Abstrak

Mekanisma kawalan capaian yang diberikan bersama-sama sistem pengendalian komputer kurang berkesan dalam menahan pencerobohan dari pengguna luar. Sistem Pengesan Pencerobohan adalah sejenis perisian keselamatan komputer yang boleh mengesan pencerobohan yang sedang berlangsung dan juga mampu mengelakkan kerosakan sistem dari berlaku. Pengesanan yang dilakukan ini bergantung kepada metodologi pengesanan yang digunakan oleh Sistem Pengesan Pencerobohan. Dari berbagai jenis metodologi pengesanan yang ada, empat jenis metodologi dipilih disini. Setiap metodologi pengesanan dibincangkan dan juga ditaksirkan dari segi keberkesanannya dalam menangani pelbagai jenis pencerobohan, kesilapan klasifikasi, dan juga dari aspek perlaksanaan sebenar. Beberapa cadangan dikemukakan untuk memperbaikan lagi metodologi pengesanan. Cadangan-cadangan ini termasuk menggabungkan metodologi pengesanan yang ada, memproses jejak audit bagi mengelakkan input yang rosak, dan juga menyertakan mekanisma pencegahan kerosakan sistem akibat dari pencerobohan. Metodologi pengesanan yang digunakan juga perlu mampu ditingkatkan lagi untuk mengikuti perkembangan infrastruktur. Pengesanan pencerobohan secara am boleh juga dipertingkatkan lagi dengan menguatkuasakan polisi keselamatan, mengawal masa capaian, dan juga menghadkan hak-hak kakitangan pentadbiran untuk mengelakkan penyalahgunaan hak-hak yang diberikan.

Abstract

Access control mechanisms included in operating systems are not very effective in preventing intrusions by the most determined of attackers. An Intrusion Detection System (IDS) is a security software that is able to detect an intrusion when it occurs and can potentially prevent a system compromise from being completed. The actual detection is done by the detection method used by the IDS. Four detection methods are discussed and assessed in terms of their effectiveness in repelling intrusion types, vulnerability to classification errors; and also performance in practical implementation. Recommendations are made to improve the general effectiveness of the detection methods in use. They include combining detection methods, pre-processing audit logs to prevent bad input, and including mechanisms to preempt intrusions from completing. The method must also be scalable to accommodate infrastructural growth. Intrusion detection can also be improved by careful enforcement of security policy, adding access time limitations, and also limiting administrative privileges to prevent abuse of the powers entrusted upon them.