การประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์โดยการเพิ่มความแข็งแกร่งกับการใช้แอลเอสเอ็ม

นางสาว รัศมีทิพย์ วิตา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2546
ISBN 974-17-4544-3

EVALUATION AND COMPARISON OF VULNERABILITY PREVENTION IN LINUX SYSTEM BASED ON HARDENING AND LSM

Miss Ratsameetip Wita

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 2003
ISBN 974-17-4544-3

หัวข้อวิทยานิพนธ์	การประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์โดยการเพิ่มความแข็งแกร่งกับการใช้แอลเอสเอ็ม
โดย	นางสาว รัศมีทิพย์ วิตา
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร.ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์)

..... อาจารย์ที่ปรึกษา
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... กรรมการ
(อาจารย์ จารุมาตร ปิ่นทอง)

..... กรรมการ
(อาจารย์ ธงชัย โรจน์กังสดาล)

รัศมีทิพย์ วิตา : การประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์โดยการเพิ่มความแข็งแกร่งกับการใช้แอลเอสเอ็ม. (EVALUATION AND COMPARISON OF VULNERABILITY PREVENTION IN LINUX SYSTEM BASED ON HARDENING AND LSM) อ. ที่ปรึกษา: อ.ดร.ยรรยง เต็งอำนวย, 101 หน้า. ISBN 974-17-4544-3.

ความผิดพลาดของการรักษาความปลอดภัยในการทำงานของระบบคอมพิวเตอร์และสารสนเทศในองค์กร หมายถึงความเสียหายอย่างมากสำหรับองค์กร ดังนั้นจึงต้องมีการป้องกันความผิดพลาดที่อาจเกิดขึ้น รวมถึงการป้องกันการโจมตีจากผู้ไม่หวังดีต่อระบบ เพื่อลดความเสี่ยงต่อความเสียหายที่อาจเกิดขึ้น

จากปัญหาดังกล่าวเป็นแรงผลักดันให้มีแนวคิดและงานวิจัยในการป้องกันความเสียหายดังกล่าว โดยการเพิ่มความสามารถในด้านการรักษาความปลอดภัยให้กับระบบปฏิบัติการ เมื่อศึกษาจากระบบปฏิบัติการลินุกซ์ พบว่ามี 2 แนวทาง แนวทางหนึ่งคือ การเสริมความแข็งแกร่งให้กับระบบ ส่วนอีกแนวทางหนึ่งคือเปลี่ยนแปลงการควบคุมการเข้าถึงของระบบ ด้วยวิธีที่มีประสิทธิภาพสูงขึ้น เพื่อลดช่องทางในการโจมตีระบบ

ในงานวิจัยนี้ จึงได้ทำการวิเคราะห์ความสามารถในการป้องกันจุดอ่อนในรูปแบบต่างๆ โดยทำการคัดเลือกและจัดกลุ่มให้กับรายการของจุดอ่อนที่พบในระบบลินุกซ์ที่มีการรวบรวมในรายการซีวีอี และทำการวิเคราะห์การทำงานของการเสริมความปลอดภัยในระบบลินุกซ์ในการเพิ่มความแข็งแกร่งและการใช้แอลเอสเอ็ม ซึ่งเป็นโครงร่างสำหรับการเพิ่มเติมการควบคุมการเข้าถึงของลินุกซ์ เพื่อทำการประเมินลักษณะของจุดอ่อนที่วิธีการเสริมความปลอดภัยในแต่ละแบบสามารถป้องกันได้ ซึ่งจากการวิจัย สามารถสรุปได้ว่า การเสริมความแข็งแกร่ง และการใช้แอลเอสเอ็ม มีความสามารถในการป้องกันจุดอ่อนในลักษณะที่ต่างกัน โดยการเสริมความแข็งแกร่ง สามารถป้องกันจุดอ่อนได้มากกว่า

ภาควิชา.....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต.....
สาขาวิชา....วิทยาศาสตร์คอมพิวเตอร์..... ลายมือชื่ออาจารย์ที่ปรึกษา.....
ปีการศึกษา 2546

4470491421 : MAJOR COMPUTER SCIENCE

KEY WORD: LINUX SECURITY / VULNERABILITY CLASSIFICATION / SECURITY ENHANCEMENT / OS HARDENING

RATSAMEETIP WITA : EVALUATION AND COMPARISON OF VULNERABILITY PREVENTION IN LINUX SYSTEM BASED ON HARDENING AND LSM. THESIS ADVISOR : DR. YUNYONG TENG-AMNUAY, 101 pp. ISBN 974-17-4544-3.

Security flaws in computer and information systems in an organization mean a serious damage for the organization. The prevention of the system vulnerabilities and also the attack activities have to be concerned to reduced the risk of the damage.

From the stated reason, many researches and methods have been developed to prevent the system security vulnerability by extended the security parts in the operating system. In Linux system, there're 2 main methods: Hardening the operating system with suitable configuration, and extending the system access control with more effective methodology.

Consequently, this research is aimed to analyze and evaluate the vulnerability prevention ability of different protection methods. First, Linux known-vulnerability from CVE list have been selected and categorized. Then, the architecture and functionality of OS hardening and LSM which are selected protection methods have been analyzed. Then, the evaluation of the vulnerability characteristics that can be reduced by applying each method have been made. The research reveals that each method can prevent different vulnerability characteristic In overall, the OS hardening prevent more number of vulnerability than LSM.

Department.....Computer Engineering..... Student's signature
Field of study.....Computer Science..... Advisor's signature
Academic year 2003 .....

กิตติกรรมประกาศ

วิทยานิพนธ์นี้จะไม่สามารถสำเร็จลุล่วงไปด้วยดี หากไม่ได้รับคำปรึกษาแนะนำอันเป็นประโยชน์ยิ่งจาก อ ดร.ยรรยง เต็งอำนวย อ ที่ปรึกษาวิทยานิพนธ์ รวมถึง ผศ. ดร ทวิตีย์ เสนียวงศ์ ณ อยุธยา อ ดร. ณัฐวุฒิ หนูไพโรจน์ และ อ จารุมาตร ปิ่นทอง อาจารย์ผู้ร่วมดำเนินโครงการวิจัย เรื่อง Object-Oriented Design and Development for Distributed Application ซึ่งจุดเริ่มต้นของวิทยานิพนธ์นี้

ขอขอบคุณ คุณณิศรา ศิริพรกุลทรัพย์ คุณกิตติพิชญ์ คุปตะวาณิช คุณรังสรรค์ เกียรติ์ภานนท์ และคุณกัน อุตตะเดช เพื่อน ๆ ผู้ร่วมวิจัยในโครงการ สำหรับความช่วยเหลือทั้งด้านทางเทคนิค และกำลังใจ

ขอบคุณห้อง ISEL และห้อง SE และสมาชิกทั้ง 2 ห้อง สำหรับอุปกรณ์ที่ใช้ประกอบการวิจัย และ บรรยากาศดี ๆ ของการทำงานวิจัย

ขอขอบคุณคุณพ่อ คุณแม่ และครอบครัว สำหรับการสนับสนุน และความเข้าใจในทุก ๆ เรื่อง รวมถึงคำแนะนำดีๆ ที่ใช้ได้ผลเสมอมา และขอขอบคุณกำลังใจอื่น ๆ ที่ทำให้การทำงานวิจัยสำเร็จลงได้ด้วยดี

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ เป็นหัวข้อที่มีการพูดถึงและเป็นที่สนใจกันมากในปัจจุบัน เนื่องจากความต้องการที่จะป้องกันข้อมูลและระบบการดำเนินงานภายในองค์กร จากการโจมตี จึงทำให้มีการพัฒนาวิธีการในการรักษาความปลอดภัยให้กับระบบ ทั้งที่เป็นฮาร์ดแวร์ และซอร์ฟแวร์ออกมามากมาย แต่ก็ยังคงไม่สามารถป้องกันระบบให้มีความปลอดภัยร้อยเปอร์เซ็นต์ ทั้งนี้ เนื่องมาจากทางผู้บุกรุกมีการคิดค้นวิธีการใหม่ๆขึ้นตลอดเวลา โดยส่วนใหญ่อาศัยช่องทางในการโจมตีจากจุดอ่อน (Vulnerability) ของซอร์ฟแวร์ หรือแม้กระทั่งของระบบปฏิบัติการ เพื่อทำให้สามารถแทรกแซงการทำงานของซอร์ฟแวร์ต่างๆ จนทำให้ระบบและหรือข้อมูลเกิดความเสียหายได้ และถ้าหากระบบปฏิบัติการซึ่งทำหน้าที่ในการดูแลและประสานการทำงานระหว่างซอร์ฟแวร์กับทรัพยากรระบบสามารถถูกแทรกแซงการทำงานแล้ว ถึงแม้จะมีการใช้ซอร์ฟแวร์ที่มีประสิทธิภาพเพียงใดก็ไม่สามารถป้องกันระบบจากการโจมตีได้ [1]

จากปัญหาดังกล่าวเป็นแรงผลักดันให้มีแนวคิดและงานวิจัยในการเพิ่มความแข็งแกร่งให้กับระบบปฏิบัติการ จากการศึกษาเบื้องต้นพบว่า ระบบปฏิบัติการที่ได้รับความสนใจในการพัฒนาคือ ระบบปฏิบัติการลินุกซ์ เนื่องจากเป็นระบบเปิด (Open System) ที่กำลังมีการพัฒนาในด้านต่างๆ และมีการอนุญาตให้บุคคลทั่วไปสามารถเป็นผู้พัฒนาระบบได้ ซึ่งแนวคิดในการเพิ่มความสามารถในด้านการรักษาความปลอดภัยให้กับระบบปฏิบัติการลินุกซ์ สามารถแบ่งออกได้เป็น 2 แนวทางใหญ่ๆ คือ

แนวคิดที่ที่เชื่อว่า ระบบลินุกซ์นั้นได้มีการจัดหาการรักษาความปลอดภัยที่เพียงพออยู่แล้ว แต่เนื่องจากระบบลินุกซ์เป็นระบบที่มีบริการมาก ในการใช้งานจริงจึงต้องมีการปรับแต่งระบบ (configuration) ให้เหมาะสมกับงาน การปรับแต่งระบบที่ไม่เหมาะสม และหรือไม่มีการปรับปรุงการแก้ไขระบบจากผู้ผลิต (OS patch) ทำให้ระบบมีจุดอ่อนที่สามารถโจมตี หรือใช้เป็นช่องทางการโจมตีระบบได้ จึงมีการเสนอเป็นข้อแนะนำในการปรับแต่งระบบเพื่อลดจุดอ่อน และเพิ่มความแข็งแกร่งให้กับระบบปฏิบัติการ (OS Hardening) [2]

แนวคิดที่เชื่อว่า รูปแบบของการควบคุมการเข้าถึง (Access Control) ที่มีอยู่ในระบบลินุกซ์นั้น ไม่เพียงพอต่อความต้องการในการรักษาความปลอดภัย และสามารถทำให้ระบบถูกล่วงละเมิดจากผู้บุกรุกได้ จึงมีการงานวิจัยที่เสนอแนวทางการเพิ่มเติมการรักษาความปลอดภัยโดยอาศัยการบังคับใช้การควบคุมการเข้าถึงแบบต่างๆ [3]

แต่เนื่องจากการเสริมระบบในส่วนของการควบคุมการเข้าถึง ซึ่งต้องมีแก้ไขการทำงานส่วนเคอร์เนล (Kernel) ของระบบลินุกซ์นั้นยากต่อการปรับแต่งระบบ และในทั้ง 2 แนวทาง ยังไม่มีการระบุระดับวามสามารถในการป้องกันจุดอ่อนที่เกิดจากระบบ ทำให้ยากในการเลือกใช้วิธีการเสริมความปลอดภัยให้มีความเหมาะสมกับการทำงานในระบบ ดังนั้น ผู้วิจัยจึงมีความคิดที่จะทำการศึกษาและวิเคราะห์การทำงาน และผลของการดำเนินการตามทั้ง 2 แนวคิด เพื่อประเมินและเปรียบเทียบความสามารถในการรักษาความปลอดภัยของระบบ โดยจะทำการประเมินจากความสามารถในการป้องกัน หรือแก้ไขจุดอ่อนแบ่งตามประเภทและเป็นจุดอ่อนที่มีอยู่ในรายการซีวีอี (CVE List) เพื่อเป็นข้อมูลในการประกอบการตัดสินใจของผู้ดูแลระบบในการเลือกใช้วิธีการเพิ่มความปลอดภัยที่เหมาะสมกับความต้องการของแต่ละระบบต่อไป

1.2 วัตถุประสงค์ของการวิจัย

เพื่อทำการวิเคราะห์และเปรียบเทียบระดับความสามารถในการป้องกันจุดอ่อนที่สามารถเกิดขึ้นได้ในระบบ โดยการปรับปรุงระบบปฏิบัติการลินุกซ์ ที่อาศัยหลักการของ การสร้างความแข็งแกร่ง กับการปรับปรุง โดยใช้แนวคิดในกลุ่มของแอลเอสเอ็ม

1.3 ขอบเขตของการวิจัย

ในงานวิจัยนี้ ได้มีการกำหนดขอบเขตไว้ดังต่อไปนี้ในการวิจัยนี้

1. จะทำการศึกษาจุดอ่อนที่เกิดขึ้นกับระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชั่น 7.2 (Redhat Linux version 7.2)บนเครื่องไมโครคอมพิวเตอร์
2. รายการจุดอ่อนที่พบจากระบบ อ้างอิงจากจุดอ่อนในรายการซีวีอีรุ่น 20020625 [4]
3. ตัวปรับแต่งล่าสุดที่ใช้กับระบบโดยวิธีการเสริมความแข็งแกร่งนั้น จะทำการดาวน์โหลดจากเวบไซต์ของบริษัทเรดแฮทและที่มีการแนะนำในรายการซีวีอีเท่านั้น
4. ทำการศึกษาตัวเสริมด้านความปลอดภัยที่สนับสนุนการทำงานตามโครงร่างแอลเอสเอ็มเท่านั้น
5. ตัวเสริมด้านความปลอดภัยจะทำการดาวน์โหลดจากเวบไซต์ที่ทำการวิจัย

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. รายการจุดอ่อนที่สามารถเกิดขึ้นกับระบบที่มีการจัดแบ่งกลุ่มตามประเภทของจุดอ่อน
2. ข้อมูลความสามารถในการป้องกันจุดอ่อนจากการใช้วิธีการเสริมความแข็งแกร่งให้กับระบบ
3. ข้อมูลความสามารถในการป้องกันจุดอ่อนจากการใช้วิธีของตัวเสริมความปลอดภัยที่มีโครงสร้างตามแอลเอสเอ็ม

1.5 วิธีดำเนินการวิจัย

1. การกำหนดขั้นตอนและวิธีการดำเนินงาน มีรายละเอียดดังนี้
2. ศึกษาวิเคราะห์จุดอ่อนในรายการซีวีอีที่เกิดขึ้นกับระบบปฏิบัติการลินุกซ์
3. จัดกลุ่มของจุดอ่อน ตามลักษณะที่ทำให้เกิดจุดอ่อน
4. ศึกษาขั้นตอนการดำเนินงานตามวิธีการเสริมความแข็งแกร่ง
5. วิเคราะห์ลักษณะการทำงานของระบบเมื่อดำเนินการตามวิธีการเสริมความแข็งแกร่งว่าสามารถป้องกันการเกิดจุดอ่อนที่สามารถเกิดขึ้นได้เพียงใด
6. ศึกษาการทำงานของแนวคิดกลุ่มแอลเอสเอ็ม โดยแบ่งออกตามกลุ่มการนำแนวคิดไปพัฒนา ซึ่งประกอบด้วย เอสอีลินุกซ์ แอลไอดีเอส และดีทีอี
7. วิเคราะห์ลักษณะการทำงานของระบบเมื่อดำเนินการตามแนวคิดของกลุ่มแอลเอสเอ็มว่าสามารถป้องกันการเกิดจุดอ่อนที่สามารถเกิดขึ้นได้เพียงใด
8. ทำการประเมินและเปรียบเทียบ ความสามารถในการป้องกันการเกิดจุดอ่อนของแนวคิดทั้ง 2 วิธีเทียบกับจุดอ่อนที่มีในรายการซีอีวี
9. สรุปผลการวิจัย และจัดทำรายงานวิทยานิพนธ์

1.6 โครงสร้างวิทยานิพนธ์

ในบทที่ 2 จะกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง ส่วนในบทที่ 3 จะกล่าวถึงรายละเอียดการดำเนินการวิจัย ซึ่งจะประกอบด้วย การคัดกรองข้อมูลจุดอ่อนที่เกิดขึ้นในระบบปฏิบัติการลินุกซ์ การปรับแต่งรูปแบบการจัดกลุ่มจุดอ่อน การให้คะแนนของจุดอ่อน การวิเคราะห์ความสามารถ ในการป้องกันจุดอ่อนของการเสริมความแข็งแกร่ง การวิเคราะห์ความสามารถในการป้องกันจุดอ่อนของโครงสร้างแอลเอสเอ็ม และประเมินผลการป้องกันจุดอ่อนที่ได้ของแต่ละวิธี บทที่ 4 กล่าวถึงผลการวิจัย ซึ่งเป็นค่าที่ได้จากการประเมินความสามารถในการป้องกันจุดอ่อนเป็นค่าดัชนีความอ่อนแอของลินุกซ์เมื่อดำเนินการตามวิธีต่างๆ โดยทำการสรุปการวิจัยและข้อเสนอแนะไว้ในบทที่ 5

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

จากการศึกษาเบื้องต้น พบว่าในงานวิจัยนี้ จำเป็นต้องทำการศึกษาแนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้องต่าง ๆ สามารถแบ่งออกเป็น 4 กลุ่มด้วยกัน คือ

1. จุดอ่อนที่สามารถเกิดขึ้นในระบบ
2. การจัดกลุ่มของจุดอ่อนและข้อผิดพลาด
3. การเพิ่มความปลอดภัยให้กับระบบปฏิบัติการ
4. การประเมินความสามารถของระบบ

ซึ่งในแต่ละกลุ่ม มีรายละเอียดของแนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้องต่างๆ ดังต่อไปนี้

2.1 จุดอ่อนที่สามารถเกิดขึ้นในระบบ (Vulnerability and Exposure)

จุดอ่อน (Vulnerability) คือช่องทางที่เป็นรอยรั่วของระบบของระบบทั่ว ๆ ไป ที่ยอมให้มีการโจมตีระบบผ่านทางรอยรั่วนั้นๆสามารถทำให้ระบบเกิดความเสียหายขึ้นได้ จุดอ่อน สามารถเกิดขึ้นได้กับทุกส่วนของระบบ เช่น โปรแกรมทั่วๆ ไปที่ใช้งานในระบบ โปรแกรมรักษาความปลอดภัยของระบบ หรือแม้กระทั่งระบบปฏิบัติการ

โอกาสเสี่ยงภัย (Exposure) เป็นจุดอ่อนของเฉพาะระบบ อาจเกิดจากความขัดแย้งของนโยบายความปลอดภัย ไม่ได้มีผลกระทบต่อระบบโดยทั่ว ๆ ไป แต่ผลกระทบที่เกิดกับระบบเหมือนกับจุดอ่อน คือสามารถทำให้ระบบเกิดความเสียหายในรูปแบบต่างๆ

ซีวีอี [4] (CVE - Common Vulnerability and Exposure) เป็นงานวิจัย ที่ริเริ่มขึ้นเมื่อปี 1999 โดย มิเตอร์ (MITRE) ร่วมกับส่วนราชการ สถานศึกษาและบริษัท เพื่อสร้างกลไกในการระบุค้นหา และแก้ไขจุดอ่อนต่างๆของซอฟต์แวร์ ให้มีความรวดเร็วและมีประสิทธิภาพมากขึ้น และเนื่องจากการประสบปัญหาในการตั้งชื่อที่ใช้ระบุปัญหาด้านความปลอดภัยในซอฟต์แวร์ ซึ่งสิ่งนี้เองทำให้เกิดความลำบากในการตรวจสอบ ควบคุม และแก้ไขจุดอ่อนและจุดอ่อนของระบบ ที่เกิดขึ้นเมื่อมีการใช้บริการ เครื่องมือ และฐานข้อมูลของจุดอ่อนที่แตกต่างกัน รวมไปถึงการประกาศการปรับปรุงของซอฟต์แวร์ ตัวอย่างเช่น จากตารางที่ 2.1 แสดงถึงความแตกต่างของการใช้ชื่อเพื่ออ้างถึงจุดอ่อน ชนิดเดียวกันที่เกิดขึ้นกับโปรแกรมซีจีไอของสมุดโทรศัพท์พีเอชเอฟ (phf phonebook CGI program) ในปี 1998 จากการใช้ชื่อเรียกที่ต่างกันนี้ ทำให้เกิดปัญหาในการทำความเข้าใจกับจุดอ่อน ที่เกิดขึ้นและการเลือกใช้เครื่องมือเพื่อป้องกันจุดอ่อน ที่เหมาะสม

จากปัญหาความยุ่งยากที่เกิดขึ้น ทางมิเตอร์ จึงได้เริ่มทำการวิจัยเพื่อสร้างวิธีการที่จะเชื่อมความสัมพันธ์ระหว่างการเรียกชื่อที่ต่างกันของข้อบกพร่องชนิดเดียวกันในฐานข้อมูล หรือ

เครื่องมือที่ต่างกัน จึงทำให้เกิดแนวคิดรายการซีวีอี โดยรายการซีวีอีนี้ ทำหน้าที่เป็นลอจิกคัลบริดจ์ (Logical Bridge) เพื่อให้มีมาตรฐานในการอ้างอิงถึงข้อบกพร่องที่ตรงกัน โดยข้อมูลของจุดอ่อนและรายละเอียดจะถูกส่งจากบริษัท และหน่วยงานด้านความปลอดภัยต่างๆ เพื่อพิจารณาหาความสัมพันธ์ของจุดอ่อนที่ได้มาจากแต่ละแหล่ง และพิจารณาเทียบกับนิยามของจุดอ่อนของซีวีอี โดยคณะทำงานที่จัดตั้งขึ้น จนกระทั่งได้ข้อสรุป ก็จะทำการเพิ่มรายการของจุดอ่อนที่ผ่านการพิจารณาเข้าสู่รายการซีวีอี ซึ่งรายละเอียดและขั้นตอนในกระบวนการพิจารณาจะไม่ขอกล่าวถึงในที่นี้

ตารางที่ 2.1 แสดงการใช้ชื่อเพื่ออ้างถึงจุดอ่อนที่เกิดขึ้นกับโปรแกรมซีจีไอของสมุดโทรศัพท์พีเอชเอฟในปี ค.ศ.1998

Organization	Name referring to vulnerability
AXENT (now Symantec)	Phf CGI allows remote command execution
Bindview	#107 – cgi-phf
Bugtraq	PHF Attacks – fun and games for the whole family
CERIAS	http_escshellcmd
CERT	CS-96.06.cgi_example_code
Cisco Systems	HTTP –cgi-phf
CyberSafe	Network: HTTP ‘phf’ attack
DARPA	0x00000025 = HTTP PHF attack
OBM ERS	ERS-SVA-E01-1996:002.1
ISS	http—cgi-phf
Symantec	#180 HTTP server CGI example code compromises http server
Security Focus	#629—phf Remote Command Execution Vulnerability

ในส่วนของการตั้งชื่อเพื่อใช้อ้างอิงเป็นมาตรฐานของจุดอ่อนของรายการซีวีอีนั้น จะมีการกำหนดหมายเลข เพื่อใช้ในการอ้างถึงที่เป็นมาตรฐาน คำอธิบายจุดอ่อน และข้อมูลอ้างอิง โดย ซีเอนเอ (CNA - CVE Candidate Numbering Authority) หมายเลขแคนดิเดตที่มีการกำหนด มีรูปแบบดังนี้ CAN-xxxx-yyyy ซึ่งเป็นเลขที่ประกอบด้วยปีที่ออกหมายเลขแคนดิเดต และหมายเลขเฉพาะที่ไม่ซ้ำเป็นลำดับของแคนดิเดตที่ออกในปีนั้น และจุดอ่อนที่ผ่านการพิจารณาจาก CVE Editoral Board จะทำการเพิ่มรายการนั้นเข้าสู่รายการซีวีอี โดยมีการกำหนดชื่อซีวีอีให้กับจุดอ่อนโดยอ้างอิงจากหมายเลขแคนดิเดต อยู่ในรูปแบบดังนี้ CVE-xxxx-yyyy ซึ่ง xxxx เป็นปีที่ออกหมายเลขแคนดิเดต และ yyyy เป็นลำดับของแคนดิเดตที่ออกในปีนั้น ดังรูปที่ 2.1

```
Cve Name    :CVE-1999-0067
Description:CGI phf program allows remote command
            execution through shell metacharacters.
Reference   :CERT:CA-96.06.cgi_example_code,XF:http-
            cgi-phf,BID:629
```

รูปที่ 2.1 แสดงตัวอย่างข้อมูลของจุดอ่อนที่ปรากฏในรายการซีวีอี

จากรูปที่ 2.1 เป็นตัวอย่างการตั้งชื่อและคำอธิบายจุดอ่อนในรายการซีวีอี เพื่ออ้างถึงจุดอ่อนที่เกิดขึ้นกับโปรแกรมซีจีไอของสมุดโทรศัพท์พีเอชเอฟ

2.2 การจัดกลุ่มของจุดอ่อนและข้อผิดพลาด (Vulnerability and flaw taxonomy)

การจัดกลุ่มให้กับจุดอ่อน หรือข้อผิดพลาดของระบบ เป็นการแบ่งส่วนของจุดอ่อน ที่มีความเหมือนหรือคล้ายคลึงกันและการหาความสัมพันธ์กันระหว่างจุดอ่อน ในการจัดแบ่งกลุ่มให้กับจุดอ่อน มี 2 ส่วนใหญ่ๆ คือ ทำการรวบรวมคำสำคัญการศึกษาจุดอ่อนต่างๆ จัดกลุ่มสิ่งที่คล้ายคลึง หรือมีความสัมพันธ์กันไว้ด้วยกัน และ โดยใช้พื้นฐานทฤษฎีการจัดแบ่งกลุ่ม ที่มีประสิทธิภาพ

2.2.1 คุณลักษณะที่เหมาะสมของการจัดแบ่งกลุ่ม

Edward G. Amoroso [5] ได้ทำการกล่าวถึงลักษณะเฉพาะที่เหมาะสมของการแบ่งจุดอ่อนไว้เป็นแนวทางในการจัดแบ่งกลุ่มไว้ดังนี้

1. ไม่มีเหตุการณ์เกิดร่วม (Mutually exclusive)
2. มีความละเอียด (Exhaustive)
3. มีความชัดเจน (Unambiguous)
4. สามารถใช้ซ้ำได้ (Repeatable)
5. เป็นที่ยอมรับ (Accepted)
6. มีประโยชน์ (Useful)

2.2.2 งานวิจัย “Use of Taxonomy of Faults”

Aslam และคณะ [6] ได้ทำการกำหนดลักษณะการจัดกลุ่มของจุดอ่อน ที่เกิดขึ้นในระบบปฏิบัติการยูนิกซ์ โดยลักษณะการจัดกลุ่มที่ในงานวิจัยนี้ได้กำหนดขึ้น ประกอบด้วย 2 กลุ่ม คือ ความผิดพลาดที่เกิดจากการเขียนโปรแกรม ซึ่งจะเกิดขึ้นจากช่วงของการพัฒนาโปรแกรม และ

ความผิดพลาดที่เกิดจากการใช้งาน เกิดจากการติดตั้งโปรแกรมที่ไม่เหมาะสม หรือความไม่เข้ากันของระบบ กับโปรแกรมที่ติดตั้ง

2.2.3 งานวิจัย “A Taxonomy of Computer Program Security Flaws”

Lanwehr และคณะ [7] เห็นว่าลักษณะของข้อผิดพลาดในระบบงานคอมพิวเตอร์ต่างๆ มีลักษณะการทำงาน ลักษณะการเกิด ตำแหน่ง และลักษณะของความเสียหายที่เกิดขึ้นมีความคล้ายคลึงกัน และสามารถจัดกลุ่มเพื่อวิเคราะห์หารูปแบบ และตำแหน่งที่มีจุดอ่อนมาก เพื่อทำการแก้ไข ปรับปรุงโปรแกรมในส่วนนั้น ๆ ได้อย่างมีประสิทธิภาพมากขึ้น

2.2.4 งานวิจัย “Maintaining Software with a Security Perspective”

