การวิเคราะห์ผลกระทบของไอดีเอสต่อคะแนนจุดอ่อนแบบเครือข่าย

นางสาวธนัชพร นพเกี้อ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2551

AN ANALYSIS OF EFFECT OF IDS ON NETWORK-BASED VULNERABILITY SCORE

Miss Thanutchaporn Noppakua

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University

Academic Year 2008

หัวข้อวิทยานิพนธ์	การวิเคราะห์ผลกระทบของไอดีเอสต่อคะแนนจุดอ่อนแบบเครือข่าย
โดย	นางสาวธนัชพร นพเกื้อ
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร.ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์

(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(อาจารย์ จารุมาตร ปิ่นทอง)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(อาจารย์ ดร.ยรรยง เต็งอำนวย)

.....กรรมการ

(รองศาสตราจารย์ ดร.ทวีตีย์ เสนีวงศ์ ณ อยุธยา)

.....กรรมการภายนอกมหาวิทยาลัย

(ดร.โกเมน พิบูลย์โรจน์)

ธนัชพร นพเกื้อ : การวิเคราะห์ผลกระทบของไอดีเอสต่อคะแนนจุดอ่อนแบบเครือข่าย. (AN ANALYSIS OF EFFECT OF IDS ON NETWORK-BASED VULNERABILITY SCORE) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: อ.ดร.ยรรยง เต็งอำนวย, จำนวนหน้า 63 หน้า.

ระบบตรวจจับการบุกรุก เป็นมาตรการการป้องกันระบบคอมพิวเตอร์และระบบเครือข่ายที่สำคัญมาก มีงานวิจัยมากมายที่มีการวิเคราะห์ถึงความสามารถของระบบตรวจจับการบุกรุกจากการป้องกันการโจมตี หรือจำนวนของการตรวจจับที่ผิดพลาด

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

จากงานวิจัยพบว่า สนอร์ทสามารถป้องกันจุดอ่อนที่มีอันตรายของระบบเครือข่ายของระบบปฏิบัติการวินโดวส์ได้ 73% และ ในระบบปฏิบัติการตระกูลยูนิกซ์ได้ 65% จากผลการทดลองทำให้ทราบได้ว่า ระบบตรวจจับการบุกรุกมีประสิทธิภาพ แต่ยังคงต้องมีการปรับปรุงในส่วนที่ยังป้องกันไม่ได้

ภาควิชา...วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต.....ธนัชพร นพเกื้อ.....
สาขาวิชา...วิทยาศาสตร์คอมพิวเตอร์..... ลายมือชื่อ อ. ที่ปรึกษาวิทยานิพนธ์หลัก.....
ปีการศึกษา.....2551.....

4970341421 : MAJOR COMPUTER SCIENCE

KEYWORDS: SNORT / SANS / CVE / VULNERABILITY SCORE / WINDOWS / UNIX

THANUTCHAPORN NOPPAKUA: AN ANALYSIS OF EFFECT OF IDS ON NETWORK-BASED VULNERABILITY SCORE. ADVISOR: YUNYONG TENG-AMNUAY, Ph.D., 63 pp.

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

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

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

Department: Computer Engineering Student's Signature: .....

Field of Study: Computer Science Advisor's Signature: .....

Academic Year: 2008

กิตติกรรมประกาศ

วิทยานิพนธ์นี้จะไม่สามารถสำเร็จลุล่วงไปได้ด้วยดี หากไม่ได้รับคำปรึกษาแนะนำอันเป็นประโยชน์อย่างยิ่งจาก อ.ดร.ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์

ขอบคุณเพื่อนๆ พี่ๆ และน้องๆ ทุกคนที่ให้กำลังใจ ข้อคิดเห็น และให้ความช่วยเหลือในทุกๆ ด้าน ตลอดจนช่วยสร้างบรรยากาศในการวิจัยที่มีค่ายิ่งให้แก่ผู้วิจัย ทำให้งานวิจัยชิ้นนี้สำเร็จลุล่วงไปได้ด้วยดี

ท้ายนี้ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ ที่ให้การสนับสนุนและดูแลเอาใจใส่ผู้วิจัยด้วยความรักและเมตตา ตลอดจนเป็นกำลังใจให้แก่ผู้วิจัยจนสามารถทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

สารบัญ

หน้า

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

หน้า

บทที่ 1

บทนำ

1.1 ที่มาและความสำคัญของปัญหา

การรักษาความมั่นคงให้กับเครือข่ายคอมพิวเตอร์เป็นเรื่องที่มีความสำคัญมาก เนื่องจากมีความพยายามที่จะป้องกันข้อมูลและป้องกันระบบการดำเนินงานภายในองค์กรจากการถูกโจมตี ซึ่งนับวันจะพัฒนาวิธีการและรูปแบบการโจมตีให้มีความหลากหลายและซับซ้อนมากยิ่งขึ้น ส่วนใหญ่การโจมตีนั้นจะมุ่งไปยังจุดอ่อน (Vulnerability) ของซอฟต์แวร์หรือของระบบปฏิบัติการ เพื่อจะใช้แทรกแซงการทำงานหรือทำให้ระบบเกิดความเสียหาย

แม้ว่าจะมีการประกาศให้ทราบต่อสาธารณะว่าระบบมีจุดอ่อนอะไรบ้าง เพื่อให้ผู้ดูแลระบบหาทางป้องกันหรือปิดจุดอ่อนนั้น แต่อย่างไรก็ตามจุดอ่อนของระบบนี้อาจไม่ได้รับการแก้ไขเนื่องมาจาก ไม่สามารถทำการปิดจุดอ่อนนั้นได้ เพราะผู้ใช้จำเป็นต้องใช้จุดอ่อนนั้นในการปฏิบัติงาน หรือเกิดความผิดพลาดในการติดตั้งระบบ รวมทั้งการที่ผู้ดูแลไม่ได้มีการติดตามว่าเครื่องใดมีการปิดจุดอ่อนนั้นบ้าง

เนื่องด้วยสาเหตุต่างๆ ดังที่ได้กล่าวมาข้างต้น จึงมีความจำเป็นที่จะต้องมีการติดตั้งเครื่องมือรักษาความมั่นคงของระบบ ซึ่งสิ่งที่เป็นด่านแรกของการป้องกัน คือ ไฟร์วอลล์ (Firewall) รวมไปถึงระบบการรักษาความมั่นคงอื่นๆ ไว้คอยตรวจสอบผู้บุกรุกที่อาจจะผ่านเข้ามาในระบบได้ เช่น มีการใช้ระบบตรวจจับการบุกรุก หรือ ไอดีเอส (IDS: Intrusion Detection System) ซึ่งเป็นเครื่องมือสำหรับตรวจจับการบุกรุกผ่านจุดอ่อนที่ยังไม่ได้รับการแก้ไข นอกจากนี้ไอดีเอสยังทำหน้าที่ในการป้องกันระบบโดยมีการรายงานว่ามีการบุกรุกเข้ามาในระบบ เพื่อให้ผู้ดูแลได้รับทราบและหาทางป้องกันได้

แม้ว่าระบบไอดีเอสจะสามารถทำการตรวจสอบผู้บุกรุกได้ แต่ไม่ได้มีการรายงานในภาพรวมถึงความสามารถในการลดจุดอ่อนของระบบ ดังนั้นจึงมีแนวความคิดที่จะศึกษาและทำการวิเคราะห์ถึงผลกระทบต่อค่าระดับคะแนนของจุดอ่อนเมื่อมีการติดตั้งระบบไอดีเอสให้กับระบบคอมพิวเตอร์ โดยวิเคราะห์จากความสามารถในการป้องกันจุดอ่อนตามรายงานของสถาบันแซนส์ (SANS Institute) [1] ซึ่งจะแบ่งเป็นประเภทต่างๆ ตามบริการที่มีในระบบปฏิบัติการวินโดวส์ (Windows) และยูนิกซ์ (UNIX) โดยใช้ระบบไอดีเอส ชื่อ สนอร์ท (Snort) [2] เป็นกรณีศึกษา เพื่อ

เป็นข้อมูลให้ผู้ดูแลระบบใช้ประกอบการตัดสินใจในการเลือกวิธีการที่เหมาะสมเพื่อเพิ่มการรักษาความมั่นคงให้กับระบบต่อไป

1.2 วัตถุประสงค์ของการวิจัย

เพื่อทำการวิเคราะห์ถึงระดับความสามารถในการลดคะแนนของจุดอ่อนของสนอร์ทและจุดอ่อนที่สนอร์ทไม่สามารถป้องกันได้ โดยการสร้างโมเดลการให้คะแนนจุดอ่อนของบริการต่างๆ ที่เป็นภัยร้ายแรงตามรายการของซีวีอี สำหรับระบบปฏิบัติการวินโดวส์ และระบบปฏิบัติการตระกูลยูนิกซ์

1.3 ขอบเขตของการวิจัย

1. ทำการตรวจจับการบุกรุกเฉพาะทางเครือข่าย
2. ข้อมูลจุดอ่อนของสถาบันแซนส์ใช้ รายงานของปี 2000-2007
3. ข้อมูลกฎของสนอร์ท ข้อมูลจุดอ่อนในรายการซีวีอี และข้อมูลจุดอ่อนในรายการเอ็นวีดี ใช้อย่างน้อยถึงเดือนกันยายน พ.ศ. 2551

1.4 ขั้นตอนของการวิจัย

1. ศึกษาการเสริมความมั่นคงให้กับระบบ
2. ศึกษารูปแบบของระบบไอดีเอส
3. ทำการคัดกรองข้อมูลจุดอ่อนที่เป็นภัยร้ายแรงต่อระบบตามรายงานของสถาบันแซนส์
4. ทำการคัดกรองรายการจุดอ่อนของสนอร์ทที่มีการอ้างอิงถึงรายการจุดอ่อนของซีวีอี
5. ศึกษารูปแบบการจัดกลุ่มของจุดอ่อน
6. ศึกษาการให้คะแนนของจุดอ่อน
7. ทำการแบ่งประเภทของจุดอ่อนที่พบ และให้คะแนนจุดอ่อนแต่ละตัว
8. ทำการคิดค่าระดับคะแนนของจุดอ่อนแต่ละประเภท
9. วิเคราะห์และประเมินผลความสามารถการป้องกันจุดอ่อนของระบบโดยการติดตั้งไอดีเอส
10. สรุปผลการวิจัย
11. เรียบเรียงและจัดทำวิทยานิพนธ์

1.5 ประโยชน์ที่ได้รับ

สามารถทราบถึงภาพรวมของผลกระทบต่อค่าความเปราะบางของระบบเมื่อทำการติดตั้งระบบไอดีเอส นอกจากนั้นผลลัพธ์ที่ได้ ช่วยให้ผู้ดูแลระบบใช้เป็นทางเลือกประกอบการตัดสินใจในการเลือกใช้สนอร์ท และหาวิธีการที่เหมาะสมในการป้องกันส่วนของจุดอ่อนที่สนอร์ทไม่สามารถป้องกันได้ รวมทั้งสามารถเป็นแนวทางให้ผู้ดูแลระบบหาวิธีการที่เหมาะสมในการเพิ่มการรักษาความมั่นคงให้กับระบบต่อไป

1.6 โครงสร้างของวิทยานิพนธ์

เนื้อหาของวิทยานิพนธ์ฉบับนี้แบ่งออกเป็น 5 บท ดังนี้คือ บทที่ 1 เป็นบทนำของงานวิจัย บทที่ 2 กล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้องกับงานวิจัยชิ้นนี้ บทที่ 3 กล่าวถึงวิธีการดำเนินงานวิจัยในแต่ละขั้นตอนอย่างละเอียด บทที่ 4 กล่าวถึงการออกแบบและการพัฒนาเครื่องมือ บทที่ 5 เป็นการทดลองและอธิบายผลการทดลองในประเด็นต่างๆ และบทที่ 6 เป็นการสรุปผลการทดลองและข้อเสนอแนะจากงานวิจัย ซึ่งอาจเป็นประโยชน์กับการวิจัยเพิ่มเติมในอนาคต

1.7 ผลงานตีพิมพ์จากวิทยานิพนธ์

ส่วนหนึ่งของงานวิทยานิพนธ์นี้ได้รับการตีพิมพ์เป็นบทความวิชาการในหัวเรื่อง “Effectiveness Analysis of IDS Using Vulnerability Scores” โดยธนัชพร นพเกื้อ และยรรยง เต็งอำนวย ในงานประชุมวิชาการ “Proceedings of 2nd National Conference on Information Technology (NCIT 2008)” ซึ่งจัดขึ้น ณ โรงแรมแกรนด์ เมอร์เคียวร์ กรุงเทพมหานคร ประเทศไทย ระหว่างวันที่ 6-7 พฤศจิกายน 2551

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 **องค์ประกอบของความมั่นคง** (The Basic Components of Security)

ความมั่นคงของระบบคอมพิวเตอร์ จะขึ้นอยู่กับคุณสมบัติทั้งสามด้าน ดังนี้

1. การเป็นความลับ (Confidentiality) คือ การซ่อนหรือบิดบังข้อมูลหรือทรัพยากรให้สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น มีกลไกที่ใช้ป้องกันคือการเข้ารหัสข้อมูล (Cryptography) และการควบคุมการเข้าถึง (Access Control)

2. ความบูรณภาพ (Integrity) คือ ความเชื่อถือได้ของข้อมูล ซึ่งหมายถึงการป้องกันไม่ให้ข้อมูลถูกเปลี่ยนแปลงไปจากเดิม ซึ่งกลไกที่ใช้ป้องกันคือการควบคุมการเข้าถึง (Access Control)

3. ความพร้อมใช้งาน (Availability) คือ ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ ซึ่งอาจมีผู้ไม่หวังดีทำการโจมตีแบบปฏิเสธการให้บริการ หรือ DoS attack

2.2 **จุดอ่อนของระบบคอมพิวเตอร์** (Computer Vulnerability)

จุดอ่อน (Vulnerability) คือ ช่องทางที่เป็นรอยรั่วหรือช่องโหว่ของระบบทั่วๆไปที่ให้ผู้ไม่หวังดีทำการโจมตีระบบ และสร้างความเสียหายได้ [3] โดยที่จุดอ่อนสามารถเกิดได้จากทุกส่วนของระบบคอมพิวเตอร์ ไม่ว่าจะเป็นซอฟต์แวร์ทั่วไปของระบบหรือแม้แต่ระบบปฏิบัติการก็ตาม

2.3 **ฐานข้อมูลจุดอ่อน** (Vulnerability Source)

ซีวีอี (CVE: Common Vulnerability and Exposures) เป็นงานวิจัยที่ริเริ่มขึ้นเมื่อปี 1999 โดยบริษัทมิตทรี (MITRE Corporation) [4] โดยมีจุดประสงค์เพื่อสร้างมาตรฐานในการอ้างอิงถึงจุดอ่อน โดยข้อมูลของจุดอ่อนนั้นถูกส่งมาจากหน่วยงานด้านความมั่นคงต่างๆ หรือบริษัทที่ทำการผลิตซอฟต์แวร์หรือฮาร์ดแวร์นั้น เพื่อจะทำการพิจารณาหาความสัมพันธ์ของจุดอ่อนแต่ละแหล่ง และจะทำการพิจารณาเทียบกับนิยามของซีวีอี หากได้ข้อสรุปแล้ว ก็จะทำการเพิ่มรายการจุดอ่อนที่ผ่านการพิจารณาแล้วเข้าสู่รายการของซีวีอี

การกำหนดชื่อให้กับจุดอ่อน มีรูปแบบเป็น CVE-xxxx-yyyy โดยที่ xxxx คือปีที่ออกหมายเลขแคนดิเดด (Candidate) และ yyyy คือลำดับของแคนดิเดดที่ออกในปีนั้น รูปที่ 2.1 แสดงตัวอย่างรายการในซีวีอี

N a m e	CVE-1999-0270
Status	Entry
Description	Directory traversal vulnerability in pfdisplay.cgi program (sometimes referred to as “pfdisplay”) for SGI’s Performer API Search Tool (performer_tools) allows remote attackers to read arbitrary files.

รูปที่ 2.1 ตัวอย่างจุดอ่อนในรายการซีวีอี

เอ็นวีดี (NVD: National Vulnerability Database) [5] เป็นฐานข้อมูลเกี่ยวกับการโจมตีตามหมายเลขของซีวีอี ถูกพัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งประเทศสหรัฐอเมริกา หรือเอ็นไอเอสที (NIST: National Institute of Standard and Technology) ซึ่งจะให้ข้อมูลเกี่ยวกับการโจมตีประเภทต่างๆ และคำแนะนำเกี่ยวกับการแก้ไข

ฐานข้อมูลจุดอ่อนระบบเปิด หรือ โอเอสวีดีบี (OSVDB: Open Source Vulnerability Database) [6] ให้บริการเกี่ยวกับจุดอ่อนต่างๆ โดยไม่คิดค่าใช้จ่าย และมีการเปิดเผยโครงสร้างของฐานข้อมูล มีการปรับปรุงข้อมูลให้ทันสมัยอยู่เสมอ โดยที่จุดอ่อนในฐานข้อมูลนี้มีการอ้างอิงมาจากที่ต่างๆ มากมาย เช่น ซีวีอี บั๊กแทรค สนอร์ท เป็นต้น

บั๊กแทรค (Bugtraq) [7] เป็นรูปแบบหนึ่งของการรายงานจุดอ่อน ซึ่งจะเป็นบัญชีจ่าหน้า (mailing list) สำหรับการถกเถียงเกี่ยวกับจุดอ่อนและวิธีการแก้ไข ซึ่งสามารถค้นหารายการจุดอ่อนได้จาก ผู้ผลิตสินค้า หรือจากรายการซีวีอี โดยจะมีคำอธิบายจุดอ่อน ชนิดของจุดอ่อน และวิธีการแก้ไขจุดอ่อนนั้น

สถาบันแซนส์ (SANS Institute) [1] เผยแพร่สรุปถึงจุดอ่อนที่สำคัญ 10 รายการโดยเริ่มในปี ค.ศ.2000 ซึ่งเป็นจุดอ่อนที่มีอันตรายต่อความมั่นคงของเครือข่ายอินเทอร์เน็ต และได้มีการเพิ่มเติมขึ้นเป็น 20 จุดอ่อน ซึ่งแบ่งได้เป็น 2 กลุ่มคือ รายการ 10 จุดอ่อนที่เป็นอันตรายต่อบริการบนระบบปฏิบัติการวินโดวส์ และ 10 จุดอ่อนที่เป็นอันตรายต่อบริการบนระบบปฏิบัติการตระกูลยูนิกซ์ แม้ว่าจะมีการโจมตีทั้งสองระบบปฏิบัติการนี้เป็นจำนวนมาก แต่การโจมตีที่ประสบความสำเร็จ ส่วนใหญ่เกิดขึ้นกับจุดอ่อนที่มีในรายงานนี้แทบทั้งสิ้น

2.4 ระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุก (IDS: Intrusion Detection System) คือระบบที่ใช้ในการตรวจตราสอดส่องการใช้งานเพื่อหาการกระทำที่ขัดกับนโยบายขององค์กร และมีผลกระทบต่อความมั่นคงของระบบคอมพิวเตอร์หรือเครือข่ายทั้ง 3 ประการ คือ การเสียความเป็นความลับ การเสียบูรณภาพ และการเสียสภาพพร้อมใช้งาน

ระบบตรวจจับการบุกรุก แบ่งตามประเภทของแหล่งข้อมูลที่นำมาวิเคราะห์ ได้ดังนี้

1. โฮสต์เบสไอดีเอส (HIDS: Host-Based Intrusion Detection System) รวบรวมข้อมูลจากเครื่องคอมพิวเตอร์ เพื่อตรวจสอบว่าโปรแกรมหรือผู้ใช้คนใดที่ทำให้เกิดการบุกรุกขึ้นในระบบ และผลของการบุกรุกเป็นอย่างไร

2. เน็ตเวิร์คเบสไอดีเอส (NIDS: Network-Based Intrusion Detection System) ติดตามและวิเคราะห์ข้อมูลที่รับส่งกันในเครือข่าย เพื่อดูว่ามีผู้บุกรุกหรือความผิดปกติเกิดขึ้นหรือไม่ โดยจะดักจับข้อมูลบนเครือข่ายแล้วนำแพ็กเก็ตมาวิเคราะห์ว่าเข้ากับรูปแบบหรือร่องรอยการบุกรุก (signature) ที่กำหนดไว้ในฐานข้อมูลของไอดีเอสตัวนั้นๆ หรือไม่

แนวทางในการตรวจจับการบุกรุกหรือความพยายามในการบุกรุก มีสองแนวทางคือการตรวจจับสิ่งผิดปกติในระบบ (Anomaly detection) และ การตรวจจับการใช้งานที่ผิดจากรูปแบบที่กำหนดไว้แล้ว (Misuse detection)

2.5 สนอร์ท

สนอร์ท [2] เป็นเครื่องมือที่ใช้ในการตรวจจับการบุกรุกทางเครือข่าย (NIDS) แบบโอเพนซอร์ซที่ได้รับความนิยมมากที่สุด ซึ่งถูกพัฒนาโดย มาร์ติน โรอีสช์ (Martin Roesch) สนอร์ทสามารถทำการสแกนแพ็กเก็ตของข้อมูลที่วิ่งบนเครือข่าย และบันทึกสิ่งที่ตรวจพบลงบนฐานข้อมูลมายเอสคิวแอล (MySQL) และใช้โปรแกรม เอซีไอดี (ACID: Analysis Console for Intrusion Database) [8] สำหรับวิเคราะห์เหตุการณ์ต่างๆ ที่เกิดขึ้น นอกจากนี้ยังสามารถหยุดการโจมตีบางอย่างได้

สนอร์ทสามารถทำงานได้ 3 รูปแบบ คือ [9]

1. แบบสนิฟเฟอร์ (Sniffer Mode) เป็นแบบที่อ่านแพ็กเก็ตจากเครือข่ายอย่างเดียว แล้วแสดงบนหน้าจออย่างต่อเนื่อง

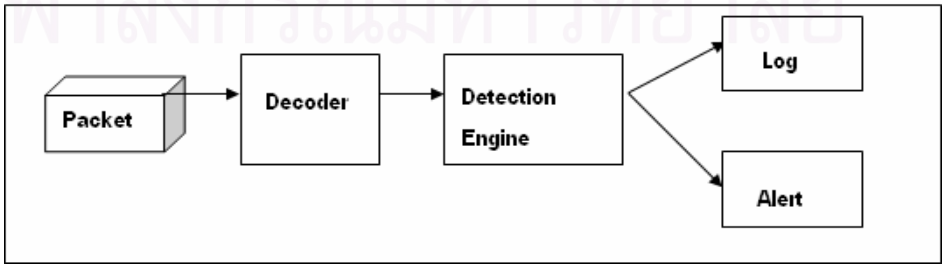
2. แบบแพ็กเก็ตล็อกเกอร์ (Packet Logger Mode) เป็นแบบที่บันทึกแพ็กเก็ตลงดิสก์

3. แบบเอ็นไอดีเอส (NIDS Mode) เป็นแบบที่มีการทำงานที่ซับซ้อนที่สุด โดยทำการวิเคราะห์ทราฟฟิกที่วิ่งบนเครือข่ายโดยเปรียบเทียบกับกฎ [10] ที่ผู้ใช้กำหนดไว้

