วิศวกรรมสาร มข. ปีที่ 36 ฉบับที่ 3 (251-259) กรกฎาคม – กันยายน 2552 บทความวิจัย
KKU Engineering Journal Vol.36 No.3 (251-259) July – September 2009

การลดการแจ้งเตือนที่ผิดพลาดสำหรับการตรวจจับของโปรแกรมสนอร์ต

ศิวนาถ เทียนงาม[*1)] และมยุรี เลิศเวชกุล[2)]

บทคัดย่อ

โปรแกรมสนอร์ต (Snort) เป็นโปรแกรมที่ใช้ในการตรวจจับการบุกรุกบนระบบเครือข่าย โดยการตรวจสอบกับกฎที่กำหนด (Rule-based IDS) ดังนั้นประสิทธิภาพและขีดความสามารถของโปรแกรมสนอร์ตจึงขึ้นอยู่กับกฎที่กำหนด หากกฎที่กำหนดไม่ครอบคลุมกิจกรรมที่เป็นอันตรายต่อระบบเครือข่ายและรูปแบบการบุกรุกระบบเครือข่ายโปรแกรมสนอร์ตจะทำงานล้มเหลว (False Negative Alarm) แต่ถ้าหากมีการกำหนดโครงสร้างของกฎที่ผิดพลาด หรือกฎที่นำมาใช้งานไม่เหมาะสมกับสภาพแวดล้อมภายในระบบเครือข่ายจะทำให้เกิดการแจ้งเตือนที่ผิดพลาด (False Positive Alarm) โดยการแจ้งเตือนที่ผิดพลาดจะส่งผลกระทบให้โปรแกรมสนอร์ตทำงานหนักกว่าปรกติจนไม่สามารถทำงานได้และส่งผลให้ระบบเครือข่ายตกอยู่ในอันตรายจากผู้บุกรุกระบบเครือข่าย การกำหนดกฎที่ทำให้โปรแกรมสนอร์ตสร้างการแจ้งเตือนที่ผิดพลาดจำนวนมากจะส่งผลกระทบให้โปรแกรมสนอร์ตทำงานล้มเหลว ด้วยเหตุนี้ผู้วิจัยจึงได้พัฒนาระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตด้วยการประยุกต์ใช้ระบบเครือข่ายใยประสาท (Neural Network) ที่ผ่านการฝึกด้วยชุดข้อมูลเบื้องต้น (Training Dataset) โดยชุดข้อมูลนำเข้า (Input Data) จะเป็นค่าพารามิเตอร์ที่เกี่ยวข้องกับสภาพแวดล้อมภายในระบบเครือข่ายในขณะที่เกิดการแจ้งเตือนของโปรแกรมสนอร์ตและข้อมูลอ้างอิง โดยผลลัพธ์ (Output Data) ที่ได้จากระบบเครือข่ายใยประสาทจะเป็นการประเมินคุณภาพการแจ้งเตือนที่มีค่าอยู่ระหว่าง 0-100 ค่าดังกล่าวจะถูกนำมาเปรียบเทียบกับเกณฑ์ที่กำหนดเพื่อกำหนดคุณภาพการแจ้งเตือน ในกรณีที่การแจ้งเตือนมีคุณภาพต่ำซึ่งมีค่าอยู่ระหว่าง 0 – 50 ผู้ดูแลระบบเครือข่ายจะนำผลที่ได้ไปปรับลดเฉพาะกฎที่เป็นสาเหตุทำให้เกิดการแจ้งเตือนที่ผิดพลาด ภายหลังจากการนำระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตมาใช้งาน พบว่าโปรแกรมสนอร์ตสามารถทำงานได้อย่างมีประสิทธิภาพ โดยสามารถลดการแจ้งเตือนที่ผิดพลาดได้ถึงร้อยละ 72.78

คำสำคัญ: ระบบเครือข่ายใยประสาท, ระบบตรวจจับการบุกรุกบนระบบเครือข่าย, โปรแกรมสนอร์ต และการลดการแจ้งเตือนที่ผิดพลาดของระบบตรวจจับการบุกรุก

[*1)] นักศึกษาปริญญาโท ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง Corresponding Author, E-mail: Siwanat_jet@hotmail.com

[2)] ผู้ช่วยศาสตราจารย์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง E-mail: Klmayure@yahoo.com

False Positive Decrement for Snort Intrusion Detection

Siwnart Thian-ngam[*1)] and Mayuree Lertwatechakul[2)]

Abstract

Snort is a freeware Intrusion Detection System (IDS). Snort uses rule-based approach to detect intrusions so that its performance and capability based on its active rule set. When a network is attacked, Snort will generate alerts to the administrator. So far false negative could be occurred in case the rule set do not cover malicious activities and attack behaviors. While false positive could be occurred in case the rule set is not appropriate for the computer and network. Since too many false positive event could overload Snort and may be an import factor to fail intrusions detection. Because of the mentioned problem, the main objective of this work is to develop the system as to reduce false positive of Snort, The system applies the neural network. The neural network was trained by well-form dataset. Input data were parameters in the environment as alert occurring and reference data from the Internet The neural network generates a score for an attack that could be rang 0 – 100. In case of low quality alert 0 - 50, the specific rules which caused low quality alert were disabling by administrator. Finally, the obtained results show that the performance of Snort increased with the false positives about 72.78 %.

