file stored in the Common Log Format has the following syntax: host ident authuser date request status bytes.

4. Indian IT ACT –

   - Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs : Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.
   - Denial of Service attacks : Section 43 IT Act