นโยบายแบบพลวัตสำหรับระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์

DYNAMIC POLICY FOR
TARGET BASED INTRUSION DETECTION SYSTEM

มติ ภิญญาธินันท์

MATI PINYATHINUN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2553

KMITL-2010-IT-M-001-009

DYNAMIC PILICY FOR

TARGET BASED INTRUSION DETECTION SYSTEM

MATI PINYATHINUN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2010

KMITL-2010-IT-M-001-009

หัวข้อวิทยานิพนธ์	นโยบายแบบพลวัตสำหรับระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์
นักศึกษา	นายมติ ภิญญาธินันท์
รหัสประจำตัว	48066423
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
พ.ศ.	2552
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ. ดร. จันทร์บูรณ์ สถิตวิริยวงศ์

บทคัดย่อ

ระบบตรวจจับการบุกรุกเป็นเครื่องมือที่รักษาความมั่นคงปลอดภัยบนระบบคอมพิวเตอร์ โดยการดักจับข้อมูลที่ส่งผ่านสื่อของเครือข่าย และทำการแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น การรักษาความมั่นคงนั้นจำเป็นต้องใช้ระบบตรวจจับการบุกรุกที่มีความแม่นยำและมีประสิทธิภาพ อย่างไรก็ตามระบบดังกล่าวยังมีข้อผิดพลาดในการตรวจจับ จึงมีการพัฒนาเป็นการตรวจจับการบุกรุกที่มีเป้าหมายเป็นเกณฑ์เพื่อลดข้อจำกัดของระบบเดิม งานวิทยานิพนธ์นี้ นำเสนอแนวทางการเพิ่มการจัดการนโยบายแบบพลวัตสำหรับระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ ตามการปรับเปลี่ยนตามคุณสมบัติของเครื่องอุปกรณ์เป้าหมาย เพื่อลดภาระงานและเพิ่มประสิทธิภาพในการตรวจจับการบุกรุก

Thesis Title	Dynamic Policy for Target-based Intrusion Detection System
Student	Mr.Mati Pinyathinun
Student ID.	48066423
Degree	Master of Science
Programme	Information Technology
Year	2552
Thesis Advisor	Assoc. Prof. Dr. Chanboon Sathitwiriyawong

ABSTRACT

Network intrusion detection system (NIDS) is an important tool for network security. It observes all transmitting packets on a network system and alerts when intrusion or nearly attack situation occurs. To analyze every single packet on the network, NIDS with good performance and high accuracy can make network more secure and reliable. However, some disadvantages of NIDS, such as evasion technique and noise, can affect the accuracy of the traditional NIDS. A new approach is a target based IDS which can increase accuracy and reduce noises. This thesis proposes a new method to reduce system workload and increase the accuracy of the typical target based IDS by providing flexibility of specifying policy for individual host or group.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยความกรุณาจาก รศ. ดร. จันทร์บูรณ์ สถิตวิริยวงศ์ ซึ่งเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ข้าพเจ้ารู้สึกซาบซึ้งสำหรับโอกาส ประสบการณ์ คำชี้แนะ คำปรึกษา และความรู้ที่ได้จากอาจารย์ และขอขอบพระคุณอย่างสูง

ขอขอบพระคุณกรรมการสอบหัวข้อวิทยานิพนธ์และโครงร่างวิทยานิพนธ์ทุกท่าน ที่ได้ให้คำชี้แนะ จนทำให้วิทยานิพนธ์เล่มนี้สำเร็จได้อย่างสมบูรณ์

ขอขอบพระคุณคณาจารย์ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาให้แก่ข้าพเจ้า

ขอขอบคุณพี่ๆห้องปฏิบัติการ Network performance and security (NPS lab) สำหรับคำแนะนำความช่วยเหลือ และความหวังดีที่มีให้อยู่ตลอด

ขอขอบคุณพี่ๆเพื่อนๆ is19.1 ทุกท่านที่เป็นกำลังใจ ช่วยเหลือ และเป็นแรงกระตุ้นในการทำวิทยานิพนธ์เล่มนี้

ขอขอบคุณบุคคลอีกหลายท่านที่ข้าพเจ้าไม่ได้เอ่ยชื่อไว้ ที่ท่านได้ให้ความช่วยเหลือ และเป็นกำลังใจในทุกๆส่วนของการทำวิทยานิพนธ์เล่มนี้จนสำเร็จไปได้ด้วยดี

กราบขอบพระคุณ บิดา มารดา และครอบครัวของข้าพเจ้า สำหรับ "ทุกๆอย่าง" และทำให้ข้าพเจ้าได้ทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยดี

สำหรับคุณความดีและประโยชน์อันพึงมาจากจากวิทยานิพนธ์เล่มนี้ ข้าพเจ้าขอมอบให้แด่ผู้มีพระคุณทุกท่าน

มติ ภิญญาธินันท์

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่

หน้า

สารบัญรูป

รูปที่

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ระบบตรวจจับการบุกรุก (Intrusion Detection System – IDS) เป็นระบบรักษาความมั่นคงปลอดภัยบนเครือข่ายคอมพิวเตอร์ประเภทหนึ่งที่นิยมใช้กันทั่วไป ระบบนี้ทำหน้าที่ตรวจจับสิ่งผิดปกติที่เกิดขึ้นภายในระบบเครือข่าย โดยการดักจับข้อมูลที่สื่อสารกันอยู่บนเครือข่ายเพื่อหาข้อมูลที่ผิดปกติหรือข้อมูลที่บ่งบอกถึงการบุกรุก ที่ผ่านเข้าออกจากทั้งภายในและภายนอกเครือข่าย ระบบตรวจจับการบุกรุกสามารถส่งสัญญาณเตือนไปยังผู้ดูแลระบบ เมื่อตรวจพบสิ่งผิดปกติที่เกิดขึ้น สามารถเก็บข้อมูลการโจมตีดังกล่าวจัดเรียงในรูปแบบของล็อกไฟล์ (Log File) หรือเก็บลงในฐานข้อมูลเพื่อให้ผู้ดูแลระบบป้องกันการบุกรุกที่กำลังเกิดขึ้น หรือแก้ไขป้องกันการบุกรุกแบบเดิมไม่ให้เกิดขึ้นอีกในอนาคต นอกจากนี้ระบบตรวจจับการบุกรุกบางชนิดยังสามารถตอบโต้เพื่อป้องกันการโจมตีดังกล่าวไม่ให้เกิดขึ้น

แต่เนื่องจากในปัจจุบันความซับซ้อนของการบุกรุกและโจมตีจากผู้ประสงค์ร้าย ความซับซ้อนของตัวโพรโทคอล (Protocol) และความซับซ้อนของเครือข่ายคอมพิวเตอร์ การใช้งานปรับแต่งของเครื่องคอมพิวเตอร์ปลายทาง (Host) รวมไปถึงสถาปัตยกรรมของเครือข่ายที่มีความหลากหลาย ทำให้ระบบตรวจจับการบุกรุกไม่สามารถตรวจสอบการโจมตีดังกล่าวว่าส่งผลกับเครื่องคอมพิวเตอร์เป้าหมายหรือไม่ ผลกระทบจากการโจมตีดังกล่าวนั้น จึงส่งผลให้ระบบตรวจจับการบุกรุกไม่สามารถทำการตรวจจับข้อมูลในเครือข่ายได้อย่างมีประสิทธิภาพ

ดังนั้นจึงได้มีการคิดค้นวิธีการต่างๆ เพื่อเพิ่มความสามารถให้กับระบบตรวจจับการบุกรุกในการวิเคราะห์ ตรวจจับข้อมูล และการโจมตีที่ซับซ้อนดังกล่าวได้ หนึ่งในวิธีการนั้นคือ การพัฒนาระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ (Target based IDS) เพื่อทำการแก้ไขช่องโหว่ดังกล่าวของระบบตรวจจับการบุกรุก ระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์จะทำการวินิจฉัยข้อมูลที่ได้รับโดยใช้ข้อมูลของเครื่องคอมพิวเตอร์เป้าหมายมาช่วยในการวินิจฉัย เพื่อตรวจหาความผิดปกติหรือการโจมตีที่ส่งผลกระทบต่อเป้าหมายดังกล่าว แต่วิธีการนี้จะส่งผลกระทบต่อสมรรถนะของระบบตรวจจับการบุกรุก ในกรณีที่เครื่องคอมพิวเตอร์เป้าหมายมีสถานะหรือข้อมูลที่เปลี่ยนแปลงไปจากข้อมูลของเครื่องเป้าหมายเดิมที่กำหนดไว้ หรือการกำหนดรายละเอียดของเครื่องเป้าหมายมีมากเกินความจำเป็น ส่งผลให้ระบบตรวจจับการบุกรุกแบบนี้มีเงื่อนไขในการวินิจฉัยที่เกินความจำเป็น รวมถึงการกำหนดข้อมูลให้ระบบตรวจจับการบุกรุกที่ไม่

เป็นไปตามสถานการณ์จริง ยังเกิดช่องโหว่ในการตรวจจับเนื่องจากระบบตรวจจับการบุกรุกถูกกำหนดให้ใช้ข้อมูลที่ไม่เหมือนเครื่องเป้าหมายเมื่อเครื่องเป้าหมายมีการเปลี่ยนแปลง

ผู้วิจัยได้เล็งเห็นถึงความสำคัญของการใช้ความร่วมมือของเครื่องมือและวิธีการต่างๆ ร่วมส่งผลการวิเคราะห์ของเครื่องเป้าหมายให้กับระบบตรวจจับการบุกรุกนั้น ทำให้การตรวจจับของระบบตรวจจับการบุกรุกทำงานได้อย่างแม่นยำและยืดหยุ่นตรงตามสถานการณ์ที่เกิดขึ้น ณ ช่วงเวลานั้นได้ รวมถึงไม่ทำให้ ระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ สร้างเงื่อนไขในการวินิจฉัยที่เกินความจำเป็น

งานวิจัยนี้จึงวางแนวทาง ในการสร้างให้ระบบตรวจจับการบุกรุกสามารถเก็บข้อมูลเพิ่มและ สามารถปรับเปลี่ยนเกณฑ์ในการวิเคราะห์ข้อมูลได้ตามการเปลี่ยนแปลงของเครื่องปลายทาง จึงเป็นอีกทางออกในการลดภาระงานและเงื่อนไขในการวินิจฉัยข้อมูลได้ด้วยตัวของระบบตรวจจับการบุกรุกเอง

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาการทำงาน ประสิทธิภาพการตรวจจับการบุกรุก และสมรรถนะของระบบตรวจจับการบุกรุกทั่วไป และการวินิจฉัยข้อมูลการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์
2. เพื่อศึกษาผลกระทบและปัจจัยต่างๆ ที่ส่งผลต่อประสิทธิภาพการตรวจจับการบุกรุกและสมรรถนะของระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์
3. เพื่อนำเสนอ ระบบนโยบายแบบพลวัตสำหรับระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ รวมถึงความจำเป็นของการร่วมมือกันของอุปกรณ์หรือวิธีการต่างๆเพื่อเพิ่มประสิทธิภาพและสมรรถนะของระบบตรวจจับการบุกรุก
4. เพื่อศึกษาแนวทางการประยุกต์การนำเครื่องมืออื่นมาเพิ่มข้อมูลเครื่องเป้าหมายให้แก่ระบบตรวจจับการบุกรุก
5. เพื่อประเมินสมรรถนะของแนวคิดการนำนโยบายแบบพลวัตมาใช้ทั้งด้านสมรรถนะของการตรวจจับและความเร็วในการประมวลผลเมื่อนำระบบนโยบายแบบพลวัตมาใช้

1.3 สมมติฐานของการศึกษา

การตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ ตามแนวคิดพื้นฐานคือการนำข้อมูลจากเครื่องเป้าหมายที่อยู่ภายใต้การตรวจจับของระบบตรวจจับการบุกรุก มาใช้เป็นเกณฑ์หนึ่งในการวินิจฉัยข้อมูล การนำข้อมูลดังกล่าวรวมถึงการกำหนดการตอบสนองของเครื่องเป้าหมายโดยใช้นโยบาย ซึ่งถูกนำไปใช้ในระบบตรวจจับการบุกรุก snort นั้น เป็นการใช้ทรัพยากรและสร้าง

เงื่อนไขเพิ่มเติมให้แก่ระบบตรวจจับการบุกรุก จากแต่เดิมที่ทำการเปรียบเทียบข้อมูลกับกฎที่มีอยู่เท่านั้น การนำข้อมูลเครื่องเป้าหมายดังกล่าวมาใช้จึงมีความจำเป็นที่จะต้องคำนึงถึงการสิ้นเปลืองหรือการนำข้อมูลมาใช้เกินความจำเป็น ซึ่งก่อให้เกิดผลเสียแก่สมรรถนะของระบบตรวจจับการบุกรุกเอง

ในกรณีที่เครื่องเป้าหมายมีการเปลี่ยนแปลงลักษณะต่างๆนั้นจะส่งผลต่อระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์สองประการคือ ประการแรก การทำให้ระบบตรวจจับการบุกรุกไม่สามารถตรวจจับการบุกรุกได้ถูกต้องเนื่องจากนโยบายของระบบตรวจจับการบุกรุกไม่ตรงกับเครื่องเป้าหมายส่งผลให้การตรวจจับเกิดข้อผิดพลาด และประการที่สอง การกำหนดนโยบายที่อาจจะเกินความจำเป็น ส่งผลต่อสมรรถนะ และความเร็วในการประมวลผลของระบบตรวจจับการบุกรุก

การสร้างนโยบายที่ปรับเปลี่ยนได้ ตามเครื่องเป้าหมายทำให้ระบบตรวจจับการบุกรุกทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยการใช้ข้อมูลเพิ่มเติมให้กับระบบตรวจจับการบุกรุก ที่ปกติขาดหายเนื่องจากการเปลี่ยนแปลงคุณลักษณะของเครื่องเป้าหมาย ทั้งภายใต้สภาวะที่ระบบต้องทำงานหนัก และภายใต้สภาวะที่ทรัพยากรระบบมีอย่างเพียงพอ ซึ่งในกรณีนี้ระบบตรวจจับการบุกรุกจะลดเงื่อนไขที่เกินความจำเป็นจึงส่งผลต่อความเร็วในการประมวลผลของระบบตรวจจับการบุกรุก

สมมติฐานของงานวิจัยนี้คือ การใช้ข้อมูลของเครื่องเป้าหมายที่เกินความจำเป็นส่งผลกระทบต่อระบบตรวจจับการบุกรุก และการลดข้อมูลที่เกินความจำเป็นนั้นสามารถช่วยลดความสิ้นเปลืองทรัพยากรที่ระบบตรวจจับการบุกรุกจะนำมาใช้

1.4 ขอบเขตการวิจัย

งานวิทยานิพนธ์ฉบับนี้ ศึกษาสมรรถนะและความเร็วในการประมวลผลของระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ และศึกษาข้อมูลของเครื่องเป้าหมายที่สามารถหาเพิ่มเติมได้จากเครื่องมือหรือวิธีการอื่นๆให้กับระบบเดิม เพื่อเพิ่มประสิทธิภาพและสมรรถนะของระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ โดยผู้วิจัยมีวัตถุประสงค์เพื่อสร้างระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ ที่มีความสามารถในการปรับเปลี่ยนนโยบายตามสถานการณ์ที่เกิดขึ้นจริงโดยใช้ข้อมูลจากอุปกรณ์อื่นเป็นเกณฑ์ปรับแต่งนโยบาย ในการวิจัยจะทำการประเมินผลกระทบที่มีต่ออัตราการละทิ้งแพ็กเก็ต (Packet) และผลกระทบต่อความเร็วในการประมวลผลของระบบตรวจจับการบุกรุก เพื่อเป็นแนวทางในการพัฒนาระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์โดยที่ไม่ต้องผ่านการกลั่นกรองสัญญาณเตือน เนื่องจากงานวิจัยนี้มุ่งเน้นให้ระบบตรวจจับการบุกรุกสามารถแก้ไขสถานการณ์ดังกล่าวได้ด้วยตัวของระบบเอง

1.5 ขั้นตอนการศึกษา

วิทยานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บท คือ

บทที่ 1 กล่าวถึงความเป็นมาของงานวิจัย ความมุ่งหมายและวัตถุประสงค์ สมมติฐาน ขอบเขตของการวิจัย และขั้นตอนการศึกษา

บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานที่ใช้ในการวิจัย ประเภทและการทำงานโดยทั่วไปของระบบตรวจจับการบุกรุก ปัญหาที่เกิดขึ้นที่นำไปสู่การพัฒนาระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ วิธีการทำงานของระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ในรูปแบต่างๆ และปัจจัยที่ส่งผลกระทบต่อระบบ รวมถึงข้อมูลที่สามารถเก็บรวบรวมเพิ่มเติมเพื่อสร้างความร่วมมือระหว่างอุปกรณ์

