การเปรียบเทียบโปรแกรมตรวจหาการบุกรุกเครือข่าย
ระหว่างโปรแกรมสนอร์ทและเรียลซีเคียวภายใต้ปัจจัยการโจมตี

นางสาว กาญจนา ศิลาวราเวทย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2545

ISBN 974-17-2386-5

THE COMPARISON OF NETWORK INTRUSION DETECTION SYSTEM BETWEEN SNORT AND REALSECURE UNDER ATTACK

Miss Kanchana Silawarawet

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Computer Science
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2002

ISBN 974-17-2386-5

หัวข้อวิทยานิพนธ์	การเปรียบเทียบโปรแกรมตรวจหาการบุกรุกเครือข่าย ระหว่างโปรแกรมสนอร์ทและเรียลซีเคียวภายใต้ปัจจัยการโจมตี
โดย	น.ส.กาญจนา ศิลาวราเวทย์
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร. ณัฐวุฒิ หนูไพโรจน์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดี คณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.สมศักดิ์ ปัญญาแก้ว)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... อาจารย์ที่ปรึกษา
(อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์)

..... กรรมการ
(อาจารย์ จารุมาตร ปิ่นทอง)

..... กรรมการ
(อาจารย์ ดร.ชัย พงศ์พันธุ์ภาณี)

กาญจนา ศิลาวราเวทย์ : การเปรียบเทียบโปรแกรมตรวจหาการบุกรุกเครือข่ายระหว่างโปรแกรมสนอร์ทและเรียลซีเคียวภายใต้ปัจจัยการโจมตี. (THE COMPARISON OF NETWORK INTRUSION DETECTION SYSTEM BETWEEN SNORT AND REALSECURE UNDER ATTACK) อ. ที่ปรึกษา : ดร.ณัฐวุฒิ หนูไพโรจน์, 87 หน้า. ISBN 974-17-2386-5.

ระบบตรวจหาการบุกรุกถูกนำมาใช้ค้นหาสัญญาณที่บ่งบอกถึงการบุกรุกหรือการโจมตีที่เกิดขึ้น จากการศึกษาค้นคว้างานวิจัยด้านการทดสอบการตรวจหาการบุกรุกพบว่างานวิจัยส่วนใหญ่เกี่ยวข้องกับวิธีการสร้างเกณฑ์เปรียบเทียบ การปรับปรุงและทดสอบการทำงานของอัลกอริทึมที่ใช้ในการค้นหารูปแบบการบุกรุก ซึ่งงานวิจัยเหล่านั้นเป็นการทดสอบในเชิงทฤษฎีและยังไม่พบการทดสอบการทำงานของระบบตรวจหาการบุกรุกเครือข่ายในสภาพแวดล้อมที่เกี่ยวข้องกับปัจจัยด้านการโจมตี

ในงานวิจัยนี้เป็นการทดสอบเพื่อเปรียบเทียบการทำงานของโปรแกรมตรวจหาการบุกรุกเครือข่ายระหว่างโปรแกรมสนอร์ทและเรียลซีเคียวภายใต้ปัจจัยการโจมตีในเครือข่ายปิด โดยทำการทดสอบในหลายสภาพแวดล้อมและใช้การโจมตีที่พบบ่อยในปัจจุบัน

จากการทดสอบและเปรียบเทียบพบว่าโปรแกรมตรวจหาการบุกรุกทั้งสองมีพฤติกรรมในการทำงาน ความสามารถในการตรวจวิเคราะห์และการใช้งานซีพียูใกล้เคียงกัน จะมีความแตกต่างกันเล็กน้อยในเรื่องของเวลาที่ใช้ในการตรวจวิเคราะห์และความผิดพลาดในการแจ้งเตือนที่โปรแกรมสนอร์ททำงานได้ดีกว่า ส่วนโปรแกรมเรียลซีเคียวมีความถูกต้องของการแจ้งเตือนมากกว่า นอกจากนี้ยังพบว่าการโจมตีและข้อมูลปะปนส่งผลกระทบทำให้ความสามารถในการทำงานของทั้งสองโปรแกรมลดลง ความผิดพลาดในการแจ้งเตือนจึงสูงขึ้น ซึ่งผลจากงานวิจัยนี้สามารถใช้เป็นแนวทางในการทดสอบโปรแกรมตรวจหาการบุกรุกอื่นได้

ภาควิชา....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต.....
สาขาวิชา...วิทยาศาสตร์คอมพิวเตอร์....ลายมือชื่ออาจารย์ที่ปรึกษา……...
ปีการศึกษา…2545…

4371404021 : MAJOR COMPUTER SCIENCE

KEY WORD: INTRUSION DETECTION SYSTEM

KANCHANA SILAWARAWET : THE COMPARISON OF NETWORK INTRUSION DETECTEION SYSTEM BETWEEN SNORT AND REALSECURE UNDER ATTACK. THESIS ADVISOR : NATAWUT NUPAIROJ, Ph.D., 87 pp.

ISBN 974-17-2386-5.

Network Intrusion Detection System has been used to find the signal that reflects intrusion or attack. According to our studies in existing intrusion detection research, we found that most studies focus in comparing, improving, and testing the intrusion detection algorithms. These researches are theoretical and usually ignore the study in the environment with actual attack.

This research is to compare performance of intrusion detection software between SNORT and RealSecure under actual attacks in isolated local area network. Our studies have been conducted in various environments using attacks commonly found in the real world. The results of our experiments indicated that both software share similar performances and characteristics, as well as, CPU utilization. There are slightly differences in response time and accuracy. SNORT can detect faster but RealSecure is more accurate. Moreover, the performances of both systems decrease when being used in environments with multiple attacks and background data. Fault alerts become higher. The results from our studies can be used as a guideline for testing other intrusion detection systems in the future.

Department.….Computer..Engineering....Student's signature .....…….
Field of study…Computer..Science.....Advisor's signature.....…….
Academic year .....2002.....

กิตติกรรมประกาศ

ขอขอบคุณอาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์ และอาจารย์ในภาควิชาฯ ทุกท่านที่ให้ความกรุณา เสียสละเวลาให้คำปรึกษา และให้ความช่วยเหลือเป็นอย่างดีในการทำวิจัยครั้งนี้

ขอขอบคุณพี่ๆ เพื่อน และน้องทุกคนที่เป็นกำลังใจ ให้คำแนะนำต่างๆ

สุดท้ายนี้ขอขอบพระคุณบิดา มารดา และครอบครัวที่ให้การสนับสนุนและเป็นกำลังใจเสมอมา

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ระบบตรวจหาการบุกรุกถูกนำมาใช้เพื่อเพิ่มสมรรถนะให้แก่ระบบรักษาความปลอดภัย และเพิ่มความต้านทานต่อการโจมตีทั้งจากภายในและภายนอกระบบ โดยทำหน้าที่ค้นหาสัญญาณที่บ่งบอกถึงการบุกรุก บอกถึงการโจมตีที่เกิดขึ้น[1] และบอกถึงกิจกรรมที่เป็นเครื่องหมายแสดงถึงการโจมตีร้ายแรง ระบบตรวจหาการบุกรุกที่ดีควรมีความผิดพลาดในการทำงานเพียงเล็กน้อย ตัวอย่างเช่น การแจ้งเตือนเกินความเป็นจริง หรือการไม่แจ้งเตือนเมื่อถูกโจมตี ซึ่งปัจจัยภายนอกที่มีผลต่อการทำงานของระบบตรวจหาการบุกรุกเครือข่าย ได้แก่ เทคนิคที่ใช้ในการตรวจหาและสภาพแวดล้อมของระบบที่ต้องการตรวจหา เช่น ปริมาณการโจมตี ปริมาณข้อมูลในเครือข่าย จำนวนผู้ใช้งาน ความหลากหลายของการโจมตี เป็นต้น ซึ่งปัจจัยเหล่านี้อาจส่งผลกระทบให้ระบบตรวจหาการบุกรุกที่เคยทำงานได้ดีในระบบหนึ่งประสบความล้มเหลวในการตรวจหาการบุกรุกในอีกระบบหนึ่ง [2] ดังนั้นการเลือกใช้ระบบตรวจหาการบุกรุกที่มีเหมาะสมกับสภาพแวดล้อม จึงมีผลต่อความถูกต้องในการตรวจหาและช่วยให้ตรวจพบการบุกรุกก่อนที่ผู้บุกรุกจะโจมตีระบบสำเร็จ

งานวิจัยด้านการทดสอบในการตรวจหาการบุกรุกส่วนใหญ่เกี่ยวข้องกับวิธีการสร้างเกณฑ์เปรียบเทียบ[3] การปรับปรุงและทดสอบการทำงานของอัลกอริทึมที่ใช้ในการค้นหารูปแบบการบุกรุก[4] การออกแบบอัลกอริทึมเพิ่มเติมเพื่อตรวจหาการโจมตีที่ต้องการ[5] ซึ่งเป็นการทดสอบในเชิงทฤษฎีและยังไม่พบการทดสอบการทำงานของระบบตรวจหาการบุกรุกเครือข่ายในสภาพแวดล้อมที่เกี่ยวข้องกับปัจจัยด้านการโจมตี ดังนั้นในงานวิจัยนี้จึงเสนอแนวคิดในการวัดทดสอบระบบตรวจหาการบุกรุกเครือข่าย เพื่อศึกษาพฤติกรรมและความสามารถในการตรวจหาในสภาพแวดล้อมของเครือข่ายปิดที่มีการเปลี่ยนแปลงปัจจัยด้านการโจมตี โดยจะทำการทดสอบและเปรียบเทียบโปรแกรมตรวจหาการบุกรุกเครือข่ายที่ใช้เทคนิคการตรวจหาตามเงื่อนไขระหว่างโปรแกรมสนอร์ท (Snort) และเรียลซีเคียว (RealSecure)

1.2 วัตถุประสงค์ของการวิจัย

เพื่อทดสอบและเปรียบเทียบโปรแกรมตรวจหาการบุกรุกเครือข่ายที่ใช้วิธีการตรวจหาตามเงื่อนไขระหว่างโปรแกรมสนอร์ทและเรียลซีเคียวภายใต้ปัจจัยการโจมตี

1.3 ขอบเขตของการวิจัย

1.3.1 ทดสอบโปรแกรมตรวจหาการบุกรุกเครือข่ายที่ใช้วิธีการตรวจหาตามเงื่อนไขระหว่างโปรแกรมสนอร์ทและเรียลซีเคียว

1.3.2 ทำการตรวจหาเฉพาะการบุกรุกที่เกิดจากพฤติกรรมการใช้งานผิดปกติ (Misuse Detection) และการบุกรุกที่ก่อให้เกิดผลกระทบต่อระบบในทันที (Active Intrusion)

1.3.3 การโจมตีที่ใช้ในการทดลองประกอบด้วยการโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมาก (SYN Flood) การโจมตีด้วยกลุ่มข้อมูลจำนวนมาก (Ping Flood) การโจมตีด้วยการกราดตรวจทีซีพีพอร์ต (Scan TCP Port) และการโจมตีด้วยการส่งกลุ่มข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์ (Smurf)

1.3.4 ทำการทดสอบภายในระบบปิดที่ไม่มีการอิ่มตัวของเครือข่าย โดยทำการทดสอบในสภาพแวดล้อม 3 แบบ ได้แก่ สภาพแวดล้อมของการโจมตีชนิดเดียว สภาพแวดล้อมของการโจมตีชนิดเดียวมีข้อมูล และสภาพแวดล้อมของการโจมตีหลายชนิดผสมกัน

1.3.5 ใช้เวลาในการทดลองครั้งละ 10 นาทีและทำการทดลองซ้ำ 2 ครั้ง

1.3.6 การวิเคราะห์จะวัดจากความสามารถในการตรวจวิเคราะห์ เวลาที่ใช้ในการตรวจพบการโจมตี การแจ้งเตือนเกินจริง การไม่แจ้งเตือนเมื่อถูกโจมตี ความถูกต้องของการแจ้งเตือน การใช้งานซีพียู

1.3.7 การเปลี่ยนแปลงอัตราเร็วในการโจมตีบนสภาพแวดล้อมที่มีการโจมตีเพียงชนิดเดียวและสภาพแวดล้อมที่มีการโจมตีปะปนกับข้อมูลจะทำการทดลองโดยส่งการโจมตีจากผู้โจมตีเดียวกันสูงสุด 3 เซสชัน (Session) และจากหลายผู้โจมตีพร้อมกันสูงสุด 3 เครื่อง

1.4 คำจำกัดความที่ใช้ในการวิจัย

ระบบตรวจหาการบุกรุกเครือข่าย (Network Intrusion Detection) การโจมตีเครือข่าย (Network Attack) การบุกรุกที่ก่อให้เกิดผลกระทบต่อระบบทันที (Active Intrusion) การบุกรุกตามลำดับ (Sequential Intrusion) การบุกรุกพร้อมกัน (Concurrent Intrusion) การโจมตีด้วยกลุ่มข้อมูลจำนวนมาก (Ping Flood) การกราดตรวจทีซีพีพอร์ต (TCP Port Scan) การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมาก (SYN Flood) และการโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์ (Smurf)

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 เป็นข้อมูลอ้างอิงใช้ในการเปรียบเทียบระบบตรวจหาการบุกรุกที่ใช้วิธีการตรวจหาตามเงื่อนไขระหว่างโปรแกรมสนอร์ทและเรียลซีเคียว

1.5.2 เป็นข้อมูลแสดงความสามารถและพฤติกรรมในการรองรับการโจมตีของระบบตรวจหาการบุกรุก

1.5.3 เป็นข้อมูลแสดงความสัมพันธ์ระหว่างความถูกต้องในการตรวจหากับอัตราเร็วในการโจมตี

1.5.4 เป็นต้นแบบในการสร้างเงื่อนไขทดสอบระบบตรวจหาการบุกรุก

1.6 วิธีดำเนินการวิจัย

1.6.1 ศึกษาการทำงานของระบบตรวจหาการบุกรุกและรูปแบบของการบุกรุก

1.6.2 วิเคราะห์ข้อบกพร่องของระบบเครือข่ายและปัญหาที่เกิดขึ้น

1.6.3 ออกแบบการทดลองและสคริปต์ที่ใช้สร้างการโจมตี

1.6.4 ทำการทดสอบระบบตรวจหาการบุกรุก

1.6.5 บันทึกและวิเคราะห์ผลการตรวจหาการบุกรุก

1.6.6 สรุปผลการทดลองและจัดทำรายงานวิทยานิพนธ์

บทที่ 2

แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในบทนี้กล่าวถึงทฤษฎีเกี่ยวกับการบุกรุกระบบ แหล่งที่มาของผู้บุกรุก ประเภทของการบุกรุกระบบ ประเภทของการโจมตี การทำงานของระบบตรวจหาการบุกรุก การทดสอบระบบตรวจหาการบุกรุก เกณฑ์ความต้องการของระบบตรวจหาการบุกรุก โปรแกรมตรวจหาการบุกรุกสนอร์ทและเรียลซีเคียว นอกจากนี้ยังกล่าวถึงงานวิจัยที่เกี่ยวข้องกับการวัดประสิทธิภาพระบบตรวจหาการบุกรุก

2.1 การบุกรุกระบบ (Intrusion Detection)

การบุกรุกระบบเป็นการลักลอบเข้าใช้ระบบ เข้าถึงข้อมูลที่เป็นความลับ เข้าทำลายข้อมูล หรือก่อกวนการให้บริการของระบบ การบุกรุกโดยผู้บุกรุกหรือผู้โจมตีส่งผลกระทบ 2 แบบ คือ ผลกระทบที่เกิดขึ้นทันทีที่มีการบุกรุก เช่น การส่งข้อมูลจำนวนมากเพื่อขัดขวางการให้บริการ และผลกกระทบที่เกิดขึ้นในภายหลังการบุกรุก เช่น การลักลอบขโมยข้อมูล จากผลกระทบดังกล่าวจึงแบ่งประเภทของผู้ลักลอบเข้าใช้ระบบออกเป็น 2 ประเภท คือ

2.1.1 ผู้บุกรุกเป็นบุคคลที่ไม่ต้องการให้ใช้ระบบแต่พยายามเข้าใช้ระบบ ได้แก่ บุคคลที่เข้าใช้ระบบโดยที่ตนเองไม่มีสิทธิ์ บุคคลที่มีสิทธิ์เข้าใช้ระบบแต่ใช้สิทธิ์ไปในทางที่ผิด หรือบุคคลที่เข้าใช้ระบบเกินสิทธิ์ของตนเอง โดยมีเป้าหมายเพื่อเข้าใช้ข้อมูลในระบบ ลักลอบดูข้อมูล ทำลายข้อมูล หรือใช้ประโยชน์จากข้อมูลและการให้บริการของระบบ

2.1.2 ผู้โจมตีเป็นบุกรุกที่มีเจตนาก่อกวนการให้บริการเพื่อเข้าใช้ข้อมูล โดยจะค้นหาข้อมูลการให้บริการต่างๆ แล้วเข้าใช้ข้อมูลและการบริการนั้นๆ หลังจากเข้าโจมตีระบบจะพยายามปลอมตัวหลบหนีจากการตรวจหา ในบางครั้งจะสร้างประตูหลัง (Backdoor) ไว้สำหรับการเข้าระบบครั้งต่อไป

2.2 แหล่งที่มาของผู้บุกรุก

ผู้บุกรุกที่เข้าสู่ระบบมีที่มา 2 แหล่ง คือ ผู้บุกรุกที่มาจากภายนอกระบบและผู้บุกรุกจากภายในระบบเอง

2.2.1 ผู้บุกรุกจากภายนอก (External Penetrates) เป็นผู้เข้าใช้ระบบจากระยะไกลที่ไม่ได้รับสิทธิ์ในการเข้าใช้ระบบ แต่เข้าสู่ระบบโดยผ่านเครือข่ายระยะไกล หรือเชื่อมต่อผ่านบริษัทคู่ค้า เพื่อมุ่งโจมตีการให้บริการภายในเครือข่าย

2.2.2 ผู้บุกรุกจากภายใน (Internal Penetrates) เป็นผู้ที่ได้สามารถเข้าใช้ระบบภายในเครือข่ายได้โดยตรง ส่วนใหญ่จะเป็นคนในองค์กรที่ลักลอบใช้งานเกินสิทธิ์ หรือใช้สิทธิ์ไปในทางที่ผิด (Misuse Privileges) ซึ่งการบุกรุกประเภทนี้ประกอบด้วย ผู้บุกรุกที่ใช้อุปกรณ์หรือคอมพิวเตอร์ในระบบ (Physical Intrusion) บุกรุกเข้าระบบในเครือข่ายเดียวกัน โดยส่วนมากจะเป็นผู้ที่สามารถเข้าใช้ระบบได้แต่มีสิทธิในการเข้าใช้น้อย จึงพยายามเปลี่ยนสิทธิ์ของตนเองให้เป็นผู้ดูแลระบบหรือผู้ที่มีสิทธิ์มากกว่า

2.3 **ประเภทของการบุกรุกระบบ** (System Intrusion Type)

รูปแบบที่ใช้ในการบุกรุกระบบเป็นวิธีการที่ช่วยเพิ่มประสิทธิภาพในการบุกรุกและช่วยเบี่ยงเบนความสนใจของระบบตรวจหา รูปแบบในการบุกรุกจึงนิยมใช้เพื่อซ่อนตรวจหา และมีส่วนช่วยทำให้การบุกรุกประสบผลสำเร็จมากยิ่งขึ้น การบุกรุกสามารถแบ่งได้ 2 ประเภทคือ การบุกรุกตามลำดับ (Sequential Intrusion) และการบุกรุกพร้อมกัน (Concurrent Intrusion)

2.4 **ประเภทของการโจมตี** (Attack Type)

การโจมตี เป็นการกระทำที่มีเป้าหมายเพื่อก่อกวนการให้บริการของระบบ ค้นหาการให้บริการของระบบในเบื้องต้น บุกรุกหรือทำลายระบบโดยอาศัยข้อบกพร่องของระบบ การโจมตีแบ่งตามวัตถุประสงค์ของผู้โจมตีได้ 3 ประเภท ได้แก่ การสำรวจระบบหาข้อมูลการให้บริการเบื้องต้น การโจมตีโดยใช้ประโยชน์จากข้อผิดพลาดของระบบและการก่อกวนการให้บริการของระบบ

2.4.1 **<u>การสำรวจระบบหาข้อมูลการให้บริการ (Reconnaissance Scans)</u>**

เป็นการค้นหาข้อมูลและเป้าหมายในการโจมตี นิยมใช้วิธีการกราดตรวจ (Scan) ระบบ การโจมตีที่ใช้เทคนิคนี้ ได้แก่

ก. การกราดตรวจด้วยการใช้คำสั่งปิง (Ping Sweeps) ไปยังช่วงเลขที่อยู่ไอพี เป็นการค้นหาว่ามีเครื่องใดบ้างที่เชื่อมต่อกับเครือข่าย

ข. การตรวจสอบทีซีพีพอร์ต (TCP Port) เพื่อค้นหาการให้บริการที่ผู้บุกรุกต้องการ นิยมใช้การกราดตรวจทีซีพี (TCP Scan) สามารถทำได้ทั้งการกราดตรวจแบบปกติ เช่น การกราดตรวจการเชื่อมต่อทีซีพี หรือลักลอบกราดตรวจด้วยการเชื่อมต่อครึ่งอัตรา (Half Connection) ซึ่งทั้งหมดที่กล่าวมานี้สามารถกำหนดรูปแบบการกราดตรวจเป็นแบบตามลำดับ แบบสุ่ม หรือกราดตรวจตามพอร์ตที่ต้องการ

ค. การค้นหาข้อมูลของโพรโทคอลที่ไม่มีข้อกำหนดของการเชื่อมต่อ (Connectionless) หรือการกราดตรวจยูดีพี (UDP Scan) ด้วยการจัดส่งกลุ่มข้อมูลยูดีพี (UDP Packet) ที่มีข้อมูลขยะไปยังพอร์ตที่ต้องการ เมื่อเครื่องปลายทางได้รับข้อมูลจะต้องตอบกลับมาด้วยโพรโทคอลไอซีเอ็มพี (ICMP Protocol)

ง. การค้นหารายละเอียดของเป้าหมาย (OS Identification Scan) ซึ่งเป็นการค้นหาข้อมูลเกี่ยวกับระบบปฏิบัติการ เพื่อให้เกิดความแม่นยำและเพิ่มสมรรถนะการโจมตี โดยการลักลอบส่งไอซีเอ็มพีหรือกลุ่มข้อมูลทีซีพีไปยังเครื่องเป้าหมาย ซึ่งปกติเครื่องที่ได้รับกลุ่มข้อมูลไอซีเอ็มพี จะส่งกลุ่มข้อมูลที่ถูกต้องไปยังอินพุตที่ถูกต้อง แต่ในกรณีนี้ระบบปฏิบัติการจะตอบสนองต่ออินพุตที่ไม่ถูกต้องด้วยรูปแบบที่ผู้เจาะระบบสามารถนำไปวิเคราะห์ได้ว่าเป็นระบบปฏิบัติการใด การค้นหาข้อมูลในลักษณะนี้จะถือว่าเป็นการค้นหาข้อมูลในระดับต่ำเพราะระบบไม่สามารถจัดการได้

จ. การค้นหาบัญชีผู้ใช้และรหัสผ่าน (Account Scan) เป็นความพยายามที่จะเข้าสู่ระบบโดยผ่านบัญชีผู้ใช้ที่ไม่ได้กำหนดรหัสผ่าน ผู้ใช้ที่ใส่รหัสผ่านที่เหมือนกับชื่อผู้ใช้ ชื่อผู้ใช้ที่เป็นมาตรฐานที่มากับผลิตภัณฑ์หรือได้มาตอนลงโปรแกรม และการใช้เอฟทีพีแบบนิรนาม (Anonymous FTP) เมื่อเข้าสู่ระบบได้แล้วจึงพยายามเปลี่ยนสิทธิ์ของตนเองให้เป็นราก (Root)

2.4.2 <u>การโจมตีความผิดพลาดของระบบ (Common Exploit)</u>

ผู้บุกรุกจะอาศัยความสามารถที่ถูกซ่อนไว้หรือใช้ข้อผิดพลาดของระบบเป็นโอกาสในการโจมตีระบบ เทคนิคของการโจมตีประเภทนี้ ได้แก่

ก. การโจมตีเครื่องบริการเว็บ (Web Server Attacks) ตรวจพบจากข้อผิดพลาดในการโต้ตอบกับสิ่งที่ทำงานภายใต้ระบบปฏิบัติการที่ต่างรุ่นกัน ตัวอย่าง เช่น ความยาวของชื่อไฟล์ ในระบบปฏิบัติการรุ่นเก่ากำหนดรูปแบบชื่อไฟล์ความยาว 8 ตัวอักษร นามสกุลยาว 3 ตัวอักษร แต่ในระบบปฏิบัติการในปัจจุบันกำหนดให้ชื่อไฟล์ยาวได้ไม่จำกัด ซึ่งระบบไฟล์ที่

ต่างกันมีผลต่อการกำหนดสิทธิ์การเข้าใช้ หรือในกรณีที่ความยาวของชื่อยูอาร์แอล (URL) ยาวกว่าปกติ (Death of Thousand Slashes) เมื่อหน่วยประมวลผลพบยูอาร์แอลชนิดนี้จะต้องประมวลผลทีละสารระบบ (Directory) ของเครื่องหมาย Slashes จึงทำให้หน่วยประมวลผลทำงานหนักขึ้น

ข. การโจมตีเว็บเบราว์เซอร์ (Web Browser Attacks) ซึ่งเบราว์เซอร์จากบริษัทไมโครซอฟต์ และเนสเคปยังคงมีช่องโหว่ในเรื่องความปลอดภัยอยู่ ตัวอย่างของโจมตีประเภทนี้ เช่น การโจมตีขณะตีความส่วนหัวของเอชทีทีพี (HTTP Header) ก่อนที่จะแสดงผลซึ่งทำให้เกิดปัญหาการล้นออกจากบัฟเฟอร์ (Buffer Overflow) การโจมตีจาวาสคริปต์ด้วยการใช้ฟังก์ชันการบรรจุไฟล์ขึ้น (Upload File) ที่ซ่อนปุ่มตกลงโดยอัตโนมัติไว้ การโจมตีกรอบข้อความ (Frame) ซึ่งเป็นส่วนหนึ่งของจาวาสคริปต์ด้วยการเชื่อมโยง (Link) ลงในกรอบข้อความแล้วแทนที่กรอบข้อความเดิมด้วยเว็บเพจ (Web Page) ของตนเอง

ค. การโจมตีด้วยการปลอมไอพี (IP Spoofing) ในขณะที่เครื่องต้นทางส่งกลุ่มข้อมูลไอพี (IP Packet) ไปยังเครื่องบริการ โดยผู้บุกรุกที่แอบอ้างเป็นเครื่องต้นทาง แล้วทำการติดต่อกับเครื่องบริการแทน เมื่อเครื่องบริการส่งสัญญาณตอบกลับมาผู้บุกรุกจะไม่รับ เนื่องจากไม่ตรงกับการร้องขอ (Request) แต่จะยังคงแอบอ้างเป็นเครื่องนั้น ตัวอย่างเช่น การโจมตีด้วยการจัดส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์ (Smurf) เป็นการกระจายปิง (Ping) จากเครื่องที่แอบอ้างขึ้นจะทำให้เกิดโอเวอร์โหลด (Overload) ที่เครื่องเป้าหมายหรือเครือข่ายได้

ง. การโจมตีที่ทำให้เกิดการล้นออกจากบัฟเฟอร์ ตัวอย่างเช่น การจัดส่งชื่อโดเมนที่มีความยาวเกินกว่าปกติ ซึ่งมีความยาว 64 ไบต์ต่อส่วนโปรแกรมย่อย (Subcomponent) และยาวไม่เกิน 256 ไบต์ ไปให้เครื่องบริการ

2.4.3 <u>การก่อกวนการให้บริการของระบบ (Denial of Service Attack)</u>

ส่วนใหญ่จะอาศัยข้อบกพร่องของโพรโตคอลประกอบกับข้อบกพร่องของระบบปฏิบัติการที่ทำงานอยู่บนเป้าหมาย การโจมตีประเภทนี้จะส่งผลกระทบอย่างรุนแรงต่อการทำงาน เทคนิคของการโจมตีประเภทนี้ได้แก่

ก. การโจมตีด้วยกลุ่มข้อมูลจำนวนมาก (Ping Flood) [9] เป็นการโจมตีด้วยการส่งการสะท้อนการร้องขอไอซีเอ็มพี (ICMP Echo Request) เป็นจำนวนมากไปยังเป้าหมายอย่างรวดเร็ว ทำให้เป้าหมายที่ถูกโจมตีต้องตอบสนองด้วยการสะท้อนการตอบกลับของไอซีเอ็มพี

(ICMP Echo Reply) ตลอดเวลา ซึ่งความรุนแรงของการโจมตีจะมากหรือน้อยแปรผันตามความเร็วของการส่งกลุ่มข้อมูลไอซีเอ็มพีเป็นหลัก นอกจากการสร้างความเสียหายให้กับเครื่องเป้าหมายแล้ว การโจมตีลักษณะนี้ยังสร้างความเสียหายแก่เครือข่ายที่เครื่องคอมพิวเตอร์เป้าหมายตั้งอยู่ด้วย ปัจจัยสำคัญที่ทำให้การโจมตีสัมฤทธิ์ผลคือ แบนด์วิดท์ (Bandwidth) ของนักเลงคอมพิวเตอร์ (Hacker) หากมีแบนด์วิดท์น้อยจะไม่เกิดผล

