Obtaining Digital Evidence from Intrusion Detection Systems

Abstract

Intrusion detection techniques have appeared to inspect all of the inbound and outbound network activities, and to identify suspicious patterns that indicate an attack that might compromise an information system. However, related information can be collected so as to supply evidence in criminal and civil legal proceedings. Several works have been carried out in the domain of Intrusion Detection and Prevention System (IDPS) but, none of the resulting models taking into account the possibility to collect intrusion related information in such a way that some of it can be turned in evidence in a proactive digital forensic purpose. In the literature, some authors have mentioned the possibility of re-designing IDPS as sources of evidence but, a formal model has never been proposed. This paper proposes an intrusion detection architecture for digital forensic purposes implemented using SNORT program.

References

- Biswanath Mukherjee, L. Todd Heberlein, and Karl N. Levitt. : Network Intrusion
Obtaining Digital Evidence from Intrusion Detection Systems


Index Terms

Computer Science  Security

Keywords

Intrusion detection and prevention system  Digital forensic  Cybercrime investigation