บทที่ 3 นำเสนอแนวทางการพัฒนาปรับปรุงสมรรถนะการทำงานของระบบตรวจจับการบุกรุกที่มีเป้าหมายเป็นเกณฑ์ โดยการใช้นโยบายแบบพลวัต

บทที่ 4 ผลการทดลองและการวิเคราะห์ผลการทดลอง

บทที่ 5 บทสรุปของงานวิจัยและข้อเสนอแนะ

บทที่ 2
ทฤษฎีพื้นฐานที่ใช้ในการวิจัย

ในบทนี้จะกล่าวถึงระบบตรวจจับการบุกรุก การตรวจจับในรูปแบบต่างๆ การตอบสนองของระบบตรวจจับการบุกรุก การแสวงหาผลประโยชน์จากช่องโหว่ของระบบตรวจจับการบุกรุก ระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ รวมถึงระบบตรวจจับการบุกรุก snort และซอฟต์แวร์ nmap ซึ่งผู้วิจัยได้นำมาพัฒนาต่อในงานวิจัยนี้

2.1 ระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุก ทำหน้าที่ตรวจจับพฤติกรรมการใช้งานและข้อมูลภายในเครือข่าย โดยการดักจับข้อมูลจากเครือข่ายเพื่อนำมาวิเคราะห์เพื่อหาพฤติกรรมที่เข้าข่ายว่าเป็นการบุกรุก จากนั้นทำการเตือนให้แก่ผู้ดูแลระบบรวมถึงบันทึกข้อมูลดังกล่าวเพื่อเป็นข้อมูลในการป้องกันการโจมตีในครั้งต่อไป

ระบบตรวจจับการบุกรุกสามารถแบ่งตามประเภทของตำแหน่งที่ใช้งานได้ดังนี้

1. Host based IDS คือ ระบบตรวจจับการบุกรุกที่ตรวจจับข้อมูลที่ใช้บนเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง ว่ามีพฤติกรรมที่ผิดปกติ หรือมีการบุกรุกบนเครื่องนั้นหรือไม่
2. Network based IDS คือ ระบบตรวจจับการบุกรุกที่ตรวจจับข้อมูลบนระบบเครือข่าย โดยการดักจับแพ็กเก็ตและนำมาวิเคราะห์ว่าเป็นพฤติกรรมที่ผิดปกติหรือเป็นการบุกรุกหรือไม่

และ ระบบตรวจจับการบุกรุกสามารถแบ่งได้ตามลักษณะการทำงานได้เป็น 2 ประเภทคือ

1. Anomaly detection based คือ ระบบตรวจจับการบุกรุกที่วินิจฉัยข้อมูลที่รับโดยการเปรียบเทียบกับพฤติกรรมที่เป็นปกติ ดังนั้นถ้าข้อมูลที่ระบบตรวจจับการบุกรุกประเภทนี้ได้รับ มีเกณฑ์ความน่าจะเป็นการบุกรุกมากกว่าข้อมูลของพฤติกรรมที่เป็นปกติ ระบบตรวจจับการบุกรุกจะถือว่าข้อมูลที่มีพฤติกรรมดังกล่าวเป็นการบุกรุก
2. Signature detection based คือ ระบบตรวจจับการบุกรุกที่นำข้อมูลที่ได้รับมาเปรียบเทียบกับกฎที่ถูกกำหนดไว้ เพื่อเปรียบเทียบว่าข้อมูลนั้นตรงกับข้อมูลที่มีอยู่ว่าเป็นการบุกรุกหรือไม่

การตอบโต้ของระบบตรวจจับการบุกรุกสามารถแบ่งได้เป็น 2 ประเภทคือ

1. Passive System คือ ระบบตรวจจับการบุกรุกทั่วไปที่ตอบโต้กับการบุกรุกโดยการแจ้งเตือนในรูปแบบต่างๆ ไปยังผู้ใช้หรือผู้ดูแลระบบ
2. Reactive System คือ ระบบป้องกันการบุกรุก (Intrusion Prevention System - IPS) เป็นระบบตรวจจับการบุกรุกที่พัฒนาขึ้นจากระบบตรวจจับการบุกรุกเดิม โดยการเพิ่มความสามารถในการส่งการตอบสนองเพื่อป้องกันการบุกรุกเมื่อมีการตรวจพบ เช่น การส่งสัญญาณไปยังไฟร์วอลล์ เพื่อปิดช่องทางในการสื่อสาร เมื่อพบว่าการสื่อสารนั้นตรวจพบสิ่งผิดปกติเพื่อทำการตอบโต้การบุกรุกดังกล่าว

2.2 การตอบสนองของระบบตรวจจับการบุกรุก

เมื่อระบบตรวจจับการบุกรุกกำลังทำงาน สถานะที่ระบบตรวจจับการบุกรุกตอบสนองตามรูปแบบของพฤติกรรมที่ได้รับ สามารถแบ่งได้ดังนี้

1. True Positive คือ สถานการณ์ที่ไม่มีการบุกรุกเกิดขึ้นในระบบจริง และ ระบบตรวจจับการบุกรุกไม่ทำการแจ้งเตือน
2. True Negative คือ สถานการณ์ที่มีการบุกรุกเกิดขึ้นในระบบจริง และระบบตรวจจับการบุกรุกสามารถแจ้งเตือนได้อย่างถูกต้อง
3. False Positive คือ สถานการณ์ที่ไม่มีการบุกรุกเกิดขึ้นในระบบจริง และระบบตรวจจับการบุกรุกส่งสัญญาณเตือน
4. False Negative คือ สถานการณ์ที่มีการบุกรุกเกิดขึ้นในระบบจริง และ ระบบตรวจจับการบุกรุกไม่ทำการแจ้งเตือน

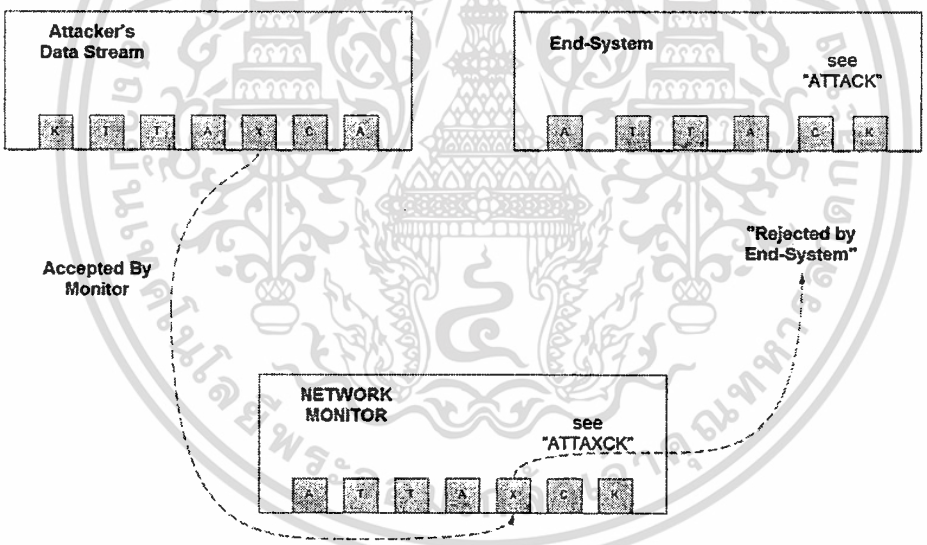
นอกจากสถานะดังกล่าวแล้ว ได้มีการพบสถานะใหม่ที่เรียกว่า Noise ซึ่งเป็นประเด็นที่ได้รับความสนใจ Noise คือ สถานการณ์ที่เกิดการโจมตีขึ้นจริงในระบบเครือข่าย แต่ว่าไม่สามารถนำไปสร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์เป้าหมายได้ ตัวอย่างเช่น เมื่อผู้บุกรุกส่งข้อมูลที่เป็น RPC DCOM Exploit ซึ่งเป็นการบุกรุกที่ใช้ช่องโหว่ของระบบปฏิบัติการ Windows แต่ว่าเครื่องเป้าหมายที่ผู้บุกรุกส่งการโจมตีไปไม่ได้เป็นเครื่องที่ติดตั้งระบบปฏิบัติการ Windows เอาไว้ ข้อมูลดังกล่าวที่ผู้บุกรุกส่งเข้ามาจะถูกระบบตรวจจับการบุกรุกดักจับ วิเคราะห์ว่าเป็นการบุกรุก จากนั้นแจ้งเตือนให้กับผู้ดูแลระบบ ผลของการกระทำของระบบตรวจจับการบุกรุกคือ True Negative แต่ว่าในแง่ของผู้ดูแลระบบจะเปรียบเสมือนว่าเป็น False Negative เนื่องจาก มีการแจ้งเตือน แต่ว่าการบุกรุกดังกล่าว ไม่ส่งผลกระทบใดๆต่อเครื่องที่เป็นเป้าหมาย

2.3 การแสวงหาผลประโยชน์จากช่องโหว่ของระบบตรวจจับการบุกรุก

จากที่ได้กล่าวไว้ว่า ความซับซ้อนของระบบเครือข่าย เช่น Packet fragmentation, reassembly retransmission เป็นช่องโหว่ประการหนึ่งสำหรับระบบตรวจจับการบุกรุกในอดีต รวมไปถึงระบบตรวจจับการบุกรุกในอดีตไม่มีการใช้คุณสมบัติของเครื่องเป้าหมายเป็นเกณฑ์ในการวิเคราะห์ ส่งผลให้ผู้บุกรุกสร้างการบุกรุกที่สามารถหลบหลีกการตรวจจับของระบบตรวจจับการบุกรุกได้ นั้น

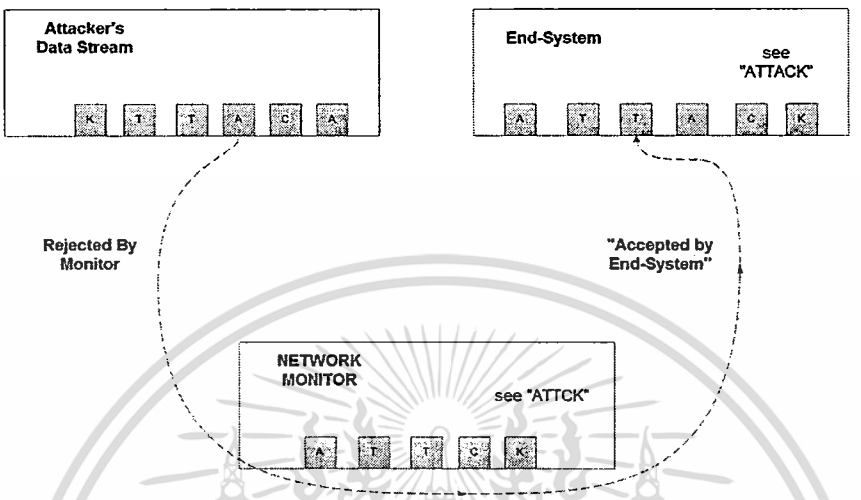
Thomas Ptacek และ Timothy Newsham [3] ได้แสดงให้เห็นถึงการหลบหลีกการตรวจจับ ซึ่งแบ่งได้เป็น 2 วิธีคือ

1. Insertion คือ การแทรกข้อมูลที่ระบบตรวจจับการบุกรุกไม่สามารถตรวจสอบได้ ลงไปในชุดข้อมูลที่เป็นการโจมตีและส่งให้เครื่องปลายทาง ระบบตรวจจับการบุกรุกจะไม่สามารถวินิจฉัยว่าข้อมูลนั้นเป็นการบุกรุกเนื่องจากมีการแทรกข้อมูลไว้ แต่ข้อมูลที่แทรกดังกล่าวจะถูกทิ้งไป เมื่อไปถึงเครื่องปลายทางทำให้ข้อมูลทั้งชุดสามารถทำการโจมตีเครื่องเป้าหมายได้ ดังแสดงในรูปที่ 2.1



รูปที่ 2.1 ภาพอธิบายเทคนิค Insertion

2. Evasion คล้ายกับการทำ Insertion แต่ในทางกลับกัน สร้างข้อมูลที่ IDS ไม่สามารถตรวจพบได้ แต่เครื่องเป้าหมายสามารถนำไปใช้ได้ เมื่อข้อมูลทั้งชุดสามารถทำการโจมตีเครื่องเป้าหมายได้เมื่อชุดข้อมูลไปถึงเครื่องเป้า ดังแสดงในรูปที่ 2.2



รูปที่ 2.2 ภาพอธิบายเทคนิค Evasion

นอกจากนี้ยังมีการใช้การปฏิเสธการให้บริการ (Denial of service) ซึ่งเป็นการโจมตีไปโดยตรงที่ระบบตรวจจับการบุกรุก เพื่อไม่ให้ระบบตรวจจับการบุกรุกสามารถตรวจสอบข้อมูลได้อย่างเต็มสมรรถนะ เนื่องจากการโจมตีแบบนี้จะทำให้ทรัพยากรของระบบตรวจจับการบุกรุกมีไม่เพียงพอที่จะทำการตรวจจับการบุกรุกได้อย่างมีประสิทธิภาพ ทำให้ระบบตรวจจับการบุกรุกทิ้งแพ็กเก็ต แพ็กเก็ตที่ถูกทิ้งจะไม่ถูกตรวจสอบโดยระบบตรวจจับการบุกรุก ซึ่งอาจทำให้ระบบตรวจจับการบุกรุกไม่สามารถตรวจจับการโจมตีได้

2.4 ระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์

จากปัญหาดังกล่าวได้มีการวิเคราะห์ถึงปัจจัยที่ส่งผลให้เกิดปัญหา โดยมีข้อสรุปว่าช่องโหว่นั้นเกิดจากการขาดแคลนข้อมูลที่สำคัญในเครือข่าย ซึ่งส่งผลให้ระบบตรวจจับการบุกรุกเกิดช่องโหว่ดังกล่าวรวมถึงการเกิด Noise ดังนั้นจึงได้มีการพัฒนาระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ขึ้นมา โดยมีหลักการพื้นฐานคือ สร้างมุมมองของระบบตรวจจับการบุกรุก ให้เป็นมุมมองเดียวกับเครื่องเป้าหมายโดยการลดช่องว่างของความผิดพลาดที่เกิดขึ้น เช่น ลดการเกิด noise

แนวคิดในการสร้างระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ สามารถแบ่งได้เป็น

- การกำหนดข้อมูลของเครื่องเป้าหมายให้กับระบบตรวจจับการบุกรุก เพื่อให้ระบบตรวจจับการบุกรุกใช้เกณฑ์การวิเคราะห์ข้อมูลเดียวกับเครื่องเป้าหมาย และลดการหลบหลีกที่เกิดขึ้น เนื่องจากระบบตรวจจับการบุกรุกสามารถทำการ stream reassembly แบบเดียวกับเครื่องเป้าหมาย และการทำ state tracking เพื่อติดตามสถานะของการเชื่อมต่อไปยังเครื่องเป้าหมายได้
- Alert Profiling คือ การใช้ข้อมูลเครื่องเป้าหมายหรือข้อมูลอื่นๆจากเครือข่ายนำมาจำแนกประเภทของสัญญาณเตือนที่ไม่จำเป็น ออกจากฐานข้อมูลของสัญญาณเตือน
- การจัดลำดับความสำคัญของสัญญาณเตือน คือ การใช้ข้อมูลของเครื่องเป้าหมายเป็นเกณฑ์ในการเลือกที่จะเตือนสัญญาณเตือนที่จะเกิดขึ้น โดยสัญญาณเตือนที่จะไปสู่ผู้ดูแลระบบนั้น จะมีการแสดงค่าความสำคัญของสัญญาณเตือนของแต่ละสัญญาณเตือน

2.5 ระบบตรวจจับการบุกรุก snort

snort ถูกพัฒนาขึ้นโดย Martin Roesch โดยแรกเริ่มจากการสร้างซอฟต์แวร์เพื่อทำการดักจับแพ็กเก็ต จากนั้นได้มีการเพิ่มเติมโดยการสร้างการเปรียบเทียบกับกฎ เป็นระบบตรวจจับการบุกรุกที่นิยมใช้กันอย่างแพร่หลาย เนื่องจากเป็นซอฟต์แวร์ open source และมีการปรับปรุงกฎในการตรวจจับการบุกรุกอย่างสม่ำเสมอ โดยมีคุณสมบัติเป็นระบบตรวจจับการบุกรุกแบบ Network Signature based