ข. การโจมตีโดยใช้ข้อบกพร่องของการแตกกระจาย (Fragmentation) หรือการโจมตีด้วยการส่ง Ping ไม่สิ้นสุด (Ping of Death) ปกติไอพีเดทาแกรม (IP Datagram) ในกลุ่มข้อมูลเดียวจะมีขนาดสูงสุดได้ไม่เกิน 65535 ไบต์ เพราะถูกจำกัดความยาวสูงสุดไว้ เมื่อส่งเดทาแกรมจะมีขนาดเกิน 65535 ไบต์จะเกิดการแตกกระจาย ซึ่งเป็นการนำหลายๆ กลุ่มข้อมูลมาต่อรวมกันเป็นเดทาแกรมเดียวกัน ทำให้ผลรวมของการแตกกระจายมีขนาดเกินกว่า 64 กิโลไบต์ ซึ่งอยู่ในหน่วยความจำส่วนที่ระบบปฏิบัติการจัดสรร จึงเกิดการล้นของข้อมูลออกมานอกหน่วยความจำที่จัดสรรไว้ เมื่อข้อมูลที่เกินออกมาไปตกในตำแหน่งของโปรแกรมอื่นที่ใช้งานอยู่จะทำให้โปรแกรมนั้นทำงานเพี้ยน หากข้อมูลส่วนเกินไปทับหน่วยความจำของระบบปฏิบัติการทำให้ระบบปฏิบัติการไม่สามารถทำงานได้อย่างถูกต้องและจะหยุดทำงานทันที (Crash)

ค. การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมาก (SYN Flood) ทำงานโดยอาศัยคุณสมบัติของทีซีพีที่เรียกว่าการจับมือ 3 ทาง (3 Way Handshake) โดยเริ่มต้นจากเครื่องต้นทางที่ต้องการติดต่อส่งสัญญาณสร้างการเชื่อมต่อ (SYN) ไปยังยังเครื่องบริการปลายทาง รอจนกว่าปลายทางจะตอบรับการเชื่อมต่อ (SYN ACK) จากนั้นเครื่องต้นทางจะตอบรับอีกครั้ง ดังนั้นเพื่อที่จะทำให้การเชื่อมต่อสามารถดำเนินไปได้อย่างต่อเนื่อง โปรแกรมที่จัดการจับมือ 3 ทางของเครื่องบริการจะต้องจัดสรรหน่วยความจำจำนวนหนึ่งเพื่อรองรับการเชื่อมต่อแต่ละเซสชันจนกว่าการจับมือ 3 ทางจะสิ้นสุดลง โดยที่เครื่องบริการมีเวลาค่าหนึ่งที่จะรอให้ได้รับสัญญาณตอบรับกลับมา หากถึงเวลาที่กำหนดแล้วไม่มีการตอบกลับมาเครื่องบริการจะต้องยุติการรอนั้นและคืนหน่วยความจำให้แก่ระบบปฏิบัติการ สำหรับการโจมตีที่ด้วยการสร้างการเชื่อมต่อจำนวนมาก เป็นเหตุการณ์ผิดปกติและเป็นสิ่งที่เครื่องบริการจะจัดการไม่ได้ หากระบบปฏิบัติการของเครื่องบริการ เป้าหมายจัดการหน่วยความจำได้ไม่มีสมรรถนะพอก็อาจจะหยุดทำงานทันที

ง. การโจมตีไปยังหมายเลขไอพี (Land Attack) เป็นการโจมตีด้วยการกำหนดให้หมายเลขไอพีต้นทางตรงกับไอพีปลายทาง หมายเลขพอร์ตต้นทางตรงกับพอร์ตปลายทาง ตั้งค่าตัวบ่งชี้การเชื่อมต่อ (SYN Flag) ให้เสมือนขอเริ่มต้นการเชื่อมต่อ ส่งกลุ่มข้อมูลไป

ยังทีซีพีพอร์ตที่เปิดอยู่ เมื่อเครื่องปลายทางได้รับสัญญาณขอสร้างการเชื่อมต่อจะตอบรับกลับไปยังผู้ส่งตามหมายเลขพอร์ตและหมายเลขไอพีต้นทาง แต่ในกรณีนี้หมายเลขไอพีต้นทาง ปลายทาง หมายเลขพอร์ตต้นทางและปลายทางจะถูกตั้งให้เป็นค่าเดียวกัน ดังนั้นการตอบกลับไปยังปลายทางซึ่งเป็นการส่งเข้าเครื่องตนเอง ซึ่งกรณีนี้ไม่มีกำหนดอยู่ในโพรโทคอลว่าควรจะทำอย่างไร ทำให้มีการตอบกลับไปกลับมาของทีซีพีวนรอบอยู่ในตัวเองด้วยความเร็วสูง คอมพิวเตอร์จึงต้องใช้ทรัพยากรที่มีอยู่ทั้งหมด เพื่อคอยจัดการกับทีซีพีที่ตอบกลับไปกลับมาดังกล่าวจนไม่อาจจะไปทำงานอื่นได้ จึงดูเหมือนว่าเครื่องคอมพิวเตอร์หยุดทำงานและไม่ตอบสนองต่อการกระตุ้นใดๆ จึงต้องใช้วิธีรีเซ็ตเครื่องหรือปิดเครื่องจึงจะสามารถหยุดการวนรอบของทีซีพีได้

จ. การโจมตีที่ใช้ข้อบกพร่องในการรวมกลุ่มข้อมูล (Teardrop) เป็นการโจมตีโดยใช้การเหลื่อมกันของกลุ่มข้อมูลในระหว่างที่มีการรวมกลุ่มข้อมูลเข้าด้วยกัน ในการแตกกระจายข้อมูล (Fragment) ตามปกติกลุ่มข้อมูลที่ถูกแบ่งออกเป็นส่วนย่อยจะถูกนำมารวมกันในตำแหน่งถูกต้องสอดคล้อง แต่ในกรณีนี้กลุ่มข้อมูลที่ใช้ในการโจมตีประเภทนี้จะถูกสร้างขึ้นมาโดยเฉพาะมิได้ผ่านกลไกการแตกกระจายตามปกติและมีการระบุออฟเซ็ต (Offset) ที่เหลื่อมเข้าไปในกลุ่มข้อมูลอื่นๆ ซึ่งจะไม่มีโอกาสเกิดขึ้นได้ในการทำงานปกติ ดังนั้นหากระบบปฏิบัติการไม่สามารถจัดการเงื่อนไขไม่ปกติได้ดีเพียงพอก็จะหยุดการทำงาน

ฉ. การปรับปรุงเทคนิคของการส่งข้อมูลจำนวนมาก (Flood) ไปยังเครือข่ายให้สามารถโจมตีเป้าหมายโดยไม่ขึ้นอยู่กับแบนด์วิดท์ (Smurf Attack) [11] ทำให้ผู้ที่มีแบนด์วิดท์ต่ำสามารถส่งข้อมูลจำนวนมากไปยังเป้าหมายได้รุนแรงขึ้น โดยผู้ประสงค์ร้ายจะส่งการสะท้อนไอซีเอ็มพีไปยังเลขที่อยู่ไอพีทั้งหมดในเครือข่าย (IP Broadcast Address) ทำให้เครื่องแม่ข่าย (Host) ทุกเครื่องได้รับกลุ่มข้อมูลนั้นอย่างทั่วถึง ดังนั้นหากมีเครื่องแม่ข่ายใดส่งการสะท้อนการร้องขอไอซีเอ็มพีกระจายไปยังทุกเครื่องแม่ข่ายบนเครือ ทำให้เกิดการตอบกลับเท่ากับจำนวนเครื่องที่อยู่ในเครือข่ายนั้น

2.5 การทำงานของระบบตรวจหาการบุกรุก

การตรวจหาการบุกรุก (Intrusion Detection) [8] เป็นกระบวนการในการเฝ้าตรวจสอบข้อมูลบนระบบคอมพิวเตอร์หรือเครือข่าย เพื่อค้นหาสัญลักษณ์บ่งบอกการบุกรุกให้ผู้ดูแลระบบ โดยจะทำหน้าที่ป้องกันความเสียหายจากการบุกรุกเมื่อตรวจหาการโจมตีที่มีรูปแบบอยู่ในฐานความรู้ข้อมูล ช่วยลดความเสียหายจากการบุกรุกที่ไม่มีรูปแบบอยู่ในฐานความรู้ข้อมูล บอกถึงกิจกรรมที่เป็นเครื่องแสดงการโจมตีร้ายแรง และบอกถึงการโจมตีที่เกิดขึ้นในขณะนั้น การ

ทำงานของระบบตรวจหาการบุกรุกเครือข่ายแบ่งได้ 3 ส่วน คือ แหล่งข้อมูลที่ใช้ในการวิเคราะห์ การวิเคราะห์ข้อมูลและการตอบสนอง

2.5.1 **แหล่งข้อมูลที่ใช้ในการวิเคราะห์ (Information Source)**

เป็นกระบวนการในการรับข้อมูลจากแหล่งข้อมูลต่างๆ เพื่อนำข้อมูลเหล่านั้นไปวิเคราะห์หาสัญลักษณ์การบุกรุก ซึ่งแบ่งเป็น 4 ประเภทตามแหล่งข้อมูลและวิธีการเก็บข้อมูล ดังนี้

ก. ระบบปฏิบัติการ (Host Based) เป็นข้อมูลจากการใช้งานบนระบบปฏิบัติการ เช่น ข้อมูลรายชื่อการพยายามเข้าสู่ระบบปฏิบัติการ ข้อมูลการใช้ระบบ (System Log) เป็นต้น

ข. เครื่องเป้าหมาย (Target Based) ที่มีข้อกำหนดของทรัพยากร ตัวอย่างของข้อมูล เช่น ข้อมูลเกี่ยวกับ อุปกรณ์ (Device) และการประมวลผล (Process) ของระบบปฏิบัติการยูนิกส์ เป็นต้นมาผ่านวิทยาการเข้ารหัสลับด้วยฟังก์ชันแฮช (Cryptographic Hash Function) แล้วนำมาเปรียบเทียบกับนโยบาย (policy) ด้านความปลอดภัยเพื่อตรวจสอบการเปลี่ยนแปลงของออบเจ็ก ซึ่งช่วยป้องกันใจกลาง (Kernel) ของระบบปฏิบัติการ

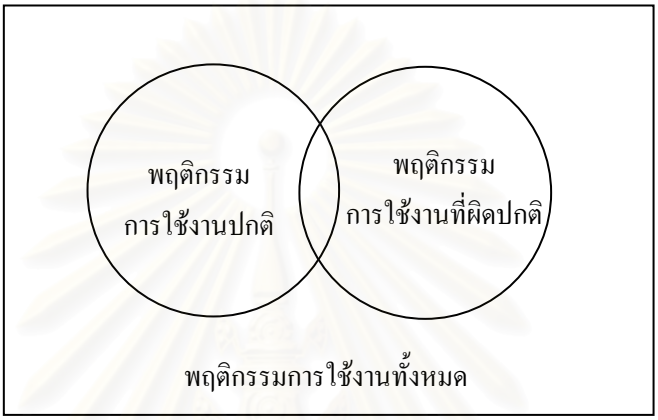
ค. โปรแกรม (Application Based) เป็นข้อมูลที่ได้จากการบันทึกทำงานของโปรแกรม เช่น แฟ้มลงบันทึกเข้าออก (Log File) เป็นต้น

ง. ข้อมูลจากเครือข่าย (Network Based) โดยการเฝ้าสังเกตเครือข่ายและเก็บกระแสข้อมูล (Traffic Stream) ของเครือข่ายในเซกเมนต์นั้น การนำข้อมูลเครือข่ายมาวิเคราะห์ทำให้ทราบถึงการกระทำของผู้ใช้เครือข่ายและเป็นสัญญาณบ่งบอกการบุกรุกให้ผู้ดูแลระบบทราบ จึงลดความน่าจะเป็นที่ผู้บุกรุกจะเข้าถึงระบบได้โดยไม่มีสัญญาณบ่งบอก การเก็บข้อมูลจากเครือข่ายได้มาจากการดักจับกลุ่มข้อมูลทั้งหมดในเครือข่าย (Promiscuous Mode) ของตัวปรับต่อข่ายงาน (Network Adapter) ซึ่งจะรับกลุ่มข้อมูลทั้งหมดที่กระจายบนเครือข่าย

2.5.2 **การวิเคราะห์ข้อมูล (Analysis Type)**

พฤติกรรมการใช้งานของผู้ใช้โดยทั่วไปประกอบด้วยพฤติกรรมการใช้งานแบบปกติและพฤติกรรมการใช้งานที่ผิดปกติ โดยพฤติกรรมผิดปกติจะมีแนวโน้มเป็นพฤติกรรมของผู้บุกรุกมากกว่าเป็นพฤติกรรมการใช้งานปกติดังรูปที่ 2.1 ซึ่งใช้วงกลมแทนพฤติกรรมการใช้งานทั้งปกติและผิดปกติ ส่วนที่ซ้อนทับกันจะแสดงถึงพฤติกรรมการใช้งานที่มีลักษณะแอบแฝงสามารถ

ตีความได้ทั้งสองแบบ แต่ในความเป็นจริงพฤติกรรมการใช้งานทั้งปกติและผิดปกติสามารถเป็นพฤติกรรมการบุกรุกได้ ขึ้นอยู่กับวัตถุประสงค์ของผู้ใช้คนนั้น เช่น การใช้คำสั่งปิง (Ping) เพื่อตรวจสอบว่าเครื่องเป้าหมายเปิดให้บริการอยู่หรือไม่ จะคล้ายกับการส่งปิงเป็นจำนวนมากเพื่อรบกวนการให้บริการ (Ping Flood) หรือความผิดพลาดในการพิมพ์รหัสผ่านผิดติดต่อกันหลายครั้งจะคล้ายกับการสุ่มใช้รหัสผ่านเพื่อเจาะเข้าระบบ เป็นต้น



รูปที่ 2.1 พฤติกรรมของผู้ใช้ระบบ

การวิเคราะห์ข้อมูล เป็นกระบวนการในการนำข้อมูลที่เก็บจากแหล่งข้อมูลมาวิเคราะห์ตามพฤติกรรมของผู้ใช้ ซึ่งแบ่งเป็น 2 ประเภท คือ การวิเคราะห์ข้อมูลจากการตรวจหาพฤติกรรมการใช้งานปกติและการวิเคราะห์ข้อมูลจากการตรวจหาพฤติกรรมการใช้งานที่ผิดปกติ

ก. การวิเคราะห์ข้อมูลจากการตรวจหาพฤติกรรมการใช้งานปกติ (Anomaly Detection) เป็นการวิเคราะห์ด้วยเก็บข้อมูลสถิติการใช้งานในรูปโพรไฟล์ (Profile) ซึ่งข้อมูลที่เก็บไว้ในครั้งแรกจะใช้เป็นแม่แบบของโพรไฟล์ การเก็บค่าสถิติในการใช้งานครั้งต่อไปจะต้องนำมาเทียบกับแม่แบบโพรไฟล์เพื่อค้นหาพฤติกรรมการใช้ที่แตกต่างไปจากเดิม ซึ่งแม่แบบโพรไฟล์ที่มีอยู่สามารถกำหนดรูปแบบการปรับปรุงให้เป็นแบบคงที่ (Fixed) หรือแบบเปลี่ยนแปลงได้ (Variable)

ข. การวิเคราะห์ข้อมูลจากการตรวจหาพฤติกรรมการใช้งานผิดปกติ (Misuse Detection) เริ่มจากรวบรวมข้อมูลในการโจมตี แล้วแทนให้อยู่ในรูปแบบที่มีความหมายเก็บไว้ในกลไกการวิเคราะห์ (Analyses Engine) ซึ่งการจัดประเภทของข้อมูลจะอยู่บนพื้นฐานของกฎเกณฑ์ (Rule) ซึ่งเป็นข้อกำหนดที่ใช้ในการเปรียบเทียบหาความแตกต่างระหว่างข้อมูลที่ต้องการตรวจสอบกับข้อมูลที่อยู่ในฐานความรู้ (Knowledge Based) ซึ่งใช้เก็บข้อมูลอธิบาย

พฤติกรรมพื้นฐานบนความรู้ที่เกี่ยวกับการบุกรุกที่มี การวิเคราะห์สามารถทำได้โดยนำข้อมูลส่วนย่อย (Atomic) เช่น การตรวจความผิดปกติของข้อมูลในกลุ่มข้อมูลไอพี หรือจากการนำข้อมูลส่วนย่อยหลายส่วนประกอบกันซึ่งเรียกว่า (Composite) มาค้นหาการบุกรุกด้วยการนำมาเปรียบเทียบกับข้อมูลที่มีอยู่ในฐานความรู้เพื่อค้นหาการโจมตี

2.5.3 **การตอบสนอง (Response)**

การตอบสนองหลังจากตรวจพบการโจมตีมีหลายรูปแบบ เช่น การจัดทำรายงานสรุปของการโจมตีที่เกิดขึ้น การตอบสนองแบบอัตโนมัติทันทีที่พบการบุกรุก การบันทึกเวลาและรูปแบบการโจมตีไว้ ซึ่งการตอบสนองของระบบตรวจหาการบุกรุกทั่วไปมี 2 แบบ คือ

ก. การตอบสนองทันทีหลังจากตรวจหาการพยายามบุกรุก (Active Response) เป็นการทำงานแบบอัตโนมัติ เช่น การตรวจพบการโจมตีต้องสงสัยที่ไม่เคยพบมาก่อน จึงบันทึกข้อมูลเกี่ยวกับการโจมตีนี้ไว้เป็นข้อมูลเมื่อตรวจพบการโจมตีแบบเดิม การตอบสนองแบบนี้จะไม่ก่อให้เกิดความเสียหายใดๆ แต่จะใช้เวลามากที่สุด

ข. การตอบสนองภายหลัง (Passive Response) เป็นการตอบสนองโดยอาศัยการตัดสินใจของผู้ดูแลระบบก่อนที่จะมีการตอบสนองใดๆ เช่น การแจ้งเตือนและรายงานการโจมตีที่เกิดขึ้นบนจอภาพ หรือส่งผลการตรวจหาไปยังระบบบริหารจัดการเครือข่ายเพื่อแจ้งให้ผู้ดูแลระบบทราบ

2.6 การทดสอบระบบตรวจหาการบุกรุก

การทดสอบการทำงานของระบบตรวจหาการบุกรุกมีวัตถุประสงค์เพื่อทดสอบและค้นหาข้อจำกัดในการทำงาน สามารถแบ่งตามวัตถุประสงค์ในการทดสอบดังนี้

2.6.1 ทดสอบความสามารถในการจำแนกลักษณะการบุกรุกออกจากพฤติการรมการใช้งานแบบปกติได้ (Broad Detection Range) การทดสอบประเภทนี้ทำเพื่อไม่ให้การบุกรุกนั้นๆ หลบหนีจากการตรวจหาไปได้

2.6.2 ทดสอบการใช้ทรัพยากร (Economy in Resource Usage) ของระบบตรวจหาการบุกรุกในขณะที่กำลังตรวจหาการบุกรุก เนื่องจากระบบตรวจหาการบุกรุกที่เสถียรควรมีฟังก์ชันในการทำงานที่ใช้ทรัพยากรของระบบน้อย ถ้าระบบตรวจหาใช้ทรัพยากร เช่น

หน่วยความจำหลัก เวลาที่ใช้ในการประมวลผล พื้นที่ว่างบนดิสก์มาก มีผลทำให้ตรวจหาการบุกรุกทำงานได้ไม่ดีในบางสภาพแวดล้อม

2.6.3 ทดสอบความถูกต้องในการทำงานเมื่ออยู่ภายใต้สภาวะที่มีความกดดันมาก (Resilience to Stress) เช่น การตรวจหาการบุกรุกในขณะที่มีจำนวนข้อมูลสูง ซึ่งอาจจะเป็นสภาวะที่เกิดขึ้นจริงหรือเกิดจากการกระทำของผู้บุกรุกที่ต้องการขัดขวางการทำงานของระบบตรวจหา โดยมีเป้าหมายเพื่อวัดความน่าเชื่อถือของระบบตรวจหาการบุกรุกนั้น

2.7 เกณฑ์ความต้องการในการทำงานของระบบตรวจหาการบุกรุก

ระบบตรวจหาการบุกรุก ที่ดีควรมีคุณสมบัติที่ต้อง ดังนี้

2.7.1 ความถูกต้องในการตรวจหา (Accuracy) ซึ่งจะบ่งบอกถึงความสามารถในการแยกแยะข้อมูลปกติออกจากข้อมูลแสดงการบุกรุก และเมื่อตรวจพบการโจมตีแล้วสามารถแสดงรายละเอียดของการโจมตีนั้นได้อย่างถูกต้อง และครบถ้วนตามการโจมตีที่เกิดขึ้นจริง

2.7.2 สมรรถนะของระบบตรวจหา แสดงถึงความสามารถและความยืดหยุ่นในการตรวจหาการโจมตีซึ่งขึ้นอยู่กับปัจจัยแวดล้อมต่างๆ ด้วย ดังนั้นระบบตรวจหาการบุกรุกที่ดีควรจะมีสมรรถนะสูงและไม่ใช้ทรัพยากรของระบบมาก เพื่อให้มีความสามารถเพียงพอที่จะทำงานและแจ้งเตือนได้ทันท่วงที

2.7.3 มีความผิดพลาดในการตรวจหาการบุกรุกน้อย ความผิดพลาดในการตรวจหาการบุกรุกขึ้นอยู่กับจำนวนและรูปแบบของการโจมตีในฐานความรู้ หากรูปแบบของการโจมตีที่เกิดขึ้นไม่มีอยู่ในฐานความรู้ก็จะเกิดการไม่แจ้งเตือนเมื่อถูกโจมตีได้ หรือหากรูปแบบของการโจมตีซ้ำซ้อนหรือใกล้เคียงกับการใช้งานปกติก็อาจเกิดการแจ้งเตือนทั้งที่ไม่มีการโจมตีก็ได้

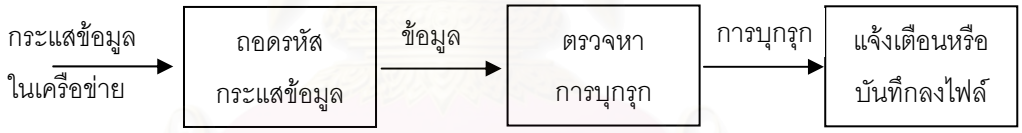
2.7.4 มีความสามารถในการต้านทานการโจมตี (False Tolerance) เพื่อให้ระบบตรวจหาทำการตรวจหาได้ตามปกติอย่างต่อเนื่อง และสามารถรองรับการโจมตีได้เมื่อเป็นเป้าหมายของการโจมตี

2.7.5 ใช้เวลาในการวิเคราะห์ (Timeline) น้อย ซึ่งช่วยให้ได้ผลการวิเคราะห์ก่อนที่การโจมตีจะทำลายเป้าหมายสำเร็จ

2.8 **โปรแกรมสนอร์ท** (Snort) [10]

สนอร์ทเป็นโปรแกรมตรวจหาการบุกรุกเครือข่ายเปิดเผยรหัสต้นฉบับ (Source Code) ที่ได้รับความนิยมมาก สามารถทำงานข้ามแพลตฟอร์มได้ ผู้ใช้สามารถดึงโปรแกรมผ่านเครือข่ายอินเทอร์เน็ต และสามารถพัฒนาเพื่อให้เหมาะสมกับจุดมุ่งหมายของการนำไปใช้

การตรวจหาการบุกรุกของสนอร์ทเริ่มจากการดักจับกระแสข้อมูล(Bit Stream) โดยใช้คลังลิบพีแคป (libpcap) หลังจากนั้นจึงทำการถอดรหัสข้อมูลแล้วนำมาตรวจหาการบุกรุกด้วยเทคนิคการเปรียบเทียบเนื้อหา (Content Pattern Matching) ซึ่งจะทำการเปรียบเทียบข้อมูลที่ได้กับรูปแบบของการโจมตีที่มีอยู่ในกฎเกณฑ์ เมื่อตรวจพบการบุกรุกสามารถแจ้งเตือนทันทีหลังจากตรวจพบ หรือบันทึกลงแฟ้มข้อมูล การปรับแต่งค่าของสนอร์ทจะสั่งผ่านส่วนต่อประสานรายคำสั่ง (Command Line) โดยโครงสร้างของสนอร์ทจะเน้นในเรื่องสมรรถนะ การใช้งานง่ายและความยืดหยุ่นในการใช้งาน องค์ประกอบของสนอร์ทประกอบด้วย ส่วนการถอดรหัสกลุ่มข้อมูล (Packet Decode) ส่วนประมวลผลการตรวจหาการบุกรุก (Detection Engine) และส่วนการบันทึกและการแจ้งเตือน (Logging and Alerting) แสดงได้ดังรูปที่ 2.2



รูปที่ 2.2 การทำงานของโปรแกรมสนอร์ท

2.8.1 ส่วนการถอดรหัสกลุ่มข้อมูล จะนำข้อมูลที่ได้จากการดักจับ มาถอดรหัสข้อมูลจากชั้นดาตา (Data Link) จนถึงชั้นขนส่ง (Transport Layer) จึงรองรับการเชื่อมต่อผ่านเครือข่ายอีเทอร์เน็ต (Ethernet) สลิป(Slip) พีพีพี(PPP) เอทีเอ็ม (ATM)

2.8.2 ส่วนประมวลผลการตรวจหา จะใช้กฎเกณฑ์การตรวจหาแบบรายการโยง (Linked List) ที่ประกอบด้วย ลูกโซ่ตัวนำ (Chain Header) ซึ่งเก็บข้อมูลไอพีต้นทาง/ปลายทาง พอร์ตต้นทาง/ปลายทาง และลูกโซ่ตัวเลือก (Chain Option) เก็บรายละเอียด เช่น เนื้อหา (Content) ตัวบ่งชี้ทีซีพี (TCP Flag) รหัส/ชนิดของโพรโตคอลไอซีเอ็มพี (ICMP Code/Type) เป็นต้น

2.8.3 ส่วนของการบันทึกและการแจ้งเตือน เป็นส่วนการตอบสนองที่สั่งผ่านส่วนต่อประสานรายคำสั่ง การบันทึกจะเป็นการบันทึกกลุ่มข้อมูลที่ถอดรหัสแล้วซึ่งอยู่ในรูปแบบเลขฐานสองหรือรูปแบบโครงสร้างพื้นฐานไอพีลงในแฟ้มข้อมูลจึงง่ายต่อการตีความ ส่วนการแจ้งเตือนจะทำด้วยการส่งข้อความเกี่ยวกับความปลอดภัยไปยังระบบหรือแจ้งเตือนทางหน้าจอ

2.9 โปรแกรมเรียลซีเคียว (RealSecure)

เรียลซีเคียวเป็นโปรแกรมตรวจหาการบุกรุกของบริษัทอินเทอร์เน็ตซีเคียวริตีซิสเต็ม จำกัด (Internet Security System) ทำงานบนระบบปฏิบัติการวินโดวส์ ผู้ใช้สามารถปรับแต่งการทำงานให้เหมาะสมด้วยการเพิ่ม-ลดรูปแบบการโจมตีที่ต้องการ นอกจากนี้ยังสามารถบริหารจัดการจากส่วนกลางโดยผ่านเครือข่ายอินทราเน็ตได้โดยการวางตัวรับรู้ (Sensor) ไว้ในตำแหน่งที่ต้องการและใช้การจัดการแบบรวมศูนย์รวบรวมข้อมูลมาลงในฐานข้อมูลเดียวกัน โดยฟังก์ชันหลักในการทำงานประกอบด้วย

2.9.1 ตัวรับรู้ ทำหน้าที่ตรวจหาการบุกรุกบนเครือข่ายหรือระบบ หากเป็นตัวรับรู้เครือข่าย จะทำงานโดยตรวจวิเคราะห์การไหลของข้อมูลในเครือข่าย เพื่อค้นหารูปแบบของการโจมตีตามที่โปรแกรมรู้จักพร้อมทั้งค้นหาการบุกรุกและส่งข้อมูลไปยังหน่วยสะสมเหตุการณ์ (Event Collector)

2.9.2 หน่วยสะสมเหตุการณ์ (Event Collector) ทำหน้าที่บันทึกเหตุการณ์ทันทีที่ได้รับจากตัวรับรู้ลงในฐานข้อมูล นอกจากนี้ยังสามารถบริหารจัดการเป็นฐานข้อมูลขนาดใหญ่ (Enterprise Database) ซึ่งเก็บข้อมูลเหตุการณ์ที่ได้จากการทำงานของตัวรับรู้และสามารถจัดแสดงข้อมูลในฐานข้อมูลให้อยู่ในรูปแบบของรายงานได้

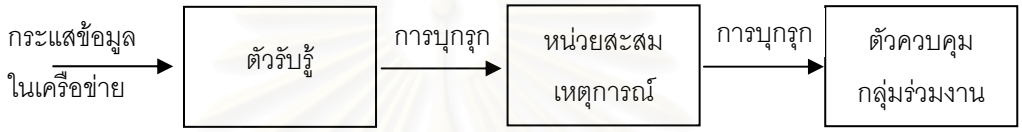
2.9.3 ตัวควบคุมกลุ่มร่วมงาน (Workgroup Manager) ทำหน้าที่เก็บรวบรวมข้อมูลจากฐานข้อมูลของตัวรับรู้

2.9.4 ฐานข้อมูลทรัพย์สิน (Asset Database) เก็บข้อมูลเบื้องต้นเกี่ยวกับเครือข่าย เช่น รายละเอียดเกี่ยวกับเครื่องคอมพิวเตอร์ ส่วนโปรแกรม (Component) สามารถกำหนดให้หลายจอเฝ้าคุม (Console) ใช้กลุ่มของทรัพย์สินเดียวกัน

2.9.5 ดีมอน (Daemon) เป็นโปรแกรมที่ทำหน้าที่เชื่อมต่อระหว่างจอเฝ้าคุมของโปรแกรม กับตัวรับรู้หรือหน่วยสะสมเหตุการณ์ เมื่อจอเฝ้าคุมส่งคำสั่งต่างๆ ไปยังดีมอน เช่น สั่ง