Jiwnani และ Zelkowitz [8] ได้เสนอแนวทางการตรวจสอบโปรแกรม โดยมีพื้นฐานจากลักษณะของจุดอ่อนที่เกิดขึ้นกับระบบ เพื่อเป็นการเพิ่มความปลอดภัยและเสถียรภาพให้แก่ระบบ ในงานวิจัยนี้ ได้มีการจัดแบ่งกลุ่มของจุดอ่อนโดยใช้การจัดแบ่ง 3 รูปแบบ ที่มีพื้นฐานการจัดแบ่งตามการจัดแบ่งของงานวิจัยของ Lanwehr และทำการประเมินโดยใช้ข้อมูลของจุดอ่อนที่เกิดขึ้นกับระบบปฏิบัติการวินโดว์เอ็นที และลินุกซ์เรดแฮด จำนวนทั้งสิ้น 1360 รายการ

2.3 การเพิ่มความปลอดภัยให้กับระบบปฏิบัติการ (Linux Security Enhancement)

แนวคิดในส่วนการเพิ่มความปลอดภัยให้กับระบบปฏิบัติการนั้นที่ทำการศึกษาในงานวิจัยนี้ ประกอบด้วย

1. การเพิ่มความแข็งแกร่งให้กับระบบ (OS Hardening)
2. โครงร่างแอลเอสเอ็ม (LSM Framework)

ซึ่งแต่ละวิธีมีรายละเอียดดังนี้

2.3.1 การเพิ่มความแข็งแกร่งให้กับระบบ

ระบบปฏิบัติการลินุกซ์มีจุดเด่นที่มีวิธีการปรับแต่ง ให้ระบบสามารถทำงานได้หลายหน้าที่ อีกทั้งยังเป็นระบบเปิด ซึ่งในขณะเดียวกันจุดเด่นในแง่นี้ ก็ทำให้เกิดประเด็นที่ต้องคำนึงถึงในเรื่องความปลอดภัย ในการสร้างระบบให้มีความปลอดภัยนั้น ขั้นตอนที่มีความสำคัญส่วนหนึ่งคือในส่วนของการจัดเตรียม ติดตั้งและ ปรับแต่งระบบให้เหมาะสมกับการใช้งาน และเมื่อพิจารณาการสร้างระบบลินุกซ์ ให้มีความปลอดภัยเข้ากับวิธีการดำเนินงานทั่ว ๆ ไปที่ สามารถแบ่งขั้นตอนการดำเนินงานออกเป็น 11 ขั้นตอน [9] คือ

1. วางแผน
2. การรักษาความปลอดภัยระดับกายภาพ

3. การติดตั้งระบบปฏิบัติการ
4. การรักษาความปลอดภัยของระบบไฟล์
5. ปรับแต่งระบบ
6. การรักษาความปลอดภัยบัญชีผู้ใช้งานระดับราก
7. การพิสูจน์ตัวตนของผู้ใช้งานระบบ
8. การรักษาความปลอดภัยจากการเข้าถึงระยะไกล
9. ติดตั้งระบบเฝ้าสังเกต
10. ทำการสำรองระบบ
11. อื่น ๆ

โดยในแต่ละขั้นตอนการทำงานมีรายละเอียดดังต่อไปนี้

2.3.1.1 วางแผน (Preliminary Planning)

ขั้นตอนนี้ เป็นขั้นตอนในการกำหนดความต้องการใช้งานระบบเบื้องต้น เพื่อเป็นการกำหนดองค์ประกอบโปรแกรมที่จำเป็นต้องใช้งาน จำนวนพื้นที่การใช้งานบนฮาร์ดดิสก์ ลักษณะของกลุ่มผู้ใช้งานระบบ รวมไปถึงการรวบรวมโปรแกรมและตัวปรับแต่งระบบ ที่จำเป็นต้องใช้ในการติดตั้งระบบทั้งหมด

ตารางที่ 2.2 เป็นตัวอย่างของ องค์ประกอบของซอฟต์แวร์ด้านการรักษาความปลอดภัยที่ต้องการ และสนับสนุนการทำงานของเมลเซิร์ฟเวอร์ โดยที่รายละเอียดขององค์ประกอบโปรแกรมและโปรแกรมรักษาความปลอดภัยที่เหมาะสมสำหรับเซิร์ฟเวอร์ประเภทอื่นๆ จะแสดงไว้ในภาคผนวก ข ซึ่งในการติดตั้งเซิร์ฟเวอร์แต่ละชนิดนั้น ควรเลือกเฉพาะส่วนโปรแกรมที่ได้ใช้งานจริงเท่านั้น แต่เนื่องจากในงานวิจัยนี้ ต้องการประเมินความสามารถในการป้องกันจุดอ่อนของระบบที่มีวัตถุประสงค์เพื่องานทั่วไป (General Purpose) จึงจะทำการประเมินจากเซิร์ฟเวอร์ที่สามารถให้บริการงานตามภาคผนวก ข

ตารางที่ 2.2 ตัวอย่างส่วนโปรแกรมและซอฟต์แวร์ด้านการรักษาความปลอดภัยที่ใช้ในเมลเซิร์ฟเวอร์

Server Type	Mail Server
Required Components	Sendmail or qmail (SMTP Server) BIND/DNS (Cache) IPTABLE Firewall IMAP/POP only for Sendmail
Optional Components	
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry Quota

2.3.1.2 การรักษาความปลอดภัยระดับกายภาพ (Physical System Security)

ขั้นตอนนี้ เป็นขั้นตอนในการรักษาความปลอดภัยในระดับกายภาพให้กับระบบ โดยการเลือกสถานที่ติดตั้งระบบที่มีความเสี่ยงต่อความเสียหายจากอุบัติเหตุน้อยที่สุด มีการติดตั้งระบบสำรองไฟ และการติดตั้งการป้องกันการเข้าถึงสถานที่ติดตั้งระบบจากบุคคลทั่วไปอย่างเหมาะสม เช่นการใส่กุญแจห้องที่มีการติดตั้งระบบไว้ รวมไปถึงการกำหนดรหัสผ่านในระดับ BIOS/RAM/EEPROM เพื่อป้องกันการปรับเปลี่ยนค่าต่างๆ และการบูทเครื่องโดยไม่ได้รับอนุญาต

2.3.1.3 การติดตั้งระบบปฏิบัติการ (Operating System Installation)

ขั้นตอนนี้ เป็นขั้นตอนในการติดตั้งระบบปฏิบัติการ และตัวเสริมของระบบปฏิบัติการ รวมถึงการกำหนดพื้นที่ในการใช้งานที่เหมาะสมและมีความปลอดภัย การดำเนินการติดตั้งระบบปฏิบัติการนี้ เริ่มจากการแบ่งพาทิชันในการใช้งานระบบ ซึ่งควรแยกส่วนของบัญชีผู้ใช้งาน

และพื้นที่ส่วนตัวของผู้ใช้งาน ออกจากพื้นที่ส่วนประมวลผล จากนั้นทำการติดตั้งระบบและตัวเสริมระบบให้ครบถ้วน และในการติดตั้งระบบปฏิบัติการนั้นควรเลือกส่วนประกอบโปรแกรมเท่าที่จำเป็นต้องใช้ตามการวางแผนในขั้นตอนที่ และทำการติดตั้งรหัสผ่านในการบูทระบบ

2.3.1.4 การรักษาความปลอดภัยของระบบไฟล์ (Securing Local File Systems)

ในขั้นตอนการรักษาความปลอดภัยของระบบไฟล์นี้ เป็นการตรวจสอบการอนุญาตในการเข้าถึงไฟล์และไดเรคทอรีที่ไม่เหมาะสมในระบบที่ทำการติดตั้ง และแก้ไขการอนุญาต

2.3.1.5 ปรับแต่งระบบ (Configuring and Disabling Services)

ขั้นตอนนี้ เป็นขั้นตอนในการปรับแต่งการทำงานของระบบโดยการกำจัดหรือยกเลิกการทำงานของบางบริการที่ไม่จำเป็น เลือกใช้การบริการที่มีการรักษาความปลอดภัยที่เหมาะสม และหากเป็นไปได้ ควรกำหนดกลุ่มพิเศษสำหรับการประมวลผลงานของเซิร์ฟเวอร์ทดแทนการให้สิทธิของผู้ใช้งานระดับรากในการประมวลผล และกำหนดสิทธิที่น้อยที่สุดที่เพียงพอต่อการทำงานสำหรับกลุ่มของการประมวลผลงานเซิร์ฟเวอร์

2.3.1.6 การรักษาความปลอดภัยบัญชีผู้ใช้งานระดับราก (Securing Root Account)

ขั้นตอนนี้เป็นขั้นตอนในการสร้างความปลอดภัยให้กับบัญชีผู้ใช้งานระดับราก โดยกำหนดรหัสผ่านที่ปลอดภัย และกำหนดให้มีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ ทำการตรวจสอบสิทธิของการเรียกใช้งานคำสั่ง su หากเป็นไปได้ ควรกำหนดกลุ่มผู้ใช้งานที่ชัดเจน และจำกัดลักษณะการล็อกอินระดับรากจากระยะไกล

2.3.1.7 การพิสูจน์ตัวตนของผู้ใช้งานระบบ (User Authentication and User Account Attributes)

ขั้นตอนนี้เป็นขั้นตอนการตรวจสอบและติดตั้งระบบการพิสูจน์ตัวตนและจัดการข้อมูลรหัสผ่านของระบบ สิ่งสำคัญที่ควรคำนึงถึงในขั้นตอนนี้คือการยกเลิกค่าดีฟอล์ทของบัญชีผู้ใช้ต่างๆ ที่มีการกำหนดมาในโปรแกรมต่างๆ

2.3.1.8 การรักษาความปลอดภัยจากการเข้าถึงระยะไกล (Securing Remote Authentication)

ขั้นตอนนี้ เป็นขั้นตอนในการควบคุมการเข้าถึงจากระยะไกล โดยการกำหนดให้การใช้ .rhosts ต้องใช้รหัสผ่านและทดแทนการใช้โปรแกรมติดต่อที่ใช้ ด้วยโปรแกรมที่มีการรักษาความปลอดภัยของข้อมูลในการส่งมากกว่า

2.3.1.9 ติดตั้งระบบเฝ้าสังเกต (Setup Ongoing System Monitoring)

ภายหลังจากการปรับแต่งระบบให้สามารถใช้งานอย่างปลอดภัยแล้ว ควรมีการควบคุมให้มีการเก็บข้อมูลการติดต่อและการทำงานต่างๆของระบบและการใช้โปรแกรมในการตรวจสอบระบบ เพื่อใช้ในการเฝ้าสังเกตความผิดปกติต่าง ๆ ที่อาจเกิดขึ้นในระบบได้

2.3.1.10 ทำการสำรองระบบ (Backup)

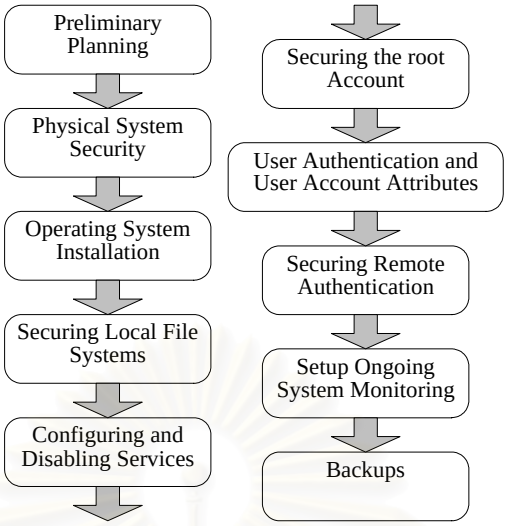
ขั้นตอนนี้ เป็นขั้นตอนที่ทำการสำรองระบบทั้งหมดไว้ในอุปกรณ์บันทึกการสำรองข้อมูล และวางแผนเพื่อทำการสำรองระบบเป็นระยะ ๆ

2.3.1.11 อื่น ๆ (Miscellaneous Activities)

ขั้นตอนนี้ เป็นการดำเนินการอื่นๆ เพื่อให้ระบบมีความปลอดภัยยิ่งขึ้น เช่นการลบข้อมูล รหัสของระบบปฏิบัติการและโปรแกรมที่ทำการติดตั้งแล้วออกจากระบบ

และนอกจากการดำเนินการทั้งหมดดังที่ได้กล่าวมาแล้ว สิ่งจำเป็นสำหรับระบบคือการจัดทำเอกสารประกอบระบบเพื่ออธิบายส่วนประกอบของระบบ และการเปลี่ยนแปลงต่างๆที่เกิดขึ้น โดยสิ่งที่ควรจัดทำในเอกสารประกอบระบบ ประกอบด้วย วันที่ที่ติดตั้ง ชื่อซอฟต์แวร์ ชื่อดิสทริบิวชันของลินุกซ์ หมายเลขรุ่นของซอฟต์แวร์

รูปที่ 2.2 แสดงแผนผังลำดับขั้นตอน ของการดำเนินการเสริมความแข็งแกร่ง ให้กับระบบลินุกซ์ โดยเริ่มจากการวางแผน การรักษาความปลอดภัยระดับกายภาพ การติดตั้งระบบปฏิบัติการ การรักษาความปลอดภัยของระบบไฟล์ ปรับแต่งระบบ การรักษาความปลอดภัยบัญชีผู้ใช้งานระดับราก การพิสูจน์ตัวตนของผู้ใช้งานระบบ การรักษาความปลอดภัยจากการเข้าถึงระยะไกล ติดตั้งระบบเฝ้าสังเกต และการทำการสำรองระบบ

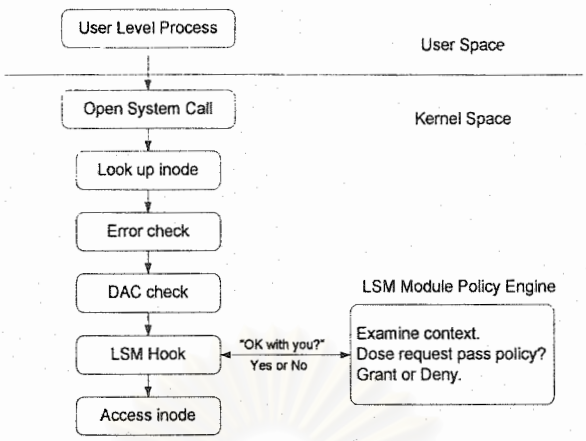


รูปที่ 2.2 แผนผังลำดับขั้นตอนของการดำเนินการเสริมความแข็งแกร่ง

2.3.2 โครงร่างแอลเอสเอ็ม

จากการที่ปัญหาด้านความปลอดภัยมีมากขึ้น เนื่องจากมีการเชื่อมระบบแบบออนไลน์มากขึ้น ทำให้มีการค้นพบจุดอ่อนของซอฟต์แวร์จากการถูกโจมตีมากขึ้น ในระบบลินุกซ์ได้มีการออกแบบให้สามารถป้องกันจุดอ่อนที่อาจจะเกิดขึ้นกับระบบได้โดยมีการกำหนดการควบคุมการเข้าถึงแบบดีเอซี (DAC - Discretionary Access Control) ซึ่งเพียงพอต่อการจัดการความเป็นส่วนตัวของข้อมูล แต่ไม่เพียงพอต่อการป้องกันระบบจากการถูกโจมตี จึงมีงานวิจัยที่เกี่ยวกับการออกแบบการควบคุมการเข้าถึงที่นอกเหนือจากแบบดีเอซีขึ้นเป็นจำนวนมาก แต่เนื่องจากส่วนใหญ่ ต้องมีการแก้ไขการทำงานบางส่วนของเคอร์เนลของระบบ ซึ่งอาจทำให้ระบบมีการทำงานผิดพลาดได้

แอลเอสเอ็ม (LSM - Linux Security Module) เป็นความพยายามในการแก้ไขปัญหาดังกล่าว โดยการกำหนดโครงร่างมอดูลด้านความปลอดภัย โดยทำการย้ายความสามารถในด้านความปลอดภัย ที่อยู่ในโครงสร้างหลักของลินุกซ์ ให้ไปอยู่ในส่วนที่เป็นส่วนเพิ่มเติม และกำหนดส่วนเชื่อมต่อระหว่างส่วนกลางของระบบลินุกซ์มอดูลด้านความปลอดภัย ทำให้การพัฒนามอดูลด้านความปลอดภัยของลินุกซ์ สามารถทำได้โดยอิสระโดยไม่ขึ้นกับโครงสร้างหลักของลินุกซ์ ในโครงสร้างหลักของแอลเอสเอ็มนั้นจะมีการเพิ่มเขตข้อมูลที่เกี่ยวกับความปลอดภัยให้กับโครงสร้างข้อมูลในส่วนกลางของระบบ และแทรกการเรียกฟังก์ชันตรวจสอบการเข้าถึง ในมอดูลความปลอดภัย เพื่อจัดการในเรื่องการควบคุมการเข้าถึงทรัพยากรในระบบ ดังแสดงในรูป 2.3



รูปที่ 2.3 สถาปัตยกรรมแอลเอสเอ็ม[10]

จากรูปที่ 2.3 โครงร่างของแอลเอสเอ็ม มอดูลด้านความปลอดภัยที่เลือกใช้จะอยู่ในส่วนเกาะเกี่ยวมอดูลของแอลเอสเอ็ม (LSM Hook) ซึ่งจะมีการกำหนดการเชื่อมต่อและกำหนดฟังก์ชันความปลอดภัยที่ทำการแยกออกจากส่วนเคอร์เนลลินุกซ์

ขณะนี้ ได้มีมอดูลด้านความปลอดภัยที่ได้รับการพัฒนา และดำเนินการตามโครงร่างของแอลเอสเอ็มตามที่ได้สำรวจมา 3 รูปแบบด้วยกัน คือ

เอสอีลินุกซ์

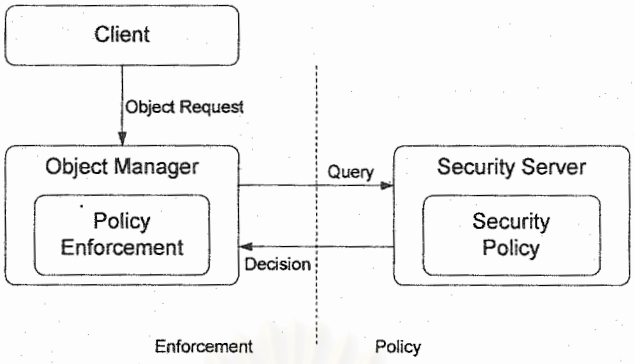
แอลไอดีเอส

ดีทีอี

รายละเอียดดังแสดงในหัวข้อถัดไป

2.3.2.1 เอสอีนุกซ์

เอสอีลินุกซ์ (SELinux - Security-Enhanced Linux) [11] เป็นมอดูลด้านความปลอดภัยที่มีจุดเริ่มต้นจากงานวิจัยสถาปัตยกรรมแฟลกซ์ (Flask Security Architecture) [12] ที่มีการจัดหาการควบคุมการเข้าถึงแบบเอ็มเอซี (MAC - Mandatory Access Control) ในโครงสร้างของสถาปัตยกรรมแฟลกซ์ ได้มีการแยกส่วนของคำสั่งในการบังคับใช้นโยบาย (Policy Enforcement Code) กับการตัดสินใจเกี่ยวกับนโยบาย (Policy Decision-making Code) ออกจากกันอย่างชัดเจน โดยในส่วนของการตัดสินใจเกี่ยวกับนโยบายนั้น ได้ถูกห่อหุ้มเป็นส่วนโปรแกรมที่แยกออกจากระบบปฏิบัติการที่เรียกว่า โปรแกรมบริการความปลอดภัย (Security Server) ทำหน้าที่ในการตัดสินใจตามนโยบายที่กำหนดไว้ โครงสร้างของเอสอีลินุกซ์สามารถแสดงได้ดังรูปที่ 2.4



รูปที่ 2.4 โครงสร้างของ เอสอีลินุกซ์

จากรูปที่ 2.4 การทำงานของเอสอีลินุกซ์นั้น เริ่มเมื่อมีการร้องขอใช้งานทรัพยากรเข้ามาที่ส่วนการจัดการวัตถุ (Object Manager) จะมีการกำหนดหมายเลขกำกับและรายละเอียดของการร้องขอนั้น เพื่อส่งไปถามสิทธิกับโปรแกรมบริการความปลอดภัย ที่จะทำหน้าที่ตรวจสอบการเข้าถึงนั้น ๆ กับนโยบายที่มีการกำหนดไว้ จากนั้น จึงจะส่งผลการตัดสินใจกลับมาให้กับส่วนจัดการวัตถุเพื่อทำการบังคับใช้ต่อไป

2.3.2.2 แอลไอดีเอส

แอลไอดีเอส (LIDS - Linux Intrusion Detection System) [13-17] เป็นตัวเสริมระบบที่หน้าที่เป็นระบบตรวจจับผู้บุกรุก ซึ่งจากการออกแบบ แอลไอดีเอสมีฟังก์ชันการทำงาน 3 ส่วนหลัก ประกอบด้วย

1. ปกป้องระบบจากผู้บุกรุก
2. ตรวจจับการบุกรุก
3. ตอบสนองต่อการบุกรุกระบบ

โดยแต่ละส่วนของการทำงาน มีรายละเอียดดังนี้

ปกป้องระบบจากผู้บุกรุก (Protection)

ในการปกป้องระบบจากผู้บุกรุกนี้ แอลไอดีเอสได้ทำการแยกการทำงานในระดับรากออกจากการทำงานในระดับผู้ใช้งานทั่ว ๆ ไป และได้มีการเพิ่มเติมการควบคุมการเข้าถึง ซึ่งประกอบด้วยการควบคุมการเข้าถึง 2 ส่วนคือ

การกำหนดระดับความสามารถของการประมวลผล ในระดับราก (System Capabilities) ให้มีความสามารถในการจัดการทรัพยากรต่าง ๆ ในระบบ ได้เท่าที่เพียงพอต่อการประมวลผลนั้นๆ

การกำหนดระดับของการเข้าถึงทรัพยากรระบบในระดับที่ต่างกัน 4 ระดับ คือ ปฏิเสธการเข้าถึงใด ๆ (Deny), การเข้าถึงเพื่อการอ่าน (Read), การเข้าถึงเพื่อทำการต่อเติมข้อมูล (Append) และการเข้าถึงในการเขียน แก้ไข และลบไฟล์ (Write)

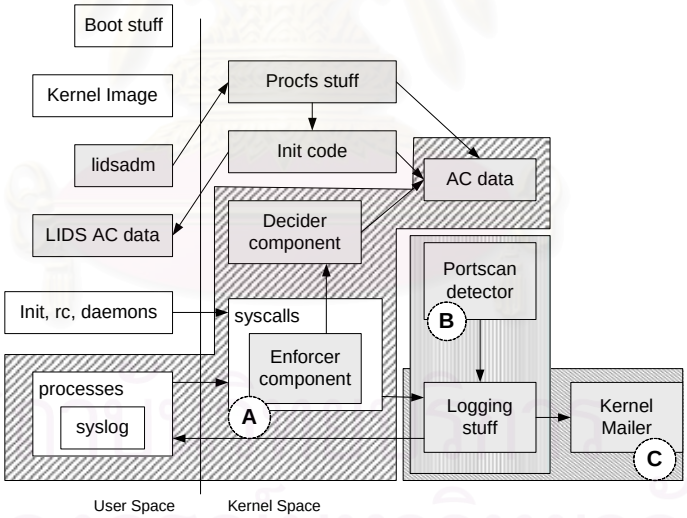
ตรวจจับการบุกรุก (Detection)

ในการตรวจจับการบุกรุกนี้ แอลไอดีเอส ทำการตรวจสอบการทำงานที่มีความผิดปกติที่เกิดขึ้นในระบบโดยการตรวจสอบไฟล์ข้อมูลการลงบันทึกต่าง ๆ ที่มีในระบบ และทำการแจ้งเตือนผู้ดูแลระบบถึงความผิดปกตินั้น

ตอบสนองต่อการบุกรุกระบบ (Response)

ภายหลังจากการตรวจจับผู้บุกรุกและพบว่าความผิดปกติที่เกิดขึ้นในระบบเป็นการฝ่าฝืนกฎของระบบ หรือเป็นการบุกรุกระบบ แอลไอดีเอสจะทำการเก็บข้อมูลรายละเอียดเกี่ยวกับการฝ่าฝืนนั้น ทำการส่งจดหมายเพื่อเตือนผู้กระทำการนั้น และทำการยกเลิกการอนุญาตในการใช้งานระบบกับผู้ฝ่าฝืนกฎของระบบ

โครงสร้างของแอลไอดีเอส สามารถแสดงได้ดังรูปที่ 2.5

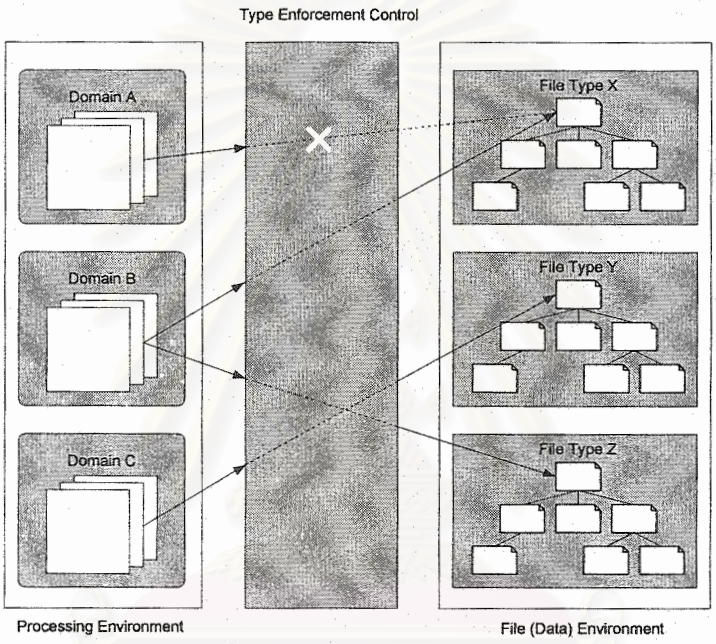


รูปที่ 2.5 โครงสร้างของแอลไอดีเอส

จากรูปที่ 2.5 แสดงการเชื่อมต่อระหว่างส่วนผู้ใช้และส่วนเคอร์เนลของลินุกซ์ ในการทำงานของแอลไอดีเอส ส่วน A เป็นส่วนการทำงานของการปกป้องระบบจากผู้บุกรุก ส่วน B เป็นส่วนการตรวจจับผู้บุกรุก และส่วน C เป็นส่วนของการตอบสนองต่อการบุกรุกระบบ

2.3.2.3 ดีทีอี

ดีทีอี (DTE - Domain and Type Enforcement) [18-20] เป็นงานวิจัยเกี่ยวกับการเสริมการควบคุมการเข้าถึงที่มีการเสนอใช้ประกอบกับการควบคุมการเข้าถึงในระบบยูนิกซ์และมีการปรับปรุงเพื่อนำมาใช้ในระบบลินุกซ์ โดยการทำงานของดีทีอีนั้น จะมีการแบ่งประเภทให้กับไฟล์ข้อมูล และแบ่งโดเมนให้กับการประมวลผล เพื่อทำการควบคุมการเข้าถึงจากโดเมนไปยังประเภท หรือจากโดเมนสู่โดเมน จากนโยบายที่กำหนดไว้ ดังแสดงในรูปที่ 2.6



รูปที่ 2.6 โครงสร้างของ ดีทีอี

จากรูปที่ 2.6 การจะเห็นการเข้าถึงข้อมูลจากกระบวนการที่อยู่ในโดเมนเอไปยังไฟล์ชนิดเอกซ์ ซึ่งไม่ได้รับอนุญาต (X) ดีทีอีจะทำการปฏิเสธการร้องขอนั้น ในขณะที่กระบวนการที่อยู่ในโดเมนบีจะสามารถเข้าถึงไฟล์ชนิดเอกซ์ได้เนื่องจากได้รับอนุญาต

2.4 การประเมินความสามารถของระบบ

จากการศึกษาพบว่ามีงานวิจัยที่เกี่ยวข้องจำนวนทั้งสิ้น 3 รายการ ประกอบด้วย

1. Security Evaluation of the Linux Operating System
2. A Comparison of SELinux and LIDS
3. Using CQUL for Static Analysis of Authorization Hook Placement

ซึ่งในแต่ละงานวิจัย มีรายละเอียดดังนี้

2.4.1 งานวิจัย “Security Evaluation of the Linux Operating System”

ในงานวิจัยนี้ Craig L. Munsee และ Chee Lee [21] ได้ทำการวิเคราะห์วิธีการโจมตีที่จะทำให้ได้รับสิทธิในการเข้าถึงระบบลินุกซ์โดยทางเครือข่ายเป็นหลัก โดยมีการอธิบายแต่ละประเภทของการโจมตี และทำการแสดงการเปรียบเทียบจุดอ่อนระหว่าง จุดอ่อนที่เกิดขึ้นกับระบบลินุกซ์ กับจุดอ่อนในระบบปฏิบัติการอื่นๆ และทำการเสนอข้อควรปฏิบัติเพื่อทำให้ระบบลินุกซ์มีความปลอดภัย

