ชื่อวิทยานิพนธ์ การวิเคราะห์ข้อมูลกิจกรรมของระบบเพื่อตรวจจับการบุกรุก
ผู้เขียน นายศุภโชค สุขเกษม
สาขาวิชา วิทยาการคอมพิวเตอร์
ปีการศึกษา 2548

บทคัดย่อ

งานวิทยานิพนธ์นี้เป็นการนำเสนอแบบจำลองของระบบตรวจจับการบุกรุกระบบคอมพิวเตอร์ โดยเลือกใช้วิธีการวิเคราะห์ข้อมูลกิจกรรมของระบบที่บันทึกไว้ในไฟล์หรือเรียกว่าล็อกไฟล์ (logfile) แบบจำลองนี้นำเสนอสำหรับการพัฒนาระบบตรวจจับการบุกรุกแบบ Host-Based Intrusion Detection System (HIDS) ประกอบด้วยส่วนการทำงาน 3 ส่วนคือ การเก็บรวบรวมข้อมูล (Data Collection Module) การวิเคราะห์ข้อมูล (Analysis Module) และ การแจ้งเตือน (Response Module) โดยส่วนของการเก็บรวบรวมข้อมูลนั้นจะอาศัยข้อมูลจากการทำงานของ syslog ส่วนการวิเคราะห์ข้อมูลจะนำข้อมูลล็อกเหล่านั้นมาวิเคราะห์โดยการกรองข้อมูลล็อกของเหตุการณ์ปกติออกไปก่อนแล้วจึงทำการวิเคราะห์เหตุการณ์ที่คาดว่าเป็นการบุกรุกด้วยวิธีการเปรียบเทียบรูปแบบข้อมูลล็อกกับล็อกของเหตุการณ์การบุกรุกในอดีต หากผลการวิเคราะห์ข้อมูลพบว่ามีเหตุการณ์บุกรุกเกิดขึ้นส่วนการแจ้งเตือนก็จะทำการแจ้งเตือนไปยังผู้ดูแลระบบ ในการบันทึกกิจกรรมของระบบโดยทั่วไปนั้น syslog จะทำการบันทึกเหตุการณ์ในระดับต่างๆ กัน เช่น เลือกบันทึกเป็นบางส่วนหรือบันทึกทั้งหมด ในกรณีแรกจะทำให้บางเหตุการณ์ที่มีความสำคัญสำหรับการตรวจจับการบุกรุกไม่ถูกบันทึก ในขณะที่การเลือกบันทึกแบบทั้งหมดนั้นจะต้องใช้พื้นที่สำหรับการบันทึกเหตุการณ์ทั้งหมดมาก ในงานวิจัยนี้ได้ทำการศึกษาวิเคราะห์และนำเสนอระดับของการบันทึกเหตุการณ์ที่เกิดขึ้น เพื่อให้ข้อมูลที่ถูกบันทึกมีประโยชน์สำหรับการวิเคราะห์กิจกรรมการบุกรุกสูงสุดและใช้พื้นที่ที่สำหรับการบันทึกที่เหมาะสม

Thesis Title	Audit Log Analysis for Intrusion Detection
Author	Mr. Supachoke Sukkasame
Major Program	Computer Science
Academic Year	2005

ABSTRACT

This thesis presented a model for intrusion detection system using audit log analysis method. The model is a Host-Based Intrusion Detection System (HIDS) that comprises of three major modules, i.e., data collection, analysis and response modules. The data collection was operated by collecting data from log files obtained from a native system log utility of a unix system. This information then is used by the analysis module to detect intrusion activities. Once an intrusion activity is found, the response module activates its relevant function. Alarms and notification of the attack are report to system administrators via several communication methods such as e-mail, Short Message Service (SMS) etc. The study also suggested level of audit log for general system log utility so that the log information is useful for intrusion detection