สนอร์ทสามารถทำงานแบบไอพีเอส (IPS: Intrusion Prevention System) โดยมีการทำงานในแบบ อินไลน์ (Inline Mode) [11] ซึ่งสนอร์ทจะตรวจสอบแพ็กเก็ตจากแฟ้มบันทึกในรูปแบบไอพีเทเบิล (iptables) แทนที่จะเป็นจากแฟ้มแบบลิบพีแค็บ (libpcap) ซึ่งสามารถสั่งให้ไอพีเทเบิลละทิ้งหรือส่งต่อแพ็กเก็ต โดยขึ้นอยู่กับกฎที่กำหนดไว้

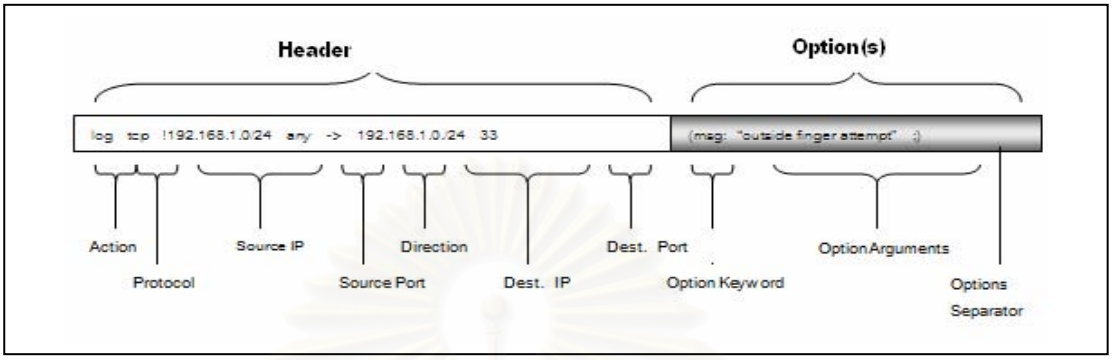
สนอร์ท ใช้ไลบรารี (Library) พื้นฐานชื่อ ลิบพีแค็บ ซึ่งใช้กันในเรื่องของการวิเคราะห์เครือข่าย โดยที่สนอร์ทนั้นสามารถทำการวิคราะห์โพรโทคอล (protocol analysis) การค้นหาและเข้าชุดกันของเนื้อหา (content searching/matching) โดยใช้อัลกอริทึมของ โบเยอร์ มัวร์ (Boyer Moore) [12] การตรวจจับการบุกรุก (Intrusion Detection) และการตรวจสอบอื่นๆ เช่น บัฟเฟอร์โอเวอร์โฟลว์ (buffer overflow) หรือ พอร์ตแสกน (port scan) เป็นต้น

ในการวิเคราะห์แพ็กเก็ต สนอร์ทจะวิเคราะห์ว่าแพ็กเก็ตนั้น ตรงกับกฎที่ตั้งไว้หรือไม่ หากเป็นไปตามกฎที่ตั้งไว้ จะดำเนินการตอบสนองต่อเหตุการณ์นั้นตามที่กำหนดไว้ในกฎ ซึ่งการทำงานของสนอร์ท แสดงได้ดังรูปที่ 2.2 [13]



รูปที่ 2.2 การทำงานของสนอร์ท

กฎของสนอร์ท (Snort Rule) ถูกพัฒนาและทดสอบโดย วีอาร์ที (VRT) แห่ง Sourcefire Vulnerability Research Team [14] กฎของสนอร์ท แบ่งออกเป็นสองส่วนคือ ส่วนของเฮดเดอร์ (Header) และส่วนของออปชัน (Option) ดังรูปที่ 2.3



รูปที่ 2.3 ส่วนประกอบของกฎของสนอร์ท

แต่ละกฎของสนอร์ทอ้างอิงถึงแหล่งที่มาเพื่อให้ทราบว่าใช้ป้องกันจุดอ่อนในเรื่องใด โดยที่ส่วนของการอ้างอิง มีการระบุอยู่ในส่วนที่เป็นออปชัน ซึ่งมีการอ้างอิงมาจากที่ต่างๆ เช่น บั๊กแทรค ซีวีอี เป็นต้น ดังแสดงในรูปที่ 2.4

```
alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ATTACK-RESPONSES
file copied ok"; flow: established; content:"1 file|28|s|29| copied"; nocase; reference: bugtraq, 1806;
reference:cve, 2000-0884; classtype:bad-unknown; sid:497; rev:12;)
```

รูปที่ 2.4 ตัวอย่างกฎของสนอร์ทที่อ้างอิงรายการซีวีอี

ตัวอย่างนี้อ้างอิงถึงจุดอ่อนตามรายการซีวีอีหมายเลข 2000-0884 (ตามที่แสดงเป็นตัวหนา) ซึ่งเป็นจุดอ่อนของ ไอไอเอส (IIS) ซึ่งเป็นเว็บเซอร์เวอร์ของไมโครซอฟท์ ที่อนุญาตให้ผู้โจมตีสามารถทำการเข้าถึงข้อมูลได้

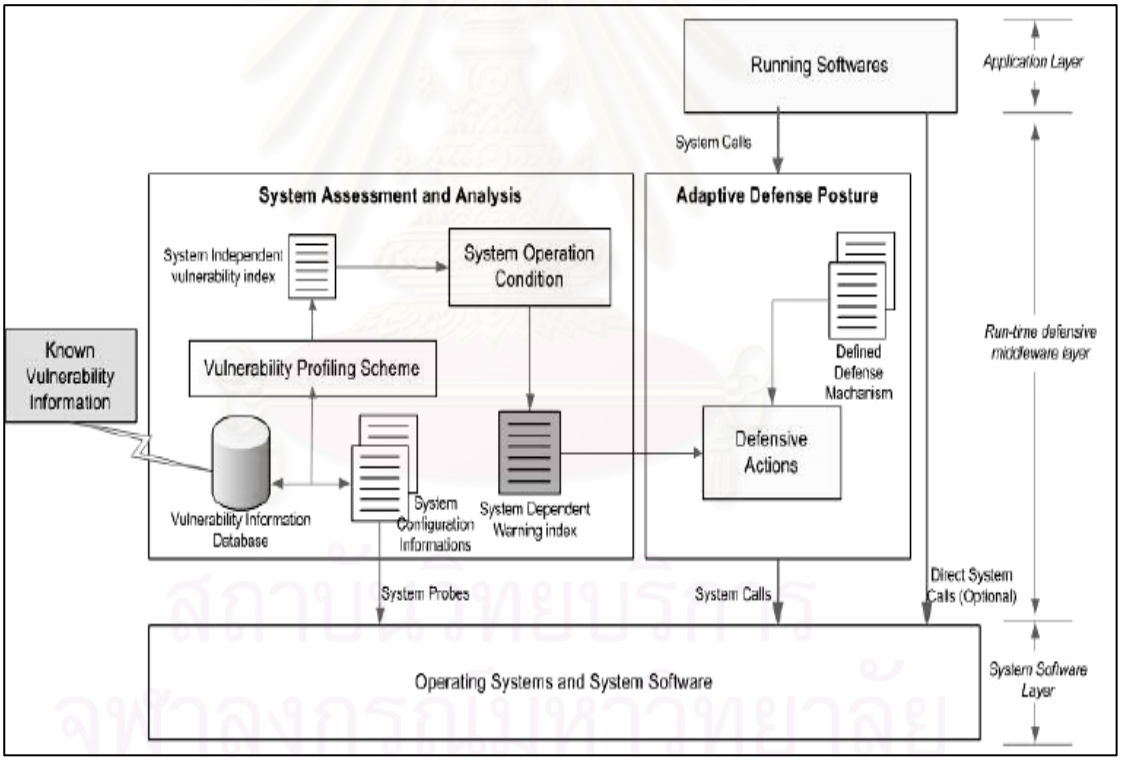
2.6 เอกสารและงานวิจัยที่เกี่ยวข้อง

ที่ผ่านมา มีการค้นพบจุดอ่อนของระบบคอมพิวเตอร์มากขึ้น ทำให้มีงานวิจัยที่เกี่ยวข้องกับการรักษาความมั่นคงโดยการป้องกันจุดอ่อนของระบบอยู่หลายชิ้น งานวิจัยประเภทนี้ออกเป็นสองกลุ่ม คือ งานวิจัยที่เกี่ยวข้องกับการเพิ่มความมั่นคงให้กับระบบ และงานวิจัยที่เกี่ยวข้องกับการแบ่งประเภทของจุดอ่อน ดังนี้

2.1 งานวิจัยที่เกี่ยวกับการเพิ่มความมั่นคงให้กับระบบ

เมื่อซอฟต์แวร์หรือแม้กระทั่งระบบปฏิบัติการมีจุดอ่อน และผู้ดูแลระบบไม่สามารถแก้ไขหรือซ่อมแซมจุดอ่อนนั้นได้ อาจจะเนื่องมาจากยังไม่มีรายงานวิธีการแก้ไขจุดอ่อนจากผู้ผลิตหรือจำนวนจุดอ่อนที่เพิ่มขึ้นอย่างมากมาย ทำให้ผู้ดูแลระบบขาดการดูแลในจุดอ่อนบางอย่างไป

จึงมีงานวิจัยในเรื่องการเพิ่มความมั่นคงให้กับระบบคอมพิวเตอร์ ภายใต้สภาวะที่ระบบคอมพิวเตอร์มีจุดอ่อนอยู่มาก โดยในปี ค.ศ.2004 วิตา และคณะ [15] มีแนวความคิดว่า ในปัจจุบันนี้ จุดอ่อนของระบบมีรายงานที่เพิ่มขึ้นในขณะที่ผู้ใช้งานต้องรอรายงานการซ่อมแซมจุดอ่อนจากผู้ผลิต ดังนั้นจึงมีการเสนอโครงร่างการป้องกันซึ่งปรับตัวได้ (ADP: Adaptive Defense Framework) ซึ่งเป็นมิดเดิลแวร์ (Middleware) ที่ทำงานอยู่ระหว่างแอพพลิเคชัน และระบบปฏิบัติการ ดังแสดงในรูปที่ 2.5



รูปที่ 2.5 โครงร่างการป้องกันซึ่งปรับตัวได้

โดยที่โครงร่างนี้แบ่งเป็น 2 ส่วนคือ ส่วนของการวิเคราะห์และประเมินระบบ (SAA: System Assessment Analysis) และส่วนของสภาวะการป้องกันซึ่งปรับตัวได้ (ADP: Adaptive Defense Posture) ซึ่งส่วนแรกวิเคราะห์หาจุดอ่อนที่มีในระบบโดยอ้างอิงฐานข้อมูลจุดอ่อน เมื่อ

ทราบถึงข้อมูลจุดอ่อนที่มีในระบบแล้ว ส่วนที่สองจะทำการหาวิธีที่เหมาะสมในการป้องกันระบบตามระดับความเสี่ยงที่จะเกิดความเสียหายต่อไป

ส่วนในเรื่องของการป้องกันระบบนั้น แอนเดอร์สัน รอสส์ [16] ได้เสนอแบบแผนการป้องกันเชิงลึก (defense-in-depth) ซึ่งแบ่งกลุ่มของเทคโนโลยีการรักษาความมั่นคงออกเป็น 3 กลุ่ม คือ การป้องกัน (Protection) การตรวจสอบ (Detection) และการกู้คืน (Recovery) ซึ่งแบบแผนการป้องกันเชิงลึกนี้ ซอน บัทเลอร์ [17] ได้ทำการจัดกลุ่มของเทคโนโลยีแต่ละประเภทไว้

จากงานวิจัยนี้ทำให้ทราบถึงเทคโนโลยีต่างๆ ของการป้องกันระบบคอมพิวเตอร์ ซึ่งในส่วนสำคัญส่วนหนึ่งคือส่วนของการตรวจจับ เนื่องจากการป้องกันระบบเพียงอย่างเดียวไม่อาจจะรักษาความมั่นคงได้ หากมีผู้ไม่หวังดีสามารถบุกรุกเข้ามาในระบบเพราะการป้องกันไม่สามารถตรวจจับการบุกรุกได้

มาร์ติน โรอีช [18] จึงได้เสนอ สนอร์ท ซึ่งเป็นระบบตรวจจับการบุกรุกทางเครือข่าย ซึ่งสามารถทำงานในได้ในหลายรูปแบบ นอกจากนั้น สนอร์ทยังมีรูปแบบการตรวจจับการบุกรุกโดยการอ้างอิงจากกฎ ซึ่งกฎนี้อ้างอิงถึงรายการจุดอ่อนจากที่ต่างๆ โดยเฉพาะซีวีอี แม้ว่าสนอร์ทจะสามารถตรวจจับการบุกรุกผ่านจุดอ่อนที่ยังไม่ได้มีการแก้ไขได้ แต่ยังมีจุดอ่อนบางอย่างที่สนอร์ทไม่สามารถที่จะป้องกันได้อาจจะเนื่องมาจากเป็นจุดอ่อนที่ไม่สามารถทำการปิดได้ เนื่องจากเป็นส่วนที่ต้องเปิดให้ใช้งาน เช่นในระบบปฏิบัติการยูนิกซ์ จะมีบริการส่งจดหมาย (Send mail) ตามรายงานของสถาบันแซนส์ถือว่าเป็นจุดอ่อนที่อันตรายเพราะจะเป็นช่องทางให้ผู้โจมตีเข้ามาได้ แต่ก็จำเป็นต้องเปิดให้ใช้งาน เป็นต้น

2.2 งานวิจัยที่เกี่ยวข้องกับการแบ่งประเภทของจุดอ่อน

การแบ่งประเภทของจุดอ่อน เป็นการจัดกลุ่มของจุดอ่อนที่มีลักษณะคล้ายคลึงกัน หรือมีความสัมพันธ์เอาไว้ด้วยกัน ซึ่งในปี ค.ศ.1994 แลนเวอร์ และคณะ [19] เสนอว่าลักษณะของข้อผิดพลาดแบ่งได้เป็น ลักษณะการทำงาน ลักษณะการเกิด ตำแหน่งที่เกิด และลักษณะของความเสียหาย

จนเมื่อปี ค.ศ. 2005 วิตา และคณะ [20] ได้ทำการปรับปรุงลักษณะการจัดกลุ่มของแลนเวอร์ โดยแบ่งตามประเภทของการโจมตีระบบ (Genesis) จุดที่เกิดจุดอ่อน (Location) และลักษณะความเสียหาย (Security Violation)

นอกจากนั้น วิตาและคณะยังเสนอการให้คะแนนของจุดอ่อน เพื่อคิดค่าความเปราะบางของระบบ ซึ่งมีแนวคิดการให้คะแนนโดยดูจากระดับความรุนแรงที่เกิดขึ้นต่อระบบของจุดอ่อนแต่ละตัว และนำคะแนนของจุดอ่อนแต่ละตัวมารวมกันตามประเภทที่ได้มีการแบ่งกลุ่มไว้แล้ว เพื่อคิดค่าความเปราะบางของจุดอ่อนแต่ละประเภท

ในปี ค.ศ.2006 ได้มีงานวิจัยในเรื่องของระบบการให้คะแนนจุดอ่อนในรูปแบบของระดับความรุนแรงที่ระบบได้รับผลกระทบจากการโจมตีผ่านช่องโหว่นั้น โดยจะมีวิธีการให้คะแนนออกเป็น 3 กลุ่ม คือ แหล่งกำเนิดพื้นฐาน (Base Metric) แหล่งกำเนิดชั่วคราว (Temporal Metric) และกลุ่มของแหล่งกำเนิดสิ่งแวดล้อม (Environmental Metric) ซึ่งมีการกำหนดปัจจัยและวิธีการคำนวณค่าออกมาเป็นสูตรสำเร็จในแต่ละกลุ่มและนำคะแนนของแต่ละกลุ่มมารวมกันเป็นคะแนนของจุดอ่อน

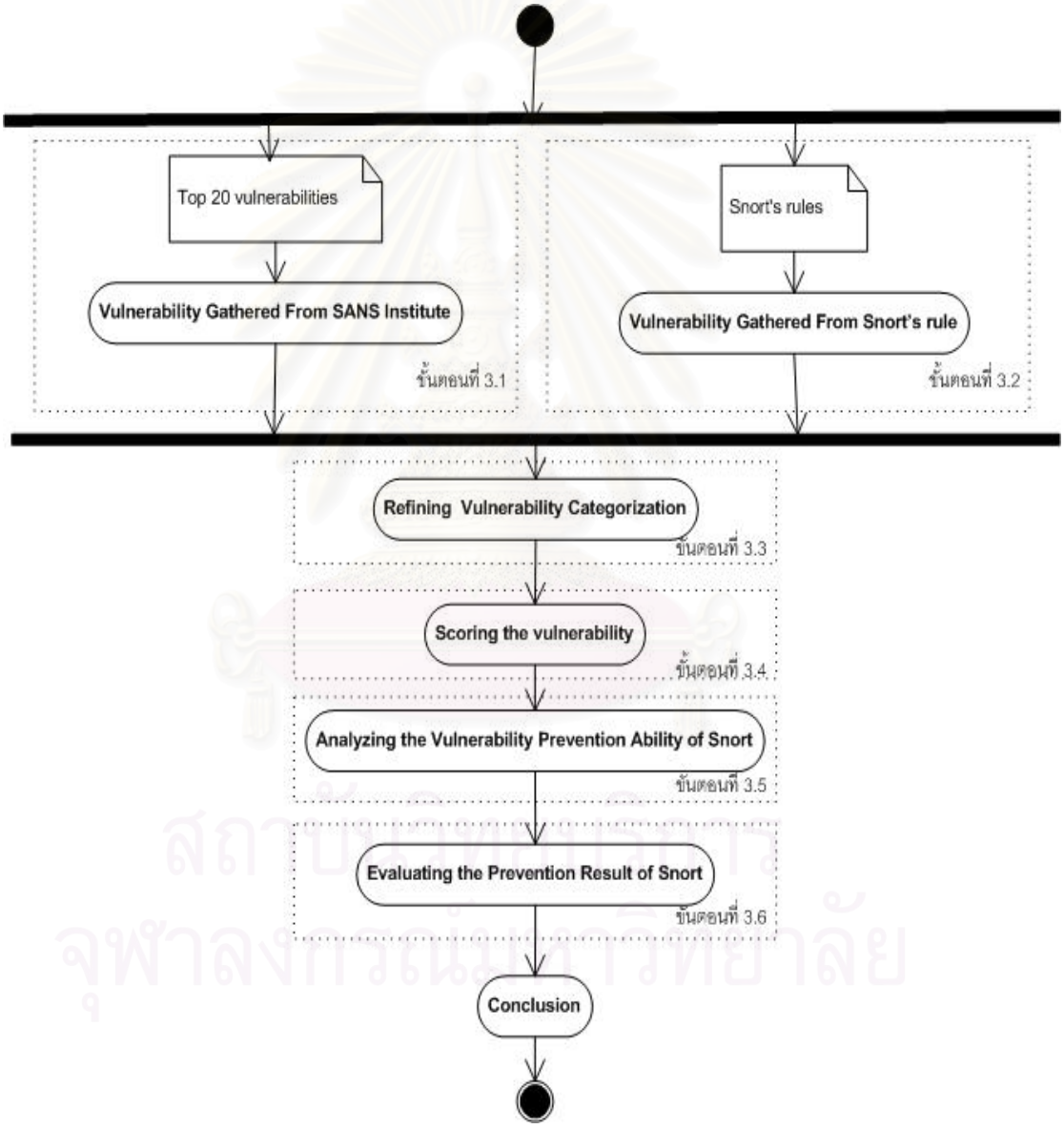
จากงานวิจัยเรื่องการเพิ่มการรักษาความมั่นคงให้กับระบบและงานวิจัยเรื่องการแบ่งประเภทของจุดอ่อน ทำให้เกิดแนวความคิดที่จะศึกษาถึงการทำงานของระบบไอดีเอส เพื่อวิเคราะห์ถึงประสิทธิภาพในการป้องกันระบบ และประสิทธิภาพในการเสริมความมั่นคงให้กับระบบ ภายใต้สภาวะที่ระบบมีจุดอ่อนมากมาย โดยมีการใช้สนอร์ทเป็นกรณีศึกษาเนื่องจากสนอร์ทมีการอ้างอิงไปที่รายการของซีวีอี

ในบทนี้ได้กล่าวถึง องค์ประกอบของความมั่นคง จุดอ่อนของระบบคอมพิวเตอร์ ฐานข้อมูลที่เกี่ยวข้อง ระบบตรวจจับการบุกรุก และ สนอร์ท ส่วนในงานวิจัยที่เกี่ยวข้อง ได้แบ่งเป็นสองหัวข้อ คือ งานวิจัยที่เกี่ยวข้องกับการเพิ่มความมั่นคงให้ระบบ และงานวิจัยที่เกี่ยวข้องกับการแบ่งประเภทของจุดอ่อน ส่วนในบทต่อไปจะกล่าวถึงขั้นตอนและวิธีการดำเนินงานวิจัย

บทที่ 3

วิธีดำเนินงานวิจัย

แนวคิดและวิธีการวิจัยของการวิเคราะห์ถึงประสิทธิภาพในการลดคะแนนของจุดอ่อนของระบบคอมพิวเตอร์ สามารถแจกแจงออกได้เป็น 6 หัวข้อ ซึ่งเขียนเป็นแผนภาพการทำงาน ดังแสดงในรูปที่ 3.1



รูปที่ 3.1 ขั้นตอนการวิจัย

โดยในแต่ละขั้นตอนมีการสร้างโปรแกรมขึ้นเพื่อช่วยอำนวยความสะดวกในการประเมินผล ซึ่งในแต่ละขั้นตอนมีรายละเอียดดังต่อไปนี้

3.1 การคัดกรองข้อมูลจุดอ่อนที่เป็นภัยต่อระบบตามรายงานของสถาบันแซนส์

จากข้อมูลรายการจุดอ่อนที่ค้นพบและมีการรวบรวมไว้ในรายงานของสถาบันแซนส์ ซึ่งเป็นข้อมูลจุดอ่อนของระบบเครือข่าย ประกอบไปด้วยข้อมูลจุดอ่อนของระบบปฏิบัติการของทั้งระบบปฏิบัติการวินโดวส์ และระบบปฏิบัติการตระกูลยูนิกซ์ รวมทั้งโปรแกรมประยุกต์ต่างๆ ที่ถูกติดตั้งลงบนระบบปฏิบัติการทั้งสองประเภท

ในงานวิจัยนี้ ได้ทำการคัดกรองข้อมูลของจุดอ่อนของระบบเครือข่ายเฉพาะที่มีในรายงานจุดอ่อนที่เป็นภัยร้ายแรงของสถาบันแซนส์ (Top 20 Vulnerabilities) ตั้งแต่ปี ค.ศ.2000 – ค.ศ.2007 โดยที่จุดอ่อนเหล่านี้มีการอ้างอิงไปถึงรายการจุดอ่อนของซีวีอี ซึ่งจุดอ่อนที่คัดกรองมานี้ประกอบไปด้วยจุดอ่อนทั้งหมด 649 ตัว แยกเป็นจุดอ่อนที่เกิดขึ้นบนระบบปฏิบัติการตระกูลวินโดวส์จำนวน 377 ตัว ดังแสดงไว้ในรูปที่ 3.2 และบนระบบปฏิบัติการตระกูลยูนิกซ์จำนวน 272 ตัว ดังแสดงไว้ในรูปที่ 3.3 ซึ่งจุดอ่อนที่ทำการคัดกรองมานั้น เป็นจุดอ่อนที่เกิดขึ้นโดยตรงกับระบบปฏิบัติการเอง และจากโปรแกรมประยุกต์ที่ถูกติดตั้งลงบนระบบปฏิบัติการนั้นๆ

W3. Microsoft Office

W3.1 Description:

Microsoft Office is the most widely used email and productivity suite worldwide. The applications include Outlook, Word, PowerPoint, Excel, Visio, FrontPage and Access.