2.4.2 งานวิจัย“A Comparison of SELinux and LIDS”

ในงานวิจัยนี้ Larabee [22] ได้ทำการเปรียบเทียบการทำงานของตัวเสริมความปลอดภัยในระบบลินุกซ์ 2 วิธี คือ เอสอีลินุกซ์และแอลไอดีเอส เนื่องจากทั้ง 2 แนวทางเป็นแนวคิดที่มีจุดประสงค์ในการเสริมความปลอดภัยให้กับระบบเหมือนกันแต่มีวิธีการในการดำเนินการที่ต่างกัน ในงานวิจัยนี้ ได้มีการพิจารณาพื้นฐาน ประวัติ โครงสร้างและลักษณะการทำงานของทั้ง 2 วิธี และมีการยกตัวอย่างข้อจำกัดในการใช้งานจริงของทั้ง 2 วิธีและทำการเปรียบเทียบจุดเด่นของทั้ง 2 วิธี

2.4.3 งานวิจัย “Using CQUAL for Static Analysis of Authorization Hook Placement”

ในงานวิจัยนี้ Zhang และคณะ [23] ได้ทำการเสนอการตรวจสอบการอนุญาตของการจัดวางจุดตรวจสอบ (Hook) ในโครงร่างแอลเอสเอ็ม เนื่องจากในการพัฒนาโครงร่างแอลเอสเอ็มให้ความสนใจทางด้านนี้น้อยมาก โดยทำการวิเคราะห์โครงสร้างของจุดตรวจสอบ โดยใช้ ซีคิวยูเอแอล (CQUAL) ที่เป็นอุปกรณ์ใช้ในการวิเคราะห์ประเภทแบบสถิต (type-based static) เมื่อทำการปรับแต่งระบบด้วยซีคิวยูเอแอลแบบพื้นฐานและการวิเคราะห์แบบจีซีซี (GCC-based analysis) ทำให้สามารถดำเนินงานของเคอร์เนลระบบได้อย่างสมบูรณ์ จากงานวิจัยดังกล่าวพบว่า โครงร่างแอลเอสเอ็มในปัจจุบันยังสามารถทำให้เกิดจุดอ่อนในด้านความปลอดภัย

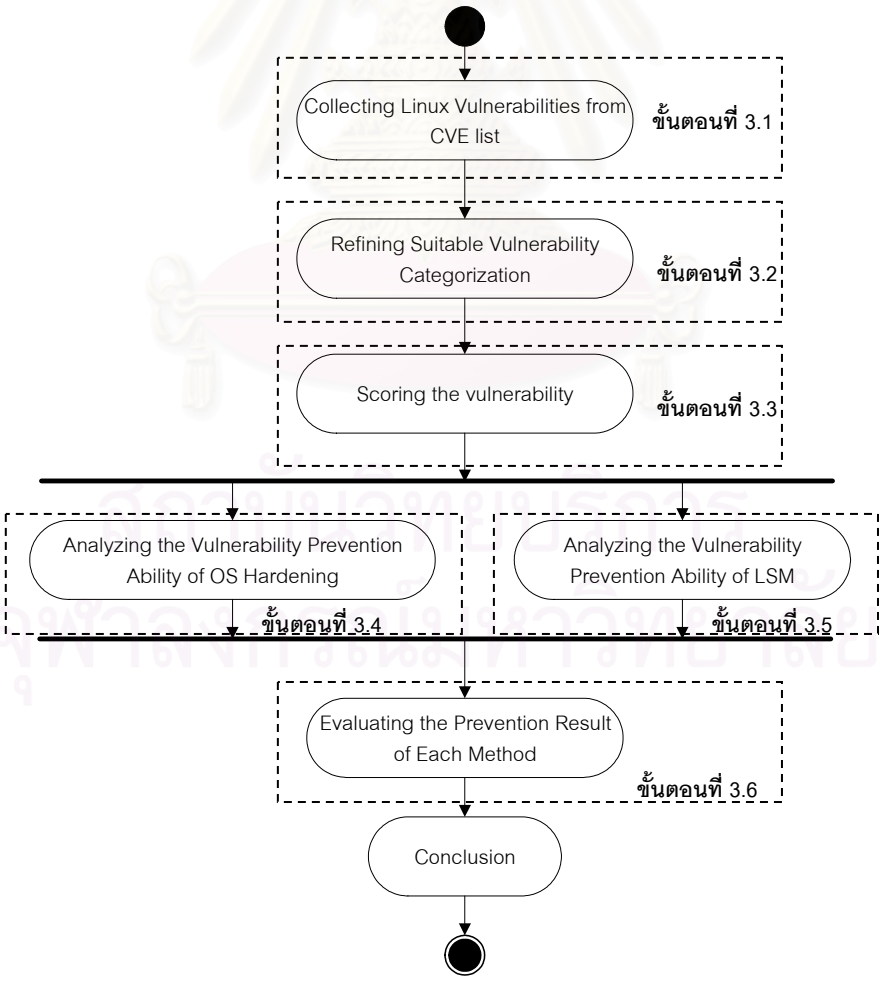
ที่กล่าวมาในบทที่ 2 นี้ เป็นแนวทาง ทฤษฎีและงานวิจัยที่เป็นแนวทางในการทำวิจัยนี้ โดยแนวทางการจัดกลุ่มของจุดอ่อนและข้อผิดพลาด และ จุดอ่อนที่สามารถเกิดขึ้นในระบบ เป็นแนวทางเพื่อใช้ในการจัดแบ่งกลุ่มของจุดอ่อนและการคิดให้คะแนนความเปราะบาง และแนวคิดเรื่องการเพิ่มความปลอดภัยให้กับระบบปฏิบัติการ และการประเมินความสามารถของระบบ เป็นแนวทางในการวิเคราะห์ และประเมินความสามารถ ในการป้องกันจุดอ่อน ของการเสริมความแข็งแกร่งและแอลเอสเอ็ม ซึ่งมีการแสดงรายละเอียดของขั้นตอนในการดำเนินการวิจัยในบทที่ 3

บทที่ 3
วิธีดำเนินการวิจัย

เนื้อหาในบทนี้ กล่าวถึงขั้นตอนในการดำเนินงานในการวิจัย ซึ่งแบ่งออกเป็นหัวข้อต่าง ๆ ได้ 6 หัวข้อ ประกอบด้วย

1. คัดกรองข้อมูลจุดอ่อนที่เกิดขึ้นในระบบปฏิบัติการลินุกซ์
2. ปรับแต่งรูปแบบการจัดกลุ่มจุดอ่อน
3. การให้คะแนนของจุดอ่อน
4. วิเคราะห์ความสามารถในการป้องกันจุดอ่อนของการเสริมความแข็งแกร่ง
5. วิเคราะห์ความสามารถในการป้องกันจุดอ่อนของโครงสร้างแอลเอสเอ็ม
6. ประเมินผลการป้องกันจุดอ่อนที่ได้ของแต่ละวิธี

ซึ่งขั้นตอนการดำเนินการวิจัย สามารถเขียนเป็นแผนภาพแอคทิวิตี ดังแสดงในรูป 3.1



รูปที่ 3.1 แผนภาพขั้นตอนการดำเนินการวิจัย

3.1 คัดกรองข้อมูลจุดอ่อนที่เกิดขึ้นในระบบปฏิบัติการลินุกซ์

จากข้อมูลรายการจุดอ่อนที่ค้นพบและมีการรวบรวมไว้ในรายการซีวีอี ซึ่งประกอบไปด้วยข้อมูลจุดอ่อนที่ค้นพบในระบบปฏิบัติการ โปรแกรมต่าง ๆ หรือกระทั่งโปรแกรมทางด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ในงานวิจัยนี้ ได้ทำการคัดกรองข้อมูลของจุดอ่อนเฉพาะที่มีความเกี่ยวข้องหรือมีผลกระทบต่อระบบปฏิบัติการลินุกซ์ โดยจุดอ่อนที่คัดกรองมานั้นมาจากรายการซีวีอีเวอร์ชัน 20020625 (วันที่ 25 มิถุนายน 2545) ประกอบไปด้วยจุดอ่อนทั้งหมด 5340 ตัว ซึ่งจุดอ่อนที่ทำการคัดกรองมานั้น เป็นจุดอ่อนที่เกิดขึ้นโดยตรงกับระบบปฏิบัติการเอง และจากโปรแกรมสนับสนุนการทำงานของระบบปฏิบัติการ ซึ่งจากการคัดกรองนี้ ทำให้ได้ข้อมูลจุดอ่อนที่เกิดกับระบบลินุกซ์จำนวน 388 ตัว ดังแสดงไว้ในรูปที่ 3.2 โดยรายละเอียดของจุดอ่อนทั้งหมดที่เกิดขึ้นในระบบลินุกซ์ได้มีการแสดงไว้ในภาคผนวก ก

อนึ่ง ขั้นตอนของการคัดกรองนี้ ทำด้วยมือ โดยการตรวจสอบข้อมูลของระบบ ที่ถูกกระทบกระเทือนจากจุดอ่อนที่มีระบุในรายการซีวีอี ดังนั้น จึงอาจมีความคลาดเคลื่อนของข้อมูลบางส่วน

CVE Number	Description
CAN-1999-0061	File creation and deletion, and remote execution, in the BSD line printer daemon (lpd).
CAN-1999-0123	Race condition in Linux mailx command allows local users to read user files.
CAN-1999-0171	Denial of service in syslog by sending it a large number of superfluous messages.
CAN-1999-0216	Denial of service of inetd on Linux through SYN and RST packets.
CAN-1999-0242	Remote attackers can access mail files via POP3 in some Linux systems that are using shadow passwords.
CAN-1999-0243	Linux cfingerd could be exploited to gain root access.

รูปที่ 3.2 ตัวอย่างจุดอ่อนจากรายการซีวีอีที่พบในระบบลินุกซ์

CVE ID	CAN-1999-0061
Severity	High
CVE Description	File creation and deletion, and remote execution, in the BSD line printer daemon (lpd).
Genesis	Serialization
Location	Support
Loss Type	Integrity, Run Arbitrary Code
CVE ID	CAN-1999-0123
Severity	Medium
CVE Description	Race condition in Linux mailx command allows local users to read user files.
Genesis	Serialization
Location	Process Management
Loss Type	Elevated Privilege
CVE ID	CAN-1999-0171
Severity	Medium
CVE Description	Denial of service in syslog by sending it a large number of superfluous messages.
Genesis	Design Error
Location	File Management
Loss Type	Avaliability

รูปที่ 3.3 แสดงรายละเอียดของจุดอ่อนที่ใช้ในการวิเคราะห์

รูปที่ 3.2 แสดงตัวอย่างรายการซีวีอีที่พบในระบบลินุกซ์ที่มีการแสดงในรายการภาคผนวก ซึ่งแต่ละรายการของซีวีอีที่นำมาใช้งานวิจัยนี้ มีรายละเอียดของข้อมูลตามรูปที่ 3.3 ซึ่งรายละเอียดของรายการซีวีอี ประกอบด้วย เลขซีวีอี รายละเอียดของจุดอ่อน ระดับความรุนแรงของจุดอ่อน ประเภทของจุดอ่อน ตำแหน่งที่มีการเกิดจุดอ่อน และลักษณะความเสียหายที่เกิดขึ้นเมื่อมีการโจมตีจุดอ่อน

3.2 ปรับแต่งรูปแบบการจัดกลุ่มจุดอ่อน

เพื่อให้การวิเคราะห์ความสามารถในการป้องกันจุดอ่อนมีประสิทธิภาพ จึงมีการกลุ่มของจุดอ่อนโดยได้ทำการศึกษาจากทฤษฎีและหลักการในการจัดกลุ่มของจุดอ่อน แบบต่าง ๆ ในทฤษฎีที่เกี่ยวข้องในบทที่ 2 แล้ว ในงานวิจัยนี้ ได้ทำการปรับแต่งลักษณะการจัดกลุ่มของจุดอ่อนดังกล่าวเพื่อให้เหมาะสมกับการวิเคราะห์นอกจากนั้น ยังมีการกำหนดคะแนนความรุนแรงให้กับจุดอ่อนแต่ละตัวโดยคำนึงถึงความรุนแรงและลักษณะความเสียหายต่อระบบที่จะเกิดขึ้นเมื่อจุดอ่อนนั้น ๆ ถูกโจมตี

การจัดกลุ่มของจุดอ่อนที่นำมาใช้ในงานวิจัยนี้ จะทำการแบ่งจุดอ่อนใน 4 รูปแบบดังนี้

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

3.2.1 ประเภทของจุดอ่อน

ในการจัดกลุ่มของจุดอ่อนโดยจัดตามประเภทของจุดอ่อนที่ใช้ในงานวิจัยนี้ ได้ทำการปรับปรุงจากลักษณะการจัดกลุ่มของจุดอ่อนของ [7] เป็นการจัดกลุ่มแบ่งโดยลักษณะในการโจมตีระบบ หรือระบบถูกโจมตีด้วยวิธีใด สามารถแบ่งได้เป็น 9 ประเภทดังนี้

1. ความผิดพลาดของการตรวจสอบข้อมูลนำเข้า
2. ความผิดพลาดของขอบเขตข้อมูล
3. ความผิดพลาดในการตรวจสอบการเข้าถึง
4. ความผิดพลาดของการเหลื่อมล้ำของการตรวจสอบสิทธิ
5. ความผิดพลาดของการปรับแต่งระบบ
6. ความผิดพลาดจากสภาพแวดล้อม
7. ความผิดพลาดจากการออกแบบระบบ
8. ความผิดพลาดจากชุดคำสั่งจัดการสิ่งผิดปกติ
9. อื่น ๆ

โดยรายละเอียดของแต่ละประเภทมีดังนี้

3.2.1.1 ความผิดพลาดของการตรวจสอบข้อมูลนำเข้า (Input Validation Error)

จุดอ่อนที่จัดอยู่ในกลุ่มที่เกิดจากความผิดพลาดของการตรวจสอบข้อมูลนำเข้า เป็นจุดอ่อนที่เกิดจากระบบได้รับข้อมูลนำเข้าที่ไม่ได้รับการตรวจสอบที่เพียงพอ เช่น การได้รับข้อมูลนำเข้าผิดลำดับ ข้อมูลนำเข้าที่มีความยาวเกินกว่าความยาวของตัวแปรที่รองรับ ซึ่งจากการโจมตีด้วยข้อมูลนำเข้าที่ไม่ถูกต้อง ผู้โจมตีสามารถทำให้ระบบล้มเหลว

3.2.1.2 ความผิดพลาดของขอบเขตข้อมูล (Boundary overflow)

จุดอ่อนที่จัดอยู่ในกลุ่มที่เกิดจากความผิดพลาดของขอบเขตข้อมูลเกิดจากระบบได้รับข้อมูลนำเข้าที่ทำที่มีขนาดใหญ่กว่าขนาดบัฟเฟอร์ของระบบ และทำให้เกิดจุดอ่อนขึ้น

3.2.1.3 ความผิดพลาดในการตรวจสอบการเข้าถึง (Access Validation Error)

จุดอ่อนที่จัดอยู่ในกลุ่มที่เกิดจากความผิดพลาดในการตรวจสอบการเข้าถึง เป็นจุดอ่อนที่เกิดจากความผิดพลาดของระบบตรวจสอบการเข้าถึง

3.2.1.4 ความผิดพลาดของการเหลื่อมล้ำของการตรวจสอบสิทธิ (Serialization)

จุดอ่อนที่จัดอยู่ในกลุ่มที่เกิดจากความผิดพลาดของการเหลื่อมล้ำของการตรวจสอบสิทธิ เกิดจากระบบขาดความเป็นหนึ่งเดียวที่แบ่งแยกไม่ได้ (atomicity) ทำให้เกิดช่วงว่างระหว่างการตรวจสอบสิทธิกับการใช้งานจริง หรือระหว่างการทำงาน 2 การทำงานที่ต่อเนื่องกัน ซึ่งผู้โจมตีสามารถใช่ช่วงเวลาดังกล่าวในการส่งให้ระบบทำงานที่ส่งผลให้ระบบสามารถถูก ล่วงละเมิดได้

3.2.1.5 ความผิดพลาดของการปรับแต่งระบบ (Configuration Error)

จุดอ่อนที่จัดอยู่ในกลุ่มที่เกิดจากความผิดพลาดของการปรับแต่งระบบ เกิดจากการปรับแต่งที่ส่วนต่าง ๆ โดยผู้ดูแลระบบที่สร้างให้เกิดจุดอ่อนขึ้นในระบบ เช่นการปรับแต่งระบบ โดยคงไว้ซึ่งค่าของผู้ดูแลระบบที่เป็นดีฟอล์ทที่เป็นที่รู้จักโดยทั่วไป

3.2.1.6 ความผิดพลาดจากสภาพแวดล้อม (Environmental Error)

จุดอ่อน ที่จัดอยู่ในกลุ่มที่เกิดจาก ความผิดพลาดจากสภาพแวดล้อมนั้น เกิดจากสภาพแวดล้อมที่ติดตั้งที่สามารถทำให้เกิดจุดอ่อนได้เช่นการโต้ตอบกันระหว่างระบบปฏิบัติการกับโปรแกรม หรือระหว่างโปรแกรม 2 ตัวในเครื่องเดียวกัน ซึ่งไม่เกิดขึ้นเมื่ออยู่ในสภาพแวดล้อมของการพัฒนา

3.2.1.7 ความผิดพลาดจากการออกแบบระบบ (Design Error)

จุดอ่อนที่จัดอยู่ในกลุ่มที่เกิดจากความผิดพลาดจากการออกแบบระบบเป็นจุดอ่อนที่เกิดจากขั้นตอนการออกแบบระบบ

3.2.1.8 ความผิดพลาดจากชุดคำสั่งจัดการข้อยกเว้น(Exceptional condition handling error)

จุดอ่อนที่จัดอยู่ในกลุ่มที่เกิดจากความผิดพลาดจากชุดคำสั่งจัดการกับข้อยกเว้น เกิดขึ้นเมื่อมีการเรียกฟังก์ชันงานเพื่อจัดการกับข้อยกเว้นของระบบ

3.2.1.9 อื่น ๆ (Others)

เป็นจุดอ่อนที่เกิดขึ้นโดยวิธีนอกเหนือจากที่กล่าวมาข้างต้น

3.2.2 จุดที่เกิดจุดอ่อน

การแบ่งกลุ่มของจุดอ่อนตามจุดที่เกิดจุดอ่อนที่ใช้ในงานวิจัยนี้ ทำการแบ่งจุดอ่อนโดยดูจากตำแหน่งที่เกิดจุดอ่อนว่าเกิด ณ. ส่วนใดของระบบ ซึ่งสามารถแบ่ง 8 ตำแหน่งได้ดังนี้

1. ส่วนการเริ่มต้นระบบ
2. ส่วนการจัดการหน่วยความจำ
3. ส่วนการจัดการการประมวลผล
4. ส่วนการจัดการอุปกรณ์
5. ส่วนการจัดการแฟ้มข้อมูล
6. ส่วนการพิสูจน์ตัวจริง
7. ส่วนโปรแกรมที่สนับสนุนการทำงานระบบปฏิบัติการ
8. ส่วนโปรแกรมประยุกต์

โดยแต่ละตำแหน่งมีรายละเอียดดังนี้

3.2.2.1 ส่วนการเริ่มต้นระบบ (System Initiation)

จุดอ่อนที่เกิดขึ้นในส่วนของการเริ่มต้นระบบ เกิดจากความผิดพลาดของระบบในการเริ่มการทำนของการป้องกันโดเมน หรือไม่มีการรักษาความปลอดภัยให้การปรับแต่งระบบสำหรับการเริ่มต้นการรักษาความปลอดภัย

3.2.2.2 ส่วนการจัดการหน่วยความจำ (Memory Management)

จุดอ่อนที่เกิดขึ้นในส่วนการจัดการหน่วยความจำ เกิดขึ้นจากข้อผิดพลาดของฟังก์ชันการควบคุมการใช้งานหน่วยความจำของระบบทำให้เกิดความผิดพลาดในการอนุมัติหรือการระงับการเข้าถึงของโปรแกรมต่าง ๆ

3.2.2.3 ส่วนการจัดการการประมวลผล (Process Management)

จุดอ่อนที่เกิดขึ้นในส่วนการจัดการการประมวลผล เกิดขึ้นจากข้อผิดพลาดของฟังก์ชันการควบคุมเวลาของหน่วยประมวลผลกลางทำให้เกิดความผิดพลาดในการอนุมัติหรือการระงับการเข้าถึงของโปรแกรมต่าง ๆ

3.2.2.4 ส่วนการจัดการอุปกรณ์ (Device Management)

จุดอ่อนที่เกิดขึ้นในส่วนการจัดการอุปกรณ์ เกิดขึ้นจากความผิดพลาดของไอโอรูทีน จากค่าของพารามิเตอร์ที่ส่งมาให้ หรือเกิดจากขั้นตอนการตรวจสอบพารามิเตอร์มีการเปลี่ยนแปลงค่าดังกล่าว

3.2.2.5 ส่วนการจัดการแฟ้มข้อมูล (File Management)

จุดอ่อนที่เกิดขึ้นในส่วนจัดการแฟ้มข้อมูล เกิดขึ้นจากความผิดพลาดของการควบคุมการเข้าถึงระดับไฟล์และการป้องกันไฟล์

3.2.2.6 ส่วนการพิสูจน์ตัวจริง (Authentication)

จุดอ่อนที่เกิดขึ้นในส่วนการพิสูจน์ตัวจริง เกิดจากความผิดพลาดของฟังก์ชันที่ดูแลข้อมูลเกี่ยวกับรายละเอียดการตรวจสอบ เช่น ไฟล์รหัสผ่าน หรือการเข้าสู่ระบบโดยไม่ผ่านการตรวจสอบ

3.2.2.7 ส่วนโปรแกรมที่สนับสนุนการทำงานระบบปฏิบัติการ(Support)

จุดอ่อนที่เกิดขึ้นในส่วนโปรแกรมที่สนับสนุนการทำงานระบบปฏิบัติการ

3.2.2.8 ส่วนโปรแกรมประยุกต์(Application)

จุดอ่อนที่เกิดขึ้นในส่วนโปรแกรมประยุกต์ รวมถึงการทำงานของ รหัสโปรแกรมที่มีวัตถุประสงค์ทำลายระบบ (Malicious Code)

3.2.3 ลักษณะความเสียหาย

ในการจัดกลุ่มจุดอ่อนตามลักษณะความเสียหายที่เกิดขึ้นนั้น อาศัยพื้นฐานการรักษาความปลอดภัยทั่ว ๆ ไปของระบบ ที่ประกอบด้วย การรักษาความลับ การรักษาบูรณภาพ และการรักษาสภาพความพร้อมใช้งาน นอกจากนี้ ในงานวิจัยนี้ ได้เพิ่มความเสียหายในกรณีที่ระบบถูกล่วงละเมิด ซึ่งจะเป็นความเสียหายที่จะเป็นตัวนำไปสู่ความเสียหาย การรักษาความลับ การรักษาบูรณภาพ และการรักษาสภาพความพร้อมใช้งานต่อไป รายละเอียดของความเสียหายต่าง ๆ มีดังนี้

3.2.3.1 เสียความเป็นความลับ (Confidentiality)

ความเสียหายประเภทที่ทำให้เสียความเป็นความลับนี้ เกิดขึ้นจากการโจมตีที่มีผลทำให้ข้อมูลหรือการทำงานถูกเปิดเผย หรือถูกขโมยไปจากระบบ

3.2.3.2 เสียสภาพบูรณภาพ (Integrity)

ความเสียหายประเภทที่ทำให้เสียสภาพบูรณภาพนั้น เกิดขึ้นจากการโจมตีที่มีผลทำให้มีการเปลี่ยนแปลงของข้อมูลต่าง ๆ ในระบบ

3.2.3.3 เสียสภาพพร้อมใช้งาน (Availability)

ความเสียหายประเภทที่ทำให้เสียสภาพบพร้อมใช้งานนั้น เกิดขึ้นจากการโจมตีที่มีผลขัดขวางการเรียกใช้งานทรัพยากรระบบของผู้ใช้งานหรือการประมวลผลใด ๆ

3.2.3.4 ระบบถูกล่วงละเมิด (System Compromise)

ความเสียหายประเภทที่ทำให้ระบบถูกล่วงละเมิดนั้น เกิดขึ้นจากการโจมตีที่เกิดความเสียหารโดยตรง แต่เป็นการอนุญาตให้ผู้โจมตีระบบได้รับสิทธิการทำงานในระบบ โดยลักษณะที่ระบบถูก ล่วงละเมิด นั้น มีลักษณะที่แตกต่างกันดังนี้

เรียกทำงานชุดคำสั่งใด ๆ (Run Arbitrary Code)

เพิ่มสิทธิในการทำงาน(Elevate Privilege)

เข้าถึงบัญชีผู้ใช้ (Account Break-in)

เข้าถึงระดับราก(Root Break-in)

ซึ่งในงานวิจัยนี้ ในการวิเคราะห์ความเสียหายที่มีผลทำให้ระบบถูกล่วงละเมิด จะคิดคะแนนของจุดอ่อน จากการความเสียหายในลักษณะย่อยของการถูกล่วงละเมิดแต่ละตัว และรวมเป็นชุดเดียวกันของประเภทระบบถูกล่วงละเมิด

3.2.4 ระดับความรุนแรง

เนื่องจากจุดอ่อนแต่ละตัวมีความสามารถในการทำให้ระบบเกิดความเสียหายที่ไม่เท่ากัน ดังนั้นจึงมีการกำหนดระดับความรุนแรงของการโจมตีจุดอ่อนไว้ 3 ระดับคือ

ระดับสูง (High)

ระดับกลาง (Medium)

ระดับต่ำ (Low)

ซึ่งในการกำหนดระดับความรุนแรงนี้ นำมาจากระดับความรุนแรงของจุดอ่อนที่มีการระบุไว้ในรายการซีวีอี

3.3 การให้คะแนนของจุดอ่อน

หลักการพื้นฐานของการให้คะแนน คือ ให้คะแนนสำหรับการปรากฏขึ้นของจุดอ่อนตามรายการซีวีอี และการจัดประเภทจุดอ่อน โดยรวมกันเป็นดัชนีความเปราะบางของระบบ ซึ่ง หากดัชนีความเปราะบางมีค่าสูง ระบบจะมีความเสี่ยงต่อความเสียหายโดยการโจมตีจุดอ่อนมากกว่าดัชนีความเปราะบางที่มีค่าน้อย

เนื่องจากมีความแตกต่างของปริมาณความเสียหาย และระดับความรุนแรงของจุดอ่อนแต่ละตัว ในการวิเคราะห์ความสามารถในการป้องกันจุดอ่อนนี้ จึงได้กำหนดระดับคะแนนที่ต่างกันขึ้นตามระดับความเสียหายและความรุนแรง

คะแนนของจุดอ่อนแต่ละตัว คิดจากประเภทของความเสียหายที่เกิดขึ้น โดยประกอบไปด้วย ความเสียหายที่เกิดจากการโจมตีจุดอ่อนโดยตรง และการที่ระบบถูกล่วงละเมิด เนื่องจากจุดอ่อนแต่ละตัว สามารถทำให้เกิดความเสียหายมากกว่า 1 แบบ ในการคิดคะแนนความเสียหายเมื่อถูกโจมตีของระบบปฏิบัติการลินุกซ์นั้น จึงมีการกำหนดให้ในแต่ละประเภทของความเสียหายโดย ซึ่งประกอบด้วย การรักษาความลับ การรักษาบูรณภาพ และการรักษาสภาพความพร้อมใช้งาน และแต่ละลักษณะย่อยของการถูกล่วงละเมิด มีคะแนนแบบละ 1 คะแนน

และในแต่ละระดับความรุนแรงของความเสียหายที่เกิดขึ้น ทำให้มีการกำหนดคะแนนที่ต่างกันในแต่ละระดับ โดยที่ความรุนแรงระดับปานกลางจะมีค่าเป็น 2 เท่า และ ระดับสูงมีค่าเป็น 3 เท่าของค่าคะแนนความเสียหายของความรุนแรงในระดับต่ำ ซึ่งการให้คะแนนของจุดอ่อนสามารถแสดงได้ดังตารางที่ 3.1

ตารางที่ 3.1 แสดงการให้คะแนนของจุดอ่อนที่ใช้ในงานวิจัยนี้ โดยความเสียหายแบบ การรักษาความลับ การรักษาบูรณภาพ และการรักษาสภาพความพร้อมใช้งาน จะได้คะแนนตัวละ 1 คะแนน และความเสียหายแบบการล่วงละเมิดระบบ จะได้คะแนน โดยคิดจากผลรวมของการล่วงละเมิดแบบต่าง ๆ ทั้ง 4 แบบ นอกจากนั้น คะแนนของจุดอ่อนจะขึ้นอยู่กับระดับความรุนแรงของจุดอ่อนด้วย