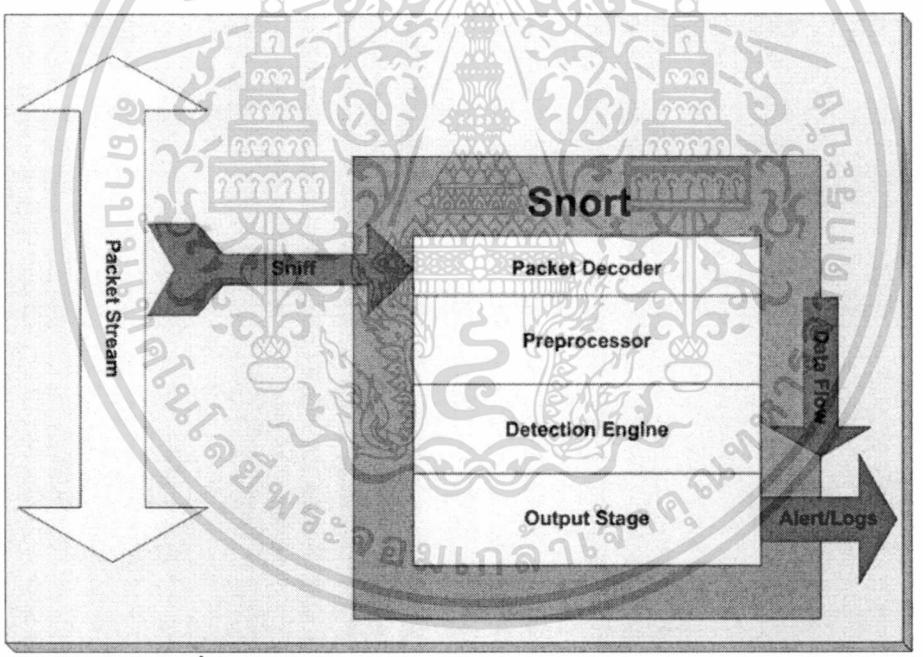
โครงสร้างการทำงานของระบบตรวจจับการบุกรุก snort แบ่งได้ดังนี้

- Packet Decoder ทำหน้าที่ในการแปลง ถอดรหัสของแพ็กเก็ตที่ได้รับจากการดักจับเพื่อเป็นข้อมูลให้กับระบบตรวจจับการบุกรุกนำไปตีความหมายเพื่อวิเคราะห์ข้อมูลได้
- Preprocessor ทำหน้าที่ในเป็นสื่อกลางให้ผู้ใช้หรือผู้ดูแลระบบสามารถกำหนดค่าคุณสมบัติต่างๆที่จำเป็น เพื่อเป็นข้อกำหนดสำหรับระบบตรวจจับการบุกรุก และสามารถปรับแต่งตามความเหมาะสมกับระบบเครือข่ายที่จะทำการตรวจจับโดยระบบตรวจจับการบุกรุก
- Detection Engine ทำหน้าที่ในการตรวจจับค้นหาความผิดปกติที่เกิดขึ้น ซึ่งยึดตามข้อกำหนดและการปรับแต่งใน preprocessor และนำข้อมูลแพ็กเก็ตที่ถูกแปลจาก

ตัวถอดรหัสแพ็กเก็ต มาเปรียบเทียบกับกฎที่มีอยู่เพื่อหาความผิดปกติที่จะเกิดขึ้น โดยใช้ pattern matching algorithm

- Output Stage เป็นขั้นตอนการแสดงผลของซอฟต์แวร์ snort โดยออกมาในรูปแบบของการเตือน เมื่อมีการพบสิ่งที่ไม่ปกติจากการตรวจสอบของอุปกรณ์ตรวจจับ ซึ่งสามารถแสดงออกมาได้หลายรูปแบบ ตัวอย่างเช่น แสดงสัญญาณเตือนออกที่หน้าจอ แสดงสัญญาณเตือนออกมาในรูปแบบล็อกไฟล์ หรือส่งสัญญาณเตือนเข้าไปเก็บในฐานข้อมูล

ในระบบตรวจจับการบุกรุก snort รุ่น 2.8.0 เป็นต้นไป ได้มีการติดตั้ง preprocessor ตัวใหม่ที่เรียกว่า Stream5 ซึ่งพัฒนาขึ้นตามหลักการของการใช้เป้าหมายเป็นเกณฑ์ โดย snort ใช้การกำหนดนโยบาย (policy) เพื่อระบุถึงคุณสมบัติและรายละเอียดของเครื่องปลายทาง เพื่อสร้างการจำลองมุมมองในการตรวจจับ ให้ตอบสนองกับคุณสมบัติต่างๆของเครื่องปลายทาง ตามแนวคิดการพัฒนาระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ ดังแสดงในรูปที่ 2.3



รูปที่ 2.3 การทำงานของระบบตรวจจับการบุกรุก snort

2.6 การค้นหาเครื่องเป้าหมายและซอฟต์แวร์ nmap

การค้นหาเครื่องเป้าหมาย (Host Discovery) คือ การส่งแพ็กเก็ตต่างๆเข้าไปในเครือข่ายเพื่อค้นหาการมีตัวตนอยู่ของเครื่องเป้าหมาย หรือค้นหาข้อมูลอย่างละเอียดของเครื่องเป้าหมาย เพื่อเป็นข้อมูลสำหรับผู้ดูแลระบบ หรืออาจจะเป็นการเริ่มต้นเพื่อทำการโจมตีของผู้ไม่หวังดี

วิธีการค้นหาเครื่องเป้าหมายและการเก็บเกี่ยวข้อมูลของเครื่องปลายทางนั้นสามารถทำได้หลายวิธี โดยการใช้รูปแบบของแพ็กเก็ตที่ส่งออกไปแตกต่างกัน

nmap (Network mapper) เป็นซอฟต์แวร์ open source ที่มีความสามารถในการสำรวจเครื่องคอมพิวเตอร์ภายในเครือข่าย สามารถค้นหาเครื่องคอมพิวเตอร์ที่เปิดใช้งาน รวมไปถึงคุณสมบัติต่างๆ เช่น พอร์ต และ ระบบปฏิบัติการที่ใช้อยู่ จากงานวิจัย [11], [12] พบว่าความแม่นยำในการค้นหาข้อมูลและคุณสมบัติมีความน่าเชื่อถือสูง และสามารถนำผลการค้นหาออกมาในรูปแบบของไฟล์ที่หลากหลายสามารถนำไปใช้ประโยชน์ในด้านต่างๆได้

จากงานวิจัย [11],[12] แสดงให้เห็นว่าการใช้ค่าโดยปริยายของซอฟต์แวร์ Nmap สามารถปรับลดเพื่อป้องกันการตรวจจับของระบบการตรวจจับการบุกรุกได้

ค่าโดยปริยายในการค้นหาข้อมูลเครื่องเป้าหมายของซอฟต์แวร์ Nmap ทำโดยการส่งแพ็กเก็ตจำนวน 16 รูปแบบ ดังต่อไปนี้

- 6 TCP SYN แพ็กเก็ต ไปยังพอร์ตที่เปิดอยู่บนเครื่องเป้าหมาย
- 3 TCP ที่มี flag ต่างๆไปยังพอร์ตที่เปิดอยู่
- 3 TCP ที่มี flag ต่างๆไปยังพอร์ตที่ปิดอยู่
- 1 TCP ที่มีการตั้งค่า explicit congestion notification control flags ไปยังพอร์ตที่เปิดอยู่
- 2 ICMP Echo แพ็กเก็ต
- 1 UDP แพ็กเก็ต

บทที่ 3
ระบบนโยบายแบบพลวัต
สำหรับระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์

จากทฤษฎีและปัญหาที่กล่าวมา วิทยานิพนธ์นี้นำเสนอวิธีการเพิ่มสมรรถนะและความเร็วในการประมวลผลของระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ จากการที่ผู้วิจัยได้ศึกษาวัตถุประสงค์ในการพัฒนาระบบตรวจจับการบุกรุกแบบเดิม มาเป็นระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์พบว่า เป้าหมายของการพัฒนาคือ สร้างความถูกต้องของการวินิจฉัยพฤติกรรมต่างๆ โดยยึดหลักการนำข้อมูลของเครื่องเป้าหมายและเครือข่ายมาช่วยในการวิเคราะห์เพื่อให้การวิเคราะห์และแสดงผลของระบบตรวจจับการบุกรุกมีความแม่นยำถูกต้องมากยิ่งขึ้น ซึ่งระบบที่มีอยู่เดิมของระบบตรวจจับการบุกรุก snort ยังสามารถปรับปรุงเพิ่มได้ การเพิ่มเติมดังกล่าวที่จะนำเสนอในงานวิจัยนี้คือการสร้างความร่วมมือกับเครื่องมืออื่น เพื่อเพิ่มข้อมูลเครื่องเป้าหมายให้กับระบบตรวจจับการบุกรุก และสร้างนโยบายที่มีความสามารถในการปรับเปลี่ยนได้ตามสถานะของเครื่องเป้าหมายให้กับระบบตรวจจับการบุกรุก เพื่อสร้างระบบตรวจจับการบุกรุกที่มีความสามารถในการหาข้อมูลของเครื่องเป้าหมายได้ด้วยตัวของระบบเอง

3.1 แนวคิดในงานวิจัย

จากการที่ผู้วิจัยได้ศึกษาการทำงานของระบบตรวจจับการบุกรุก snort ที่ทำงานโดยใช้หลักการของการใช้เป้าหมายเป็นเกณฑ์แล้ว งานวิจัยนี้ใช้สมมติฐานเริ่มต้นจาก เมื่อมีนโยบายหรือคุณสมบัติของเครื่องเป้าหมายในนโยบายที่เกินความจำเป็น จะทำให้เกิดการใช้ทรัพยากรและการสร้างเงื่อนไขที่ไม่จำเป็นบนระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ การที่เงื่อนไขดังกล่าวจะเกิดขึ้นก็ต่อเมื่อ เครื่องเป้าหมายที่ระบบตรวจจับการบุกรุกทำการตรวจจับอยู่ มีการเปลี่ยนแปลงค่าต่างๆไป จากที่ระบบตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ได้ถูกกำหนดไว้

การทำงานของระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ บนระบบตรวจจับการบุกรุก snort เป็นการใช้ preprocessor ที่เรียกว่า stream5 ซึ่งมีหน้าที่วิเคราะห์การตอบสนองของเป้าหมายกับข้อมูลที่จะได้รับ ข้อมูลของเป้าหมายนั้นถูกกำหนดไว้ในรูปแบบของนโยบาย

นโยบายในระบบตรวจจับการบุกรุก snort คือ การกำหนดรูปแบบการตรวจสอบให้แก่ระบบตรวจจับการบุกรุก โดยกำหนดจากหมายเลขไอพีของเครื่องเป้าหมายหรือหมายเลขไอพี ของเครือข่ายเข้ากับระบบปฏิบัติการที่ใช้อยู่ ภายในประกอบด้วยรายละเอียดเพื่อประกอบการวินิจฉัยต่างๆ เช่น หมายเลขพอร์ต เป็นต้น ซึ่งมีรูปแบบที่เป็นการกำหนดตายตัวดังตัวอย่างในรูปที่ 3.1

```
preprocessor stream5_global: track_tcp yes
preprocessor stream5_tcp: bind_to 192.168.1.0/24, policy windows
preprocessor stream5_tcp: bind_to 10.1.1.0/24, policy linux
preprocessor stream5_tcp: policy solaris
```

รูปที่ 3.1 ตัวอย่างนโยบายที่กำหนดไว้ใน Preprocessor Stream5

โดยหลักการแล้วหลังจากที่แพ็กเก็ตถูกดักจับและนำไปวิเคราะห์ใน preprocessor stream5 preprocessor จะใช้ข้อมูลของเครื่องเป้าหมายเพื่อทำการวิเคราะห์ผล ทำการจัดเรียงข้อมูลใหม่ และติดตามสถานะตามนโยบายที่กำหนด เพื่อวินิจฉัยข้อมูลที่ได้รับและการตอบสนองของเครื่องเป้าหมายต่อข้อมูลดังกล่าวได้อย่างถูกต้อง

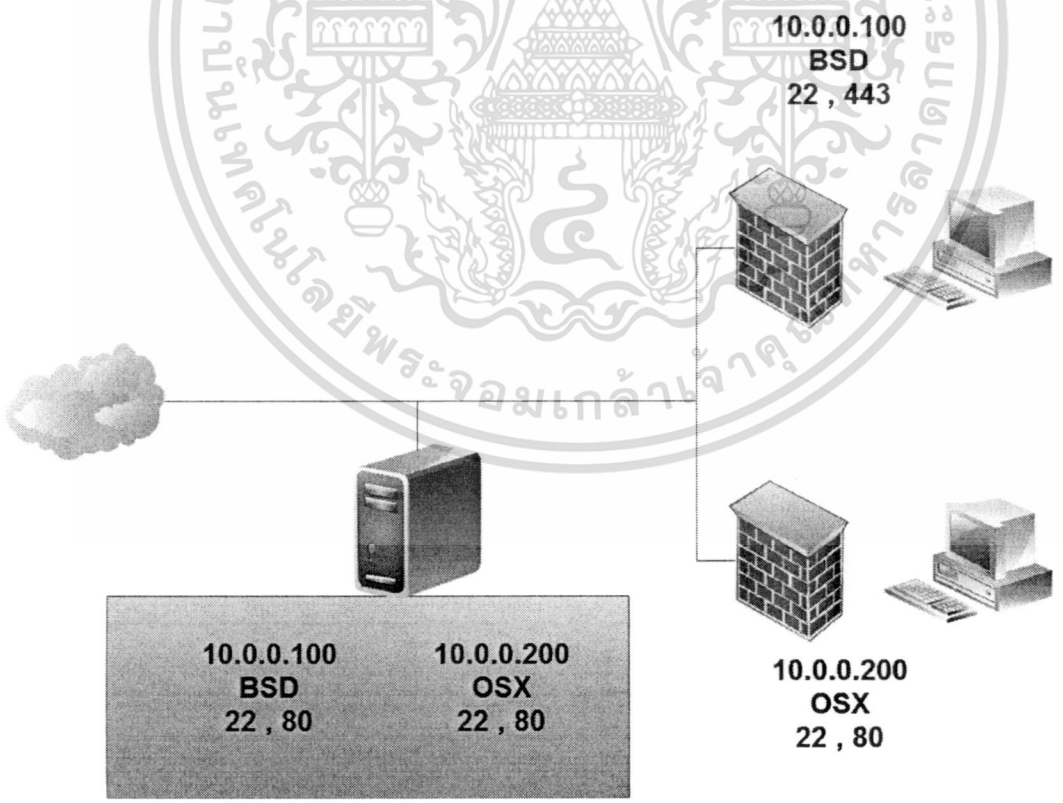
โดยคุณสมบัติต่างของเครื่องเป้าหมายที่ถูกกำหนดไว้ในนโยบาย snort ได้แก่

- *bind_to <ip address>* คือ การกำหนดหมายเลขไอพีของเครื่องเป้าหมายหรือเครือข่ายให้แก่นโยบายดังกล่าว
- *timeout <num seconds>* คือ การกำหนด timeout ให้แก่ session ของการสื่อสารที่เกิดขึ้น
- *policy <policy_id>* คือ การกำหนดประเภทของระบบปฏิบัติการของเครื่องเป้าหมายหรือเครือข่ายให้กับนโยบาย
- *min_ttl <number>* คือ การกำหนดค่าต่ำสุดของ Time to live (TTL)
- *overlap_limit <number>* คือ การจำกัดปริมาณของการทับซ้อนกันของแพ็กเก็ตในแต่ละ session
- *max_windows <number>* คือ การกำหนดค่าสูงสุดที่เป็นไปได้ของ TCP window
- *require_3whs [<number seconds>]* คือ การติดตามการทำ SYN/SYN ACK/ACK handshake
- *detect_anomalies* คือ การตรวจสอบและส่งสัญญาณเตือนเมื่อพบการใช้โพรโทคอล TCP ที่ผิดปกติ
- *check_session_hijacking* คือ การตรวจหา TCP session hijacking โดยการตรวจสอบค่า MAC address จากทั้งสองฝั่ง
- *use_static_footprint_sizes* คือ ข้อกำหนดของ stream4 (แบบเก่า)การกำหนดให้ทำ reassemble แพ็กเก็ต

- *dont_store_large_packets* คือ การเพิ่มสมรรถนะโดยการไม่เก็บคิว (queue) ให้กับแพ็กเก็ตขนาดใหญ่เพื่อทำการ reassembly
- *port <client|server|both> <all|numbers>* คือ การกำหนดให้มีการตรวจสอบพอร์ตสำหรับเครื่องต้นทางและปลายทาง