เริ่มทำงาน ปิดการทำงาน (Shutdown) หรือสั่งปรับปรุงนโยบาย เมื่อดีมอนได้รับคำสั่งจะส่งคำสั่งเหล่านั้นไปยังองค์ประกอบที่จำเป็นต้องใช้ข้อมูลนั้นแล้วส่งผลกลับมาให้จอเฝ้าคุม

การทำงานของโปรแกรมเมื่อตัวรับรู้ตรวจพบการโจมตีตามรูปแบบที่มีอยู่จะส่งรายละเอียดของการโจมตีนั้นไปยังหน่วยสะสมเหตุการณ์เพื่อบันทึกลงฐานข้อมูลหลังจากนั้นจึงแสดงข้อความแจ้งเตือนผ่านตัวควบคุมกลุ่มร่วมงาน การแจ้งเตือนเป็นข้อความสนเทศ (Information Message) ที่ถูกสร้างขึ้นโดยตัวรับรู้เพื่อใช้แสดงสถานะ เช่น เป็นข้อมูล เป็นคำเตือน หรือเป็นข้อผิดพลาดต่างๆ



รูปที่ 2.3 การทำงานของโปรแกรมเรียลซีเคียว

โปรแกรมสามารถเลือกการตอบสนองได้หลายรูปแบบ เช่น บันทึกวัน-เวลาที่เกิดการโจมตี บันทึกต้นทาง-ปลายทางของเหตุการณ์ที่เกิดขึ้น บันทึกเนื้อหา (Content) ของการโจมตีหรือการบุกรุกนั้น แจ้งให้ผู้ดูแลเครือข่ายทราบ ปรับแต่งค่าของไฟล์วอลล์ ตัดการเชื่อมต่อของผู้บุกรุก เป็นต้น

2.10 งานวิจัยที่เกี่ยวข้อง

Nicholas J.Pukketza [2]. A Methodology for Testing Intrusion Detection System ได้นำเสนอภาพรวมของซอฟต์แวร์แพลตฟอร์มที่ใช้ประเมินการทำงานของระบบตรวจหาการบุกรุกด้วยวิธีการเดียวกับการทดสอบซอฟต์แวร์ ซึ่งในงานวิจัยนี้ได้เสนอแนวทางและกลยุทธในการเลือกกรณีที่ต้องการทดสอบ (Test Case) รวมถึงการหาระเบียบในการทดสอบ (Test Procedure) และความปลอดภัย หากนำมาใช้ในการประเมินจริงจะได้ผลลัพธ์เป็นตัวเลข

Terrence Champion [3]. A Benchmark Evaluation of Network Intrusion Detection System กล่าวถึงวิธีการสร้างเกณฑ์เปรียบเทียบสมรรถนะ (Benchmarking) เพื่อหาความไวในการตรวจหาการบุกรุกเครือข่าย และทดสอบด้วยการโจมตีที่มีวัตถุประสงค์เพื่อก่อกวนระบบแบบทันที (Real Time) ในการงานวิจัยนี้ได้ทำการทดสอบกับฐานข้อมูลสัญลักษณ์ (Signature Based) ที่ใช้ทางการค้าและฐานข้อมูลของดาร์พา (DARPA) โดยมีจุดประสงค์เพื่อหา

ขอบเขตของการทำงานของเครื่องมือที่ใช้โจมตีว่าจะมีผลต่อสมรรถนะการตรวจหาหรือไม่ ซึ่งผลการทดลองสรุปว่าระบบที่วิจัยขึ้นมีขอบเขตในการตรวจหาการบุกรุกมากกว่าระบบทางการค้า

Nei Kato [6]. A Real Time Intrusion Detection System (IDS) for Large Scale Networks and Its Evaluations กล่าวถึงกลไกในการลดจำนวนข้อมูลในเหตุการณ์ที่เก็บให้น้อยลง แต่ยังมีความสามารถเพียงพอที่จะวิเคราะห์และวัดระดับความปลอดภัยได้ โดยทำการทดลองกับระบบการตรวจหาการบุกรุกเครือข่ายที่มีการทำงานแบบโต้ตอบทันที การทำงานของระบบตรวจหาการบุกรุกจะเริ่มจากการค้นหากลุ่มข้อมูลตอบสนองทีซีพี (TCP ACK/RST Packet) เป็นรูปแบบทั่วไปที่ใช้ในการกราดตรวจเครือข่าย จากนั้นนำข้อมูลที่ได้มาหาแนวโน้มด้วยคลัสเตอร์ (Time Based Clustering) และใช้เทคนิคโครงสร้างต้นไม้แบบไดนามิก (Dynamic Access Tree) ซึ่งเป็นอัลกอริทึมของอาร์มอน (RMON) มาใช้ในการวิเคราะห์ โดยผลการทดลองพบว่าอัลกอริทึมที่ออกแบบขึ้นมีสมรรถนะดีกว่าและอนาคตคาดว่าสามารถใช้พัฒนาให้นำมาใช้งานกับเครือข่ายความเร็วสูงได้

Mandy Chung [7]. Simulating Concurrent Intrusions for Testing Intrusion Detection Systems: Parallelizing Intrusion ได้นำเสนอการออกแบบและพัฒนาอัลกอริทึมที่มีกลไกการเปลี่ยนรูปอัตโนมัติ จากสคริปต์การบุกรุกแบบตามลำดับไปเป็นสคริปต์การบุกรุกแบบขนาน ซึ่งมีทั้งลักษณะการบุกรุกแบบพร้อมกันและการบุกรุกแบบบังคับลำดับ โดยจัดรูปแบบเป็นประเภทตามผลกระทบที่เกิดขึ้น เพื่อนำไปใช้ในการทดสอบความสามารถในการตรวจหาการบุกรุกของระบบตรวจหา

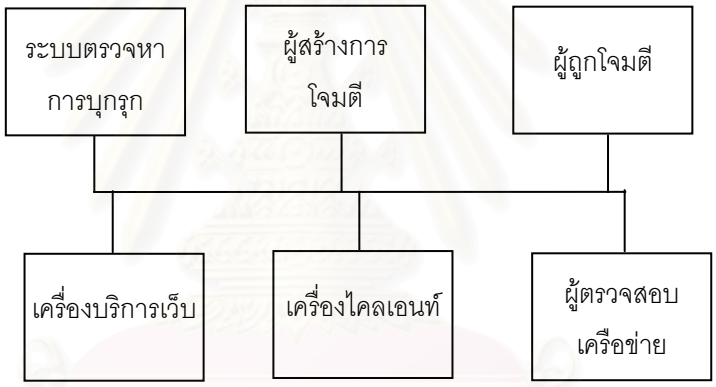
บทที่ 3

วิธีดำเนินการวิจัย

ในบทนี้กล่าวถึงองค์ประกอบและฟังก์ชันของระบบที่ใช้ในการทดลอง ปัจจัยที่มีผลต่อการทำงานของระบบตรวจหาการบุกรุก รูปแบบและวิธีการทดลอง ผลที่บันทึกได้จากการทดลอง การคำนวณผลที่บันทึกได้ และเกณฑ์ในการทดสอบการทำงาน

3.1 องค์ประกอบและฟังก์ชันของระบบในการทดลอง

องค์ประกอบของการทดลองประกอบด้วย ระบบตรวจหาการบุกรุก ผู้สร้างการโจมตี ผู้ถูกโจมตี ผู้ตรวจสอบเครือข่าย เครื่องบริการเว็บและเครื่องไคลเอนท์ แสดงได้ดังรูปที่ 3.1 โดยองค์ประกอบต่างๆ มีทำหน้าที่ดังนี้



รูปที่ 3.1 องค์ประกอบของการทดลอง

3.1.1 โปรแกรมตรวจหาการบุกรุกสนอร์ทและเรียลซีเคียวทำหน้าที่ตรวจหาการโจมตีโดยใช้กฎเกณฑ์มาตรฐานของโปรแกรม ในการทดลองจะทำการตรวจหาการบุกรุกพร้อมกับบันทึกการใช้งานซีพียูของเครื่องไว้

3.1.2 ผู้สร้างการโจมตี (Attacker) ทำหน้าที่สร้างการโจมตีไปเป้าหมาย ในขณะทำการทดลองจะบันทึกปริมาณข้อมูลที่เกิดขึ้นบนส่วนต่อประสานของเครื่อง เพื่อนำมาคำนวณหาอัตราเร็วในการโจมตี

3.1.3 ผู้ถูกโจมตีหรือเป้าหมายของการโจมตี (Target) จะรอรับการโจมตีพร้อมทั้งบันทึกปริมาณข้อมูลที่เกิดขึ้นบนส่วนต่อประสาน

3.1.4 ผู้ตรวจสอบเครือข่าย (Network monitor) ทำหน้าที่บันทึกปริมาณข้อมูลทั้งหมดที่เกิดขึ้นบนเครือข่าย

3.1.5 เครื่องบริการเว็บ (Web Server) จะรอรับการเชื่อมต่อจากไคลเอนท์เพื่อสร้างการรับ-ส่งข้อมูลในเครือข่ายพร้อมทั้งบันทึกปริมาณข้อมูลที่เกิดขึ้นบนส่วนต่อประสาน

3.1.6 เครื่องไคลเอนท์ (Client) จะดึงข้อมูลจากเครื่องบริการเว็บผ่านพอร์ต 80 เพื่อจำลองการรับ-ส่งข้อมูลบนเครือข่าย

3.2 ปัจจัยที่มีผลต่อการทำงานของระบบตรวจหาการบุกรุก

การทำงานของระบบตรวจหาการบุกรุกที่ติดตั้งในสภาพแวดล้อมที่ต่างกันจะมีความสามารถทำงานแตกต่างกัน สาเหตุเนื่องมาจากมีปัจจัยแวดล้อมที่ส่งผลกระทบต่อการทำงานไม่เหมือนกัน หากปัจจัยที่เกี่ยวข้องมีความเหมาะสมจะช่วยส่งเสริมให้ระบบสามารถตรวจสอบเหตุการณ์ได้ดี ครบถ้วนและทันเวลา ปัจจัยเกี่ยวข้องที่ส่งผลกระทบต่อการตรวจหาการบุกรุก ได้แก่ ปัจจัยภายนอกและปัจจัยภายใน

3.2.1 <u>ปัจจัยภายนอก</u>

เกิดจากสิ่งรอบข้างของระบบตรวจหาการบุกรุกที่มีผลต่อความสามารถในการทำงานของระบบตรวจหาการบุกรุก ได้แก่ ปัจจัยด้านสภาพแวดล้อมและปัจจัยด้านการโจมตี

ก. ปัจจัยด้านสภาพแวดล้อม เช่น

(1) แบนด์วิดท์ของเครือข่าย (Bandwidth) แสดงถึงขีดจำกัดในการรองรับการโจมตี เพราะเครือข่ายที่มีแบนด์วิดท์น้อยเมื่อถูกก่อกวนระบบหรือถูกโจมตีจะส่งกระทบต่อระบบได้ทันที

(2) จำนวนผู้โจมตี (Number of Attacker) การโจมตีบางชนิดจะทำงานได้ดีที่สุดเมื่อถูกส่งจากผู้โจมตีเดียว แต่การโจมตีบางชนิดจะรุนแรงขึ้นเมื่อส่งการโจมตีจากหลายผู้โจมตี ดังนั้นจำนวนของผู้โจมตีมีผลต่อการเพิ่มขึ้นหรือลดความรุนแรงของการโจมตีได้

(3) โครงสร้างของเครือข่าย (Network Architecture) และที่ตั้งของโปรแกรมตรวจหาการบุกรุก เครือข่ายที่ใช้ฮับหรืออุปกรณ์สลับสาย (Switch) ที่มีฟังก์ชันในการ

ตรวจสอบเครือข่ายจะช่วยให้โปรแกรมตรวจหาการบุกรุกได้ตรวจวิเคราะห์ข้อมูลทั้งหมดบนเครือข่ายได้

(4) สมรรถนะของเครื่องที่ลงโปรแกรมตรวจหาการบุกรุก เป็นองค์ประกอบหลักที่มีส่วนอย่างมากในการทำงานของระบบตรวจหาการบุกรุก ถ้าเครื่องที่ใช้มีสมรรถนะต่ำอาจจะทำให้โปรแกรมตรวจหาการบุกรุกไม่สามารถตรวจวิเคราะห์ข้อมูลจำนวนมากในเวลาเดียวกันได้ทัน ส่งผลให้เกิดการแจ้งเตือนน้อยกว่าการโจมตีที่เกิดขึ้น หรือเครื่องอาจจะหยุดทำงานได้เมื่อต้องตรวจสอบข้อมูลพร้อมกันจำนวนมาก

ข. ปัจจัยด้านการโจมตี เกี่ยวข้องกับวิธีการโจมตี วัตถุประสงค์ของการโจมตี และชนิดหรือรูปแบบที่ใช้โจมตี เช่น

(1) รูปแบบของการโจมตี (Attack Pattern) การโจมตีมุ่งไปที่ช่องโหว่แต่ละแห่งความร้ายแรงของการโจมตีจะไม่เท่ากัน หากเป็นการโจมตีแฝงซึ่งมีความคล้ายหรือใกล้เคียงกับการใช้งานปกติโปรแกรมตรวจหาการบุกรุกอาจจะตรวจไม่พบการโจมตีนั้น

(2) ความเร็วในการโจมตี (Attack Rate) สำหรับการโจมตีที่เน้นความเร็วจะส่งผลกระทบอย่างรุนแรงและทันที หากเป็นการโจมตีเพื่อค้นหาจุดอ่อนจะไม่เน้นเรื่องความเร็วในการโจมตีและส่งผลกระทบต่อระบบเมื่อถูกโจมตีที่จุดอ่อนนั้น

(3) ระยะเวลาในการโจมตี เมื่อถูกโจมตีความสามารถในการให้บริการจะลดลง ถ้าโจมตีอย่างต่อเนื่องเป็นเวลานานจะส่งผลทำให้ระบบหยุดให้บริการได้

(4) ข้อมูลปะปนกับการโจมตีหรือการโจมตีอื่นผสมกัน อาจจะส่งผลให้โปรแกรมตรวจหาการบุกรุกแยกการโจมตีผิดพลาดหรือตรวจหาการบุกรุกได้ไม่ครบถ้วน ซึ่งทำให้เกิดการแจ้งเตือนเกินจริงหรือไม่แจ้งเตือนเมื่อถูกโจมตี

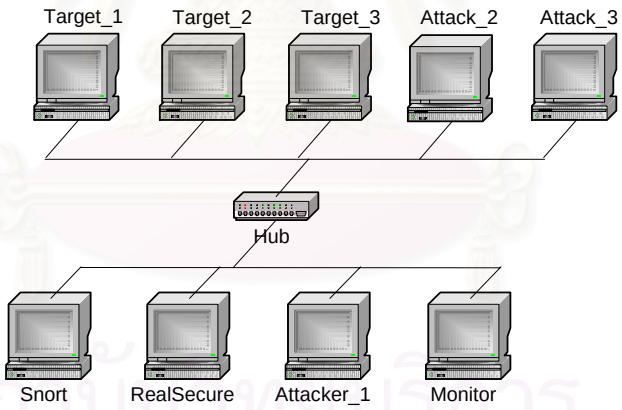
3.2.2 <u>ปัจจัยภายใน</u>

เป็นปัจจัยที่เกิดขึ้นจากระบบตรวจหาการบุกรุกเอง ซึ่งมีความเกี่ยวข้องโดยตรงกับอัลกอริทึมในการตรวจหา ความครบถ้วนถูกต้องของกฎเกณฑ์หรือรูปแบบการโจมตีที่มีอยู่ หากรูปแบบของการโจมตีหรือกฎเกณฑ์ของการตรวจหาที่ใกล้เคียงกับการใช้งานปกติ อาจทำให้เกิดการแจ้งเตือนเกินจริง ถ้ารูปแบบของการโจมตีไม่ครบถ้วนก็อาจจะตรวจไม่พบการโจมตีได้

3.3 รูปแบบและวิธีการทดลอง

การทดลองเพื่อทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกเริ่มจากผู้โจมตีส่งการโจมตีด้วยกลุ่มข้อมูลจำนวนมาก การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมาก การโจมตีด้วยการกราดตรวจทีซีพีพอร์ตและการโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์ ไปยังเป้าหมายในรูปแบบต่างๆ เพื่อให้โปรแกรมตรวจหาการบุกรุกได้ตรวจหาการโจมตีที่เกิดขึ้น ในการวิจัยนี้จะแบ่งการทดลองออกเป็น 3 ส่วน ตามสภาพแวดล้อมของการทดลอง ได้แก่ การทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียว การทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียวมีข้อมูล และการทดลองในสภาพแวดล้อมของการโจมตีหลายชนิดผสมกัน

3.3.1 การทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมของการโจมตีชนิดเดียวที่ไม่มีข้อมูลหรือการโจมตีอื่นปะปน เป็นการทดสอบเพื่อหาความสัมพันธ์ระหว่างความเร็วในการโจมตีกับความสามารถในการตรวจวิเคราะห์ ความถูกต้องของข้อความแจ้งเตือน และระยะเวลาที่ใช้ในการตรวจหา โดยสภาพแวดล้อมของการทดลองประกอบด้วยผู้โจมตี ผู้ถูกโจมตี โปรแกรมตรวจหาการบุกรุก เครื่องเฝ้าตรวจสอบเครือข่าย ดังรูปที่ 3.2

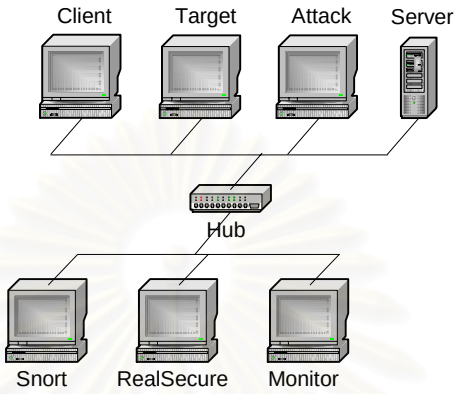


รูปที่ 3.2 สภาพแวดล้อมของการโจมตีชนิดเดียว

การทดสอบเริ่มจากผู้โจมตีส่งการโจมตีไปยังเป้าหมายด้วยความเร็วในการโจมตีที่แตกต่างกัน การเปลี่ยนแปลงความเร็วในการโจมตีจะทำโดยเพิ่มจำนวนผู้โจมตีและจำนวนเซสชันของการโจมตี

3.3.2 การทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมของการโจมตีชนิดเดียวมีข้อมูล เป็นทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมเสมือนจริง เพื่อทดสอบว่าข้อมูลจำนวนมากที่ปะปนอยู่จะมีผลต่อความสามารถใน

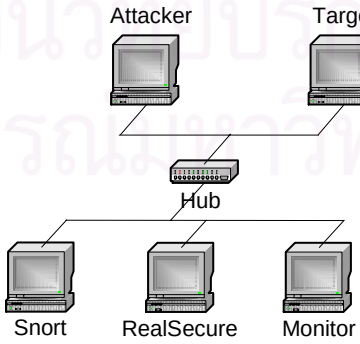
การตรวจหาหรือไม่ สภาพแวดล้อมของการทดลองนี้จะคล้ายกับสภาพแวดล้อมที่ใช้ในการทดลองแรกแต่จะเพิ่มเติมในส่วนของการรับ-ส่งข้อมูล โดยให้เครื่องไคลเอนท์ดึงข้อมูลจากเครื่องบริการเว็บผ่านพอร์ต 80 โดยมีสภาพแวดล้อมของการทดลองดังรูปที่ 3.3



รูปที่ 3.3 สภาพแวดล้อมของการโจมตีชนิดเดียวมีข้อมูล

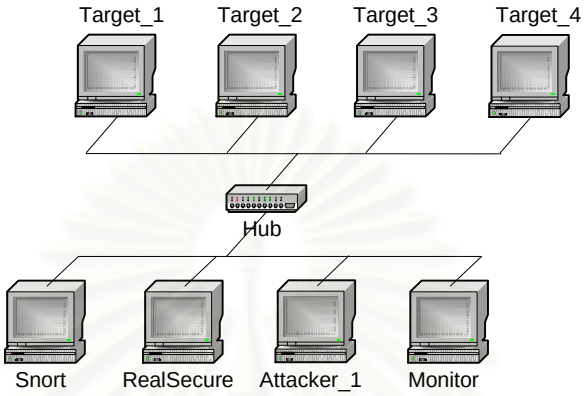
3.3.3 การทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมของการโจมตีหลายชนิดผสมกัน เพื่อทดสอบการทำงานในด้านความถูกต้องและครบถ้วนในการตรวจหาการบุกรุก โดยจัดส่งการโจมตีแบบพร้อมกันทั้ง 4 ชนิดไปยังเป้าหมาย ซึ่งในการทดลองนี้ได้จัดส่งการโจมตี 3 รูปแบบ คือ

ก. การทดลองโดยส่งการโจมตีจากผู้โจมตีเดียวไปยังเป้าหมายเดียว โดยผู้โจมตีจะสร้างการโจมตีเป็นจำนวน 4 เซสชัน แต่ละเซสชันจะส่งการโจมตีแต่ละชนิดไปยังเป้าหมายเดียวกันพร้อมกัน สภาพแวดล้อมของการทดลองแสดงได้ดังรูปที่ 3.4



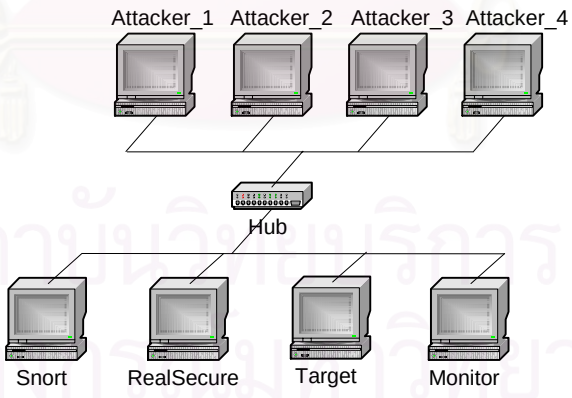
รูปที่ 3.4 สภาพแวดล้อมของการโจมตีจากผู้โจมตีเดียวไปยังเป้าหมายเดียว

ข. การทดลองโดยส่งการโจมตีจากผู้โจมตีเดียว 4 เซสชัน แต่ละเซสชันจะสร้างการโจมตีแต่ละชนิดและจัดส่งการโจมตีไปยังเป้าหมาย 4 แห่งพร้อมกัน โดยมีสภาพแวดล้อมของการทดลองดังรูปที่ 3.5



รูปที่ 3.5 สภาพแวดล้อมของการโจมตีจากผู้โจมตีเดียวไปยังเป้าหมาย 4 แห่ง

ค. การทดลองโดยส่งการโจมตี 4 ชนิดๆ ละเซสชันจากผู้โจมตี 4 เครื่องไปยังเป้าหมายของการโจมตีเดียวกัน ซึ่งสภาพแวดล้อมของการทดลองแสดงได้ดังรูปที่ 3.6



รูปที่ 3.6 สภาพแวดล้อมของการโจมตีจากผู้โจมตี 4 เครื่องไปยังเป้าหมายเดียว

3.4 ผลที่บันทึกได้จากการทดลอง

ในขณะทำการทดลองในสภาพแวดล้อมต่างๆ สามารถบันทึกค่าการทำงานแยกตามองค์ประกอบแต่ละส่วนได้ตารางที่ 3.1

ตารางที่ 3.1 ค่าที่บันทึกได้จากการทดลอง

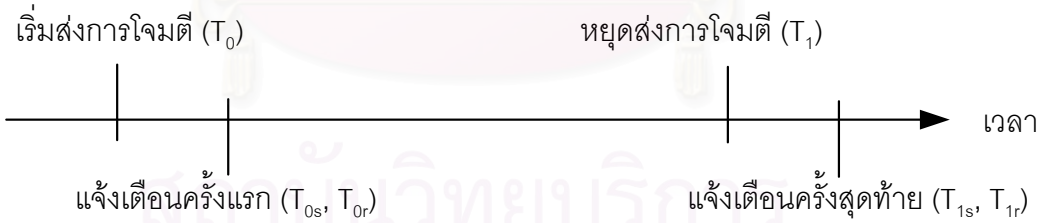
องค์ประกอบ	ค่าที่สามารถบันทึกได้
โปรแกรมตรวจหาการบุกรุกสนอร์ท	เวลาเริ่มต้น (T_{0s}) และเวลาสุดท้ายของการแจ้งเตือน (T_{1s})
	เปอร์เซ็นต์การใช้งานซีพียู ($\%CPU_s$)
	จำนวนกลุ่มข้อมูลทั้งหมดที่สนอร์ทตรวจพบ (Total)
	จำนวนกลุ่มข้อมูลทั้งหมดที่สนอร์ทได้ตรวจวิเคราะห์หาการโจมตี (Analyze)
	จำนวนกลุ่มข้อมูลที่ไม่สามารถวิเคราะห์ได้ทัน (Drop)
	จำนวนครั้งของการแจ้งเตือน (Alert)
	ข้อความแจ้งเตือนที่เกิดขึ้นเมื่อตรวจพบการโจมตี (Alert Name)
โปรแกรมตรวจหาการบุกรุกเรียลซีเคียว	เวลาเริ่มต้น (T_{0r}) และเวลาสุดท้ายของการแจ้งเตือน (T_{1r})
	เปอร์เซ็นต์การใช้งานซีพียู ($\%CPU_r$)
	จำนวนเหตุการณ์โจมตีที่ตรวจพบ (Event)
	จำนวนครั้งของการโจมตี (Hit) สำหรับเหตุการณ์นั้น
	ข้อความแจ้งเตือนของเหตุการณ์โจมตีที่ตรวจพบ (Event Name)
ผู้โจมตี	เวลาเริ่มต้น (T_0) และหยุดส่งการโจมตี (T_1)
	ชื่อการโจมตีที่ส่งออกไป (Attack Name)
	จำนวนเหตุการณ์โจมตีที่ส่งออกไป (No. of Attack Event)
	จำนวนครั้งของการโจมตีทั้งหมดที่ส่งออกไป (No. of Attack Hit)
	จำนวนกลุ่มข้อมูล (Total $Packet_a$) และไบต์ข้อมูลทั้งหมด (Total $Byte_a$) ที่เกิดขึ้นบนส่วนต่อประสาน
	จำนวนกลุ่มข้อมูล (Outgoing $Packet_a$) และไบต์ข้อมูล (Outgoing $Byte_a$) ที่ส่งออกจากส่วนต่อประสาน

ตารางที่ 3.1 ค่าที่บันทึกได้จากการทดลอง (ต่อ)

องค์ประกอบ	ค่าที่สามารถบันทึกได้
ผู้ถูกโจมตี	จำนวนกลุ่มข้อมูล (Total $Packet_t$) และไบต์ข้อมูลทั้งหมด (Total $Byte_t$)
เครื่องบริการเว็บ	จำนวนกลุ่มข้อมูล (Total $Packet_w$) และไบต์ข้อมูลทั้งหมด (Total $Byte_w$) ที่เกิดขึ้นบนส่วนต่อประสาน
เครื่องไคลเอนท์	เวลาเริ่มต้น (T_{0c}) และเวลาหยุดดึงข้อมูล (T_{1c})
	จำนวนกลุ่มข้อมูล (Total $Packet_c$) และไบต์ข้อมูลทั้งหมด (Total $Byte_c$) ที่เกิดขึ้นบนส่วนต่อประสาน
ผู้ตรวจสอบเครือข่าย	จำนวนกลุ่มข้อมูล (Total $Packet_m$) และไบต์ข้อมูลทั้งหมด (Total $Byte_m$) ที่เกิดขึ้นบนเครือข่าย

3.5 ความสัมพันธ์ของเวลาในโปรแกรมตรวจหาการบุกรุก

หลังจากผู้โจมตีเริ่มส่งการโจมตีออกไป โปรแกรมตรวจหาการบุกรุกจะตรวจวิเคราะห์ในหน่วยความจำและบันทึกข้อความแจ้งเตือนเมื่อตรวจพบการโจมตีลงในจานบันทึกแบบแข็ง โดยมีความสัมพันธ์ของเวลาในการส่งการโจมตีและแจ้งเตือนดังรูปที่ 3.7



รูปที่ 3.7 ความสัมพันธ์ระหว่างเวลาของการโจมตีกับเวลาของการแจ้งเตือน

เวลาของการแจ้งเตือนในครั้งแรกอาจจะเท่ากับหรือช้ากว่าเวลาเริ่มส่งการโจมตี ในขณะที่การโจมตีนั้นยังคงดำเนินต่อไป โปรแกรมตรวจหาการบุกรุกจะตรวจวิเคราะห์และแสดงข้อความแจ้งเตือนอย่างต่อเนื่อง เมื่อหยุดส่งการโจมตีเวลาของการแจ้งเตือนครั้งสุดท้ายที่บันทึกไว้อาจจะเป็นเวลาเดียวกันกับเวลาที่หยุดส่งการโจมตีหรือแตกต่างกันเล็กน้อยได้

รูปที่ 3.8 ความแตกต่างระหว่างเวลาที่คำนวณได้

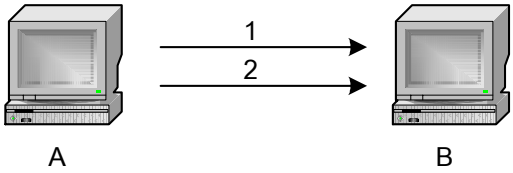
จากรูปที่ 3.8 ได้จากการคำนวณหาความแตกต่างระหว่างเวลาเริ่มส่งการโจมตีกับเวลาของแจ้งเตือนครั้งแรกแล้วแสดงเป็นเวลาล่าช้าในการแจ้งเตือน (Start Delay) และได้คำนวณหาความแตกต่างระหว่างเวลาหยุดส่งการโจมตีกับเวลาสุดท้ายของการแจ้งเตือนเป็นช่วงเวลาล่าช้าในการหยุดแจ้งเตือน (Stop Delay) โดยความแตกต่างของเวลาจะมากหรือน้อยขึ้นอยู่กับรูปแบบและพฤติกรรมของการโจมตี เช่น การโจมตีด้วยการกราดตรวจโปรแกรมตรวจหาการบุกรุกอาจจะต้องใช้เวลาในการตรวจวิเคราะห์นานกว่าการโจมตีแบบก่อกวนระบบที่เป็นการโจมตีด้วยความเร็วสูง เป็นต้น