Keywords: False Alarm, Neural Network, IDS, Snort and Reduce False Positive

[*1)] Post graduated Students, Department of Information Engineering, King Mongkut's Institute of Technology Ladkrabang, Corresponding Author, E-mail: siwanat_jet@hotmail.com

[2)] Assistant Professor, Department of Information Engineering, King Mongkut's Institute of Technology Ladkrabang, E-mail: Klmayure@yahoo.com

1. บทนำ

โปรแกรมสนอร์ต (B. Caswell et al., 2003) เป็นโปรแกรมที่ใช้ในการตรวจจับการบุกรุกบนระบบเครือข่ายโดยไม่เสียค่าใช้จ่ายโปรแกรมสนอร์ตสามารถตรวจจับการบุกรุกได้อย่างมีประสิทธิภาพทำให้มีผู้ใช้งานโปรแกรมสนอร์ตเพิ่มมากขึ้น จึงได้เกิดการรวมตัวกันเป็นสังคมของผู้ใช้งานโปรแกรมสนอร์ตขึ้น กลุ่มบุคคลเหล่านี้จะเขียนกฎของโปรแกรมสนอร์ตขึ้นมาเพื่อให้ผู้ใช้งานโปรแกรมสนอร์ตสามารถดาวน์โหลดนำไปใช้ได้ แต่กฎของโปรแกรมสนอร์ตที่ดาวน์โหลดไปใช้งานนั้นอาจจะยังไม่ได้รับการตรวจสอบที่ดี หรือผู้ดูแลระบบกำหนดกฎที่นำไปใช้งานไม่เหมาะสมกับสภาพแวดล้อมของระบบเครือข่ายทำให้โปรแกรมสนอร์ตสร้างการแจ้งเตือนที่ผิดพลาดขึ้นจำนวนมาก

บทความนี้นำเสนอวิธีการเพิ่มประสิทธิภาพในการทำงานของโปรแกรมสนอร์ตโดยการประยุกต์ใช้ระบบเครือข่ายใยประสาทในการประเมินคุณภาพการแจ้งเตือนที่เกิดขึ้น บันทึกและวิเคราะห์ข้อมูลเพื่อการปรับลดกฎที่ทำให้เกิดการแจ้งเตือนที่ผิดพลาด เนื้อหาในบทความนี้ประกอบไปด้วย ข้อมูลสาเหตุที่ทำให้เกิดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต งานวิจัยที่เกี่ยวข้อง กลไกการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต ผลการทดลองเมื่อเปรียบเทียบกับวิธีพื้นฐานและส่วนสุดท้ายเป็นสรุปผลการทดลอง

2.สาเหตุการเกิดการแจ้งเตือนที่ผิดพลาด

การแจ้งเตือนที่ผิดพลาดของระบบตรวจจับการบุกรุกบนระบบเครือข่าย (K. Timm, 2001) ที่เกิดขึ้นเป็นจำนวนมากนั้นเป็นปัญหาหลักในการรักษาความปลอดภัยในระบบเครือข่ายและการทำธุรกรรมผ่านระบบอินเตอร์เน็ต ซึ่งการการแจ้งเตือนที่ผิดพลาดเป็นจำนวนมาก ได้สร้างปัญหาให้แก่ผู้ดูแลระบบเครือข่ายเป็นอย่างยิ่ง โดยเฉพาะการจำแนกว่าการเชื่อมต่อหรือกิจกรรมใดที่เกิดขึ้นในระบบเครือข่ายเป็นการบุกรุกระบบเครือข่ายหรือเป็นอันตรายต่อระบบเครือข่ายและกิจกรรมใดหรือการเชื่อมต่อใดเป็นการใช้งานปกติบนระบบเครือข่าย โดยในบทความนี้ได้แบ่งสาเหตุการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ตเป็น 2 สาเหตุหลัก คือ กฎมีความผิดพลาด (M. Norton and D. Roelker, 2004) และการกำหนดกฎที่ใช้งาน ไม่เหมาะสมกับสภาพแวดล้อมของระบบเครือข่าย

