Abstract

This paper is deliberated to provide a model for Host-based Intrusion Detection and Prevention (HIDPS). HIDPS is increasingly becoming important to protect the host computer systems and its own network activities. HIDPS with intelligence is integrated into the computer systems to detect the intruder attacks activities, malicious Behaviour, application anomalies and protect the Information Systems from intruders and report the events to the HIDPS System Administrator. HIDPS is composed of software to monitor and analyze events occurring in the computer systems and information systems and to identify and stop potentially harmful incidents to the Systems. In this context, computer security is an essential property. HIDPS is one of the promising research areas of computer security as most of the security violations in systems occur due to malicious code and intruder activities being able to penetrate to the system barriers. Malicious code and intruder activities affect the computer systems by compromising integrity, confidentiality and availability of resources. It also changes the system Behaviour and extracts the system's vital informations. This paper reviewed and compared the related various research papers on HIDPS to provide a suitable norm on HIDPS at two levels of intrusion detection and prevention i. e. , user level and kernel level along with two phases of
intrusion detection engines- Misuse and Anomaly detections for the best-fit system to any unique host computer systems.

References

- Reza Entezari-Maleki, Arash Rezaei, and Behrouz Minaei-Bidgoli. Comparison of Classification Methods Based on the Type of Attributes and Sample Size.
- Giovanni Vigna and Christopher Kruegel. 2005. Host-Based Intrusion Detection, JWBS001C.

**Index Terms**

Computer Science

Security

**Keywords**

Misuse detection Anomaly detection Support Vector Machine (SVM) algorithm C4.5 Algorithm