W3.2 Operating Systems Affected:

Windows 9x, Windows 2000, Windows XP, Windows 2003 are all vulnerable depending on the version of Office software installed.

W3.3 CVE Entries:

CVE-2006-5296, CVE-2006-4694, CVE-2006-4534, CVE-2006-3649, CVE-2006-3590, CVE-2006-3059, CVE-2006-2492, CVE-2006-1540, CVE-2006-1301, CVE-2006-0002

รูปที่ 3.2 ตัวอย่างรายการซีวีอีที่มีการอ้างถึงในรายงานจุดอ่อนที่เป็นภัยกับระบบวินโดวส์

U2 - Sendmail Vulnerabilities

U2.1 Description:

Sendmail is the program that sends, receives, and forwards most electronic mail processed on UNIX and Linux computers. Sendmail's widespread use on the Internet makes it a prime target of attackers. Several flaws have been found over the years. In fact, the very first advisory issued by CERT/CC, in 1988, made reference to an exploitable weakness in Sendmail. In one of the most common exploits, the attacker sends a crafted mail message to the machine running Sendmail, and Sendmail reads the message as instructions requiring the victim machine to send its password file to the attacker's machine (or to another victim) where the passwords can be cracked.

U2.2 Systems impacted:

Most versions of Unix and Linux

U2.3 CVE entries:

CVE-1999-0047, CVE-1999-0130, CVE-1999-0131, CVE-1999-0203, CVE-1999-0204, CVE-1999-0206

รูปที่ 3.3 ตัวอย่างรายการซีวีอีที่มีการอ้างถึงในรายงานจุดอ่อนที่เป็นภัยกับระบบยูนิกซ์

3.2 การคัดกรองข้อมูลจุดอ่อนของรายการซีวีอีที่สนอร์ทมีการอ้างถึง

ในข้อมูลกฎของสนอร์ท จะมีการอ้างอิงว่ากฎนี้ใช้ในการป้องกันจุดอ่อนใดของรายการซีวีอี โดยจะอยู่ในส่วนของออปชัน ดังแสดงในรูปที่ 3.4

```
alert  tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ATTACK-
RESPONSES file copied ok"; flow: established; content:"1 file|28|s|29| copied"; nocase;
reference:bugtraq,1806; reference:cve,2000-0884; classtype:bad-unknown; sid:497; rev:12;)
```

รูปที่ 3.4 ตัวอย่างกฎของสนอร์ทที่มีการอ้างถึงรายการซีวีอี

ในงานวิจัยนี้จะทำการคัดกรองกฎของสนอร์ท โดยใช้เวอร์ชันประกาศ ณ วันที่ 13 มกราคม พ.ศ. 2552 ซึ่งประกอบไปด้วยกฎทั้งหมด 54 กลุ่ม เช่น ftp, icmp, pop3, telnet, web-attacks, web อนึ่ง ในขั้นตอนนี้มีการใช้โปรแกรมเพื่อทำการคัดกรองรายการซีวีอีที่สนอร์ทมีการอ้างอิงถึง จากทุกกฎของสนอร์ท

3.3 การปรับแต่งรูปแบบการจัดกลุ่มจุดอ่อน

ในขั้นตอนนี้จะทำการจัดกลุ่มของจุดอ่อนโดยได้ทำการศึกษาจากทฤษฎีที่เกี่ยวข้องในบทที่ 2 ไปแล้ว และในงานวิจัยนี้ ได้มีการปรับแต่งลักษณะการจัดกลุ่มของจุดอ่อนเพื่อให้เหมาะสมกับการวิเคราะห์ และประเภทของจุดอ่อนบนระบบเครือข่าย นอกจากนั้นยังมีการกำหนดคะแนนความรุนแรงให้กับจุดอ่อนแต่ละตัวโดยมีการคำนึงถึงความรุนแรงและลักษณะของความเสียหายที่เกิดแก่ระบบ ตามที่ได้ศึกษาจากงานวิจัยที่เกี่ยวข้องในบทที่ 2

การจัดกลุ่มของจุดอ่อนของงานวิจัยนี้ จะทำการแบ่งออกเป็น 4 รูปแบบคือ

1. ประเภทของจุดอ่อน
2. จุดที่เกิดจุดอ่อน
3. ลักษณะความเสียหาย
4. ระดับความรุนแรง

โดยในแต่ละประเภทมีรายละเอียด ดังต่อไปนี้

3.3.1 ประเภทของจุดอ่อน

แบ่งกลุ่มตามลักษณะการโจมตีระบบได้เป็น 7 ประเภท ดังนี้

1. ความผิดพลาดของการตรวจสอบข้อมูลนำเข้า (Input Validation Error)
2. ความผิดพลาดของขอบเขตข้อมูล (Boundary Condition Error)
3. ความผิดพลาดในการตรวจสอบการเข้าถึง (Access Validation Error)
4. ความผิดพลาดของการปรับแต่งระบบ (Configuration Error)

5. ความผิดพลาดจากการออกแบบระบบ (Design Error)

6. ความผิดพลาดจากชุดคำสั่งจัดการสิ่งผิดปกติ (Exceptional Condition Handling Error)

7. อื่นๆ (Other)

3.3.2 จุดที่เกิดจุดอ่อน

แบ่งกลุ่มตามตำแหน่งที่เกิดจุดอ่อนได้เป็น 5 ประเภท ดังนี้

1. ส่วนการเริ่มต้นระบบ (System Initialization)

2. ส่วนการจัดการแฟ้มข้อมูล (File Management)

3. ส่วนการพิสูจน์ตัวจริง (Authentication)

4. ส่วนโปรแกรมที่สนับสนุน (Support)

5. ส่วนโปรแกรมประยุกต์ (Application)

3.3.3 ลักษณะความเสียหาย

แบ่งได้ 4 ประเภทตามพื้นฐานการรักษาความมั่นคงทั่วๆไปซึ่งประกอบด้วย การรักษาความลับ การรักษาบูรณภาพ และการรักษาสภาพพร้อมใช้งาน และนอกจากนี้ งานวิจัยนี้ได้เพิ่มความเสียหายในกรณีที่ระบบถูกล่วงละเมิด ซึ่งเป็นความเสียหายที่จะนำไปสู่ความเสียหายอื่นๆ

3.3.4 ระดับความรุนแรง

เนื่องจากจุดอ่อนแต่ละตัวจะมีความสามารถในการทำให้ระบบเกิดความเสียหายไม่เท่ากัน จึงได้กำหนดระดับความรุนแรงไว้ 3 ระดับ คือ สูง กลาง และต่ำ ซึ่งในการกำหนดระดับความรุนแรงนี้ นำมาจากระดับความรุนแรงของจุดอ่อนที่มีการระบุไว้ในรายการซีวีอี

3.4 การให้คะแนนจุดอ่อน

จะมีการให้คะแนนสำหรับจุดอ่อนตามรายการของซีวีอี และการจัดประเภทของจุดอ่อน ซึ่งจุดอ่อนแต่ละตัวจะมีการให้คะแนนจากระดับความเสียหายโดยอ้างอิงวิธีการคิดคะแนนจาก

งานวิจัย “Vulnerability Profile for Linux” และ “CVSS” โดยมีวิธีการคำนวณ คือ ให้คะแนนของจุดอ่อนโดยรวมเป็นดัชนีความเปราะบางของระบบ ซึ่งหากว่าดัชนีความเปราะบางมีค่าสูง ระบบจะมีความเสี่ยงต่อความเสียหายมากกว่าดัชนีความเปราะบางที่มีค่าน้อย

เนื่องจากมีความแตกต่างของปริมาณความเสียหายและระดับความรุนแรงของจุดอ่อนแต่ละตัว ในการวิเคราะห์ความสามารถในการป้องกันจุดอ่อนนี้ จึงได้กำหนดระดับคะแนนที่แตกต่างกันขึ้นตามระดับความเสียหายและความรุนแรง

คะแนนของจุดอ่อนแต่ละตัว คิดจากประเภทของความเสียหายที่เกิดขึ้น โดยประกอบไปด้วยความเสียหายที่เกิดจากการโจมตีจุดอ่อนโดยตรง และการที่ระบบถูกล่วงละเมิดเนื่องจากจุดอ่อนแต่ละตัว สามารถทำให้เกิดความเสียหายมากกว่า 1 แบบ ดังนั้นในการคิดคะแนนความเสียหายของจุดอ่อนนั้น จึงได้มีการกำหนดให้ในแต่ละประเภทของความเสียหาย ซึ่งประกอบด้วย การเสียความเป็นความลับ การเสียสภาพบูรณภาพ การเสียสภาพพร้อมใช้งาน และการที่ระบบถูกล่วงละเมิด มีการคิดคะแนนอย่างละ 1 คะแนน

แต่จุดอ่อนแต่ละตัว ก็มีระดับความรุนแรงที่ต่างกัน ทำให้มีการกำหนดคะแนนที่ต่างกันในแต่ละระดับ โดยที่ความรุนแรงระดับปานกลางจะมีค่าเป็น 2 คะแนน และระดับสูงมีค่าเป็น 3 คะแนน ซึ่งการให้คะแนนจุดอ่อนสามารถแสดงได้ดังตารางที่ 3.1

ตารางที่ 3.1 การให้คะแนนจุดอ่อน

ระดับความรุนแรง / ลักษณะความ เสียหาย	ไม่ก่อให้เกิดความเสียหาย	ระดับต่ำ	ระดับกลาง	ระดับสูง
Confidentiality	0	1	2	3
Integrity	0	1	2	3
Availability	0	1	2	3
System Compromised	0	1	2	3

เมื่อให้คะแนนจุดอ่อนในแต่ละลักษณะแล้ว จะมีการนำคะแนนที่ได้มารวมกัน เพื่อเป็นคะแนนของจุดอ่อนแต่ละตัว โดยใช้สมการดังนี้

$$S_i = S_{C_i} + S_{I_i} + S_{A_i} + S_{S_i}$$

ซึ่งแต่ละตัวแปรมีความหมายดังนี้

i	หมายถึง	รายการซีวีอี
S_i	หมายถึง	คะแนนรวมทั้งหมดของจุดอ่อนแต่ละตัว
S_{C_i}	หมายถึง	คะแนนความเสียหายที่เกิดจากการเสียความเป็นความลับ
S_{I_i}	หมายถึง	คะแนนความเสียหายที่เกิดจากการเสียความบูรณภาพ
S_{A_i}	หมายถึง	คะแนนความเสียหายที่เกิดจากการเสียความพร้อมใช้งาน
S_{S_i}	หมายถึง	คะแนนความเสียหายที่เกิดจากการที่ระบบถูกล่วงละเมิด

3.5 การวิเคราะห์ความสามารถในการป้องกันจุดอ่อนของสนอร์ท

การวิเคราะห์ความสามารถในการป้องกันจุดอ่อนของสนอร์ทนี้ จะทำการวิเคราะห์ว่าในกฎของสนอร์ทที่ติดตั้งลงไปนั้น มีการอ้างอิงไปถึงรายการซีวีอีที่อยู่ในรายการจุดอ่อนของสถาบันแซนส์หรือไม่ หากมีการอ้างอิงไปถึง ก็หมายความว่าหากติดตั้งสนอร์ทที่มีกฎเช่นนี้ จะสามารถป้องกันจุดอ่อนนั้นๆ ได้ ซึ่งมีขั้นตอนวิเคราะห์แบ่งออกเป็นสองส่วน คือ การรวบรวมคะแนนของแต่ละกลุ่มจุดอ่อน และการเปรียบเทียบคะแนนจุดอ่อนจากสถาบันแซนส์กับกฎของสนอร์ท โดยในแต่ละขั้นตอนมีรายละเอียด ดังนี้

3.5.1 การรวบรวมคะแนนของแต่ละกลุ่มจุดอ่อน

เมื่อได้คะแนนจุดอ่อนแต่ละตัว จากขั้นตอนที่ 3.4 แล้ว ในขั้นตอนนี้ จะนำจุดอ่อนแต่ละตัวมารวมกันตามกลุ่มที่ได้แยกประเภทไว้ในขั้นตอนที่ 3.3 โดยมีการใช้สมการดังนี้

$$\sum_{i=1}^{n} S_i$$

ในขั้นตอนนี้จะได้ผลลัพธ์เป็นระดับคะแนนของจุดอ่อนแต่ละประเภทของสถาบันแซนส์ ซึ่งหลังจากนี้จะนำมาเปรียบเทียบกับกฎของสนอร์ทต่อไป

3.5.2 การเปรียบเทียบคะแนนจุดอ่อนจากสถาบันแซนส์กับกฎของสนอร์ท

ในขั้นตอนนี้ จะมีการนำรายการซีวีอีที่ได้จากการคัดกรองจากกฎของสนอร์ทในขั้นตอนที่ 3.2 มาเปรียบเทียบกับรายการซีวีอีที่ได้คัดกรองจากสถาบันแซนส์ในขั้นตอนที่ 3.1 เพื่อทำการตรวจสอบดูว่ามีรายการซีวีอีใดบ้างที่สนอร์ทมีการอ้างอิงถึง ในขั้นตอนนี้จะได้ระดับคะแนนจุดอ่อน

ที่สนอร์ทสามารถป้องกันได้ ผลลัพธ์จากขั้นตอนนี้จะนำมาใช้ในการประเมินผลความสามารถในการป้องกันจุดอ่อนของสนอร์ทในขั้นตอนต่อไป

3.6 การประเมินผลความสามารถในการป้องกันจุดอ่อนของสนอร์ท

การประเมินผลโดยวิเคราะห์จากความสามารถในการลดระดับคะแนนของจุดอ่อนแต่ละประเภทที่ได้มีการจำแนกไว้แล้วในกระบวนการจัดกลุ่มจุดอ่อน ซึ่งหากว่าระดับคะแนนที่ได้มีค่าสูง หมายความว่า สนอร์ท สามารถป้องกันจุดอ่อนประเภทนั้นได้มาก ทำให้ลดโอกาสจากการถูกโจมตีในส่วนนั้นได้มาก และขณะเดียวกัน หากระดับคะแนนที่ได้มีค่าต่ำ หมายความว่าสนอร์ท มีความสามารถในการป้องกันจุดอ่อนประเภทนั้นได้น้อย ทำให้ลดโอกาสเสี่ยงที่ระบบจะถูกโจมตีตรงส่วนนั้นได้น้อย

อนึ่ง การประเมินความสามารถในการป้องกันจุดอ่อนของระบบตรวจจับการบุกรุกโดยใช้สนอร์ทเป็นกรณีศึกษาในงานวิจัยนี้ ได้ทำการพิจารณาจุดอ่อนที่ถูกระบุในรายการจุดอ่อนของสถาบันแซนส์ ตั้งแต่ปี ค.ศ. 2000 – ค.ศ. 2007 เท่านั้น ไม่ได้มีการประเมินถึงจุดอ่อนในรายการซีวีอีทั้งหมด และไม่ได้รวมถึงการทดสอบการทำงานจริงของระบบตรวจจับการบุกรุก ผลที่ได้จากการวิจัยนี้ จึงเป็นเพียงแนวทางและแนวโน้มในการป้องกันจุดอ่อนของระบบตรวจจับการบุกรุกแบบหนึ่งเท่านั้น

จากการรวบรวมข้อมูลจุดอ่อน การจัดกลุ่มจุดอ่อนเพื่อให้เหมาะสม และให้คะแนนจุดอ่อนแต่ละตัวแล้ว ในบทต่อไป จะเป็นการออกแบบและพัฒนาเครื่องมือช่วยในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก

บทที่ 4

การออกแบบและพัฒนาเครื่องมือช่วยในการประเมินประสิทธิภาพของไอดีเอส

ในบทนี้จะกล่าวถึงวิธีการออกแบบและการพัฒนาเครื่องมือช่วยในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก ซึ่งจะแบ่งได้เป็น 2 ส่วนคือ ส่วนการออกแบบและส่วนการพัฒนา

4.1 การออกแบบเครื่องมือ

ในส่วนนี้จะกล่าวถึงความต้องการโดยรวมของระบบ ฟังก์ชันการทำงานของเครื่องมือช่วยในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก และฐานข้อมูลที่ใช้

4.1.1 ความต้องการโดยรวมของระบบ

เครื่องมือช่วยประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก เป็นเครื่องมือที่ช่วยในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก โดยวัดจากความสามารถในการป้องกันจุดอ่อนที่เป็นภัยร้ายแรงต่อเครือข่ายคอมพิวเตอร์ ซึ่งถูกประกาศออกมาโดยสถาบันแซนส์ ความสามารถของระบบได้แก่ การรวบรวมข้อมูลรายการจุดอ่อน การค้นหารายการจุดอ่อนตามหมายเลขซีวีอี การบันทึกลักษณะของจุดอ่อนแต่ละตัว และการประเมินผล

จากผลการวิเคราะห์ สามารถสรุปเพื่อสร้างแผนภาพยูสเคส ได้ดังนี้

1. แอคเตอร์ (Actor) ได้แก่ ผู้ใช้

2. ยูสเคส (Use case) ได้แก่ การรวบรวมข้อมูลรายการจุดอ่อน การค้นหารายการจุดอ่อนตามหมายเลขซีวีอี การบันทึกลักษณะจุดอ่อน และการประเมินผล

งานวิจัยนี้จะเป็นการประเมินผลความสามารถของระบบตรวจจับการบุกรุก โดยตรวจสอบจากกฎของที่มีการอ้างอิงไปถึงรายการจุดอ่อนซีวีอี เปรียบเทียบกับจุดอ่อนที่ถูกประกาศออกมาโดยสถาบันแซนส์ ทำให้ได้แผนภาพยูสเคส ดังแสดงในแผนภาพที่ 4.1 และคำอธิบายยูสเคสอยู่ในตารางที่ 4.1

รูปที่ 4.1 ยูสเคสของเครื่องมือช่วยประเมินประสิทธิภาพของระบบไอดีเอส

ตารางที่ 4.1 อธิบายความหมายของแต่ละยูสเคส

ยูสเคส	คำอธิบาย
1. การรวบรวมข้อมูล	กระทำโดยผู้ใช้ เพื่อทำการรวบรวมข้อมูลจุดอ่อนจากรายงานของสถาบันแซนส์ และจากกฎระบบตรวจจับการบุกรุก ซึ่งในงานวิจัยนี้จะใช้สนอร์ท
2. การค้นหารายการจุดอ่อนตามหมายเลขซีวีอี	กระทำโดยผู้ใช้ เพื่อทำการค้นหารายการจุดอ่อนตามหมายเลขซีวีอี หรือตามปีที่ประกาศ ผลลัพธ์ที่ได้จะเป็นรายการซีวีอีตามเงื่อนไขที่ผู้ใช้เลือก
3. การบันทึกลักษณะจุดอ่อน	กระทำโดยผู้ใช้ เพื่อทำการแสดงลักษณะเฉพาะของจุดอ่อนที่ผู้ใช้เลือก และสามารถบันทึกข้อมูลลักษณะลงไปในฐานข้อมูลได้

4. การประเมินผล	กระทำโดยผู้ใช้ เพื่อทำการประเมินผลประสิทธิภาพของระบบตรวจจับการบุกรุก โดยผลลัพธ์ที่ได้จะออกมาในรูปแบบกราฟแท่ง และผู้ใช้สามารถเลือกตามให้แสดงผลลัพธ์ตามเงื่อนไขที่ต้องการได้

4.1.2 ฟังก์ชันการทำงานของเครื่องมือช่วยในการประเมินประสิทธิภาพของระบบไอดีเอส

จากภาพรวมของระบบ นำมาสู่การออกแบบฟังก์ชันการทำงานของเครื่องมือ โดยจะมีการอธิบายในแต่ละฟังก์ชันการทำงานดังนี้

4.1.2.1 การรวบรวมข้อมูลจุดอ่อน

ในมอดูลนี้ มีวัตถุประสงค์เพื่อทำการจัดการรวบรวมข้อมูล โดยมีการรวบรวมข้อมูลจาก 2 ส่วน คือ ส่วนการรวบรวมข้อมูลจุดอ่อนจากสถาบันแซนส์ ส่วนการรวบรวมข้อมูลจุดอ่อนจากกฎของสนอร์ท ซึ่งแต่ละส่วนมีรายละเอียดดังนี้

4.1.2.1.1 ส่วนการรวบรวมข้อมูลจุดอ่อนจากสถาบันแซนส์

ส่วนนี้มีการมีวัตถุประสงค์เพื่อทำการรวบรวมข้อมูลจากสถาบันแซนส์ โดยมีขั้นตอนการทำงานดังนี้

4.1.2.1.1.1 ทำการคัดกรองข้อมูลรายการจุดอ่อนในแต่ละปี

ในขั้นตอนนี้ ได้ทำการคัดกรองข้อมูลจุดอ่อนที่อยู่ในรายการจุดอ่อนในแต่ละปี เพื่อให้ได้รายการจุดอ่อนทั้งหมดให้อยู่ในรูปแบบไฟล์ Text เพื่อจะใช้นำเข้าสู่ฐานข้อมูลต่อไป อนึ่ง การคัดกรองจุดอ่อนนี้ มีการทำด้วยมือ อาจจะมีข้อผิดพลาดอยู่บ้าง

4.1.2.1.1.2 ทำการนำเข้าข้อมูลจุดอ่อน

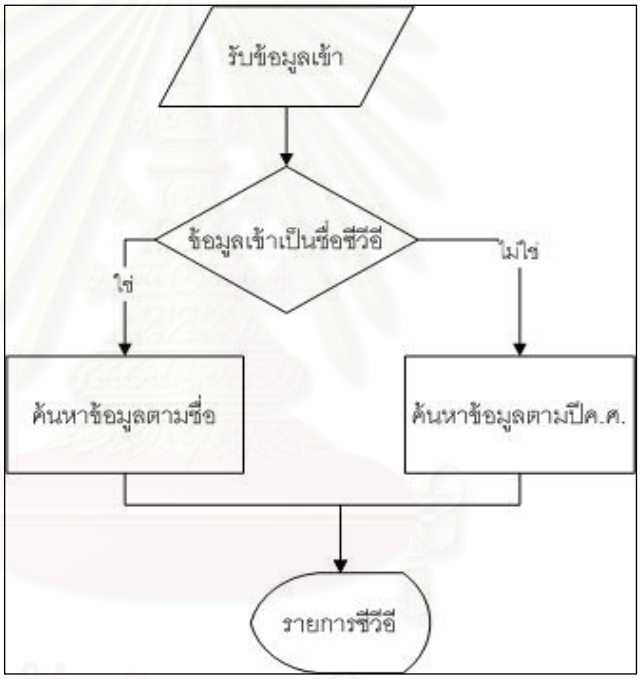
เมื่อได้รายการจุดอ่อนทั้งหมดในรูปแบบ ไฟล์ Text แล้ว จะมีการเรียกมอดูลที่ใช้ในการนำเข้าข้อมูลเพื่อทำการบันทึกลงฐานข้อมูล จากขั้นตอนนี้จะได้รายการข้อมูลจุดอ่อนทั้งหมดที่ถูกประกาศโดยสถาบันแซนส์ อยู่ในฐานข้อมูลพร้อมสำหรับการจัดทำโปรไฟล์จุดอ่อนในขั้นตอนถัดไป

