199851

วิทยานิพนธ์นี้เป็นการพัฒนาชุดซอฟต์แวร์ตรวจจับผู้บุกรุกโดยการสุ่มกระแสข้อมูล ซึ่งใช้การสุ่มแบบ Stratified random ประยุกต์ร่วมกับการตรวจจับผู้บุกรุกของโปรแกรมสนอร์ต เพื่อลดปริมาณข้อมูลของระบบเครือข่าย สำหรับการตรวจจับการบุกรุกในระบบเครือข่ายขนาดใหญ่ ซึ่งเหมาะสำหรับเครื่องคอมพิวเตอร์ขนาดเล็ก

โปรแกรมสนอร์ต เป็นโปรแกรมตรวจจับการบุกรุกผ่านทางระบบเครือข่ายที่ได้รับความนิยมสูงในปัจจุบัน แต่การตรวจจับการบุกรุกนั้นต้องรวบรวมข้อมูลทั้งหมดในระบบเครือข่าย ด้วยเทคนิคการตรวจจับการบุกรุกสองวิธีคือ 1) วิธีการวิเคราะห์พฤติกรรมของข้อมูล และ 2) การวิเคราะห์ลักษณะของการโจมตีเปรียบเทียบกับกฎของโปรแกรม ในระบบเครือข่ายขนาดใหญ่ การรวบรวมข้อมูลจะมีปริมาณมากและมีความต้องการประสิทธิภาพของเครื่องคอมพิวเตอร์สูงสำหรับใช้ในการตรวจจับการบุกรุกของโปรแกรมสนอร์ต

ดังนั้นในงานวิจัยนี้เสนอวิธีการลดปริมาณข้อมูลโดยใช้การสุ่มด้วยวิธี Stratified random และถูกนำไปใช้ในโปรแกรมสนอร์ต งานวิจัยนี้ได้วัดประสิทธิภาพของการตรวจจับผู้บุกรุกประเภทสแกนพอร์ตด้วยโปรแกรมสนอร์ตร่วมกับการสุ่มแบบ Stratified random ซึ่งผลการทดลองพบว่า การสุ่มช่วยลดปริมาณข้อมูลลงอย่างมาก โดยไม่มีผลกระทบต่อประสิทธิภาพการตรวจจับด้วยวิธีการวิเคราะห์ลักษณะการโจมตีเปรียบเทียบกับกฎของโปรแกรมสนอร์ต อย่างไรก็ตามระบบนี้มีผลกระทบต่อประสิทธิภาพการตรวจจับด้วยการวิเคราะห์พฤติกรรม

The objective of this research is to propose the intrusion detection software suite based on the open source intrusion detection system (Snort) with Stratified random sampling. By applying Stratified random sampling, it significantly reduces the amount of collected data needed for the intrusion detection of the Snort. The proposed solution is suitable to the computer with low computation power to be able to handle the large amount data of the large network for intrusion detection.

Snort is the famous network IDS software. Data is collected from the network to analyze the traffic pattern and determine if there is any attack to the network. Snort executes two intrusion detection techniques 1) Behavior-based intrusion detection technique which analyzes the intrusion traffic pattern and 2) Rules-based intrusion detection technique which analyzes intrusion signature within the traffic. Snort requires high performance computer to handle the large amount of data of the large network.

Therefore, this research proposes the software suite that includes Snort with Stratified random sampling. The research investigates the trade-off of applying Stratified random sampling to the Snort in several aspects such as the decreasing amount of collected data, the accuracy of the intrusion detection. By experimented with the real generated data of the port scan attack, the Snort with Stratified random sampling reduces the amount of collected data but still provides the detection accuracy of the Snort in Rule-based detection. However the Snort with Stratified random sampling reduces the accuracy of Behavior-based intrusion detection.