อย่างไรก็ตาม ในสภาวะที่เครื่องคอมพิวเตอร์ภายในเครือข่ายเกิดการเปลี่ยนแปลง นโยบายที่ไม่ตรงกับความเป็นจริงจะทำให้การตรวจจับการบุกรุกเกิดความผิดพลาด ซึ่งส่งผลต่อประสิทธิภาพการตรวจจับ เช่น เมื่อมีการเชื่อมต่อเครือข่ายจากเครื่องคอมพิวเตอร์ที่ติดตั้งระบบปฏิบัติการที่ไม่เหมือนกับที่กำหนดให้นโยบาย หรือ ไม่มีระบบปฏิบัติการนั้นถูกกำหนดอยู่ใน preprocessor Stream5 หรือ การเปลี่ยนรูปแบบการใช้งานที่จำเป็นต้องเปิดพอร์ตเพิ่มจากที่นโยบายใน preprocessor Stream5 กำหนดไว้ หรือ มีเครื่องเป้าหมายนอกเหนือจากที่กำหนดไว้ ในนโยบายหรือไม่ได้ถูกกำหนดไว้ให้กับนโยบายใดๆเลย เข้ามาในระบบเครือข่าย

ตัวอย่างดังรูปที่ 3.2 คือตัวอย่างของการกำหนดนโยบายที่ตายตัวบนระบบตรวจจับการบุกรุก เมื่อมีการเปลี่ยนคุณสมบัติบางอย่าง ในรูปที่ 3.2 แสดงให้เห็นว่า เครื่องเป้าหมาย 10.0.0.100 ได้มีการเปลี่ยนคุณสมบัติจากที่เปิดพอร์ต 80 เปลี่ยนเป็นเปิดพอร์ต 443 แต่ว่านโยบายบนระบบตรวจจับการบุกรุกไม่ได้เปลี่ยนตามหมายเลขพอร์ตที่ถูกเปิดขึ้นมาใหม่



รูปที่ 3.2 ความแตกต่างระหว่างนโยบายและข้อมูลเครื่องเป้าหมาย

ความสามารถในการเปลี่ยนแปลงข้อมูลของเครื่องเป้าหมายที่ได้กล่าวนี้ ถูกนำเสนอไว้โดย Ranum [4] ได้กล่าวถึงการหลีกเลี่ยง Noise และ False positive โดยการสร้างการเปลี่ยนแปลงข้อมูลของเครื่องเป้าหมายในการตรวจจับให้แก่ระบบตรวจจับการบุกรุก และงานวิจัย [3] ได้เสนอกรณีของระบบตรวจจับการบุกรุกที่สร้าง Noise และ False positive ซึ่งส่งผลต่อสมรรถนะโดยรวม กล่าวคือ เมื่อระบบตรวจจับการบุกรุกสร้าง False positive ซึ่งเป็นการแจ้งเตือนที่ไม่มีความจำเป็น การแจ้งเตือนดังกล่าวจะถูกจัดเก็บในลักษณะของล็อกไฟล์และฐานข้อมูล ในกรณีที่ระบบตรวจจับการบุกรุกยังคงสร้าง False positive หรือ Noise อย่างต่อเนื่องจะส่งผลให้คอมพิวเตอร์ใช้ทรัพยากรในการจัดเก็บสัญญาณเตือน รวมถึงใช้เวลาในการประมวลผลเพื่อแสดงผล วิเคราะห์ ล็อกไฟล์และฐานข้อมูล ผลกระทบของการตรวจสอบที่ผิดพลาดจะส่งผลต่อสมรรถนะของระบบตรวจจับการบุกรุก รวมถึงผลกระทบที่เกิดจากการใช้หน่วยความจำจะส่งผลต่อการเกิดการทิ้งแพ็กเก็ต เนื่องจากระบบตรวจจับการบุกรุกไม่มีหน่วยความจำพอที่จะรองรับการวิเคราะห์แพ็กเก็ต

นอกจากนี้สถานการณ์เปลี่ยนแปลงของเครื่องเป้าหมายที่ได้กล่าวข้างต้น ยังส่งผลกระทบโดยตรงต่อสมรรถนะของระบบตรวจจับการบุกรุกเนื่องจาก preprocessor Stream5 จำเป็นที่จะต้องทำการเตรียมข้อมูลของเครื่องเป้าหมายไว้เพื่อวิเคราะห์ ทำการจัดเรียงข้อมูลและติดตามสถานะก่อนที่เครื่องเป้าหมายจะเปิดหรือยังไม่ได้เชื่อมต่อกับเครือข่าย ในกรณีดังกล่าว การใช้ทรัพยากรในการกระทำนั้นจึงเกินความจำเป็น ตัวอย่างเช่น การกำหนดนโยบายให้กับ preprocessor Stream5 ไว้ให้เครื่องเป้าหมายจำนวน 20 เครื่อง ทำให้ระบบตรวจจับการบุกรุก snort ทำการจองหน่วยความจำเพื่อรองรับนโยบายตามที่กำหนด แต่มีในความเป็นจริง ณ เวลาดังกล่าว มีเครื่องเป้าหมายเปิดใช้งานเพียง 10 เครื่อง ส่งผลให้เกิดการจองหน่วยความจำที่เกินความจำเป็นขึ้น เป็นต้น

ผู้วิจัยจึงมีแนวคิดที่จะใช้เครื่องมืออื่นหาข้อมูล เพื่อเพิ่มข้อมูลของเครื่องเป้าหมายที่สามารถปรับเปลี่ยนได้ตามสถานการณ์ให้แก่นโยบายของ Stream5 เพื่อรองรับการเปลี่ยนแปลงที่อาจเกิดขึ้นกับเครื่องเป้าหมายที่อยู่ภายในเครือข่าย ทั้งการลดนโยบายที่เกินความจำเป็น เพิ่มนโยบายเมื่อมีเครื่องหรือเครือข่ายเป้าหมายที่ไม่ได้กำหนดไว้ในนโยบาย การเปลี่ยนแปลงคุณสมบัติของเครื่องเป้าหมายให้สัมพันธ์กับคุณสมบัติของเครื่องเป้าหมายที่ใช้งานอยู่จริง

3.2 การส่งข้อมูลของเครื่องเป้าหมายให้กับระบบตรวจจับการบุกรุก

ข้อมูลที่ระบบตรวจจับการบุกรุกยังต้องการโดยทั่วไปแล้ว คือข้อมูลที่มีการเปลี่ยนแปลงของเครื่องเป้าหมายภายในเครือข่าย ในเบื้องต้นงานวิจัยนี้ได้นำการทำพอร์ตสแกนเพื่อเก็บข้อมูลของเครื่องเป้าหมาย ซึ่งโดยพื้นฐานของการทำพอร์ตสแกนสามารถค้นหาระบบปฏิบัติการของเครื่องเป้าหมาย และพอร์ตต่างๆที่เปิดใช้งานอยู่ โดยมีระบบสื่อกลางเพื่อรวบรวมข้อมูล ตรวจสอบการเปลี่ยนแปลงกับนโยบายเดิมที่มีอยู่ จากนั้นแปลข้อมูลดังกล่าวเป็นข้อมูลที่สามารถติดตั้งใน

นโยบาย จึงจะเป็นการปรับเปลี่ยนนโยบาย ทั้งนี้จำเป็นที่จะต้องคำนึงถึงผลกระทบต่อระบบเครือข่ายโดยรวมเนื่องจากการใช้งานและการค้นหาข้อมูลจากการทำพอร์ตสแกน อาจจะส่งผลกระทบต่อการทำงานของตัวระบบเองและสร้างความคับคั่งในเครือข่ายได้

ระบบนโยบายแบบพลวัต เป็นระบบที่ผู้วิจัยทำการพัฒนาขึ้นเพื่อเพิ่มข้อมูลให้แก่นโยบายของระบบตรวจจับการบุกรุก โดยใช้การทำพอร์ตสแกนมาร่วมกับระบบที่ถูกพัฒนาขึ้น จากนั้นจึงนำไปทำการแก้ไขนโยบายในโปรแกรม snort

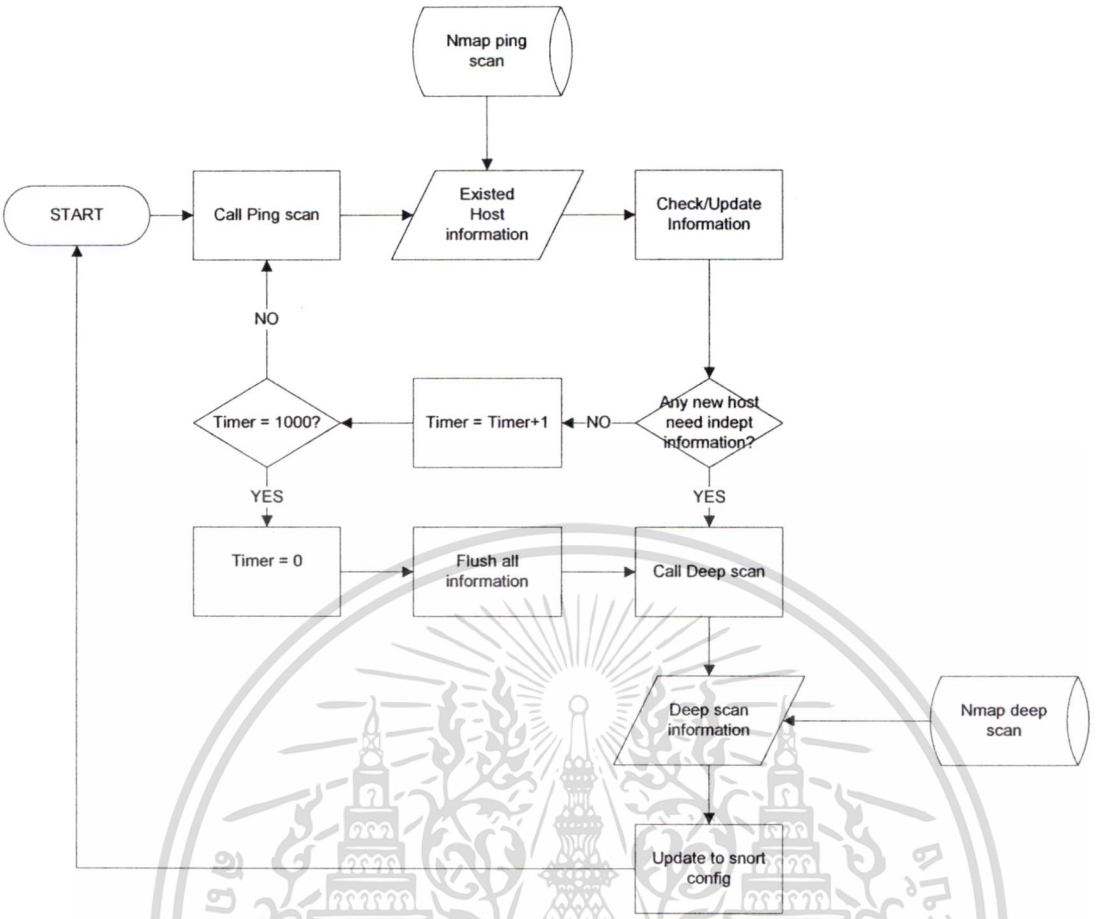
ในงานวิจัยนี้ ผู้วิจัยได้นำซอฟต์แวร์ nmap มาทำหน้าที่ในการค้นหาเครื่องเป้าหมาย และค้นหาคุณสมบัติต่างๆบนเครื่องเป้าหมายดังกล่าว โดยเลือกใช้ฟังก์ชั่น 2 ส่วนคือ 1.การค้นหาเครื่องเป้าหมายซึ่งจะเป็นการทำซ้ำอย่างต่อเนื่อง 2.การค้นหาข้อมูลของเครื่องเป้าหมายอย่างละเอียด

การทำงานของระบบ จะมีการเก็บข้อมูลเพื่อนำไปเปรียบเทียบกับข้อมูลจากการค้นหาครั้งก่อนหน้า โดยการค้นหาเครื่องเป้าหมายจะเรียกใช้ฟังก์ชั่นพอร์ตสแกนของซอฟต์แวร์ nmap เนื่องจากสามารถค้นหาเครื่องเป้าหมายที่อยู่ในเครือข่ายได้อย่างรวดเร็ว

จากนั้นทำการเปรียบเทียบกับข้อมูลเก่า เมื่อมีเครื่องเป้าหมายเครื่องใหม่ระบบจะทำการเรียกใช้พอร์ตสแกนเพื่อทำการตรวจหาข้อมูลของเครื่องเป้าหมายดังกล่าวอย่างละเอียด เนื่องจากการค้นหาข้อมูลเครื่องเป้าหมายอย่างละเอียด จำเป็นที่จะต้องใช้เวลานานกว่าในการค้นหาเครื่องเป้าหมาย ดังนั้นการเรียกค้นหาข้อมูลละเอียดนี้ จะทำเมื่อมีการค้นพบเครื่องเป้าหมายใหม่หรือทำตามกำหนดการของผู้ดูแลระบบเท่านั้น

จากนั้นระบบจะทำการนำข้อมูลรายละเอียดดังกล่าวแปลให้เป็นรูปแบบเดียวกับนโยบายใน Stream5 เพื่อนำไปแทนที่นโยบายเดิมในโปรแกรม snort ต่อไป ดังแสดงในรูปที่ 3.3

การค้นหาเครื่องเป้าหมายของซอฟต์แวร์ nmap นั้นสามารถทำได้ด้วยการใช้พอร์ตสแกนเช่นกัน แต่จะใช้เวลาในการประมวลผล ใช้ทรัพยากรของระบบ และเพิ่มภาระงานในเครือข่ายมากกว่า ดังนั้นการทำงานของระบบนโยบายแบบพลวัต จำเป็นที่จะต้องคำนึงถึงผลกระทบต่อปัจจัยดังกล่าว



รูปที่ 3.3 ลำดับการทำงานของการจัดการนโยบายแบบพลวัต

ผู้วิจัยจึงได้พัฒนาให้นโยบายแบบพลวัตใช้การค้นหาเครื่องเป้าหมายโดยการทำ ping scan คือ ฟังก์ชั่นในการค้นหาเครื่องเป้าหมายอย่างรวดเร็วของซอฟต์แวร์ nmap ซึ่งผู้วิจัยกำหนดให้ ping scan ทำงานบ่อยครั้งกว่าการทำพอร์ตสแกน โดยการเก็บข้อมูลของการค้นหาครั้งก่อน เพื่อเปรียบเทียบกับการค้นหาข้อมูลแบบ ping scan ซึ่งช่วยให้ลดการทำงานของการทำพอร์ตสแกน และเมื่อระบบจำเป็นต้องหาคุณสมบัติของเครื่องปลายทางจึงจะทำการเรียกใช้พอร์ตสแกน การทำพอร์ตสแกนนี้ใช้เวลานานและใช้ทรัพยากรเครือข่ายมากกว่า ดังนั้นการหาข้อมูลแบบ ping scan แล้วนำมาเปรียบเทียบเพื่อเรียกใช้พอร์ตสแกน จึงเป็นการลดภาระงานให้กับตัวระบบและเครือข่ายมากที่สุดเท่าที่จะทำได้ หลังจากได้รับข้อมูลการค้นหาเครื่องเป้าหมายอย่างละเอียดแล้ว ระบบจะทำการแปลงข้อมูลที่ได้รับไปเป็นนโยบายที่สามารถนำไปปรับใช้กับนโยบายของระบบตรวจจับการบุกรุก snort ได้

ในงานวิจัยนี้มุ่งเน้นไปที่การปรับแต่งนโยบาย และค่าคุณสมบัติของเครื่องเป้าหมายในนโยบายที่อยู่ภายใต้การทำงานของ preprocessor stream5 จากนั้นจึงส่งข้อมูลดังกล่าวกลับไปแก้ไขให้กับระบบตรวจจับการบุกรุก snort ต่อไป

ผู้วิจัยทำการวิเคราะห์ เปรียบเทียบเงื่อนไขของระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ทั่วไปกับระบบตรวจจับการบุกรุกที่ใช้นโยบายแบบพลวัตตามแนวคิดในงานวิจัย ดังนี้

เงื่อนไข True positive เงื่อนไขเมื่อไม่มีการบุกรุกและระบบตรวจจับการบุกรุกไม่ส่งสัญญาณเตือนนั้น ระบบตรวจจับการบุกรุกทั้งสองแบบไม่ส่งผลกระทบต่อเงื่อนไขดังกล่าว