4.1.2.1.2 ส่วนการรวบรวมข้อมูลจุดอ่อนจากกฎของสนอร์ท

ในส่วนนี้มีวัตถุประสงค์เพื่อทำการรวบรวมข้อมูลจากกฎของสนอร์ท เพื่อทำการตรวจสอบดูว่า จุดอ่อนที่อยู่ในกฎของสนอร์ทนั้น รองรับจุดอ่อนที่ถูกประกาศโดยสถาบันแซนส์หรือไม่

4.1.2.2 การค้นหาข้อมูลในรายการซีวีอี

ในมอดูลนี้มีวัตถุประสงค์เพื่อทำการค้นหารายการซีวีอีทั้งหมด ซึ่งมีการทำงานดังแผนภาพการทำงาน ดังรูปที่ 4.2



รูปที่ 4.2 แผนภาพการทำงาน

จากแผนภาพ มีรายละเอียดการทำงานดังนี้ ผู้ใช้ใส่ข้อมูลนำเข้าได้สองรูปแบบ คือ ใส่หมายเลขรายการซีวีอีแบบเต็มรูปแบบ เช่น "CVE-1999-0002" หรือเลือกตามปี ค.ศ.ที่ออกรายการจุดอ่อนนั้นๆ อนึ่ง ในงานวิจัยนี้ จะใช้เฉพาะรายการจุดอ่อน ตั้งแต่ปี 1999-2007 โดยไฟล์ที่ใช้แสดงรายละเอียด นำมาจาก เอ็นวีดี เป็นรูปแบบ XML เมื่อเลือกแล้ว เครื่องมือนี้จะแสดงรายการจุดอ่อนตามที่เงื่อนไขที่ผู้ใช้เลือกลงบน list view โดยแสดงข้อมูลชื่อ และรายละเอียดของรายการจุดอ่อนนั้นๆ โดยที่ผู้ใช้สามารถเลือกจุดอ่อนแต่ละตัวเพื่อดูรายละเอียดอื่นๆ หรือ ทำการบันทึกค่าโปรไฟล์ของจุดอ่อนนั้นๆ

4.1.2.3 การจัดทำโปรไฟล์ของจุดอ่อนแต่ล ะตัว

มอดูลนี้มีวัตถุประสงค์ เพื่อแสดงรายละเอียดของรายการซีวีอีที่เลือกมาจากข้อ 4.2 และหากรายการซีวีอีนี้ มีอยู่ในประกาศของสถาบันแซนส์ จะสามารถจัดทำโปรไฟล์ของจุดอ่อน คือการจัดกลุ่มและการให้คะแนนจุดอ่อน เพื่อนำมาใช้ประเมินผลในขั้นตอนถัดไป ซึ่งมีรายละเอียดการทำงานดังนี้

4.1.2.3 .1 การแสดงรายละเอียดจุดอ่อน

ในส่วนนี้ จะมีการแสดงข้อมูลจุดอ่อนของรายการซีวีอี ตามที่ได้เลือกมาจากขั้นตอนที่ 4.2 โดยจะแสดงข้อมูลในส่วนของ ชื่อ รายละเอียด รุ่นของโปรแกรมที่เกิดจุดอ่อนนี้ ซึ่งรายละเอียดในส่วนนี้จะมีการอ่านมาจากรายงานของ NVD ที่รวบรวมจุดอ่อนตามซีวีอี ซึ่งข้อมูลในส่วนนี้ผู้ใช้จะไม่สามารถทำการแก้ไขได้

4.1.2.3 .2 การแสดงข้อมูลโปรไฟล์ของจุดอ่อน

ในส่วนนี้ จะเปิดให้ผู้ใช้สามารถทำการแก้ไขได้ เพราะจะเป็นส่วนของการจัดทำโปรไฟล์ของจุดอ่อนตามงานวิจัยนี้ คือจะมีการจัดกลุ่มและให้คะแนนจุดอ่อนแต่ละตัว ซึ่งในส่วนนี้ หากว่ารายการจุดอ่อนที่เลือกมาจากข้อ 4.2 มีอยู่ในประกาศจากสถาบันแซนส์ ส่วนนี้จะ เปิดให้ผู้ใช้งานทำการแก้ไขและบันทึกข้อมูลได้ แต่หากไม่มีในประกาศ ส่วนนี้จะทำการปิดไว้ เพื่อไม่ให้ผู้ใช้ทำการบันทึกรายการซีวีอีนอกเหนือจากที่ประกาศลงไป ป้องกันความผิดพลาดในการเพิ่มหมายเลขซีวีอีลงไปเอง

4.1.2.3 .3 การบันทึกลงฐานข้อมูล

ในส่วนนี้จะทำการบันทึกข้อมูลรายการซีวีอีที่ถูกแก้ไขลงไปในฐานข้อมูล

4.1.2.4 การประเมินผล

ในมอดูลนี้ มีวัตถุประสงค์เพื่อทำการ ประเมินผลการวิเคราะห์ประสิทธิภาพของระบบตรวจจับการบุกรุก หลังจากทำการจัดกลุ่มและให้คะแนนเรียบร้อยแล้ว

4.1.3 ฐานข้อมูล

ในการทำงานของเครื่องมือช่วยประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก จำเป็นจะต้องมีการเก็บข้อมูลลักษณะของจุดอ่อนไว้ที่เครื่องคอมพิวเตอร์เพื่อใช้ในการประเมินผล โดยมีคำอธิบายรายละเอียดในแต่ละคอลัมน์อยู่ในตารางที่ 4.2

ตารางที่ 4.2 คำอธิบายลักษณะข้อมูลของรายการซีวีอี

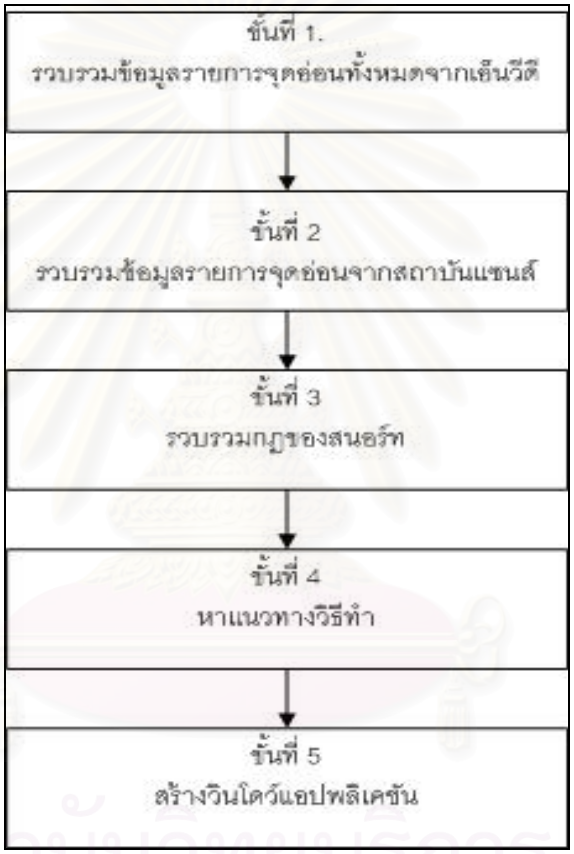
ชื่อคอลัมน์	คำอธิบาย
Name	ใช้เก็บหมายเลขซีวีอี มีชนิดข้อมูลเป็นข้อความ
Genesis	ใช้เก็บชนิดของจุดอ่อนตามประเภทจุดอ่อน มีชนิดข้อมูลเป็นตัวเลข
Location	ใช้เก็บชนิดของจุดอ่อนตามแหล่งที่เกิดจุดอ่อน มีชนิดเป็นตัวเลข
OS	ใช้เก็บชนิดของจุดอ่อนตามระบบปฏิบัติการ มีชนิดเป็นตัวเลข
Confidentiality	ใช้เก็บคะแนนของความเสียหายจากการเสียความเป็นความลับ มีชนิดเป็นตัวเลข
Integrity	ใช้เก็บคะแนนของความเสียหายจากการเสียความบูรณภาพ มีชนิดเป็นตัวเลข
Availability	ใช้เก็บคะแนนของความเสียหายจากการเสียความพร้อมใช้ มีชนิดเป็นตัวเลข
System_Compomise	ใช้เก็บคะแนนของความเสียหายจากการที่ระบบถูกล่วงละเมิด มีชนิดเป็นตัวเลข
Total	ใช้เก็บคะแนนรวมของจุดอ่อน มีชนิดเป็นตัวเลข
Has_Snort	ใช้เก็บค่าว่าจุดอ่อนนี้มีในกฎของสนอร์ทหรือไม่ มีชนิดเป็นตัวเลข

4.2 การพัฒนาเครื่องมือ

ในส่วนนี้จะกล่าวถึงการพัฒนาเครื่องมือช่วยในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก ตามที่ได้ออกแบบไว้ในหัวข้อที่ 4.1

4.2.1 ขั้นตอนในการพัฒนาระบบ

ขั้นตอนในการพัฒนาระบบประกอบด้วย 5 ขั้นตอน ดังรูปที่ 4.3



รูปที่ 4.3 ขั้นตอนในการพัฒนาระบบ

4.2.1.1 รวบรวมข้อมูลรายการจุดอ่อนทั้งหมดจากเอ็นวีดี

รวบรวมรายการจุดอ่อนจากเว็บไซต์ของเอ็นวีดี ซึ่งจะมีให้ดาวน์โหลดเอกสารรายละเอียดของรายการซีวีอีทั้งหมด ในรูปแบบของไฟล์เอกเอ็มแอล (XML) เพื่อให้สามารถระบุรายละเอียดของจุดอ่อนแต่ละตัวได้อย่างถูกต้อง โดยไฟล์ที่ดาวโหลดมาทั้งหมด ประกอบด้วย

- nvdcve-2002.xml เก็บข้อมูลของจุดอ่อนตั้งแต่ปี ค.ศ.1999-2002
- nvdcve-2003.xml เก็บข้อมูลจุดอ่อนของปี ค.ศ. 2003
- nvdcve-2004.xml เก็บข้อมูลจุดอ่อนของปี ค.ศ. 2004
- nvdcve-2005.xml เก็บข้อมูลจุดอ่อนของปี ค.ศ. 2005
- nvdcve-2006.xml เก็บข้อมูลจุดอ่อนของปี ค.ศ. 2006
- nvdcve-2007.xml เก็บข้อมูลจุดอ่อนของปี ค.ศ. 2007

4.2.1.2 รวบรวมข้อมูลรายการจุดอ่อนจากสถาบันแซนส์

รวบรวมรายการจุดอ่อนจากสถาบันแซนส์ตั้งแต่ปี ค.ศ.2000-2007 แล้วทำการคัดกรองรายการซีวีอีออกมาเป็นให้อยู่ในรูปแบบไฟล์text เพื่อใช้นำเข้าสู่ฐานข้อมูล

4.2.1.3 รวบรวมกฎของสนอร์ท

ทำการดาวโหลดกฎของสนอร์ทรุ่นล่าสุดจากเว็บไซต์ www.snort.org เพื่อนำมาคัดกรองข้อมูลสู่ฐานข้อมูล

4.2.1.4 หาแนวทางวิธีทำ

การพัฒนานี้ได้ออกแบบวิธีการออกมาในรูปแบบวินโดวส์แอปพลิเคชัน เพื่อให้ผู้ใช้สามารถใช้งานที่เครื่องของตนเองได้ โดยได้พัฒนาโดยใช้ภาษาวีบีดอทเน็ต

4.2.1.5 สร้างวินโดวส์แอปพลิเคชัน

ทำการกำหนดและพัฒนาเครื่องมือตามฟังก์ชันการทำงานที่ได้ออกแบบไว้ในหัวข้อที่ 4.1

4.2.2 สภาพแวดล้อมที่ใช้ในการพัฒนาเครื่องมือ

1. ฮาร์ดแวร์ ใช้ เครื่องคอมพิวเตอร์ จำนวน 1 เครื่อง Intel Core 2 Duo CPU 2.49 GHz RAM 2GB Hard Disk 160GB

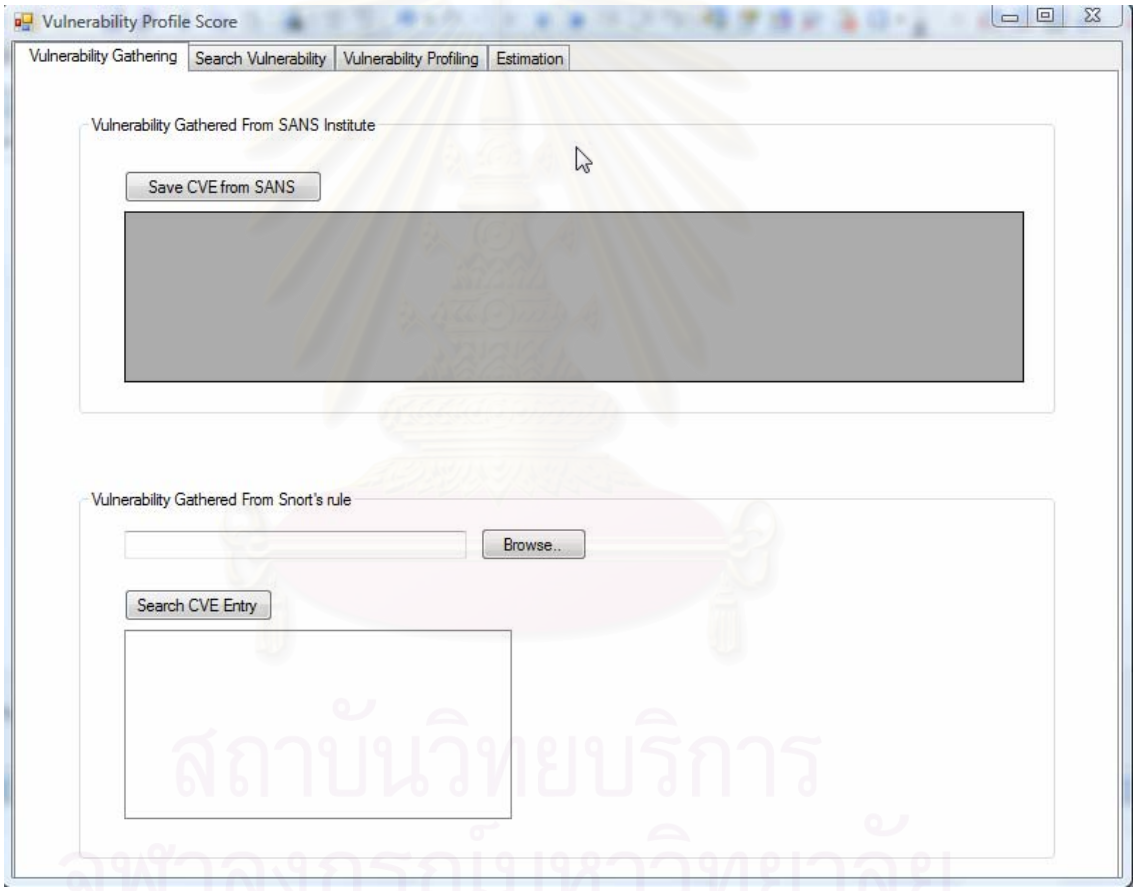
2. ซอฟต์แวร์

- ไมโครซอฟท์ ด็อตเน็ต เฟรมเวิร์ค (Microsoft.Net Framework) รุ่น 2.0

- วิชวลสตูดิโอ 2005 (Visual Studio 2005)

4.2.3 ส่วนติดต่อกับผู้ใช้

ในการใช้งานเครื่องมือช่วยประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก ในส่วนพื้นที่การใช้งานจะแบ่งเป็น 4 ส่วน ดังรูปที่ 4.4

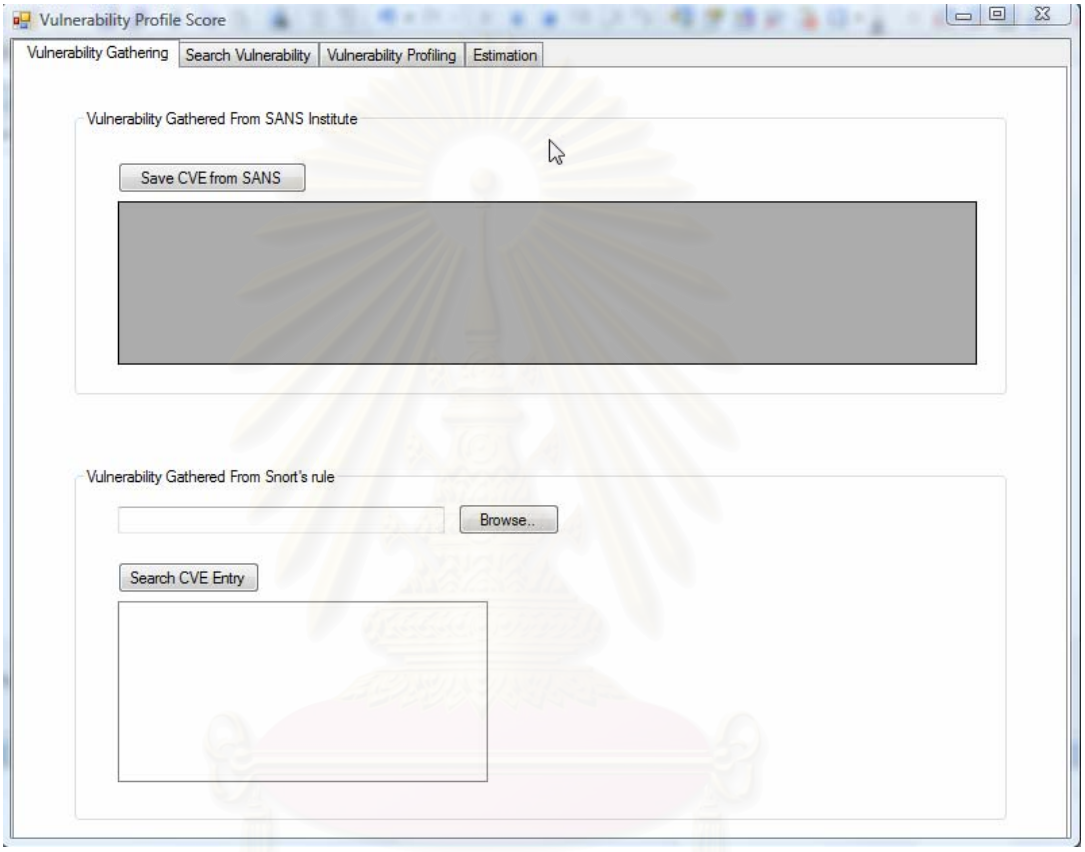


รูปที่ 4.4 หน้าจอการใช้งานเครื่องมือ

โดยที่แต่ละส่วนจะมีรายละเอียดดังนี้

4.2.3.1 ส่วนการรวบรวมข้อมูล

ในส่วนนี้จะเป็นการนำเข้าข้อมูลซึ่งจะแบ่งเป็น 2 ส่วนคือ ส่วนการนำเข้าข้อมูลจากสถาบันแซนส์ ดังแสดงในรูปที่ 4.5 และส่วนการคัดกรองข้อมูลจุดอ่อนจากกฎของสนอร์ทซึ่งแต่ละตัวมีการทำงานดังนี้



รูปที่ 4.5 หน้าจอส่วนการรวบรวมข้อมูล

4.2.3.1.1 ส่วนการคัดกรองข้อมูลจากสถาบันแซนส์

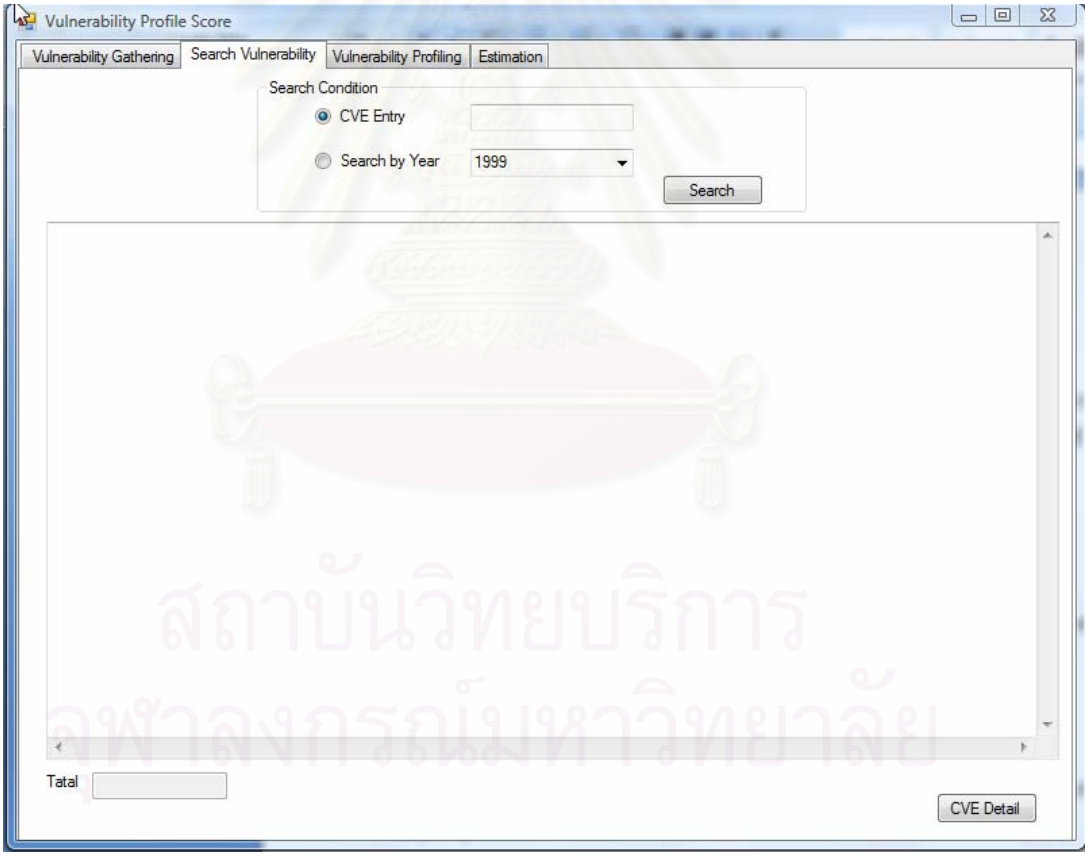
จากรูป ผู้ใช้ต้องกดปุ่ม Browse เพื่อทำการเลือกไฟล์ข้อมูลรายการจุดอ่อน เมื่อเลือกได้แล้ว ก็หน้าจอจะแสดงข้อมูลรายการจุดอ่อนบนกริด เพื่อให้ผู้ใช้ทำการตรวจสอบดูอีกครั้งก่อนที่จะบันทึกลงไปในฐานข้อมูล เมื่อผู้ใช้ตรวจสอบความถูกต้องเสร็จแล้วจะทำการกดปุ่ม Save เพื่อบันทึกลงฐานข้อมูล พร้อมสำหรับการประเมินผลในขั้นตอนถัดไป