ตารางที่ 3.1 การให้คะแนนของจุดอ่อนที่ใช้ในงานวิจัย

Loss Type/ Severity	Low	Medium	High
Confidentiality	1	2	3
Integrity	1	2	3
Availability	1	2	3
System compromise	4	8	12

	Low	Medium	High
Run arbitrary code	1	2	3
Elevate Privilege	1	2	3
Account Break-in	1	2	3
Root Break-in	1	2	3

3.4 วิเคราะห์ความสามารถในการป้องกันจุดอ่อนของการเสริมความแข็งแกร่ง

การวิเคราะห์ความสามารถในการป้องกันจุดอ่อนของการเสริมความแข็งแกร่งให้กับระบบลินุกซ์นี้ จะทำการวิเคราะห์จาก ขั้นตอนการดำเนินการทั้ง 11 ขั้นที่ได้กล่าวไว้ในบทที่ 2

ซึ่งจากการศึกษาขั้นตอนการดำเนินงานของการเสริมความแข็งแกร่ง พบว่า สามารถจัดเป็น 3 กลุ่มใหญ่ ๆ คือ

การติดตั้งระบบ

การปรับแต่งระบบ

การบำรุงรักษาระบบ

ซึ่งในแต่ละขั้นตอน สามารถวิเคราะห์ได้ดังนี้

<u>ขั้นตอนการติดตั้งระบบ</u> ประกอบด้วยวางแผน การรักษาความปลอดภัยระดับกายภาพ และการติดตั้งระบบปฏิบัติการ โดยในการทำงานของกลุ่มนี้เป็นการทำงานเริ่มต้นในการสร้างระบบ ในการเลือกโปรแกรมที่เหมาะสมกับการทำงานในระบบนั้น เป็นส่วนที่ลดช่องทางการโจมตีระบบ และวางขอบเขตการดูแลรักษาระบบได้อย่างมีประสิทธิภาพ และการติดตั้งระบบปฏิบัติการและตัวแต่งระบบ (patch) เป็นการแก้ไขจุดอ่อนได้โดยตรง ซึ่งในการประเมิน จะทำการตรวจสอบจากรายการของตัวแต่งระบบที่มีกำหนดจากรายการซีวีอี

ขั้นตอนการปรับแต่งระบบ ประกอบด้วยการรักษาความปลอดภัยของระบบไฟล์ การปรับแต่งระบบ การรักษาความปลอดภัยบัญชีผู้ใช้งานระดับราก การพิสูจน์ตัวตนของผู้ใช้งานระบบ และการรักษาความปลอดภัยจากการเข้าถึงระยะไกล ขั้นตอนนี้ เป็นขั้นตอนที่ปรับแต่งระบบให้มีระดับความปลอดภัยตามความต้องการของระบบ และในการตรวจสอบการอนุญาตสิทธิต่าง ๆ และการปรับแต่งระบบ เป็นการดำเนินการที่สามารถแก้ไขความผิดพลาดที่เกิดจากการปรับแต่งได้

ขั้นตอนการบำรุงรักษาระบบ ประกอบด้วยการติดตั้งระบบเฝ้าสังเกต ทำการสำรองระบบและขั้นตอนอื่น ๆ เป็นขั้นตอนที่ติดตามเฝ้าระวังสิ่งผิดปกติที่อาจเกิดขึ้นกับระบบได้ นอกจากนี้ การทำเอกสารประกอบระบบ เป็นการบันทึกสิ่งที่มีในระบบ เพื่อเป็นรายการอ้างอิง ทำให้การแก้ปัญหา เมื่อมีสิ่งผิดปกติสามารถทำได้อย่างมีประสิทธิภาพ

3.5 วิเคราะห์ความสามารถในการป้องกันจุดอ่อนของโครงสร้างแอลเอสเอ็ม

การวิเคราะห์ความสามารถในการป้องกันจุดอ่อนของโครงสร้างแอลเอสเอ็มนี้ จะทำการวิเคราะห์จากโครงสร้างหลักและการทำงานของโครงร่างแอลเอสเอ็ม และมอดูลด้านความปลอดภัยตัวอย่างที่มีการอิมพลีเมนต์ด้วยโครงร่างแอลเอสเอ็ม ซึ่งในงานวิจัยนี้ ได้ทำการยกมา 3 ตัวอย่างคือเอสอีลินุกซ์ แอลไอดีเอส และดีทีอี

ในการทำการวิเคราะห์การทำงานของมอดูลด้านความปลอดภัยนั้น จะทำการวิเคราะห์ใน 2 ส่วนคือ หลักการการทำงานและนโยบายตัวอย่างที่มีการกำหนดไว้

โครงสร้างของแอลเอสเอ็ม เป็นโครงร่างอเนกประสงค์ สำหรับลินุกซ์เคอร์เนลในการอิมพลีเมนต์ระบบการควบคุมการเข้าถึง มีการกำหนดจุดเชื่อมต่อมาตรฐานสำหรับการบังคับใช้มอดูลนโยบายทางความปลอดภัย เพื่อให้ส่วนดูแลความปลอดภัยทำหน้าที่เป็นมอดูลความปลอดภัยซึ่งสามารถสับเปลี่ยนและเลือกใช้ได้ แอลเอสเอ็มได้กำหนดแนวทางเน้นในการเป็นสื่อกลางในการเข้าถึงอ็อบเจคภายในเคอร์เนล เช่น ทาสก์ (tasks) ไอโนด(inodes) ไฟล์ ฯลฯ ซึ่งทำหน้าที่โดยฟังก์ชันเชื่อมต่อ (Hook Function)ไปยังมอดูลความปลอดภัยที่ใช้งานอยู่ เพื่อทำการตรวจสอบสิทธิในการเข้าถึงข้อมูลนั้น จากรูปที่ 2.2 ในบทที่ 2 จะเห็นว่าแอลเอสเอ็มเลือกใช้ฟังก์ชันเชื่อมต่อที่ทำหน้าที่ตรวจสอบ อยู่ในตำแหน่งที่ใกล้กับการเข้าถึงข้อมูลนั้น ๆ ที่สุด แทนการใช้ system call interposition เพื่อลดความเสี่ยงที่จะเกิดความผิดพลาดจากช่วงเวลา ระหว่างการตรวจสอบกับการใช้งานจริง

ส่วนของการกำหนดฟังก์ชันการเชื่อมของแอลเอสเอ็มนั้น ได้มีการกำหนดในส่วนการโหลดใช้งานมอดูลด้านความปลอดภัย การจัดการเกี่ยวกับเขตข้อมูลความปลอดภัย ที่ใช้เป็นสิ่งระบุ

นโยบายที่จะใช้ควบคุมการเข้าถึงอ็อบเจคใด ๆ ในระบบ และฟังก์ชันในการจัดการเกี่ยวกับการเข้าถึง

3.5.1 เอสอีลินุกซ์

เอสอีลินุกซ์ (SE Linux – Secured Enhanced Linux) เป็นตัวปรับแต่งเคอร์เนล เกี่ยวกับการควบคุมการเข้าถึงแบบเอ็มเอซี ที่มีการอิมพลีเมนต์เป็นมอดูลด้านความปลอดภัย ตามแบบโครงร่างแอลเอสเอ็ม นโยบายในการควบคุมการเข้าถึงที่ใช้ในเอสอีลินุกซ์นั้น ได้ทำการปรับปรุงเพื่อสนับสนุนการทำงานร่วมกันระหว่างนโยบายแบบการกำหนดชนิด(Type Enforcement) และนโยบายแบบกำหนดหน้าที่ (RBAC) โดยการกำหนดนโยบายเพื่อใช้ในเอสอีลินุกซ์ มีจุดประสงค์ 8 ประการดังต่อไปนี้

เพื่อควบคุมการเข้าถึงข้อมูลโดยตรง โดยทำการกำหนดประเภทแยกจากกัน ให้กับทรัพยากรทุกอย่างที่อยู่ในระบบ เช่นไฟล์ข้อมูล หน่วยความจำของเคอร์เนล และข้อมูลใน /proc/kcore และทำการกำหนดโดเมนที่ต่างกัน ของการประมวลผลที่เข้าถึงข้อมูลประเภทดังกล่าว

เพื่อปกป้องบูรภาพให้กับเคอร์เนล โดยการกำหนดประเภทให้กับไฟล์ ที่ใช้ในการเริ่มใช้งานระบบ และ มอดูลต่าง ๆ เช่น ยูทิลิตี้ อ็อบเจคไฟล์ และข้อมูลการปรับแต่งระบบ และมีการกำหนดโดเมนสำหรับการประมวลผล ที่มีการเข้าถึงในการเขียนทับไฟล์ประเภทนี้ กำหนดโดเมนเฉพาะสำหรับการเข้าถึงมอดูลยูทิลิตี้ และจำกัดความสามารถ ในการใช้งานสำหรับโดเมนนี้อนุญาตสิทธิเพียงบางโดเมน ที่สามารถผันตัวเองมาอยู่ในโดเมนยูทิลิตี้

เพื่อปกป้องบูรณภาพให้กับโปรแกรมระบบ ข้อมูลการปรับแต่งระบบ และแฟ้มลงบันทึกเข้าออกระบบ โดยการกำหนดประเภทให้กับคลังโปรแกรม และข้อมูลฐานสองของระบบเพื่อควบคุมการเข้าถึงข้อมูลนั้น ๆ และอนุญาตเพียงผู้ดูแลระบบ ที่สามารถเปลี่ยนแปลงโปรแกรมระบบ มีการกำหนดประเภทให้กับ ข้อมูลการปรับแต่งระบบ และแฟ้มลงบันทึกเข้าออกระบบ และกำหนดโดเมนให้กับการประมวลผลที่ใช้ในการเขียนไฟล์เหล่านี้

จำกัดความเสียหายที่เป็นไปได้จากการโจมตีจุดบกพร่อง ในการประมวลผลที่มีเอกสิทธิ โดยการกำหนดการประมวลผลที่มีเอกสิทธิ และโปรแกรมอยู่ในโดเมนที่แยกจากกัน โดยที่แต่ละโดเมนมีการกำหนดการอนุญาตที่น้อยที่สุด และกำหนดประเภทที่ต่างกันให้กับอ็อบเจคที่มีการเข้าถึงจากโดเมนประเภทนี้

ป้องกันการเอ็กซิคิวท์รหัสคำสั่ง ที่อาจมีผลเสียต่อระบบ โดยการประมวลผลที่มีเอกสิทธิ โดยมีการกำหนดประเภทของโปรแกรม ที่สามารถเอ็กซิคิวท์ให้กับโปรแกรมที่เข้าถึง โดยการ

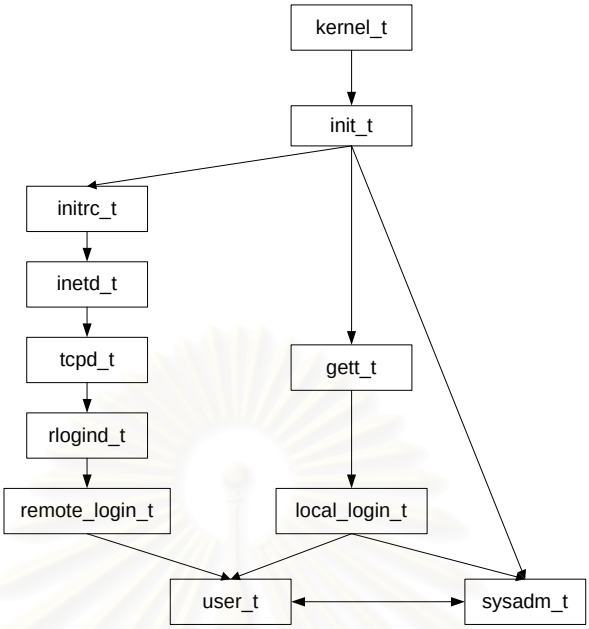
ประมวลผลที่มีเอกสิทธิ และอนุญาตการผันตัวไปยังโดเมนที่มีสิทธิได้ ผ่านการเอ็กซิคิวท์ประเภทที่ระบุเท่านั้น

ป้องกันการเข้าถึงบทบาทของผู้ดูแลระบบ และโดเมนที่เกี่ยวข้องจากยูสเซอร์ที่ไม่ผ่านการตรวจสอบสิทธิ โดยกำหนดให้มีการผันสิทธิและบทบาทเป็นผู้ดูแลระบบและโดเมนจากการล็อกอินเท่านั้นป้องกันการผันสิทธิและบทบาทเป็นผู้ดูแลระบบและโดเมนจากการล็อกอินระยะไกล .rhosts โดยเปลี่ยนเป็นการใช้คำสั่ง Newrole ที่ต้องมีการตรวจสอบสิทธิซ้ำ

ป้องกันการรบกวนการทำงาน ของการประมวลผลของระบบหรือของผู้ดูแลระบบ โดยจำกัดการเข้าถึง ข้อมูล procfs ของการประมวลผลในโดเมนอื่น ๆ ไว้เฉพาะการทำงานของการประมวลผลของระบบ หรือของผู้ดูแลระบบ และควบคุมการใช้ ptrace ของการประมวลผลอื่น ๆ มีการกำหนดประเภทแยกจากกัน สำหรับhome directory ของยูสเซอร์กับผู้ดูแลระบบ

ป้องกันยูสเซอร์และผู้ดูแลระบบ จากการถูกโจมตีจุดบกพร่องในโปรแกรมเบราเซอร์ โดยการเอ็กซิคิวท์รหัส ที่อาจทำให้เกิดความเสียหาย โดยการกำหนดโดเมนและการอนุญาต ที่ต่างออกไปสำหรับเบราเซอร์ ในการอ่านไฟล์

รูปที่ 3.4 แสดงตัวอย่างความสัมพันธ์ระหว่างโดเมน ที่มีการกำหนดไว้ในนโยบายตัวอย่างของเอสอีลินุกซ์ ซึ่งเมื่อเริ่มต้นระบบ เคอร์เนลของระบบที่อยู่ในโดเมน kernel_t จะทำการผันตัวเข้าสู่โดเมน init_t เพื่อทำการการประมวลผลการเริ่มต้นระบบ และเซทค่าในส่วนต่าง ๆ ส่วนโดเมน inetd_t เป็นการเซทระบบการติดต่อสู่เน็ตเวิร์ก ส่วนโดเมน remote_login_t เป็นโดเมนที่จัดการการล็อกอินระยะไกล โดยที่จำกัดสิทธิในการล็อกอินได้เพียงการเป็นผู้ใช้งานระบบธรรมดาเท่านั้น ไม่สามารถล็อกอินในระดับผู้ควบคุมระบบได้ โดยที่โดเมน local_login_t ที่ควบคุมการล็อกอินระยะใกล้ จะสามารถทำการล็อกอินได้ทั้งการเป็นผู้ใช้งานระบบธรรมดา และระดับผู้ควบคุมระบบ



รูปที่ 3.4 ตัวอย่างความสัมพันธ์ระหว่างโดเมนของเอสอีลินุกซ์

จากจุดประสงค์ของการปรับแต่งนโยบายตัวอย่างที่มีใช้ในเอสอีลินุกซ์ พบว่ามีการมุ่งควบคุมการเข้าถึงข้อมูลต่าง ๆ ในระบบให้มีความละเอียดและมีประสิทธิภาพมากขึ้น โดยใช้หลักของการอนุญาตสิทธิให้การประมวลผลและโปรแกรมต่าง ๆ เท่าที่จำเป็นในการใช้งานจริง ทำให้สามารถป้องกันข้อบกพร่อง จากระบบลินุกซ์ทั่ว ๆ ไปได้ ในส่วนของการกำหนดการควบคุมการเข้าถึง ซึ่งในตัวอย่างของนโยบายควบคุมการเข้าถึง ไม่ได้ทำการปกป้องจุดบกพร่องประเภทอื่น ๆ แต่จากการกำหนดสิทธิการเอ็กซิคิวท์และโดเมนที่จำกัด ทำให้สามารถป้องกันความสูญเสียในส่วนของการล่วงละเมิดระบบได้

3.5.2 แอลไอดีเอส

แอลไอดีเอส (LIDS – Linux Intrusion Detection System) เป็นระบบตรวจจับผู้บุกรุกบนระบบลินุกซ์ ที่ได้รับการพัฒนาให้มีความสามารถในการป้องกันการบุกรุก โดยการเพิ่มองค์ประกอบในส่วนของการควบคุมการเข้าถึง โดยมีพื้นฐานจากการกำหนดการเพิ่มเติมสิทธิระดับรากแบบพีโอเอสไอเอกซ์ (POSIX Capability)

ส่วนของการควบคุมการเข้าถึงของแอลไอดีเอส ประกอบด้วย 2 ส่วนคือ ส่วนที่มีการกำหนดโดยการกำหนดกฎของการเข้าถึงและส่วนของการกำหนดการเพิ่มเติมสิทธิระดับรากแบบพีโอเอสไอเอกซ์ โดยในการกำหนดการเข้าถึงโดยกำหนดกฎนั้น ได้มีการกำหนดไว้ 4 ลักษณะคือ 1.ปฏิเสธ (deny) 2.อ่านอย่างเดียว (read) 3. เพิ่มเติม (append) และ 4.เขียน (write)

ส่วนของการกำหนดการเพิ่มเติมสิทธิระดับรากแบบพีโอเอสไอเอกซ์ แอลไอดีเอส ได้มีการออกแบบส่วนต่อประสานที่ทำให้การจัดการปรับแต่งส่วนของการเพิ่มเติมสิทธิระดับรากแบบพีโอเอสไอเอกซ์ได้สะดวกขึ้น และมีการเพิ่มเติมการกำหนดการเพิ่มเติมสิทธิระดับรากอีก 3 รูปแบบ ตามตารางที่ 3.2

ตารางที่ 3.2 แสดงการกำหนดการเพิ่มเติมสิทธิพื้นฐานที่ใช้ในลินุกซ์

Linux Capability	Descriptions
CAP_CHOWN	Override restrictions on changing file ownership and group ownership
CAP_DAC_OVERRIDE	Override all DAC access on files
CAP_DAC_READ_SEARCH	Overrides all DAC restrictions regarding read and search on files and directories
CAP_FOWNER	Overrides all restrictions about allowed operations on files, where file owner ID must be equal to the user ID
CAP_FSETID	Overrides the following restrictions that the effective user ID shall match the file owner ID when setting the S_ISUID and S_ISGID bits on that file

ตารางที่ 3.2 แสดงการกำหนดการเพิ่มเติมสิทธิพื้นฐานที่ใช้ในลินุกซ์ (ต่อ)

Linux Capability	Descriptions
CAP_KILL	Overrides the restriction that the real or effective user ID of a process sending a signal must match the real or effective user ID of the process receiving the signal.
CAP_SETGID	Allows setgid(2) manipulation
CAP_SETUID	Allows set*uid(2) manipulation (including fsuid).
CAP_SETPCAP	Transfer any capability in your permitted set to any pid, remove any capability in your permitted set from any pid
CAP_LINUX_IMMUTABLE	Allow modification of S_IMMUTABLE and S_APPEND file attributes
CAP_NET_BIND_SERVICE	Allows binding to TCP/UDP sockets below 1024
CAP_NET_BROADCAST	Allow broadcasting, listen to multicast
CAP_NET_ADMIN	Administration of the network interfaces, firewall, routing tables, masquerading, etc
CAP_NET_RAW	Allow use of RAW sockets
CAP_IPC_LOCK	Allow locking of shared memory segments
CAP_IPC_OWNER	Override IPC ownership checks
CAP_SYS_MODULE	Insert and remove kernel modules - modify kernel without limit
CAP_SYS_RAWIO	Allow ioperm/iopl access
CAP_SYS_CHROOT	Allow use of chroot()
CAP_SYS_PTRACE	Allow ptrace() of any process
CAP_SYS_PACCT	Allow configuration of process accounting
CAP_SYS_ADMIN	Many admin task, disk quota, setting domainname, setting hostname, mount, etc
CAP_SYS_BOOT	Allow use of reboot()
CAP_SYS_NICE	Allow raising priority and setting priority on other (different UID) processes
CAP_SYS_RESOURCE	Override resource limits, set resource limits
CAP_SYS_TIME	Allow manipulation of system clock
CAP_SYS_TTY_CONFIG	Allow configuration of tty devices
CAP_MKNOD	Allow the privileged aspects of mknod()
CAP_LEASE	Allow taking of leases on files

ตารางที่ 3.3 แสดงการกำหนดการเพิ่มเติมสิทธิที่มีการเพิ่มเติมโดยแอลไอดีเอส

Linux Capability	Descriptions
CAP_HIDDEN	Restricts viewable processes by a user
CAP_KILL_PROTECTED	Allow to kill protected processes
CAP_PROTECTED	Protect process against signals

จากตารางที่ 3.2 - 3.3 เป็นการแสดงความสามารถของการทำงานระดับรากที่มีการแยกกำหนดให้กับการประมวลผลต่าง ๆ ในแอลไอดีเอส ซึ่งแต่ละการประมวลผลจะได้รับสิทธิการดำเนินการเพียงเฉพาะอย่าง เท่าที่จำเป็นต้องใช้งานจริงเท่านั้น เพื่อป้องกันการการโจมตีโดยอาศัยสิทธิของการประมวลผล

จากการวิเคราะห์ตัวอย่างการปรับแต่งนโยบายความปลอดภัยของแอลไอดีเอส พบว่ามีการกำหนดการควบคุมการเข้าถึงให้กับไฟล์ข้อมูล ที่อยู่ในระบบในส่วนที่เป็นไบนารีไฟล์ ไลบรารีไฟล์ ไฟล์ข้อมูลการปรับแต่งระบบ ไฟล์ในระบบการตรวจสอบสิทธิผู้ใช้งาน ส่วนการเริ่มระบบ และแฟ้มลงบันทึกเข้าออก และจำกัดสิทธิการทำงานของการประมวลผลที่มีเอกสิทธิในการติดต่อกับอุปกรณ์ไอโอ การเชื่อมต่อพอร์ตและอำนาจในการปรับเปลี่ยนระบบบางประการ เพื่อจำกัดความสามารถของผู้ใช้งานระดับราก

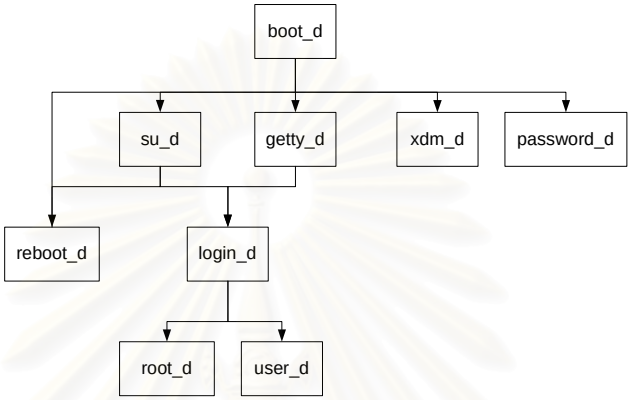
3.5.3 ดีทีอี

ดีทีอี (DTE – Domain and Type Enforcement) เป็นรูปแบบของการควบคุมการเข้าถึงที่มีการจำกัดการเข้าถึงทรัพยากรระบบ ของการประมวลผลแต่ละตัว ตามความต้องการของการประมวลผลนั้น ๆ ทำให้มีการจัดแบ่งกลุ่มให้กับการประมวลผลและทรัพยากรในระบบ และกำหนดนโยบายของการควบคุมการเข้าถึง แตกต่างกันออกไป ตามประเภท ของการประมวลผลและทรัพยากร การกำหนดนโยบายเพื่อควบคุมการเข้าถึงทรัพยากรระบบในดีทีอี มีการกำหนดดังนี้คือ

1. โดเมน (domain) เป็นการกำหนดกลุ่มของการประมวลผล และความสามารถในการเข้าถึงทรัพยากรในระบบ และกำหนดการส่งสัญญาณระหว่างการประมวลผลในต่างโดเมน

2. ประเภท (type) เป็นการกำหนดคลาสให้กับข้อมูลและทรัพยากรต่าง ๆ ที่มีในระบบ

รูปที่ 3.5 แสดงความสัมพันธ์ระหว่างโดเมนในนโยบายตัวอย่างของดีทีอี ซึ่งมีการกำหนดไว้เฉพาะการเริ่มต้นระบบ และการล็อกอินเท่านั้น ซึ่งจะคล้ายกับการกำหนดไว้ในเอสอีลินุกซ์ โดยในดีทีอี ได้กำหนดโดเมนของผู้ใช้งานระบบธรรมดา แยกออกจากผู้ใช้งานระดับราก ซึ่งมีการกำหนดระดับของการเข้าถึงไฟล์ข้อมูลในระบบที่ต่างกัน



รูปที่ 3.5 แสดงความสัมพันธ์ระหว่างโดเมนของดีทีอี

จากตัวอย่างนโยบายของดีทีอี จะเห็นว่า โครงสร้างของนโยบายมีการกำหนดโดเมนและประเภทให้กับการเริ่มต้นระบบและการควบคุมการเข้าสู่ระบบของผู้ใช้งาน โดยแยกส่วนระหว่างผู้ใช้งานทั่วไปกับผู้ใช้งานระดับราก และมีการกำหนดสิทธิในการเข้าถึงไฟล์ข้อมูลต่าง ๆ ในระบบทำให้สามารถป้องกันการเข้าถึงไฟล์ข้อมูลในระดับรากได้

3.6 การประเมินผลการป้องกันจุดอ่อนของแต่ละวิธี

จากการวิเคราะห์การทำงาน ของวิธีเพิ่มความปลอดภัยให้กับระบบลินุกซ์ทั้ง 4 วิธี จะเห็นว่าการดำเนินการเพิ่มความแข็งแกร่งให้กับระบบ เป็นลักษณะของการแก้ไขปัญหาที่เกิดขึ้นกับระบบซึ่งจะเป็นการป้องกันการโจมตีจุดอ่อนโดยการกำจัดส่วนที่มีความเสี่ยงที่จะทำให้ถูกโจมตี อาจเรียกได้ว่าเป็นการป้องกันจุดอ่อนในทางตรง ส่วนวิธีการของแอลเอสเอ็ม จะเป็นลักษณะของการเพิ่มประสิทธิภาพในการควบคุมการเข้าถึงของทรัพยากรระบบในรูปแบบต่าง ๆ ซึ่งจะเป็นการป้องกันการโจมตีจุดอ่อน โดยการกันการเข้าถึงจุดอ่อน หรือลดความเสียหายที่เกิดจากการโจมตีจุดอ่อนแล้ว ทำให้การทำงานในส่วนของแอลเอสเอ็ม สามารถป้องกันการสิทธิเพิ่มเติม จากการโจมตี หรือเป็นการป้องกันการที่ทั้งระบบจะถูกล่วงละเมิด และจากการวิเคราะห์นโยบายตัวอย่างของมอดูลด้านความปลอดภัยตัวอย่างในรูปแบบแอลเอสเอ็ม เห็นว่าเป็นนโยบายที่มุ่งเน้นในการป้องกันการเข้าถึงข้อมูลระดับเคอร์เนลของระบบ การแก้ไขปรับแต่งระบบเป็นหลัก

อนึ่ง การประเมินความสามารถในการป้องกันจุดอ่อนในงานวิจัยนี้ ได้ทำการพิจารณาจากลักษณะโครงสร้างและการทำงานของการเสริมความปลอดภัยในแต่ละวิธีเท่านั้น ไม่ได้รวมถึงการทดสอบการทำงานจริง ผลที่ได้จากการวิจัยนี้ จึงเป็นเพียงแนวทางและแนวโน้มของความสามารถในการป้องกันจุดอ่อนเท่านั้น

จากการรวบรวมข้อมูลจุดอ่อน ปรับปรุงการจัดกลุ่มของจุดอ่อนเพื่อให้เหมาะสม และทำการวิเคราะห์การทำงานของขั้นตอนในการเสริมความปลอดภัยให้กับระบบทั้ง การเสริมความแข็งแกร่ง และการดำเนินการตามโครงร่างแอลเอสเอ็ม และมอดูลตัวอย่างด้านความปลอดภัยของแอลเอสเอ็มแล้ว ในบทต่อไป จะเป็นการประเมินผลการทำงานของลักษณะดังกล่าว ในการลดจำนวนจุดอ่อนที่เกิดขึ้นในระบบลินุกซ์

บทที่ 4
ผลการวิจัย

จากการศึกษา วิเคราะห์การทำงานและประเมินความสามารถในการป้องกันจุดอ่อนของการดำเนินการเสริมความปลอดภัยของทั้งการเสริมความปลอดภัย (OS Hardening) และโครงร่างแอลเอสเอ็ม (LSM Framework) ทำให้ได้ผลการวิจัยดังนี้