3.6 การจำแนกเหตุการณ์แจ้งเตือนของโปรแกรมเรียลซีเคียว

การจำแนกเหตุการณ์แจ้งเตือนของโปรแกรมเรียลซีเคียวจะพิจารณาจากต้นทางปลายทางและชนิดของการโจมตีเป็นหลัก

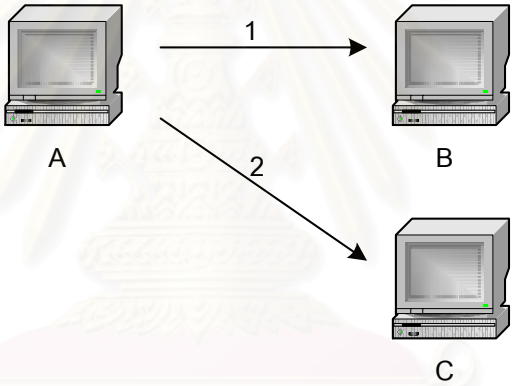
รูปที่ 3.9 ภาพจำลองของการโจมตีจากเครื่อง A ไปยังเครื่อง B

จากรูปที่ 3.9 เมื่อเครื่อง A ส่งการโจมตีชนิดหนึ่งไปยังเครื่อง B เป็นจำนวน 1 ครั้ง โปรแกรมเรียลซีเคียวจะตรวจพบการโจมตี 1 เหตุการณ์ (Event) จากต้นทาง (ผู้โจมตี) คือเครื่อง A ไปยังเป้าหมายของการโจมตีคือเครื่อง B โดยเหตุการณ์โจมตีนั้นเกิดขึ้นเป็นจำนวน 1 ครั้ง (Hit)



รูปที่ 3.10 ภาพจำลองของการโจมตีครั้งที่สองจากเครื่อง A ไปยังเครื่อง B

จากรูปที่ 3.10 หากเครื่อง A ส่งการโจมตีชนิดเดิมไปยังเครื่อง B โปรแกรมเรียลซีเคียวจะไม่เพิ่มจำนวนเหตุการณ์โจมตีแต่จะเพิ่มจำนวนครั้งของการแจ้งเตือนในเหตุการณ์โจมตีนั้นเป็น 2 ครั้งแต่ถ้าการโจมตีที่เครื่อง A ส่งไปยังเครื่อง B เป็นการโจมตีชนิดอื่น (ไม่ใช่ชนิดเดิมที่ตรวจพบและแจ้งเตือนไว้แล้ว) โปรแกรมเรียลซีเคียวจะแจ้งเตือนเพิ่มขึ้นอีก 1 เหตุการณ์รวมเป็น 2 เหตุการณ์โจมตี โดยแต่ละเหตุการณ์จะมีจำนวนครั้งของการโจมตีเป็น 1 ครั้ง



รูปที่ 3.11 ภาพจำลองของการโจมตีจากเครื่อง A ไปยังเครื่อง B และ C

จากรูปที่ 3.11 ซึ่งแสดงภาพจำลองของการโจมตีที่เพิ่มเป้าหมายของการโจมตีเป็น 2 เครื่อง หลังจากที่เครื่อง A ส่งการโจมตีมายังเครื่อง B แล้ว เครื่อง A ได้ส่งการโจมตีชนิดเดิมไปยังเครื่อง C ด้วย ทำให้โปรแกรมเรียลซีเคียวตรวจพบเหตุการณ์โจมตี 2 เหตุการณ์ คือ เหตุการณ์การโจมตีที่เกิดจากต้นทางคือเครื่อง A มายังเป้าหมายของการโจมตีคือเครื่อง B และการโจมตีที่เกิดจากต้นทางคือเครื่อง A มายังเป้าหมายของการโจมตีอีกเครื่องหนึ่งซึ่งเป็นเครื่อง C โดยแต่ละเหตุการณ์โจมตีที่ตรวจพบจะแสดงจำนวนครั้งของการโจมตีในเหตุการณ์นั้นเป็นจำนวน 1 ครั้ง ซึ่งแต่ละครั้งของการโจมตีที่ตรวจพบอาจเกิดจากกลุ่มข้อมูลจำนวนมาก ซึ่งแตกต่างจากโปรแกรมสนอร์ทที่แจ้งเตือนทุกกลุ่มข้อมูลที่ตรวจวิเคราะห์แล้วพบว่าเป็นการโจมตี

3.7 การคำนวณผลที่บันทึกได้จากการทดลอง

เป็นการนำค่าที่บันทึกได้มาคำนวณเพื่อนำไปเป็นข้อมูลประกอบการวิเคราะห์ผลการทำงานของโปรแกรมตรวจหาการบุกรุก ซึ่งการคำนวณผลทั้งหมดแบ่งตามองค์ประกอบมีดังนี้

3.7.1 <u>การคำนวณผลที่ได้จากการบันทึกการทำงานของโปรแกรมสนอร์ท</u>

ก. เวลาล่าช้าในการแจ้งเตือน (Start Delay) เป็นช่วงเวลา (วินาที) ที่ใช้ในการวิเคราะห์ข้อมูลจนกระทั่งแจ้งเตือนครั้งแรก โดยคำนวณจากเวลาเริ่มต้นของการแจ้งเตือนและเวลาเริ่มต้นส่งการโจมตี ดังสมการ

$$\text{Start Delay} = T_{0s} - T_0$$

ข. เวลาล่าช้าในการหยุดแจ้งเตือน (Stop Delay) เป็นช่วงต่างของเวลาสุดท้ายของการแจ้งเตือนและเวลาหยุดส่งการโจมตี คำนวณได้จากสมการ

$$\text{Stop Delay} = T_{1s} - T_1$$

ค. เปอร์เซ็นต์การวิเคราะห์ข้อมูล (%Analyze) แสดงถึงความสามารถในการตรวจวิเคราะห์เพื่อค้นหาการโจมตีในช่วงเวลาของการทดลอง โดยเป็นสัดส่วนระหว่างจำนวนข้อมูลที่สามารถตรวจวิเคราะห์ได้กับจำนวนข้อมูลทั้งหมดที่โปรแกรมตรวจพบ ซึ่งคำนวณได้จากสมการ

$$\%\text{Analyze} = \frac{Analyze}{Total} * 100$$

ง. เปอร์เซ็นต์การทิ้งข้อมูล (%Drop) เป็นเปอร์เซ็นของจำนวนกลุ่มข้อมูลที่ไม่สามารถตรวจวิเคราะห์หาการโจมตีได้ในเวลานั้น สาเหตุเกิดจากข้อมูลที่นำมาวิเคราะห์ถูกส่งอย่างต่อเนื่องด้วยความเร็วสูง ซึ่งเปอร์เซ็นต์การทิ้งข้อมูลนี้คำนวณได้จากจำนวนกลุ่มข้อมูลที่โปรแกรมไม่สามารถตรวจวิเคราะห์ได้เทียบกับจำนวนกลุ่มข้อมูลทั้งหมดที่สนอร์ทตรวจพบ และค่าที่ได้จากการคำนวณนี้ยังเป็นส่วนกลับของเปอร์เซ็นต์การวิเคราะห์ข้อมูลดังสมการ

$$\%\text{Drop} = \frac{Drop}{Total} * 100$$

จ. เปอร์เซ็นต์การแจ้งเตือน (%Alert) เป็นเปอร์เซ็นต์ของจำนวนครั้งของการแจ้งเตือนที่เกิดขึ้นในขณะตรวจหาการโจมตีเทียบกับจำนวนกลุ่มข้อมูลทั้งหมดที่สนอร์ทตรวจวิเคราะห์ได้ทัน คำนวณได้จากสมการ

$$\%\text{Alert} = \frac{Alert}{Analyze} * 100$$

ฉ. เปอร์เซ็นต์ความผิดพลาดในการแจ้งเตือนเกินจริง (%False Positive) คำนวณจากจำนวนครั้งของการแจ้งเตือนที่มากกว่าการโจมตีที่ส่งออกไปเทียบกับจำนวนครั้งของการโจมตีที่ผู้โจมตีสร้างขึ้น ดังสมการ

$$\%\text{False positive} = \frac{Alert - Outgoing\ Packet_a}{Outgoing\ Packet_a} * 100$$

ช. เปอร์เซ็นต์ความผิดพลาดในการไม่แจ้งเตือนเมื่อถูกโจมตี (%False Negative) โดยคำนวณจากจำนวนครั้งของการโจมตีที่ไม่แจ้งเตือนเทียบกับจำนวนครั้งของการโจมตีที่ส่งออกไป แสดงได้ดังสมการ

$$\%\text{False negative} = \frac{Outgoing\ Packet_a - Alert}{Outgoing\ Packet_a} * 100$$

3.7.2 <u>การคำนวณผลที่ได้จากการบันทึกการทำงานของโปรแกรมเรียลซีเคียว</u>

ก. เวลาล่าช้าในการแจ้งเตือน (Start Delay) เป็นช่วงเวลา (วินาที) ที่ใช้ในการตรวจวิเคราะห์จนกระทั่งแจ้งเตือนครั้งแรก ซึ่งคำนวณจากเวลาเริ่มต้นของการแจ้งเตือนและเวลาเริ่มต้นส่งการโจมตี ดังสมการ

$$\text{Start Delay} = T_{0r} - T_0$$

ข. เวลาล่าช้าในการหยุดแจ้งเตือน (Stop Delay) เป็นช่วงต่างของเวลาระหว่างเวลาสุดท้ายของการแจ้งเตือนกับเวลาหยุดส่งการโจมตี ซึ่งโปรแกรมเรียลซีเคียวจะแสดงเวลาสุดท้ายของการแจ้งเตือนได้เมื่อเป็นการโจมตีที่สร้างการเชื่อมต่ออย่างต่อเนื่องจึงสามารถคำนวณหาค่านี้ได้เฉพาะการโจมตีนี้เท่านั้น ส่วนการโจมตีชนิดอื่นโปรแกรมจะแจ้งเตือนเมื่อตรวจพบการโจมตีในครั้งแรกเพียงครั้งเดียว การคำนวณหาเวลาล่าช้าในการหยุดแจ้งเตือนดังสมการ

$$\text{Stop Delay} = T_{1r} - T_1$$

ค. เปอร์เซ็นต์การวิเคราะห์ข้อมูล (%Analyze) เนื่องจากโปรแกรมเรียลซีเคียวตรวจหาการโจมตีและแจ้งเตือนตามเหตุการณ์โจมตี ดังนั้นการคำนวณหาเปอร์เซ็นต์การวิเคราะห์ข้อมูลจึงคำนวณจากจำนวนเหตุการณ์โจมตีที่ตรวจพบเทียบกับจำนวนเหตุการณ์โจมตีที่ผู้โจมตีสร้างขึ้น การคำนวณแสดงได้ดังสมการ

$$\%\text{Analyze} = \frac{Event}{No.of\ Attack\ Event} * 100$$

ง. เปอร์เซ็นต์การทิ้งข้อมูล (%Drop) คำนวณได้จากจำนวนเหตุการณ์โจมตีที่โปรแกรมตรวจไม่พบ เทียบกับจำนวนเหตุการณ์โจมตีที่สร้างขึ้น การคำนวณแสดงได้ดังสมการ

$$\%\text{Drop} = \frac{No.of\ Attack\ Event - Event}{No.of\ Attack\ Evetn} * 100$$

จ. เปอร์เซ็นต์การแจ้งเตือน (%Alert) คำนวณได้จากจำนวนครั้งของการแจ้งเตือนที่เกิดขึ้นในขณะตรวจหาการโจมตีเทียบกับจำนวนครั้งของการโจมตีที่ส่งออกไป การคำนวณแสดงได้ดังสมการ

$$\%\text{Alert} = \frac{Hit}{No.\ of\ Attack\ Hit} * 100$$

ฉ. เปอร์เซ็นต์ความผิดพลาดในการแจ้งเตือนเกินจริง (%False Positive) เป็นค่าความผิดพลาดที่เกิดขึ้นเมื่อตรวจพบการโจมตีโดยไม่มีการโจมตีนั้นเกิดขึ้นจริง คำนวณได้จากจำนวนครั้งของการแจ้งเตือนที่มากกว่าจำนวนครั้งการโจมตีที่ส่งออกไปเทียบกับจำนวนครั้งของการโจมตีที่สร้างขึ้น คำนวณได้ดังสมการ

$$\%\text{False positive} = \frac{Hit - No.of\ Attack\ Hit}{No.of\ Attack\ Hit} * 100$$

ช. เปอร์เซ็นต์ความผิดพลาดในการไม่แจ้งเตือนเมื่อถูกโจมตี (%False Negative) เป็นค่าความผิดพลาดที่พบเมื่อโปรแกรมตรวจหาการบุกรุกไม่แจ้งเตือนเมื่อถูกโจมตี โดยคำนวณจากจำนวนครั้งของการโจมตีที่ไม่แจ้งเตือนเทียบกับจำนวนครั้งของการโจมตีที่ส่งออกไป คำนวณได้ดังสมการ

$$\%\text{False negative} = \frac{No.of\ Attack\ Hit - Hit}{No.of\ Attack\ Hit} * 100$$

3.7.3 การคำนวณผลที่ได้จากการบันทึกการทำงานของผู้โจมตี

ก. เวลาในการทดลอง (Test Time) เป็นช่วงเวลาตั้งแต่เริ่มส่งการโจมตีจนกระทั่งหยุดส่งการโจมตี (วินาที) คำนวณได้ดังสมการ

$$\text{Test Time} = T_1 - T_0$$

ข. อัตราเร็วในการโจมตี (Attack Rate) แสดงถึงความสามารถในการสร้างการโจมตี (ไบต์ต่อวินาที) โดยคำนวณจากจำนวนไบต์ข้อมูลทั้งหมดที่ส่งออกไปจากผู้โจมตีเทียบกับเวลาทั้งหมดที่ส่งการโจมตีออกมา การคำนวณแสดงได้ดังสมการ

$$\text{Attack Rate} = \frac{Outgoing\ Byte_a}{Test\ Time}$$

3.7.4 การคำนวณผลที่ได้จากการบันทึกการทำงานของผู้ถูกโจมตี

ก. ปริมาณข้อมูลของที่เกิดขึ้นบนส่วนต่อประสาน (Target Traffic) คำนวณได้จากจำนวนกลุ่มข้อมูลทั้งหมดที่เกิดขึ้นบนส่วนต่อประสานของเครื่องเทียบกับเวลาทั้งหมดของการทดลองนั้น แสดงได้ดังสมการ

$$\text{Target Traffic} = \frac{Total\ Byte_t}{Test\ Time}$$

3.7.5 การคำนวณผลที่ได้จากการบันทึกการทำงานของเครื่องไคลเอนท์

ก. เปอร์เซ็นต์ของข้อมูลที่ปนกับการโจมตี (%Data) เป็น

$$\%\text{Data} = \frac{Total\ Byte_c}{Total\ Byte_t} * 100$$

3.7.6 การคำนวณผลที่ได้จากการบันทึกการทำงานของผู้ตรวจสอบเครือข่าย

ก. ปริมาณข้อมูลในเครือข่าย (Monitor Traffic) คำนวณได้จากจำนวนกลุ่มข้อมูลทั้งหมดที่เกิดขึ้นบนเครือข่ายเทียบกับเวลาทั้งหมดของการทดลองครั้งนั้น

$$\text{Monitor Traffic} = \frac{Total\ Byte_m}{Test\ Time}$$

3.8 เกณฑ์ในการทดสอบการทำงาน

การทำงานของโปรแกรมตรวจหาการบุกรุกขึ้นอยู่กับปัจจัยและความสามารถในการทำงานดังต่อไปนี้

3.8.1 ความสามารถในการตรวจวิเคราะห์ พิจารณาจากเปอร์เซ็นต์การตรวจวิเคราะห์และสรุปว่าโปรแกรมสามารถตรวจวิเคราะห์ได้ดีเมื่อโปรแกรมสามารถตรวจวิเคราะห์ข้อมูลได้มากกว่า 80% ของกลุ่มข้อมูลในเครือข่าย

3.8.2 การตรวจพบการโจมตีได้เร็ว เป็นการวิเคราะห์ช่วงเวลาที่โปรแกรมใช้เริ่มตั้งแต่ตรวจวิเคราะห์ข้อมูลจนกระทั่งแจ้งเตือน โดยในการทดลองนี้หากใช้เวลาในการแจ้งเตือนนานกว่า 5 วินาทีเป็นต้นไป จึงจะสรุปว่าโปรแกรมใช้เวลาในการตรวจพบการโจมตีนั้นได้รวดเร็ว ซึ่งเป็นเวลานานเพียงพอที่ผู้โจมตีจะทำความเสียหายต่อระบบได้

3.8.3 ไม่เกิดการแจ้งเตือนเกินจริง การแจ้งเตือนที่มีมากเกินกว่าการโจมตีที่เกิดขึ้นจริงหรือมีการแจ้งเตือนทั้งที่ไม่มีการโจมตีเกิดขึ้น แสดงถึงข้อผิดพลาดในการตรวจหาการโจมตีของโปรแกรม การแจ้งเตือนเกินจริงเพียงเล็กน้อยจะช่วยเตือนให้ผู้ดูแลระบบให้ความสนใจกับพฤติกรรมหรือเหตุการณ์นั้นๆ แต่ถ้าการแจ้งเตือนเกิดขึ้นมากเกินไปจะส่งผลให้ความน่าเชื่อถือของโปรแกรมลดลง

3.8.4 การแจ้งเตือนทุกครั้งเมื่อถูกโจมตี โปรแกรมตรวจหาการบุกรุกจะมีหน้าที่ค้นหาการบุกรุกและแจ้งเตือนเมื่อตรวจพบการบุกรุก หากเกิดการโจมตีแล้วโปรแกรมตรวจไม่พบการโจมตี สาเหตุอาจเนื่องมาจากรูปแบบของการโจมตีนั้นไม่มีอยู่ในกฎเกณฑ์รูปแบบหรือมีปัจจัยอื่นที่ช่วยซ่อนการโจมตีนั้น ทำให้เกิดการโจมตีแล้วโปรแกรมไม่แจ้งเตือน ผู้โจมตีอาจจะทำลายระบบหรือคัดลอกข้อมูลได้สำเร็จอย่างง่ายดายโดยไม่มีการต่อต้านหรือตอบสนองต่อการโจมตีนั้น

3.8.5 ความถูกต้องของการแจ้งเตือน เมื่อตรวจพบการโจมตีแล้วต้องพิจารณาถึงรายละเอียดของข้อความแจ้งเตือนว่าตรงกับการโจมตีที่เกิดขึ้นหรือไม่ หากข้อความแจ้งเตือนที่เกิดขึ้นมีรายละเอียดไม่ครบถ้วน รายละเอียดบางส่วนหรือส่วนใหญ่ไม่ตรงกับความเป็นจริง เช่น แสดงเลขที่อยู่ของผู้โจมตีหรือผู้ถูกโจมตีผิดไป ไม่แสดงเลขที่อยู่ไอพีของผู้โจมตี หรือแสดงรายละเอียดเกี่ยวกับการโจมตีผิดไป เป็นต้น ทำให้ผู้ดูแลระบบวิเคราะห์เหตุการณ์โจมตีผิดจากความเป็นจริงส่งผลให้ไม่สามารถยับยั้งหรือตอบสนองต่อการโจมตีผิดพลาด

3.8.6 การใช้งานซีพียู เมื่อโปรแกรมสามารถตรวจวิเคราะห์การโจมตีได้แต่ต้องใช้งานซีพียูสูง ขณะที่โปรแกรมตรวจวิเคราะห์การโจมตีที่มีความรุนแรงมากอย่างต่อเนื่องอาจส่งผลให้เครื่องหยุดการทำงานลงได้ โดยในงานวิจัยนี้จะสรุปว่าโปรแกรมตรวจหาใช้งานซีพียูต่ำเมื่อมีการใช้งานซีพียูน้อยกว่า 90 เปอร์เซ็นต์

บทที่ 4

การวิเคราะห์ผลการวิจัย

ในบทนี้กล่าวถึงเครื่องมือที่ใช้ในงานวิจัย ผลการทดสอบการตรวจหาการบุกรุกของโปรแกรมสนอร์ทและเรียลซีเคียวในสภาพแวดล้อมของการโจมตีชนิดเดียว ในสภาพแวดล้อมของการโจมตีชนิดเดียวมีข้อมูล และในสภาพแวดล้อมของการโจมตีหลายชนิดผสมกัน

4.1 เครื่องมือที่ใช้ในการวิจัย

งานวิจัยนี้ได้ทำการทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกเครือข่ายแลน เนื่องจากโปรแกรมตรวจหาการบุกรุกทั้งสองจะต้องวิเคราะห์ข้อมูลทั้งหมดบนเครือข่าย ดังนั้นในการทดลองทั้งหมดจึงเลือกใช้ฮับศูนย์กลางของการเชื่อมต่อ ในการทดลองทั้งหมดจะใช้เครื่องมือและโปรแกรม ดังนี้

4.1.1 เครื่องคอมพิวเตอร์รุ่น Celeron 733 MHz, หน่วยความจำหลัก (RAM) 128 MB

4.1.2 ฮับ (HUB) Linksys รุ่น EF2H24

4.1.3 โปรแกรมสนอร์ทเวอร์ชัน 1.8.3 ทำงานบนระบบปฏิบัติการลินุกซ์

4.1.4 โปรแกรมเรียลซีเคียวเวิร์คกรุปเมเนเจอร์ (RealSecure Workgroup Manager) เวอร์ชัน 6.5 ทำงานบนระบบปฏิบัติการวินโดวส์ 2000 โปรเฟสชันนอล

4.1.5 โปรแกรมเรียลซีเคียวเน็ตเวิร์คเซ็นเซอร์ (RealSecure Network Sensor) เวอร์ชัน 6.5 (สำหรับทดลองใช้)

4.1.6 โปรแกรมไอพีทราฟ (IPTraf) เวอร์ชัน 2.5.3 ใช้สำหรับบันทึกปริมาณข้อมูลที่เกิดขึ้นบนเครือข่ายหรือปริมาณข้อมูลที่เกิดขึ้นบนส่วนต่อประสาน โดยทำงานบนระบบปฏิบัติการลินุกส์

4.1.7 โปรแกรมดึงข้อมูลจากเครื่องบริการเว็บ (Wget) เวอร์ชัน 1.8.2

4.2 การทดสอบเบื้องต้น

ก่อนทำการทดสอบในสภาพแวดล้อมที่กำหนดได้ทำการทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกโดยทดลองส่งการโจมตีแต่ละชนิดไปยังเป้าหมายเพื่อค้นหาข้อความแจ้งเตือนที่เกิดขึ้นและปรับแต่กฎเกณฑ์ให้เหมาะสมกับการทดลอง จากการทดสอบพบว่าการใช้กฎเกณฑ์มาตรฐานที่มากับโปรแกรมจะทำให้เกิดความผิดพลาดในการแจ้งเตือนน้อยกว่าการเพิ่มกฎเกณฑ์ใหม่ลงไป ดังนั้นในงานวิจัยนี้จึงใช้กฎเกณฑ์มาตรฐานที่มาพร้อมโปรแกรม นอกจากนี้ยังพบว่าโปรแกรมสนอร์ททำการแจ้งเตือนอย่างต่อเนื่องตั้งแต่ตรวจพบการโจมตีไปจนกระทั่งการโจมตีนั้นถูกยกเลิก ส่วนโปรแกรมเรียลซีเคียวจะแจ้งเตือนตามเหตุการณ์ โดยพิจารณาจากคอนเน็กชันและชนิดของการโจมตีแล้วแสดงข้อความแจ้งเตือนตามเหตุการณ์โจมตี ซึ่งในการทดลองพบว่าการโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมากเพียงชนิดเดียวที่ทำให้โปรแกรมเรียลซีเคียวจะแจ้งเตือนหนึ่งเหตุการณ์และมีจำนวนครั้งของการโจมตีเป็นจำนวนมาก ส่วนการโจมตีชนิดอื่นโปรแกรมเรียลซีเคียวจะแจ้งเตือนหนึ่งเหตุการณ์และมีจำนวนครั้งของการโจมตีเพียงครั้งเดียว โดยข้อความแจ้งเตือนที่เกิดขึ้นทั้งหมดสามารถสรุปได้ดังตารางที่ 4.1

ตารางที่ 4.1 ข้อความแจ้งเตือนจากการทดลองเบื้องต้น

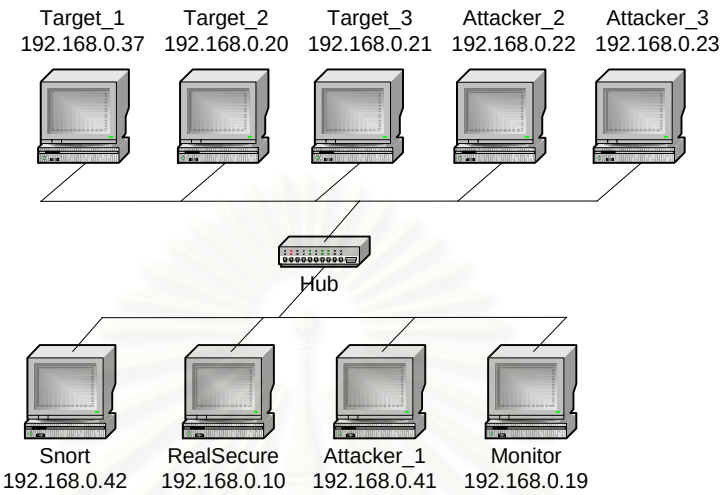
การโจมตี	ข้อความแจ้งเตือนของ โปรแกรมสนอร์ท	ข้อความแจ้งเตือนของ โปรแกรมเรียลซีเคียว
Smurf	MISC Large ICMP packet	Ping Flood (Low priority)
Scan port	Spp_portscan ICMP Destination Unreachable (port unreachable)	Portscan (Medium priority)
Synflood	ICMP Destination Unreachable (port unreachable)	Synflood (Medium priority)
Ping flood	ICMP_PING *NIX	Ping Flood (Low priority)

4.3 ผลการทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียว

การทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมนี้แบ่งออกเป็นการทดลองย่อยได้ 4 ชุด สำหรับการโจมตีแต่ละชนิดโดยมีเงื่อนไขในการทดลองเหมือนกัน

เริ่มจากผู้โจมตีที่ 1 ซึ่งใช้เลขที่อยู่ไอพี192.168.0.41 ส่งการโจมตีจำนวน 1 เซสชันไปยังเป้าหมายที่ 1 ซึ่งใช้เลขที่อยู่ไอพี 192.168.0.37 เมื่อครบเวลาทดลอง 10 นาที จึงเปลี่ยนแปลงความเร็วของการโจมตีด้วยการเพิ่มจำนวนเซสชันของผู้โจมตีขึ้นเป็น 2 และ 3 เซสชันตามลำดับ

หลังจากนั้นจึงเปลี่ยนแปลงความเร็วในการโจมตีด้วยการเพิ่มจำนวนผู้โจมตีขึ้นเป็น 2 และ 3 โดยส่งการโจมตีจากผู้โจมตีละ 2 เซสชัน โดยมีผังเครือข่ายของการทดลองดังรูปที่ 4.1



รูปที่ 4.1 ผังเครือข่ายการทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียว

เมื่อนำผลที่บันทึกได้จากการทดลอง (ในภาคผนวก ค) มาคำนวณผล (ในภาคผนวก ง) แล้วนำมาแยกวิเคราะห์ตามเกณฑ์การทดสอบได้ผลการวิเคราะห์ดังนี้

4.3.1 <u>ความสามารถในการตรวจวิเคราะห์</u>

จากการทดลองพบว่าพฤติกรรมการโจมตีแต่ละชนิดมีอัตราเร็วในการโจมตีต่างกันส่งผลให้ปริมาณการไหลของข้อมูลในเครือข่ายแตกต่างกัน ในขณะทำการทดสอบโดยส่งการโจมตีที่ต้องการก่อกวนระบบ โปรแกรมสนอร์ทสามารถตรวจวิเคราะห์ได้น้อยกว่า 10% ของการโจมตีที่เกิดขึ้นทั้งหมดส่วนการโจมตีด้วยการกราดตรวจซึ่งเป็นการโจมตีที่ไม่เน้นความเร็วโปรแกรมสนอร์ทจึงตรวจวิเคราะห์ได้สูงถึง 100 เปอร์เซ็นต์ ส่วนโปรแกรมเรียลซีเคียวสามารถแจ้งเตือนได้ครบทุกเหตุการณ์

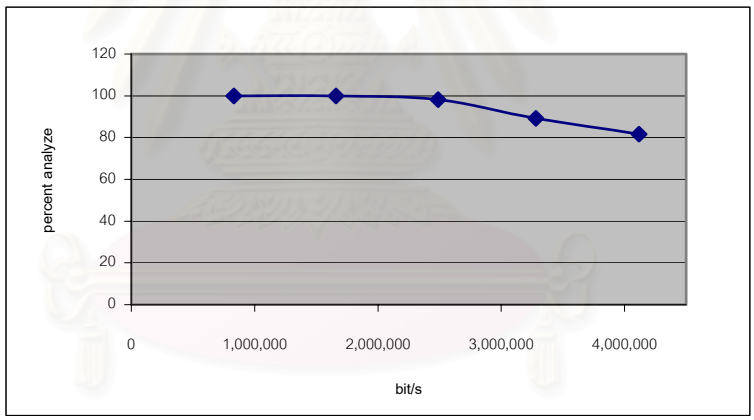
เมื่อเพิ่มความเร็วในการโจมตีด้วยการเพิ่มเซสชันของการโจมตี พบว่าการโจมตีด้วยการกราดตรวจและการโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์ทำให้ความเร็วและปริมาณข้อมูลที่ไหลในเครือข่ายสูงขึ้น ส่วนการโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมากทำให้ความเร็วในการโจมตีใกล้เคียงกันแต่ปริมาณข้อมูลที่ไหลในเครือข่ายสูงขึ้น และการโจมตีด้วยกลุ่มข้อมูลจำนวนมากทำให้ความเร็วของการโจมตีลดลงแต่ทำให้ปริมาณข้อมูลในเครือข่ายสูงขึ้น เมื่อทดลองเปลี่ยนแปลงความเร็วในการโจมตีทำให้ทราบว่าปริมาณข้อมูลที่ไหลใน

