Abstract

Network forensics is a branch of digital forensics, which applies to network security. It is used to relate monitoring and analysis of the computer network traffic, that helps us in collecting information and digital evidence, for the protection of network that can use as firewall and IDS. Firewalls and IDS can’t always prevent and find out the unauthorized access within a network. This paper presents an extensive survey of several forensic frameworks. There is a demand of a system which not only detects the complex attack, but also it should be able to understand what had happened. Here it talks about the concept of the distributed network forensics. The concept of the Distributed network forensics is based on the distributed techniques, which are useful for providing an integrated platform for the automatic forensic evidence gathering and important data storage, valuable support and an attack attribution graph generation mechanism to depict hacking events.

References

Distributed Network Forensics Framework: A Systematic Review

- D. Wang, T. Li, S. Liu, J. Zhang, C. Liu, 2007. Dynamical Network Forensics Based on Immune Agent Third International Conference on Natural Computation (ICNC) IEEE.
- Yin Zhang, Detecting Stepping Stones Http:// www. icir. org /vern/papers/stepping/.
Index Terms

Computer Science

Security

Keywords

Network security  Distributed framework  Agent  Proxy