2.1 กฎมีความผิดพลาด

โปรแกรมสนอร์ตเป็นฟรีแวร์เมื่อมีการบุกรุกระบบเครือข่ายรูปแบบใหม่เกิดขึ้นผู้ใช้งานสามารถปรับปรุงชุดกฎของโปรแกรมสนอร์ตโดยการดาวน์โหลดจากเว็บไซต์ที่ให้บริการ ผู้ใช้งานที่ไม่มีความชำนาญจะไม่สามารถทราบได้เลยว่ากฎที่นำมาใช้งานนั้นมีประสิทธิภาพในการตรวจจับการบุกรุกบนระบบเครือข่ายหรือไม่ จะทราบได้ก็ต่อเมื่อนำกฎเหล่านั้นมาใช้งานจริง เป็นผลให้โปรแกรมสนอร์ตมีความเสี่ยงสูงที่จะทำให้เกิดการแจ้งเตือนการบุกรุกที่ผิดพลาดขึ้น

2.2 การกำหนดกฎที่ใช้งานไม่เหมาะสมกับสภาพแวดล้อมของระบบเครือข่าย

โครงสร้างระบบเครือข่ายภายในของแต่ละองค์กรย่อมแตกต่างกันขึ้นอยู่กับขนาดขององค์กรและนโยบายการรักษาความปลอดภัยทำให้กิจกรรมและพฤติกรรมการใช้งานในแต่ละองค์กรมีความแตกต่างกันไป การกำหนดกฎให้เหมาะสมกับพฤติกรรมผู้ใช้งานบนระบบเครือข่ายจึงมีความสำคัญมากเพื่อป้องกันไม่ให้โปรแกรมสนอร์ตเข้าใจว่าพฤติกรรมปรกติในระบบเครือข่ายเป็นการบุกรุกระบบเครือข่ายและ สร้างการแจ้งเตือนที่ผิดพลาดขึ้นจำนวนมาก บทความนี้จึงได้แบ่งพฤติกรรมที่โปรแกรมสนอร์ตมองว่าเป็นการบุกรุกระบบเครือข่ายเพื่อให้ผู้ใช้งานสามารถกำหนดชุดของกฎได้อย่างถูกต้องแสดงดังต่อไปนี้

- การล็อกอินเข้าใช้งานฐานข้อมูลในระบบเครือข่ายที่มีความผิดพลาดสูง
- ความถี่ของการสื่อสารของโปรโตคอลภายในระบบเครือข่ายสูง
- การกำหนดค่าพารามิเตอร์ที่มีความยาวเกินกำหนด

- การแจ้งเตือนที่เกิดจากส่วนหัว (Header) ของโปรโตคอลที่ใช้ในการส่งเมลล์และไฟล์ข้อมูลตัวอย่างเช่น IM AIM (ICQ) File Transfer

- การแบ่งย่อยแพ็คเก็จ (fragments) ไม่ปรกติ

- ระบบตรวจจับการบุกรุกเข้าใจว่าการใช้งานเครือข่ายภายในจากระยะไกล (remote) เป็นการบุกรุกระบบเครือข่าย

- ความล้มเหลวในการล็อกอินเข้าใช้งานระบบเครือข่ายมีความถี่สูง

3. งานวิจัยที่เกี่ยวข้อง

การแจ้งเตือนที่ผิดพลาดที่เกิดขึ้นกับระบบตรวจจับการบุกรุกบนระบบเครือข่ายนั้นได้สร้างปัญหาให้กับผู้ดูแลระบบเครือข่ายเป็นอย่างยิ่ง ได้มีผู้นำเสนอวิธีการลดการแจ้งเตือนที่ผิดพลาดที่เกิดขึ้นด้วยวิธีที่แตกต่างกันออกไปตามความเหมาะสมโดยสามารถสรุปได้ 4 วิธี ดังต่อไปนี้

3.1 การวิเคราะห์ค่าทางสถิติ (Statistics)

เป็นการกำหนดและจัดเก็บพฤติกรรมทั่วไปที่เกิดจากผู้ใช้งานและสภาพแวดล้อมภายในระบบเครือข่ายเพื่อนำมากำหนดเป็นต้นแบบในการตรวจสอบพฤติกรรมที่เข้ามาในระบบเครือข่าย การใช้ค่าทางสถิติระบบตรวจจับการบุกรุกเครือข่ายจะทำงานได้ช้า และมีขีดจำกัดในการตรวจจับการบุกรุกระบบเครือข่ายรูปแบบใหม่ NIDES (Next – generation Intrusion Detection Expert System เป็นตัวอย่างการทำงานโดยใช้ค่าทางสถิติ

3.2 การเรียนรู้พฤติกรรม

เป็นรูปแบบการทำงานโดยอัตโนมัติ ระบบจะมีการสร้างชุดข้อมูลต้นแบบ (Training data sets) เพื่อกำหนดรูปแบบพฤติกรรมปรกติในระบบเครือข่ายเพื่อใช้ตรวจสอบพฤติกรรมที่เกิดขึ้นในระบบเครือข่าย RIPPER เป็นตัวอย่างของการตรวจลดการแจ้งเตือนที่ผิดพลาดโดยใช้การเรียนรู้กฎของระบบตรวจจับการบุกรุก