เครือข่ายนี้เองที่ส่งผลกระทบโดยตรงต่อความสามารถในการตรวจวิเคราะห์ ดังตัวอย่างผลการทดลองในตาราง 4.2

ตารางที่ 4.2 ตัวอย่างผลการทดลอง

ความเร็วของการโจมตี (bit/s)	**เปอร์เซ็นต์การวิเคราะห์**	**เปอร์เซ็นต์การดร๊อป**
831,421	100	0.000
1,660,215	100	0.000
2,487,381	98	1.770
3,281,248	89	10.777
4,118,135	81	18.266

จากข้อมูลในตารางที่ 4.2 เป็นตัวอย่างซึ่งได้จากการทดลองส่งการโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์ เมื่อนำเปอร์เซ็นต์การวิเคราะห์ข้อมูลและความเร็วของการโจมตีมาเขียนกราฟจะมีแนวโน้มดังรูป



รูปที่ 4.2 กราฟแสดงความสัมพันธ์ระหว่างอัตราเร็วในการโจมตีกับเปอร์เซ็นต์การวิเคราะห์ข้อมูล

4.3.2 <u>เวลาที่ใช้ในการตรวจพบการโจมตี</u>

โปรแกรมสนอร์ทยังใช้เวลาตรวจพบการโจมตีใกล้เคียงกันทุกการโจมตี ส่วนโปรแกรมเรียลซีเคียวใช้เวลานานขึ้นถ้าเป็นการโจมตีด้วยการกราดตรวจ

4.3.3 ไม่เกิดการแจ้งเตือนเกินจริง

ข้อความแจ้งเตือนที่บันทึกได้จากการทดลองแสดงได้ดังตารางที่ 4.3

ตารางที่ 4.3 ข้อความแจ้งเตือนเมื่อทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียว

การโจมตี	ข้อความแจ้งเตือนของโปรแกรมสนอร์ท	ข้อความแจ้งเตือนของโปรแกรมเรียลซีเคียว
Smurf	MISC Large ICMP packet	Ping Flood IP Duplicate
Scan port	Spp_portscan ICMP Destination Unreachable (port unreach)	Portscan
Synflood	ICMP Destination Unreachable (port unreach)	Synflood
Ping flood	ICMP_PING *NIX	Ping Flood Loki

เมื่อนำข้อความแจ้งเตือนที่ได้มาเปรียบเทียบกับข้อความแจ้งเตือนที่ได้ทดลองไว้เบื้องต้นพบการแจ้งเตือนเกินจริงดังตารางที่ 4.4

ตารางที่ 4.4 ข้อความแจ้งเตือนเกินจริงเมื่อทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียว

การโจมตี	ข้อความแจ้งเตือนของโปรแกรมสนอร์ท	ข้อความแจ้งเตือนของโปรแกรมเรียลซีเคียว
Smurf	-	IP Duplicate
Ping flood	-	Loki

จากการเปรียบเทียบการแจ้งเตือนที่เกิดขึ้นในการทดลองทั้งหมดกับการแจ้งเตือนที่ได้จากการทดลองเบื้องต้นพบว่าโปรแกรมเรียลซีเคียวเกิดการแจ้งเตือนเกินจริง ได้แก่ การแจ้งเตือนที่เกิดขึ้นเมื่อตรวจพบกลุ่มข้อมูลที่มีเลขที่อยู่ไอพีเดียวกันแต่มีเลขที่อยู่ของอีเทอร์เน็ตแตกต่างกัน (IPDuplicate) และการแจ้งเตือนเกินจริงที่เกิดจากการตรวจพบปิงจำนวนมาก (LOKI) ส่วนโปรแกรมสนอร์ทไม่พบการแจ้งเตือนเกินจริง

4.3.4 แจ้งเตือนทุกครั้งเมื่อถูกโจมตี

ปริมาณข้อมูลที่ไหลในเครือข่ายที่สูงขึ้นจะทำให้ความสามารถในการตรวจวิเคราะห์ของโปรแกรมสนอร์ทลดลงจึงตรวจไม่พบการโจมตี และส่งผลทำให้โปรแกรมเรียลซีเคียวเกิดความผิดพลาดในการแจ้งเตือนทั้งการแจ้งเตือนเกินจริงและไม่แจ้งเตือนด้วย แต่การแจ้งเตือน

ไม่ครบทุกครั้งที่เกิดการโจมตีสำหรับการโจมตีชนิดเดียวจะไม่ส่งผลกระทบต่อความน่าเชื่อถือของระบบเนื่องจากการแจ้งเตือนที่เกิดขึ้นเพียงพอที่จะบอกได้ว่าเกิดเหตุการณ์ใด

4.3.5 <u>ความถูกต้องของการแจ้งเตือน</u>

จากการตรวจสอบรายละเอียดของข้อความแจ้งเตือนพบว่าโปรแกรมเรียลซีเคียวสามารถแจ้งเตือนได้อย่างถูกต้องตามพฤติกรรมการโจมตีนั้น ซึ่งแตกต่างจากสนอร์ทที่ไม่สามารถแสดงเลขที่อยู่ไอพีของเครื่องเป้าหมายที่ถูกกราดตรวจทีซีพีพอร์ตและไม่สามารถแสดงเลขที่อยู่ไอพีที่ถูกซ่อนไว้ได้

4.3.6 <u>การใช้งานซีพียู</u>

โปรแกรมสนอร์ทใช้งานซีพียูสูงถึง 100% ซึ่งเท่ากับโปรแกรมเรียลซีเคียวเมื่อส่งการโจมตีที่ต้องต้องการก่อกวนระบบ ยกเว้นการโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์ (Smurf) ที่โปรแกรมสามารถวิเคราะห์ได้ดีและใช้งานซีพียูต่ำกว่า 20 เปอร์เซ็นต์ ส่วนการโจมตีด้วยการกราดตรวจซึ่งเป็นการโจมตีที่ไม่เน้นความเร็วโปรแกรมสนอร์ทใช้งานซีพียูต่ำกว่า 5 เปอร์เซ็นต์ จากการผลทดลองทั้งหมดในสภาพแวดล้อมของการโจมตีชนิดเดียวสามารถสรุปโดยย่อได้ดังตารางที่ 4.5 และ 4.6

ตารางที่ 4.5 สรุปผลการทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียว

การโจมตี	SYN Flood		Smurf		Ping Flood		Scan Port	
ระบบตรวจหาการบุกรุก / **เกณฑ์การวัด**	สนอร์ท	เรียลซีเคียว	สนอร์ท	เรียลซีเคียว	สนอร์ท	เรียลซีเคียว	สนอร์ท	เรียลซีเคียว
สามารถตรวจวิเคราะห์ได้ดี (>80%)	✗	✗	✓	✓	✗	✓	✓	✓
ตรวจพบการโจมตีได้เร็ว (<5 วินาที)	✓	✓	✓	✓	✓	✓	✓	✗
ไม่เกิดการแจ้งเตือนเกินจริง	✓	✓	✓	✗	✗	✗	✓	✓
แจ้งเตือนทุกครั้งเมื่อถูกโจมตี	✗	✗	✓	✗	✗	✗	✓	✓
มีความถูกต้องของการแจ้งเตือน	✓	✓	✗	✗	✓	✓	✗	✓
ใช้งานซีพียูต่ำ (<90%)	✗	✗	✓	✓	✗	✗	✓	✓

หมายเหตุ เครื่องหมาย ✓ หมายถึง ถูกต้องหรือเป็นจริง

เครื่องหมาย ✗ หมายถึง ไม่ถูกต้องหรือเป็นเท็จ

ตาราง 4.6 ผลการเปรียบเทียบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมของการโจมตีชนิดเดียว

เกณฑ์การเปรียบเทียบ	โปรแกรมสนอร์ท	โปรแกรมเรียลซีเคียว
ความสามารถในการตรวจวิเคราะห์	สามารถตรวจวิเคราะห์ได้ดีเมื่อเกิดการโจมตีที่ไม่มีความเร็วมากนัก เช่น การโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์และการกราดตรวจที่ซีพีพอร์ต ส่วนการโจมตีที่อาศัยความเร็วในการโจมตีจะทำให้ปริมาณข้อมูลในเครือข่ายมีมาก โปรแกรมจะไม่สามารถตรวจวิเคราะห์ได้ครบถ้วนทันเหตุการณ์ได้ทั้งหมด แต่การแจ้งเตือนที่เกิดขึ้นก็เพียงพอที่จะบ่งบอกถึงการโจมตีที่เกิดขึ้นได้ถูกต้อง	สามารถตรวจวิเคราะห์ได้ดีเพราะวิเคราะห์จากความครบถ้วนของการแจ้งเตือนที่เกิดขึ้น ซึ่งโปรแกรมสามารถแจ้งเตือนครบทุกเหตุการณ์ มีเพียงการโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมากเพียงชนิดเดียวที่โปรแกรมไม่สามารถนับจำนวนครั้งของการโจมตีได้มากกว่าหนึ่งครั้ง
ความเร็วในการตรวจพบการโจมตี	ใช้เวลาในการตรวจพบการโจมตีทุกชนิดอย่างรวดเร็วใกล้เคียงกัน	ตรวจพบการโจมตีรวดเร็วถ้าเป็นการโจมตีด้วยการส่งข้อมูลจำนวนมาก (Flood) แต่จะใช้เวลาในการตรวจพบการโจมตีมากขึ้นเมื่อเป็นการโจมตีด้วยการกราดตรวจที่ซีพีพอร์ต
ความผิดพลาดในการแจ้งเตือน	ความผิดพลาดในการไม่แจ้งเตือนเมื่อถูกโจมตีจะเกิดขึ้นเมื่อตรวจหาการโจมตีที่มีความเร็วมาก	ตรวจพบการแจ้งเตือนเกินจริง เมื่อเป็นการโจมตีที่มีลักษณะซ่อน เช่น ซ่อนเลขที่อยู่ไอพีของการโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์ (Smurf)

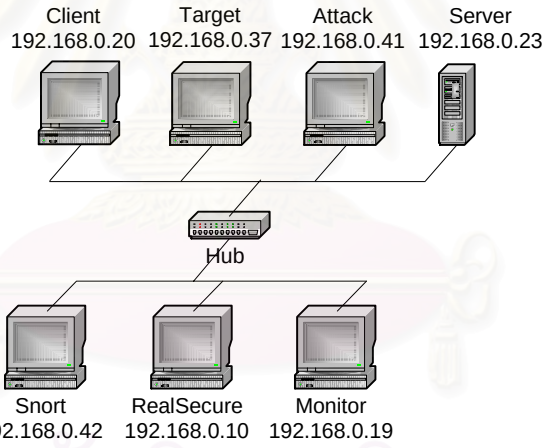
ตาราง 4.6 ผลการเปรียบเทียบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมของการโจมตีชนิดเดียว (ต่อ)

เกณฑ์การเปรียบเทียบ	โปรแกรมสนอร์ท	โปรแกรมเรียลซีเคียว
ความถูกต้องของการแจ้งเตือน	- การกราดตรวจทีซีพีพอร์ตแสดงการแจ้งเตือนถึงการโจมตีจากต้นทางที่ถูกต้อง แต่ไม่บอกเลขไอพีของเป้าหมาย - การโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์จะแสดงเลขไอพีต้นทางเป็นเลขไอพีปลอม ซึ่งเป็นเลขไอพีเป้าหมายของการโจมตี และไม่สามารถบอกเลขไอพีของผู้สร้างการโจมตีได้ - การโจมตีด้วยกลุ่มข้อมูลจำนวนมากจะแสดงเลขไอพีต้นทางและปลายทางได้อย่างถูกต้อง - การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมากจะแสดงเลขไอพีต้นทาง ปลายทางและพอร์ตที่ถูกสแกนได้อย่างถูกต้อง	- การกราดตรวจทีซีพอร์ตแสดงรายละเอียดได้อย่างถูกต้อง - การโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์แสดงเลขไอพีต้นทางเป็นเลขไอพีปลอม (เป็นเลขไอพีเป้าหมายของการโจมตี) และสามารถแสดงรายละเอียดของเลขที่อยู่อีเทอร์เน็ตต้นทาง (Source Ethernet Address) ของผู้โจมตีได้อย่างถูกต้อง - การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมากจะแสดงเลขไอพีต้นทางเป็น 0.0.0.0 ซึ่งเป็นเลขไอพีปลอม และแสดงเลขไอพีจริงซึ่งเป็นผู้โจมตีพร้อมทั้งเลขที่อยู่อีเทอร์เน็ตต้นทางได้อย่างถูกต้อง
การใช้งานซีพียู	ใช้ซีพียูต่ำเมื่อเป็นการโจมตีที่มีความเร็วต่ำ	ใช้ซีพียูต่ำเมื่อเป็นการโจมตีที่มีความเร็วต่ำ

ทั้งนี้ค่าความสามารถในการตรวจวิเคราะห์ของสนอร์ทไม่ใช่ตัวเลขที่จะยืนยันว่าสนอร์ททำงานได้อย่างถูกต้อง เมื่อสนอร์ทไม่สามารถตรวจวิเคราะห์ข้อมูลได้ครบทั้งหมด อาจจะทำให้ไม่แจ้งเตือนเมื่อถูกโจมตี แต่การตรวจวิเคราะห์ได้ทั้งหมดและแจ้งเตือนทุกครั้งที่ถูกโจมตีก็ไม่มีความจำเป็นถ้าการโจมตีที่เกิดขึ้นเป็นการโจมตีที่มีลักษณะเหมือนเดิม และค่าการตรวจวิเคราะห์ได้สูงไม่ได้เป็นตัวบ่งชี้ว่าโปรแกรมจะทำงานได้อย่างถูกต้อง ทั้งนี้ต้องขึ้นอยู่กับกฎเกณฑ์ที่มีอยู่ว่าถูกต้องและตรงกับการโจมตีนั้นมากน้อยเพียงไร

4.4 ผลการทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียวมีข้อมูล

ในการทดลองนี้มีสภาพแวดล้อมในการทดลองเหมือนกับสภาพแวดล้อมที่มีการโจมตีชนิดเดียวแต่เพิ่มเครื่องบริการเว็บและไคลเอนท์ เมื่อเริ่มการทดลองไคลเอนท์ดึงข้อมูลจากเครื่องบริการเว็บพร้อมกันกับผู้โจมตีสร้างการโจมตีไปยังเป้าหมาย ผังเครือข่ายของการทดลองแสดงได้ดังรูปที่ 4.3



รูปที่ 4.3 ผังเครือข่ายของการทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียวมีข้อมูล

จากการทดลองพบว่าปริมาณข้อมูลที่เพิ่มขึ้นทำให้สนอร์ทใช้เวลาในการตรวจวิเคราะห์เพิ่มขึ้นเป็น 4-5 วินาที จากเดิมใช้เวลาประมาณ 1-2 วินาที ส่วนโปรแกรมเรียลซีเคียวเกิดการไม่แจ้งเตือนเมื่อถูกโจมตี ซึ่งข้อมูลเข้ามาปนมีส่วนทำให้ปริมาณข้อมูลที่ไหลในเครือข่ายสูงขึ้นส่งผลให้ความสามารถในการตรวจวิเคราะห์ลดลงเมื่อเทียบกับการส่งการโจมตีโดยไม่มีข้อมูลปะปน โปรแกรมต้องใช้งานซีพียูสูงขึ้น (สำหรับการโจมตีด้วยการกราดตรวจ)

ข้อความแจ้งเตือนที่เกิดขึ้นในขณะทำการทดลอง เมื่อนำมาเปรียบเทียบกับข้อความแจ้งเตือนจากการทดลองเบื้องต้นจะพบข้อความแจ้งเตือนเกินจริงดังตารางที่ 4.7

ตารางที่ 4.7 ข้อความแจ้งเตือนเมื่อทดลองในสภาพแวดล้อมของการโจมตีมีข้อมูล

การโจมตี	ข้อความแจ้งเตือนของโปรแกรมสนอร์ท	ข้อความแจ้งเตือนของโปรแกรมเรียลซีเคียว
Smurf	-	IP Duplicate
Scan port	-	-
Synflood	Scan myscan MISC Source port 20 to < 1024 Bad Traffic Port 0	IP Duplicate
Ping flood	-	Loki

ผลการทดลองทั้งหมดในสภาพแวดล้อมของการโจมตีมีข้อมูลสรุปได้ดังตารางที่ 4.8

ตารางที่ 4.8 สรุปผลการทดลองในสภาพแวดล้อมของการโจมตีชนิดเดียวมีข้อมูล

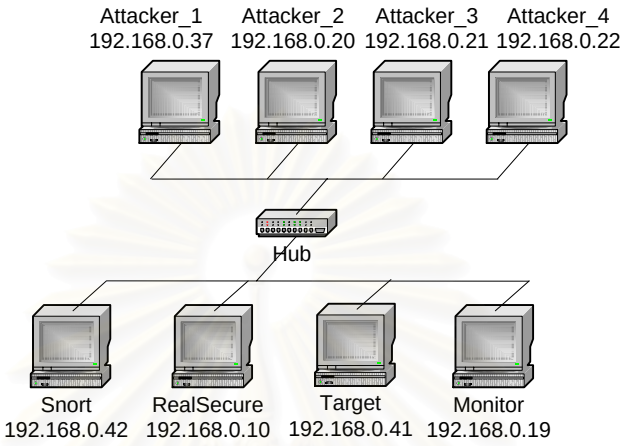
การโจมตี	SYN Flood		Smurf		Ping Flood		Scan Port	
ระบบตรวจหาการบุกรุก / เกณฑ์การวัด	สนอร์ท	เรียลซีเคียว	สนอร์ท	เรียลซีเคียว	สนอร์ท	เรียลซีเคียว	สนอร์ท	เรียลซีเคียว
สามารถตรวจวิเคราะห์ได้ดี (>80%)	✘	✘	✘	✓	✘	✓	✘	✓
ตรวจพบการโจมตีได้เร็ว (<5 วินาที)	✓	✘	✓	✘	✓	✓	✓	✘
ไม่เกิดการแจ้งเตือนเกินจริง	✘	✓	✓	✘	✓	✓	✓	✓
แจ้งเตือนทุกครั้งเมื่อถูกโจมตี	✘	✘	✓	✘	✓	✘	✓	✓
ความถูกต้องของการแจ้งเตือน	✓	✓	✘	✘	✓	✓	✘	✓
ใช้งานซีพียูต่ำ (<90%)	✘	✘	✘	✘	✘	✘	✘	✘

4.5 ผลการทดลองในสภาพแวดล้อมของการโจมตีหลายชนิดผสมกัน

การทดลองในสภาพแวดล้อมนี้แบ่งออกเป็น 3 ส่วนย่อยคือ การทดลองโดยส่งการโจมตีจากผู้โจมตี 4 เครื่องไปยังเป้าหมายเดียวกัน การส่งการโจมตีจากผู้โจมตีเดียวไปยังเป้าหมายหลายแห่ง และการส่งการโจมตีจากผู้โจมตีเดียวไปยังเป้าหมายเดียวกัน

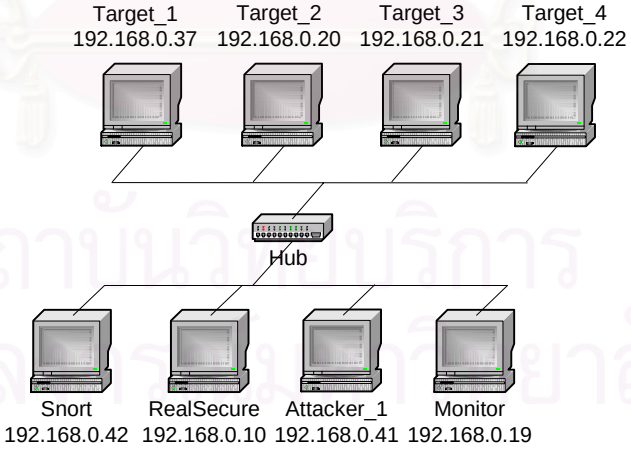
จากการทดลองพบว่าการจัดส่งการโจมตีจากผู้โจมตี 4 เครื่องไปยังเป้าหมายเดียวกันจะให้ความรุนแรงของการโจมตีสูงที่สุด ซึ่งส่งผลให้ความสามารถในการตรวจวิเคราะห์ของสนอร์ท

ลดลงจนเหลือเพียง 1 เปอร์เซ็นต์ ใช้เวลาในการแจ้งเตือน 0 วินาทีและเกิดการไม่แจ้งเตือนเมื่อถูกโจมตี ส่วนโปรแกรมเรียลซีเคียวใช้เวลาในการแจ้งเตือนครั้งแรกสูงถึง 20 วินาทีและไม่สามารถแจ้งเตือนได้ครบทุกเหตุการณ์ของการโจมตีที่ส่งออกไป โดยมีผังเครือข่ายของการทดลองดังรูปที่ 4.4



รูปที่ 4.4 ผังเครือข่ายของการส่งการโจมตีจาก 4 ผู้โจมตีเดียวไปยังเป้าหมายเดียวกัน

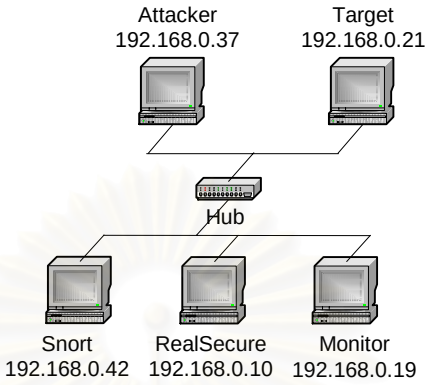
การทดลองโดยส่งการโจมตีจากผู้โจมตีเดียวไปยังเป้าหมายหลายแห่ง พบว่าโปรแกรมสนอร์ทตรวจวิเคราะห์ได้ดีกว่าการทดลองอื่นในสภาพแวดล้อมเดียวกัน ใช้เวลาในการแจ้งเตือนไม่แตกต่างจากเดิมมากนัก ซึ่งผังเครือข่ายที่ใช้ในการทดลองแสดงได้ดังรูปที่ 4.5



รูปที่ 4.5 ผังเครือข่ายของการส่งการโจมตีจากผู้โจมตีเดียวไปยังเป้าหมาย 4 แห่ง

การทดลองโดยส่งการโจมตีจากผู้โจมตีเดียวไปยังเป้าหมายแห่งเดียว พบว่าการสร้างการโจมตีรูปแบบนี้ให้ความเร็วในการโจมตีต่ำที่สุด ทำให้สนอร์ทสามารถวิเคราะห์ได้ดีที่สุด แต่ทั้ง

สองโปรแกรมยังคงเกิดการไม่แจ้งเตือนเมื่อถูกโจมตีอยู่ โดยมีผังเครือข่ายของการทดลองแสดงได้ดังรูปที่ 4.6



รูปที่ 4.6 ผังเครือข่ายของการส่งการโจมตีจากผู้โจมตีเดียวไปยังเป้าหมายเดียว

จากการทดลองทั้งสามรูปแบบที่ได้กล่าวมาแล้วสามารถสรุปผลการทดลองได้ดังตารางที่ 4.9

ตารางที่ 4.9 สรุปผลการทดลองในสภาพแวดล้อมของการโจมตีหลายชนิดผสมกัน

ระบบตรวจหาการบุกรุก	Snort	RealSecure
สามารถตรวจวิเคราะห์ได้ดี (>80%)	✗	✗
ตรวจพบการโจมตีได้เร็ว (<5 วินาที)	✓	✗
ไม่เกิดการแจ้งเตือนเกินจริง	✓	✗
แจ้งเตือนทุกครั้งเมื่อถูกโจมตี	✗	✗
มีความถูกต้องของการแจ้งเตือน	✗	✓
ใช้งานซีพียูต่ำ (<90%)	✗	✗

จากตารางสรุปแสดงให้เห็นว่าโปรแกรมทั้งสองมีความสามารถในการทำงานใกล้เคียงกัน แตกต่างกันเล็กน้อยในเรื่องของเวลาที่ใช้ตรวจหาการโจมตี การแจ้งเตือนเกินจริง ความถูกต้องของการแจ้งเตือน ซึ่งผลที่ได้จากการทดลองจะเปลี่ยนแปลงเมื่อรูปแบบหรือลักษณะของการโจมตีเปลี่ยนแปลงไป

บทที่ 5

สรุปผลการวิจัย และข้อเสนอแนะ

ในบทนี้กล่าวถึงผลสรุปของการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

ในการวิจัยนี้พบว่าการทำงานของระบบตรวจหาการบุกรุกที่ใช้วิธีการตรวจหาและทำงานพร้อมกันขณะที่เกิดการบุกรุกมีความสามารถในการทำงานใกล้เคียงกันแต่มีความแตกต่างกันเล็กน้อย สาเหตุเนื่องมาจากปัจจัยเกี่ยวข้อง เช่น ความครบถ้วนและถูกต้องของกฎเกณฑ์ที่ใช้ตรวจหา พฤติกรรมหรือความเร็วในการโจมตี ปริมาณข้อมูลที่ไหลในเครือข่าย เป็นต้น ซึ่งปัจจัยเหล่านี้จะส่งผลกระทบต่อความสามารถในการตรวจวิเคราะห์ เวลาที่ใช้การแจ้งเตือน ความผิดพลาดในการแจ้งเตือน ความถูกต้องของการแจ้งเตือนและการใช้งานซีพียู โดยผลการทดลองแยกตามสภาพแวดล้อมของการทดลอง แสดงได้ดังตารางที่ 5.1

ตารางที่ 5.1 สรุปผลการทำงานของโปรแกรมสนอร์ทและเรียลซีเคียวในสภาพแวดล้อมต่าง ๆ

ผลทดลอง / การโจมตี	การโจมตีชนิดเดียว		การโจมตีชนิดเดียว มีข้อมูล		การโจมตีผสม	
	สนอร์ท	เรียลซีเคียว	สนอร์ท	เรียลซีเคียว	สนอร์ท	เรียลซีเคียว
สามารถตรวจวิเคราะห์ได้ดี	✓	✓	✗	✗	✗	✗
ตรวจพบการโจมตีได้เร็ว	✓	✓	✓	✓	✓	✗
ไม่เกิดการแจ้งเตือนเกินจริง	✗	✗	✗	✗	✗	✓
แจ้งเตือนทุกครั้งเมื่อถูกโจมตี	✗	✓	✓	✓	✓	✓
มีความถูกต้องของการแจ้งเตือน	✗	✓	✗	✗	✗	✗
ใช้งานซีพียูต่ำ	✓	✓	✓	✓	✗	✓

จากตารางดังกล่าวแสดงให้เห็นว่าข้อมูลหรือการโจมตีอื่นปะปนมีผลทำให้ระบบตรวจหาการบุกรุกทั้งสองตรวจวิเคราะห์ได้ลดลง เนื่องจากข้อมูลและการโจมตีที่ปะปนทำให้ปริมาณการไหลของข้อมูลในเครือข่ายสูงขึ้น โปรแกรมจึงไม่สามารถตรวจวิเคราะห์ได้ทัน โดยการทดลองในสภาพแวดล้อมที่มีการโจมตีหลายชนิดผสมกันจะใช้เวลาในการตรวจวิเคราะห์หาการบุกรุกนานกว่าการทำงานในสภาพแวดล้อมอื่นรวมถึงยังทำให้เกิดความผิดพลาดในการแจ้งเตือนทั้งการแจ้งเตือนเกินจริงและการไม่แจ้งเตือนเมื่อถูกโจมตีมากกว่าผลการทดสอบในสภาพแวดล้อมอื่น

เมื่อเปรียบเทียบความสามารถในการทำงานของโปรแกรมทั้งสองจากเครื่องหมายถูกและผิดพบว่าโปรแกรมมีจุดเด่นและด้อยต่างกัน โดยโปรแกรมสนอร์ทมีจุดเด่นในเรื่องความเร็วของการแจ้งเตือนทุกการโจมตีที่ได้ทดลองไป ส่วนโปรแกรมเรียลซีเคียวแม้จะแจ้งเตือนช้ากว่าเล็กน้อยแต่มีจุดเด่นเรื่องความครบถ้วนและถูกต้องของการแจ้งเตือน ซึ่งผลจากการวิจัยนี้สามารถนำมาใช้ประกอบการตัดสินใจเลือกใช้ระบบตรวจหาการบุกรุกได้ โดยคำนึงถึงปัจจัยหลักที่ส่งผลกระทบต่อการทำงานของโปรแกรม ดังตารางที่ 5.2 เมื่อปัจจัยเหล่านี้มีค่าเพิ่มขึ้นจะส่งผลเสียต่อการทำงานของโปรแกรม

