Sammanfattning

Detta examensarbete behandlar loggning i samband med intrång i Windows NT (NT). I början av projektet gjorde någon utomstående ett intrång på vår dator. Angriparna använde vår dator för att lagra olagliga spel. Detta är bara en av många anledningar till att göra ett intrång. Genom logginformationen som genererades under detta intrång kunde vi analysera och förstå vad angriparen hade gjort med vårt system. För att fortsätta detta arbete började vi reproducera egna intrång genom att använda speciella program. Dessa intrång genererade i sin tur loggar som vi kunde analysera. Den här analysen hjälpte oss att bestämma om loggarna i NT fungerar tillräckligt bra eller inte. Vidare har vi under detta arbete lärt oss att detektera ett intrång med hjälp av loggarna.

Det här examensarbetet svarar även på frågorna vilka angriparna kan tänkas vara, vad svagheterna i ett system är och hur loggning fungerar i NT. Dokumentet är baserat på våra egna erfarenheter.

Analysis of audit logs from intrusions in Windows NT

Abstract

This Bachelor's project considers auditing in relation to intrusions in Windows NT (NT). At the beginning of this project someone made an intrusion in our system. These intruders were using our computer to store illegal computer games. This is just one of several purposes to conduct an intrusion. Through the audit logs that were generated during this intrusion, we were able to analyze and understand what the intruder had done with our computer. To proceed this work we started to use special programs to reproduce known intrusions by ourselves. These intrusions generated logs that we could analyze. The analysis helped us decide whether the logs in NT are sufficient or not. From this work we also learned how to detect an intrusion from the logs.

This Bachelor's project also answers the questions: who the intruders might be, what the weaknesses in a system can be and how auditing works in NT. The document is based on our own experiences.