เงื่อนไข True negative เงื่อนไขเมื่อมีการบุกรุกและระบบตรวจจับการบุกรุกส่งสัญญาณเตือนได้อย่างถูกต้อง ระบบตรวจจับการบุกรุกที่มีนโยบายแบบพลวัต มีความสามารถที่จะเพิ่มโอกาสที่จะเกิดเงื่อนไข True negative เนื่องจากความแม่นยำของระบบตรวจจับการบุกรุกถูกเพิ่มขึ้น เมื่อมีระบบตรวจจับการบุกรุกที่มีข้อมูลอย่างละเอียดของเครื่องเป้าหมาย จะทำให้การวินิจฉัยการโจมตีที่เกิดขึ้นเป็นไปอย่างมีประสิทธิภาพมากกว่า รวมถึงในกรณีที่มีความคับคั่งของข้อมูลหรือกรณีที่ทรัพยากรของระบบตรวจจับการบุกรุกมีอย่างจำกัด ซึ่งจะส่งผลต่อสมรรถนะและก่อให้เกิดอัตราการทิ้งแพ็กเก็ต การใช้นโยบายแบบพลวัตสามารถลดการใช้เงื่อนไขของระบบตรวจจับการบุกรุกที่เกินจากความเป็นจริง ส่งผลให้ระบบตรวจจับการบุกรุกลดอัตราการทิ้ง แพ็กเก็ตและทำให้การตรวจจับการบุกรุกทำได้อย่างมีประสิทธิภาพมากยิ่งขึ้น กรณีของเงื่อนไข True negative ระบบตรวจจับการบุกรุกที่มีนโยบายแบบพลวัตจึงมีความสามารถที่ดีกว่าระบบตรวจจับการบุกรุกทั่วไป

เงื่อนไข False positive เงื่อนไขเมื่อไม่มีการบุกรุกเกิดขึ้นแต่ระบบตรวจจับการบุกรุกส่งสัญญาณเตือน ระบบตรวจจับการบุกรุกที่มีการใช้ระบบนโยบายแบบพลวัตมีความสามารถในการลด False positive ที่จะเกิดขึ้นได้มากกว่าระบบตรวจจับการบุกรุกแบบเดิม เนื่องจากการที่ระบบตรวจจับการบุกรุกมีข้อมูลของเครื่องเป้าหมายที่ตรงกับความเป็นจริง และสามารถปรับเปลี่ยนได้ตามสถานการณ์ที่เกิดขึ้นเมื่อมีการเปลี่ยนแปลงของเครื่องเป้าหมาย หรือมีการเปลี่ยนแปลงอื่นๆในระบบเครือข่ายนั้น ส่งผลให้ลดความผิดพลาดในการวินิจฉัยข้อมูลในกรณีที่ข้อมูลของระบบตรวจจับการบุกรุกไม่สัมพันธ์กับคุณสมบัติของเครื่องเป้าหมาย หรือระบบเครือข่ายที่มีอยู่จริง

เงื่อนไข False negative เงื่อนไขเมื่อเกิดการบุกรุกและระบบตรวจจับการบุกรุกไม่สามารถทำการตรวจจับการบุกรุกที่เกิดขึ้นได้อย่างถูกต้องนั้น ทั้งระบบตรวจจับการบุกรุกเดิมและการบุกรุกที่ใช้นโยบายแบบพลวัต จะได้รับผลกระทบจากเงื่อนไขนี้เท่ากัน เนื่องจากสาเหตุของการเกิดเงื่อนไขนี้ คือระบบตรวจจับการบุกรุกมีข้อมูลของการโจมตีที่ไม่เพียงพอในการตรวจจับการบุกรุกที่เกิดขึ้น หรือการบุกรุกดังกล่าวเป็นการบุกรุกใหม่ที่เกิดขึ้นโดยที่ระบบตรวจจับการบุกรุกไม่ได้มีการเตรียมกฎขึ้นมาเพื่อป้องกัน

3.3 การวิเคราะห์ข้อมูล

จากที่ได้นำเสนอ การใช้นโยบายแบบพลวัตบนระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์จากสมมติฐานที่ได้ตั้งไว้ การประเมินสมรรถนะของระบบตรวจจับการบุกรุกในการทดลองที่จะทำต่อไปเน้นที่ประสิทธิภาพในการตรวจจับการบุกรุก ซึ่งได้แก่ความสามารถในการตรวจจับความแม่นยำของการตรวจจับ และความเร็วในการประมวลผลของระบบตรวจจับการบุกรุก

ผู้วิจัยได้เลือกตัวชี้วัดสองตัวได้แก่ อัตราการทิ้งแพ็กเก็ต (Drop rate) และ เวลาในการประมวลผล (Processing time) โดยอัตราการทิ้งแพ็กเก็ตผู้วิจัยได้อ้างอิงจากงานวิจัย[3] ซึ่งได้ศึกษาไว้ว่า อัตราการทิ้งแพ็กเก็ต เป็นตัวชี้วัดอย่างหนึ่งที่สามารถระบุได้ถึงสมรรถนะ และความสามารถในการตรวจจับของระบบตรวจจับการบุกรุก ซึ่งอัตราการทิ้งแพ็กเก็ตมีค่าที่ออกมาเป็นเปอร์เซ็นต์โดยบ่งบอกถึงอัตราการทิ้งแพ็กเก็ตที่เกิดขึ้น เนื่องจากระบบตรวจจับการบุกรุกไม่สามารถที่จะนำแพ็กเก็ตมาวิเคราะห์ได้ ตัวชี้วัดอีกตัวคือ เวลาการประมวลผล ผู้วิจัยได้นำ Packet Performance Monitor (PPM) เป็นความเร็วในการประมวลผลต่อหนึ่งแพ็กเก็ตของระบบตรวจจับการบุกรุก โดยนับตั้งแต่ได้รับแพ็กเก็ต จนสิ้นสุดกระบวนการ ซึ่งการกำหนดให้ snort ทำการแสดงค่า PPM นี้ได้จากการคอมไพล์(compile)โค้ดของระบบตรวจจับการบุกรุก snort เนื่องจาก PPM เป็นส่วนเสริมที่ไม่ได้มีการติดตั้งโดยปริยายให้แก่ระบบตรวจจับการบุกรุก snort แต่มีไว้เพื่อให้นักพัฒนาระบบสามารถนำค่า PPM ไปใช้ในการพัฒนาปรับปรุงระบบตรวจจับการบุกรุกsnort ต่อไป

บทที่ 4
การทดลองและรายงานผลการทดลอง

ในบทนี้กล่าวถึงการทดลอง รูปแบบข้อมูลที่ใช้ในการทดสอบ การสมมติสถานการณ์ของเครื่องเป้าหมาย และการประเมินสมรรถนะของการใช้การนโยบายแบบพลวัตสำหรับการตรวจจับการบุกรุกแบบใช้เป้าหมายเป็นเกณฑ์ นำมาเปรียบเทียบกับการใช้นโยบายปกติตามสถานการณ์ต่างๆ

4.1 ขั้นตอนและการออกแบบการทดลอง

ในการทดลองนี้ได้กำหนดให้มีเครื่องที่ทำหน้าที่เป็นระบบตรวจจับการบุกรุก โดยมีการติดตั้งระบบตรวจจับการบุกรุก snort ที่มีการใช้กฎตามที่ได้กำหนดมาไว้ให้แต่แรกเริ่ม ทั้งนี้ได้มีการคอมไพล์ใหม่โดยการเพิ่มให้สามารถตรวจจับประสิทธิภาพของแพ็กเก็ต PPM (Packet Performance Mornitor) และมีการเรียกใช้นโยบายบน preprocessor stream5 พร้อมทั้งติดตั้งระบบนโยบายแบบพลวัต และมีเครื่องเป้าหมายที่อยู่บนเครื่องเซิร์ฟเวอร์ที่ติดตั้งซอฟต์แวร์ virtual machine เพื่อให้ง่ายต่อการปรับเปลี่ยนและเพิ่มเติมเครื่องเป้าหมาย นอกจากนี้ยังกำหนดคุณสมบัติให้เครื่องเป้าหมายแต่ละเครื่องต่างกัน เช่น จำนวนพอร์ตที่เปิดอยู่ หมายเลขไอพี และระบบปฏิบัติการ ทั้งบังคับให้มีการเปลี่ยนแปลงคุณสมบัติ และมีการเปิดปิดเครื่องสลับกันไปเสมอ เครื่องคอมพิวเตอร์สำหรับสร้างแพ็กเกตพื้นฐานทั่วไปและแพ็กเก็ตที่เป็นการโจมตี ใช้สคริปต์ที่ชื่อว่า stickz ในการสร้างแพ็กเก็ตที่มีลักษณะตรงกับกฎของระบบตรวจจับการบุกรุกโดยถือว่าเป็นการโจมตี การสร้างการโจมตีที่ตรงกับกฎเป็นการกำหนดเงื่อนไขในการทดลอง เนื่องจากการโจมตีที่จะเกิดขึ้นจากสคริปต์ไม่มีความแตกต่างกับกฎของระบบตรวจจับการบุกรุก และถือว่าไม่มีการโจมตีอื่นๆนอกเหนือจากกฎของระบบตรวจจับการบุกรุก

4.2 ผลการทดลอง

การทดลองแบ่งออกเป็นสองรูปแบบคือ

1. การประเมินสมรรถนะและความแม่นยำของระบบตรวจจับการบุกรุก โดยมีตัวชี้วัดคือ อัตราการทิ้งแพ็กเก็ต (Drop rate) ซึ่งเป็นค่าที่วัดจากความสามารถในการรองรับแพ็กเก็ตเพื่อนำมาวิเคราะห์ เมื่อการทิ้งแพ็กเก็ตเกิดขึ้น หมายความว่า ระบบตรวจจับการบุกรุกไม่มีทรัพยากรมากพอที่จะรองรับแพ็กเก็ตเพื่อนำมาวินิจฉัยหรือวิเคราะห์

2. การประเมินความเร็วในการประมวลผลของระบบตรวจจับการบุกรุก โดยมีตัวชี้วัดคือ PPM ซึ่งเป็นเวลานับตั้งแต่แพ็กเก็ตจากเครือข่ายเริ่มเข้ากระบวนการวิเคราะห์จนสิ้นสุดกระบวนการ เหตุที่ผู้วิจัยได้เลือกตัวชี้วัดนี้ขึ้นมาวิเคราะห์เนื่องจากได้คำนึงถึงกรณีที่ทรัพยากรที่มีให้ระบบตรวจจับการบุกรุกนั้นมีได้อย่างไม่จำกัด และไม่เกิดการทิ้งแพ็กเก็ต

ในการทดลองแต่ละครั้ง จะใช้นโยบายที่ครอบคลุมเครื่องเป้าหมายในเครือข่ายทั้งหมดและนโยบายที่เป็นแบบพลวัต จากนั้นนำผลจากการทดลองมาเปรียบเทียบกัน

รายละเอียดฟิลด์(Field)ของข้อมูลในตารางที่จะนำเสนอ มีดังต่อไปนี้คือ

- ชุดข้อมูล Tx คือ สถานการณ์ที่ x เป็นจำนวนของนโยบายที่มีอยู่ในเครือข่ายจริง
- ชุดข้อมูล Px คือ สถานการณ์ที่ y เป็นจำนวนของคุณสมบัติในนโยบายที่มีอยู่จริงบนเครือข่าย

4.2.1 การประเมินสมรรถนะและความแม่นยำของระบบตรวจจับการบุกรุก

การทดลองเพื่อประเมินสมรรถนะและความแม่นยำของระบบตรวจจับการบุกรุก ทำโดยการคิดค่าการทิ้งแพ็กเก็ต ผู้วิจัยทำการสร้างสถานการณ์ที่เครือข่ายอยู่ในภาวะความคับคั่งสูง เนื่องจากต้องการเห็นความแตกต่างในการทิ้งแพ็กเก็ตที่ชัดเจน เพื่อแสดงผลกระทบของการใช้นโยบายที่ไม่จำเป็นในระบบตรวจจับการบุกรุก โดยมีการกำหนดค่าพารามิเตอร์ดังแสดงในตารางที่ 4.1

ตารางที่ 4.1 พารามิเตอร์ที่สำคัญในการจำลองระบบเพื่อประเมินสมรรถนะ

Parameter	Value
จำนวนกฎที่ระบบตรวจจับการบุกรุกนำมาใช้	6770 rules
ความเร็วในการส่งข้อมูล	64.43 Mb/s
จำนวน attribute มีอยู่ในแต่ละนโยบาย	2-14 attributes
จำนวนนโยบาย	1-10 policies

การสื่อสารในเครือข่ายทดลองที่เป็นข้อมูลการสื่อสารในการทดลองนี้ เป็นการส่งข้อมูลที่ทำการสร้างจากซอฟต์แวร์และบันทึกจากเครือข่ายที่ใช้ในการทดลอง ทั้งหมด 432,058 แพ็กเก็ต แบ่งได้เป็น ข้อมูลจากการโจมตีที่ตรงตามกฎที่ระบบตรวจจับการบุกรุกนำมาใช้ทั้งหมดที่ถูกสร้างโดยสคริปต์ 184,243 แพ็กเก็ต และแพ็กเก็ตทั่วไป 247,815 แพ็กเก็ต ซึ่งแพ็กเก็ตทั้งหมดถูกบันทึกโดยซอฟต์แวร์ tcpdump และนำมาใช้ใหม่ทุกครั้งที่มีการทำการทดลองโดยใช้ซอฟต์แวร์ tcpreplay

และการส่งข้อมูลที่ความเร็ว 64.43 Mb/s โดยจำนวนเครือข่ายและคุณสมบัติของเครื่องเป้าหมายจะมีการสลับเปลี่ยนแปลง

การปรับแต่งของระบบตรวจจับการบุกรุกแบ่งเป็นสองแบบคือ ระบบตรวจจับการบุกรุกทั่วไปที่มีการใช้นโยบายในการตรวจจับการบุกรุกครอบคลุมเครื่องเป้าหมายทั้งหมด และระบบตรวจจับการบุกรุกที่มีการใช้นโยบายแบบพลวัตในการตรวจจับการบุกรุก และทำการทดลองทั้งหมด 10 ครั้งเพื่อนำผลการทดลองมาหาค่าเฉลี่ย ดังแสดงในตารางที่ 4.2

ตารางที่ 4.2 อัตราการทิ้งแพ็กเก็ตจากการใช้นโยบายแบบพลวัต ตามสถานการณ์ที่กำหนด

	P14	P12	P10	P8	P6	P4	P2
T1	50.59	47.19	47.97	47.41	47.35	47.42	47.84
T2	54.93	48.14	49.36	48.566	48.67	48.41	47.43
T3	61.02	55.53	53.30	47.97	49.31	48.441	47.54
T4	68.04	58.32	54.05	48.62	49.22	48.67	47.41
T5	71.05	62.38	54.93	50.76	50.02	49.25	48.10
T6	74.06	64.74	59.41	54.08	51.05	51.78	49.78
T7	83.67	65.19	59.98	55.84	51.59	51.29	50.29
T8	87.09	68.51	61.48	59.93	52.48	52.35	51.52
T9	89.15	73.18	63.45	60.02	53.46	52.69	52.17
T10	90.68	75.29	70.57	65.68	55.19	53.10	51.67

ในการทดลองนี้นโยบายของระบบ stream5 เดิมมีอัตราการทิ้งแพ็กเก็ต โดยเฉลี่ยที่ 89.54% จากตารางที่ 4.2 จะเห็นได้ว่าเมื่อเครือข่ายเป้าหมายมีจำนวนเป้าหมายตามนโยบายต่ำสุดคือ 1 นโยบาย และคุณสมบัติของเครื่องเป้าหมายต่ำสุดที่ 2 คุณสมบัติ จะส่งผลให้อัตราการทิ้งแพ็กเก็ตลดลงเหลือ 47.84% เมื่อใช้นโยบายที่เป็นแบบพลวัต และมีอัตราการทิ้งแพ็กเก็ตสูงสุดในการทดลองเมื่อเครือข่ายเป้าหมายมีจำนวนเครื่องเป้าหมายตามนโยบายสูงสุด และจำนวนคุณสมบัติของเครื่องเป้าหมายสูงสุด จะส่งผลให้อัตราการทิ้งแพ็กเก็ตเพิ่มขึ้นเป็น 90.68%

4.2.2 การประเมินเวลาในการประมวลผลของระบบตรวจจับการบุกรุก

การทดลองเพื่อประเมินเวลาในการประมวลผลของระบบตรวจจับการบุกรุก ทำโดยการเฝ้าสังเกตการประมวลผลแพ็กเก็ต (Packet Performance Monitor : PPM) โดยค่าดังกล่าวมีหน่วยเป็นไมโครวินาที (microsecond) ผู้วิจัยทำการสร้างสถานการณ์ที่เครือข่ายอยู่ในภาวะความคับคั่งต่ำที่สุดโดยจัดการทดลองให้ระบบตรวจจับการบุกรุกไม่มีการทิ้งแพ็กเก็ต เนื่องจากต้องการแสดงผล

กระทบและความแตกต่างเมื่อการใช้ทรัพยากรของระบบมีสมรรถนะที่ดี อีกนัยหนึ่งคือ ระบบมีทรัพยากรไม่จำกัด เพื่อแสดงความแตกต่างด้านเวลาในการประมวลผลของการใช้นโยบายที่ไม่จำเป็นในระบบตรวจจับการบุกรุก โดยมีการกำหนดค่าพารามิเตอร์ดังแสดงในตารางที่ 4.3