ตารางที่ 5.2 ปัจจัยที่ส่งผลกระทบต่อการทำงานของโปรแกรม

ส่งผลกระทบต่อ	**ปัจจัยที่มีผลกระทบ**	
	โปรแกรมสนอร์ท	**โปรแกรมเรียลซีเคียว**
ความสามารถในการตรวจวิเคราะห์	ความเร็วของการโจมตี การไหลของข้อมูลในเครือข่าย	การไหลของข้อมูลในเครือข่าย ความหลากหลายของการโจมตี ข้อมูลปน
เวลาที่ใช้ตรวจหาการโจมตี	ไม่สัมพันธ์กับปัจจัยใด	พฤติกรรมของการโจมตี เช่น การก่อกวนหรือการกราดตรวจ
ไม่เกิดการแจ้งเตือนเกินจริง	ข้อมูลปน	พฤติกรรมของการโจมตี
แจ้งเตือนทุกครั้งเมื่อถูกโจมตี	ความเร็วของการโจมตี กฎเกณฑ์รูปแบบของการโจมตี	ความหลากหลายของการโจมตี ความเร็วของการโจมตี ข้อมูลปน
ความถูกต้องของการแจ้งเตือน	กฎเกณฑ์รูปแบบของการโจมตี	กฎเกณฑ์รูปแบบของการโจมตี
การใช้งานซีพียู	ความเร็วของการโจมตี พฤติกรรมของการโจมตี ข้อมูลปน	ความเร็วของการโจมตี พฤติกรรมของการโจมตี ข้อมูลที่ปะปน

จากตารางสรุปดังกล่าวพบว่าปัจจัยหลักที่มีผลกระทบต่อการทำงานของโปรแกรมทั้งสองคือ ความเร็วของการโจมตี พฤติกรรมการโจมตี ข้อมูลหรือการโจมตีอื่นที่ปะปน นอกจากปัจจัยเหล่านั้นแล้วการทำงานของระบบตรวจหาการบุกรุกยังขึ้นอยู่กับตำแหน่งที่ตั้งและโครงสร้างของเครือข่ายด้วย เช่น ในเครือข่ายที่ใช้ฮับเมื่อเกิดการโจมตีจะทำให้มีความรุนแรงของการโจมตีมากกว่าเครือข่ายที่ใช้อุปกรณ์สลับสาย และต้องใช้อุปกรณ์สลับสายที่มีความสามารถในการเข้าถึงข้อมูลทั้งหมดในเครือข่ายโปรแกรมตรวจหาการบุกรุกตรวจวิเคราะห์ข้อมูลทั้งหมดไม่ได้ ดังนั้นการนำระบบตรวจหาการบุกรุกเข้ามาใช้จึงควรพิจารณาวัตถุประสงค์ของการนำมาใช้

โครงสร้างเครือข่ายที่จะวางระบบตรวจหาการบุกรุก เพื่อเลือกระบบตรวจหาการบุกรุกที่เหมาะสม และเพื่อได้รับประโยชน์สูงสุดตามที่คาดไว้ควรจะวางแผนการตอบสนองเมื่อตรวจพบการโจมตีด้วย

5.2 ข้อเสนอแนะ

จากงานวิจัยที่เน้นทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาวะที่ถูกกดดันด้านการโจมตีนี้ สามารถนำรูปแบบการทดลองมาประยุกต์ใช้เป็นแนวทางในการทดสอบด้านอื่นๆ เช่น ทดสอบความสามารถในการจำแนกลักษณะการบุกรุก ทดสอบการใช้ทรัพยากร ทดสอบความสามารถในการทำงานบนเครือข่ายที่มีการใช้งานจริง ทดสอบความสามารถในการตรวจหาการบุกรุกเครื่องให้บริการ ทดสอบความต้านทานต่อการถูกโจมตีของโปรแกรมตรวจหาการบุกรุก ทดสอบโดยใช้การโจมตีรูปแบบใหม่ที่มีความรุนแรงของการโจมตีมากขึ้น หรือปรับเปลี่ยนอุปกรณ์รวมสายจากฮับไปเป็นอุปกรณ์สลับสาย เป็นต้น

รายการอ้างอิง

1. Tim Bass. Intrusion Detection Systems and Multisensor Data Fusion. Communications of ACM 43, 4 (April 2000) : 99-105.
2. Nicholas J.Puketza, Kui Zhang, Mandy Chung, Biswanath Mukherjee and Ronald A.Olsson. A Mothodology for Testing Intrusion Detection System. University of California September (1996).
3. Terrence Champion and Mary L.Denz. A Benchmark Evaluation of Network Intrusion Detection Systems. IEEE Proceedings 6 (2001) : 2705-2712.
4. Coit C.J., Staniford S. and McAlerney J.. Towards Faster String Matching for Intrusion Detection or Exceeding the Speed of Snort. DARPA Information Survivability Conference and Exposition II 1 (2001) : 367-373.
5. Kanlayasiri U., Sanguanpong S. and Jaratmanachor W.. A Rule-Based Approach for Port Scanning Detection. Proceedings of the 12rd Electrical Engineering Conference (2000).
6. Nei Kato, Hiroaki Nitou, Kohei ohta, Glenn Mansfield and Yoshiaki Nemoto. A Real-Time Intrusion Detection System (IDS) for Large Scale Networks and Its Evaluations. E82-B (1999) : 1817-1825.
7. Mandy Chung, Nicholas Puketza, Ronald A. Olsson and Biswanath Mukherjee. Simulating Concurrent Intrusions for Testing Intrusion Detection Systems: Parallelizing Intrusions. Proceedings of the 1995 National Information Systems Security Conference (October 1995) : 173-183.
8. Rebeca Gurley Bace. Intrusion Detection. Indianapolis : Macmillan Technical Publishing, 2002.
9. เรืองไกร รังสิพล. เจาะระบบ TCP/IP จุดอ่อนของโปรโตคอลและวิธีป้องกัน. กรุงเทพฯ : บริษัทด่านสุทธาการพิมพ์, 2544.
10. Martin Roesch. Snort-Lightweight Intrusion Detection for Network. (Online).Available from : http://www.snort.org
11. Stuart McClure, Joel Scambray and George Kurtz. Hacking Exposed: Network Security Secrets and Solutions. Osborne : McGraw-Hill, 1999.

ภาคผนวก

ภาคผนวก ก

คำสั่งที่ใช้ในการทดลอง

คำสั่งในการเรียกใช้โปรแกรมสนอร์ทให้ทำงาน หลังจากติดตั้งโปรแกรมเรียบร้อยแล้ว

. /usr/local/bin/snort -d -h 192.168.0.0/24 -c /etc/snort/snort.conf

คำสั่งโจมตีด้วยการกราดตรวจทีซีพอร์ต

. /scan [target]

ตัวอย่างเช่น

. /scan 192.168.0.37

คำสั่งโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์

. /smurf [target] [broadcast file] [no. of packet, 0=flood]
[delay time, milisecond] [packet size]

ตัวอย่างเช่น

. /smurf 192.168.0.37 message 0 0 1000

คำสั่งโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมาก

. /synflood [source] [destination] [port] [no. of attack]

ตัวอย่างเช่น

. /synflood 192.168.0.21 192.168.0.37 80 10000000000

คำสั่งโจมตีด้วยกลุ่มข้อมูลจำนวนมาก

ping –f [target]

ตัวอย่างเช่น

ping –f 192.168.0.37

ภาคผนวก ข

ตัวอย่างการแสดงผลของโปรแกรมสนอร์ท

```
[root@localhost bin]# ./snort -d -h 192.168.0.0/24 -c /etc/snort/snort.conf
Log directory = /var/log/snort
Initializing Network Interface eth0
        --== Initializing Snort ==--
Decoding Ethernet on interface eth0
Initializing Preprocessors!
Initializing Plug-ins!
Initializating Output Plugins!
Parsing Rules file /etc/snort/snort.conf
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
No arguments to frag2 directive, setting defaults to:
    Fragment timeout: 60 seconds
    Fragment memory cap: 4194304 bytes
Stream4 config:
    Stateful inspection: ACTIVE
    Session statistics: INACTIVE
    Session timeout: 30 seconds
    Session memory cap: 8388608 bytes
    State alerts: INACTIVE
    Scan alerts: ACTIVE
    Log Flushed Streams: INACTIVE
No arguments to stream4_reassemble, setting defaults:
     Reassemble client: ACTIVE
     Reassemble server: INACTIVE
     Reassemble ports: 21 23 25 53 80 143 110 111 513
     Reassembly alerts: ACTIVE
Back Orifice detection brute force: DISABLED
Using LOCAL time
1238 Snort rules read...
1238 Option Chains linked into 146 Chain Headers
```

จำนวนกฎเกณฑ์ทั้งหมดที่เรียกใช้

```
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Rule application order: ->activation->dynamic->alert->pass->log
        --== Initialization Complete ==--
-*> Snort! <*-
Version 1.8.3 (Build 88)
By Martin Roesch (roesch@sourcefire.com, www.snort.org)
=============================================================
Snort analyzed 810571 out of 14589699 packets, dropping 13779128(94.444%)
packets
Breakdown by protocol:                  Action Stats:
    TCP: 196191     (1.345%)            ALERTS: 614383
    UDP: 3          (0.000%)            LOGGED: 614383
    ICMP: 614369    (4.211%)            PASSED: 0
    ARP: 8          (0.000%)
    IPv6: 0         (0.000%)
    IPX: 0          (0.000%)
  OTHER: 0          (0.000%)
DISCARD: 0          (0.000%)
=============================================== Fragmentation Stats:
Fragmented IP Packets: 0          (0.000%)
   Fragment Trackers: 0
   Rebuilt IP Packets: 0
   Frag elements used: 0
   Discarded(incomplete): 0
   Discarded(timeout): 0
   Frag2 memory faults: 0
========================================== TCP Stream Reassembly Stats:
        TCP Packets Used: 196191     (1.345%)
         Stream Trackers: 85258
         Stream flushes: 0
```

จำนวนกลุ่มข้อมูลที่ได้วิเคราะห์ (Analyze)

จำนวนกลุ่มข้อมูลที่ไม่สามารถวิเคราะห์ได้ทัน (Drop)

จำนวนครั้งของการแจ้งเตือน (Alert)

จำนวนกลุ่มข้อมูลทั้งหมดที่ตรวจพบ (Total)

```
        Segments used: 0
        Stream4 Memory Faults: 1
=================================== Snort received signal 2, exiting
[root@localhost bin]#
```

ภาคผนวก ค

ผลการทดลองที่บันทึกได้

การโจมตีด้วยกลุ่มข้อมูลจำนวนมาก

Session/Attacker/Target		1/1/1	1/1/1	2/1/2	2/1/2	3/1/3	3/1/3	6/1/3	6/1/3	4/2/2	4/2/2	6/3/1	6/3/1
Attacker	Total pkt.	5,801,738	5,784,184	5,845,083	5,652,248	4,465,558	4,526,277	2,001,793	1,993,401	7,103,041	7,089,324	6,419,867	4,901,172
	Total byte	568,569,671	566,849,313	537,536,669	553,918,705	437,622,755	443,573,978	196,175,063	195,351,876	696,096,911	694,753,175	629,145,987	480,313,761
	Out. pkt.	2,892,929	2,884,538	2,724,964	2,815,195	2,210,881	2,240,904	987,274	982,621	3,500,189	3,492,621	3,154,038	2,418,316
	Out. byte	283,506,482	282,684,220	267,045,520	275,887,990	216,665,106	219,607,808	96,752,404	96,296,018	343,017,626	342,276,354	309,095,108	236,994,240
	T0	14:13:27	14:26:09	14:38:55	14:53:35	15:06:39	16:04:55	16:32:44	16:52:18	15:38:38	15:51:45	17:07:11	17:24:30
	T1	14:23:33	14:36:17	14:49:01	15:03:44	15:16:47	16:15:08	16:42:55	17:02:27	15:48:49	16:01:57	17:20:10	17:34:44
Target	Total pkt.	8,188,412	8,083,044	9,819,794	9,782,123	9,851,039	9,957,733	8,884,746	9,113,067	12,854,907	12,645,368	17,354,910	13,616,598
	Total byte	802,463,053	792,137,405	962,337,839	958,645,761	965,398,447	975,854,835	870,702,297	893,077,683	1,259,776,841	1,239,242,018	1,700,775,732	1,334,422,306
Monitor	Total pkt.	8,198,423	8,085,280	9,973,467	9,903,800	9,910,602	10,011,159	8,898,496	9,125,743	17,751,479	17,489,265	21,731,362	17,378,469
	Total byte	803,445,729	792,357,567	977,400,041	970,572,675	971,239,271	981,093,857	872,052,883	894,323,089	1,739,645,217	1,713,948,251	2,129,673,878	1,703,090,089
Snort	Total	8,200,751	8,090,162	9,982,402	9,915,704	9,920,989	10,038,769	8,906,851	9,134,653	21,453,782	21,673,079	24,859,093	19,277,958
	Analyze	450,146	440,072	454,250	426,622	412,334	435,496	443,186	360,045	288,298	298,123	386,016	308,354
	Drop	7,750,605	7,650,090	9,528,152	9,489,082	9,508,655	9,603,273	8,463,665	8,774,608	21,165,484	21,374,956	24,473,077	18,969,604
	Alert	450,142	440,068	454,240	426,611	412,323	435,483	443,163	360,034	288,296	298,122	386,008	308,354
	T0s	14:13:29	14:26:10	14:38:57	14:53:37	15:06:41	16:04:56	16:32:46	16:52:20	15:38:39	15:51:47	17:07:13	17:24:32
	T1s	14:23:32	14:36:14	14:49:00	15:03:44	15:16:46	16:15:07	16:42:54	17:02:26	15:48:49	16:01:57	17:20:10	17:34:43
	$\%CPU_s$	100	100	100	100	100	100	100	100	100	100	100	100
RealSecure	T0r	14:13:29	14:26:10	14:38:56	14:53:36	15:06:40	16:04:56	16:32:45	16:52:19	15:38:39	15:51:46	17:07:12	17:24:31
	Name / Event	ping flood / 1	ping flood / 1	ping flood / 3	ping flood / 1	ping flood / 3	ping flood / 3	ping flood / 3	ping flood / 3	ping flood / 2	ping flood / 2	ping flood / 2	ping flood / 3
	Hit	1	1	3	1	3	3	3	3	2	2	2	3
	Other Event	-	Loki / 2	-	-	Loki / 3	-	Loki / 2	Loki / 2	-	-	-	Loki / 4
	$\%CPU_r$	88	85	87	86	97	96	98	96	100	100	100	100

การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมาก

Session/Attacker/Target		1/1/1	1/1/1	2/1/2	2/1/2	3/1/3	3/1/3	6/1/3	6/1/3	4/2/2	4/2/2	6/3/1	6/3/1
Attacker	Total pkt.	11,681,595	11,462,342	10,453,808	9,903,691	10,380,464	10,892,902	10,971,676	10,631,321	11,747,097	11,252,098	10,227,401	10,207,381
	Total byte	630,818,564	618,978,710	564,531,146	534,827,784	560,589,664	588,261,727	592,514,727	574,134,014	634,357,267	607,627,188	552,296,146	551,215,587
	Out. pkt.	11,681,133	11,461,882	10,452,861	9,902,631	10,378,814	10,891,242	10,970,025	10,629,735	11,746,571	11,251,568	10,226,768	10,206,731
	Out. byte	630,780,870	618,941,268	564,453,870	534,741,426	560,454,984	588,126,132	592,370,318	574,004,898	634,314,462	607,584,336	552,245,712	551,163,078
	T0	10:37:42	10:53:31	11:07:17	11:21:50	11:36:57	11:49:37	12:31:44	13:22:13	12:04:16	12:18:29	13:39:37	13:57:11
	T1	10:47:47	11:03:35	11:17:23	11:31:54	11:47:01	11:59:44	12:42:12	13:32:22	12:14:33	12:28:37	13:49:52	14:07:20
Target	pkt	1,227,606	12,122,648	13,543,840	13,380,901	14,712,533	15,100,611	15,999,701	15,697,583	15,368,956	15,368,371	365,103	1,697,876
	Total byte	736,563,576	727,368,424	812,630,398	802,854,067	882,751,969	906,036,677	959,982,071	922,137,346	117,506,042	93,753,104	129,537,433	101,872,572
Monitor	Total pkt.	15,189,728	15,096,675	15,299,258	14,866,745	15,822,861	16,384,293	17,437,163	16,897,091	4,148,814	3,247,005	4,116,932	4,029,375
	Total byte	911,394,512	905,811,156	917,976,530	892,010,459	949,408,213	983,094,917	1,046,265,943	1,013,860,120	248,933,455	194,823,402	247,019,770	241,780,042
Snort	Total	22,777,915	23,915,662	26,414,394	27,275,146	27,060,381	26,607,491	29,305,839	28,510,656	55,777,157	56,743,961	55,686,759	55,409,904
	Analyze	563,925	714,734	677,884	649,776	664,804	675,743	713,172	661,428	183,289	155,813	181,356	170,712
	Drop	22,213,990	23,200,928	25,736,510	26,625,370	26,395,577	25,931,748	28,592,667	27,849,228	55,593,868	56,588,148	55,505,403	55,239,192
	Alert	130	114	441	384	624	788	516	368	24	28	28	23
	T0s	10:37:43	10:53:32	11:07:19	11:21:51	11:36:58	11:49:39	12:31:45	13:22:14	12:04:17	12:18:30	13:39:39	13:57:13
	T1s	10:47:44	11:03:17	11:17:19	11:31:53	11:47:01	11:59:43	12:42:09	13:32:18	12:13:18	12:28:19	13:49:51	14:07:19
	$\%CPU_s$	100	100	100	100	100	100	100	100	100	100	100	100
RealSecure	T0r	10:37:43	10:53:32	11:07:18	11:21:50	11:36:58	11:49:38	12:31:45	13:22:14	12:04:17	12:18:30	13:39:38	13:57:13
	T1r	10:47:49	11:03:38	11:17:26	11:31:57	11:47:04	11:59:49	12:42:15	13:32:25	12:14:33	12:28:40	13:49:55	14:07:21
	Name / Event	synflood / 1	synflood / 1	synflood / 2	synflood / 2	synflood / 3	synflood / 3	synflood / 3	synflood / 3	synflood / 2	synflood / 2	synflood / 3	synflood / 3
	Hit	7,422	6,659	7,112	6,633	7,194	7,826	9,327	9,284	2,505	2,280	2,760	2,456
	Other Event	-	-	-	-	-	-	-	-	-	-	-	-
	$\%CPU_r$	100	100	100	100	100	100	100	100	100	100	100	100

การโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์

Session/Attacker/Target		1/1/1	1/1/1	2/1/2	2/1/2	3/1/3	3/1/3	6/1/3	6/1/3	4/2/2	4/2/2	6/3/1	6/3/1
Attacker	Total pkt.	60,613	60,255	120,338	120,334	180,949	180,706	181,026	180,278	241,745	241,280	362,096	303,388
	Total byte	62,669,230	62,759,463	125,347,796	125,320,159	188,423,511	188,225,801	188,511,673	188,297,515	251,838,868	251,353,338	377,251,538	316,069,484
	Out. pkt.	60,152	60,239	120,315	120,297	180,883	180,668	180,964	180,740	241,709	241,244	362,064	303,353
	Out. byte	62,668,384	62,758,038	125,346,230	125,317,474	188,419,086	188,223,056	188,507,488	188,294,080	251,835,778	251,350,248	377,248,328	316,066,826
	T0	8:24:17	8:37:05	9:11:35	9:23:48	9:36:22	15:43:04	16:57:53	15:03:33	10:41:41	10:53:57	11:06:38	11:18:44
	T1	8:34:20	8:47:09	9:21:39	9:33:52	9:46:28	15:53:10	17:08:00	15:13:42	10:51:55	11:04:07	11:16:48	11:28:58
Target	Total pkt.	60,163	60,255	120,346	120,319	180,905	180,715	180,990	180,783	241,788	241,322	362,196	343,456
	Total byte	62,669,230	62,759,463	125,347,994	125,319,928	188,423,712	188,226,197	188,512,357	188,297,515	251,838,241	251,352,753	377,250,971	316,069,163
Monitor	Total pkt.	60,144	60,237	120,295	120,270	180,827	180,706	181,031	180,281	241,749	241,223	362,047	303,331
	Total byte	62,668,452	62,758,860	125,345,795	125,316,895	188,417,289	188,225,801	188,511,997	188,297,707	251,838,979	251,349,921	377,248,529	316,066,457
Snort	Total	60,163	60,255	120,342	120,330	180,945	180,706	181,026	180,782	241,739	241,275	326,091	303,384
	Analyze	60,163	60,255	120,342	120,201	177,742	163,976	170,155	167,479	215,686	212,029	299,709	247,969
	Drop	0	0	0	129	3,203	16,730	10,871	13,303	26,053	29,246	26,382	55,415
	Alert	60,142	60,228	120,293	120,136	177,619	163,905	170,040	167,404	215,631	211,972	299,660	247,911
	T0s	8:24:18	8:37:06	9:11:36	9:23:49	9:36:23	15:43:06	16:57:55	15:03:35	10:41:42	10:53:58	11:06:39	11:18:45
	T1s	8:34:19	8:47:09	9:21:38	9:33:52	9:46:28	15:53:10	17:08:00	15:13:42	10:51:54	11:04:07	11:16:48	11:28:58
	$\%CPU_s$	1	1	1	1	2	2	2	2	2	2	2	2
RealSecure	T0r	8:24:18	8:37:07	9:11:37	9:23:50	9:36:23	15:43:06	16:57:55	15:03:37	10:41:43	10:53:59	11:06:39	11:18:45
	Name / Event	ping flood / 1	ping flood / 1	ping flood / 1	ping flood / 2	ping flood / 3	ping flood / 3	ping flood / 3	ping flood / 3	ping flood / 5	ping flood / 5	ping flood / 6	ping flood / 6
	Hit	1	1	1	2	3	3	3	3	5	5	6	6
	Other Event	-	IPDuplicate / 2	-	-	IPDuplicate / 2	-	-	-	-	-	-	-
	$\%CPU_r$	12	14	20	21	29	28	28	28	26	27	31	32

การโจมตีด้วยการกราดตรวจทีซีพีพอร์ต

Session/Attacker/Target		1/1/1	1/1/1	2/1/2	2/1/2	3/1/3	3/1/3	6/1/3	6/1/3	4/2/2	4/2/2	6/3/1	6/3/1
Attacker	Total pkt.	1,820	1,822	3,852	3,622	5,453	5,413	5,584	5,523	3,709	3,686	3,723	3,757
	Total byte	147,986	148,403	314,989	294,329	443,331	440,801	456,777	453,107	303,810	301,602	304,428	307,514
	Out. pkt.	1,010	1,009	2,141	2,009	3,026	3,005	3,394	3,361	2,252	2,151	2,184	2,292
	Out. byte	73,748	73,706	156,802	146,906	221,076	219,938	248,052	246,314	164,760	157,542	160,980	167,528
	T0	10:22:45	10:37:18	10:51:26	11:05:38	11:19:06	11:32:03	11:44:28	11:57:25	11:34:42	11:51:01	12:03:17	12:15:17
	T1	10:32:49	10:47:21	11:02:23	11:15:41	11:29:13	11:42:08	11:54:39	12:07:33	11:44:51	12:01:10	12:13:28	12:25:27
Target	Total pkt.	1,820	1,822	3,893	3,645	5,491	5,458	5,665	5,616	3,755	3,724	3,763	3,800
	Total byte	146,954	147,371	314,371	294,329	443,325	440,669	457,377	453,437	303,177	300,729	303,825	306,791
Monitor	Total pkt.	1,820	1,822	3,852	3,622	5,453	5,413	5,584	5,523	3,709	3,686	3,723	3,757
	Total byte	147,986	148,403	314,989	294,329	443,331	440,801	456,777	453,107	303,810	301,602	304,428	307,514
Snort	Total	1,820	1,822	3,852	3,622	5,453	5,413	5,584	5,523	3,703	3,680	3,719	3,759
	Analyze	1,820	1,822	3,852	3,622	5,453	5,413	5,584	5,523	3,703	3,680	3,719	3,752
	Drop	0	0	0	0	0	0	0	0	0	0	0	0
	Alert	707	707	1,456	1,310	1,970	1,946	1,982	1,976	1,513	1,486	1,504	1,505
	T0s	10:22:47	10:37:20	10:51:28	11:05:39	11:19:07	11:32:05	11:44:29	11:57:26	11:34:43	11:51:02	12:03:18	12:15:18
	T1s	10:32:47	10:47:20	11:02:19	11:15:39	11:29:11	11:42:05	11:54:36	12:07:31	11:44:50	12:01:08	12:13:28	12:25:25
	$\%CPU_s$	2	2	3	3	4	5	5	5	3	4	3	4
RealSecure	T0r	10:23:15	10:37:48	10:51:59	11:06:10	11:19:35	11:32:30	11:44:38	11:57:27	11:35:23	11:51:59	12:03:47	12:15:36
	T1r	10:32:33	10:47:06	11:02:14	11:15:31	11:28:52	11:41:46	11:54:11	12:07:12	11:44:36	12:00:34	12:12:50	12:25:03
	Name / Event	port_scan / 1	port_scan / 1	port_scan / 2	port_scan / 2	port_scan / 3	port_scan / 3	port_scan / 3	port_scan / 3	port_scan / 2	port_scan / 2	port_scan / 3	port_scan / 3
	Hit	10	10	20	20	30	30	30	30	20	21	30	32
	Other Event	-	-	-	-	-	-	-	-	-	-	-	-
	$\%CPU_r$	0	0	1	1	2	2	3	3	1	1	2	2

การโจมตีด้วยกลุ่มข้อมูลจำนวนมากมีข้อมูลปน

Test No.		1	2	3	4	5
Attacker	Total pkt.	5,396,314	6,787,671	5,393,917	1,503,709	891,203
	Total byte	528,837,865	665,190,999	528,602,683	147,356,893	87,331,167
	Out. pkt.	2,670,869	3,393,535	2,680,325	757,861	451,567
	Out. Byte	261,744,546	332,565,814	262,671,066	74,265,526	44,249,030
	T0	13:34:54	9:16:07	13:50:15	9:03:57	8:51:11
	T1	13:45:01	9:26:17	14:00:21	9:14:03	9:01:16
Target	Total pkt.	8,511,650	10,117,661	8,763,179	4,654,197	3,976,956
	Total byte	3,849,140,599	4,737,280,983	4,247,731,722	4,116,762,841	3,995,162,878
Server	Total pkt.	2,499,152	3,142,967	2,820,941	3,034,286	2,999,677
	Total byte	3,234,816,569	4,007,854,668	3,653,348,947	3,931,411,015	3,884,821,406
Client	Total pkt.	2,527,006	3,161,660	2,845,047	3,062,916	3,022,704
	Total byte	3,276,196,381	4,106,453,790	3,688,864,055	3,973,798,969	3,919,486,380
	Tc0	13:32:26	9:13:38	13:47:53	9:01:29	8:48:42
	Tc1	13:42:26	9:23:35	13:57:47	9:11:09	8:58:36
Monitor	Total pkt.	8,572,237	10,361,614	8,813,977	4,761,780	4,094,532
	Total byte	3,866,111,925	4,795,110,426	4,269,725,996	4,139,794,613	4,026,375,048
Snort	Total	8,589,758	10,415,511	8,828,245	4,771,706	4,105,283
	Analyze	398,535	367,424	356,455	706,522	768,526
	Drop	8,191,223	10,048,087	8,471,790	4,065,184	3,336,757
	Alert	330,076	262,906	297,053	84,542	65,482
	T0s	13:34:57	9:16:10	13:50:16	9:03:59	8:51:13
	T1s	13:45:01	9:26:17	14:00:22	9:14:09	9:01:16
	$\%CPU_s$	100	100	100	96	96
RealSecure	T0r	13:34:59	9:16:11	13:50:19	9:04:01	8:51:15
	Name / Event	ping flood / 1	ping flood / 0	ping flood / 1	ping flood / 0	ping flood / 1
	Hit	1	0	1	0	1
	Other Event	-	-	-	-	-
	$\%CPU_r$	100	100	100	100	100

การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมากมีข้อมูล

Test No.		1	2	3	4	5	6
Attacker	Total pkt.	7,422,173	14,284,445	14,035,237	14,193,169	13,141,049	10,993,857
	Total byte	400,810,349	771,374,871	757,918,325	766,446,131	709,631,459	934,202,664
	Out. pkt.	7,421,661	14,283,892	14,034,659	14,192,610	13,140,489	10,719,357
	Out. Byte	400,769,418	771,329,808	757,871,274	766,400,652	709,585,986	578,844,966
	T0	13:45:19	15:32:42	15:19:26	15:45:24	14:08:57	16:41:49
	T1	13:55:24	15:42:50	15:29:32	15:55:30	14:19:01	16:51:55
Target	Total pkt.	11,010,508	17,521,863	17,242,552	17,557,967	17,103,343	11,741,328
	Total byte	4,183,780,853	4,363,801,261	4,320,689,513	4,340,816,226	4,262,539,269	1,052,205,428
Server	Total pkt.	2,841,911	2,802,395	2,763,247	2,763,707	2,658,025	779,320
	Total byte	3,695,742,524	3,628,591,079	3,593,091,745	3,580,332,467	3,470,089,183	1,017,413,910
Client	Total pkt.	2,856,951	2,815,830	2,774,707	2,785,972	2,675,658	28,113,678
	Total byte	3,718,752,732	3,647,874,845	3,609,629,179	3,611,815,293	3,496,138,473	363,631,097
	Tc0	13:42:46	15:30:14	15:16:58	15:42:55	14:06:54	16:39:39
	Tc1	13:52:41	15:40:12	15:26:58	15:52:56	14:16:20	16:48:41
	Time (Sec.)	595	598	600	601	566	542
Monitor	Total pkt.	11,228,108	18,845,392	18,566,081	18,889,358	17,735,375	4,439,296
	Total byte	4,179,284,074	4,492,417,247	4,449,304,399	4,460,092,914	4,321,571,119	1,081,721,353
Snort	Total	12,216,854	21,278,292	20,914,012	21,432,925	19,419,164	20,847,671
	Analyze	781,227	669,321	662,742	678,928	769,795	726,546
	Drop	11,435,627	20,608,971	20,251,270	20,753,997	18,649,369	20,121,125
	Alert	116	167	179	171	169	103
	T0s	13:45:22	15:32:44	15:19:28	15:45:26	14:09:01	16:41:50
	T1s	13:55:14	15:42:41	15:29:27	15:55:29	14:19:00	16:51:53
	$\%CPU_s$	100	98	100	100	100	100
RealSecure	T0r	13:45:20	15:32:47	15:19:31	15:45:29	14:09:01	16:41:51
	T1r	13:55:25	15:42:55	15:29:43	15:55:34	14:19:04	16:52:01
	Name / Event	synflood / 1	synflood / 1	synflood / 1	synflood / 1	synflood / 1	synflood / 1
	Hit	7,490	8,669	7,998	8,236	10,572	7,921
	Other Event	-	-	-	-	IPDuplicate	-
	$\%CPU_r$	100	100	100	100	100	100

การโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์และมีข้อมูล

Test No.		1	2	3	4	5	6	7
Attacker	Total pkt.	52,093	60,333	60,269	681,985	340,513	68,563	63,154
	Total byte	54,250,509	62,834,793	62,774,051	866,187,171	426,631,228	67,967,747	64,527,367
	Out. pkt.	52,075	60,314	60,253	62,968	60,078	60,500	60,203
	Out. Byte	54,249,150	62,833,188	62,772,626	64,985,656	62,581,276	63,025,000	62,721,526
	T0	14:33:07	14:57:41	14:45:42	16:45:43	15:56:32	15:56:04	15:40:44
	T1	14:43:12	15:07:46	14:55:46	16:56:00	16:06:34	16:06:10	15:50:49
Target	Total pkt.	2,831,184	3,219,982	2,946,466	684,610	341,515	68,563	63,154
	Total byte	3,656,255,410	4,157,052,134	3,803,117,779	869,985,045	427,993,792	67,967,747	64,527,367
Server	Total pkt.	2,755,802	3,118,996	2,854,886	653,072	325,782	65,404	60,245
	Total byte	3,567,863,770	4,035,047,102	3,694,951,645	845,241,420	415,821,034	66,034,647	62,692,116
Client	Total pkt.	2,774,106	3,153,312	3,102,859	615,051	280,852	3,813	1,392
	Total byte	3,595,949,834	4,086,862,694	3,988,375,615	790,579,470	363,999,309	4,941,787	1,805,241
	Tc0	14:30:39	14:55:13	14:39:09	16:43:43	15:54:28	15:53:47	15:38:17
	Tc1	14:40:37	15:05:09	14:49:14	16:52:33	16:02:14	16:03:32	15:48:11
	Time (Sec.)	598	596	605	530	466	585	594
Monitor	Total pkt.	2,831,042	3,218,576	2,947,058	706,713	369,566	77,778	75,101
	Total byte	3,656,166,952	4,155,342,798	3,804,072,901	895,677,901	453,532,650	74,131,874	72,439,770
Snort	Total	2,832,022	3,221,899	2,948,860	684,740	341,875	68,563	63,154
	Analyze	740,604	759,889	714,760	173,371	117,320	68,563	63,154
	Drop	2,091,418	2,462,010	2,234,100	511,369	224,555	0	0
	Alert	21,905	18,366	21,905	54,099	56,646	60,484	60,193
	T0s	14:34:52	14:57:43	14:45:43	16:45:45	15:56:32	15:56:04	15:40:15
	T1s	14:43:12	15:07:46	14:55:46	16:55:58	16:06:33	16:06:09	15:50:47
	$\%CPU_s$	92	93	91	93	89	12	8
RealSecure	T0r	14:34:52	14:57:43	14:45:45	16:45:44	15:56:35	15:56:05	15:40:45
	Name / Event	ping flood / 3	ping flood / 1	ping flood / 1	ping flood / 1	ping flood / 1	ping flood / 1	ping flood / 1
	Hit	3	1	1	1	1	1	1
	Other Event	-	-	-	-	-	-	-
	$\%CPU_r$	81	82	82	78	66	9	5

การโจมตีด้วยการกราดตรวจทีซีพีพอร์ตและมีข้อมูล

Test No.		1	2	3	4	5	6	7
Attacker	Total pkt.	1,816	1,826	1,825	1,822	1,827	4,007	2,682
	Total byte	148,147	149,044	149,055	148,657	148,956	584,350	321,561
	Out. pkt.	1,007	1,011	1,011	1,009	1,013	1,015	1,008
	Out. Byte	73,750	73,918	74,046	73,834	74,130	74,214	73,920
	T0	13:21:44	15:10:20	13:08:09	10:28:01	15:23:05	14:47:44	13:05:50
	T1	13:31:50	15:20:31	13:18:19	10:38:08	15:33:13	14:57:54	13:15:59
Target	Total pkt.	3,160,332	2,898,139	2,915,996	2,405,057	2,732,579	4,007	2,684
	Total byte	4,093,904,384	3,754,266,756	3,777,294,222	3,114,549,416	3,539,801,586	583,318	320,631
Server	Total pkt.	3,124,322	2,858,475	2,873,733	2,364,237	2,704,522	3,966	2,656
	Total byte	4,043,812,400	3,699,439,442	3,717,981,216	3,057,262,637	3,501,278,700	576,970	317,142
Client	Total pkt.	3,158,359	2,895,247	2,912,619	2,399,979	2,724,160	2,181	869
	Total byte	4,094,014,874	3,753,055,690	3,775,446,900	3,110,857,791	3,531,561,255	435,754	173,637
	Tc0	13:19:16	15:07:51	13:05:40	10:25:33	15:17:43	14:45:41	13:03:37
	Tc1	13:29:16	15:17:42	13:15:23	10:35:33	15:27:51	14:53:10	13:13:13
	Time (Sec.)	600	591	583	600	608	449	576
Monitor	Total pkt.	3161480	2897714	2915312	2406105	2732573	4,007	2,684
	Total byte	4095631696	3753853050	3776503554	3116183799	3539903186	583,335	320,640
Snort	Total	3,163,356	2,899,674	2,917,254	2,406,689	2,733,005	4,007	2,684
	Analyze	931,866	881,050	857,390	675,505	844,983	4,007	2,684
	Drop	2,231,490	2,018,624	2,059,864	1,731,184	1,888,022	0	0
	Alert	419	436	473	483	433	735	727
	T0s	13:21:47	15:10:21	13:08:11	10:28:03	15:23:06	14:47:45	13:05:51
	T1s	13:31:49	15:20:24	13:18:17	10:38:06	15:33:12	14:57:51	13:15:57
	$\%CPU_s$	94	93	93	95	87	2	2
RealSecure	T0r	13:22:19	15:10:26	13:08:50	10:28:36	15:23:30	14:48:10	13:06:20
	T1r	13:31:40	15:19:41	13:18:10	10:37:54	15:32:51	14:57:28	13:15:38
	Name / Event	port_scan / 1	port_scan / 1	port_scan / 1	port_scan / 1	port_scan / 1	port_scan / 1	port_scan / 1
	Hit	10	10	10	10	10	10	10
	Other Event	-	-	-	-	-	-	-
	$\%CPU_r$	100	100	100	100	100	100	100

การโจมตีหลายชนิดผสมกัน

Test No.		1	2	3	4	5	6
Attacker	Total pkt.	6,127,822	6,018,763	16,261,810	20,353,160	7,141,651	7,036,870
	Total byte	520,344,465	509,284,749	984,754,532	989,806,921	600,262,327	589,925,856
	Out. pkt.	4,355,836	4,308,658	11,908,354	11,894,473	5,067,620	5,004,721
	Out. Byte	346,695,260	341,699,452	713,818,800	711,852,406	397,017,196	390,787,934
	T0	15:12:48	16:37:13	15:33:51	16:24:04	15:56:00	16:08:37
	T1	15:22:55	16:47:23	15:44:12	16:34:27	16:06:05	16:18:39
Target	Total pkt.	9,581,312	9,479,213	14,083,794	14,089,091	6,888,208	6,726,122
	Total byte	824,147,125	815,157,539	965,533,181	967,292,425	675,044,659	659,160,083
Monitor	Total pkt.	12,259,514	12,232,379	18,174,326	18,181,161	12,097,755	12,176,182
	Total byte	1,005,610,407	983,394,319	1,164,805,329	1,166,927,655	1,038,669,847	1,037,267,335
Snort	Total	14,589,699	14,193,147	25,113,003	25,531,963	14,998,927	14,860,758
	Analyze	810,571	421,764	359,417	365,851	364,656	400,123
	Drop	13,779,128	13,771,383	24,753,586	2,566,112	14,634,362	14,460,635
	Alert	614,383	337,172	82,529	89,362	293,628	314,174
	T0s	15:12:49	16:37:15	15:33:51	16:24:05	15:56:00	16:08:37
	T1s	15:22:53	16:47:20	15:44:12	16:34:23	16:06:03	16:18:37
	$\%CPU_s$	97	100	100	100	91	99
RealSecure	T0r	15:12:50	16:37:20	15:33:52	16:24:25	15:56:01	16:08:40
	T1r	15:22:54	16:47:21	15:44:12	16:34:29	16:06:08	16:18:44
	Name / Event	synflood/1, pingflood/1, pingflood/1	synflood/1, port_scan/1, pingflood/1, pingflood/1	synflood/1, pingflood/1, port_scan/1	synflood/1, port_scan/1, pingflood/1, pingflood/1	synflood/1, port_scan/1, pingflood/1, pingflood/1	synflood/1, port_scan/1
	Hit	10,179	10,161	6,070	6,011	10,117	10,114
	Other Event	-	-	-	-	-	Loki
	$\%CPU_r$	100	100	100	100	100	100

ภาคผนวก ง

ค่าที่คำนวณได้จากการทดลอง

การโจมตีด้วยกลุ่มข้อมูลจำนวนมาก

Session/Attacker/Target		1/1/1	1/1/1	2/1/2	2/1/2	3/1/3	3/1/3	6/1/3	6/1/3	4/2/2	4/2/2	6/3/1	6/3/1
Test Time	Sec.	606	608	606	609	608	613	611	609	611	612	779	614
Attk. rate	bit/s	3,742,660	3,719,529	3,525,353	3,624,144	2,850,857	2,866,007	1,266,807	1,264,972	4,491,229	4,474,201	3,174,276	3,087,873
Targ Traffic	bit/s	10,593,572	10,422,861	12,704,130	12,593,048	12,702,611	12,735,463	11,400,357	11,731,727	16,494,623	16,199,242	17,466,246	17,386,610
Mon Traffic	bit/s	10,606,544	10,425,757	12,902,971	12,749,723	12,779,464	12,803,835	11,418,041	11,748,087	22,777,679	22,404,552	21,870,849	22,190,099
Snort	Start delay	0:00:02	0:00:01	0:00:02	0:00:02	0:00:02	0:00:01	0:00:02	0:00:02	0:00:01	0:00:02	0:00:02	0:00:02
	Stop before	0:00:01	0:00:03	0:00:01	0:00:00	0:00:01	0:00:01	0:00:01	0:00:01	0:00:00	0:00:00	0:00:00	0:00:01
	%CPU_s	100	100	100	100	100	100	100	100	100	100	100	100
Snort Analyze	%Analyze	5.489	5.440	4.551	4.302	4.156	4.338	4.976	3.942	1.344	1.376	1.553	1.600
	%Drop	94.511	94.560	95.449	95.698	95.844	95.662	95.024	96.058	98.656	98.624	98.447	98.400
	%Alert	99.999	99.999	99.998	99.997	99.997	99.997	99.995	99.997	99.999	100.000	99.998	100.000
	%F-Pos	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
	%F-Neg	84.440	84.744	83.330	84.846	81.350	80.567	55.112	63.360	91.763	91.464	87.761	87.249
RealSecure	Start delay	0:00:02	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01
	Name / Event	ping flood / 1	ping flood / 1	ping flood / 3	ping flood / 1	ping flood / 3	ping flood / 3	ping flood / 3	ping flood / 3	ping flood / 2	ping flood / 2	ping flood / 2	ping flood / 3
	Hit	1	1	3	1	3	3	3	3	2	2	2	3
	Other Event	-	Loki / 2	-	-	Loki / 3	-	Loki / 2	Loki / 2	-	-	-	Loki / 4
	%CPU_r	88	85	87	86	97	96	98	96	100	100	100	100
RealSecure Analyze	%Analyze	100.000	100.000	100.000	50.000	100.000	100.000	100.000	100.000	100.000	100.000	66.667	100.000
	%Drop	0.000	0.000	0.000	50.000	0.000	0.000	0.000	0.000	0.000	0.000	33.333	0.000
	%Alert	100.000	300.000	150.000	50.000	200.000	100.000	83.333	83.333	50.000	50.000	33.333	116.667
	%F-Pos	0.000	200.000	50.000	0.000	100.000	0.000	0.000	0.000	0.000	0.000	0.000	16.667
	%F-Neg	0.000	0.000	0.000	50.000	0.000	0.000	16.667	16.667	50.000	50.000	66.667	0.000

การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมาก

Session/Attacker/Target		1/1/1	1/1/1	2/1/2	2/1/2	3/1/3	3/1/3	6/1/3	6/1/3	4/2/2	4/2/2	6/3/1	6/3/1
Test Time	Sec.	605	604	606	604	604	607	628	609	617	608	735	609
Attk. rate	bit/s	8,340,904	8,197,898	7,451,536	7,082,668	7,423,245	7,751,251	7,546,119	7,540,294	8,224,499	7,994,531	6,010,838	7,240,237
Targ Traffic	bit/s	9,739,684	9,634,019	10,727,794	10,633,829	11,692,079	11,941,175	12,229,071	12,113,463	1,523,579	1,233,593	1,409,931	1,338,228
Mon Traffic	bit/s	12,051,498	11,997,499	12,118,502	11,814,708	12,574,943	12,956,770	13,328,229	13,318,360	3,227,662	2,563,466	2,688,651	3,176,093
Snort	Start delay	0:00:01	0:00:01	0:00:02	0:00:01	0:00:01	0:00:02	0:00:01	0:00:01	0:00:01	0:00:01	0:00:02	0:00:02
	Stop before	0:00:03	0:00:18	0:00:04	0:00:01	0:00:00	0:00:01	0:00:03	0:00:04	0:01:15	0:00:18	0:00:01	0:00:01
	$\%CPU_s$	100	100	100	100	100	100	100	100	100	100	100	100
Snort Analyze	%Analyze	2.476	2.989	2.566	2.382	2.457	2.540	2.434	2.320	0.329	0.275	0.326	0.308
	%Drop	97.524	97.011	97.434	97.618	97.543	97.460	97.566	97.680	99.671	99.725	99.674	99.692
	%Alert	0.023	0.016	0.065	0.059	0.094	0.117	0.072	0.056	0.013	0.018	0.015	0.013
	%F-Pos	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
	%F-Neg	99.999	99.999	99.996	99.996	99.994	99.993	99.995	99.997	100.000	100.000	100.000	100.000
RealSecure	Start delay	0:00:01	0:00:01	0:00:01	0:00:00	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:02
	Stop delay	0:00:02	0:00:03	0:00:03	0:00:03	0:00:03	0:00:05	0:00:03	0:00:03	0:00:00	0:00:03	0:00:03	0:00:01
	Name / Event	synflood / 1	synflood / 1	synflood / 2	synflood / 2	synflood / 3	synflood / 3	synflood / 3	synflood / 3	synflood / 2	synflood / 2	synflood / 3	synflood / 3
	Hit	7,422	6,659	7,112	6,633	7,194	7,826	9,327	9,284	2,505	2,280	2,760	2,456
	Other Event	-	-	-	-	-	-	-	-	-	-	-	-
	$\%CPU_r$	100	100	100	100	100	100	100	100	100	100	100	100
RealSecure Analyze	%Analyze	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000
	%Drop	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	%Alert	0.064	0.058	0.068	0.067	0.069	0.072	0.085	0.087	0.021	0.020	0.027	0.024
	%F-Pos	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	%F-Neg	99.936	99.942	99.932	99.933	99.931	99.928	99.915	99.913	99.979	99.980	99.973	99.976

การโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์

Session/Attacker/Target		1/1/1	1/1/1	2/1/2	2/1/2	3/1/3	3/1/3	6/1/3	6/1/3	4/2/2	4/2/2	6/3/1	6/3/1
Test Time	Sec.	603	604	604	604	606	606	607	609	614	610	730	614
Attk. rate	bit/s	831,421	831,232	1,660,215	1,659,834	2,487,381	2,484,793	2,484,448	2,473,485	3,281,248	3,296,397	4,134,228	4,118,135
Targ Traffic	bit/s	831,433	831,251	1,660,238	1,659,867	2,487,442	2,484,834	2,484,512	2,473,531	3,281,280	3,296,430	4,134,257	4,118,165
Mon Traffic	bit/s	831,422	831,243	1,660,209	1,659,826	2,487,357	2,484,829	2,484,507	2,473,533	3,281,290	3,296,392	4,134,230	4,118,130
Snort	Start delay	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:02	0:00:02	0:00:02	0:00:01	0:00:01	0:00:01	0:00:01
	Stop before	0:00:01	0:00:00	0:00:01	0:00:00	0:00:00	0:00:00	0:00:00	0:00:00	0:00:01	0:00:00	0:00:00	0:00:00
	$\%CPU_s$	1	1	1	1	2	2	2	2	2	2	2	2
Snort Analyze	%Analyze	100.000	100.000	100.000	99.893	98.230	90.742	93.995	92.641	89.223	87.879	91.910	81.734
	%Drop	0.000	0.000	0.000	0.107	1.770	9.258	6.005	7.359	10.777	12.121	8.090	18.266
	%Alert	99.965	99.955	99.959	99.946	99.931	99.957	99.932	99.955	99.974	99.973	99.984	99.977
	%F-Pos	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
	%F-Neg	0.017	0.018	0.018	0.134	1.804	9.278	6.037	7.379	10.789	12.134	17.236	18.276
RealSecure	Start delay	0:00:01	0:00:02	0:00:02	0:00:02	0:00:01	0:00:02	0:00:02	0:00:04	0:00:02	0:00:02	0:00:01	0:00:01
	Name / Event	ping flood / 1	ping flood / 1	ping flood / 1	ping flood / 2	ping flood / 3	ping flood / 3	ping flood / 3	ping flood / 3	ping flood / 5	ping flood / 5	ping flood / 6	ping flood / 6
	Hit	1	1	1	2	3	3	3	3	5	5	6	6
	Other Event	-	IPDuplicate / 2	-	-	IPDuplicate / 2	-	-	-	-	-	-	-
	$\%CPU_r$	12	14	20	21	29	28	28	28	26	27	31	32
RealSecure Analyze	%Analyze	100.000	100.000	50.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000
	%Drop	0.000	0.000	50.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	%Alert	100.000	100.000	50.000	100.000	100.000	100.000	50.000	50.000	125.000	125.000	100.000	100.000
	%F-Pos	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	25.000	25.000	0.000	0.000
	%F-Neg	0.000	0.000	50.000	0.000	0.000	0.000	50.000	50.000	0.000	0.000	0.000	0.000

การโจมตีด้วยการกราดตรวจทีซีพีพอร์ต

Session/Attacker/Target		1/1/1	1/1/1	2/1/2	2/1/2	3/1/3	3/1/3	6/1/3	6/1/3	4/2/2	4/2/2	6/3/1	6/3/1
Test Time	Sec.	600	603	657	603	607	605	611	608	609	609	731	610
Attk. rate	bit/s	983	978	1,909	1,949	2,914	2,908	3,248	3,241	2,164	2,070	1,762	2,197
Targ Traffic	bit/s	1,959	1,955	3,828	3,905	5,843	5,827	5,989	5,966	3,983	3,950	3,325	4,023
Mon Traffic	bit/s	1,973	1,969	3,835	3,905	5,843	5,829	5,981	5,962	3,991	3,962	3,332	4,033
Snort	Start delay	0:00:02	0:00:02	0:00:02	0:00:01	0:00:01	0:00:02	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01	0:00:01
	Stop before	0:00:02	0:00:01	0:00:04	0:00:02	0:00:02	0:00:03	0:00:03	0:00:02	0:00:01	0:00:02	0:00:00	0:00:02
	$\%CPU_s$	2	2	3	3	4	5	5	5	3	4	3	4
Snort Analyze	%Analyze	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	99.814
	%Drop	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	%Alert	38.846	38.804	37.799	36.168	36.127	35.950	35.494	35.778	40.859	40.380	40.441	40.112
	%F-Pos	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	%F-Neg	30.000	29.931	31.994	34.793	34.898	35.241	41.603	41.208	32.815	30.916	31.136	34.337
RealSecure	Start delay	0:00:30	0:00:30	0:00:33	0:00:32	0:00:29	0:00:27	0:00:10	0:00:02	0:00:41	0:00:58	0:00:30	0:00:19
	Stop before	0:00:16	0:00:15	0:00:09	0:00:10	0:00:21	0:00:22	0:00:28	0:00:21	0:00:15	0:00:36	0:00:38	0:00:24
	Name / Event	port_scan / 1	port_scan / 1	port_scan / 2	port_scan / 2	port_scan / 3	port_scan / 3	port_scan / 3	port_scan / 3	port_scan / 2	port_scan / 2	port_scan / 3	port_scan / 3
	Hit	10	10	20	20	30	30	30	30	20	21	30	32
	Other Event	-	-	-	-	-	-	-	-	-	-	-	-
	$\%CPU_r$	0	0	1	1	2	2	3	3	1	1	2	2
RealSecure Analyze	%Analyze	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000
	%Drop	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	%Alert	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	100.000	105.000	100.000	106.667
	%F-Pos	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	5.000	0.000	6.667
	%F-Neg	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

การโจมตีด้วยกลุ่มข้อมูลจำนวนมากมีข้อมูลปน

Test No.		1	2	3	4	5
Test Time	Sec.	607	610	606	606	605
Attk. rate	bit/s	3,449,681	4,361,519	3,467,605	980,403	585,111
Targ Traffic	bit/s	50,730,024	62,128,275	56,075,666	54,346,704	52,828,600
Mon Traffic	bit/s	50,953,699	62,886,694	56,366,020	54,650,754	53,241,323
%Data		85.115	86.684	86.843	96.527	98.106
Snort	Start delay	0:00:03	0:00:03	0:00:01	0:00:02	0:00:02
	Stop before	0:00:00	0:00:00	0:00:01	0:00:06	0:00:00
	$\%CPU_s$	100	100	100	96	96
Snort Analyze	%Analyze	4.640	3.528	4.038	14.806	18.720
	%Drop	95.360	96.472	95.962	85.194	81.280
	%Alert	82.822	71.554	83.335	11.966	8.520
	%F-Pos	0.0000	0.0000	0.0000	0.0000	0.0000
	%F-Neg	87.642	92.253	88.917	88.845	85.499
RealSecure	Start delay	0:00:05	0:00:04	0:00:04	0:00:04	0:00:04
	Name / Event	ping flood / 1	ping flood / 0	ping flood / 1	ping flood / 0	ping flood / 1
	Hit	1	0	1	0	1
	Other Event	-	-	-	-	-
	$\%CPU_r$	100	100	100	100	100
RealSecure Analyze	%Analyze	100.000	0.000	100.000	0.000	100.000
	%Drop	0.000	100.000	0.000	100.000	0.000
	%Alert	100.000	0.000	100.000	0.000	100.000
	%F-Pos	0.000	0.000	0.000	0.000	0.000
	%F-Neg	0.000	100.000	0.000	100.000	0.000

การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมากมีข้อมูล

Test No.		1	2	3	4	5	6
Test Time	Sec.	605	608	606	606	604	606
Attk. rate	bit/s	5,299,430	10,149,076	10,004,901	10,117,500	9,398,490	7,641,518
Targ Traffic	bit/s	55,322,722	57,418,438	57,038,805	57,304,505	56,457,474	13,890,501
Mon Traffic	bit/s	55,263,260	59,110,753	58,736,692	58,879,114	57,239,353	14,280,150
%Data		88.885	83.594	83.543	83.206	82.020	34.559
Snort	Start delay	0:00:03	0:00:02	0:00:02	0:00:02	0:00:04	0:00:01
	Stop before	0:00:10	0:00:09	0:00:05	0:00:01	0:00:01	0:00:02
	$\%CPU_s$	100	98	100	100	100	100
Snort Analyze	%Analyze	6.395	3.146	3.169	3.168	3.964	3.485
	%Drop	93.605	96.854	96.831	96.832	96.036	96.515
	%Alert	0.015	0.025	0.027	0.025	0.022	0.014
	%F-Pos	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
	%F-Neg	99.998	99.999	99.999	99.999	99.959	99.999
RealSecure	Start delay	0:00:01	0:00:05	0:00:05	0:00:05	0:00:04	0:00:02
	Stop delay	0:00:01	0:00:05	0:00:11	0:00:04	0:00:03	0:00:06
	Name / Event	synflood / 1	synflood / 1	synflood / 1	synflood / 1	synflood / 1	synflood / 1
	Hit	7,490	8,669	7,998	8,236	10,572	7,921
	Other Event	-	-	-	-	IPDuplicate	-
	$\%CPU_r$	100	100	100	100	100	100
RealSecure Analyze	%Analyze	100.000	100.000	100.000	100.000	100.000	100.000
	%Drop	0.000	0.000	0.000	0.000	0.000	0.000
	%Alert	0.101	0.061	0.057	0.058	0.080	0.074
	%F-Pos	0.000	0.000	0.000	0.000	0.000	0.000
	%F-Neg	99.899	99.939	99.943	99.942	99.920	99.926

การโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์และมีข้อมูล

Test No.		1	2	3	4	5	6	7
Test Time	Sec.	605	605	604	617	602	606	605
Attk. rate	bit/s	717,344	830,852	831,426	842,602	831,645	832,013	829,376
Targ Traffic	bit/s	48,347,179	54,969,284	50,372,421	11,280,195	5,687,625	897,264	853,254
Mon Traffic	bit/s	48,346,009	54,946,682	50,385,072	11,613,328	6,027,012	978,639	957,881
Snort	Start delay	0:01:45	0:00:02	0:00:01	0:00:02	0:00:00	0:00:00	0:00:01
	Stop before	0:00:00	0:00:00	0:00:00	0:00:02	0:00:01	0:00:01	0:00:02
	$\%CPU_s$	92	93	91	93	89	12	8
%Data		98.351	98.312	98.236	90.873	85.048	7.271	2.798
Snort Analyze	%Analyze	26.151	23.585	24.239	25.319	34.317	100.000	100.000
	%Drop	73.849	76.415	75.761	74.681	65.683	0.000	0.000
	%Alert	2.958	2.417	3.065	31.204	48.283	88.217	95.311
	%F-Pos	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
	%F-Neg	57.936	69.549	63.645	14.085	5.713	0.026	0.017
RealSecure	Start delay	0:01:45	0:00:02	0:00:03	0:00:01	0:00:03	0:00:01	0:00:01
	Name / Event	ping flood / 3	ping flood / 1	ping flood / 1	ping flood / 1	ping flood / 1	ping flood / 1	ping flood / 1
	Hit	3	1	1	1	1	1	1
	Other Event	-	-	-	-	-	-	-
	$\%CPU_r$	81	82	82	78	66	9	5
RealSecure Analyze	%Analyze	100.000	100.000	100.000	100.000	100.000	100.000	100.000
	%Drop	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	%Alert	300.000	100.000	100.000	100.000	100.000	100.000	100.000
	%F-Pos	200.000	0.000	0.000	0.000	0.000	0.000	0.000
	%F-Neg	0.000	0.000	0.000	0.000	0.000	0.000	0.000

การโจมตีด้วยการกราดตรวจทีซีพีพอร์ตและมีข้อมูล

Test No.		1	2	3	4	5	6	7
Test Time	Sec.	606	611	610	607	608	610	609
Attk. rate	bit/s	974	968	971	973	975	973	971
Mon Traffic	bit/s	54,044,942	49,155,702	49,538,285	41,048,427	46,576,337	7,650	4,212
%Data		100.003	99.968	99.951	99.881	99.767	74.703	54.155
Snort	Start delay	0:00:03	0:00:01	0:00:02	0:00:02	0:00:01	0:00:01	0:00:01
	Stop before	0:00:01	0:00:07	0:00:02	0:00:02	0:00:01	0:00:03	0:00:02
	$\%CPU_s$	94	93	93	95	87	2	2
Snort Analyze	%Analyze	29.458	30.384	29.390	28.068	30.918	100.000	100.000
	%Drop	70.542	69.616	70.610	71.932	69.082	0.000	0.000
	%Alert	0.045	0.049	0.055	0.072	0.051	18.343	27.086
	%F-Pos	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
	%F-Neg	58.391	56.874	53.215	52.131	57.256	27.586	27.877
RealSecure	Start delay	0:00:35	0:00:06	0:00:41	0:00:35	0:00:25	0:00:26	0:00:30
	Stop before	0:00:10	0:00:50	0:00:09	0:00:14	0:00:22	0:00:26	0:00:21
	Name / Event	port_scan / 1	port_scan / 1	port_scan / 1	port_scan / 1	port_scan / 1	port_scan / 1	port_scan / 1
	Hit	10	10	10	10	10	10	10
	Other Event	-	-	-	-	-	-	-
	$\%CPU_r$	100	100	100	100	100	100	100
RealSecure Analyze	%Analyze	100.000	100.000	100.000	100.000	100.000	100.000	100.000
	%Drop	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	%Alert	100.000	100.000	100.000	100.000	100.000	100.000	100.000
	%F-Pos	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	%F-Neg	0.000	0.000	0.000	0.000	0.000	0.000	0.000

