ระบบตรวจจับการบุกรุก เป็นมาตรการการป้องกันระบบคอมพิวเตอร์และระบบเครือข่ายที่สำคัญมาก มีงานวิจัยมากมายที่มีการวิเคราะห์ถึงความสามารถของระบบตรวจจับการบุกรุกจากการป้องกันการโจมตี หรือจำนวนของการตรวจจับที่ผิดพลาด

ในงานวิจัยนี้ได้มีการอธิบายถึงวิธีการใหม่ในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก โดยมีการใช้คะแนนของจุดอ่อนแบบเครือข่ายที่ได้จากการคัดกรองจากรายงานของสถาบันแซนส์มาเปรียบเทียบกับกฎของสนอร์ท โดยที่จุดอ่อนแต่ละรายการได้มีการให้คะแนนจากลักษณะของความเสียหายต่อระบบ นอกจากนี้ งานวิจัยนี้ ได้ทำการแบ่งกลุ่มของจุดอ่อนออกเป็น 3 กลุ่ม คือ ตามประเภทของจุดอ่อน ตามแหล่งที่เกิดของจุดอ่อน และตามผลกระทบที่เกิดขึ้นกับระบบ

จากงานวิจัยพบว่า สนอร์ทสามารถป้องกันจุดอ่อนที่มีอันตรายของระบบเครือข่ายของระบบปฏิบัติการวินโดวส์ได้ 73% และ ในระบบปฏิบัติการตระกูลยูนิกซ์ได้ 65% จากผลการทดลองทำให้ทราบได้ว่า ระบบตรวจจับการบุกรุกมีประสิทธิภาพ แต่ยังคงต้องมีการปรับปรุงในส่วนที่ยังป้องกันไม่ได้

227177

Intrusion detection system (IDS) is an important defensive measure protecting computer systems and networks from abuse. Many researchers analyzed performance of IDS from ability to defend attack or the number of false positives.

In this research is described a new method for analyzing performance of IDS using network-based vulnerability scores by comparing Top 20 vulnerabilities presented by SANS Institute to rules of Snort. Each vulnerability gives the damage score and this research presents these vulnerabilities in three groups: genesis, location, and impact to computer system.

The research reveals that Snort can protect 73% of the critical network vulnerabilities in Windows operating system and 65% in UNIX-like operating system. From this result, it can be readily seen that intrusion detection systems although effective, can still be improved.