3.3 ตรวจหาร่องรอยการบุกรุก

เมื่อระบบเครือข่ายถูกบุกรุกหรือมีผู้พยายามสร้างความเสียหายให้กับระบบเครือข่าย ย่อม ต้องมีร่องรอย ความเสียหายเกิดขึ้นกับระบบเครือข่าย ด้วยแนวคิดดังกล่าวการตรวจหาร่องรอยจึงเป็นการหาหลักฐานเพื่อนำมายืนยันว่าการแจ้งเตือนที่เกิดขึ้นเป็นการแจ้งเตือนที่ถูกต้อง เอเจ็น (Agent) เป็นวิธีที่ใช้กันอย่างแพร่หลายในการตรวจหาหลักฐานการบุกรุกระบบเครือข่าย

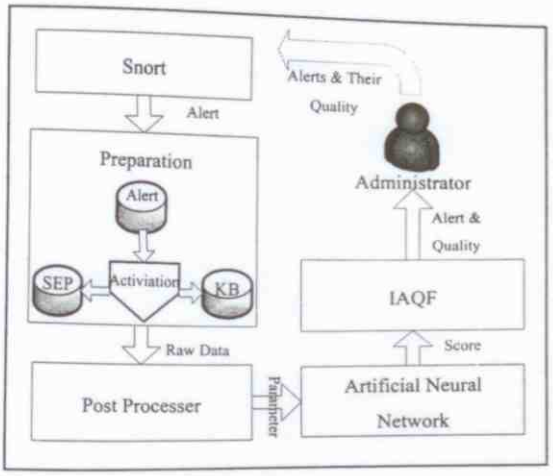
3.4 ประเมินคุณภาพให้กับการแจ้งเตือน

การแจ้งเตือนจะยังไม่ถูกส่งไปยังผู้ดูแลระบบโดยทันที แต่จะถูกนำไปสู่กระบวนการประเมินคุณภาพให้กับ การแจ้งเตือน และนำมาเปรียบเทียบกับเกณฑ์ที่กำหนดเพื่อกำหนดระดับคุณภาพการแจ้งเตือน

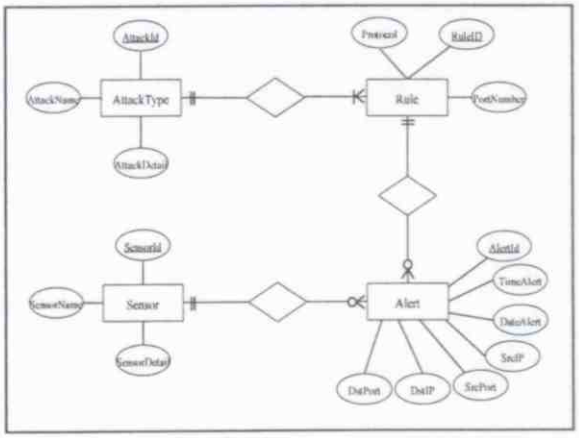
4.กลไกการประเมินคุณภาพการแจ้งเตือน

กลไกการการประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตสามารถแสดงได้ดังรูปที่ 1 ระบบจะทำการจัดเก็บข้อมูลการแจ้งเตือนที่เกิดขึ้นลงในฐานข้อมูล และในขณะเดียวกันระบบก็จะทำการเก็บข้อมูลสภาพแวดล้อมภายในระบบเครือข่ายขณะที่เกิดการแจ้งเตือน เพื่อใช้เป็นข้อมูลนำเข้าสำหรับระบบเครือข่ายใยประสาทในการประเมินคุณภาพของการแจ้งเตือนที่เกิดขึ้น

- **จัดเก็บการแจ้งเตือนที่เกิดขึ้น** ระบบได้สร้างฐานข้อมูลสำหรับจัดเก็บข้อมูลการแจ้งเตือนของโปรแกรมสนอร์ต ประกอบไปด้วย ข้อมูลของหมายเลขพอร์ตต้นทาง (SrcPort) ไอพีต้นทาง (SrcIP) หมายเลขพอร์ตปลายทาง (DstPort) ไอพีปลายทาง (DstIP) วันที่เกิดการแจ้งเตือน (DateAlert) เวลาที่เกิดการแจ้งเตือน (TimeAlert) หมายเลขเครื่องเซ็นเซอร์ที่สร้างการแจ้งเตือน (SensorID) ชนิดโปรโตคอล (Protocol) หมายเลขพอร์ต (PortNumber) และ หมายเลขกฎที่สร้างการแจ้งเตือน (RuleId) แสดงในรูปที่ 2



รูปที่ 1 *ขั้นตอนการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต*



รูปที่ 2 *ER Diagram แสดงโครงสร้างฐานข้อมูลสำหรับบันทึกข้อมูล*

- SEP (Network/System Environment Parameter) สถานะของโฮสต์และสภาพแวดล้อมของระบบเครือข่ายในขณะที่เกิดการแจ้งเตือนจะถูกจัดเก็บไปพร้อมกับการแจ้งเตือนที่เกิดขึ้น ข้อมูลดังกล่าวถูกนำมากำหนดเป็นพารามิเตอร์นำไปใช้งานในส่วนของ Artificial Neural Network เพื่อประเมินคุณภาพการแจ้งเตือนต่อไป