4.1 รูปแบบการจัดกลุ่มของจุดอ่อน

ในงานวิจัยนี้ได้มีการปรับแต่งรูปแบบของการจัดแบบกลุ่มของจุดอ่อนเพื่อให้เหมาะสมกับการวิเคราะห์ความสามารถของตัวปรับแต่งระบบ โดยจากการปรับแต่งที่เกิดขึ้น ทำให้ได้รูปแบบของการจัดแบ่งกลุ่มเพื่อประกอบในการวิเคราะห์การป้องกันจุดอ่อนซึ่งรูปแบบของการจัดแบ่งได้ 3 ลักษณะ ประกอบด้วย

การจัดกลุ่มโดยแบ่งตามประเภทของจุดอ่อน

การจัดกลุ่มตามตำแหน่งที่เกิดจุดอ่อน

การจัดกลุ่มตามลักษณะความเสียหายจากการโจมตีจุดอ่อน

ซึ่งรายละเอียดของการจัดแบ่งในแต่ละวิธี แสดงไว้ตามตารางที่ 4.1-4.3

ตารางที่ 4.1 แสดงการจัดกลุ่มตามประเภทของจุดอ่อนที่ใช้ในงานวิจัย

Genesis	Input Validation Error
	Boundary Condition Error
	Access Validation Error
	Serialization
	Configuration Error
	Environmental Error
	Design Error
	Exceptional Handling Error
	Others

ตารางที่ 4.2 แสดงการจัดกลุ่มตามตำแหน่งที่เกิดจุดอ่อนที่ใช้ในงานวิจัย

Location	System Initialization
	Memory Management
	Process Management
	Device Management
	File Management
	Authentication
	Support
	Application

ตารางที่ 4.3 แสดงการจัดกลุ่มตามลักษณะความเสียหายของการโจมตีที่ใช้ในงานวิจัย

Security Violation	Confidentiality
	Integrity
	Availability
	System compromised
	Run Arbitrary Code
	Elevated Privilege
	Account Break-in
	Root Break-in

4.2 ค่าดัชนีความเปราะบางตั้งต้นของลินุกซ์

จากการจัดกลุ่มและให้คะแนนจุดอ่อนที่เกิดขึ้นกับระบบปฏิบัติการลินุกซ์ที่ได้จากรายการซีวีอีทั้งสิ้น 388 รายการ โดยกลุ่มของจุดอ่อนที่นำมาใช้ในงานวิจัยทุกตัว จะต้องมีข้อมูลรายละเอียดของจุดอ่อนที่ครบถ้วน ตามรูปที่ 3.3 และจากรายการของจุดอ่อนที่ใช้ ข้อมูลของจุดอ่อนในส่วนของประเภท และตำแหน่งที่เกิดจุดอ่อน ไม่มีเหตุการณ์ที่เกิดร่วมกัน (Mutually exclusive) และจุดอ่อนสามารถก่อให้เกิดความเสียหายได้มากกว่า 1 ลักษณะ โดยคะแนนของจุดอ่อนในแต่ละความเสียหาย จะมีระดับความรุนแรงเดียวกัน เมื่อทำการให้คะแนนตามความรุนแรงและผลการโจมตี ทำให้สามารถกำหนดดัชนีความตั้งต้นของลินุกซ์ทั้งหมดเป็น 1216 คะแนน สามารถแสดงรายละเอียดดังตารางที่ 4.4 - 4.5

ตารางที่ 4.4 ค่าดัชนีความเปราะบางตั้งต้นโดยแบ่งตามประเภทของจุดอ่อน

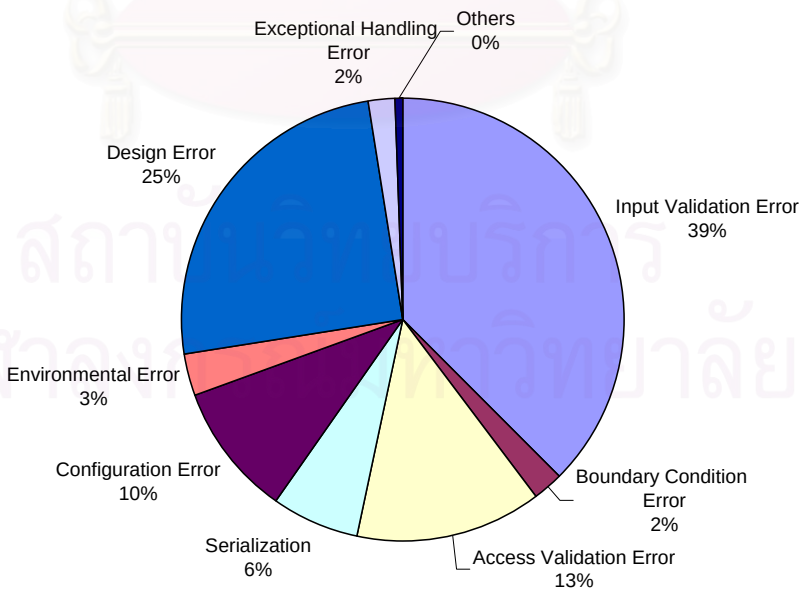
No.	Genesis	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	Input Validation Error	9	12	56	380	457
2	Boundary Condition Error	2	0	12	12	26
3	Access Validation Error	18	37	11	98	164
4	Serialization	0	33	6	39	78
5	Configuration Error	30	19	5	65	119
6	Environmental Error	4	7	7	20	38
7	Design Error	28	39	67	169	303
8	Exceptional Handling Error	2	0	16	7	25
9	Others	0	0	0	6	6
	Total	93	147	180	796	1216

ตารางที่ 4.4 เป็นคะแนนความเปราะบางตั้งต้นของระบบลินุกซ์ โดยแจกแจงตามประเภทของจุดอ่อน ผลคะแนนที่ได้ ทั้งหมด 1216 คะแนน แยกตามประเภท ของความเสียหายที่เกิดจากการโจมตีจุดอ่อน ความเสียหายประเภทสูญเสียความลับ 93 คะแนน ความเสียหายประเภทสูญเสียบูรณภาพของระบบ 147 คะแนน ความเสียหายประเภทสูญเสียสภาพพร้อมใช้งาน 180 คะแนน และความเสียหายประเภทระบบถูกล่วงละเมิด 796 คะแนน ซึ่งคะแนนเหล่านี้สามารถอธิบายในรูปแบบกราฟได้ ดังรูปที่ 4.1

ตารางที่ 4.5 ค่าดัชนีความเปราะบางตั้งต้นโดยแบ่งตามตำแหน่งที่เกิดจุดอ่อน

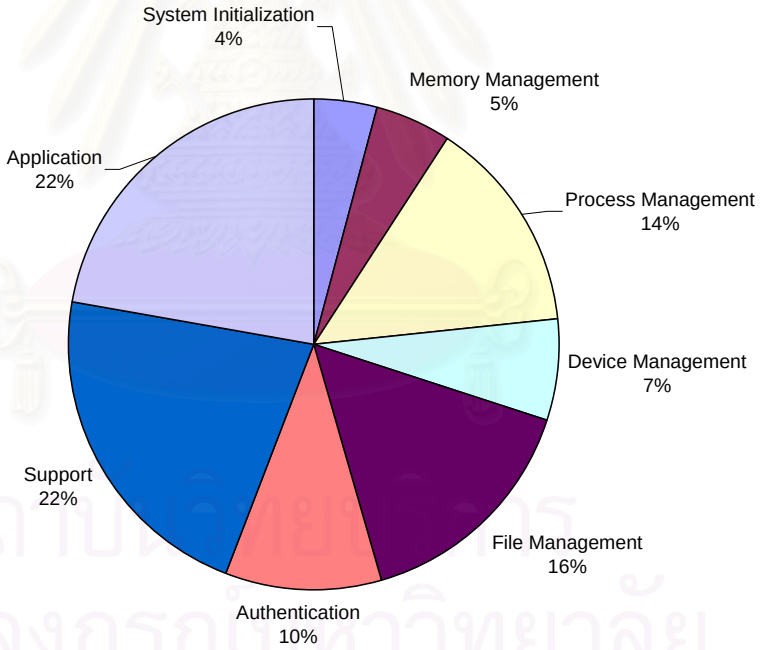
No.	Location	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	System Initialization	4	4	15	26	49
2	Memory Management	0	7	10	47	64
3	Process Management	9	13	41	108	171
4	Device Management	12	9	21	38	80
5	File Management	21	55	24	89	189
6	Authentication	7	12	5	103	127
7	Support	25	26	25	189	265
8	Application	15	21	39	196	271
	Total	93	147	180	796	1216

ตารางที่ 4.5 เป็นการแจกแจงคะแนนความเปราะบางตั้งต้นของลินุกซ์ตามตำแหน่งของการเกิดจุดอ่อน โดยแจกแจงตามประเภทของความเสียหายที่เกิดขึ้นจากการโจมตีจุดอ่อน ซึ่งคะแนนเหล่านี้สามารถอธิบายในรูปแบบกราฟได้ ดังรูปที่ 4.2



รูปที่ 4.1 แผนภาพสัดส่วนเชิงปริมาณของจุดอ่อนที่พบในแต่ละประเภท

รูปที่ 4.1 แสดงสัดส่วนเชิงปริมาณของจุดอ่อนที่พบในระบบลินุกซ์ซึ่งแบ่งตามประเภทของจุดอ่อน จะพบว่า จุดอ่อนที่มีจำนวนมากที่สุดที่พบในระบบคือ ความผิดพลาดของการตรวจสอบข้อมูลนำเข้า (Input Validation Error) ซึ่งคิดเป็น 39% ของปริมาณจุดอ่อนที่ตรวจพบในระบบลินุกซ์ รองลงมาเป็นจุดอ่อนที่เกิดจากความผิดพลาดของการออกแบบระบบ (Design Error) คิดเป็น 25% ของปริมาณจุดอ่อนที่ตรวจพบในระบบลินุกซ์ อันดับสามเป็นจุดอ่อนที่เกิดจากความผิดพลาดของการตรวจสอบการเข้าถึงข้อมูล (Access Validation Error) ซึ่งคิดเป็น 13% ของปริมาณจุดอ่อนที่ตรวจพบในระบบลินุกซ์ ตามด้วยจุดอ่อนที่เกิดจากความผิดพลาดของการปรับแต่งระบบ (Configuration Error) ความเหลื่อมล้ำของการตรวจสอบสิทธิ (Serialization) ความผิดพลาดจากสภาพแวดล้อม (Environmental Error) ความผิดพลาดจากขอบเขตข้อมูล (Boundary Condition Error) ความผิดพลาดจากการจัดการข้อยกเว้น (Exceptional Handling Error)และความผิดพลาดอื่นๆ (Other) ตามลำดับ



รูปที่ 4.2 แผนภาพสัดส่วนเชิงปริมาณของจุดอ่อนที่พบแบ่งตามตำแหน่งของจุดอ่อน

รูปที่ 4.2 แสดงสัดส่วนเชิงปริมาณของจุดอ่อนที่พบโดยแบ่งตามตำแหน่งที่เกิดจุดอ่อน จะเห็นว่า ตำแหน่งของระบบที่มีจุดอ่อนมากที่สุด คือ โปรแกรมสนับสนุนการทำงานของระบบ (Support) และโปรแกรมประยุกต์ (Application) ซึ่งมีปริมาณของจุดอ่อนตำแหน่งละ 22% ของปริมาณจุดอ่อนทั้งหมดที่พบในระบบ รวมกันเป็น 44% ของจุดองจุดอ่อนทั้งหมด อันดับสามเป็นส่วนการจัดการแฟ้มข้อมูล (File Management) ซึ่งมีจุดอ่อนคิดเป็น 16% ของปริมาณจุดอ่อนที่พบในระบบลินุกซ์ จากนั้นเป็นส่วนจัดการการประมวลผล (Process Management) ส่วนการพิสูจน์ตัวจริง (Authentication) ส่วนการจัดการอุปกรณ์ (Device Management) ส่วนการจัดการหน่วยความจำ (Memory Management) และส่วนการเริ่มต้นระบบ (System Initialization) ตามลำดับ

4.3 ค่าดัชนีความเปราะบางของลินุกซ์เมื่อใช้การเสริมความแข็งแกร่ง

จากการวิเคราะห์การดำเนินการ ของการเสริมความแข็งแกร่งพบว่า การเสริมความแข็งแกร่งนั้น สามารถช่วยลดจุดอ่อน ตามที่มีการระบุคำแนะนำไว้ในรายการซีวีอี เป็นจำนวนทั้งสิ้น 300 ตัว คิดเป็น 966 คะแนน ซึ่งจุดอ่อนดังกล่าว มีการกระจายอยู่ในประเภท และ ตำแหน่งต่าง ๆ ในระบบ นอกจากนี้ ขั้นตอนของการปรับแต่งระบบให้มีความเหมาะสม จะสามารถลดการเกิดจุดอ่อนที่อยู่ในประเภทความผิดพลาดจากการปรับแต่งระบบ (Configuration Error) นอกเหนือ จาก ส่วนที่สามารถแก้ไขโดยการติดตั้งส่วนต่อของโปรแกรม (patch) เพิ่มเติมอีก 12 ตัว คิดเป็น 35 คะแนนได้ ทำให้ค่าดัชนีความเปราะบางเมื่อดำเนินการเสริมความแข็งแกร่งในระบบลินุกซ์ มีค่าเหลือ 215 คะแนน ซึ่งสามารถแสดงรายละเอียดโดยแบ่งตามประเภทของจุดอ่อน ได้ดังตารางที่ 4.6 และรายละเอียดตามตำแหน่งที่เกิดจุดอ่อน ได้ดังตารางที่ 4.7

ตารางที่ 4.6 ดัชนีความเปราะบางเมื่อเสริมความแข็งแกร่ง ตามประเภทของจุดอ่อน

No.	Genesis	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	Input Validation Error	0	2	17	52	71
2	Boundary Condition Error	0	0	2	5	7
3	Access Validation Error	4	16	0	18	38
4	Serialization	0	3	0	5	8
5	Configuration Error	0	0	0	0	0
6	Environmental Error	0	0	2	0	2
7	Design Error	1	12	31	36	80
8	Exceptional Handling Error	0	0	6	3	9
9	Others	0	0	0	0	0
	Total	5	33	58	119	215

ตารางที่ 4.7 ดัชนีความเปราะบางเมื่อเสริมความแข็งแกร่ง ตามตำแหน่งที่เกิดจุดอ่อน

No.	Location	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	System Initialization	0	0	5	0	5
2	Memory Management	0	2	2	2	6
3	Process Management	0	2	11	12	25
4	Device Management	1	2	13	8	24
5	File Management	4	11	4	23	42
6	Authentication	0	5	2	11	18
7	Support	0	7	6	34	47
8	Application	0	4	15	29	48
	Total	5	33	58	119	215

ตารางที่ 4.6-4.7 เป็นการแจกแจงค่าดัชนีความเปราะบางของการเสริมความแข็งแกร่งของลินุกซ์ที่ได้จากการวิเคราะห์ในบทที่ 3 โดยตารางที่ 4.6 แจกแจกรายละเอียดตามประเภทของจุดอ่อน และ ตารางที่ 4.7 แจกแจงตามตำแหน่งที่เกิดจุดอ่อน ผลคะแนนที่ได้ ทั้งหมด 215 คะแนน แยกตามประเภท ของความเสียหายที่เกิดจากการโจมตีจุดอ่อน ความเสียหายประเภทสูญเสียความลับ 5คะแนน ความเสียหายประเภทสูญเสียบูรณภาพของระบบ 33 คะแนน ความเสียหายประเภทสูญเสียสภาพพร้อมใช้งาน 58 คะแนน และความเสียหายประเภทล่วงละเมิดระบบ 119 คะแนน

4.4 ค่าดัชนีความเปราะบางของลินุกซ์เมื่อดำเนินการตามโครงร่างแอลเอสเอ็ม

จากการวิเคราะห์การดำเนินการของโครงร่างงแอลเอสเอ็ม พบว่า โครงร่างแอลเอสเอ็มที่สมบูรณ์ ต้องติดตั้งโดยมีมอดูลด้านความปลอดภัย ทำงานประกอบกัน ซึ่งในงานวิจัยนี้ ได้ทำการวิเคราะห์ถึงการทำงานของมอดูลด้านความปลอดภัยตัวอย่างที่ดำเนินการตามโครงร่างแอลเอสเอ็ม ซึ่งในการวิเคราะห์การทำงานพบว่า การป้องกันจุดอ่อนเมื่อดำเนินการตามโครงร่างแอลเอสเอ็มและมอดูลตัวอย่างดังกล่าว สามารถแบ่งได้ 2 ส่วน คือ

โครงสร้างของแอลเอสเอ็ม

โครงสร้างและ ฟังก์ชันการทำงานของมอดูลด้านความปลอดภัย

4.4.1 โครงสร้างของแอลเอสเอ็ม

จากการวิเคราะห์โครงสร้างของโครงร่างแอลเอสเอ็มในบทที่ 3 พบว่า จากโครงสร้างของแอลเอสเอ็ม สามารถป้องกันการเกิดจุดอ่อนในส่วนที่เกิดจากความเหลื่อมล้ำของการตรวจสอบสิทธิ ซึ่งมีทั้งหมด 25 ตัว คิดเป็น 81 คะแนน

4.4.2 โครงสร้างและ ฟังก์ชันการทำงานของมอดูลด้านความปลอดภัย

จากการวิเคราะห์โครงสร้าง และฟังก์ชันการทำงานของมอดูลด้านความปลอดภัยตัวอย่างในบทที่ 3 พบว่า ทั้ง 3 มอดูลซึ่งได้แก่ เอสอีลินุกซ์ แอลไอดีเอส และดีทีอี เป็นมอดูลที่มีฟังก์ชันในการตรวจสอบสิทธิ และควบคุมการเข้าถึงในระบบ ทำให้สามารถป้องกันจุดอ่อน ในประเภทความผิดพลาดของระบบความคุมการเข้าถึงได้ เป็นจำนวน 49 ตัว คิดเป็น 164 คะแนน และ เนื่องจากมีการแยกสิทธิสำหรับแต่ละการประมวลผลในระบบ ดังนั้นจึงสามารถป้องกัน การล่วงละเมิดระบบจากการโจมตีจุดอ่อนได้

นอกจากนั้น เมื่อทำการวิเคราะห์จาก รูปแบบการปรับแต่ง และ นโยบายตัวอย่าง ที่กำหนดมาพร้อมกับมอดูลพบว่า ทั้ง 3 มอดูล สามารถป้องกันจุดอ่อนในลักษณะต่าง ๆ เพิ่มเติมอีก ซึ่งสามารถแสดงได้ดังต่อไปนี้

4.4.2.1 เอสอีลินุกซ์

จากการวิเคราะห์การทำงานของมอดูลเอสอีลินุกซ์ พบว่าส่วนนโยบายตัวอย่างที่มีการกำหนดไว้ เป็นการกำหนดสิทธิของอ็อบเจคที่มีในระบบ เพื่อใช้ในการควบคุมการเข้าถึง ซึ่งจะทำให้สามารถป้องกันจุดอ่อนที่ทำให้เกิดความเสียหายในการล่วงละเมิดระบบ ที่เกิดในตำแหน่งต่างๆ ทุกส่วน ยกเว้นส่วนของโปรแกรมประยุกต์ที่ไม่ได้มีการกำหนดนโยบายไว้

ทำให้เมื่อใช้เอสอีลินุกซ์เป็นมอดูลด้านความปลอดภัย จะทำให้สามารถป้องกัน จุดอ่อนที่เกิดจากความผิดพลาดของการการควบคุมการเข้าถึง และการเหลื่อมล้ำในการตรวจสอบสิทธิ ในส่วนต่าง ๆ ของระบบ ยกเว้นส่วนโปรแกรมประยุกต์ และสามารถป้องกันการล่วงละเมิดระบบจากการโจมตีจุดอ่อนใด ๆ โดยทำให้ค่าดัชนีความเปราะบางของลินุกซ์ลดลงเหลือ 285 ซึ่งสามารถแสดงรายละเอียดได้ดังตารางที่ 4.8-4.9

ตารางที่ 4.8 ดัชนีความเปราะบางเมื่อติดตั้งเอสอีลินุกซ์ ตามประเภทของจุดอ่อน

No.	Genesis	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	Input Validation Error	9	12	56	0	77
2	Boundary Condition Error	2	0	12	0	14
3	Access Validation Error	5	9	3	0	17
4	Serialization	0	3	0	0	3
5	Configuration Error	4	0	0	0	4
6	Environmental Error	4	7	7	0	18
7	Design Error	28	39	67	0	134
8	Exceptional Handling Error	2	0	16	0	18
9	Others	0	0	0	0	0
	Total	57	70	161	0	285

ตารางที่ 4.9 ดัชนีความเปราะบางเมื่อติดตั้งเอสอีลินุกซ์ ตามตำแหน่งที่เกิดจุดอ่อน

No.	Location	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	System Initialization	2	4	12	0	18
2	Memory Management	0	7	10	0	17
3	Process Management	9	8	39	0	56
4	Device Management	7	2	21	0	30
5	File Management	10	13	15	0	38
6	Authentication	2	4	2	0	8
7	Support	9	11	23	0	43
8	Application	15	21	39	0	75
	Total	57	70	161	0	285

ตารางที่ 4.8-4.9 เป็นการแจกแจงค่าดัชนีความเปราะบางของการใช้แอลเอสเอ็มโดยมีเอสอีลินุกซ์เป็นมอดูลด้านความปลอดภัยที่ได้จากการวิเคราะห์ในบทที่ 3 โดยตารางที่ 4.8 แจกแจกรายละเอียดตามประเภทของจุดอ่อน และ ตารางที่ 4.9 แจกแจงตามตำแหน่งที่เกิดจุดอ่อน ผลคะแนนที่ได้ ทั้งหมด 285 คะแนน แยกตามประเภท ของความเสียหายที่เกิดจากการโจมตีจุดอ่อน ความเสียหายประเภทสูญเสียความลับ 57คะแนน ความเสียหายประเภทสูญเสียบูรณภาพของระบบ 70 คะแนน ความเสียหายประเภทสูญเสียสภาพพร้อมใช้งาน 161 คะแนน และความเสียหายประเภทล่วงละเมิดระบบ 0 คะแนน

4.4.2.2 แอลไอดีเอส

จากการวิเคราะห์การทำงานของมอดูลแอลไอดีเอส พบว่าในตัวอย่างของการปรับแต่งการควบคุมการเข้าถึง ที่มีการกำหนดไว้นั้น ได้ควบคุมการเข้าถึงการใช้งานในส่วนการเริ่มต้นระบบ ส่วนการจัดการหน่วยความจำ ส่วนการจัดการการประมวลผล ส่วนการจัดการแฟ้มข้อมูล และส่วนการพิสูจน์ตัวจริง จึงสามารถป้องกันจุดอ่อน ที่เกิดขึ้นในตำแหน่งดังกล่าว ที่มีผลในการล่วงละเมิดระบบได้ แต่ในส่วนการจัดการอุปกรณ์ ส่วนโปรแกรม ที่สนับสนุนการทำงานระบบปฏิบัติการ และส่วนโปรแกรมประยุกต์ ไม่ได้มีการกำหนดการควบคุมการเข้าถึงไว้

ทำให้เมื่อใช้แอลไอดีเอสเป็นมอดูลด้านความปลอดภัย จะทำให้สามารถป้องกัน จุดอ่อนที่เกิดจากความผิดพลาดจากการปรับแต่งระบบ ความผิดพลาดของการการควบคุมการเข้าถึง และ

การเหลื่อมล้ำในการตรวจสอบสิทธิ ในส่วนต่าง ๆ ของระบบ ยกเว้นส่วนการจัดการอุปกรณ์ ส่วนโปรแกรม ที่สนับสนุนการทำงานระบบ ปฏิบัติการ และส่วนโปรแกรมประยุกต์ และสามารถป้องกันการล่วงละเมิดระบบจากการโจมตีจุดอ่อนใด ๆ โดยทำให้ค่าดัชนีความเปราะบางของลินุกซ์ลดลงเหลือ 335 ซึ่งสามารถแสดงรายละเอียดได้ดังตารางที่ 4.10-4.11

ตารางที่ 4.10 ดัชนีความเปราะบางเมื่อติดตั้งแอลไอดีเอส ตามประเภทของจุดอ่อน

No.	Genesis	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	Input Validation Error	9	12	56	0	77
2	Boundary Condition Error	2	0	12	0	14
3	Access Validation Error	5	9	3	0	17
4	Serialization	0	3	0	0	3
5	Configuration Error	30	19	5	0	54
6	Environmental Error	4	7	7	0	18
7	Design Error	28	39	67	0	134
8	Exceptional Handling Error	2	0	16	0	18
9	Others	0	0	0	0	0
	Total	80	89	166	0	335

ตารางที่ 4.11 ดัชนีความเปราะบางเมื่อติดตั้งแอลไอดีเอสตามตำแหน่งที่เกิดจุดอ่อน

No.	Location	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	System Initialization	4	4	15	0	23
2	Memory Management	0	7	10	0	17
3	Process Management	9	8	39	0	56
4	Device Management	9	6	21	0	36
5	File Management	12	15	15	0	42
6	Authentication	7	9	2	0	18
7	Support	24	19	25	0	68
8	Application	15	21	39	0	75
	Total	80	89	166	0	335

ตารางที่ 4.10-4.11 เป็นการแจกแจง ค่าดัชนีความเปราะบางของการใช้แอลเอสเอ็มโดยมีแอลไอดีเอสเป็นมอดูลด้านความปลอดภัย ที่ได้จากการวิเคราะห์ในบทที่ 3 โดยตารางที่ 4.10 แจกแจกรายละเอียดตามประเภทของจุดอ่อน และ ตารางที่ 4.11 แจกแจงตามตำแหน่งที่เกิดจุดอ่อน ผลคะแนนที่ได้ ทั้งหมด 335 คะแนน แยกตามประเภท ของความเสียหายที่เกิดจากการโจมตีจุดอ่อน ความเสียหายประเภทสูญเสียความลับ 80 คะแนน ความเสียหายประเภทสูญเสียบูรณภาพของระบบ 89 คะแนน ความเสียหายประเภทสูญเสียสภาพพร้อมใช้งาน 166 คะแนน และความเสียหายประเภทล่วงละเมิดระบบ 0 คะแนน

4.4.2.3 ดีทีอี

จากการวิเคราะห์การทำงานของมอดูลดีทีอี พบว่าในตัวอย่างของการปรับแต่งการควบคุมการเข้าถึง ที่มีการกำหนดไว้นั้น ได้ควบคุมการเข้าถึงการใช้งานในส่วนการเริ่มต้นระบบ ส่วนการจัดการหน่วยความจำ ส่วนการจัดการการประมวลผล ส่วนการจัดการแฟ้มข้อมูล และส่วนการพิสูจน์ตัวจริง จึงสามารถป้องกันจุดอ่อน ที่เกิดขึ้นในตำแหน่งดังกล่าว ที่มีผลในการล่วงละเมิดระบบได้ แต่ในส่วนการจัดการอุปกรณ์ ส่วนโปรแกรม ที่สนับสนุนการทำงานระบบ ปฏิบัติการ และส่วนโปรแกรมประยุกต์ ไม่ได้มีการกำหนดการควบคุมการเข้าถึงไว้

ทำให้เมื่อใช้ดีทีอีเป็นมอดูลด้านความปลอดภัย จะทำให้สามารถป้องกัน จุดอ่อนที่เกิดจากความผิดพลาดของการการควบคุมการเข้าถึง และการเหลื่อมล้ำในการตรวจสอบสิทธิ ในส่วนต่าง ๆ ของระบบ ยกเว้นส่วนการจัดการอุปกรณ์ ส่วนโปรแกรม ที่สนับสนุนการทำงานระบบปฏิบัติการ และส่วนโปรแกรมประยุกต์ และสามารถป้องกันการล่วงละเมิดระบบจากการโจมตีจุดอ่อนใด ๆ โดยทำให้ค่าดัชนีความเปราะบางของลินุกซ์ลดลงเหลือ 341 ซึ่งสามารถแสดงรายละเอียดได้ดังตารางที่ 4.12-4.13

ตารางที่ 4.12 ดัชนีความเปราะบางเมื่อติดตั้งดีทีอี ตามประเภทของจุดอ่อน

No.	Genesis	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	Input Validation Error	9	12	56	0	77
2	Boundary Condition Error	2	0	12	0	14
3	Access Validation Error	8	9	3	0	20
4	Serialization	0	6	0	0	6
5	Configuration Error	30	19	5	0	54
6	Environmental Error	4	7	7	0	18
7	Design Error	28	39	67	0	134
8	Exceptional Handling Error	2	0	16	0	18
9	Others	0	0	0	0	0
	Total	83	92	166	0	341