4.2.3.2 การคัดกรองข้อมูลจุดอ่อนจากกฎของสนอร์ท

จากรูป ผู้ใช้ต้องกดปุ่ม Browse เพื่อทำการเลือกไฟล์กฎของสนอร์ท จากนั้นกด Search เพื่อทำการคัดกรองรายการซีวีอีจากกฎของสนอร์ทที่มีการอ้างอิงถึง แล้วแสดงให้ผู้ใช้ดูบน list จากนั้นเมื่อ ผู้ใช้กด save เครื่องมือจะทำการเปรียบเทียบกฎของสนอร์ท กับจุดอ่อนที่ได้คัดกรองไว้แล้วจากข้อ 4.1.2 หากรายการซีวีอีในกฎของสนอร์ท ตรงกับ รายการซีวีอีจากสถาบันแซนส์ จะทำการมาร์ก รายการจุดอ่อนนั้นในฐานข้อมูลว่ามีอยู่ในรายการจุดอ่อนจากกฎของสนอร์ท

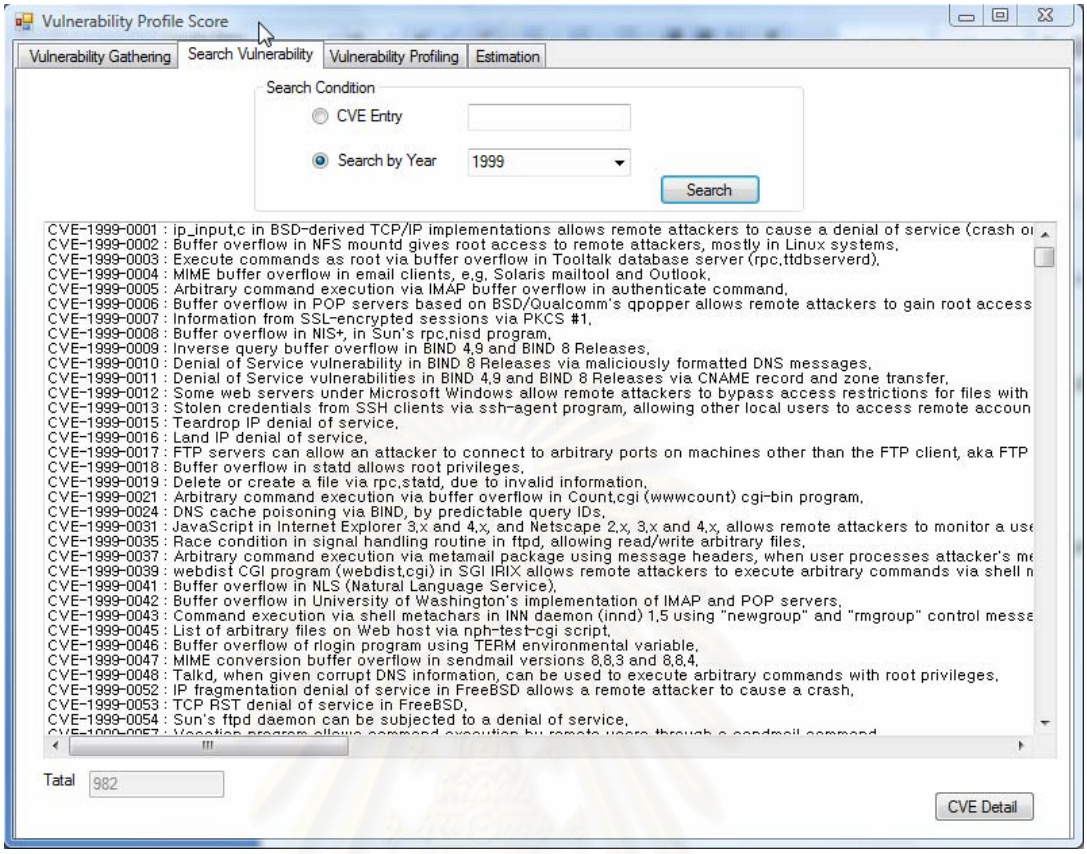
4.2.3.2 ส่วนการค้นหารายการจุดอ่อน

ในส่วนนี้จะเป็นการค้นหาข้อมูลจุดอ่อนที่มีในรายการซีวีอี โดยผู้ใช้สามารถเลือกได้ตามปี หรือจะใส่ชื่อหมายเลขซีวีอีตรง แล้วเครื่องมือจะทำการค้นหาออกมาแสดงบนหน้าจอ ดังรูปที่ 4.6



รูปที่ 4.6 หน้าจอส่วนการค้นหาข้อมูล

จากรูป ผู้ใช้ใส่เงื่อนไขในการค้นหา โดยสามารถใส่ชื่อแบบเต็มรูปแบบ หรือเลือกตามปี หากใส่ข้อมูลผิด จะขึ้นข้อความเตือน และเมื่อเลือกแล้วจะแสดงข้อมูลดังรูปที่ 4.7

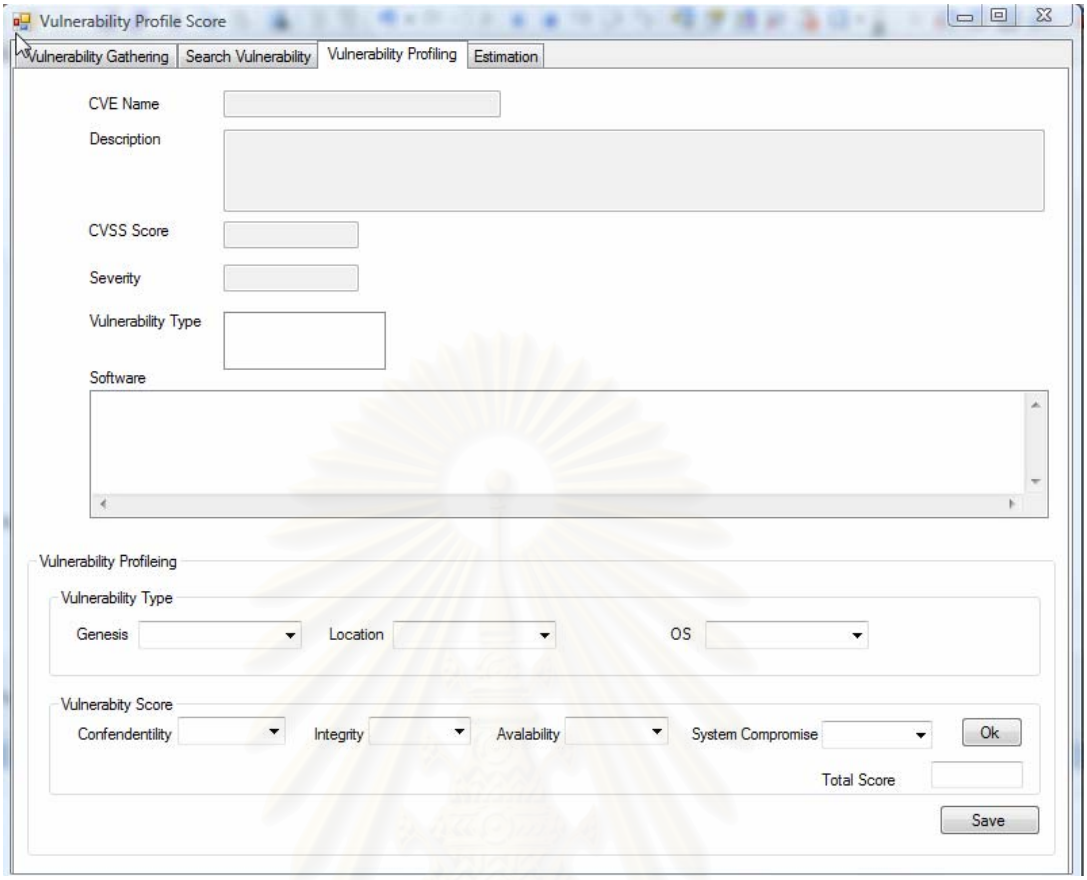


รูปที่ 4.7 หน้าจอส่วนการค้นหาข้อมูลเมื่อผู้ใช้เลือกตามปี ค.ศ.

ผู้ใช้สามารถเลือกข้อมูล แล้วกดปุ่ม "CVE Detail" เพื่อดูรายละเอียด และบันทึกข้อมูลอื่นๆของจุดอ่อนนี้ได้

4.2.3.3 ส่วนการบันทึกรายละเอียดจุดอ่อน

ในส่วนนี้จะเป็นการแสดงรายละเอียดข้อมูลจุดอ่อน ผู้ใช้สามารถบันทึกข้อมูลในส่วนของการจัดกลุ่มและการให้คะแนนจุดอ่อนได้ ดังรูปที่ 4.8

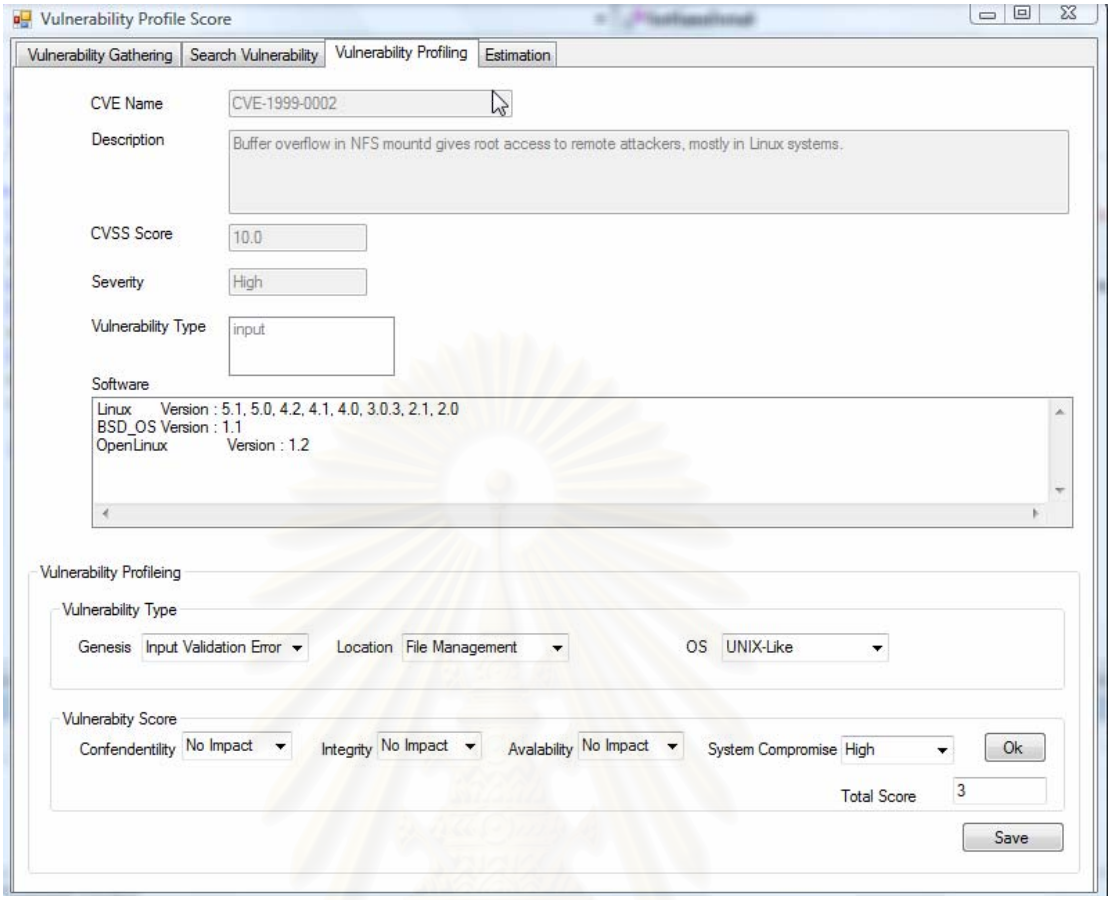


รูปที่ 4.8 หน้าจอส่วนการบันทึกรายละเอียดจุดอ่อน

จากรูป เมื่อผู้ใช้เลือกรายการซีวีอีจากหน้า Search CVE แล้ว รายการซีวีอีนั่นจะมาปรากฏในหน้านี้ โดยถ้าหากมีในประกาศของสถาบันแซนส์ ส่วนของ Vulnerability Profile จะ enable เพื่อให้ผู้ใช้สามารถเพิ่มข้อมูลได้ แต่หากไม่มีส่วนนี้จะทำการ Disable

ในส่วนของ Vulnerability Profile จะใช้ทำการจัดข้อมูลของจุดอ่อน ตามขั้นตอนการวิจัย โดยจะแบ่งเป็นสองส่วนคือ ส่วนของการจัดกลุ่มข้อมูลจุดอ่อน และการให้คะแนนจุดอ่อน โดยส่วนของการจัดกลุ่มจุดอ่อนจะแบ่งเป็น ให้เลือกเป็น 3 กลุ่มคือตามระบบปฏิบัติการ, ตามประเภทจุดอ่อน และจุดที่เกิดจุดอ่อน

ต่อมาทำการให้คะแนนจุดอ่อน โดยจะมีลักษณะความเสียหาย 4 ประเภท และแต่ละประเภทมีลักษณะความรุนแรงสามระดับ คือ ระดับ 1 , 2, 3 หรือ ไม่มีผลกระทบต่อระบบ เมื่อทำการ เลือกทั้งสามแล้ว กด ok เพื่อดูคะแนนรวมของจุดอ่อนตัวนี้ ดังรูปที่ 4.9 เมื่อผู้ใช้ปรับแต่งลักษณะจุดอ่อนเสร็จแล้วจะทำการกดปุ่ม Save เพื่อบันทึกลงฐานข้อมูลรอการประเมินผลในขั้นตอนต่อไป

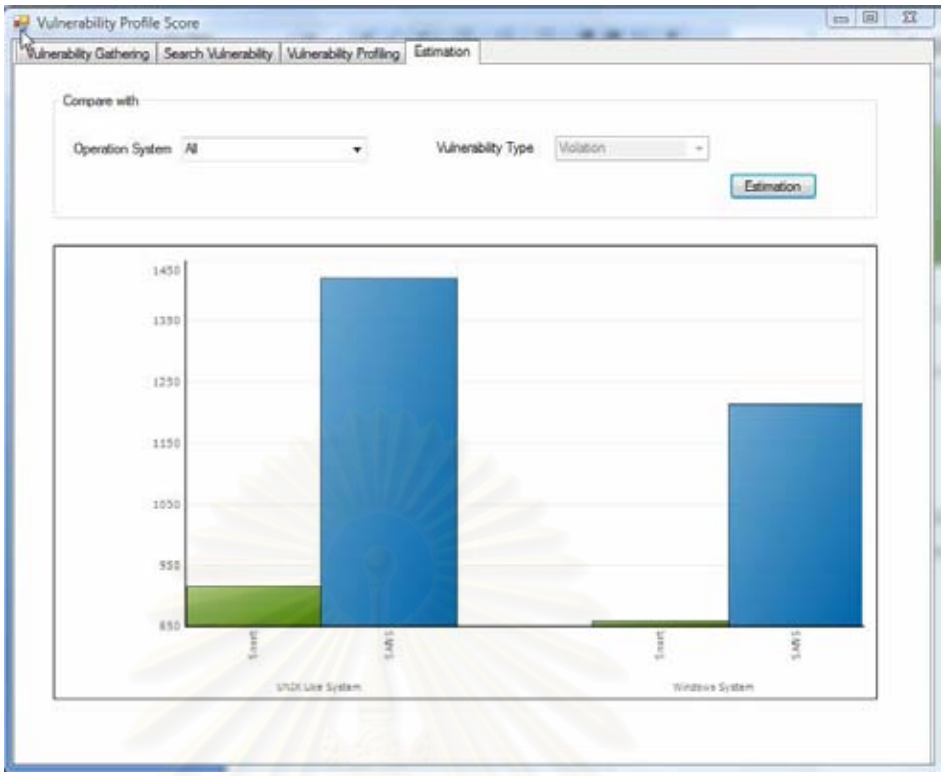


รูปที่ 4.9 หน้าจอเมื่อผู้ใช้ทำการบันทึกรายละเอียดจุดอ่อน

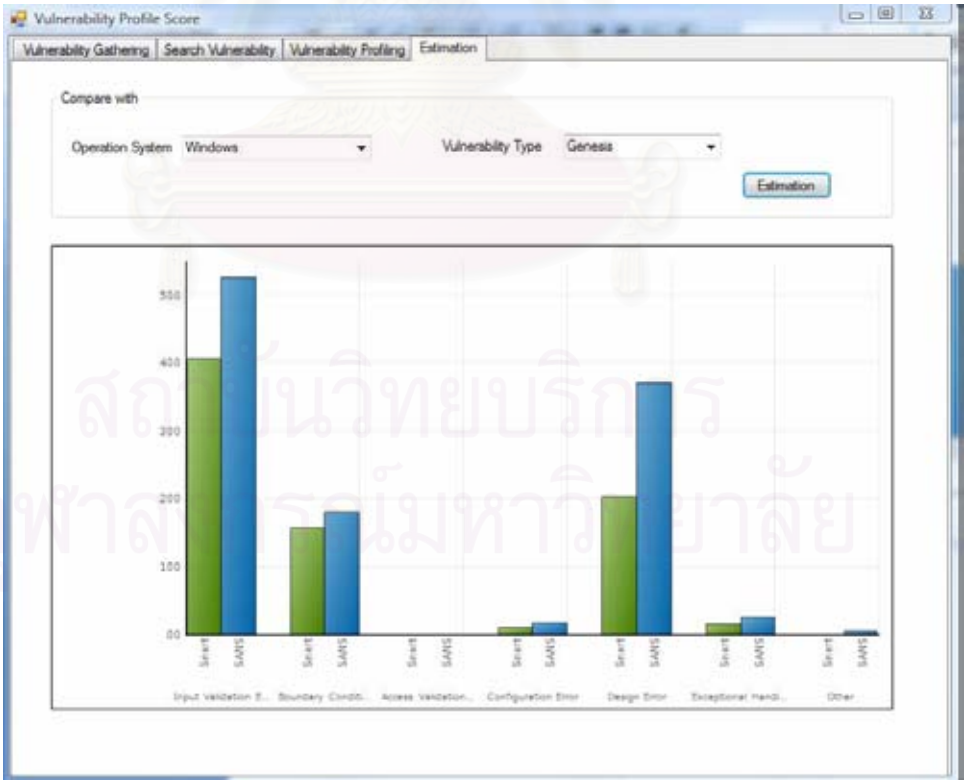
4.2.3.4 ส่วนการประเมินผล

ในส่วนนี้จะเป็นการแสดงผลการประเมินประสิทธิภาพในรูปแบบกราพแท่ง ดังตัวอย่างในรูปที่ 4.10, 4.11, 4.12 โดยผู้ใช้สามาถเลือกได้ตามเงื่อนไขดังนี้

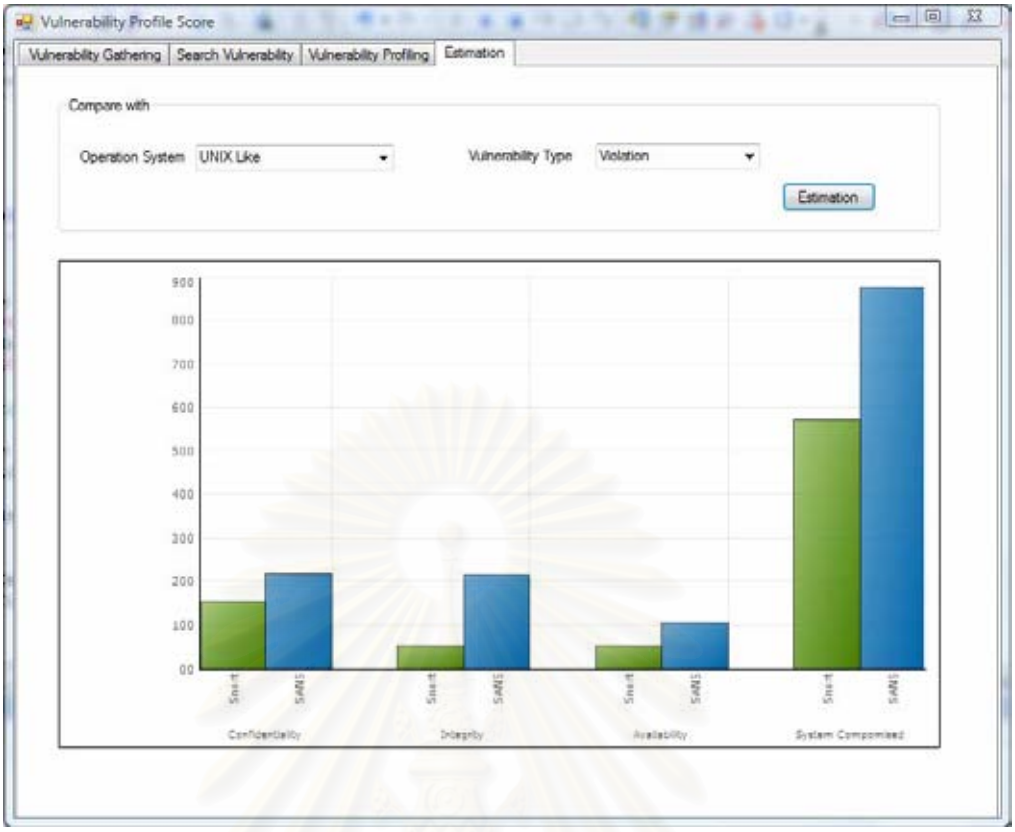
- เลือกทั้งหมด
- เลือกตามระบบปฏิบัติการ คือ ระบบปฏิบัติการวินโดวส์และตระกูลยูนิกซ์
- เลือกตามประเภทจุดอ่อน
- เลือกตามแหล่งที่เกิดจุดอ่อน
- เลือกตามลักษณะที่ส่งผลต่อความเสียหายต่อระบบ



รูปที่ 4.10 หน้าจอเมื่อผู้ใช้ต้องการดูผลลัพธ์ในภาพรวม



รูปที่ 4.11 หน้าจอเลือกระบบปฏิบัติการวินโดวส์ตามประเภทจุดอ่อน



รูปที่ 4.12 หน้าจอเมื่อเลือกระบบปฏิบัติการยูนิกซ์ตามลักษณะความสียหาย

4.2.4 การทดสอบระบบ

ในส่วนของการทดสอบระบบนี้ ผู้วิจัยได้ทำการทดสอบระบบโดยเปรียบเทียบกับการทำด้วยมือ ตั้งแต่ขั้นตอนคัดกรอง การจัดกลุ่ม และการให้คะแนน พบว่าได้ผลลัพธ์ เหมือนกับที่ใช้เครื่องมือ

ในบทนี้ได้มีการกล่าวถึง การออกแบบและพัฒนาเครื่องมือในการช่วยประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก และในบทต่อไปจะขอกล่าวถึงผลของงานวิจัย

