Sammanfattning

För att undersöka möjligheterna att upptäcka intrång med hjälp av Window NTs inbyggda loggningssystem, har vi med hjälp av information från tidigare projekt på Karlstads universitet (KaU) reproducerat intrång, designat en databas för intrång och undersökt möjligheterna att jämföra framtagna intrångssignaturer mot de av operativsystemet genererade. Parallellt med detta har vi tagit fram beskrivningar på vanliga säkerhetsbrister, intrångsdetekteringsmetoder och intrångsteknik. Vi kom fram till att inte tillräckligt stor mängd av de program som finns, använder det inbyggda loggsystemet för att det ska vara givande att bygga ett intrångsdetekteringssystem utifrån det. Mycket av vår arbetstid gick åt till att förstå loggstrukturen och att skriva ett program som kan läsa filerna som loggarna lagras i. Utifrån detta kom vi fram till att loggsystemet var onödigt invecklat och inte tillräckligt exakt. Det verkar mer anpassat för att visa läsbara loggar än att ge information lämpad för detektering av händelser.

Analysis and detection of intrusions

in Windows NT

Abstract

The aim of this thesis is to investigate the possibilities to automatically discover intrusions with the help of Windows NTs build-in logging system. We have with information from earlier projects on Karlstads University (KaU) reproduced intrusions, designed a database for intrusions and tried to compare in advance generated intrusion signatures with the ones generated from the operating system. Our conclusion is that not enough of the available programs are using Windows NTs built-in logging system in order for it to be valuable or possible to build a functional Intrusion Detection System (IDS) from it. A large part of our work went into the understanding of the logging structure and to create a program that could read from it. We are also not convinced that enough logs are generated by the operating system itself. The logs are often unnecessary complex and not specific enough. We believe that it is designed to present viewable logs from which conclusions can be drawn from, and not to give information that can be used directly to detect certain events.