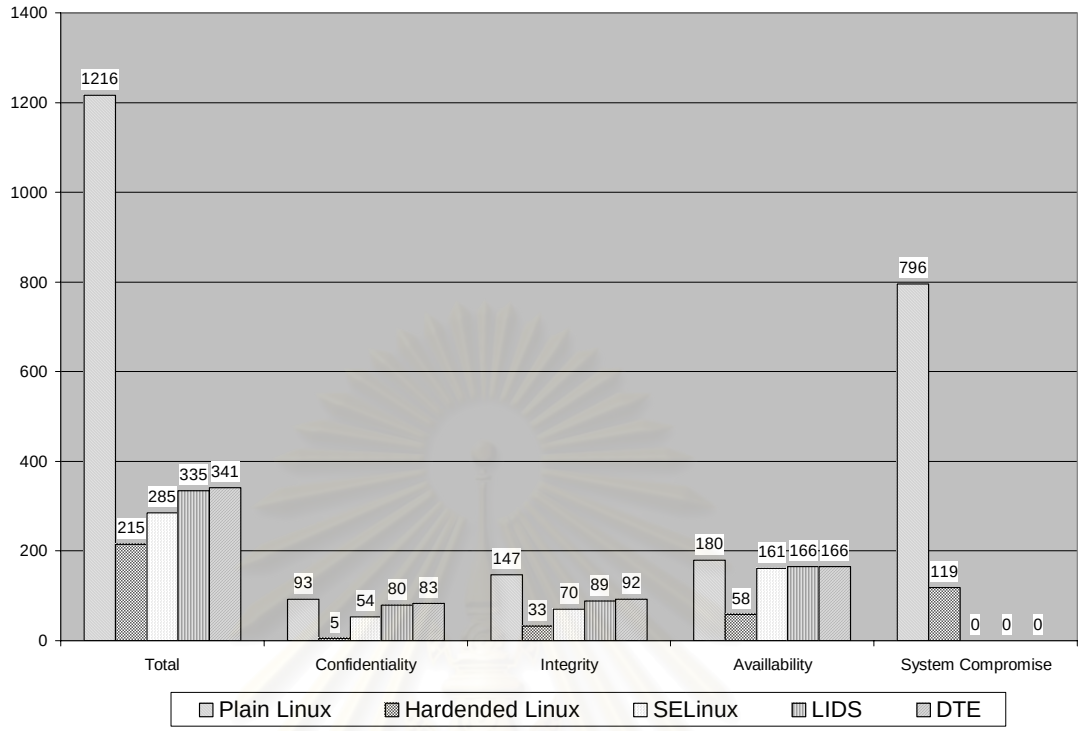
ตารางที่ 4.13 ดัชนีความเปราะบางเมื่อติดตั้งดีทีอี ตามตำแหน่งที่เกิดจุดอ่อน

No.	Location	Loss Type				Total
		Confidentiality	Integrity	Availability	System Compromise	
1	System Initialization	4	4	15	0	23
2	Memory Management	0	7	10	0	17
3	Process Management	9	8	39	0	56
4	Device Management	12	9	21	0	42
5	File Management	12	15	15	0	42
6	Authentication	7	9	2	0	18
7	Support	24	19	25	0	68
8	Application	15	21	39	0	75
	Total	83	92	166	0	341

ตารางที่ 4.12-4.13 เป็นการแจกแจง ค่าดัชนีความเปราะบางของการใช้แอลเอสเอ็มโดยมีแอลไอดีเอสเป็นมอดูลด้านความปลอดภัย ที่ได้จากการวิเคราะห์ในบทที่ 3 โดยตารางที่ 4.12 แจกแจกรายละเอียดตามประเภทของจุดอ่อน และ ตารางที่ 4.13 แจกแจงตามตำแหน่งที่เกิดจุดอ่อน ผลคะแนนที่ได้ ทั้งหมด 335 คะแนน แยกตามประเภท ของความเสียหายที่เกิดจากการโจมตีจุดอ่อน ความเสียหายประเภทสูญเสียความลับ 83 คะแนน ความเสียหายประเภทสูญเสียบูรณภาพของระบบ 92 คะแนน ความเสียหายประเภทสูญเสียสภาพพร้อมใช้งาน 166 คะแนน และความเสียหายประเภทล่วงละเมิดระบบ 0 คะแนน

4.5 การเปรียบเทียบความสามารถในการป้องกันจุดอ่อน

จากผลการวิเคราะห์ความสามารถในการป้องกันจุดอ่อนของการเสริมความปลอดภัยแบบต่างๆ จะเห็นว่า แต่ละวิธีสามารถทำให้จุดอ่อนที่เกิดขึ้นในระบบลดลงในปริมาณที่ต่างกัน ดังสามารถแสดงในรูปที่ 4.3



รูปที่ 4.3 กราฟเปรียบเทียบค่าดัชนีความเปราะบางของลินุกซ์ แยกตามความเสียหาย

จากรูปที่ 4.3 แสดงถึงการเปรียบเทียบค่าดัชนีความเปราะบางของลินุกซ์ ระหว่าง ระบบลินุกซ์ปกติ ระบบลินุกซ์ที่มีการเสริมความแข็งแกร่ง ระบบลินุกซ์ที่มีการติดตั้งเอสอีลินุกซ์ แอลไอดีเอส และดีทีอี โดยแจกแจงตามความเสียหายของการโจมตีจุดอ่อน ซึ่งประกอบด้วย ความเสียหายประเภทสูญเสียความลับ (Confidentiality) ความเสียหายประเภทสูญเสียบูรณภาพของระบบ (Integrity) ความเสียหายประเภทสูญเสียสภาพพร้อมใช้งาน (Availability) และความเสียหายประเภทระบบถูกล่วงละเมิด (System Compromise)

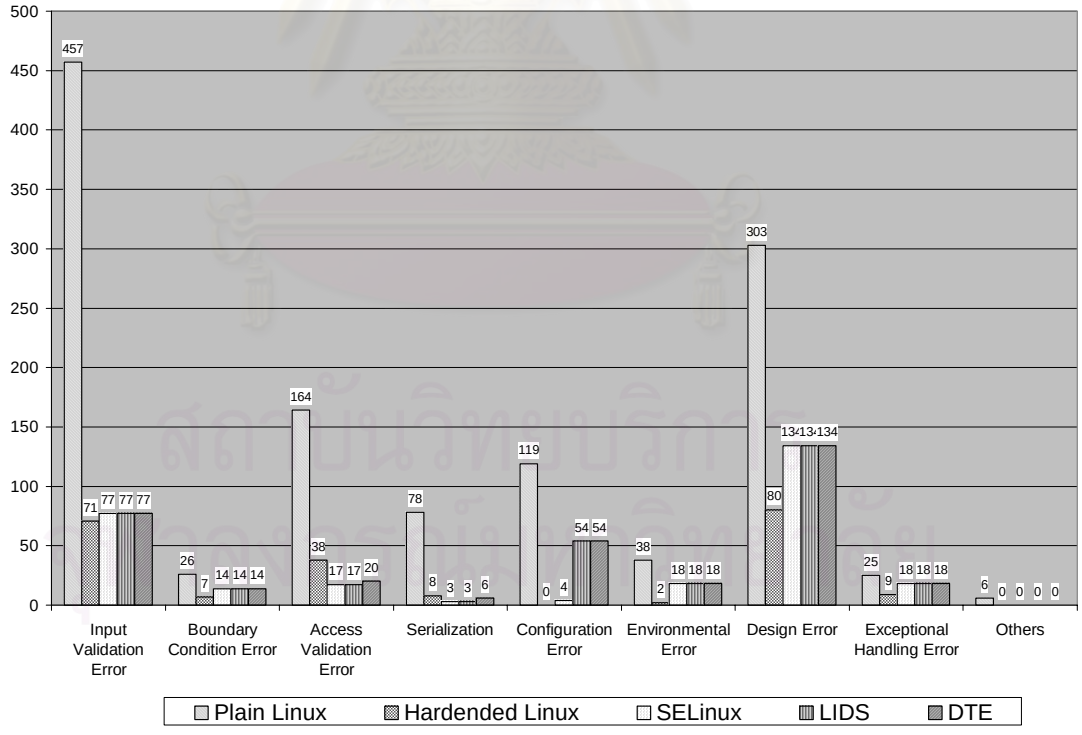
เมื่อพิจารณาผลรวมของจุดอ่อนทั้งหมด จะเห็นได้ว่า การเสริมความแข็งแกร่ง เป็นวิธีที่สามารถลดจุดอ่อนได้มากที่สุด โดยสามารถทำให้จุดอ่อนในระบบลดลงไปถึง 82.32% ของจุดอ่อนทั้งหมด เอสอีลินุกซ์เป็นวิธีการลดจุดอ่อนได้มากเป็นอันดับสอง โดยสามารถลดจุดอ่อนลงได้ 76.56% ของจุดอ่อนทั้งหมด ส่วนแอลไอดีเอส และ ดีทีอี สามารถลดจุดอ่อนได้ 72.45% และ 71.96% ตามลำดับ

เมื่อพิจารณาแยกตามลักษณะความเสียหายประเภทต่าง ๆ จะพบว่า การดำเนินการเสริมความปลอดภัยให้กับลินุกซ์ทั้ง 4 วิธี มีความสามารถในการลดจุดอ่อนที่แตกต่างกัน โดยสามารถแสดงเปอร์เซ็นต์การลดลงของจุดอ่อนโดยวิธีต่าง ๆ โดยแบ่งตามลักษณะความเสียหายที่เกิดขึ้นได้ดังตารางที่ 4.14

ตารางที่ 4.14 เปอร์เซ็นต์การลดลงของจุดอ่อน แยกตามลักษณะความเสียหาย

Los Type	OS Hardening	SELinux	LIDS	DTE
Confidentiality	94.62%	41.94%	13.98%	10.75%
Integrity	77.55%	52.38%	39.46%	37.41%
Avaliability	67.78%	10.56%	7.78%	7.78%
System Compromised	85.05%	100%	100%	100%

เมื่อสังเกตเปอร์เซ็นต์การลดลงของ ค่าดัชนีความเปราะบางของลินุกซ์เมื่อดำเนินการด้านความปลอดภัยแต่ละประเภท โดยพิจารณาตามลักษณะความเสียหาย จะพบว่า การดำเนินการตามโครงร่างแอลเอสเอ็มสามารถ ป้องกันให้ระบบไม่ถูกล่วงละเมิด จากการโจมตีจุดอ่อนได้ดีกว่าการเสริมความแข็งแกร่ง ในขณะที่การเสริมความแข็งแกร่ง สามารถป้องกันความเสียหายที่เกิดจากการโจมตีระบบโดยตรง ซึ่งประกอบด้วย ความเสียหายประเภทสูญเสียความลับ ความเสียหายประเภทสูญเสียบูรณภาพของระบบ และความเสียหายประเภทสูญเสียสภาพพร้อมใช้งานได้ดีกว่าแอลเอสเอ็ม



รูปที่ 4.4 กราฟเปรียบเทียบค่าดัชนีความเปราะบางของลินุกซ์แยกตามประเภทของจุดอ่อน

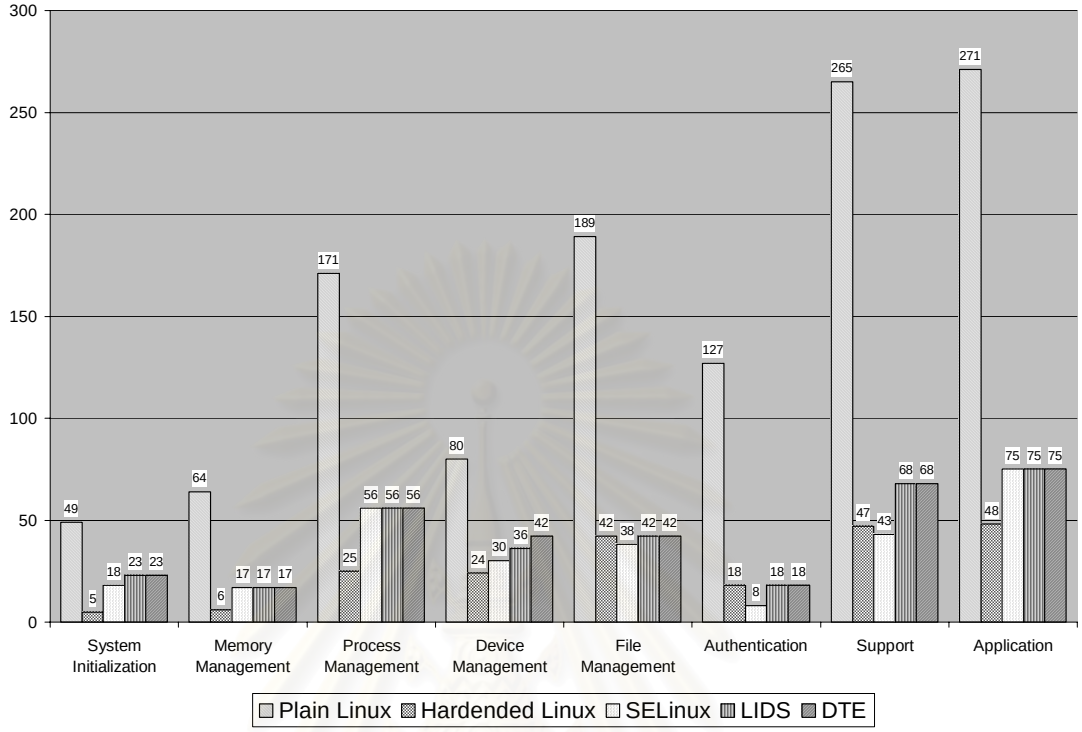
จากรูปที่ 4.4 แสดงถึงการเปรียบเทียบค่าดัชนีความเปราะบางของลินุกซ์ ระหว่าง ระบบลินุกซ์ปกติ ระบบลินุกซ์ที่มีการเสริมความแข็งแกร่ง ระบบลินุกซ์ที่มีการติดตั้งเอสอีลินุกซ์ แอลไอดีเอส และดีทีอี โดยแจกแจงตามประเภทของจุดอ่อน ซึ่งประกอบด้วย จุดอ่อนที่เกิดจาก ความผิดพลาดของการตรวจสอบข้อมูลนำเข้า ความผิดพลาดของขอบเขตข้อมูล ความผิดพลาดในการตรวจสอบการเข้าถึง ความผิดพลาดของการเหลื่อมล้ำของการตรวจสอบสิทธิ ความผิดพลาดของการปรับแต่งระบบ ความผิดพลาดจากสภาพแวดล้อม ความผิดพลาดจากการออกแบบระบบ ความผิดพลาดจากชุดคำสั่งจัดการสิ่งผิดปกติ และความผิดพลาดแบบอื่น ๆ

เมื่อพิจารณาแยกตามประเภทของจุดอ่อน จะพบว่า การดำเนินการเสริมความปลอดภัยให้กับลินุกซ์ทั้ง 4 วิธี มีความสามารถในการลดจุดอ่อนที่แตกต่างกัน โดยสามารถแสดงเปอร์เซ็นต์การลดลงของจุดอ่อนโดยวิธีต่าง ๆ โดยแบ่งตามประเภทของจุดอ่อนได้ดังตารางที่ 4.15

ตารางที่ 4.15 เปอร์เซ็นต์การลดลงของจุดอ่อน แยกตามประเภทของจุดอ่อน

Genesis	OS Hardening	SELinux	LIDS	DTE
Input Validation Error	84.46%	83.15%	83.15%	83.15%
Boundary Condition Error	73.08%	46.15%	46.15%	46.15%
Access Validation Error	76.83%	89.63%	89.63%	89.63%
Serialization	89.74%	96.15%	96.15%	96.15%
Configuration Error	100%	96.64%	54.62%	54.62%
Environmental Error	73.60%	55.78%	55.78%	55.78%
Design Error	73.60%	55.78%	55.78%	55.78%
Exceptional Handling Error	64%	28%	28%	28%
Others	100%	100%	100%	100%

เมื่อสังเกตเปอร์เซ็นต์การลดลงของ ค่าดัชนีความเปราะบางของลินุกซ์เมื่อดำเนินการด้านความปลอดภัยแต่ละประเภท โดยพิจารณาตามประเภทของจุดอ่อน จะเห็นว่า การเสริมความแข็งแกร่ง สามารถป้องกันการเกิดจุดอ่อนที่อยู่ในประเภท ความผิดพลาดของขอบเขตข้อมูล ความผิดพลาดของการปรับแต่งระบบ ความผิดพลาดจากสภาพแวดล้อม ความผิดพลาดจากการออกแบบระบบ และความผิดพลาดจากชุดคำสั่งจัดการสิ่งผิดปกติ ได้ดีกว่าการใช้แอลเอสเอ็ม โดยที่การใช้แอลเอสเอ็มสามารถป้องกันจุดอ่อนที่อยู่ในประเภท ความผิดพลาดในการตรวจสอบการเข้าถึง ความผิดพลาดของการเหลื่อมล้ำของการตรวจสอบสิทธิ ได้ดีกว่าการเสริมความแข็งแกร่ง และทั้ง 2 วิธี มีความสามารถในการป้องกันจุดอ่อนในประเภท ความผิดพลาดของการตรวจสอบข้อมูลนำเข้า และความผิดพลาดแบบอื่น ๆ ได้ใกล้เคียงกัน



รูปที่ 4.5 กราฟเปรียบเทียบค่าดัชนีความเปราะบางของลินุกซ์ แยกตามตำแหน่งของจุดอ่อน

จากรูปที่ 4.5 แสดงถึงการเปรียบเทียบค่าดัชนีความเปราะบางของลินุกซ์ ระหว่าง ระบบลินุกซ์ปกติ ระบบลินุกซ์ที่มีการเสริมความแข็งแกร่ง ระบบลินุกซ์ที่มีการติดตั้งเอสอีลินุกซ์ แอลไอดีเอส และดีทีอี โดยแจกแจงตามความเสียหายของการโจมตีจุดอ่อน ซึ่งประกอบด้วย ส่วนการเริ่มต้นระบบ ส่วนการจัดการหน่วยความจำ ส่วนการจัดการการประมวลผล ส่วนการจัดการอุปกรณ์ ส่วนการจัดการแฟ้มข้อมูล ส่วนการพิสูจน์ตัวจริง ส่วนโปรแกรมที่สนับสนุนการทำงานระบบปฏิบัติการ และส่วนโปรแกรมประยุกต์

เมื่อพิจารณาแยกตามตำแหน่งที่เกิดจุดอ่อน จะพบว่า การดำเนินการเสริมความปลอดภัยให้กับลินุกซ์ทั้ง 4 วิธี มีความสามารถในการลดจุดอ่อนที่แตกต่างกัน โดยสามารถแสดงเปอร์เซ็นต์การลดลงของจุดอ่อนโดยวิธีต่าง ๆ โดยแบ่งตาม ตำแหน่งที่เกิดจุดอ่อน ได้ดังตารางที่ 4.16

ตารางที่ 4.16 เปอร์เซ็นต์การลดลงของจุดอ่อน แยกตามตำแหน่งที่เกิดจุดอ่อน

Location	OS Hardening	SELinux	LIDS	DTE
System Initialization	89.80 %	63.27%	53.06%	53.06%
Memory Management	90.63 %	73.44%	73.44%	73.44%
Process Management	85.38%	67.25%	67.25%	67.25%
Device Management	70%	62.50%	55%	47.50%
File Management	77.78%	79.89%	77.78%	77.78%
Authentication	85.83%	93.70%	85.83%	85.83%
Support	82.26 %	83.77%	74.34%	74.34%
Application	82.29%	72.32%	72.32%	72.32%

เมื่อสังเกตเปอร์เซ็นต์การลดลงของ ค่าดัชนีความเปราะบางของลินุกซ์เมื่อดำเนินการด้านความปลอดภัยแต่ละประเภท โดยพิจารณาตามตำแหน่งที่เกิดจุดอ่อน จะพบว่า โดยภาพรวม การเสริมความแข็งแกร่ง สามารถลดจุดอ่อนที่เกิดขึ้นในส่วนต่าง ๆ ระบบได้ดีกว่าแอลเอสเอ็ม ยกเว้นส่วนการจัดการแฟ้มข้อมูล และส่วนการพิสูจน์ตัวจริง ที่การใช้เอสอีลินุกซ์สามารถลดจุดอ่อนที่เกิดขึ้นได้ดีกว่าวิธีอื่น ทั้งนี้เนื่องจากลักษณะการกำหนดนโยบายของเอสอีลินุกซ์

4.6 อภิปรายผลการวิจัย

จากผลของดัชนีความเปราะบางที่ได้ของทั้ง 2 วิธีนั้น จะเห็นว่าการเสริมความแข็งแกร่งสามารถป้องกันจุดอ่อนได้มากกว่าการใช้แอลเอสเอ็ม แต่เมื่อทำการวิเคราะห์ในรายละเอียด จะเห็นว่า ทั้งการเสริมความแข็งแกร่ง และการใช้แอลเอสเอ็มนั้น สามารถป้องกันจุดอ่อนในรูปแบบที่ต่างกัน จึงไม่สามารถสรุปได้ว่า การใช้การเสริมความแข็งแกร่ง ทำให้ระบบปลอดภัยกว่าการใช้แอลเอสเอ็ม ทั้งนี้ ต้องคำนึงถึงลักษณะการใช้งานและความต้องการด้านความปลอดภัยที่ต่างกันของแต่ละระบบด้วย

เมื่อทำการพิจารณาลักษณะความเสียหายของเซิร์ฟเวอร์ตัวอย่าง ตามตารางที่ ข.1 ในภาคผนวก ข โดยรวบรวมจาก [24] และสามารถสรุปลักษณะความเสียหายที่สำคัญในเซิร์ฟเวอร์ตัวอย่างได้ดังตารางที่ 4.17

ตารางที่ 4. 17 ลักษณะความเสียหายที่สำคัญในเซิร์ฟเวอร์ประเภทต่าง ๆ

Server Type	Most Critical Loss Type
Mail Server	Confidentiality
Web Server	Availability
FTP Server	Confidentiality
DNS Server	Availability
Gateway Server	Availability
File sharing Server	System Compromised
Database Server	System Compromised
VPN Server	System Compromised

จากตารางที่ 4.17 จะเห็นว่า เซิร์ฟเวอร์ที่ทำหน้าที่ให้บริการด้านระบบร่วมแฟ้ม (File Sharing Server) ระบบฐานข้อมูล (Database Server) และวีพีเอ็น (VPN Server) มีความต้องการในการป้องกันความเสียหายจากการล่วงละเมิดระบบ มากกว่าเซิร์ฟเวอร์อื่นๆ ซึ่งในแง่มุมนี้ แอลเอสเอ็มสามารถแก้ปัญหาได้ดีกว่าการเสริมความแข็งแกร่ง ดังนั้น จากผลการวิจัยที่ได้ ทำให้สามารถเสนอวิธีการเสริมความปลอดภัยที่เหมาะสมกับเซิร์ฟเวอร์ประเภทต่าง ๆ ได้ดังตารางที่ 4.18

ตารางที่ 4. 18 วิธีการเสริมความปลอดภัยที่เหมาะกับเซิร์ฟเวอร์ประเภทต่าง ๆ

Server Type	Most Critical Loss Type	Recommended Method
Mail Server	Confidentiality	OS Hardening
Web Server	Availability	OS Hardening
FTP Server	Confidentiality	OS Hardening
DNS Server	Availability	OS Hardening
Gateway Server	Availability	OS Hardening
File sharing Server	System Compromised	LSM
Database Server	System Compromised	LSM
VPN Server	System Compromised	LSM

ในบทที่ 4 ที่ผ่านมา เป็นข้อมูลผลการดำเนินการวิจัย โดยผลที่ได้ ประกอบด้วย วิธีการจัดแบ่งกลุ่มจุดอ่อนใช้ในงานวิจัย ข้อมูลของจุดอ่อนที่รวบรวมได้ การให้คะแนนจุดอ่อน ผลค่าดัชนีความเปราะบางของลินุกซ์และการเปรียบเทียบความสามารถในการลดจุดอ่อน เมื่อดำเนินการตามการเสริมความแข็งแกร่ง และ มอดูลด้านความปลอดภัยของแอลเอสเอ็ม ซึ่งประกอบด้วย เอสอีลินุกซ์ แอลไอดีเอส และดีทีอี และในบทที่ 5 จะทำการสรุปผลการวิจัยที่ได้ และเสนอข้อเสนอแนะที่เกี่ยวข้องกับงานวิจัยต่อไป

บทที่ 5
สรุปผลการวิจัย และข้อเสนอแนะ

จากการดำเนินการวิเคราะห์การทำงานของการดำเนินการเสริมความปลอดภัยในลินุกซ์ในแบบต่างๆ และได้ผลของค่าดัชนีความอ่อนแอของลินุกซ์ปกติ และลินุกซ์เมื่อดำเนินการเสริมความปลอดภัยในแบบต่างๆ ทำให้สามารถสรุปผลการวิจัย และเสนอแนะแนวทางเพื่อการทำวิจัยต่อไป ได้ดังนี้

5.1 สรุปผลการวิจัย

จากการศึกษาและวิจัยเพื่อประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์โดยการเพิ่มความแข็งแกร่งกับการใช้แอลเอสเอ็ม สามารถสรุปผลการวิจัยได้ดังต่อไปนี้

1. ความสามารถในการป้องกันจุดอ่อน ของการป้องกันรูปแบบต่าง ๆ ที่ได้ทำการวิจัย สามารถจัดลำดับจากมากไปน้อย ได้ดังนี้ การเสริมความแข็งแกร่ง สามารถป้องกันจุดอ่อนที่สามารถเกิดขึ้นในระบบลินุกซ์ได้ 82.32% เอสอีลินุกซ์ สามารถป้องกันได้ 76.56% แอลไอดีเอส สามารถป้องกันได้ 72.45% และ ดีทีอี สามารถป้องกันได้ 71.96%
2. การดำเนินการตามโครงร่างแอลเอสเอ็มสามารถ ป้องกันให้ระบบจากการถูกล่วงละเมิดจากการโจมตีจุดอ่อนได้ดีกว่าการเสริมความแข็งแกร่ง ในขณะที่การเสริมความแข็งแกร่งสามารถป้องกันความเสียหายที่เกิดจากการโจมตีระบบโดยตรง ซึ่งประกอบด้วย ความเสียหายประเภทสูญเสียความลับ ความเสียหายประเภทสูญเสียบูรณภาพของระบบ และความเสียหายประเภทสูญเสียสภาพพร้อมใช้งาน ได้ดีกว่าแอลเอสเอ็ม
3. การเสริมความแข็งแกร่ง สามารถป้องกันการเกิดจุดอ่อนที่อยู่ในประเภท ความผิดพลาดของขอบเขตข้อมูล ความผิดพลาดของการปรับแต่งระบบ ความผิดพลาดจากสภาพแวดล้อม ความผิดพลาดจากการออกแบบระบบ และความผิดพลาดจากชุดคำสั่งจัดการสิ่งผิดปกติ ได้ดีกว่าการใช้แอลเอสเอ็ม โดยที่การใช้แอลเอสเอ็มสามารถป้องกันจุดอ่อนที่อยู่ในประเภท ความผิดพลาดในการตรวจสอบการเข้าถึง ความผิดพลาดของการเหลื่อมล้ำของการตรวจสอบสิทธิ ได้ดีกว่าการเสริมความแข็งแกร่ง และทั้ง 2 วิธี มีความสามารถในการป้องกันจุดอ่อนในประเภท ความผิดพลาดของการตรวจสอบข้อมูลนำเข้า และความผิดพลาดแบบอื่น ๆ ได้ใกล้เคียงกัน
4. การเสริมความแข็งแกร่ง สามารถลดจุดอ่อนที่เกิดขึ้นในส่วนต่าง ๆ ระบบได้ดีกว่าแอลเอสเอ็ม ยกเว้น ส่วนการจัดการแฟ้มข้อมูล และส่วนการพิสูจน์ตัวจริง ที่การใช้เอสอีลินุกซ์

สามารถลดจุดอ่อนที่เกิดขึ้นได้ดีกว่าวิธีอื่น ทั้งนี้เนื่องจากลักษณะการกำหนดนโยบายของเอสอีลินุกซ์ มีความละเอียดในการป้องกันการเข้าถึงที่ส่วนดังกล่าว

5. การเสริมความแข็งแกร่ง เหมาะกับการใช้งานกับเมลล์เซิร์ฟเวอร์ เวบเซิรฟเวอร์ เอฟทีพีเซิร์ฟเวอร์ ดีเอนเอสเซิร์ฟเวอร์ และ เกตเวย์เซิร์ฟเวอร์ ซึ่งเป็นเซิร์ฟเวอร์ประเภทอินเตอร์เน็ตเซิร์ฟเวอร์ (Internet Server) ส่วนแอลเอสเอ็มเหมาะกับเซิร์ฟเวอร์ที่ทำหน้าที่ให้บริการด้านระบบร่วมแฟ้ม ระบบฐานข้อมูล และวีพีเอ็น ซึ่งเป็นเซิร์ฟเวอร์ประเภทอินทราเน็ตเซิร์ฟเวอร์ (Intranet Server)

