Abstract

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPS have become a necessary addition to the security infrastructure of nearly every organization. False positives and false negatives happen
A Data Mining Analysis and Approach with Intrusion Detection / Prevention with Real Traffic
to every intrusion detection and intrusion prevention system. This work proposes a mechanism for false positive/negative assessment with multiple IDSs/IPSs to collect FP and FN cases from real-world traffic and statistically analyze these cases. Over a period of 16 months, more than 2000 FPs and FNs have been collected and analyzed. From the statistical analysis results, we obtain three interesting findings. First, more than 92.85 percent of false cases are FPs even if the numbers of attack types for FP and FN are similar. That is mainly because the behavior of applications or the format of the application content is self-defined; that is, there is not complete conformance to the specifications of RFCs. Accordingly, when this application meets an IDS/IPS with strict detection rules, its traffic will be regarded as malicious traffic, resulting in a lot of FPs. Second, about 91 percent of FP alerts, equal to about 85 percent of false cases, are not related to security issues, but to management policy. For example, some companies and campuses limit or forbid their employees and students from using peer-to-peer applications; therefore, in order to easily detect P2P traffic, an IDS/IPS is configured to be sensitive to it. Hence, this causes alerts to be triggered easily regardless of whether the P2P application has malicious traffic or not. The last finding shows that buffer overflow, SQL server attacks, and worm slammer attacks account for 93 percent of FNs, even though they are aged attacks. This indicates that these attacks always have new variations to evade IDS/IPS detection.

References


**Index Terms**

Computer Science

Egovernance And Cloud

Computing Services

**Keywords**

Ids  Fps  Fns  Fp