บทที่ 5

ผลการวิจัย

จากการศึกษา และวิเคราะห์ประสิทธิภาพในการป้องกันจุดอ่อนของระบบตรวจจับการบุกรุก ซึ่งมีการวิเคราะห์โดยใช้คะแนนจุดอ่อนที่มีอยู่ในรายงานของสถาบันแซนส์ เปรียบเทียบกับการอ้างอิงรายการจุดอ่อนของกฎของสนอร์ท ทำให้ได้ผลการวิจัยดังนี้

5.1 ค่าดัชนีความเปราะบางของจุดอ่อนในรายงานของสถาบันแซนส์

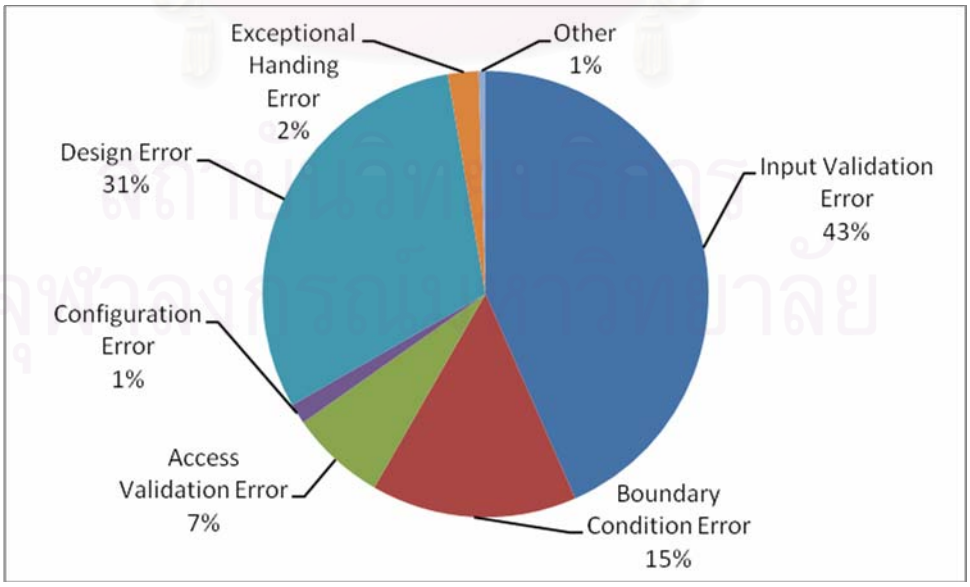
จากการจัดกลุ่มและให้คะแนนจุดอ่อนที่เกิดขึ้นกับจุดอ่อนที่อยู่ในรายงานของสถาบันแซนส์ตั้งแต่ปี ค.ศ. 2000-2007 จำนวน 649 รายการ แยกเป็นจุดอ่อนที่อยู่ในระบบปฏิบัติการวินโดวส์ จำนวน 377 รายการ และจุดอ่อนที่อยู่ในระบบปฏิบัติการตระกูลยูนิกซ์ จำนวน 272 รายการ ซึ่งจุดอ่อนแต่ละรายการสามารถก่อให้เกิดความเสียหายได้มากกว่า 1 ลักษณะ โดยที่คะแนนของจุดอ่อนแต่ละความเสียหาย จะมีระดับความรุนแรงเดียวกัน เมื่อทำการให้คะแนนตามความรุนแรงและผลการโจมตี ทำให้สามารถกำหนดดัชนีความเปราะบางของระบบปฏิบัติการแต่ละประเภทได้เป็น 1214 คะแนนในระบบปฏิบัติการวินโดวส์ และ 711 คะแนนในระบบปฏิบัติการตระกูลยูนิกซ์ สามารถแสดงรายละเอียดดังตารางที่ 5.1 – 5.4

ตารางที่ 5.1 ค่าดัชนีความเปราะบางตามประเภทของจุดอ่อนในระบบปฏิบัติการวินโดวส์

No.	Genesis	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	Input Validation Error	70	29	96	332	527
2	Boundary Condition Error	9	6	58	108	181
3	Access Validation Error	42	10	10	22	84
4	Configuration Error	7	0	2	9	18

5	Design Error	75	44	91	161	371
6	Exceptional Handling Error	3	0	19	5	27
7	Other	2	2	2	0	6
	Total	208	91	278	637	1214

ตารางที่ 5.1 เป็นการแจกแจงคะแนนความเปราะบางของจุดอ่อนที่อยู่ในรายงานของสถาบันแซนส์ ซึ่งเป็นจุดอ่อนที่อยู่ในระบบปฏิบัติการวินโดวส์ โดยแจกแจงตามประเภทของจุดอ่อน ผลคะแนนที่ได้ทั้งหมด 1214 คะแนน แยกตามประเภทของความเสียหายที่เกิดจากการโจมตีจุดอ่อน ความเสียหายประเภทสูญเสียความลับ 208 คะแนน ความเสียหายประเภทสูญเสียบูรณภาพของระบบ 91 คะแนน ความเสียหายประเภทสูญสียสภาพพร้อมใช้งาน 278 คะแนน และความเสียหายประเภทระบบถูกล่วงละเมิด 637 คะแนน ซึ่งคะแนนเหล่านี้สามารถอธิบายในรูปแบบกราฟได้ ดังรูปที่ 5.1



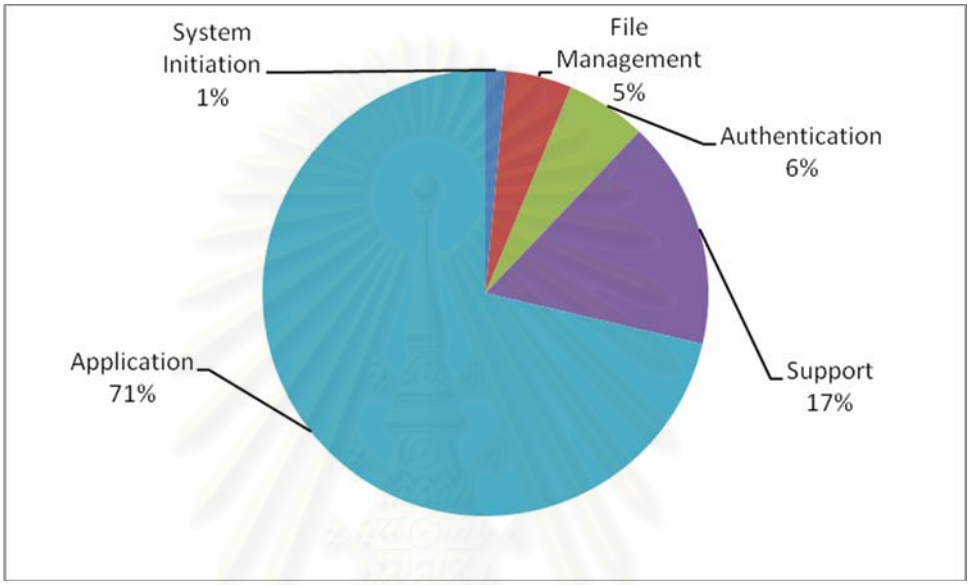
รูปที่ 5.1 ความเสียหายแยกตามประเภทของจุดอ่อนในระบบปฏิบัติการวินโดวส์

รูปที่ 5.1 แสดงสัดส่วนระดับคะแนนของจุดอ่อน ที่พบในรายงานของสถาบันแซนส์ของระบบปฏิบัติการวินโดวส์ ซึ่งแบ่งตามประเภทของจุดอ่อน จะพบว่า จุดอ่อนที่มีระดับคะแนนมากที่สุดที่พบในระบบคือ จุดอ่อนที่เกิดจากความผิดพลาดของการตรวจสอบข้อมูลนำเข้า (Input Validation Error) ซึ่งคิดเป็น 43% ของคะแนนจุดอ่อนทั้งหมด รองลงมาเป็นจุดอ่อนที่เกิดจากความผิดพลาดของการออกแบบ (Design Error) คิดเป็น 31% ของคะแนนจุดอ่อนทั้งหมด อันดับสามเป็นจุดอ่อนที่เกิดจากความผิดพลาดของขอบเขตข้อมูล (Boundary Condition Error) ซึ่งคิดเป็น 15% ของคะแนนจุดอ่อนทั้งหมด ตามด้วยจุดอ่อนที่เกิดจากความผิดพลาดของการตรวจสอบการเข้าถึงข้อมูล (Access Validation Error) ความผิดพลาดจากการจัดการข้อยกเว้น (Exceptional Handling Error) ความผิดพลาดของการปรับแต่งระบบ (Configuration Error) และความผิดพลาดอื่นๆ ตามลำดับ

ตารางที่ 5.2 ค่าดัชนีความเปราะบางตามแหล่งที่เกิดจุดอ่อนในระบบปฏิบัติการวินโดวส์

No.	Location	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	System Initiation	5	5	5	3	18
2	File Management	34	5	7	12	58
3	Authentication	24	13	18	16	71
4	Support	19	12	36	134	201
5	Application	126	56	212	472	866
	Total	208	91	278	637	1214

ตารางที่ 5.2 เป็นการแจกแจงคะแนนความเปราะบางของจุดอ่อน ที่มีอยู่ในรายงานของสถาบันแซนส์ ซึ่งเป็นจุดอ่อนที่อยู่ในระบบปฏิบัติการวินโดวส์ โดยแจกแจงตามตำแหน่งของการเกิดจุดอ่อน โดยที่คะแนนเหล่านี้สามารถอธิบายในรูปแบบกราฟวงกลมได้ดังรูปที่ 5.2



รูปที่ 5.2 ความเสียหายตามแหล่งที่เกิดของจุดอ่อนในระบบปฏิบัติการวินโดวส์

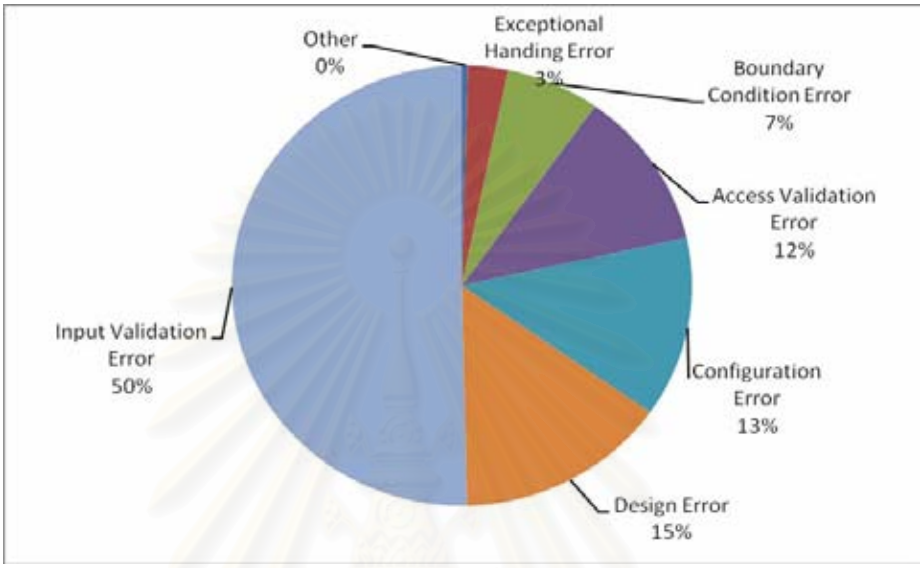
รูปที่ 5.2 แสดงสัดส่วนระดับคะแนนของจุดอ่อน ที่พบในรายงานของสถาบันแซนส์ของระบบปฏิบัติการวินโดวส์ ซึ่งแบ่งตามตำแหน่งที่เกิดของจุดอ่อน จะพบว่า ตำแหน่งของระบบที่มีระดับคะแนนความเสียหายมากที่สุด คือ ส่วนของโปรแกรมประยุกต์ (Application) ซึ่งมีระดับคะแนนเป็น 71% ของคะแนนทั้งหมด รองลงมาคือส่วนของโปรแกรมสนับสนุนการทำงานของระบบ (Support) คิดเป็น 17% ของคะแนนทั้งหมด จากนั้นเป็นส่วนการพิสูจน์ตัวจริง (Authentication) ส่วนการจัดการแฟ้มข้อมูล (File Management) และส่วนการเริ่มต้นระบบ (System Initiation) ตามลำดับ

ตารางที่ 5.3 ค่าดัชนีความเปราะบางตามประเภทของจุดอ่อนในระบบปฏิบัติการตระกูลยูนิกซ์

No.	Genesis	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	Input Validation Error	31	19	45	263	358
2	Boundary Condition Error	0	0	12	35	47
3	Access Validation Error	26	8	5	44	83
4	Configuration Error	32	16	13	33	94
5	Design Error	17	8	30	51	106
6	Exceptional Handling Error	4	2	4	10	20
7	Other	0	0	0	3	3
	Total	110	53	109	439	711

ตารางที่ 5.3 เป็นการแจกแจงคะแนนความเปราะบางของจุดอ่อนที่อยู่ในรายงานของสถาบันแซนส์ ซึ่งเป็นจุดอ่อนที่อยู่ในระบบปฏิบัติการตระกูลยูนิกซ์ โดยแจกแจงตามประเภทของจุดอ่อน ผลคะแนนที่ได้ทั้งหมด 711 คะแนน แยกตามประเภทของความเสียหายที่เกิดจากการโจมตีจุดอ่อน ความเสียหายประเภทสูญเสียความลับ 110 คะแนน ความเสียหายประเภทสูญเสียบูรณภาพของระบบ 53 คะแนน ความเสียหายประเภทสูญสียสภาพพร้อมใช้งาน 109 คะแนน

และความเสียหายประเภทระบบถูกล่วงละเมิด 439 คะแนน ซึ่งคะแนนเหล่านี้สามารถอธิบายในรูปแบบกราฟได้ ดังรูปที่ 5.3



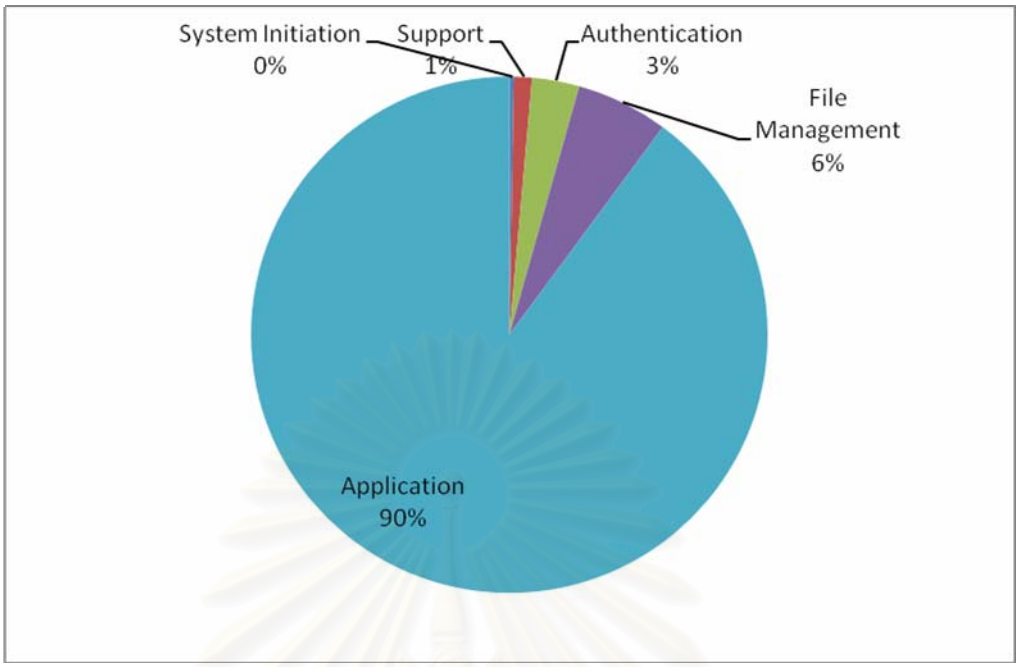
รูปที่ 5.3 ความเสียหายแยกตามประเภทของจุดอ่อนในระบบปฏิบัติการตระกูลยูนิกซ์

รูปที่ 5.3 แสดงสัดส่วนระดับคะแนนของจุดอ่อน ที่พบในรายงานของสถาบันแซนส์ของระบบปฏิบัติการตระกูลยูนิกซ์ ซึ่งแบ่งตามประเภทของจุดอ่อน จะพบว่า จุดอ่อนที่มีระดับคะแนนมากที่สุดที่พบในระบบคือ จุดอ่อนที่เกิดจากความผิดพลาดของการตรวจสอบข้อมูลนำเข้า (Input Validation Error) ซึ่งคิดเป็น 50% ของคะแนนจุดอ่อนทั้งหมด รองลงมาเป็นจุดอ่อนที่เกิดจากความผิดพลาดของการออกแบบ (Design Error) คิดเป็น 15% ของคะแนนจุดอ่อนทั้งหมด อันดับสามเป็นจุดอ่อนที่เกิดจากความผิดพลาดของการปรับแต่งระบบ (Configuration Error) ซึ่งคิดเป็น 13% ของคะแนนจุดอ่อนทั้งหมด ตามด้วยจุดอ่อนที่เกิดจากความผิดพลาดของการตรวจสอบการเข้าถึงข้อมูล (Access Validation Error) ความผิดพลาดของขอบเขตข้อมูล (Boundary Condition Error) ความผิดพลาดจากการจัดการข้อยกเว้น (Exceptional Handling Error) และความผิดพลาดอื่นๆ ตามลำดับ

ตารางที่ 5.4 ค่าดัชนีความเปราะบางตามแหล่งที่เกิดจุดอ่อนในระบบปฏิบัติการตระกูลยูนิกซ์

No.	Location	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	System Initiation	0	2	0	0	2
2	File Management	14	3	7	17	41
3	Authentication	4	1	3	13	21
4	Support	2	0	0	6	8
5	Application	90	47	99	403	639
	Total	110	53	109	439	711

ตารางที่ 5.4 เป็นการแจกแจงคะแนนความเปราะบางของจุดอ่อน ที่มีอยู่ในรายงานของสถาบันแซนส์ ซึ่งเป็นจุดอ่อนที่อยู่ในระบบปฏิบัติการตระกูลยูนิกซ์ โดยแจกแจงตามตำแหน่งของการเกิดซึ่งมีการแจกแจงตามประเภทของความเสียหายที่เกิดขึ้นจากการโจมตีจุดอ่อน โดยที่คะแนนเหล่านี้สามารถอธิบายในรูปแบบกราฟวงกลมได้ดังรูปที่ 5.4



รูปที่ 5.4 ความเสียหายตามแหล่งที่เกิดของจุดอ่อนในระบบปฏิบัติการตระกูลยูนิกซ์

รูปที่ 5.4 แสดงสัดส่วนระดับคะแนนของจุดอ่อน ที่พบในรายงานของสถาบันแซนส์ของระบบปฏิบัติการตระกูลยูนิกซ์ ซึ่งแบ่งตามตำแหน่งที่เกิดของจุดอ่อน จะพบว่า ตำแหน่งของระบบที่มีระดับคะแนนความเสียหายมากที่สุด คือ ส่วนของโปรแกรมประยุกต์ (Application) ซึ่งมีระดับคะแนนเป็น 90% ของคะแนนทั้งหมด รองลงมาคือส่วนของโปรแกรมสนับสนุนการทำงานของระบบ (Support) คิดเป็น 17% ของคะแนนทั้งหมด จากนั้นเป็นส่วนการพิสูจน์ตัวจริง (Authentication) ส่วนการจัดการแฟ้มข้อมูล (File Management) และส่วนการเริ่มต้นระบบ (System Initiation) ตามลำดับ

5.2 ค่าดัชนีความเปราะบางของจุดอ่อนเมื่อเปรียบเทียบกับกฎของสนอร์ท

จากการวิเคราะห์ดำเนินการของประสิทธิภาพการป้องกันจุดอ่อนของระบบตรวจจับการบุกรุก โดยใช้สนอร์ท พบว่าสนอร์ทสามารถช่วยป้องกันจุดอ่อนตามที่มีการอ้างอิงถึงรายการซีวีอีคิดเป็น 888 คะแนน ในระบบปฏิบัติการวินโดวส์ และ 464 คะแนนในระบบปฏิบัติการตระกูลยูนิกซ์ ทำให้ค่าดัชนีความเปราะบางของระบบปฏิบัติการวินโดวส์มีค่าลดลงเหลือ 326 คะแนน และในระบบปฏิบัติการตระกูลยูนิกซ์มีค่าลดลงเหลือ 247 คะแนน ซึ่งสามารถแสดงรายละเอียด

โดยแบ่งตามประเภทจุดอ่อน ได้ดังตารางที่ 5.5 - 5.6 ตามตำแหน่งที่เกิดของจุดอ่อนได้ ดังตารางที่ 5.7 - 5.8 และแสดงรายละเอียดตามลักษณะของความเสียหายได้ดังตารางที่ 5.9 - 5.10

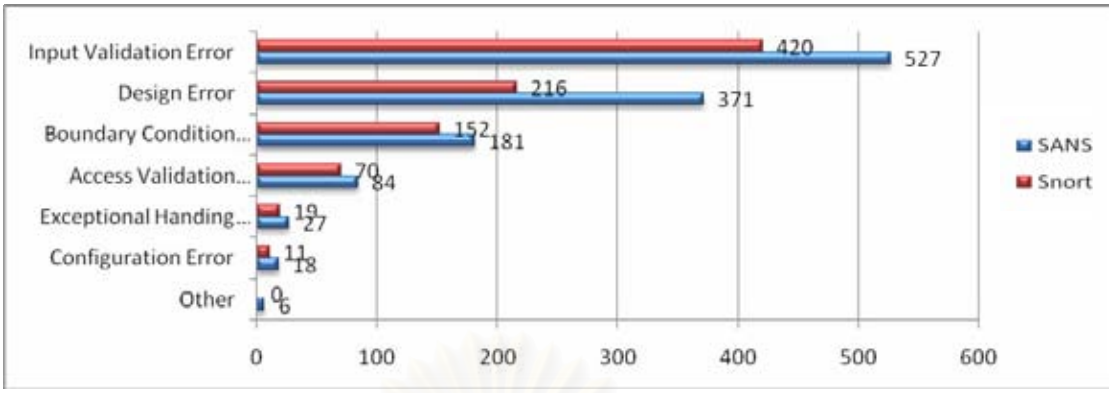
ตารางที่ 5.5 ผลการป้องกันจุดอ่อนตามประเภทของจุดอ่อนของระบบปฏิบัติการวินโดวส์

Genesis	SANS	Snort	Remain	%
Input Validation Error	527	420	107	79.7
Boundary Condition Error	181	152	29	84
Access Validation Error	84	70	14	83.3
Configuration Error	18	11	7	61.1
Design Error	371	216	155	58.2
Exceptional Handling Error	27	19	8	70.3
Other	6	0	6	0

จากผลการทดลองพบว่า จุดอ่อนที่มีเปอร์เซ็นต์การป้องกันจุดอ่อนของสนอร์ทมากที่สุด คือจุดอ่อนที่เกิดจากความผิดพลาดของขอบเขตข้อมูล โดยพบว่าสนอร์ท สามารถป้องกันจุดอ่อนประเภทนี้ได้ 83.3% ส่วนจุดอ่อนที่มีเปอร์เซ็นต์ของการป้องกันน้อยที่สุดคือ จุดอ่อนประเภทอื่นๆ รองลงมาคือจุดอ่อนที่เกิดจากความผิดพลาดของการออกแบบ โดยพบว่าสนอร์ทสามารถป้องกันจุดอ่อนประเภทนี้ได้เพียง 58.2%

