# บทคัดย่อ



ระบบรักษาความปลอดภัยบนเครือข่ายที่ให้บริการเว็บเซิร์ฟเวอร์ในปัจจุบันประกอบด้วยระบบไฟร์วอลล์ (Firewall) สำหรับกลั่นกรองข้อมูลระหว่างเครือข่ายและระบบตรวจสอบการบุกรุก (Intrusion Detection System-IDS) สำหรับตรวจสอบการบุกรุกภายในเครือข่าย โดยระบบตรวจสอบการบุกรุกบนเครือข่าย (Network-based IDS) มักจะแสดงผลการแจ้งเตือน (alert) ที่ผสมกันระหว่างการแจ้งเตือนการบุกรุกที่ประสบความสำเร็จและการบุกรุกที่ไม่ประสบความสำเร็จเป็นจำนวนมาก ทำให้ผู้ดูแลระบบประสบปัญหาในการจัดลำดับความสำคัญในการป้องกันและแก้ไขปัญหาการบุกรุกได้อย่างเหมาะสม ปกติแล้วทั้งไฟร์วอลล์และ IDS มักจะบันทึกข้อมูลต่าง ๆ ลงล็อกไฟล์ (log files) เป็นจำนวนมาก การวิเคราะห์ข้อมูลจากล็อกในปัจจุบันนิยมทำแยกกันระหว่างไฟร์วอลล์และ IDS ในความเป็นจริงข้อมูลล็อกของไฟร์วอลล์และ IDS จะมีข้อมูลบางส่วนที่มีความสัมพันธ์เชื่อมโยงกันอยู่ ดังนั้นวิทยานิพนธ์นี้จึงนำเสนอวิธีการจำแนกประเภทการแจ้งเตือนการบุกรุก โดยการนำล็อกไฟล์จากเว็บพร็อกซีซึ่งเป็นไฟร์วอลล์ในระดับแอพพลิเคชันชนิดหนึ่งมาหาความสัมพันธ์กับล็อกของ Network-based IDS ทำให้สามารถทราบถึงข้อมูลประกอบอื่น ๆ ของการบุกรุกนั้น ๆ ซึ่งข้อมูลเหล่านี้จะตัวแปรสำคัญในการพิจารณาจัดลำดับการแจ้งเตือนการบุกรุกของระบบ IDS ในปัจจุบัน

ABSTRACT TE 160603

Presently, network security system consists of firewall for data filtering transferring between network and intrusion detection system (IDS) for detecting intrusion. Network-based IDS always launches alerts that comprise of many of succeeded and unsucceeded attack. These make troubles for administrator to arrange the priority of protection and intrusion problem solving appropriately. Firewall and IDS always record data into many of log files. Today, analyzing log files data for firewall and IDS have been separated but some part of log data from firewall related to IDS log data. This thesis proposed approach to classified the intrusion alerts by correlating log data from WEB proxy in application layer to log data from network-based IDS. By this way, we will able to get other intrusion information in which important for arranging the priority of intrusion alert for IDS.