5.2 **ข้อเสนอแนะ**

จากการดำเนินการวิจัย จนได้ข้อสรุปแล้วนั้น ได้มีจุดที่ควรคำนึงถึงเมื่อมีการเลือกใช้การเสริมความปลอดภัยในระบบลินุกซ์ ดังนี้

1. ผลที่ได้จากการประเมินความสามารถในการป้องกันจุดอ่อนนี้ เป็นผลที่ได้จากการวิเคราะห์ลักษณะโครงสร้างของการดำเนินการในแต่ละประเภท ดังนั้น ค่าที่ได้จากการประเมินนี้ จึงเป็นค่าประมาณที่มีแนวโน้มใกล้เคียงกับการใช้งานจริงที่มีการดำเนินการตามที่ได้มีการกำหนดไว้ในงานวิจัยนี้
2. การดำเนินการปรับแต่งระบบโดยตัวปรับแต่ง (patch) ของการเสริมความแข็งแกร่ง เป็นการแก้ไขข้อผิดพลาดของระบบโดยตรง ซึ่งจำเป็นต้องมีการตรวจสอบและดำเนินการอย่างสม่ำเสมอ เพื่อให้สามารถป้องกันจุดอ่อนของระบบได้อย่างมีประสิทธิภาพ
3. การเสริมความปลอดภัยให้กับระบบโดยการดำเนินการตามแอลเอสเอ็มนั้น เป็นการเพิ่มความสามารถในการควบคุมการเข้าถึงให้มีความละเอียดมากยิ่งขึ้น ข้อคำนึงถึงในการเลือกใช้การปรับแต่งระบบในแบบนี้ คือการกำหนดนโยบายที่เพียงพอต่อการทำงานของระบบ และไม่ขัดต่อการทำงานหลักของระบบ

5.3 **งานวิจัยในอนาคต**

จากงานวิจัยนี้ ยังมีประเด็นที่สามารถนำมาทำการวิจัยต่อเนื่องได้ ดังนี้

1. การประเมินจุดอ่อนและการปรับแต่งที่มีใช้ในระบบปฏิบัติการอื่นๆ ที่สามารถลดการเกิดจุดอ่อนในระบบปฏิบัติการนั้นๆ ได้
2. การเปรียบเทียบ และประเมินการป้องกันจุดอ่อน ระหว่างระบบปฏิบัติการลินุกซ์ กับระบบปฏิบัติการอื่น ๆ
3. การประเมินความสามารถในการป้องกันจุดอ่อน โดยใช้การป้องกันระบบแบบอื่น ๆ เช่น การใช้เทคโนโลยีช่องอากาศ (Air Gap) ระหว่างการติดต่อผ่านเน็ตเวิร์ค

รายการอ้างอิง

1. Loscocco, P., et al. The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments. Proceedings of 21th National Information Systems Security Conference. 1998.
2. Bauer, M.D. Building Secure Server with Linux. O'Reilly, 2002.
3. Ferraiolo, D. and Kuhn, R. Role-Bases Access Controls. Proceedings of 15th National Computer Security Conference. 1992.
4. Common Vulnerability and Exposure. [Online]. Available from: http://cve.mitre.org: [2004, Feb 14]
5. Amoroso, E.G. Fundamentals of Computer Security Technology. Upper Saddle River, NJ: Prentice-Hall PTR, 1994.
6. Aslam, T., Krsul, I., and Spafford, E.H. Use of Taxonomy of Security Faults. Proceedings of Proc. 19th NIST-NCSC National Information Systems Security Conference. 1996.
7. Landwehr, C.E., et al. A Taxonomy of Computer Program Security Flaws. ACM Computing Surveys 26 (1994): 211-254.
8. Jiwnani, K. and Zelkowitz, M. Maintaining Software with a Security Perspective. Proceedings of IEEE International Conference on Software Maintenance (ICSM'02). 2002.
9. Frisch, A. Essential System Administration, 3rd Edition. O?Reilly & Associates, 2002.
10. Wright, C., et al. Linux Security Module Framework. Proceedings of The Ottawa Linux Symposium 2002. 2002.
11. Smalley, S., Vance, A., and Salaman, W. *Implementing SELinux as a Linux Security Module*. 2002, NSA: SELinux Technical Report.
12. Spencer, R., Smalley, S., and Loscocco, P. The Flask Architecture: System Support for Diverse Security Policies. Proceedings of the Eighth USENIX Security Symposium. 1999.
13. Huagang, X. *Building a Secure System with LIDS*. 2002, Linux Intrusion Detection System.

14. Hatch, B. An Overview of LIDS, Part One. [Online]. Available from: http://www.securityfocus.com/infocus/1496: [2004, Feb 14]

15. Hatch, B. An Overview of LIDS, Part Two. [Online]. Available from: http://www.securityfocus.com/infocus/1502: [2004, Feb 14]

16. Hatch, B. An Overview of LIDS, Part Three. [Online]. Available from: http://www.securityfocus.com/infocus/1510: [2004, Feb 14]

17. Hatch, B. An Overview of LIDS, Part Four. [Online]. Available from: http://www.securityfocus.com/infocus/1517: [2004, Feb 14]

18. Hallyn, S. and Kearns, P. Domain and Type Enforcement for Linux. Proceedings of 4th Annual Linux Showcase and Conference. 2000.

19. Badger, L., Sterne, D.F., and al., e. A Domain and Type Enforcement UNIX Prototype. Proceedings of the USENIX Security Conference. 1995.

20. Badger, L., et al. Practical Domain and Type Enforcement for UNIX. Proceedings of Security and Privacy, 1995. Proceedings., 1995 IEEE Symposium on. 1995.

21. Munsee, C.L. and Lee, C. Security Evaluation of the Linux Operating System. [Online]. Available from: http://islab.oregonstate.edu/koc/ece478/project/2002RP/ML.pdf: [2004, Mar 12]

22. Larabee, R. A Comparison of SELinux and LIDS. [Online]. Available from: http://www.giac.org/practical/Rick_Larabee_GSEC.doc: [2004, Feb 15]

23. Edwards, A. and Zhang, X. Using CQUAL for static Analysis of Authorization Hook Placement. Proceedings of USENIX Security Symposium. 2002.

24. The Twenty Most Critical Internet Security Vulnerabilities. [Online]. Available from: http://www.sans.org/top20/: SANS Institute, [2004, Apr 21]

25. Mourani, G. Securing and Optimizing Linux: The Ultimate Solution. Open Network Architecture, Inc, 2001.

ภาคผนวก

ภาคผนวก ก

รายละเอียดของจุดอ่อนที่พบบนระบบลินุกซ์ที่คัดกรองมาจากรายการซีวีอี

ในส่วนนี้จะแสดงรายการของจุดอ่อนที่พบบนระบบลินุกซ์ที่คัดกรองมาจากรายการซีวีอีที่ใช้ในงานวิจัยนี้ จำนวนทั้งสิ้น 388 ตัว ซึ่งมีการแสดงรายละเอียดของจุดอ่อนดังนี้

CVE Number หมายเลขอ้างอิงจากรายการซีวีอี

Description รายละเอียดของจุดอ่อนที่ระบุในรายการซีวีอี

CVE Number	Description
CAN-1999-0061	File creation and deletion, and remote execution, in the BSD line printer daemon (lpd).
CAN-1999-0123	Race condition in Linux mailx command allows local users to read user files.
CAN-1999-0171	Denial of service in syslog by sending it a large number of superfluous messages.
CAN-1999-0216	Denial of service of inetd on Linux through SYN and RST packets.
CAN-1999-0242	Remote attackers can access mail files via POP3 in some Linux systems that are using shadow passwords.
CAN-1999-0243	Linux cfingerd could be exploited to gain root access.
CAN-1999-0257	Nestea variation of teardrop IP fragmentation denial of service.
CAN-1999-0298	ypbind with -ypset and -ypsetme options activated in Linux Slackware and SunOS allows local and remote attackers to overwrite files via a .. (dot dot) attack.
CAN-1999-0317	Buffer overflow in Linux su command gives root access to local users.
CAN-1999-0330	Linux bdash game has a buffer overflow that allows local users to gain root access.
CAN-1999-0389	Buffer overflow in the bootp server in the Debian Linux netstd package.
CAN-1999-0398	In some instances of SSH 1.2.27 and 2.0.11 on Linux systems, SSH will allow users with expired accounts to login.
CAN-1999-0400	Denial of service in Linux 2.2.0 running the ldd command on a core file.
CAN-1999-0401	A race condition in Linux 2.2.1 allows local users to read arbitrary memory from /proc files.
CAN-1999-0426	The default permissions of /dev/kmem in Linux versions before 2.0.36 allows IP spoofing.
CAN-1999-0431	Linux 2.2.3 and earlier allow a remote attacker to perform an IP fragmentation attack, causing a denial of service.
CAN-1999-0434	XFree86 xfs command is vulnerable to a symlink attack, allowing local users to create files in restricted directories, possibly allowing them to gain privileges or cause a denial of service.
CAN-1999-0451	Denial of service in Linux 2.0.36 allows local users to prevent any server from listening on any non-privileged port.

CVE Number	Description
CAN-1999-0459	Local users can perform a denial of service in Alpha Linux, using MILO to force a reboot.
CAN-1999-0460	Buffer overflow in Linux autofs module through long directory names allows local users to perform a denial of service.
CAN-1999-0461	Versions of rpcbind including Linux, IRIX, and Wietse Venema's rpcbind allow a remote attacker to insert and delete entries by spoofing a source address.
CAN-1999-0462	suidperl in Linux Perl does not check the nosuid mount option on file systems, allowing local users to gain root access by placing a setuid script in a mountable file system, e.g. a CD-ROM or floppy disk.
CAN-1999-0698	Denial of service in IP protocol logger (ippl) on Red Hat and Debian Linux.
CAN-1999-0798	Buffer overflow in bootpd on OpenBSD, FreeBSD, and Linux systems via a malformed header type.
CAN-1999-1018	IPChains in Linux kernels 2.2.10 and earlier does not reassemble IP fragments before checking the header information, which allows a remote attacker to bypass the filtering rules using several fragments with 0 offsets.
CAN-1999-1166	Linux 2.0.37 does not properly encode the Custom segment limit, which allows local users to gain root privileges by accessing and modifying kernel memory.
CAN-1999-1173	Corel Word Perfect 8 for Linux creates a temporary working directory with world-writable permissions, which allows local users to (1) modify Word Perfect behavior by modifying files in the working directory, or (2) modify files of other users via a sym
CAN-1999-1182	Buffer overflow in run-time linkers (1) ld.so or (2) ld-linux.so for Linux systems allows local users to gain privileges by calling a setuid program with a long program name (argv[0]) and forcing ld.so/ld-linux.so to report an error.
CAN-1999-1186	rxvt, when compiled with the PRINT_PIPE option in various Linux operating systems including Linux Slackware 3.0 and RedHat 2.1, allows local users to gain root privileges by specifying a malicious program using the -print-pipe command line parameter.
CAN-1999-1187	Pine before version 3.94 allows local users to gain privileges via a symlink attack on a lockfile that is created when a user receives new mail.

CVE Number	Description
CAN-1999-1225	rpc.mountd on Linux, Ultrix, and possibly other operating systems, allows remote attackers to determine the existence of a file on the server by attempting to mount that file, which generates different error messages depending on whether the file exist
CAN-1999-1229	Quake 2 server 3.13 on Linux does not properly check file permissions for the config.cfg configuration file, which allows local users to read arbitrary files via a symlink from config.cfg to the target file.
CAN-1999-1285	Linux 2.1.132 and earlier allows local users to cause a denial of service (resource exhaustion) by reading a large buffer from a random device (e.g. /dev/urandom), which cannot be interrupted until the read has completed.
CAN-1999-1299	rcp on various Linux systems including Red Hat 4.0 allows a "nobody" user or other user with UID of 65535 to overwrite arbitrary files, since 65535 is interpreted as -1 by chown and other system calls, which causes the calls to fail to modify the owner
CAN-1999-1346	PAM configuration file for rlogin in Red Hat Linux 6.1 and earlier includes a less restrictive rule before a more restrictive one, which allows users to access the host via rlogin even if rlogin has been explicitly disabled using the /etc/nologin file.
CAN-1999-1347	Xsession in Red Hat Linux 6.1 and earlier can allow local users with restricted accounts to bypass execution of the .xsession file by starting kde, gnome or anotherlevel from kdm.
CAN-1999-1348	Linuxconf on Red Hat Linux 6.0 and earlier does not properly disable PAM-based access to the shutdown command, which could allow local users to cause a denial of service.
CAN-1999-1352	mknod in Linux 2.2 follows symbolic links, which could allow local users to overwrite files or gain privileges.
CAN-1999-1381	Buffer overflow in dbadmin CGI program 1.0.1 on Linux allows remote attackers to execute arbitrary commands.
CAN-1999-1387	Windows NT 4.0 SP2 allows remote attackers to cause a denial of service (crash), possibly via malformed inputs or packets, such as those generated by a Linux smbmount command that was compiled on the Linux 2.0.29 kernel but executed on Linux 2.0.25.

CVE Number	Description
CAN-1999-1390	suidexec in suidmanager 0.18 on Debian 2.0 allows local users to gain root privileges by specifying a malicious program on the command line.
CAN-1999-1406	dumpreg in Red Hat Linux 5.1 opens /dev/mem with O_RDWR access, which allows local users to cause a denial of service (crash) by redirecting fd 1 (stdout) to the kernel.
CAN-1999-1434	login in Slackware Linux 3.2 through 3.5 does not properly check for an error when the /etc/group file is missing, which prevents it from dropping privileges, causing it to assign root privileges to any local user who logs on to the server.
CAN-1999-1441	Linux 2.0.34 does not properly prevent users from sending SIGIO signals to arbitrary processes, which allows local users to cause a denial of service by sending SIGIO to processes that do not catch it.
CAN-1999-1442	Bug in AMD K6 processor on Linux 2.0.x and 2.1.x kernels allows local users to cause a denial of service (crash) via a particular sequence of instructions, possibly related to accessing addresses outside of segments.
CAN-1999-1445	Vulnerability in imapd and ipop3d in Slackware 3.4 and 3.3 with shadowing enabled, and possibly other operating systems, allows remote attackers to cause a core dump via a short sequence of USER and PASS commands that do not provide valid usernames or
CAN-1999-1477	Buffer overflow in GNOME libraries 1.0.8 allows local user to gain root access via a long --espeaker argument in programs such as nethack.
CAN-1999-1489	Buffer overflow in TestChip function in XFree86 SuperProbe in Slackware Linux 3.1 allows local users to gain root privileges via a long -nopr argument.
CAN-1999-1490	xosview 1.5.1 in Red Hat 5.1 allows local users to gain root access via a long HOME environmental variable.
CAN-1999-1491	abuse.console in Red Hat 2.1 uses relative pathnames to find and execute the undrv program, which allows local users to execute arbitrary commands via a path that points to a Trojan horse program.
CAN-1999-1496	Sudo 1.5 in Debian Linux 2.1 and Red Hat 6.0 allows local users to determine the existence of arbitrary files by attempting to execute the target filename as a program, which generates a different error message when the file does not exist.
CAN-1999-1498	Slackware Linux 3.4 pkgtool allows local attacker to read and write to arbitrary files via a symlink attack on the reply file.

CVE Number	Description
CAN-2000-0017	Buffer overflow in Linux linuxconf package allows remote attackers to gain root privileges via a long parameter.
CAN-2000-0109	The mcsp Client Site Processor system (MultiCSP) in Standard and Poor's ComStock is installed with several accounts that have no passwords or easily guessable default passwords.
CAN-2000-0118	The Red Hat Linux su program does not log failed password guesses if the su process is killed before it times out, which allows local attackers to conduct brute force password guessing.
CAN-2000-0219	Red Hat 6.0 allows local users to gain root access by booting single user and hitting ^C at the password prompt.
CAN-2000-0227	The Linux 2.2.x kernel does not restrict the number of Unix domain sockets as defined by the wmem_max paremeter, which allows local users to cause a denial of service by requesting a large number of sockets.
CAN-2000-0248	The web GUI for the Linux Virtual Server (LVS) software in the Red Hat Linux Piranha package has a backdoor passowrd that allows remote attackers to execute arbitrary commands.
CAN-2000-0293	aaa_base in SuSE Linux 6.3, and cron.daily in earlier versions, allow local users to delete arbitrary files by creating files whose names include spaces, which are then incorrectly interpreted by aaa_base when it deletes expired files from the /tmp direct
CAN-2000-0355	pg and pb in SuSE pbpg 1.x package allows an attacker to read arbitrary files.
CAN-2000-0357	ORBit and esound in Red Hat Linux 6.1 do not use sufficiently random numbers, which allows local users to guess the authentication keys.
CAN-2000-0358	ORBit and gnome-session in Red Hat Linux 6.1 allows remote attackers to crash a program.
CAN-2000-0364	screen and rxvt in Red Hat Linux 6.0 do not properly set the modes of tty devices, which allows local users to write to other ttys.
CAN-2000-0365	Red Hat Linux 6.0 installs the /dev/pts file system with insecure modes, which allows local users to write to other tty devices.
CAN-2000-0433	The SuSE aaa_base package installs some system accounts with home directories set to /tmp, which allows local users to gain privileges to those accounts by creating standard user startup scripts such as profiles.

CVE Number	Description
CAN-2000-0491	Buffer overflow in the XDMCP parsing code of GNOME gdm, KDE kdm, and wdm allows remote attackers to execute arbitrary commands or cause a denial of service via a long FORWARD_QUERY request.
CAN-2000-0520	Buffer overflow in restore program 0.4b17 and earlier in dump package allows local users to execute arbitrary commands via a long tape name.
CAN-2000-0531	Linux gpm program allows local users to cause a denial of service by flooding the /dev/gpmctl device with STREAM sockets.
CAN-2000-0545	Buffer overflow in mailx mail command (aka Mail) on Linux systems allows local users to gain privileges via a long -c (carbon copy) parameter.
CAN-2000-0606	Buffer overflow in kon program in Kanji on Console (KON) package on Linux may allow local users to gain root privileges via a long -StartupMessage parameter.
CAN-2000-0607	Buffer overflow in fld program in Kanji on Console (KON) package on Linux may allow local users to gain root privileges via an input file containing long CHARSET_REGISTRY or CHARSET_ENCODING settings.
CAN-2000-0614	Tnef program in Linux systems allows remote attackers to overwrite arbitrary files via TNEF encoded compressed attachments which specify absolute path names for the decompressed output.
CAN-2000-0617	Buffer overflow in xconq and cconq game programs on Red Hat Linux allows local users to gain additional privileges via long USER environmental variable.
CAN-2000-0618	Buffer overflow in xconq and cconq game programs on Red Hat Linux allows local users to gain additional privileges via long DISPLAY environmental variable.
CAN-2000-0667	Vulnerability in gpm in Caldera Linux allows local users to delete arbitrary files or conduct a denial of service.
CAN-2000-0701	The wrapper program in mailman 2.0beta3 and 2.0beta4 does not properly cleanse untrusted format strings, which allows local users to gain privileges.
CAN-2000-0714	Some problems like this one are related to installations of files that set improper permissions. Should each separate file get a separate CVE entry? Or should dot notation be used? This question has been labeled as CD:INSTALL-PERM.
CAN-2000-0715	DiskCheck script diskcheck.pl in Red Hat Linux allows local users to create or overwrite arbitrary files via a symlink attack.
CAN-2000-0747	The logrotate script for openldap earlier than 1.2.11 in Conectiva Linux sends an improper signal to the kernel log daemon (klogd) and kills it.

CVE Number	Description
CAN-2000-0800	String parsing error in rpc.kstatd in the linuxnfs or knfsd packages in SuSE and possibly other Linux systems allows remote attackers to gain root privileges.
CAN-2000-0843	Buffer overflow in pam_smb and pam_ntdom pluggable authentication modules (PAM) allow remote attackers to execute arbitrary commands via a login with a long user name.
CAN-2000-0866	Interbase 6 SuperServer for Linux allows an attacker to cause a denial of service via a query containing 0 bytes.
CAN-2000-0963	Buffer overflow in ncurses library allows local users to execute arbitrary commands via long environmental information such as TERM or TERMINFO_DIRS.
CAN-2000-0986	Buffer overflow in Oracle 8.1.5 applications such as names, namesctl, onrsd, osslogin, tnslsnr, tnsping, trcasst, and trcroute possibly allow local users to gain privileges via a long ORACLE_HOME environmental variable.
CAN-2000-1009	dump in Red Hat Linux 6.2 trusts the pathname specified by the RSH environmental variable, which allows local users to obtain root privileges by modifying the RSH variable to point to a Trojan horse program.
CAN-2000-1125	restore 0.4b15 and earlier in Red Hat Linux 6.2 trusts the pathname specified by the RSH environmental variable, which allows local users to obtain root privileges by modifying the RSH variable to point to a Trojan horse program.
CAN-2000-1134	tcsh, csh, sh, and bash on various Unix systems follow symlinks when processing << redirects (aka here-documents or in-here documents), which allows local users to overwrite files of other users via a symlink attack.
CAN-2000-1175	Buffer overflow in Koules 1.4 allows local users to execute arbitrary commands via a long command line argument.
CAN-2000-1183	Buffer overflow in socks5 server on Linux allows attackers to execute arbitrary commands via a long connection request.
CAN-2000-1207	userhelper in the usermode package on Red Hat Linux executes non-setuid programs as root, which does not activate the security measures in glibc and allows the programs to be exploited via format string vulnerabilities in glibc via the LANG or LC_ALL envi
CAN-2000-1208	Format string vulnerability in startprinting() function of printjob.c in BSD-based lpr lpd package may allow local users to gain privileges via an improper syslog call that uses format strings from the checkremote() call.

CVE Number	Description
CAN-2000-1213	ping in iputils before 20001010, as distributed on Red Hat Linux 6.2 through 7J and other operating systems, does not drop privileges after acquiring a raw socket, which increases ping's exposure to bugs that otherwise would occur at lower privileges.
CAN-2000-1214	Buffer overflows in the (1) outpack or (2) buf variables of ping in iputils before 20001010, as distributed on Red Hat Linux 6.2 through 7J and other operating systems, may allow local users to gain privileges.
CAN-2001-0073	Buffer overflow in the find_default_type function in libsecure in NSA Security-enhanced Linux, which may allow attackers to modify critical data in memory.
CAN-2001-0107	Veritas Backup agent on Linux allows remote attackers to cause a denial of service by establishing a connection without sending any data, which causes the process to hang.
CAN-2001-0112	Multiple buffer overflows in splitvt before 1.6.5 allow local users to execute arbitrary commands.
CAN-2001-0131	htpasswd and htdigest in Apache 2.0a9, 1.3.14, and others allows local users to overwrite arbitrary files via a symlink attack.
CAN-2001-0172	Buffer overflow in ReiserFS 3.5.28 in SuSE Linux allows local users to cause a denial of service and possibly execute arbitrary commands by via a long directory name.
CAN-2001-0181	Format string vulnerability in the error logging code of DHCP server and client in Caldera Linux allows remote attackers to execute arbitrary commands.
CAN-2001-0229	Chili!Soft ASP for Linux before 3.6 does not properly set group privileges when running in inherited mode, which could allow attackers to gain privileges via malicious scripts.
CAN-2001-0468	Buffer overflow in FTPFS allows local users to gain root privileges via a long user name.
CAN-2001-0496	kdesu creates world readable temporary files containing authentication info, which can allow local users to gain privileges.
CAN-2001-0623	sendfiled, as included with Simple Asynchronous File Transfer (SAFT), on various Linux systems does not properly drop privileges when sending notification emails, which allows local attackers to gain privileges.

CVE Number	Description
CAN-2001-0632	Sun Chili!Soft 3.5.2 on Linux and 3.6 on AIX creates a default admin username and password in the default installation, which can allow a remote attacker to gain additional privileges.
CAN-2001-0755	Buffer overflow in ftp daemon (ftpd) 6.2 in Debian Linux allows attackers to cause a denial of service and possibly execute arbitrary code via a long SITE command.
CAN-2001-0759	Buffer overflow in bctool in Jetico BestCrypt 0.8.1 and earlier allows local users to execute arbitrary code via a file or directory with a long pathname, which is processed during an unmount.
CAN-2001-0763	Buffer overflow in Linux xinetd 2.1.8.9pre11-1 and earlier may allow remote attackers to execute arbitrary code via a long ident response, which is not properly handled by the svc_logprint function.
CAN-2001-0775	Buffer overflow in xloadimage 4.1 (aka xli 1.16 and 1.17) in Linux allows remote attacker to execute arbitrary code via a FACES format image containing a long (1) Firstname or (2) Lastname field.
CAN-2001-0907	Linux kernel 2.2.1 through 2.2.19, and 2.4.1 through 2.4.10, allows local users to cause a denial of service via a series of deeply nested symlinks, which causes the kernel to spend extra time when trying to access the link.
CAN-2001-0914	Linux kernel before 2.4.11pre3 in multiple Linux distributions allows local users to cause a denial of service (crash) by starting the core vmlinux kernel, possibly related to poor error checking during ELF loading.
CAN-2001-1012	Vulnerability in screen before 3.9.10, related to a multi-attach error, allows local users to gain root privileges when there is a subdirectory under /tmp/screens/.
CAN-2001-1013	Apache on Red Hat Linux with with the UserDir directive enabled generates different error codes when a username exists and there is no public_html directory and when the username does not exist, which could allow remote attackers to determine valid use
CAN-2001-1028	Buffer overflow in ultimate_source function of man 1.5 and earlier allows local users to gain privileges.
CAN-2001-1069	libCoolType library as used in Adobe Acrobat (acroread) on Linux creates the AdobeFnt.lst file with world-writable permissions, which allows local users to modify the file and possibly modify acroread's behavior.

CVE Number	Description
CAN-2001-1190	The default PAM files included with passwd in Mandrake Linux 8.1 do not support MD5 passwords, which could result in a lower level of password security than intended.
CAN-2001-1244	Multiple TCP implementations could allow remote attackers to cause a denial of service (bandwidth and CPU exhaustion) by setting the maximum segment size (MSS) to a very small number and requesting large amounts of data, which generates more packets with
CAN-2001-1245	Opera 5.0 for Linux does not properly handle malformed HTTP headers, which allows remote attackers to cause a denial of service, possibly with a header whose value is the same as a MIME header name.
CAN-2001-1273	The "mxcsr P4" vulnerability in the Linux kernel before 2.2.17-14, when running on certain Intel CPUs, allows local users to cause a denial of service (system halt).
CAN-2001-1304	Buffer overflow in SHOUTcast Server 1.8.2 allows remote attackers to cause a denial of service (crash) via several HTTP requests with a long (1) user-agent or (2) host HTTP header.
CAN-2001-1327	pmake before 2.1.35 in Turbolinux 6.05 and earlier is installed with setuid root privileges, which could allow local users to gain privileges by exploiting vulnerabilities in pmake or programs that are used by pmake.
CAN-2001-1332	Buffer overflows in Linux CUPS before 1.1.6 may allow remote attackers to execute arbitrary code.
CAN-2001-1333	Linux CUPS before 1.1.6 does not securely handle temporary files, possibly due to a symlink vulnerability that could allow local users to overwrite files.
CAN-2001-1374	expect before 5.32 searches for its libraries in /var/tmp before other directories, which could allow local users to gain root privileges via a Trojan horse library that is accessed by mkpasswd.
CAN-2001-1383	initscript in setserial 2.17-4 and earlier uses predictable temporary file names, which could allow local users to conduct unauthorized operations on files.
CAN-2001-1384	ptrace in Linux 2.2.x through 2.2.19, and 2.4.x through 2.4.9, allows local users to gain root privileges by running ptrace on a setuid or setgid program that itself calls an unprivileged program, such as newgrp.
CAN-2001-1390	Unknown vulnerability in binfmt_misc in the Linux kernel before 2.2.19, related to user pages.