ตารางที่ 4.3 พารามิเตอร์ที่สำคัญในการจำลองระบบเพื่อประเมินเวลาในการประมวลผล

Parameter	Value
ปริมาณกฎที่ระบบตรวจจับการบุกรุกนำมาใช้	3,580 rules
ความเร็วในการสื่อสาร	18.04 Mb/s
ปริมาณ attribute มีอยู่ในนโยบาย	2-14 attributes
ปริมาณนโยบาย	1-10 policies

การสื่อสารในเครือข่ายทดลองที่เป็นข้อมูลการในการทดลองนี้ เป็นการส่งข้อมูลที่ทำการสร้างจากซอฟต์แวร์และบันทึกจากเครือข่ายที่ใช้ในการทดลองทั้งหมด 446,218 แพ็กเก็ต แบ่งได้เป็น ข้อมูลจากการโจมตีที่ตรงตามกฎที่ระบบตรวจจับการบุกรุกนำมาใช้ทั้งหมดที่ถูกสร้างโดยสคริปต์ 165,190 แพ็กเก็ต และแพ็กเก็ตทั่วไป 281,028 แพ็กเก็ต การเปลี่ยนชุดข้อมูลในการทดลองนี้ เนื่องจากความจำเป็นที่จะต้องกำหนดให้ไม่มีอัตราการทิ้งแพ็กเก็ตโดยการลดกฎของระบบการตรวจจับการบุกรุก ทำให้การสร้างแพ็กเก็ตไม่ตรงกับกฎที่มีดังนั้นการสร้างข้อมูลเข้าชุดนี้จึงสร้างขึ้นตามกฎที่ระบบตรวจจับการบุกรุกจะนำมาใช้เท่านั้น ซึ่งแพ็กเก็ตทั้งหมดถูกบันทึกโดยซอฟต์แวร์ tcpdump และนำมาใช้ใหม่ทุกครั้งที่มีการทำการทดลองโดยใช้ซอฟต์แวร์ tcpreplay โดยส่งข้อมูลที่ความเร็ว 18.04 Mb/s การกำหนดค่าดังกล่าว เพื่อสร้างสภาวะที่ระบบตรวจจับการบุกรุกไม่มีการทิ้งแพ็กเก็ต โดยจำนวนเครือข่ายและคุณสมบัติของเครื่องเป้าหมายจะมีการสลับเปลี่ยนแปลง

การปรับแต่งของระบบตรวจจับการบุกรุกแบ่งเป็นสองรูปแบบคือ ระบบตรวจจับการบุกรุกทั่วไปที่มีการใช้นโยบายในการตรวจจับการบุกรุกครอบคลุมเครื่องเป้าหมายทั้งหมด และระบบตรวจจับการบุกรุกที่มีการใช้นโยบายแบบพลวัตในการตรวจจับการบุกรุก โดยทำการทดลองซ้ำทั้งหมด 10 ครั้งเพื่อนำผลการทดลองมาหาค่าเฉลี่ย ดังแสดงในตารางที่ 4.4

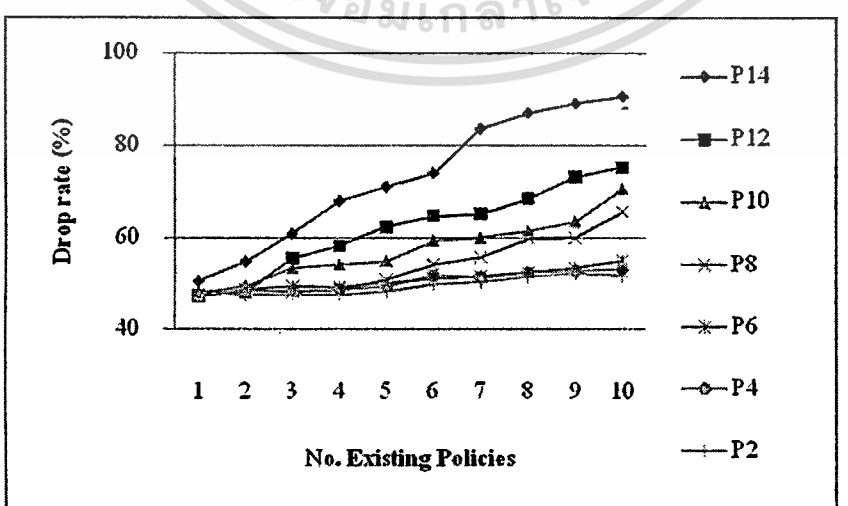
ตารางที่ 4.4 ค่า PPM จากการทดลองใช้นโยบายแบบพลวัต ตามสถานการณ์ที่กำหนด

	P14	P12	P10	P8	P6	P4	P2
T1	4.196	4.189	4.174	4.172	4.153	4.150	4.147
T2	4.271	4.271	4.329	4.245	4.210	4.200	4.180
T3	4.683	4.598	4.506	4.445	4.402	4.270	4.215
T4	4.867	4.806	4.794	4.750	4.671	4.604	4.560
T5	4.891	4.890	4.841	4.800	4.781	4.751	4.680
T6	5.002	4.891	4.875	4.870	4.851	4.723	4.702
T7	5.193	5.072	4.957	4.942	4.951	4.828	4.715
T8	5.347	5.287	5.257	5.238	5.193	5.068	4.996
T9	5.898	5.801	5.793	5.672	5.583	5.432	5.306
T10	6.423	6.284	5.900	5.781	5.683	5.603	5.426

ในการทดลองนี้ นโยบายของระบบ stream5 เดิมมี PPM เฉลี่ย 6.251 ไมโครวินาที จากตารางที่ 4.4 จะเห็นได้ว่าเมื่อเครือข่ายเป้าหมายมีจำนวนเป้าหมายตามนโยบายต่ำสุดที่ 1 นโยบาย และคุณสมบัติของเครื่องเป้าหมายต่ำที่ 2 คุณสมบัติ ส่งผลให้ PPM ลดลงเหลือ 4.147 ไมโครวินาที เมื่อใช้นโยบายที่เป็นแบบพลวัต

4.3 วิเคราะห์ผลการทดลอง

จากตารางที่ 4.2 สามารถนำข้อมูลมาสร้างกราฟได้ดังรูปที่ 4.1

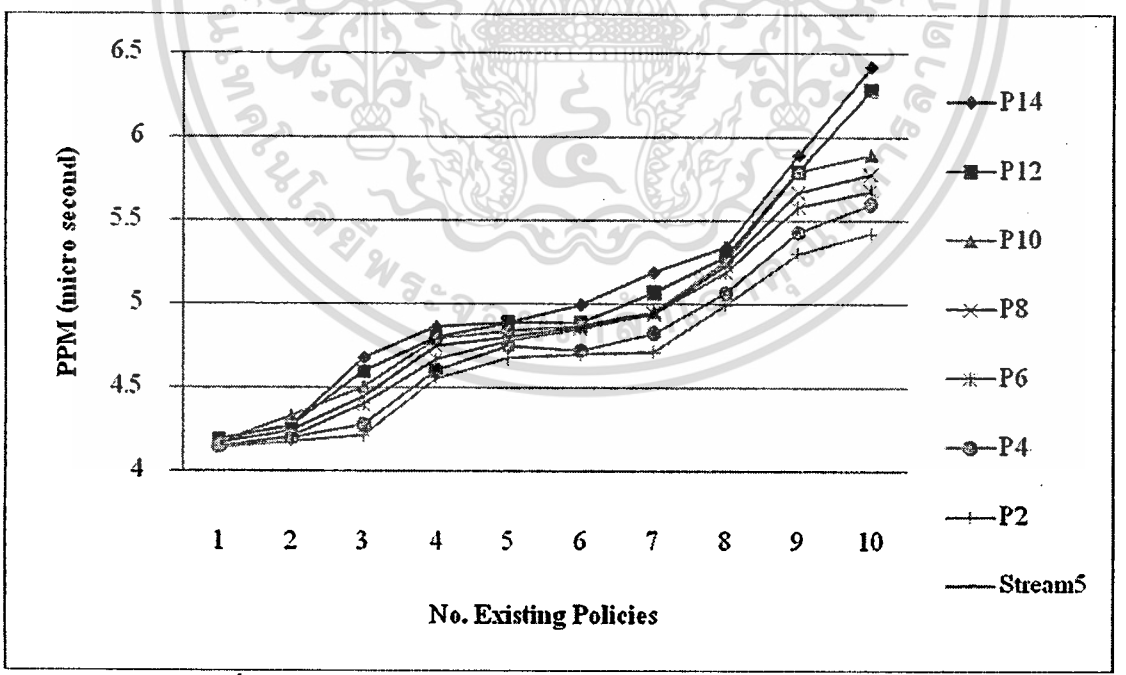


รูปที่ 4.1 กราฟแสดงความสัมพันธ์ของสถานการณ์ต่างๆกับอัตราการทิ้งแพ็กเก็ต

จากรูปที่ 4.1 เป็นกราฟแสดงความสัมพันธ์ของสถานการณ์ต่างๆกับอัตราการทิ้งของแพ็กเก็ต โดยแกนตั้งคืออัตราการทิ้งแพ็กเก็ตที่เกิดขึ้น แกนนอนคือจำนวนของนโยบายที่มีอยู่จริงบนเครือข่ายทดลอง และแต่ละชุดข้อมูล P คือจำนวนของคุณสมบัติที่มีอยู่ในนโยบาย โดยค่าของ stream5 หมายถึงค่าอัตราการทิ้งแพ็กเก็ตของระบบตรวจจับการบุกรุกเดิม ซึ่งแสดงให้เห็นได้ว่าการใช้นโยบายแบบพลวัตส่งผลต่ออัตราการทิ้งแพ็กเก็ต เมื่อมีจำนวนของนโยบายและคุณสมบัติในนโยบายที่มีอยู่จริงลดลง นโยบายของระบบตรวจจับการบุกรุกที่ใช้นโยบายแบบพลวัตจะลดจำนวนของนโยบายและคุณสมบัติลงตามความเป็นจริง ส่งผลให้ลดเงื่อนไขการทำงานของระบบตรวจจับการบุกรุก และทำให้อัตราการทิ้งแพ็กเก็ตลดลงตามไปด้วย รวมทั้งแนวโน้มของอัตราทิ้งแพ็กเก็ตนั้น มีแนวโน้มสูงขึ้นเมื่อมีการสร้างเงื่อนไขให้แก่ระบบตรวจจับการบุกรุกสูงขึ้น

สำหรับชุดข้อมูล P14 ที่จำนวนนโยบาย 10 นโยบาย แสดงให้เห็นว่าระบบนโยบายแบบพลวัต มีอัตราการทิ้งแพ็กเก็ตสูงกว่าค่าของ stream5 เนื่องจากการใช้นโยบายแบบพลวัตส่งผลต่อสมรรถนะของระบบตรวจจับการบุกรุก โดยการนำระบบพลวัตส่งผลต่อสมรรถนะและอัตราทิ้งแพ็กเก็ตเพิ่มขึ้นจากระบบตรวจจับการบุกรุกทั่วไป 2.51 เปอร์เซ็นต์ เมื่อมีสภาวะที่ระบบเครือข่ายไม่มีการเปลี่ยนแปลงและมีการใช้นโยบายอย่างครบถ้วน

จากตารางที่ 4.4 สามารถมาสร้างกราฟได้ดังแสดงในรูปที่ 4.2

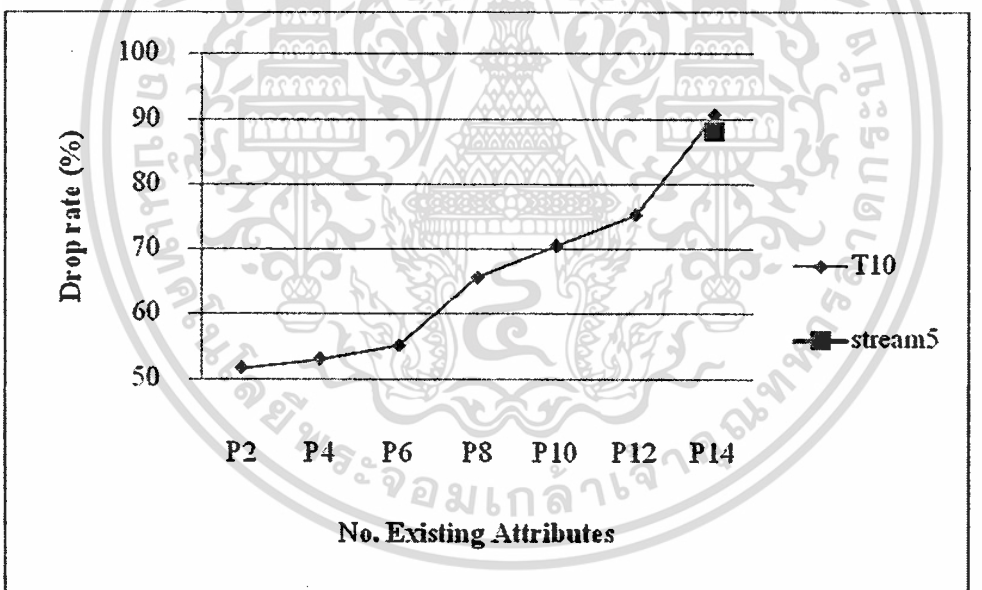


รูปที่ 4.2 กราฟแสดงความสัมพันธ์ของสถานการณ์ต่างๆกับ PPM

จากรูปที่ 4.2 เป็นกราฟแสดงความสัมพันธ์ระหว่างการเปลี่ยนแปลงของนโยบายกับความเร็วในการประมวลผล โดยแกนนอนคือจำนวนนโยบายที่มีอยู่จริงในเครือข่าย และแกนตั้งคือความเร็วในการประมวลผลของระบบตรวจจับการบุกรุก ซึ่งแสดงให้เห็นถึงแนวโน้มที่สูงขึ้นของเวลาของการประมวลผลตามการใช้นโยบายที่แตกต่างกัน และแต่ละชุดข้อมูลคือ จำนวนของคุณสมบัติที่มีอยู่ในนโยบาย โดยชุดข้อมูลของ stream5 หมายถึงค่า PPM ของระบบตรวจจับการบุกรุกเดิม ซึ่งแสดงให้เห็นได้ว่าการใช้นโยบายแบบพลวัตส่งผลต่อค่า PPM โดยค่าของ PPM มีแนวโน้มสูงขึ้นเมื่อมีการใช้นโยบายและคุณสมบัติที่เพิ่มขึ้น เนื่องจากการสร้างเงื่อนไขให้กับระบบตรวจจับการบุกรุกนั้นส่งผลต่อความเร็วในการประมวลผลของในแต่ละแพ็กเก็ต

ในชุดข้อมูลที่ P14 และ P12 มีค่า PPM สูงกว่าค่าของ stream5 ซึ่งเป็นระบบเดิม เนื่องจากการใช้ทรัพยากรเพื่อการทำงานของระบบนโยบายแบบพลวัตส่งผลต่อสมรรถนะของระบบ

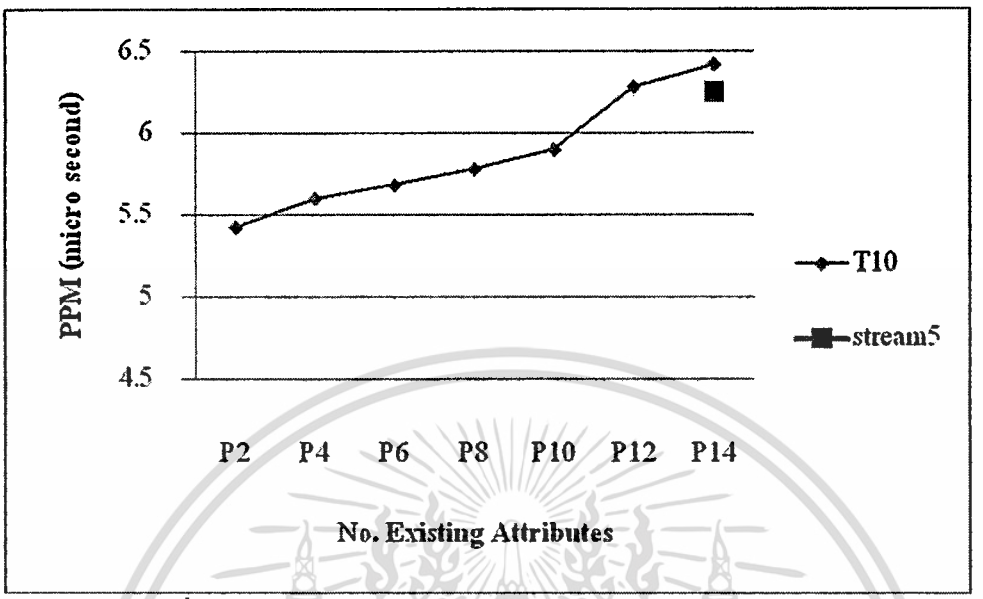
ผู้วิจัยได้นำกราฟทั้งสองรูปมาวิเคราะห์ เพื่อหาความสัมพันธ์ของคุณสมบัติต่างๆที่กำหนดให้ภายในนโยบายของระบบตรวจจับเพื่อหาความสัมพันธ์ของคุณสมบัติ และสมรรถนะรวมทั้งประสิทธิภาพของระบบตรวจจับการบุกรุก ดังแสดงในรูปที่ 4.3 และ 4.4