ส่วนประเภทของจุดอ่อนที่ส่งผลกระทบต่อระดับความเสียหายมากที่สุด ได้แก่ จุดอ่อนที่เกิดจากการตรวจสอบข้อมูลนำเข้า โดยพบว่าในระบบปฏิบัติการวินโดวส์มีคะแนนคิดเป็น 527 คะแนนและสนอร์ท สามารถป้องกันจุดอ่อนประเภทนี้ได้ 420 คะแนนคิดเป็น 80% ของคะแนนจุดอ่อนประเภทนี้ โดยมีคะแนนจุดอ่อนที่ยังเหลืออยู่คิดเป็น 107 คะแนน

ผลลัพธ์ของการป้องกันจุดอ่อนตามประเภทจุดอ่อนของระบบปฏิบัติการวินโดวส์แสดงไว้ดังรูปที่ 5.5



รูปที่ 5.5 ผลการป้องกันตามประเภทของจุดอ่อนของระบบปฏิบัติการวินโดวส์

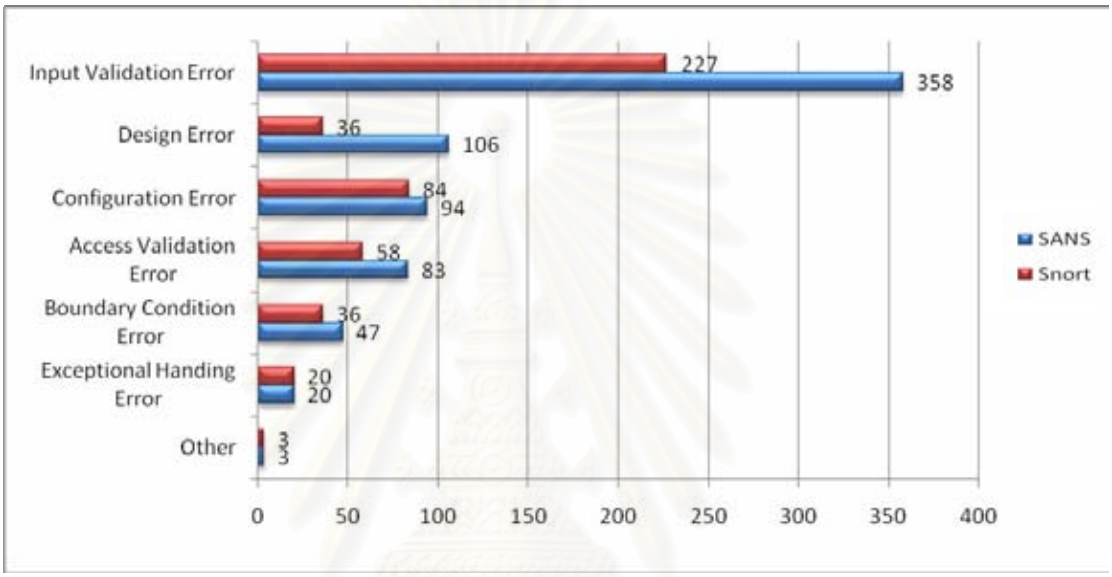
ตารางที่ 5.6 ผลการป้องกันจุดอ่อนตามประเภทของจุดอ่อนของระบบปฏิบัติการยูนิกซ์

Genesis	SANS	Snort	Remain	%
Input Validation Error	358	227	131	63.4
Boundary Condition Error	47	36	11	76.6
Access Validation Error	83	58	25	69.9
Configuration Error	94	84	10	89.4
Design Error	106	36	70	34
Exceptional Handling Error	20	20	0	100
Other	3	3	0	100

จากผลการทดลองพบว่า จุดอ่อนที่มีเปอร์เซ็นต์การป้องกันจุดอ่อนของสนอร์ทมากที่สุด คือจุดอ่อนที่เกิดจากความผิดพลาดของการปรับแต่งระบบ โดยพบว่าสนอร์ท สามารถป้องกันจุดอ่อนประเภทนี้ได้ 89.4% ส่วนจุดอ่อนที่มีเปอร์เซ็นต์ของการป้องกันน้อยที่สุดคือ จุดอ่อนที่เกิดจากความผิดพลาดของการออกแบบ โดยพบว่าสนอร์ทสามารถป้องกันจุดอ่อนประเภทนี้ได้เพียง 34%

ในระบบปฏิบัติการตระกูลยูนิกซ์มีคะแนนความเสียหายที่เกิดจากความผิดพลาดของการนำเข้าข้อมูลมากที่สุด โดยคิดเป็น 358 คะแนน และสนอร์ทสามารถป้องกันจุดอ่อนประเภทนี้ได้ 227 คะแนน คิดเป็น 63% ของคะแนนจุดอ่อนประเภทนี้

ผลลัพธ์ของการป้องกันจุดอ่อนตามประเภทจุดอ่อนของระบบปฏิบัติการตระกูลยูนิกซ์แสดงไว้ในรูปที่ 5.6



รูปที่ 5.6 ผลการป้องกันตามประเภทของจุดอ่อนของระบบปฏิบัติการตระกูลยูนิกซ์

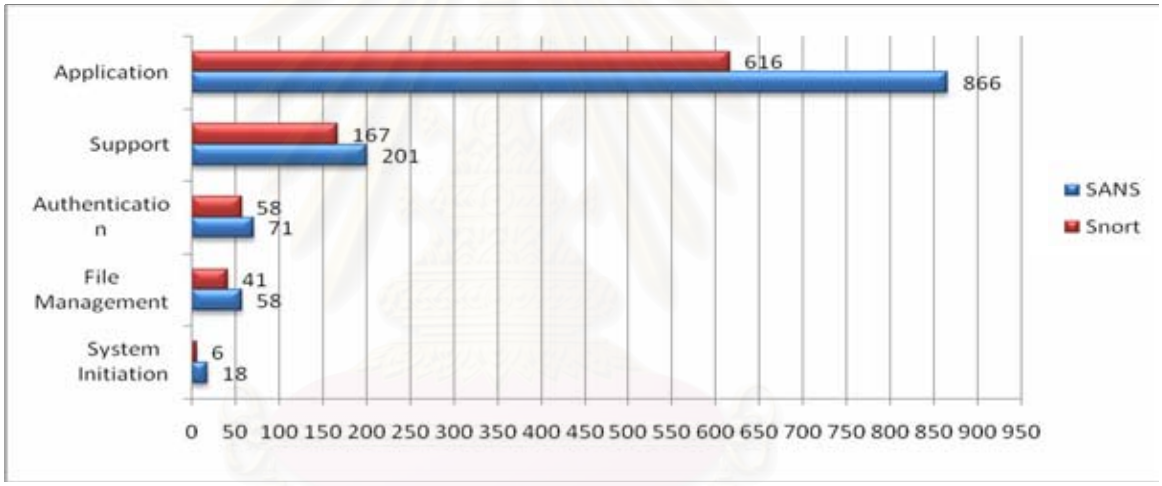
ตารางที่ 5.7 ผลการป้องกันจุดอ่อนตามแหล่งที่เกิดจุดอ่อนของระบบปฏิบัติการวินโดวส์

Location	SANS	Snort	Remain	%
System Initiation	18	6	12	33.3
File Management	58	41	17	70.7
Authentication	71	58	13	81.7
Support	201	167	34	83.1
Application	866	616	250	71.1

จากผลการทดลองพบว่า จุดอ่อนที่มีเปอร์เซ็นต์การป้องกันจุดอ่อนของสนอร์ทมากที่สุด คือจุดอ่อนที่เกิดในส่วนของการพิสูจน์ตัวจริง โดยพบว่าสนอร์ท สามารถป้องกันจุดอ่อนประเภทนี้ได้ 81.7% ส่วนจุดอ่อนที่มีเปอร์เซ็นต์ของการป้องกันน้อยที่สุดคือ จุดอ่อนที่เกิดในส่วนของการเริ่มต้นระบบ โดยพบว่าสนอร์ทสามารถป้องกันจุดอ่อนประเภทนี้ได้เพียง 33.3%

ส่วนจุดที่เกิดจุดอ่อนที่ส่งผลกระทบต่อระดับความเสียหายมากที่สุด ได้แก่ จุดอ่อนที่เกิดจากส่วนของโปรแกรมประยุกต์ คิดเป็น 866 คะแนน และสนอร์ทสามารป้องกันจุดอ่อนประเภทนี้ได้ 616 คะแนน คิดเป็น 71% ของคะแนนจุดอ่อนประเภทนี้

ผลลัพธ์ของการป้องกันจุดอ่อนตามแหล่งที่เกิดจุดอ่อนของระบบปฏิบัติการวินโดวส์แสดงไว้ในรูปที่ 5.7



รูปที่ 5.7 ผลการป้องกันตามแหล่งที่เกิดจุดอ่อนของระบบปฏิบัติการวินโดวส์

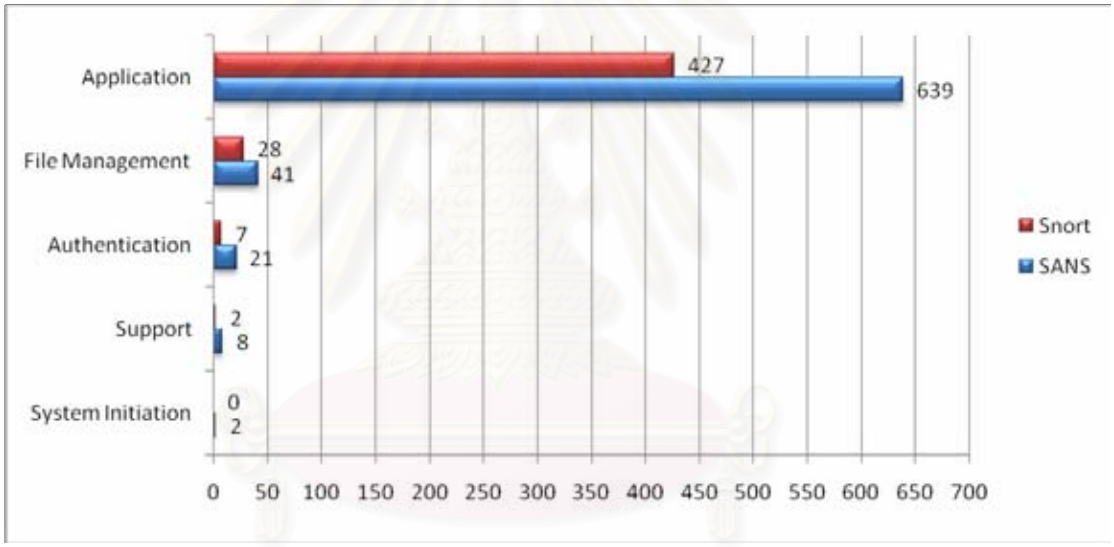
ตารางที่ 5.8 ผลการป้องกันจุดอ่อนตามแหล่งที่เกิดจุดอ่อนของระบบปฏิบัติการยูนิกซ์

Location	SANS	Snort	Remain	%
System Initiation	2	0	2	0
File Management	41	28	13	68.3
Authentication	21	7	14	33.3
Support	8	2	6	25
Application	639	427	212	66.9

จากผลการทดลองพบว่า จุดอ่อนที่มีเปอร์เซ็นต์การป้องกันจุดอ่อนของสนอร์ทมากที่สุด คือจุดอ่อนที่เกิดในส่วนของการจัดการแฟ้มข้อมูล โดยพบว่าสนอร์ท สามารถป้องกันจุดอ่อนประเภทนี้ได้ 68.3% ส่วนจุดอ่อนที่มีเปอร์เซ็นต์ของการป้องกันน้อยที่สุดคือ จุดอ่อนที่เกิดในส่วนของการเริ่มต้นระบบ โดยพบว่าสนอร์ทสามารถไม่สามารถป้องกันจุดอ่อนประเภทนี้ได้

ในระบบปฏิบัติการตระกูลยูนิกซ์พบว่าจุดอ่อนที่เกิดจากส่วนของโปรแกรมประยุกต์มีคะแนนมากที่สุด โดยคิดเป็น 639 คะแนน และสนอร์ทสามารถป้องกันจุดอ่อนประเภทนี้ได้ 427 คะแนนคิดเป็น 66.9% ของคะแนนจุดอ่อนประเภทนี้

ผลลัพธ์ของการป้องกันจุดอ่อนตามแหล่งที่เกิดจุดอ่อนของระบบปฏิบัติการตระกูลยูนิกซ์แสดงไว้ในรูปที่ 5.8



รูปที่ 5.8 ผลการป้องกันตามแหล่งที่เกิดจุดอ่อนของระบบปฏิบัติการตระกูลยูนิกซ์

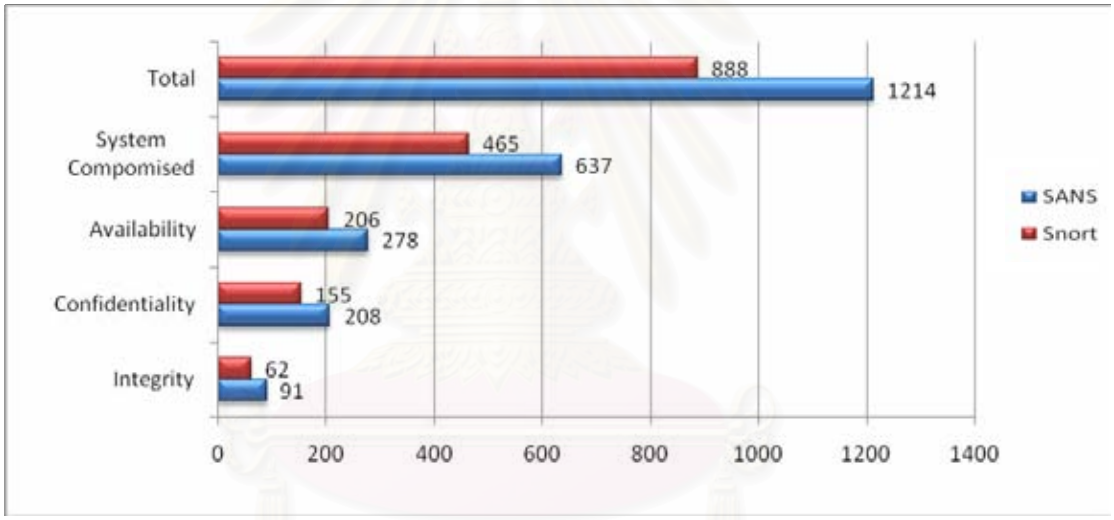
ตารางที่ 5.9 ผลการป้องกันจุดอ่อนตามลักษณะความเสียหายของระบบปฏิบัติการวินโดวส์

Total	1214	888	326	73.2
Genesis	**SANS**	**Snort**	**Remain**	**%**
Confidentiality	208	155	53	74.5
Integrity	91	62	29	68.1
Availability	278	206	72	74.1
System Compromised	637	465	172	73

จากผลการทดลองพบว่า จุดอ่อนที่มีเปอร์เซ็นต์การป้องกันมากที่สุด คือจุดอ่อนที่เกิดจากการเสียความเป็นความลับ โดยพบว่าสนอร์ท สามารถป้องกันจุดอ่อนประเภทนี้ได้ 74.5% ส่วนจุดอ่อนที่มีเปอร์เซ็นต์ของการป้องกันน้อยที่สุดคือ จุดอ่อนที่เกิดจากการเสียสภาพบูรณภาพ ซึ่งพบว่าสนอร์ทสามารถป้องกันจุดอ่อนประเภทนี้ได้เพียง 68.1%

ส่วนลักษณะความเสียหายที่มีผลกระทบต่อความเสียหายมากที่สุดคือ ลักษณะความเสียหายที่เกิดจากการที่ระบบถูกล่วงละเมิด โดยพบว่ามีคะแนนเป็น 637 คะแนนและสนอร์ทสามารถป้องกันจุดอ่อนประเภทนี้ได้ 465 คะแนน คิดเป็น 73% ของคะแนนจุดอ่อนประเภทนี้

ผลลัพธ์ของการป้องกันจุดอ่อนตามลักษณะความเสียหายของระบบปฏิบัติการวินโดวส์แสดงไว้ในรูปที่ 5.9



รูปที่ 5.9 ผลการป้องกันตามลักษณะความเสียหายของระบบปฏิบัติการวินโดวส์

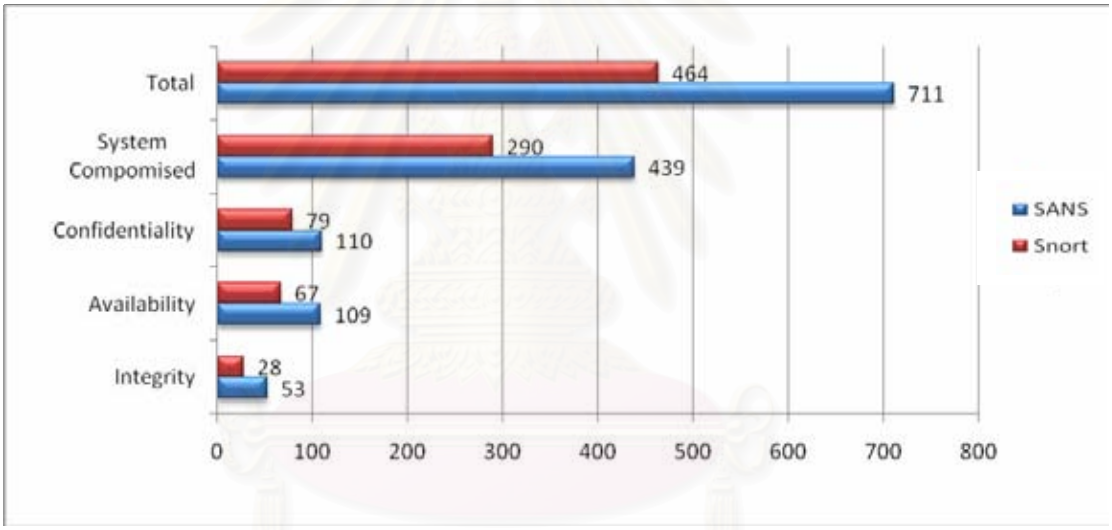
ตารางที่ 5.10 ผลการป้องกันจุดอ่อนตามลักษณะความเสียหายของระบบปฏิบัติการยูนิกซ์

Genesis	SANS	Snort	Remain	%
Confidentiality	110	79	31	71.9
Integrity	53	28	25	52.9
Availability	109	67	42	61.5
System Compromised	439	290	149	66.1
Total	711	464	247	65.3

จากผลการทดลองพบว่า จุดอ่อนที่มีเปอร์เซ็นต์การป้องกันมากที่สุด คือจุดอ่อนที่เกิดจากการเสียความเป็นความลับ โดยพบว่าสนอร์ท สามารถป้องกันจุดอ่อนประเภทนี้ได้ 71.9% ส่วนจุดอ่อนที่มีเปอร์เซ็นต์ของการป้องกันน้อยที่สุดคือ จุดอ่อนที่เกิดจากการเสียสภาพบูรณภาพ ซึ่งพบว่าสนอร์ทสามารถป้องกันจุดอ่อนประเภทนี้ได้เพียง 52.9%

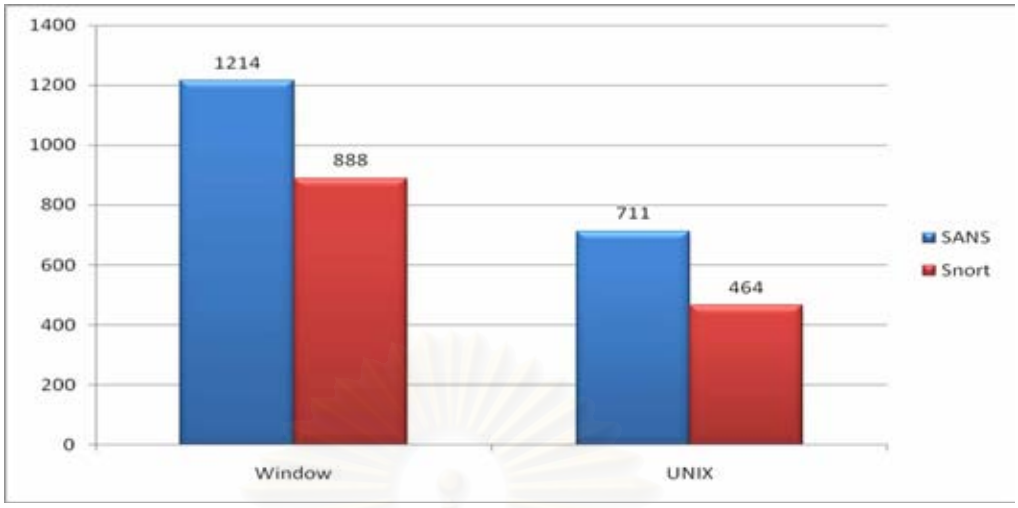
ส่วนลักษณะความเสียหายที่มีผลกระทบต่อความเสียหายมากที่สุดคือ ลักษณะความเสียหายที่เกิดจากการที่ระบบถูกล่วงละเมิด โดยพบว่ามีคะแนนเป็น 439 คะแนนและสนอร์ทสามารถป้องกันจุดอ่อนประเภทนี้ได้ 290 คะแนน คิดเป็น 66.1% ของคะแนนจุดอ่อนประเภทนี้

ผลลัพธ์ของการป้องกันจุดอ่อนตามลักษณะความเสียหายของระบบปฏิบัติการตระกูลยูนิกซ์แสดงไว้ในรูปที่ 5.10



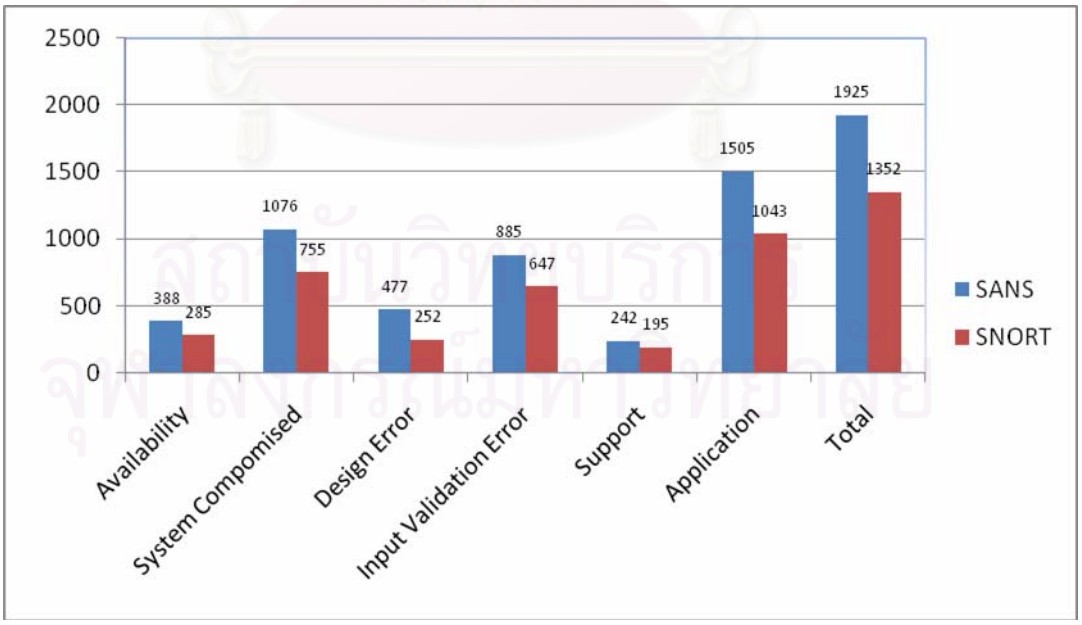
รูปที่ 5.10 ผลการป้องกันตามลักษณะความเสียหายของระบบปฏิบัติการตระกูลยูนิกซ์