- KB (Knowledge Base) เป็นฐานความรู้ประกอบไปด้วยข้อมูล 2 ส่วน ส่วนแรกเป็นเงื่อนไขการกำหนดค่าพารามิเตอร์ ช่องโหว่ (Vulnerability) ของระบบปฏิบัติการ ช่องโหว่โปรโตคอล และช่องโหว่โปรแกรม (J. Haines, L. Lippman, and R. Cunninghem, 2001) ที่ใช้งานซึ่งเป็นข้อมูลที่ได้มาจาก CVE Mitre (http://www.cve.mitre.org, 2005) และ CERT (http://www.cert.org/Advisories, 2005) ส่วนที่สองเป็นข้อมูลที่เกี่ยวข้องกับโปรแกรมที่ใช้งาน เช่น หมายเลขเวอร์ชั่นล่าสุดของโปรแกรมที่ใช้งาน รูปแบบการตรวจจับการบุกรุก (Signature) ล่าสุดที่สามารถดาวน์โหลดมาใช้งาน

- Post Processor เป็นกระบวนการกำหนดค่าและปรับค่าพารามิเตอร์ให้อยู่ในรูปแบบที่กำหนดเพื่อใช้เป็นข้อมูลนำเข้าระบบเครือข่ายใยประสาท โดยตารางที่ 1 ได้แสดงเงื่อนไขในการกำหนดค่าให้กับพารามิเตอร์ที่ใช้งาน

ตารางที่ 1 *แสดงพารามิเตอร์และเงื่อนไขการกำหนดค่าพารามิเตอร์*

พารามิเตอร์	เงื่อนไขทำให้พารามิเตอร์เท่ากับ 1
Correctness	โฮสต์มีอยู่จริงบนระบบเครือข่าย
Host_OS_Vulnerability	OS ไม่ได้อัพเดท patch ล่าสุด
Host_Port_Vulnerability	พอร์ตที่ใช้งานมีช่องโหว่
Host_App_Vulnerability	โปรแกรมที่ใช้งานมีช่องโหว่
Host _Memory_Status	หน่วยความจะทำงานไม่ปรกติ
Host_CPU_Status	หน่วยประมวลผลทำงานไม่ปรกติ
Host_AV_Installation	โฮสต์ไม่ได้ติดตั้งโปรแกรมป้องกันไวรัส
Host_AV_Uptodate	รูปแบบการตรวจจับไวรัสไม่ใช่เวอร์ชั่นล่าสุด
Host_Permission_Control	ไม่มีการกำหนดสิทธิ์การใช้งาน
IDS_Rule_Reliability	ไม่มีการทดสอบกฎก่อนใช้งาน
IDS_Rule_ Sensitivity	กฎที่ใช้งานไม่ใช่เวอร์ชั่นล่าสุด
IDS_OS_Vulnerability	OS ที่ IDS ทำงานไม่ได้อัพเดท patch ล่าสุด
IDS_Version_Uptodate	โปรแกรมสนอร์ตที่ใช้งานไม่ใช่เวอร์ชั่นล่าสุด
Firewall_Availiability	ระบบเครือข่ายไม่มีไฟร์วอลล์
Firewall_OS_Vulnerability	OS ที่ ไฟร์วอลล์ ทำงานไม่ได้อัพเดท patch ล่าสุด
Firewall_Version_Uptodate	เวอร์ชั่นไฟร์วอลล์ไม่ใช่เวอร์ชั่นล่าสุด
Firewall_URL_Filtering	ไม่มีการควบคุมใช้งานอินเตอร์เน็ต
Firewall_URL_Uptodate	ฐานข้อมูลเว็บไซต์ไม่อัพเดท
Security_Policy	องค์กรไม่มีนโยบายความปลอดภัย
Username_Pattern	ไม่มีรูปแบบของชื่อผู้ใช้งาน
Password_ Complexility	ไม่มีการควบคุมการกำหนดรหัสผ่าน

Password_Expiration	รหัสผ่านไม่มีการหมดอายุ
Username_Systematic	ไม่มีระบบจัดการชื่อผู้ใช้งานและรหัสผ่าน
External_Drive_Control	ไม่มีการควบคุมอุปกรณ์ต่อพ่วง

