Abstract

An intrusion detection system is an essential security component of any computing or network resource. Its function is to verify that an intrusive activity has occurred within the target system. However, as with any security technology, it has its limitations. The reality is that intruders are always a step ahead of the security measures of the target system and will likely find a loophole.

Even if a computing infrastructure is equipped with an intrusion detection system, it does not mean that the intrusion detection system will detect 100% of the malicious activities that occur. There is a need for the security personnel to be made aware of the strengths and weaknesses of their running intrusion detection systems in order to keep vigilant of potential attacks and to undertake countermeasures to known weaknesses. Evaluation of intrusion detection systems provides for this need.

The main purpose of evaluations is to determine the performance of intrusion detection systems which reveals their strengths and weaknesses. Evaluations are beneficial in terms of helping to focus effort on eliminating current weaknesses, documenting existing technologies and guiding research.

This dissertation describes the evaluation on intrusion detection systems using publicly available test data sets and open source intrusion detection systems. The performance of the selected intrusion detection systems is measured and performance ranking conferred based on their detection rates. In addition, this dissertation also highlights the weaknesses of previous evaluations to improve future evaluations.