Applying Data Mining Technology to Intrusion Dection System

Student：CHAO-HSIANG CHANG Advisor：Dr. Chieh-Yuan Tsai

Institute of Industrial Engineering and Management
Yuan-Ze University

ABSTRACT

Quick development of the information technology made Internet and E-Commerce growth rapidly, and people can communicate each other more easily. When people is dependent on the advance technology more and more,the Information security will be an issue come after. The bussiness will attach greate importance to information secuity because it will cause goodwill damage and poor public image if ignored that.
In recent years, Intrusion Detection System(IDS) that have immediately security detect and response is a very popular information security protection system. It enables to dection abnormal activity, monitor network security, response no authentication required and miss used from internal or external user. Current IDS technology is a perfect alarm system to intrusion and virus, but the log generate from IDS is to detail to read. It's not easy to figure out the intrusion attack behavior from the huge log records, even the expert of information security can look out easily.
Generally speaking, Hacker will use several different kinds of porb and attack attack scripts to the aim until the attack sucessful or all the scripts used. During Hacker raises attacks, it will trigger one to several intrusion alarm that can be collected to generalize attack mode. The generalized attack mode is not common in normal network activity. Therefor, this research will use the logs that record from IDS to generalize the attack source, type, date and count. In order to find out the attack methods, using data mining to build a system that can automatic alarm to administrator and generate attack report from huge IDS records. The solution can help system administrator and manager more easily to understand what kind of attrack they detected, and where the attack from.

Keyword: Intrusion Detection System Data Mining Hacker Network Attack