- Artificial Neural Network (I.V.M. Lima, 2005) และ (J. Cannady, 1998) โครงสร้างของระบบเครือข่ายใยประสาทเป็นแบบ Feed-Forward ระบบเครือข่ายใยประสาทจะทำหน้าที่ในการประเมินคุณภาพให้กับการแจ้งเตือน การฝึกระบบเครือข่ายใยประสาทในบทความนี้ได้ใช้ข้อมูลการแจ้งเตือนที่เกิดขึ้นจริง จำนวน 1,000 ระเบียน (record) ข้อมูลนำเข้าจะเป็นพารามิเตอร์จำนวน 24 ตัว และผลลัพธ์จะเป็นค่าระดับคุณภาพการแจ้งเตือน คือ การแจ้งเตือนที่ถูกต้องและการแจ้งเตือนที่ผิดพลาด ในการกำหนดคุณภาพให้กับการแจ้งเตือนที่เกิดขึ้นสำหรับข้อมูลที่ใช้ฝึกระบบเครือข่ายใยประสาท ผู้วิจัยได้ใช้สมมุติฐานในการกำหนดคุณภาพการแจ้งเตือนดังต่อไปนี้

- การแจ้งเตือนที่ถูกต้องจะต้องสามารถตรวจหาร่องรอยการบุกรุกหรือความเสียหายที่เกิดขึ้นได้

- การแจ้งเตือนที่ถูกต้องจะต้องมีรูปแบบการบุกรุกระบบเครือข่ายเหมือนหรือใกล้เคียงกับรูปแบบการบุกรุกระบบเครือข่ายที่สร้างขึ้น

- การแจ้งเตือนที่ถูกต้องต้องมีคุณภาพการแจ้งเตือนมากกว่าหรือเท่ากับเกณฑ์ที่กำหนด

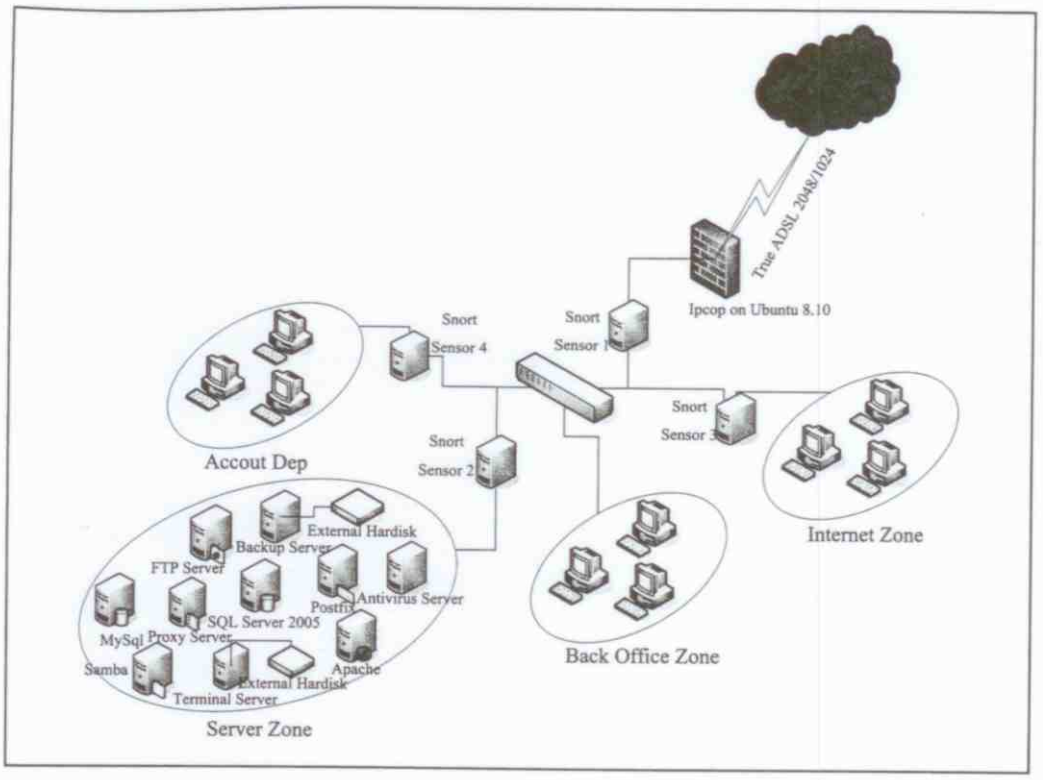
- IAQF (Intrusion Alert Quality Framework) ทำหน้าที่นำเสนอข้อมูลคุณภาพการแจ้งเตือนที่ได้จากระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตต่อผู้ดูแลระบบเครือข่าย ขั้นตอนการทำงานทั้งหมดของกลไกลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ตอาจแบ่งได้เป็นสองส่วน ส่วนแรกคือการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต ส่วนที่สองคือกระบวนการนำเสนอผลลัพธ์ที่ได้จากการทำงานต่อผู้ดูแลระบบเครือข่าย ผู้ใช้งานสามารถกำหนดสีเพื่อระบุระดับคุณภาพของการแจ้งเตือนได้ตามความเหมาะสม ดังตัวอย่างแสดงในตารางที่ 2