รูปที่ 4.3 ความสัมพันธ์ของคุณสมบัติภายในนโยบายและอัตราการทิ้งแพ็กเก็ต

จากรูปที่ 4.3 แสดงให้เห็นถึงความสัมพันธ์ระหว่างคุณสมบัติภายในนโยบายและอัตราการทิ้งแพ็กเก็ต โดยนำเอาทุก T10 หรือการใช้นโยบาย 10 นโยบาย ของทุกๆชุดข้อมูลจากรูปที่ 4.2 นำมาสร้างกราฟใหม่ โดยแกนนอนคือ จำนวนของคุณสมบัติภายใน T10 และ แกนตั้งคืออัตราการทิ้งแพ็กเก็ต แสดงให้เห็นถึงแนวโน้มของอัตราการทิ้งแพ็กเก็ตเมื่อเพิ่มข้อกำหนดของคุณสมบัติภายในนโยบายที่มีแนวโน้มเพิ่มขึ้น

ในกรณีที่กำหนดคุณสมบัติให้ทุกนโยบาย 14 คุณสมบัติ แต่ในสถานการณ์จริงมีการใช้ 2 คุณสมบัติ ระบบพลวัตสามารถลดอัตราการทิ้งแพ็กเก็ตได้เกือบ 40 เปอร์เซ็นต์



รูปที่ 4.4 ความสัมพันธ์ของคุณสมบัติภายในนโยบายและPPM

จากรูปที่ 4.4 แสดงให้เห็นถึงความสัมพันธ์ระหว่างคุณสมบัติภายในนโยบายและความเร็วในการประมวลผล โดยนำเอาทุก T10 หรือการใช้นโยบาย 10 นโยบาย ของทุกชุดข้อมูลจากรูปที่ 4.2 นำมาสร้างกราฟใหม่ โดยแกนนอนคือ จำนวนของคุณสมบัติภายใน T10 และ แกนตั้งคือ PPM แสดงให้เห็นถึงแนวโน้มของเวลาในการประมวลผลของระบบตรวจจับการบุกรุกเพิ่มขึ้น เมื่อเพิ่มคุณสมบัติภายในนโยบาย

4.4 การวิเคราะห์ผลกระทบเมื่อนำระบบนโยบายแบบพลวัตมาใช้

ผู้วิจัยได้คำนึงถึงผลกระทบของการนำพอร์ตสแกนเนอร์มาใช้ในการพัฒนา ระบบนโยบายแบบพลวัต เนื่องจากการทำพอร์ตสแกนมีการใช้แบนด์วิดท์ (Bandwidth) ของเครือข่ายซึ่งถือว่าเป็นค่าใช้จ่ายอื่น (Overhead) ที่เกี่ยวข้องกับสมรรถนะของแบนด์วิดท์เครือข่าย จึงได้ทำการทดสอบซอฟต์แวร์ nmap ซึ่งเป็นพอร์ตสแกนเนอร์ที่นำมาใช้ในงานวิจัย โดยการวัดค่าเฉลี่ยจากการscan ทั้งหมด 10 ครั้งเพื่อหาค่าเฉลี่ย ได้ผลการทดสอบดังนี้

1. การทำ ping scan เครือข่ายเพื่อค้นหาการมีอยู่ของเครื่องเป้าหมาย ใช้ปริมาณแบนด์วิดท์เพิ่มขึ้นจากการใช้แบนด์วิดท์ทั่วไป 1,160.421 ไบต์ต่อวินาทีตลอดระยะเวลาในการค้นหา โดยภายในเครือข่ายทดสอบ การทำ ping scan สามารถจับเวลาในการค้นหาเครื่องเป้าหมายได้ 1.03-3.6 วินาที ต่อ256หมายเลขไอพี ในการทดลองมีการใช้10

เครือข่าย หรือระยะ 2560 หมายเลขไอพี ซึ่งใช้เวลาในการค้นหาเป้าหมาย 4.06-11.47 วินาที

2. การทำพอร์ตสแกนในแต่ละเครื่องเป้าหมาย ใช้ปริมาณแบนด์วิดท์เพิ่มขึ้นจากการใช้แบนด์วิดท์ทั่วไป 11,170.552 ไบต์ต่อวินาทีตลอดระยะเวลาในการค้นหา โดยภายในเครือข่ายทดสอบ ทำการพอร์ตสแกน สามารถจับเวลาได้ 0.86-3.00วินาที ต่อหนึ่งเครื่อง

ระบบนโยบายแบบพลวัตใช้เวลาการทำงานโดยทำงานทั้ง ping scan และพอร์ตต่อรอบประมาณ 3.06-4.53 วินาที ดังนั้นการหน่วงเวลาของระบบนโยบายแบบพลวัตในกรณีที่เลวร้ายที่สุดที่จะเกิดขึ้นคือ เมื่อมีเครื่องเป้าหมายที่ไม่เคยมีข้อมูลมาก่อนเข้ามาใหม่ในระบบเครือข่าย หลังจากที่ทำการ ping scan และระบบนโยบายแบบพลวัตต้องทำงานรอบที่สองเพื่อค้นหารายละเอียดของเครื่องดังกล่าวแล้ว ความล่าช้าที่เกิดขึ้นในการปรับปรุงนโยบาย ของกรณีที่เลวร้ายที่สุดจะอยู่ที่ 11.47+4.53+11.47+4.53+3.00 = 35 วินาที

การวัดค่าดังกล่าว แสดงให้เห็นถึงความล่าช้าที่จะเกิดขึ้น ของระบบนโยบายแบบพลวัตเฉพาะในการทดลองของผู้วิจัยเท่านั้น เวลาในการทำงานของซอฟต์แวร์ nmap ขึ้นอยู่กับหลายปัจจัย เช่นคุณภาพของสายสัญญาณ จำนวนช่วงเชื่อมต่อ (Hop) รวมถึงวิธีการเรียกใช้ซอฟต์แวร์ nmap ซึ่งผู้วิจัยได้ทดลองกับหลายๆเครือข่ายพบว่าเวลาความล่าช้าดังกล่าวไม่เท่ากัน

บทที่ 5
สรุปผลการวิจัย และข้อเสนอแนะ

5.1 สรุปผลการวิจัย

จากการศึกษาการทำงานของระบบตรวจจับการบุกรุกที่ใช้เป้าหมายเป็นเกณฑ์ พบว่าปริมาณของข้อมูลของเครื่องเป้าหมาย และปริมาณการสื่อสารภายในเครือข่ายที่ระบบตรวจจับการบุกรุกตรวจจับส่งผลต่อสมรรถนะของตัวระบบเอง เนื่องจากการกำหนดข้อมูลเครื่องเป้าหมาย และปริมาณนโยบายนั้น สร้างเงื่อนไขเพิ่มเติมให้กับระบบตรวจจับการบุกรุก ทั้งยังส่งผลให้การวินิจฉัยแพ็กเก็ตมีความผิดพลาดโดยการทิ้งแพ็กเก็ต รวมถึงมีอัตราการทิ้งแพ็กเก็ตเพิ่มขึ้นตามปริมาณของข้อมูลที่กำหนดไว้ การพัฒนาต้นแบบของการใช้นโยบายแบบพลวัต ช่วยลดการใช้นโยบายและข้อมูลของคุณสมบัติเครื่องเป้าหมายที่เกินความจำเป็น และปรับปรุงนโยบายให้ถูกต้องเสมอ โดยยึดหลักการของการสร้างระบบตรวจจับการบุกรุกที่มีข้อมูลเครื่องเป้าหมายถูกต้องและแม่นยำเมื่อสภาวะของเครื่องเป้าหมายเปลี่ยนแปลง ภายใต้ทรัพยากรของอุปกรณ์ที่มีอย่างจำกัด และเพื่อเป็นแนวทาง ในการสร้างระบบการตรวจจับการบุกรุกที่ข้อมูลของเครื่องเป้าหมายถูกต้องอยู่ตลอดเวลา และลดข้อมูลที่เกินความจำเป็นที่อาจจะเกิดขึ้นได้

ทั้งนี้การจัดการนโยบายแบบพลวัตใช้ได้อย่างมีประสิทธิภาพมากกว่าภายใต้สภาวะที่เครื่องเป้าหมายมีการเปลี่ยนแปลงบ่อยครั้ง

5.2 ข้อเสนอแนะเพื่องานวิจัยในอนาคต

จากผลการทดลองในงานวิจัยแสดงให้เห็นถึง ผลกระทบของการเปลี่ยนแปลงของเครื่องเป้าหมายภายในระบบเครือข่าย ที่มีผลต่อสมรรถนะระบบตรวจจับการบุกรุก และแสดงให้เห็นถึงข้อบกพร่องบางอย่างที่เกิดขึ้นกับข้อมูลภายในนโยบาย เมื่อมีการเปลี่ยนแปลงคุณสมบัติของเครื่องเป้าหมายของเครือข่ายที่มีอยู่จริง กับนโยบายของระบบตรวจจับการบุกรุก

ระบบที่ผู้วิจัยพัฒนา เป็นระบบที่ต่อพ่วงกับตัวระบบตรวจจับการบุกรุก การทำงานในบางกรณีอาจเกิดความผิดพลาด ดังนั้นระบบตรวจจับการบุกรุกควรจะมีความสามารถในการสับเปลี่ยนนโยบายรวมถึงการต่อพ่วงของระบบที่ง่ายมากขึ้น และการใช้ port scanner ในบางกรณีจำเป็นที่จะต้องสร้างกฎเพิ่มเติมเนื่องจาก การสแกนในบางกรณีส่งผลให้ระบบตรวจจับการบุกรุกวินิจฉัยว่าเป็นการค้นหาช่องโหว่เพื่อการโจมตี

ระบบตรวจจับแบบใช้เป้าหมายเป็นเกณฑ์ ยังต้องการการปรับปรุงพัฒนาเนื่องจากด้านความคิดริเริ่มในการใช้ข้อมูลของเป้าหมายมาใช้ร่วมในการวินิจฉัยนั้น เป็นแนวทางที่มีประสิทธิภาพและสามารถแก้ไขปัญหาที่เคยเกิดขึ้นมาก่อนได้เป็นอย่างดี ทว่าทางปฏิบัตินั้นการ

สร้างข้อมูลหรือการสร้างความรู้ให้กับระบบตรวจจับการบุกรุกนั้น ยังไม่เป็นไปตามแนวคิดข้างต้นอย่างสมบูรณ์ ดังนั้นการพัฒนาระบบตรวจจับการบุกรุกดังกล่าวให้เป็นไปตามแนวความคิดนั้นยังคงต้องมีการปรับปรุงและพัฒนาต่อไป

บรรณานุกรม

[1] Puketza, N. J., Zhang K. and Chung, M. "A Methodology for Testing Intrusion Detection Systems". In IEEE Transactions on Software Engineering, Vol. 22, No.10, 719-729. 1996.

[2] Novak, J. and Sturges, S. "Target-Based TCP Timestamp Stream Reassembly", Sourcefire, Inc. 2007.

[3] Schaelicke, L., Slabach, T., Moore, B. and Freeland, C. "Characterizing the Performance of Network Intrusion Detection Sensors", In Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection (RAID 2003), Springer-Verlag, Berlin - Heidelberg - New York, 155-172. 2003.

[4] Ranum, M. J. "False Positives: A User's Guide to Making Sense of IDS Alarms", ICSA Labs IDSC. . 2003.

[5] Ranum, M. J. "Experiences Benchmarking Intrusion Detection Systems", Technical Report, NFR Security, Inc. 2001.

[6] Ptacek, T. and Newsham, T. "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection System" , Technical Report, Secure Networks, Inc. 1998.

[7] Roesch, M. "Snort - Lightweight Intrusion Detection for Networks" , In Proceedings of the 13th Systems Administration Conference (Seattle, WA, November 7-12, 1999), 229-238. 1999.

[8] Debar, H., Dacier, M. and Wespi, A. "Towards a Taxonomy of Intrusion-detection Systems" . Computer Networks, Vol. 31, 805-822. 1999.

[9] Novak, J. and Sturges, S. "Target-Based TCP Stream Reassembly" , Sourcefire, Inc. 2007.

[10] Novak, J. "Target-Based Fragmentation Reassembly" , Sourcefire, Inc. 2005.

[11] Lloyd G. Greenwald and Tavaris J. Thomas, "Evaluating Tests used in Operating System Fingerprint" . LGS Bell Labs Innovations Technical Memorandum . TM-071207, July 2007.

[12] Lloyd G. Greenwald and Tavaris J. Thomas, "Toward Undetected Operation System Fingerprint" . Proceedings of the first USENIX workshop on Offensive Technologies . Article no.6 , 2007.

[13] Nmap. [Online]. Available: http://nmap.org

ภาคผนวก

ผลงานวิจัยที่ได้รับการตีพิมพ์เผยแพร่

1. Mati Pinyathinun and Chanboon Sathitwiriyawong, **"Dynamic policy for Target based Intrusion Detection System"**, 2009 International Conference on Computer Sciences and Convergence Information Technology (ICCIT2009)

ICCIT2009

ICCIT2009: 4th ICCIT: 2009 International Conference on Computer Sciences and Convergence Information Technology

Official web site: http://www.aicit.org/ICCIT
E-mail: ICCIT@aicit.org

Receipt / Invoice

Description :

ICCIT2009, Registration and Publication Fee

The Title of the Paper(s) :

'Dynamic Policy Model for Target Based Intrusion Detection System'

The Author/Payer's Name :

Mati Pinyathinun

Total Amount :

550(USD)

Date : 2009-11-26

Signature

AICIT : Advanced Institute of Convergence Information Technology
President: Prof. Franz Ko, Ph.D.

Address: 707, Seokjang-dong, Gyeongju-si, Gyeongbuk, 780-741, Korea(Rep. of)
Registration Number: 505-10-96301

ICCIT2009

ICCIT2009: 2009 International Conference on Computer Sciences and Convergence Information Technology
Address: 707 Seokjang, Gyeongju-si, Gyeongbuk, 780-714 Korea (Rep. of)
Web site: http://www.aicit.org/iccit/, E-mail: iccit@aicit.org

AICIT : Advanced Institute of Convergence Information Technology

General Chair: Prof. Franz Ko

Certificate of Participation & Presentation

Paper Title:

Dynamic Policy Model for Target Based Intrusion Detection System

Presenter: Mati Pinyathinun

On behalf of the Organizing Committee of ICCIT2009, we want to express our special thanks to the person above for his participation and successful paper presentation in ICCIT, which took place at the Olympic Parktel , Seoul, Korea, November 24th – 26th, 2009.

General Chair of ICCIT2009

Prof. Franz Ko (Dongguk University, Korea / IBC, UK) Signature Franz Ko

AICIT

Dynamic Policy Model for Target Based Intrusion Detection System

Mati Pinyathinun
Faculty of Information Technology
King Mongkut's Institute of Technology Ladkrabang
Bangkok, Thailand 10520
+66816660898
rbx6jmz@hotmail.com

Chanboon Sathitwiriyawong
Faculty of Information Technology
King Mongkut's Institute of Technology Ladkrabang
Bangkok, Thailand 10520
+6627234911
chanboon@it.kmitl.ac.th

ABSTRACT
Network intrusion detection system (NIDS) is an important tool for network security. It observes all transmitting packets on a network system and alerts when intrusion or nearly attack situation occurs. To analyze every single packet on the network, NIDS with good performance and high accuracy can make network more secure and reliable. However, some disadvantages of NIDS, such as evasion technique and noise, can affect the accuracy of the traditional NIDS. A new approach is a target based IDS which can increase accuracy and reduce noises. This paper proposes a new method to reduce system workload and increase the accuracy of the typical target based IDS by providing flexibility of specifying policy for individual host or group.

Keywords
Intrusion Detection System, Performance, Target Based IDS.

1. INTRODUCTION
Network intrusion detection system (NIDS) is an important tool to secure network infrastructure. It automates detection by collecting data from medium and analyzes those data. If it notices security threats or abnormal behavior, it reports alert messages to the site administrators. It can also provide automatic active responses to those security threats if this feature is built into the NIDS (in case of Intrusion Prevention System or IPS).

One of the most popular NIDS is Snort - Lightweight Intrusion Detection for Networks. The lightweight IDS can be easily deployed on most network nodes, with minimal disruption to normal operations. It should also be cross-platform.