ในภาพรวม สนอร์ทสามารถป้องกันจุดอ่อนซึ่งเป็นจุดอ่อนที่ถูกประกาศโดยสถาบันแซนส์ตั้งแต่ปี ค.ศ. 2000-2007 โดยเทียบกับจุดอ่อนที่มีการอ้างอิงถึงในกฎของสนอร์ท ที่ถูกประกาศออกมา ณ วันที่ 13 มกราคม พ.ศ. 2552 พบว่าในระบบปฏิบัติการตระกูลวินโดวส์ มีค่าดัชนีความเปราะบางของระบบ หรือคะแนนของจุดอ่อนที่คำนวณได้คิดเป็น 1214 คะแนน และคะแนนจากกฎของสนอร์ทคิดเป็น 888 คะแนน พบว่า สนอร์ทสามารถป้องกันจุดอ่อนได้ 73.2% ส่วนของระบบปฏิบัติการตระกูลยูนิกซ์ คำนวณค่าดัชนีความเปราะบางของระบบได้ 711 คะแนน และคะแนนจากกฎของสนอร์ทคิดเป็น 464 คะแนน พบว่า สนอร์ทสามารถป้องกันจุดอ่อนได้ 65.3% ดังรูปที่ 5.11



รูปที่ 5.11 ผลการป้องกันจุดอ่อนในภาพรวมของแต่ละระบบปฏิบัติการ

เมื่อนำคะแนนทั้งหมดของระบบปฏิบัติการตระกูลวินโดวส์และตระกูลยูนิกซ์มารวมกันเพื่อดูผลลัพธ์ในภาพรวมของค่าดัชนีความเปราะบางทั้งหมด พบว่ามีค่าดัชนีความเปราะบางของระบบทั้งหมด 1925 คะแนน และสนอร์ทสามารถป้องกันไปได้ 1325 คะแนน คิดเป็น 69% และคงเหลือค่าดัชนีความเปราะบางของระบบทั้งหมด 600 คะแนน โดยมีการแสดงภาพการป้องกันจุดอ่อนตามประเภทจุดอ่อนแบบต่างๆ ซึ่งนำมาเฉพาะจุดอ่อนที่มีระดับคะแนนสูงสุดสองอันดับดังรูปที่ 5.12



รูปที่ 5.12 ผลการป้องกันจุดอ่อนในภาพรวม

รูปที' 5.12 ผลการป้ องกันจุดอ่อนในภาพรวม

ในบทที่ 5 เป็น งกันจุดอ่อนตามประเภทของจุดอ่อน ตามจุดที่เกิดจุดอ่อน และตามลักษณะความเสียหาย ของสนอร์ทเมื่อเทียบกับจุดอ่อนที่ถูกประกาศตามรายงานของสถาบันแซนส์ และในบทที่ 6 จะทำการสรุปผลการวิจัยที่ได้ และเสนอข้อเสนอแนะที่เกี่ยวข้องกับงานวิจัยต่อไป

บทที่ 6

สรุปผลการวิจัยและข้อเสนอแนะ

จากการดำเนินการวิเคราะห์การวัดประสิทธิภาพของระบบตรวจจับการบุกรุก โดยวัดจากความสามารถในการป้องกันจุดอ่อนของระบบเครือข่ายตามรายงานของสถาบันแซนส์ซึ่งจากการรวบรวมจุดอ่อนทั้งหมดตั้งปีค.ศ. 2000-2007 ได้จุดอ่อนทั้งสิ้น 649 รายการ โดยแยกเป็นจุดอ่อนของระบบปฏิบัติการวินโดวส์ 377 รายการและจุดอ่อนของระบบปฏิบัติการตระกูลยูนิกส์ 272 รายการ จากนั้นนำมาเปรียบเทียบกับรายการจุดอ่อนจากกฎของสนอร์ทซึ่งเป็นระบบตรวจจับการบุกรุกประเภทหนึ่ง ที่มีการอ้างอิงรายการจุดอ่อนไปที่รายการซีวีอี และมีการสร้างเครื่องมือช่วยในการวิเคราะห์ ทำให้สามารถสรุปผลการวิจัย และเสนอแนะแนวทางเพื่อทำการวิจัยต่อไป ได้ดังนี้

6.1 สรุปผลการวิจัย

จากการศึกษาและวิจัยเพื่อประเมินผลการวิเคราะห์ประสิทธิภาพของระบบตรวจจับการบุกรุกโดยใช้สนอร์ทเป็นกรณีศึกษา สามารถสรุปผลการวิจัยดังนี้

1. จากการรวบรวม แบ่งกลุ่ม และให้คะแนนจุดอ่อน พบว่า ทั้งระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการตระกูลยูนิกส์ ประเภทของจุดอ่อนที่ทำให้เกิดค่าดัชนีความเปราะบางของระบบมากที่สุด คือจุดอ่อนที่เกิดจากการนำเข้าข้อมูลผิดพลาด รองลงมาคือจุดอ่อนที่เกิดจากความผิดพลาดในส่วนของการออกแบบระบบ และจากการเปรียบเทียบการป้องกันจุดอ่อนของสนอร์ท พบว่าสนอร์ท ป้องกันจุดอ่อนที่เกิดจากความผิดพลาดในการออกแบบระบบได้น้อยที่สุด

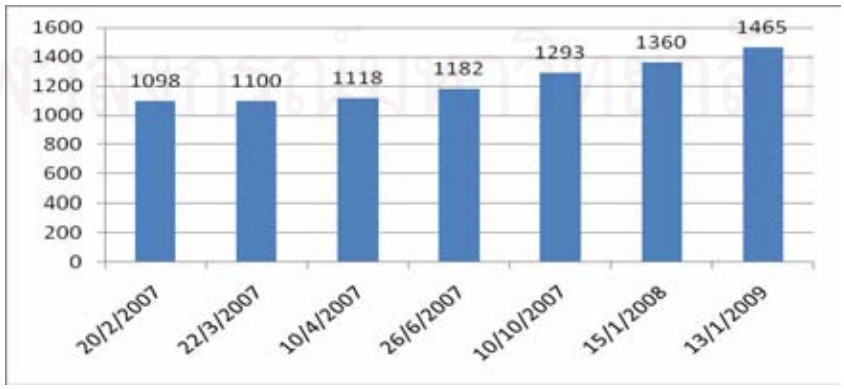
2. ทั้งในระบบปฏิบัติการวินโดวส์ และระบบปฏิบัติการตระกูลยูนิกส์พบว่า ตำแหน่งที่เกิดจุดอ่อนมากที่สุด คือ จุดอ่อนที่เกิดในส่วนของโปรแกรมประยุกต์ ซึ่งจากการเปรียบเทียบกับกฎของสนอร์ท พบว่าสนอร์ท สามารถป้องกันจุดอ่อนในส่วนนี้ ได้ดีพอสมควร คือ 71% ในระบบปฏิบัติการวินโดวส์ และ 67% ในระบบปฏิบัติการตระกูลยูนิกส์ และพบว่าจุดอ่อนของโปรแกรมประยุกต์ของระบบปฏิบัติการวินโดวส์ ที่สนอร์ทป้องกันได้น้อย คือ โปรแกรม Internet Explorer รองลงมาคือโปรแกรม MSSQL ส่วนในระบบปฏิบัติการตระกูลยูนิกส์ คือ โปรแกรม Firefox รองลงมาคือ โปรแกรม SendMail จากผลการทดลองพบว่า โปรแกรมที่ทำให้เหลือค่าดัชนีความเปราะบางของระบบมากที่สุด คือโปรแกรมประยุกต์ประเภท เบราเซอร์ ซึ่งจุดอ่อนที่ยังเหลือนี้ สามารถหาวิธีการอื่นมาป้องกันได้ เช่น การติดตั้ง Antivirus การดาวน์โหลด patch หรือ update เพื่อเสริมโปรแกรมนี้ให้มั่นคงขึ้น หรือการค้นหาวิธีการแก้ไขจุดอ่อนตัวนี้ ตามเว็บไซต์ของ

ผู้ให้บริการ หรือหลีกเลี่ยงโปรแกรมตัวนี้ หากไม่จำเป็นต้องใช้ หรือสามารถใช้ตัวอื่นที่มีจุดอ่อนน้อยกว่ามาทดแทน

3. ส่วนในเรื่องของจุดอ่อนที่ส่งผลกระทบต่อความเสียหายต่อระบบพบว่า จุดอ่อนที่ทำให้เกิดความเสียหายต่อระบบมากที่สุดคือ จุดอ่อนที่เกิดจากการล่วงละเมิดระบบ เช่นการพยายามเข้าเป็นระดับราก (root) เพื่อให้ได้สิทธิสูงสุดในระบบ รองลงมาคือจุดอ่อนที่เกิดจากการเสียความเป็นความลับ และจุดอ่อนที่เกิดจากการเสียสภาพพร้อมใช้งาน และสุดท้ายจุดอ่อนที่มีผลกระทบต่อระบบน้อยที่สุด คือจุดอ่อนที่เกิดจากการเสียสภาพบูรณภาพ ในส่วนของจุดอ่อนที่ยังเหลืออยู่นี้ ทางผู้ดูแล ต้องหาวิธีการอื่นๆ มาป้องกันจุดอ่อน เช่นการใช้ Firewall หรือการตั้ง Password ที่เหมาะสม เพื่อป้องกันการล่วงละเมิดระบบ

4. ในภาพรวม สนอร์ทสามารถป้องกันจุดอ่อนซึ่งเป็นจุดอ่อนที่ถูกประกาศโดยสถาบันแซนส์ ตั้งแต่ปี ค.ศ. 2000-2007 โดยเทียบกับจุดอ่อนที่มีการอ้างอิงถึงในกฎของสนอร์ท ที่ถูกประกาศออกมา ณ วันที่ 10 กุมภาพันธ์ พ.ศ. 2553 พบว่าสนอร์ท สามารถป้องกันจุดอ่อนในส่วนของระบบปฏิบัติการวินโดวส์ ได้ 73% และป้องกันจุดอ่อนในระบบปฏิบัติการตระกูลยูนิกซ์ได้ 65%

5. การประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก ขึ้นอยู่กับกฎของการตรวจจับ ดังนั้น จำเป็นต้องมีการตรวจสอบติดตั้งกฎอยู่เสมอ เพื่อให้การวิเคราะห์มีประสิทธิภาพ เพราะจุดอ่อนมีการประกาศออกมาอยู่เสมอ ดังนั้น กฎของการตรวจจับจำเป็นต้องได้รับการปรับปรุงอยู่เสมอด้วย ดังจะเห็นว่า กฎของสนอร์ท ที่ประกาศออกมา ณ วันที่ 13 มกราคม 2552 จะมีการระบุรายการซีวีอี มากกว่ากฎของสนอร์ทที่ถูกประกาศออกมา ณ วันที่ก่อนหน้านี้ เนื่องจากมีการเพิ่มเติมจุดอ่อนที่เกิดขึ้นใหม่เข้าไปด้วย ดังรูปที่ 6.1



รูปที่ 6.1 จำนวนรายการซีวีอีในกฎของสนอร์ท

6.2 ข้อจำกัดและข้อเสนอแนะ

1. การให้คะแนนจุดอ่อนและการจัดกลุ่มจุดอ่อน จำเป็นต้องทำการจัดทำด้วยตนเอง เนื่องจากต้องมีการวิเคราะห์รายละเอียดต่างๆ ของจุดอ่อนแต่ละตัวจึงยังไม่สามารถทำแบบอัตโนมัติ

2. จุดอ่อนที่ถูกประกาศออกมาโดยสถาบันแซนส์ อาจจะไม่เป็นจุดอ่อนที่ล่าสุด ดังเช่น ณ วันที่ 17 เมษายน พ.ศ. 2552 จุดอ่อนล่าสุดของสถาบันแซนส์ ยังคงเป็นจุดอ่อนของปี ค.ศ. 2007 ดังนั้นอาจทำให้การวิเคราะมีการคลาดเคลื่อนไปบ้าง

3. การวิเคราะห์ประสิทธิภาพของระบบตรวจจับการบุกรุกโดยใช้สนอร์ทเป็นกรณีศึกษานั้น เป็นการวิเคราะห์โดยเปรียบเทียบจากกฎของสนอร์ทเท่านั้น ไม่ได้มีการทำการติดตั้งและตรวจจับการบุกรุกในระบบเครือข่ายจริงๆ

4. สนอร์ทเองก็มีจุดอ่อนดังภาคผนวก ข จึงควรมีการป้องกันจุดอ่อนของสนอร์ทเองด้วย

6.3 งานวิจัยในอนาคต

จากงานวิจัยนี้ ยังมีประเด็นที่สามารถนำมาวิจัยได้ต่อเนื่องได้ ดังนี้

1. ในการวิเคราะห์ประสิทธิภาพของระบบตรวจจับการบุกรุก เพื่อให้ได้ผลที่ถูกต้องมากยิ่งขึ้น ควรจะมีการใช้ระบบตรวจจับการบุกรุกตัวอื่นมาวิเคราะห์เปรียบเทียบด้วย

2. ทำการวิเคราะห์ประสิทธิภาพของระบบตรวจจับการบุกรุก โดยดูจากลักษณะที่ละเอียดย่อยมากขึ้น เช่นจุดอ่อนตามประเภทของโปรแกรมที่ใช้ เป็นต้น

3. ปรับปรุงความสามารถของเครื่องมือให้ทำงานอย่างอัตโนมัติครอบคลุมนับแต่การสืบค้นซีวีอีจากกฎของสนอร์ท และจากเวปไซต์ของสถาบันแซนส์ เพื่อสะดวกต่อการนำไปใช้งานโดยผู้ดูแลระบบ

4. มีการพัฒนาเครื่องมือในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุกให้เป็นรูปแบบ Web-Based เพื่อให้ผู้ใช้งานสามารถใช้งานได้สะดวกยิ่งขึ้น

รายการอ้างอิง

[1] SANS. (2009). Top 20 Vulnerabilities [Online]. Available from: http://www.sans.org [1 Febuary 2009]

[2] Sourcefire Inc. (2009). Snort [Online]. Available from: http://www.snort.org [1 Febuary 2009]

[3] Bishop, M. (2005). Introduction to Computer Security. New York : Addision-Wesly.

[4] MITRE. (2009). Common Vunerability and Exposure [Online]. Available from: http://cve.mitre.org [1 Febuary 2009]

[5] NIST. (2009). National Vulnerability Database [Online]. Available from: http://nvd.nist.gov [1 Febuary 2009]

[6] OSVDB. (2008). Open Source Vulnerability Database [Online]. Available from: http://osvdb.org [1 July 2008]

[7] SecurityFocus. (2008). Bugtraq [Online]. Available from: http://www.securityfocus.com/bid [1 July 2008]

[8] Rehman, R.U. (2003). Advanced IDS Techniques Using Snort , Apache, MySQL, PHP and ACID. New York: Prentice Hall PTR.

[9] Sourcefire Inc, Roesch, M. and Green, C. (2007). SNORT User Manual – SNORT Release: 2.6.0 [Online]. Available from: http://www.snort.org/docs [1 July 2007]

[10] Sourcefire Inc. (2009). Snort rules [Online]. Available from: http://cvs.sourceforge.net/ [1 Febuary 2009]

[11] Savage, P. (2007). Snort Inline [Online]. Available from: http://linuxgazette.net [1 July 2007]

[12] Boyer, R. S. and Moore, J. S. (1997). A fast stringsearching algorithm. Communications of the Association for Computing Machinery 1977, p. 762-772

[13] Nalneesh Gaur. (2007). Snort: Planning IDS for Your Enterprise [Online]. Available from: http://www.linuxjournal.com/ [1 July 2007]

[14] Sourcefire Inc. (2007). Discover. Determine. Defend [Online] Available from: http://www.snort.org/vrt [1 July 2007]

[15] Wita , R., Teng-Amnuay, T., Anchanon, K. and Janluechai, P. (2005) A Framework for Application Survivability in Vunerability Operational Environment. The Workshop of International Conferences on Computation Intelligence and Security 2005, p. 120-125.

[16] Ross, A. (2001). Security Engineering: A Guide to Building Dependable Distributed System. New York: Wiley Computer Publishing.

[17] Butler, S. (2002). Security Attribute Evaluation Method: A Cost-Benefit Approach. Proceedings of the 24th International Conference on Software Engineering 2002, p. 232-240.

[18] Roesh, M. (1999). Snort-Lightweight Intrusion Detection for Networks. Proceedings of LISA '99: 13th Systems Administration Conference , p.55-60.

[19] Landwer, C.E. and et al (1994). A Taxonomy of Computer Program Security Flaws. ACM Computing Surveys 26, p. 211-254.

[20] Wita, R. and Teng-Amnuay, Y. (2005). Vulnerability Profile for Linux. 19th International Conference on Advanced Information Networking and Applications, p. 953-958

ภาคผนวก

ภาคผนวก ก

ผลงานตีพิมพ์

ส่วนหนึ่งของงานวิทยานิพนธ์นี้ได้รับการตีพิมพ์เป็นบทความวิชาการในหัวเรื่อง “Effectiveness Analysis of IDS Using Vulnerability Scores” โดยธนัชพร นพเกื้อ และยรรยง เต็งอำนวย ในงานประชุมวิชาการ “Proceedings of NCIT 2008 The 2nd National Conference on Information Technology 2008 (NCIT 2008)” ซึ่งจัดขึ้น ณ โรงแรมแกรนด์ เมอรีคิว กรุงเทพมหานคร ประเทศไทย ระหว่างวันที่ 6-7 พฤศจิกายน 2551

ภาคผนวก ข

รายการจุดอ่อนที่มีในสนอร์ท

CVE-2001-0669 Various Intrusion Detection Systems (IDS) including (1) Cisco Secure Intrusion Detection System, (2) Cisco Catalyst 6000 Intrusion Detection System Module, (3) Dragon Sensor 4.x, (4) Snort before 1.8.1, (5) ISS RealSecure Network Sensor 5.x and 6.x before XPU 3.2, and (6) ISS RealSecure Server Sensor 5.5 and 6.0 for Windows, allow remote attackers to evade detection of HTTP attacks via non-standard "%u" Unicode encoding of ASCII characters in the requested URL.

CVE-2001-1558 Unknown vulnerability in IP defragmenter (frag2) in Snort before 1.8.3 allows attackers to cause a denial of service (crash).

CVE-2002-0115 Snort 1.8.3 does not properly define the minimum ICMP header size, which allows remote attackers to cause a denial of service (crash and core dump) via a malformed ICMP packet.

CVE-2002-1970 SnortCenter 0.9.5, when configured to push Snort rules, stores the rules in a temporary file with world-readable and world-writable permissions, which allows local users to obtain usernames and passwords for the alert database servers.

CVE-2003-0033 Buffer overflow in the RPC preprocessor for Snort 1.8 and 1.9.x before 1.9.1 allows remote attackers to execute arbitrary code via fragmented RPC packets.

CVE-2003-0209 Integer overflows in the TCP stream reassembly module (stream4) for Snort 2.0 and earlier allows remote attackers to execute arbitrary code via large sequence numbers in packets, which enable a heap-based

buffer overflow.

CVE-2003-1379 clarkconnectd in ClarkConnect Linux 1.2 allows remote attackers to obtain sensitive information about the server via the characters (1) A, which reveals the date and time, (2) F, (3) M, which reveals 'ifconfig' information, (4) P, which lists the processes, (5) Y, which reveals the snort log files, or (6) b, which reveals /var/log/messages.

CVE-2004-2652 The DecodeTCPOptions function in decode.c in Snort before 2.3.0, when printing TCP/IP options using FAST output or verbose mode, allows remote attackers to cause a denial of service (crash) via packets with invalid TCP/IP options, which trigger a null dereference.

CVE-2005-3252 Stack-based buffer overflow in the Back Orifice (BO) preprocessor for Snort before 2.4.3 allows remote attackers to execute arbitrary code via a crafted UDP packet.

CVE-2006-0839 The frag3 preprocessor in Sourcefire Snort 2.4.3 does not properly reassemble certain fragmented packets with IP options, which allows remote attackers to evade detection of certain attacks, possibly related to IP option lengths.

CVE-2006-2769 The HTTP Inspect preprocessor (http_inspect) in Snort 2.4.0 through 2.4.4 allows remote attackers to bypass "uricontent" rules via a carriage return (\r) after the URL and before the HTTP declaration.

CVE-2006-6931 Algorithmic complexity vulnerability in Snort before 2.6.1, during predicate evaluation in rule matching for certain rules, allows remote attackers to cause a denial of service (CPU consumption and detection outage) via crafted network traffic, aka a "backtracking attack."

CVE-2007-0251 Integer underflow in the DecodeGRE function in src/decode.c in Snort

2.6.1.2 allows remote attackers to trigger dereferencing of certain memory locations via crafted GRE packets, which may cause corruption of log files or writing of sensitive information into log files.

CVE-2006-5276 Stack-based buffer overflow in the DCE/RPC preprocessor in Snort before 2.6.1.3, and 2.7 before beta 2; and Sourcefire Intrusion Sensor; allows remote attackers to execute arbitrary code via crafted SMB traffic.

CVE-2007-1398 The frag3 preprocessor in Snort 2.6.1.1, 2.6.1.2, and 2.7.0 beta, when configured for inline use on Linux without the ip_conntrack module loaded, allows remote attackers to cause a denial of service (segmentation fault and application crash) via certain UDP packets produced by send_morefrag_packet and send_overlap_packet.

CVE-2008-1804 Preprocessors/spp_frag3.c in Sourcefire Snort before 2.8.1 does not properly identify packet fragments that have dissimilar TTL values, which allows remote attackers to bypass detection rules by using a different TTL for each fragment.

CVE-2009-1031 Directory traversal vulnerability in the FTP server in Rhino Software Serv-U File Server 7.4.0.1 allows remote attackers to create arbitrary directories via a \.. (backslash dot dot) in an MKD request.

ประวัติผู้เขียนวิทยานิพนธ์

นางสาว ธนัชพร นพเกื้อ เกิดเมื่อวันที่ 25 ตุลาคม พ.ศ. 2526 ที่จังหวัดชุมพร สำเร็จการศึกษาระดับปริญญาตรี วิทยาศาสตรบัณฑิต จากภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาตร์ มหาวิทยาลัยสงขลานครินทร์ ในปีการศึกษา 2548 จากนั้นเข้าศึกษาต่อในหลักสูตร วิทยาศาสตรมหาบัณฑิต ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2549