ตารางที่ 2 *แสดงเกณฑ์ในการกำหนดคุณภาพของการแจ้งเตือนโดยแบ่งคุณภาพการแจ้งเตือนออกเป็น 5 ระดับ*

เงื่อนไข	คุณภาพ
การแจ้งเตือนมีคะแนนเท่ากับ 0	เป็นการแจ้งเตือนที่ผิดพลาด
การแจ้งเตือนมีคะแนนอยู่ระหว่าง 0 < คะแนน < 50	มีความเป็นไปได้ที่จะเป็นการแจ้งเตือนที่ผิดพลาด
การแจ้งเตือนมีคะแนนอยู่ระหว่าง 50 =< คะแนน < 80	มีความเป็นไปได้ที่จะเป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคะแนนอยู่ระหว่าง 80 =< คะแนน < 100	เกือบจะเป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคะแนนเท่ากับ = 100	เป็นการแจ้งเตือนที่ถูกต้อง

5.ผลการทดลอง

ระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต ได้ถูกทดสอบใช้งานกับระบบเครือข่ายจริงขององค์กรแห่งหนึ่งที่มีโครงสร้างของระบบเครือข่ายในรูปที่ 3 ระบบเครือข่ายจะถูกแบ่งตามลักษณะการใช้งานออกเป็น 4 ระบบเครือข่ายย่อยอย่างชัดเจนประกอบไปด้วย เครือข่ายย่อยสำหรับแผนกบัญชี เครือข่ายย่อยสำหรับการใช้งานอินเตอร์เน็ต เครือข่ายย่อยสำหรับเครื่องแม่ข่าย (Server) และเครือข่ายย่อยสำหรับการใช้งานอินเทราเน็ต (Intranet) โดยระบบประกอบไปด้วยเครื่องแม่ข่ายจำนวน 9 เครื่องและเครื่องลูกข่าย (client) จำนวน 141 เครื่อง โดยข้อมูลของระบบและข้อมูลการแจ้งเตือนเป็นข้อมูลที่บันทึกจากข้อมูลจริงของระบบที่เริ่มบันทึกตั้งแต่วันที่ 20 เมษายน 2552 ถึง วันที่ 20 พฤษภาคม 2552 รวม เป็นระยะเวลา 1 เดือน



รูปที่ 3 *โครงสร้างระบบเครือข่ายที่ใช้ทดลองระบบลดการแจ้งเตือนที่ผิดพลาดของโปรแกรม*

ผลการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตแสดงในตารางที่ 3 สนอร์ตเซ็นเซอร์ 1 (Snort Sensor) ทำงานอยู่หลังไฟร์วอลล์ถูกตรวจพบการแจ้งเตือนที่ผิดพลาดหรือการแจ้งเตือนที่มีคุณภาพต่ำ(Low Quality) ได้ร้อยละ 36.86 สนอร์ตเซ็นเซอร์ 2 ทำงานตรวจสอบทราฟฟิคระบบเครือข่ายย่อยเครื่องแม่ข่ายถูกตรวจพบการแจ้งเตือนที่ผิดพลาดได้ร้อยละ 30.96 สนอร์ตเซ็นเซอร์ 3 ตรวจสอบทราฟฟิคระบบเครือข่ายย่อยสำหรับการใช้งานอินเตอร์เน็ตถูกตรวจพบการแจ้งเตือนที่ผิดพลาดร้อยละ 37.32 และสนอร์ตเซ็นเซอร์ 4 ทำงานตรวจสอบทราฟฟิคแผนกบัญชีถูกตรวจพบการแจ้งเตือนที่ผิดพลาดได้ร้อยละ 19.160 การทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตทั้งหมดตรวจพบการแจ้งเตือนที่ผิดพลาดได้โดยเฉลี่ยร้อยละ 32.31 เมื่อระบบได้กำหนดให้การแจ้งเตือนที่ผิดพลาดมีระดับค่าการประเมินคุณภาพต่ำกว่า 50 เมื่อนำผลการทดลองจากตารางที่ 3 มาวิเคราะห์ถึงสาเหตุการแจ้งเตือนที่ผิดพลาด ของโปรแกรมสนอร์ตที่เกิดขึ้นภายในระบบเครือข่ายสามารถจำแนกได้ตารางที่ 4 ให้ "B" แทนการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ตก่อนปรับลดกฎ "A" แทนการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ตหลังปรับลดกฎ S1, S2, S3, S4 คือ Snort Sensor 1, Snort Sensor 2, Snort Sensor 3 และ Snort Sensor 4 ตามลำดับ การกำหนดกฎที่ผิดพลาดการแจ้งเตือนจากส่วนหัวของโปรโตคอลสำหรับรับส่งเมลล์ และการแบ่งย่อยแพ็คเก็จ ไม่ปรกติ เป็นสาเหตุหลักทำให้เกิดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ตโดยพบเป็นร้อยละ 47.19, 9.07 และ 8.72 ตามลำดับ ดังนั้นหากปรับลดกฎที่ทำให้เกิดการแจ้งเตือนที่ผิดพลาดเหล่านี้ก็จะทำให้สามารถลดการแจ้งเตือนที่ผิดพลาดลงได้ร้อยละ 72.78