While false positive alarms are excessive and annoying, noises are alarms in which the NIDS sends an alert on a condition that is non-threatening or not applicable to the site that is being monitored. In this case, the IDS diagnoses correctly and does not make any mistake but the alarm is of questionable value [4]. False positive alarms and noises can annoy the administrator since they are not real attacks or security threats.

Some problems discovered by [6], showed the insufficiency of information obtained from the wire that can cause noises and NIDS vulnerability to evasion attacks. Another issue in IDS research [4] considers about the flexibility of signature and policy that makes NIDS more accurate.

These problems bring about a new approach of NIDS: target-based IDS. It aims for noise reduction and tries to add more information to NIDS. The concept of target based IDS is that it can diagnose the packet stream in the same perspective as the host. There are some issues in target based IDS that need an improvement.

In the performance research field, NIDS performs as a packet sniffer by analyzing all packets that are connected through the monitored network segments. Since NIDS has to handle a lot of packets, it is vulnerable to overload that can cause the administrator to miss attacks since some packets are not analyzed.

This paper proposes a new method to specify policy in Stream5 target based in Snort to improve its performance and accuracy, by reducing workload, using correct and flexible policy, and making IDS to perform less target based and less pattern matching algorithm as possible. The new approach of target based IDS should performance as close as possible to the ideal target based IDS that can perform and analyze information exactly the same perspective as targeted hosts.

2. INTRUSION DETECTION
2.1 Intrusion Detection System
An intrusion detection system (IDS) is a system that attempts to identify intrusions, which defined to be unauthorized uses, misuses, or abuses of computer systems by either authorized users or external perpetrators.

It tries to detect a suspected intrusion in the monitored system and sends alarms to system administrator. It has a few basic objectives that characterize what properties the IDS is attempting to provide.

2.1.1 The objective of IDS:
Confidentiality – ensuring that the data, system or system resources are not disclosed to unauthorized individuals, processes, or systems.

Integrity – ensuring that the data is accurate, complete, consistent, intended use, and associated with its representation.

Availability – making sure that the data and system are accessible and usable to authorized individuals and/or processes.

2.1.2 Categorize of IDS:
Host-Based Intrusion Detection System (HIDS): HIDS analyzes intrusions on a computer system, reacts on use and system behavior, activities and attacks that affect a host.

Network-Based Intrusion Detection System (NIDS): The development of network and distributed computing has led IDS to secure network by analyzing captured network traffic. NIDS monitors entire network using packet sniffer methodology without effecting network performance.

2.1.3 Basic detection approach

Anomaly detection based – diagnoses behavior for anomalies on network that is close to attacks. The basic principle is awareness that "attack behavior" differs enough from "normal user behavior", so it can detect new types of attacks that never happened before.

Signature based – detects behavior that "match" patterns of attack patterns, it is very accurate with a known attack with recently update signature but it inaccuracy when deal with uncommon attack pattern and poor performance when behavior matches multiple attack signature.

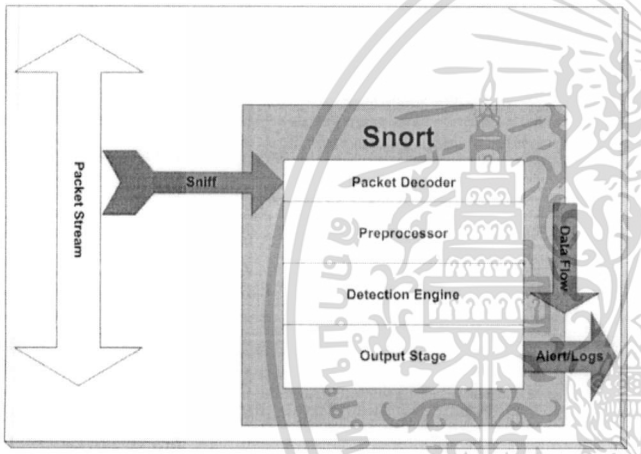


Figure 1. Basic Snort data flow.

A basic Snort data flow is shown in Figure 1. Snort is a network signature based intrusion detection system that uses packet sniffer to allow an application to eavesdrop on network traffic and send them to the preprocessor. The preprocessor allows the functionality of Snort to be extended by allowing users and programmers to put modular plug-ins into Snort. The preprocessor checks sniffed packets against certain plug-ins and sends them to the detection engine. The detection engine uses pattern matching algorithm to match packets with rules to detect intrusions. Then it sends the response or alert to the administrator if the packets match the rule.

2.2 False positives and noises

Mostly, alerts or alarms generated by IDS when a system or host has just been attacked. However, some alarms are not threatening and have no effect, but they can annoy the administrator since these alarms are useless in the IDS log. There are four conditions when IDS reacts to packet or behavior.

- True negative – IDS generates alarms when an attack occurs.
- True positive – IDS does not generate alarms to actually benign behavior.
- False negative – IDS fails to generate alarms when an attack occurs.
- False positive – IDS misdiagnoses benign behavior, or IDS makes a mistake.

Noise is an alert that IDS sends on non-threatening or non-applicable events, to hosts but IDS diagnoses them correctly. Therefore, the target host will not be affected by the attack. In general, noise resembles to false positive and true negative. Noise and false positive represent inaccuracy of IDS. IDS suffered from false positive and noise causing inaccuracy to the IDS itself.

2.3 IDS Evasion

In TCP/IP there are different implementations and complexity such as packet fragmentation, reassembly or retransmission, IDS cannot process all contents on each other hosts and its can be compromised network security.

Thomas Ptacek and Timothy Newsham showed some weaknesses of IDS [6]. There is a problem in reliability on the IDS suffered from the insufficient information on the wire. Either IDS cannot diagnose what is actually happening on network machines or host may responses other ways as IDS responses.

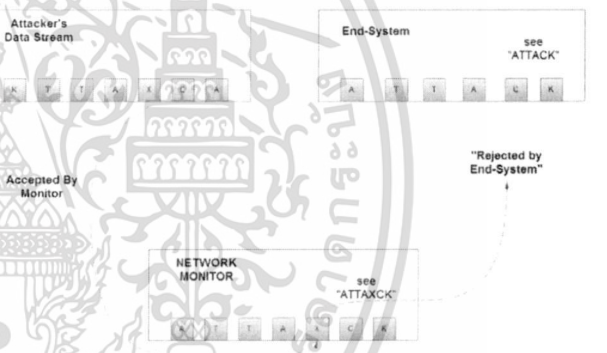


Figure 2. Insertion of the letter 'X'.

As shown in Figure 2, "Insertion" occurs when IDS accepts a packet that a target host rejects. The IDS fails to diagnose what the end-system has accepted and processes the packet that IDS does not accept. An intruder can exploit this condition by sending decoy packets among attack packets causing IDS to fail on detection then host target rejects decoy packet.

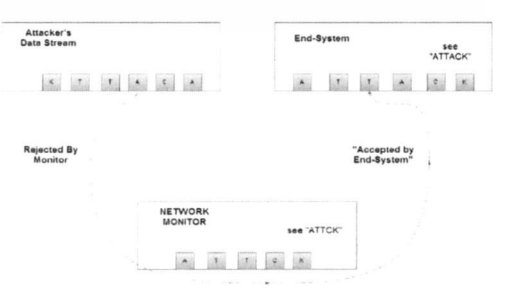


Figure 3. Evasion of the letter 'A'.

As shown in Figure 3, "Evasion" occurs when target host accepts packet that IDS has already rejected. This is the easiest way to exploit and the most destroying to the accuracy of an IDS.

Similarly, overlapping IP fragments presents a problem to an IDS/IPS because the IDS/IPS may not examine or honor the same IP fragment as the destination host. Yet, an administrator may be able to configure an IPS to drop any overlapping IP fragments.

Realistically, this should pose no problems for legitimate traffic. Completely overlapping TCP segments, however, may appear in normal traffic as a retransmission of unacknowledged data.

Basically, IDS cannot perform accurately because of all data that modified for evasion exploiting the IDS disadvantage that the information from the medium are not enough to diagnose completely. There is a gap of information between IDS detection and how the host responses to those packets.

2.4 Target based IDS

The term "Target-based IDS" means an intelligent IDS that is informed about hosts residing on the protected network. It is capable of analyzing traffic sent to those hosts as the host itself analyzing the traffic. This does not solve all of the problems discussed by Ptacek and Newsham, but it certainly improves the accuracy of the IDS.

All problems mentioned above: false positive, noise, and IDS evasion, have led IDS to a new approach: target based IDS using target policy/profile to eliminate noise and increase detection's accuracy.

Target based IDS focuses on the host target of the transiting packet as much as on the malicious signature contained within the packet. The older generation IDS, simply checked packet payload for a match with its database of malicious signatures, or figured out anomalous traffic patterns and then threw up alerts if a match or anomaly was detected.

Snort developed target based IDS as Stream5, Stream5 has ability to reassembly overlapping TCP segments by using policy the same as the host. It can configure specific TCP reassembly policy to individual hosts or networks.

2.5 Performance of typical NIDS

Commonly, the performance of a network intrusion detection system is characterized by the probability that an attack is detected in combination with the number of false alerts. However, equally important is the system's ability to process traffic at the maximum rate offered by the network with minimal packet loss.

When IDS generates an alert, it logs information to the file or database on the storage. If they are too many false alarms or noises, it will take excessive time to query log. And if it uses too much memory or resources for detection and analysis, the packet dropping rate will increase. The performance of IDS depends to a large extent on memory system [3]. These can directly affect its performance and accuracy.

3. DYNAMIC POLICY MODEL FOR TARGET BASED IDS

This paper proposes a dynamic policy model that adds realistic host information to the target based IDS in order to achieve more accurate and better performance. This model uses an agent to correlate information between firewall and IDS to make the IDS more informative.

In case of Snort Stream5 target based IDS, when IDS sniffs a packet, there is a preprocessor to handle packets that allows users or programmer to manage modular plug-ins into Snort before pattern matching occurs.

Stream5 preprocessor is an essential part of Snort target based IDS. The policy for each host or group is specified in Stream5 to offer host information such as IP address, OS, and open ports, as shown in Figure 4. Stream5 will then perform target based detection on hosts according to the specified policy. However, Stream5 needs the most current information about hosts and network specifications to perform intrusion detection accurately.

```
preprocessor stream5_global: track_tcp yes
preprocessor stream5_tcp: bind_to 192.168.1.0/24, policy windows
preprocessor stream5_tcp: bind_to 10.1.1.0/24, policy linux
preprocessor stream5_tcp: policy solaris
```

Figure 4. Snort Stream5 configuration.

In a situation that Stream5 has inappropriate policy, every elements of Stream5 policy can be monitored. Stream5 preprocessor will trigger stream reassembly and state tracking.

In another way, pattern matching algorithm in IDS performs after preprocessing. It will perform the pattern matching using information from preprocessors and the rule or signature.

In dept Snort Stream5 performs both target based and stream reassembly which performs detection of every port in the policy configuration, and tries to illustrate the same perspective as target hosts. This will slightly increase the workload because unnecessary detection is worthless and detection on ports that do not exist or have already closed. The protection by host's firewall has no effect when intruders try to attack.

In this case port scanner cannot be used because it can perform only active ports on those hosts. Ports that are not attended or not currently used will not be detected. For these reasons, the solution approach is to use host's firewall to identify the exactly ports on each host to reconfigure the Stream5 new policy and fulfill information that might improve Stream5 performance and accuracy.

We propose a dynamic policy model for Stream5 by reconfiguring its preprocessor with dynamic targets port. Figure 5 is the flowchart depicting the procedures of this model.

Since Snort configuration file is fixed, the Stream5 policy will not correspond to current online hosts. Therefore, we use firewall rule information from target host to reconfigure the Stream5 policy. From the above model we can reconfigure the Stream5 policy by interpreting firewall rules set. Therefore, the workload of IDS can be reduced since closed ports can be ignored.

This model needs an agent to retrieve port information from firewall and apply to target based policy. Information that has to be added for the flexibility of Stream5 is the open ports on each host. In Stream5 policy is fixed. We get port information from firewall rules because port scanner can detect only ports that are currently active.

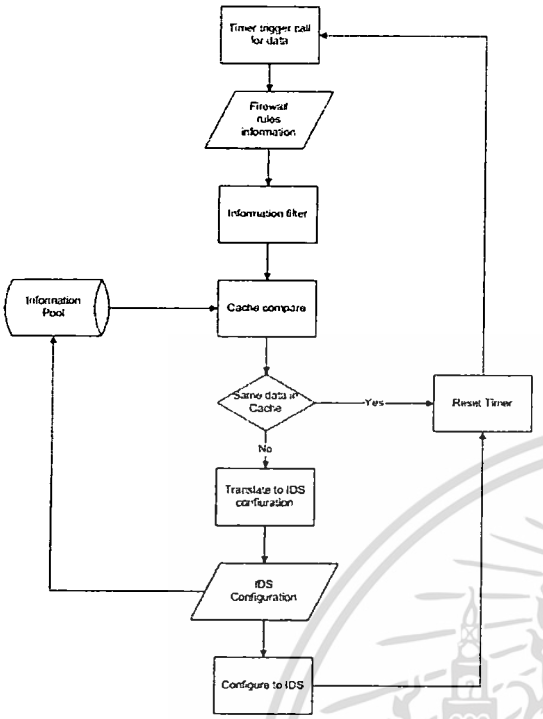


Figure 5. Dynamic policy dataflow.

All information need to be filtered and use only open ports from each host and translate to Stream5 configuration then check with cache to compare information from the last process. If hosts information does not change, there is no reason to update again. The new updated information will be stored in cache for comparing with the next loop of the process and send to Stream5 policy for reconfiguration.

We use a timer to adjust appropriate looping time, which can slightly affect the network performance. According to our model, the performance of IDS can be improved by eliminating all unused ports and increasing range of detection when a new host port is open.

To improve performance, accuracy and flexibility of target based IDS, only real host information is provided to Stream5 policy because they affect both accuracy and performance at the same time. It makes IDS more accurate to every kind of hosts if there is an agent that can feed host information correctly and continually.

Its performance is improved since IDS detects only policy that matches existing hosts. Closed port should not be diagnosed if it has a good policy. To have efficient policy in Stream5, we need third parties or some add-ons to manage the policy. Firewall information is important for this model to assign open ports to IDS.

4. CONCLUSION

This paper proposes a dynamic policy model for target based IDS that improve its performance and accuracy by providing flexibility and feeding more information to the Stream5 target based IDS. The proposed model uses an agent to manage the correlation between firewall and IDS since some information can fulfill Stream5 policy, such as open ports from the personal firewall. It makes Stream5 more flexible to detect and obtain informative host profile. Therefore, it can increase the accuracy and reduce the workload of analyzing those unused port in Stream5 policy. However, transferring firewall information via the network is of a great concern since it should not have much affect to the network performance. In the future work, this issue will be experiment for optimal traffic and try to get other information or correlate with other network device to improve target based IDS.

5. REFERENCES

[1] Puketza, N. J., Zhang K. and Chung, M. 1996. A Methodology for Testing Intrusion Detection Systems. In IEEE Transactions on Software Engineering, Vol. 22, No.10, 719-729.

[2] Novak, J. and Sturges, S. 2007. Target-Based TCP Timestamp Stream Reassembly, Sourcefire, Inc.

[3] Schaelicke, L., Slabach, T., Moore, B. and Freeland, C. 2003. Characterizing the Performance of Network Intrusion Detection Sensors, In Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection (RAID 2003), Springer-Verlag, Berlin - Heidelberg - New York, 155-172.

[4] Ranum, M. J. 2003. False Positives: A User's Guide to Making Sense of IDS Alarms, ICSA Labs IDSC.

[5] Ranum, M. J. 2001. Experiences Benchmarking Intrusion Detection Systems, Technical Report, NFR Security, Inc.

[6] Ptacek, T. and Newsham, T. 1998. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection System, Technical Report, Secure Networks, Inc.

[7] Roesch, M. 1999. Snort - Lightweight Intrusion Detection for Networks, In Proceedings of the 13th Systems Administration Conference (Seattle, WA, November 7-12, 1999), 229-238.

[8] Debar, H., Dacier, M. and Wespi, A. 1999. Towards a Taxonomy of Intrusion-detection Systems. Computer Networks, Vol. 31, 805-822.

[9] Novak, J. and Sturges, S. 2007. Target-Based TCP Stream Reassembly, Sourcefire, Inc.

[10] Novak, J. 2005. Target-Based Fragmentation Reassembly, Sourcefire, Inc.

ประวัติผู้เขียน

นายมติ ภิญญาธินันท์ เกิดเมื่อ 31 มีนาคม พ.ศ. 2526 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาปริญญาตรีวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ จากคณะวิทยาศาสตร์ มหาวิทยาลัยหอการค้าไทย ในปีการศึกษา 2547

จากนั้นเข้าศึกษาต่อในระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต (วท.ม) สาขาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2548