Sammanfattning

Denna rapport beskriver arbetet att vidareutveckla Veriscan Security AB:s prototyp för logghanteringssystemet Matrix. Bakgrunden till detta projekt är att arbetet med att kontrollera/granska loggfiler ofta är mycket tidskrävande, då det genereras enorma mängder information i loggfiler i ett nätverk. Veriscan Security AB:s mål med projektet är att förenkla och effektivisera systemadministratörers arbete med kontroll av logginformation. Detta skulle öka chansen att upptäcka t.ex. intrångsförsök.

Tyngdpunkten i detta arbete ligger på design och implementation av ett protokoll för kommunikation mellan olika datorsystem och en server i ett nätverk. Ytterligare delar som täcks in av examensarbetet är design och implementation av både servern, som hela systemet ska kretsa kring, och programvara för insamling av logginformation från de olika datorsystemen. En managerkonsol för konfiguration och fjärrstyrning av systemet, samt ett grafiskt användargränssnitt till denna, ska även konstrueras.

Resultatet av arbetet har blivit ett fungerande, körbart system, vilket styrs från ovan nämnda managerkonsol med tillhörande användargränssnitt. Systemet Matrix behöver dock vidareutvecklas ytterligare innan det blir komplett.

Matrix – a network-based system for centralizing and administration of log-information

Abstract

This report describes the further development of a system-prototype for log-handling called Matrix, which is owned by Veriscan Security AB. The reason for this project is, that inspection of log-files often is very time-consuming since the amount of log generated in a network is huge. Veriscan Security AB's purpose with this project is to simplify and increase the efficiency of the work that system-administrators have to perform in order to inspect log-information. As a result, the probability of detecting attempts of intrusion for example would be significantly higher. The emphasis of this project lies on the design and implementation of a protocol for communication between computer-systems and a server in a network. Also included in the project is the design and implementation of both the server, which is the central part of the system, and the application used to gather log-information from the computer-systems. A manager-console with a graphical user interface for configuration and remote control of the system is also to be constructed.

The result of this bachelor's project is a working system, which is controlled from the manager-console mentioned above. The manager-console has a graphical user interface. Further development of the system Matrix needs to be done before it's complete.