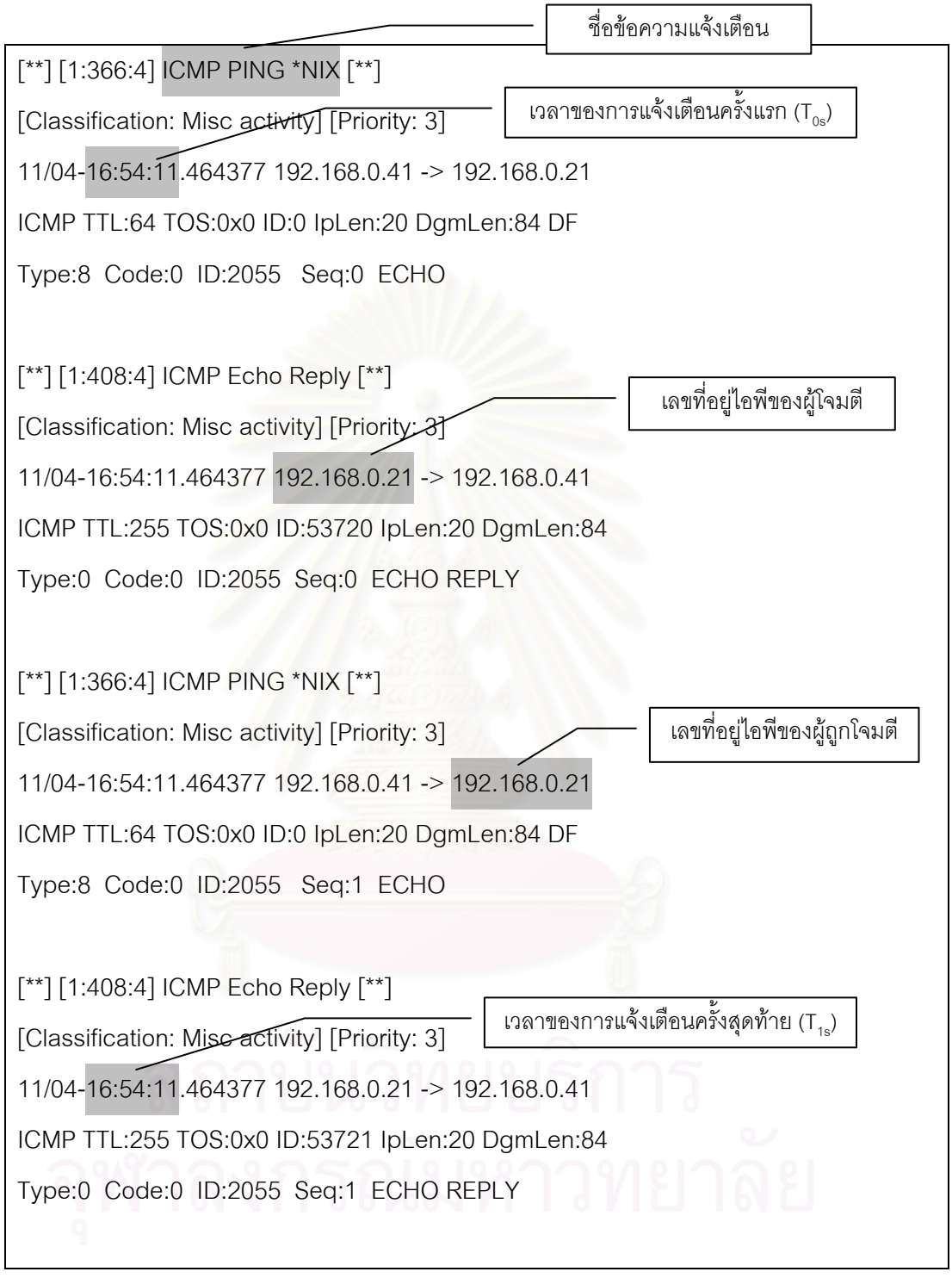
การโจมตีหลายชนิดผสมกัน

Test No.		1	2	3	4	5	6
Test Time	Sec.	607	610	621	623	605	602
Attk. rate	bit/s	4,569,295	4,481,304	9,195,733	9,140,962	5,249,814	5,193,195
Targ Traffic	bit/s	10,861,906	10,690,591	12,438,431	12,421,091	8,926,210	8,759,602
Mon Traffic	bit/s	13,253,514	12,896,975	15,005,544	14,984,625	13,734,477	13,784,284
Snort	Start delay	0:00:01	0:00:02	0:00:00	0:00:01	0:00:00	0:00:00
	Stop before	0:00:02	0:00:03	0:00:00	0:00:04	0:00:02	0:00:02
	$\%CPU_s$	97	100	100	100	91	99
Snort Analyze	%Analyze	5.556	2.972	1.431	1.433	2.431	2.692
	%Drop	1699.929	3265.187	6887.149	701.409	4013.197	3614.047
	%Alert	75.7963	79.9433	22.9619	24.4258	80.5219	78.5194
	%F-Pos	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
	%F-Neg	85.895	92.175	99.307	99.249	94.206	93.722
RealSecure	Start delay	0:00:02	0:00:07	0:00:19	0:00:21	0:00:01	0:00:03
	Stop before	0:00:01	0:00:02	0:00:00	0:00:02	0:00:03	0:00:05
	Name / Event	synflood/1, pingflood/1, pingflood/1	synflood/1, port_scan/1, pingflood/1, pingflood/1	synflood/1, pingflood/1, port_scan/1	synflood/1, port_scan/1, pingflood/1, pingflood/1	synflood/1, port_scan/1, pingflood/1, pingflood/1	synflood/1, port_scan/1
	Hit	10,179	10,161	6,070	6,011	10,117	10,114
	Other Event	-	-	-	-	-	Loki
	$\%CPU_r$	100	100	100	100	100	100
RealSecure Analyze	%Analyze	75.000	100.000	75.000	100.000	100.000	50.000
	%Drop	2.500	0.000	2.500	0.000	0.000	5.000
	%Alert	0.234	0.236	0.051	0.051	0.200	0.202
	%F-Pos	0.000	4.000	9.000	15.000	21.000	26.000
	%F-Neg	99.766	99.764	99.949	99.949	99.800	99.798

ภาคผนวก จ

ตัวอย่างข้อความแจ้งเตือนของโปรแกรมสนอร์ท

ข้อความแจ้งเตือนที่บันทึกลงไฟล์ เมื่อตรวจพบการโจมตีด้วยกลุ่มข้อมูลจำนวนมาก



ข้อความแจ้งเตือนที่บันทึกลงไฟล์ เมื่อตรวจพบการโจมตีด้วยการกราดตรวจทีซีพีพอร์ต

```
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
11/05-09:48:27.472119 192.168.0.37 -> 192.168.0.41
ICMP TTL:255 TOS:0xC0 ID:48347 IpLen:20 DgmLen:88
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.0.41:1520 -> 192.168.0.37:3
TCP TTL:64 TOS:0x0 ID:14846 IpLen:20 DgmLen:60
******S* Seq: 0xB767EACC  Ack: 0x0  Win: 0x16D0  TcpLen: 40
** END OF DUMP

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 192.168.0.41
(THRESHOLD 4 connections exceeded in 0 seconds) [**]
11/05-09:48:27.538364

[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
11/05-09:48:27.472119 192.168.0.37 -> 192.168.0.41
ICMP TTL:255 TOS:0xC0 ID:48349 IpLen:20 DgmLen:88
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.0.41:1522 -> 192.168.0.37:7
TCP TTL:64 TOS:0x0 ID:15195 IpLen:20 DgmLen:60
******S* Seq: 0xB771E868  Ack: 0x0  Win: 0x16D0  TcpLen: 40
** END OF DUMP

[**] [100:2:1] spp_portscan: portscan status from 192.168.0.41: 6 connections across
1 hosts: TCP(6), UDP(0) [**] 11/05-09:52:27.478032
```

ข้อความแจ้งเตือนที่บันทึกลงไฟล์ เมื่อตรวจพบการโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์

```
[**] [1:499:1] MISC Large ICMP Packet [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
10/02-15:27:05.888773 192.168.0.37 -> 255.255.255.255
ICMP TTL:255 TOS:0x0 ID:59688 IpLen:20 DgmLen:1028
Type:8  Code:0  ID:0   Seq:0  ECHO
[Xref => http://www.whitehats.com/info/IDS246]

[**] [1:499:1] MISC Large ICMP Packet [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
10/02-15:27:05.908773 192.168.0.37 -> 58.0.0.17
ICMP TTL:255 TOS:0x0 ID:59689 IpLen:20 DgmLen:1028
Type:8  Code:0  ID:0   Seq:0  ECHO
[Xref => http://www.whitehats.com/info/IDS246]

[**] [1:499:1] MISC Large ICMP Packet [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
10/02-15:27:05.928773 192.168.0.37 -> 255.255.255.255
ICMP TTL:255 TOS:0x0 ID:59690 IpLen:20 DgmLen:1028
Type:8  Code:0  ID:0   Seq:0  ECHO
[Xref => http://www.whitehats.com/info/IDS246]

[**] [1:499:1] MISC Large ICMP Packet [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
10/02-15:27:05.948773 192.168.0.37 -> 255.255.255.255
ICMP TTL:255 TOS:0x0 ID:59691 IpLen:20 DgmLen:1028
Type:8  Code:0  ID:0   Seq:0  ECHO
[Xref => http://www.whitehats.com/info/IDS246]
```

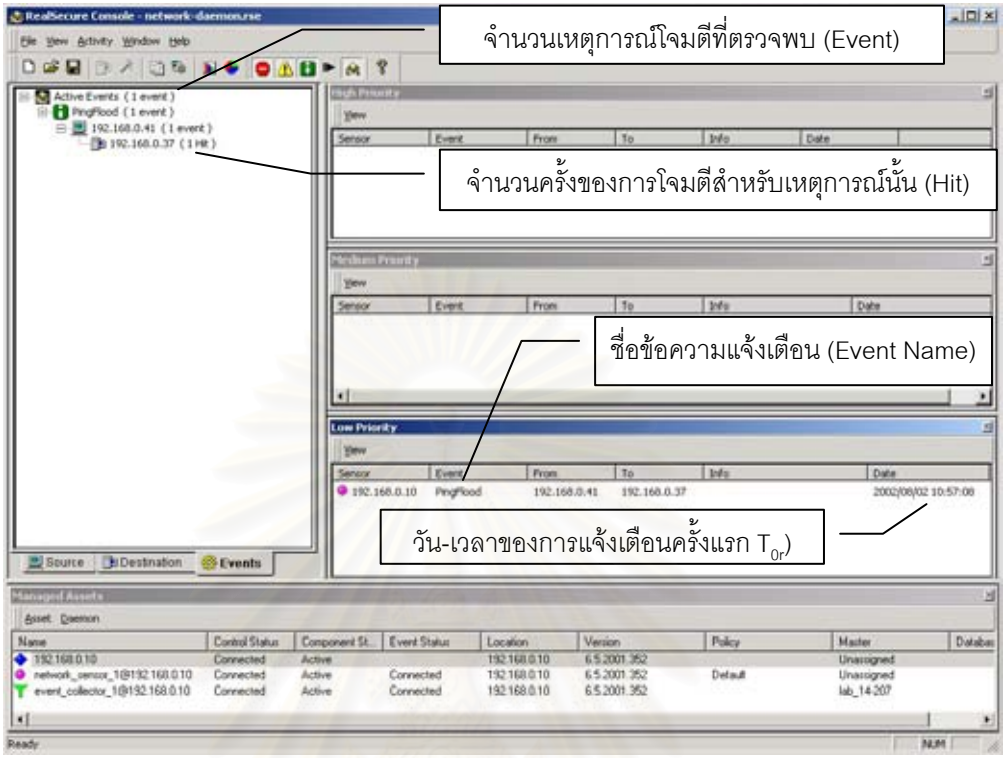
ข้อความแจ้งเตือนที่บันทึกลงไฟล์ เมื่อตรวจพบการโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมาก

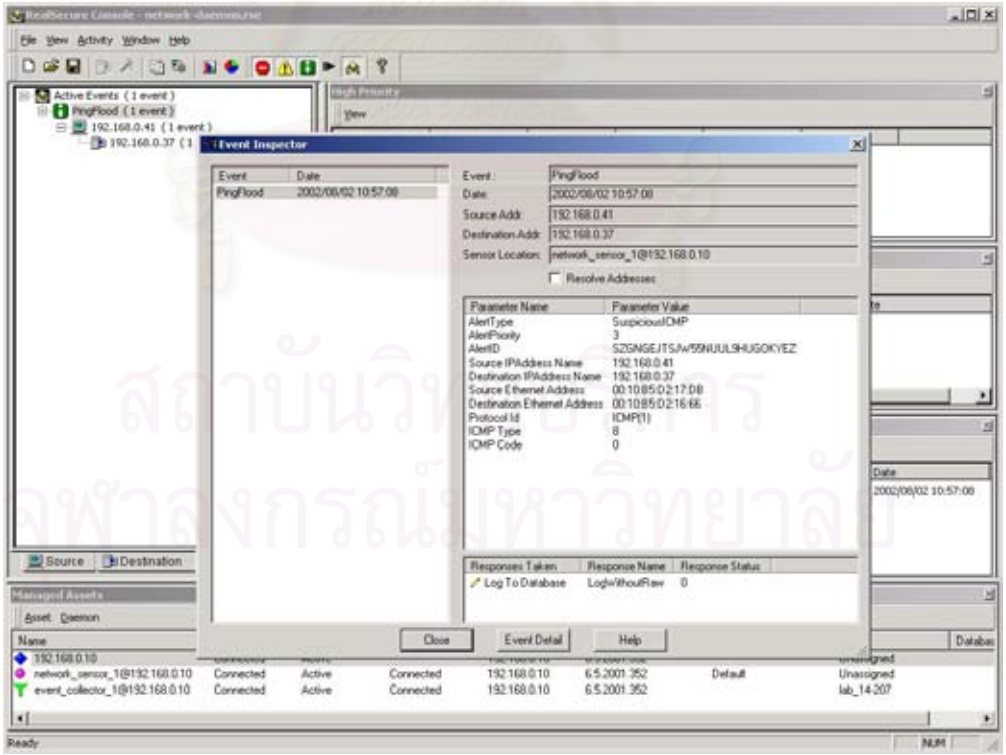
```
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
01/23-16:21:22.526505 192.168.0.37 -> 192.168.0.41
ICMP TTL:255 TOS:0xC0 ID:10762 IpLen:20 DgmLen:68
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.0.41:52004 -> 192.168.0.37:80
TCP TTL:255 TOS:0x0 ID:52004 IpLen:20 DgmLen:40
******S* Seq: 0xCB240000  Ack: 0x0  Win: 0x200  TcpLen: 20
** END OF DUMP

[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
01/23-16:21:22.526505 192.168.0.37 -> 192.168.0.41
ICMP TTL:255 TOS:0xC0 ID:10763 IpLen:20 DgmLen:68
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.0.41:52260 -> 192.168.0.37:80
TCP TTL:255 TOS:0x0 ID:52260 IpLen:20 DgmLen:40
******S* Seq: 0xCC240000  Ack: 0x0  Win: 0x200  TcpLen: 20
** END OF DUMP
```

ภาคผนวก ฉ

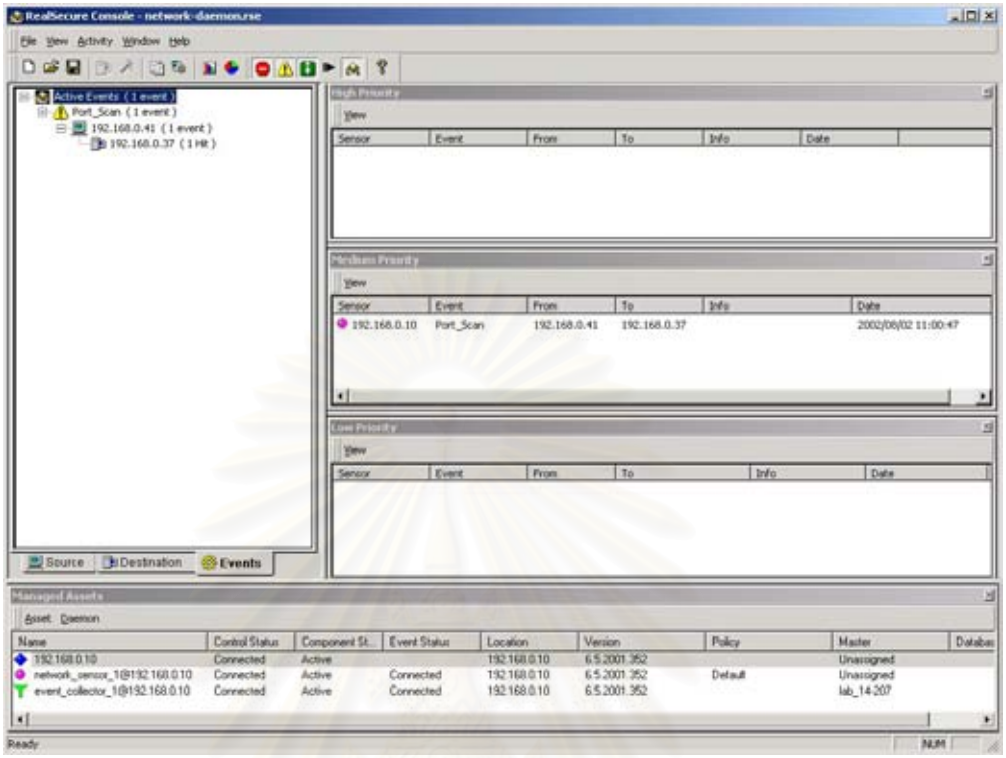
ตัวอย่างการแจ้งเตือนของโปรแกรมเรียลซีเคียว

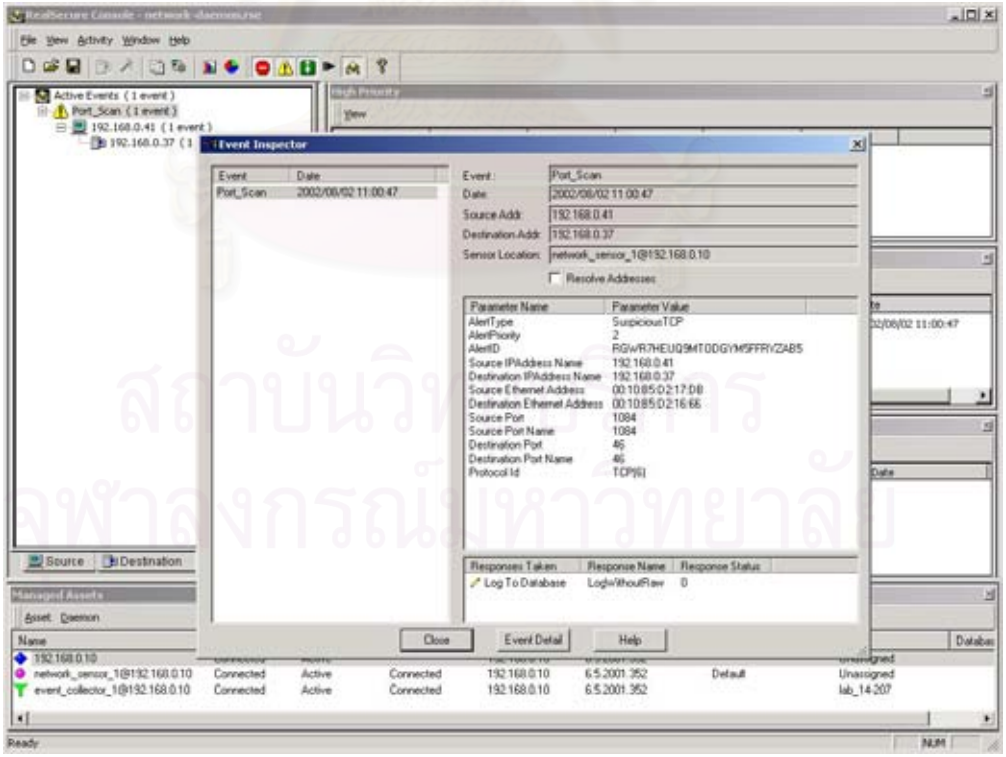
การแจ้งเตือนที่เกิดขึ้นเมื่อตรวจพบการโจมตีด้วยกลุ่มข้อมูลจำนวนมาก



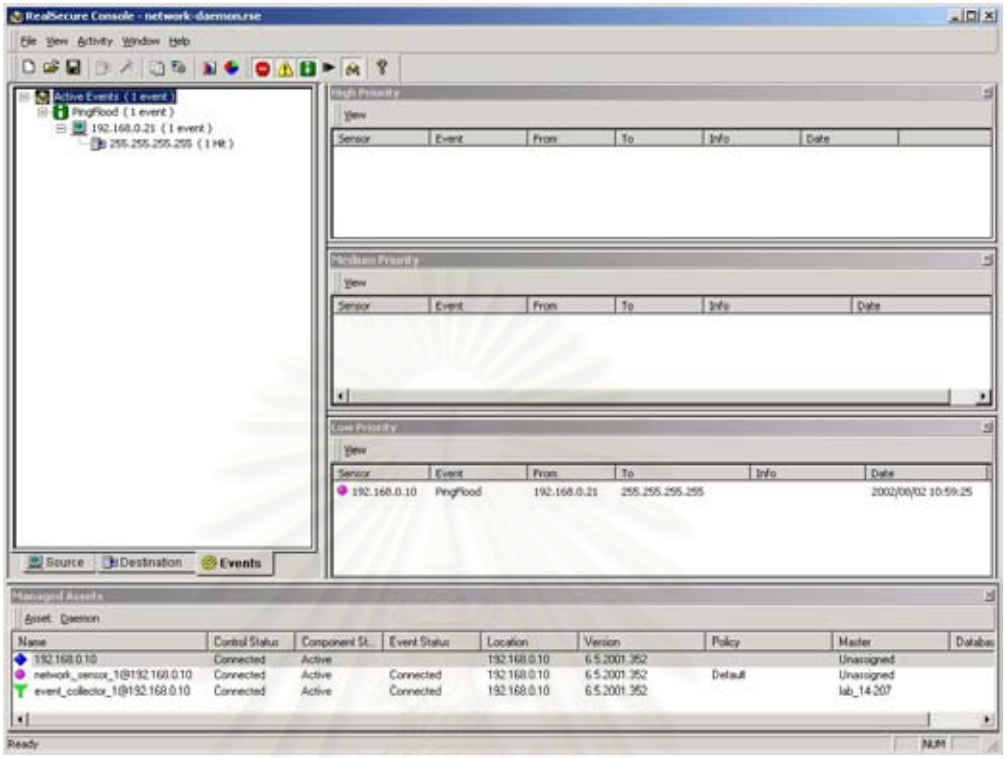


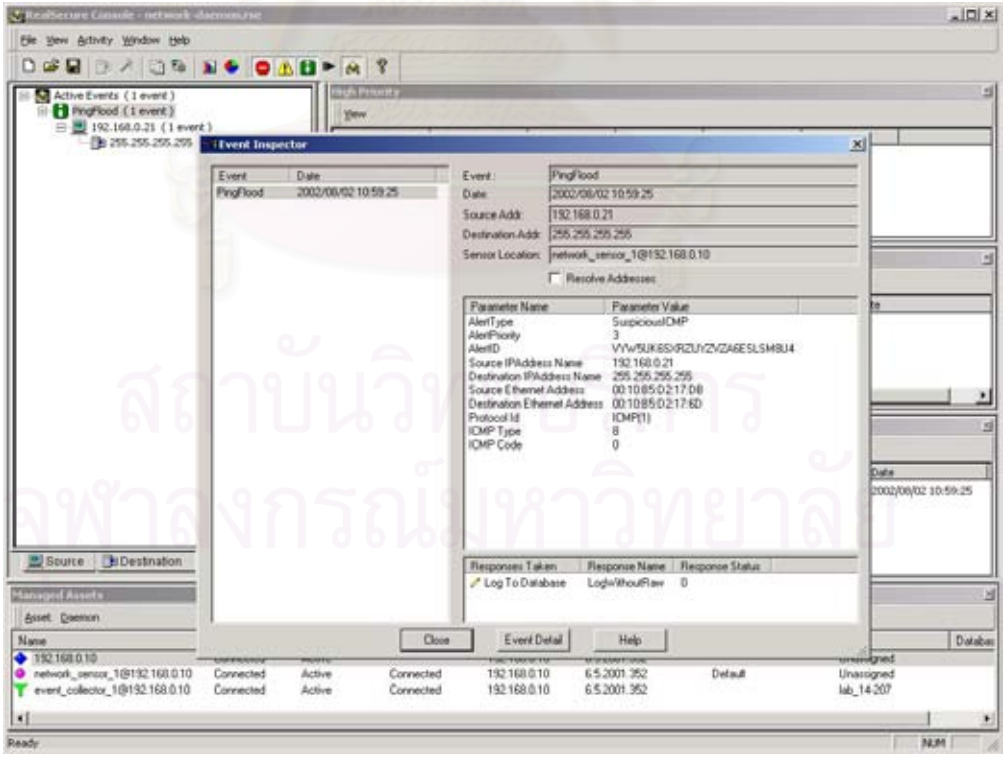
การแจ้งเตือนเมื่อตรวจพบการโจมตีด้วยการกราดตรวจทีซีพีพอร์ต



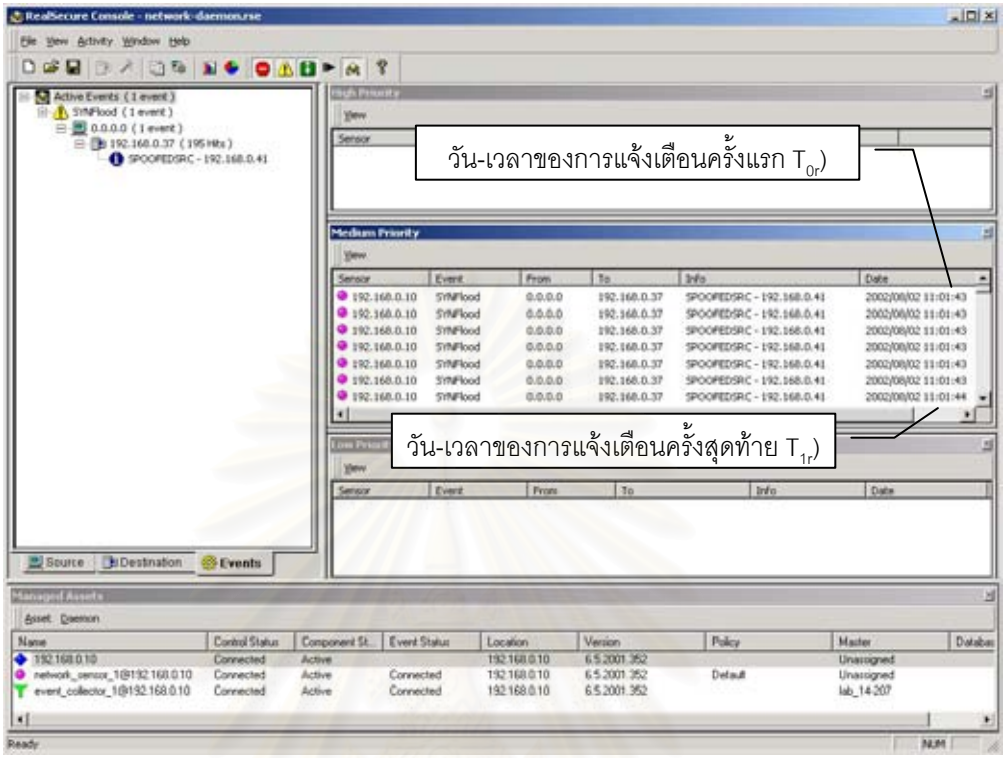


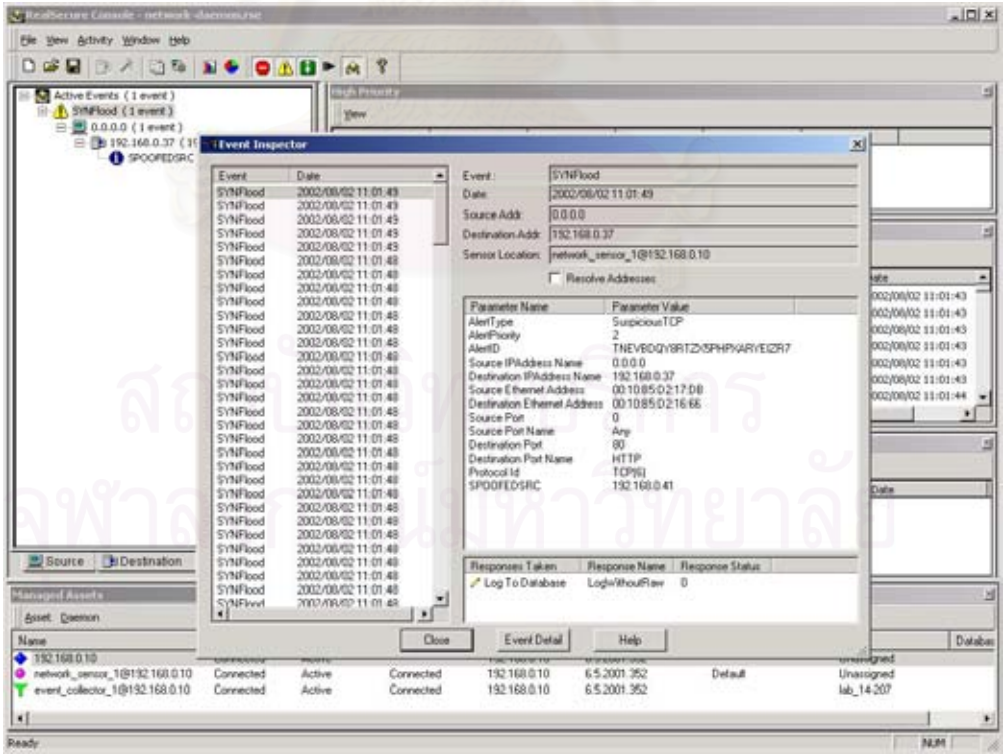
การแจ้งเตือนเมื่อตรวจพบการโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์





การแจ้งเตือนเมื่อตรวจพบการโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมาก





ประวัติผู้เขียนวิทยานิพนธ์

นางสาว กาญจนา ศิลาวราเวทย์ เกิดวันพฤหัสบดีที่ 10 กรกฎาคม พ.ศ. 2518 จ. กรุงเทพฯ จบการศึกษาชั้นปริญญาตรีที่มหาวิทยาลัยสยาม สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ ปัจจุบัน (พ.ศ. 2546) เป็นอาจารย์อยู่ที่มหาวิทยาลัยสยาม