ตารางที่ 3 *ผลการทดลองที่ได้จากระบบลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต*

Sensor	Alert	High Quality			Low Quality		False Alarm
		Score = 100	100< score <=80	80 < score <=50	0 < score < 50	Score = 0	
Sensor 1	1476	314	211	407	114	430	36.86%
Sensor 2	1715	224	426	534	372	159	30.96%
Sensor 3	635	220	3	175	217	20	37.32%
Sensor 4	574	72	124	268	56	54	19.16%
Average							32.31%

ตารางที่ 4 *จำแนกสาเหตุของการเกิดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ตและผลการปรับผลกฎ*

ประเภท FP (False Positive)	S1		S2		S3		S4		All False Alarm		Reduction Rate
	B	A	B	A	B	A	B	A	Btotal	Atotal	
	544	114	531	140	237	86	110	47	1422	387	72.78%
1. การใช้งานฐานข้อมูลในระบบเครือข่าย	0	0	53	37	5	5	41	25	99	67	32.32%
2.ความถี่ในการสื่อสารของโปรโตคอล	19	11	46	30	12	12	8	8	85	61	28.24%
3.ค่าพารามิเตอร์ยาวเกินกำหนด	48	37	5	5	38	17	0	0	91	59	35.16%
4.แจ้งเตือนจากส่วนหัวของ Mail โปรโตคอล	61	22	43	9	25	11	0	0	129	42	67.44%
5.การแบ่งย่อยแพ็คเก็จไม่ปรกติ	60	19	47	21	11	7	7	5	125	52	58.40%
6.IDS มองว่าการรีโมทใช้งานเป็นการบุกรุก	49	14	62	23	13	9	0	0	124	46	62.90%
7. ความล้มเหลวในการล็อกอินเข้าใช้งานมีความถี่สูง	25	11	17	15	44	25	12	9	98	60	38.78%
8. การกำหนดกฎที่ผิดพลาด	282	0	258	0	89	0	42	0	671	0	0%

6. สรุปผลการทดลอง

บทความนี้ได้แสดงถึงกลไกการประมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตโดยใช้ระบบเครือข่ายใยประสาทและจัดเตรียมข้อมูลนำเสนอต่อผู้ดูแลระบบเครือข่าย ผู้ดูแลระบบเครือข่ายจะทำงานได้ง่ายขึ้นและมีประสิทธิภาพมากขึ้น การทำงานของระบบมีความยืดหยุ่นสูง ผู้ใช้งานสามารถปรับเปลี่ยนค่าพารามิเตอร์และระดับคุณภาพของการแจ้งเตือนให้เหมาะสมกับระบบเครือข่ายภายในองค์กร เมื่อนำวิธีที่นำเสนอเปรียบเทียบกับวิธีพื้นฐานโปรแกรมสนอร์ตจะสร้างการแจ้งเตือนที่ผิดพลาดลดลงร้อยละ 72.78

7. กิตติกรรมประกาศ

บทความฉบับนี้สำเร็จได้ ด้วยคำแนะนำ และคำปรึกษาจาก ผศ .มยุรี เลิศเวชกุล ข้าพเจ้ารู้สึกทราบซึ้งในความอนุเคราะห์จากท่านอาจารย์ และขอขอบพระคุณเป็นอย่างสูง

8. เอกสารอ้างอิง

B. Caswell, J. Bealeand, J. C. Foster, and J. Faircloth, "Snort 2.0 Intrusion Detection, "Syngress, Feburary 2003

"CERT/CC Advisories",http://www.cert.org/advisories/ (27 July 2005).

"Common Vulnerabilities and Exposures- The Standard for Information Security Vulnerability Names",http://www.cve.mitre.org (27 July 2005).

I.V.M. Lima, "A Simplified Accost of Intrusion Detection Based in Artificial Neural Networks", in portuguese, Master's thesis, Federal University of Sant Catarina, February, 2005

J. Cannady, "Artificial Neural Networks to Misuse Detection", First International Workshop on the Recent Advances in Intrusion Detection, 1998.

J. Haines, L. Lippman, R. Cunninghem, "Extending the DARPA Off - Line intrusion detection evaluation", Proceedings of DARPA Information Survivability Conference & Exposition II, Vol 1, 2001,pp.35-45.

K. Timm, "Strategies to Reduce False Positives and False Negatives in NIDS," SecurityFocus Article, 2001 http:H/www.securityfocus.com/ infocus/l463 (27July 2005).

M. Norton and D. Roelker, "Snort 2.0 Rule Optimizer", Sourcefire Network Security White Paper, April 2004.