CVE Number	Description
CAN-2001-1391	off-by-one vulnerability in CPIA driver of Linux kernel before 2.2.19 allows users to modify kernel memory.
CAN-2001-1392	The Linux kernel before 2.2.19 does not have unregister calls for (1) CPUID and (2) MSR drivers, which could cause a DoS (crash) by unloading and reloading the drivers.
CAN-2001-1393	Unknown vulnerability in classifier code for Linux kernel before 2.2.19 could result in denial of service (hang).
CAN-2001-1394	Signedness error in (1) getsockopt and (2) setsockopt for Linux kernel before 2.2.19 allows local users to cause a denial of service.
CAN-2001-1395	Unknown vulnerability in sockfilter for Linux kernel before 2.2.19 related to "boundary cases," with unknown impact.
CAN-2001-1396	Unknown vulnerabilities in strnlen_user for Linux kernel before 2.2.19, with unknown impact.
CAN-2001-1397	The System V (SYS5) shared memory implementation for Linux kernel before 2.2.19 could allow attackers to modify recently freed memory.
CAN-2001-1398	Masquerading code for Linux kernel before 2.2.19 does not fully check packet lengths in certain cases, which may lead to a vulnerability.
CAN-2001-1399	Certain operations in Linux kernel before 2.2.19 on the x86 architecture copy the wrong number of bytes, which might allow attackers to modify memory, aka "User access asm bug on x86."
CAN-2001-1400	Unknown vulnerabilities in the UDP port allocation for Linux kernel before 2.2.19 could allow local users to cause a denial of service (deadlock).
CAN-2002-0062	Buffer overflow in ncurses 5.0, and the ncurses4 compatibility package which is based on it, allows local users to gain privileges.
CAN-2002-0086	Buffer overflow in bindsock in Lotus Domino 5.0.4 and 5.0.7 on Linux allows local users to gain root privileges via a long (1) Notes_ExecDirectory or (2) PATH environment variable.
CAN-2002-0164	Vulnerability in the MIT-SHM extension of the X server on Linux allows local users to read and write arbitrary shared memory, possibly to cause a denial of service or gain privileges.

CVE Number	Description
CAN-2002-0169	The default stylesheet for DocBook on Red Hat Linux 6.2 through 7.2 is installed with an insecure option enabled, which could allow users to overwrite files outside of the current directory from an untrusted document by using a full pathname as an element
CAN-2002-0203	ttawebtop.cgi in Tarantella Enterprise 3.20 on SPARC Solaris and Linux, and 3.1x and 3.0x including 3.11.903, allows remote attackers to view directory contents via an empty pg parameter.
CAN-2002-0378	The default configuration of LPRng print spooler in Red Hat Linux 7.0 through 7.3 accepts print jobs from arbitrary remote hosts.
CAN-2002-0429	The iBCS routines in arch/i386/kernel/traps.c for Linux kernels 2.4.18 and earlier on x86 systems allow local users to kill arbitrary processes via a a binary compatibility interface (lcall).
CAN-2002-0488	Linux Directory Penguin traceroute.pl CGI script 1.0 allows remote attackers to execute arbitrary code via shell metacharacters in the host parameter.
CAN-2002-0489	Linux Directory Penguin NsLookup CGI script (nslookup.pl) 1.0 allows remote attackers to execute arbitrary code via shell metacharacters in the (1) query or (2) type parameters.
CAN-2002-0499	The d_path function in Linux kernel 2.2.20 and earlier, and 2.4.18 and earlier, truncates long pathnames without generating an error, which could allow local users to force programs to perform inappropriate operations on the wrong directories.
CAN-2002-0510	The UDP implementation in Linux 2.4.x kernels keeps the IP Identification field at 0 for all non-fragmented packets, which could allow remote attackers to determine that a target system is running Linux.
CAN-2002-0512	startkde in KDE for Caldera OpenLinux 2.3 through 3.1.1 sets the LD_LIBRARY_PATH environment variable to include the current working directory, which could allow local users to gain privileges of other users running startkde via Trojan horse libraries.
CAN-2002-0570	The encrypted loop device in Linux kernel 2.4.10 and earlier does not authenticate the entity that is encrypting data, which allows local users to modify encrypted data without knowing the key.

CVE Number	Description
CAN-2002-0638	setpwnam.c in the util-linux package, as included in Red Hat Linux 7.3 and earlier, and other operating systems, does not properly lock a temporary file when modifying /etc/passwd, which may allow local users to gain privileges via a complex race conditio
CAN-2002-0660	Buffer overflow in libpng 1.0.12-3.woody.2 and libpng3 1.2.1-1.1.woody.2 on Debian Linux 3.0, and other operating systems, may allow attackers to cause a denial of service and possibly execute arbitrary code, a different vulnerability than CAN-2002-0728.
CAN-2002-0704	The Network Address Translation (NAT) capability for Netfilter ("iptables") 1.2.6a and earlier leaks translated IP addresses in ICMP error messages.
CAN-2002-0758	ifup-dhcp script in the sysconfig package for SuSE 8.0 allows remote attackers to execute arbitrary commands via spoofed DHCP responses, which are stored and executed in a file.
CAN-2002-0762	shadow package in SuSE 8.0 allows local users to destroy the /etc/passwd and /etc/shadow files or assign extra group privileges to some users by changing filesize limits before calling programs that modify the files.
CAN-2002-0767	simpleinit on Linux systems does not close a read/write FIFO file descriptor before creating a child process, which allows the child process to cause simpleinit to execute arbitrary programs with root privileges.
CAN-2002-0817	Format string vulnerability in super for Linux allows local users to gain root privileges via a long command line argument.
CAN-2002-0820	FreeBSD kernel 4.6 does not properly close and redirect the file descriptors 0, 1, and 2 to /dev/null when the original descriptors reference procfs, which could allow local users to reuse the file descriptors in a setuid or setgid program to modify criti
CAN-2002-0836	dvips converter for Postscript files in the tetex package calls the system() function insecurely, which allows remote attackers to execute arbitrary commands via certain print jobs, possibly involving fonts.
CAN-2002-0849	Linux-iSCSI iSCSI implementation installs the iscsi.conf file with world-readable permissions on some operating systems, including Red Hat Linux Limbo Beta #1, which could allow local users to gain privileges by reading the cleartext CHAP password.

CVE Number	Description
CAN-2002-0854	Buffer overflows in ISDN Point to Point Protocol (PPP) daemon (ipppd) in the i4l package on SuSE 7.3, 8.0, and possibly other operating systems, may allow local users to gain privileges.
CAN-2002-0875	Vulnerability in FAM 2.6.8, 2.6.6, and other versions allows unprivileged users to obtain the names of files whose access is restricted to the root group.
CAN-2002-0912	in.uucpd UUCP server in Debian GNU/Linux 2.2, and possibly other operating systems, does not properly terminate long strings, which allows remote attackers to cause a denial of service, possibly due to a buffer overflow.
CAN-2002-0915	autorun in Xandros based Linux distributions allows local users to read the first line of arbitrary files via the -c parameter, which causes autorun to print the first line of the file.
CAN-2002-1232	Memory leak in ypdb_open in yp_db.c for ypserv before 2.5 in the NIS package 3.9 and earlier allows remote attackers to cause a denial of service (memory consumption) via a large number of requests for a map that does not exist.
CAN-2002-1278	The mailconf module in Linuxconf 1.24 on Conectiva Linux 6.0 through 8 generates the Sendmail configuration file (sendmail.cf) in a way that configures Sendmail to run as an open mail relay, which allows remote attackers to send Spam email.
CAN-2002-1285	runlpr in the LPRng package allows the local lp user to gain root privileges via certain command line arguments.
CVE-1999-0002	Buffer overflow in NFS mountd gives root access to remote attackers, mostly in Linux systems.
CVE-1999-0034	Buffer overflow in suidperl (sperl), Perl 4.x and 5.x
CVE-1999-0046	Buffer overflow of rlogin program using TERM environmental variable.
CVE-1999-0074	Listening TCP ports are sequentially allocated, allowing spoofing attacks.
CVE-1999-0128	Oversized ICMP ping packets can result in a denial of service, aka Ping o' Death.
CVE-1999-0137	The dip program on many Linux systems allows local users to gain root access via a buffer overflow.
CVE-1999-0183	Linux implementations of TFTP would allow access to files outside the restricted directory.
CVE-1999-0234	Bash treats any character with a value of 255 as a command separator.
CVE-1999-0245	Some configurations of NIS+ in Linux allowed attackers to log in as the user "+"

CVE Number	Description
CVE-1999-0262	faxsurvey CGI script on Linux allows remote command execution via shell metacharacters.
CVE-1999-0297	Buffer overflow in Vixie Cron library up to version 3.0 allows local users to obtain root access via a long environmental variable.
CVE-1999-0316	Buffer overflow in Linux splitvt command gives root access to local users.
CVE-1999-0318	Buffer overflow in xmcd 2.0p12 allows local users to gain access through an environmental variable.
CVE-1999-0335	Buffer overflow in BSD and linux lpr command allows local users to execute commands as root through the classification option.
CVE-1999-0340	Buffer overflow in Linux Slackware crond program allows local users to gain root access.
CVE-1999-0341	Buffer overflow in the Linux mail program "deliver" allows local users to gain root access.
CVE-1999-0342	Linux PAM modules allow local users to gain root access using temporary files.
CVE-1999-0363	SuSE 5.2 PLP lpc program has a buffer overflow that leads to root compromise.
CVE-1999-0373	Buffer overflow in the "Super" utility in Debian Linux and other operating systems allows local users to execute commands as root.
CVE-1999-0374	Debian Linux cfengine package is susceptible to a symlink attack.
CVE-1999-0390	Buffer overflow in Dosemu Slang library in Linux.
CVE-1999-0403	A bug in Cyrix CPU's on Linux allows local users to perform a denial of service.
CVE-1999-0405	A buffer overflow in lsof allows local users to obtain root privilege.
CVE-1999-0409	Buffer overflow in gnuplot in Linux version 3.5 allows local users to obtain root access.
CVE-1999-0414	In Linux before version 2.0.36, remote attackers can spoof a TCP connection and pass data to the application layer before fully establishing the connection.
CVE-1999-0421	During a reboot after an installation of Linux Slackware 3.6, a remote attacker can obtain root access by logging in to the root account without a password.
CVE-1999-0457	Linux ftpwatch program allows local users to gain root privileges.
CVE-1999-0502	A Unix account has a default, null, blank, or missing password.
CVE-1999-0513	ICMP messages to broadcast addresses are allowed, allowing for a Smurf attack that can cause a denial of service.
CVE-1999-0628	The rwho/rwhod service is running, which exposes machine status and user information.

CVE Number	Description
CVE-1999-0678	A default configuration of Apache on Debian Linux sets the ServerRoot to /usr/doc, which allows remote users to read documentation files for the entire server.
CVE-1999-0704	Buffer overflow in Berkeley automounter daemon (amd) logging facility provided in the Linux am-utils package and others.
CVE-1999-0706	Linux xmonisdn package allows local users to gain root privileges by modifying the IFS or PATH environmental variables.
CVE-1999-0720	The pt_chown command in Linux allows local users to modify TTY terminal devices that belong to other users.
CVE-1999-0733	Buffer overflow in VMWare 1.0.1 for Linux via a long HOME environmental variable.
CVE-1999-0740	Remote attackers can cause a denial of service on Linux in.telnetd telnet daemon through a malformed TERM environmental variable.
CVE-1999-0746	A default configuration of in.identd in SuSE Linux waits 120 seconds between requests, allowing a remote attacker to conduct a denial of service.
CVE-1999-0769	Vixie Cron on Linux systems allows local users to set parameters of sendmail commands via the MAILTO environmental variable.
CVE-1999-0780	KDE klock allows local users to kill arbitrary processes by specifying an arbitrary PID in the .kss.pid file.
CVE-1999-0781	KDE allows local users to execute arbitrary commands by setting the KDEDIR environmental variable to modify the search path that KDE uses to locate its executables.
CVE-1999-0804	Denial of service in Linux 2.2.x kernels via malformed ICMP packets containing unusual types, codes, and IP header lengths.
CVE-1999-0831	Denial of service in Linux syslogd via a large number of connections.
CVE-1999-0832	Buffer overflow in NFS server on Linux allows attackers to execute commands via a long pathname.
CVE-1999-0856	login in Slackware 7.0 allows remote attackers to identify valid users on the system by reporting an encryption error when an account is locked or does not exist.
CVE-1999-0894	Red Hat Linux screen program does not use Unix98 ptys, allowing local users to write to other terminals.

CVE Number	Description
CVE-1999-0906	Buffer overflow in sccw allows local users to gain root access via the HOME environmental variable.
CVE-1999-0914	Buffer overflow in the FTP client in the Debian GNU/Linux netstd package.
CVE-1999-0978	htdig allows remote attackers to execute commands via filenames with shell metacharacters.
CVE-1999-0986	The ping command in Linux 2.0.3x allows local users to cause a denial of service by sending large packets with the -R (record route) option.
CVE-1999-1008	xsoldier program allows local users to gain root access via a long argument.
CVE-1999-1048	Buffer overflow in bash 2.0.0, 1.4.17, and other versions allows local attackers to gain privileges by creating an extremely large directory name, which is inserted into the password prompt via the \w option in the PS1 environmental variable when another
CVE-1999-1276	fte-console in the fte package before 0.46b-4.1 does not drop root privileges, which allows local users to gain root access via the virtual console device.
CVE-1999-1288	Samba 1.9.18 inadvertently includes a prototype application, wsmbconf, which is installed with incorrect permissions including the setgid bit, which allows local users to read and write files and possibly gain privileges via bugs in the program.
CVE-1999-1327	Buffer overflow in linuxconf 1.11r11-rh2 on Red Hat Linux 5.1 allows local users to gain root privileges via a long LANG environmental variable.
CVE-1999-1328	linuxconf before 1.11.r11-rh3 on Red Hat Linux 5.1 allows local users to overwrite arbitrary files and gain root access via a symlink attack.
CVE-1999-1329	Buffer overflow in SysVInit in Red Hat Linux 5.1 and earlier allows local users to gain privileges.
CVE-1999-1330	The snprintf function in the db library 1.85.4 ignores the size parameter, which could allow attackers to exploit buffer overflows that would be prevented by a properly implemented snprintf.
CVE-1999-1331	netcfg 2.16-1 in Red Hat Linux 4.2 allows the Ethernet interface to be controlled by users on reboot when an option is set, which allows local users to cause a denial of service by shutting down the interface.
CVE-1999-1332	gzexe in the gzip package on Red Hat Linux 5.0 and earlier allows local users to overwrite files of other users via a symlink attack on a temporary file.

CVE Number	Description
CVE-1999-1333	automatic download option in ncftp 2.4.2 FTP client in Red Hat Linux 5.0 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in the names of files that are to be downloaded.
CVE-1999-1335	snmpd server in cmu-snmp SNMP package before 3.3-1 in Red Hat Linux4.0 is configured to allow remote attackers to read and write sensitive information.
CVE-1999-1339	Vulnerability when Network Address Translation (NAT) is enabled in Linux 2.2.10 and earlier with ipchains, or FreeBSD 3.2 with ipfw, allows remote attackers to cause a denial of service (kernel panic) via a ping -R (record route) command.
CVE-1999-1341	Linux kernel before 2.3.18 or 2.2.13pre15, with SLIP and PPP options, allows local unprivileged users to forge IP packets via the TIOCSETD option on tty devices.
CVE-1999-1407	ifdhcpc-done script for configuring DHCP on Red Hat Linux 5 allows local users to append text to arbitrary files via a symlink attack on the dhcplog file.
CVE-1999-1411	The installation of the fsp package 2.71-10 in Debian Linux 2.0 adds the anonymous FTP user without notifying the administrator, which could automatically enable anounymous FTP on some servers such as wu-ftp.
CVE-1999-1512	The AMaViS virus scanner 0.2.0-pre4 and earlier allows remote attackers to execute arbitrary commands as root via an infected mail message with shell metacharacters in the reply-to field.
CVE-2000-0031	The initscripts package in Red Hat Linux allows local users to gain privileges via a symlink attack.
CVE-2000-0048	get_it program in Corel Linux Update allows local users to gain root access by specifying an alternate PATH for the cp program.
CVE-2000-0052	Red Hat userhelper program in the usermode package allows local users to gain root access via PAM and a .. (dot dot) attack.
CVE-2000-0076	nviboot boot script in the Debian nvi package allows local users to delete files via malformed entries in vi.recover.
CVE-2000-0107	Linux apcd program allows local attackers to modify arbitrary files via a symlink attack.
CVE-2000-0112	The default installation of Debian Linux uses an insecure Master Boot Record (MBR) which allows a local user to boot from a floppy disk during the installation.
CVE-2000-0145	The libguile.so library file used by gnucash in Debian Linux is installed with world-writable permissions.

CVE Number	Description
CVE-2000-0170	Buffer overflow in the man program in Linux allows local users to gain privileges via the MANPAGER environmental variable.
CVE-2000-0171	atsadc in the atsar package for Linux does not properly check the permissions of an output file, which allows local users to gain root privileges.
CVE-2000-0172	The mtr program only uses a seteuid call when attempting to drop privileges, which could allow local users to gain root privileges.
CVE-2000-0184	Linux printtool sets the permissions of printer configuration files to be world-readable, which allows local attackers to obtain printer share passwords.
CVE-2000-0186	Buffer overflow in the dump utility in the Linux ext2fs backup package allows local users to gain privileges via a long command line argument.
CVE-2000-0192	The default installation of Caldera OpenLinux 2.3 includes the CGI program rpm_query, which allows remote attackers to determine what packages are installed on the system.
CVE-2000-0193	The default configuration of Dosemu in Corel Linux 1.0 allows local users to execute the system.com program and gain privileges.
CVE-2000-0194	buildxconf in Corel Linux allows local users to modify or create arbitrary files via the -x or -f parameters.
CVE-2000-0195	setxconf in Corel Linux allows local users to gain root access via the -T parameter, which executes the user's .xserverrc file.
CVE-2000-0196	Buffer overflow in mhshow in the Linux nmh package allows remote attackers to execute commands via malformed MIME headers in an email message.
CVE-2000-0206	The installation of Oracle 8.1.5.x on Linux follows symlinks and creates the orainstRoot.sh file with world-writeable permissions, which allows local users to gain privileges.
CVE-2000-0218	Buffer overflow in Linux mount and umount allows local users to gain root privileges via a long relative pathname.
CVE-2000-0231	Linux kreatecd trusts a user-supplied path that is used to find the cdrecord program, allowing local users to gain root privileges.
CVE-2000-0233	SuSE Linux IMAP server allows remote attackers to bypass IMAP authentication and gain privileges.
CVE-2000-0263	The X font server xfs in Red Hat Linux 6.x allows an attacker to cause a denial of service via a malformed request.

CVE Number	Description
CVE-2000-0274	The Linux trustees kernel patch allows attackers to cause a denial of service by accessing a file or directory with a long name.
CVE-2000-0289	IP masquerading in Linux 2.2.x allows remote attackers to route UDP packets through the internal interface by modifying the external source IP address and port number to match those of an established connection.
CVE-2000-0314	traceroute in NetBSD 1.3.3 and Linux systems allows local users to flood other systems by providing traceroute with a large waittime (-w) option, which is not parsed properly and sets the time delay for sending packets to zero.
CVE-2000-0315	traceroute in NetBSD 1.3.3 and Linux systems allows local unprivileged users to modify the source address of the packets, which could be used in spoofing attacks.
CVE-2000-0336	Linux OpenLDAP server allows local users to modify arbitrary files via a symlink attack.
CVE-2000-0340	Buffer overflow in Gnomelib in SuSE Linux 6.3 allows local users to execute arbitrary commands via the DISPLAY environmental variable.
CVE-2000-0344	The knfsd NFS server in Linux kernel 2.2.x allows remote attackers to cause a denial of service via a negative size value.
CVE-2000-0354	mirror 2.8.x in Linux systems allows remote attackers to create files one level above the local target directory.
CVE-2000-0356	Pluggable Authentication Modules (PAM) in Red Hat Linux 6.1 does not properly lock access to disabled NIS accounts.
CVE-2000-0362	Buffer overflows in Linux cdwtools 093 and earlier allows local users to gain root privileges.
CVE-2000-0363	Linux cdwtools 093 and earlier allows local users to gain root privileges via the /tmp directory.
CVE-2000-0366	dump in Debian Linux 2.1 does not properly restore symlinks, which allows a local user to modify the ownership of arbitrary files.
CVE-2000-0367	Vulnerability in eterm 0.8.8 in Debian Linux allows an attacker to gain root privileges.
CVE-2000-0369	The IDENT server in Caldera Linux 2.3 creates multiple threads for each IDENT request, which allows remote attackers to cause a denial of service.
CVE-2000-0370	The debug option in Caldera Linux smail allows remote attackers to execute commands via shell metacharacters in the -D option for the rmail command.

CVE Number	Description
CVE-2000-0374	The default configuration of kdm in Caldera Linux allows XDMCP connections from any host, which allows remote attackers to obtain sensitive information or bypass additional access restrictions.
CVE-2000-0378	The pam_console PAM module in Linux systems performs a chown on various devices upon a user login, but the ownership of some devices is not reset when the user logs out, which allows that user to sniff activity on these devices when subsequent users log i
CVE-2000-0438	Buffer overflow in fdmount on Linux systems allows local users in the "floppy" group to execute arbitrary commands via a long mountpoint parameter.
CVE-2000-0454	Buffer overflow in Linux cdrecord allows local users to gain privileges via the dev parameter.
CVE-2000-0460	Buffer overflow in KDE kdesud on Linux allows local uses to gain privileges via a long DISPLAY environmental variable.
CVE-2000-0467	Buffer overflow in Linux splitvt 1.6.3 and earlier allows local users to gain root privileges via a long password in the screen locking function.
CVE-2000-0483	The Zope DocumentTemplate package allows a remote attacker to modify DTMLDocuments or DTMLMethods without authorization.
CVE-2000-0506	The "capabilities" feature in Linux before 2.2.16 allows local users to cause a denial of service or gain privileges by setting the capabilities to prevent a setuid program from dropping privileges, aka the "Linux kernel setuid/setcap vulnerability."
CVE-2000-0508	rpc.lockd in Red Hat Linux 6.1 and 6.2 allows remote attackers to cause a denial of service via a malformed request.
CVE-2000-0566	makewhatis in Linux man package allows local users to overwrite files via a symlink attack.
CVE-2000-0573	The lreply function in wu-ftpd 2.6.0 and earlier does not properly cleanse an untrusted format string, which allows remote attackers to execute arbitrary commands via the SITE EXEC command.
CVE-2000-0584	Buffer overflow in Canna input system allows remote attackers to execute arbitrary commands via an SR_INIT command with a long user name or group name.

CVE Number	Description
CVE-2000-0594	BitchX IRC client does not properly cleanse an untrusted format string, which allows remote attackers to cause a denial of service via an invite to a channel whose name includes special formatting characters.
CVE-2000-0602	Secure Locate (slocate) in Red Hat Linux allows local users to gain privileges via a malformed configuration file that is specified in the LOCATE_PATH environmental variable.
CVE-2000-0604	gkermit in Red Hat Linux is improperly installed with setgid uucp, which allows local users to modify files owned by uucp.
CVE-2000-0633	Vulnerability in Mandrake Linux usermode package allows local users to to reboot or halt the system.
CVE-2000-0655	Netscape Communicator 4.73 and earlier allows remote attackers to cause a denial of service or execute arbitrary commands via a JPEG image containing a comment with an illegal field length of 1.
CVE-2000-0666	rpc.statd in the nfs-utils package in various Linux distributions does not properly cleanse untrusted format strings, which allows remote attackers to gain root privileges.
CVE-2000-0668	pam_console PAM module in Linux systems allows a user to access the system console and reboot the system when a display manager such as gdm or kdm has XDMCP enabled.
CVE-2000-0676	Netscape Communicator and Navigator 4.04 through 4.74 allows remote attackers to read arbitrary files by using a Java applet to open a connection to a URL using the "file", "http", "https", and "ftp" protocols, as demonstrated by Brown Orifice.
CVE-2000-0698	Minicom 1.82.1 and earlier on some Linux systems allows local users to create arbitrary files via a symlink attack.
CVE-2000-0703	suidperl (aka sperl) does not properly cleanse the escape sequence "~!" before calling /bin/mail to send an error report, which allows local users to gain privileges by setting the "interactive" environmental variable and calling suidperl with a filename
CVE-2000-0712	Linux Intrusion Detection System (LIDS) 0.9.7 allows local users to gain root privileges when LIDS is disabled via the security=0 boot option.
CVE-2000-0718	A race condition in MandrakeUpdate allows local users to modify RPM files while they are in the /tmp directory before they are installed.

CVE Number	Description
CVE-2000-0725	Zope before 2.2.1 does not properly restrict access to the getRoles method, which allows users who can edit DTML to add or modify roles by modifying the roles list that is included in a request.
CVE-2000-0727	xpdf PDF viewer client earlier than 0.91 does not properly launch a web browser for embedded URL's, which allows an attacker to execute arbitrary commands via a URL that contains shell metacharacters.
CVE-2000-0728	xpdf PDF viewer client earlier than 0.91 allows local users to overwrite arbitrary files via a symlink attack.
CVE-2000-0749	Buffer overflow in the Linux binary compatability module in FreeBSD 3.x through 5.x allows local users to gain root privileges via long filenames in the linux shadow file system.
CVE-2000-0750	Buffer overflow in mopd (Maintenance Operations Protocol loader daemon) allows remote attackers to execute arbitrary commands via a long file name.
CVE-2000-0751	mopd (Maintenance Operations Protocol loader daemon) does not properly cleanse user-injected format strings, which allows remote attackers to execute arbitrary commands.
CVE-2000-0763	xlockmore and xlockf do not properly cleanse user-injected format strings, which allows local users to gain root privileges via the -d option.
CVE-2000-0787	IRC Xchat client versions 1.4.2 and earlier allows remote attackers to execute arbitrary commands by encoding shell metacharacters into a URL which XChat uses to launch a web browser.
CVE-2000-0816	Linux tmpwatch --fuser option allows local users to execute arbitrary commands by creating files whose names contain shell metacharacters.
CVE-2000-0824	The unsetenv function in glibc 2.1.1 does not properly unset an environmental variable if the variable is provided twice to a program, which could allow local users to execute arbitrary commands in setuid programs by specifying their own duplicate environ
CVE-2000-0829	The tmpwatch utility in Red Hat Linux forks a new process for each directory level, which allows local users to cause a denial of service by creating deeply nested directories in /tmp or /var/tmp/.
CVE-2000-0844	Some functions that implement the locale subsystem on Unix do not properly cleanse user-injected format strings, which allows local attackers to execute arbitrary commands via functions such as gettext and catopen.

CVE Number	Description
CVE-2000-0867	Kernel logging daemon (klogd) in Linux does not properly cleanse user-injected format strings, which allows local users to gain root privileges by triggering malformed kernel messages.
CVE-2000-0868	The default configuration of Apache 1.3.12 in SuSE Linux 6.4 allows remote attackers to read source code for CGI scripts by replacing the /cgi-bin/ in the requested URL with /cgi-bin-sdb/.
CVE-2000-0869	The default configuration of Apache 1.3.12 in SuSE Linux 6.4 enables WebDAV, which allows remote attackers to list arbitrary directories via the PROPFIND HTTP request method.
CVE-2000-0883	The default configuration of mod_perl for Apache as installed on Mandrake Linux 6.1 through 7.1 sets the /perl/ directory to be browseable, which allows remote attackers to list the contents of that directory.
CVE-2000-0913	mod_rewrite in Apache 1.3.12 and earlier allows remote attackers to read arbitrary files if a RewriteRule directive is expanded to include a filename whose name contains a regular expression.
CVE-2000-0917	Format string vulnerability in use_syslog() function in LPRng 3.6.24 allows remote attackers to execute arbitrary commands.
CVE-2000-0934	Glint in Red Hat Linux 5.2 allows local users to overwrite arbitrary files and cause a denial of service via a symlink attack.
CVE-2000-0948	GnoRPM before 0.95 allows local users to modify arbitrary files via a symlink attack.
CVE-2000-0949	Heap overflow in savestr function in LBNL traceroute 1.4a5 and earlier allows a local user to execute arbitrary commands via the -g option.
CVE-2000-0956	cyrus-sasl before 1.5.24 in Red Hat Linux 7.0 does not properly verify the authorization for a local user, which could allow the users to bypass specified access restrictions.
CVE-2000-0967	PHP 3 and 4 do not properly cleanse user-injected format strings, which allows remote attackers to execute arbitrary commands by triggering error messages that are improperly written to the error logs.
CVE-2000-1010	Format string vulnerability in talkd in OpenBSD and possibly other BSD-based OSes allows remote attackers to execute arbitrary commands via a user name that contains format characters.

CVE Number	Description
CVE-2000-1016	The default configuration of Apache (httpd.conf) on SuSE 6.4 includes an alias for the /usr/doc directory, which allows remote attackers to read package documentation and obtain system configuration information via an HTTP request for the /doc/packages UR
CVE-2000-1042	Buffer overflow in ypserv in Mandrake Linux 7.1 and earlier, and possibly other Linux operating systems, allows an attacker to gain root privileges when ypserv is built without a vsyslog() function.
CVE-2000-1043	Format string vulnerability in ypserv in Mandrake Linux 7.1 and earlier, and possibly other Linux operating systems, allows an attacker to gain root privileges when ypserv is built without a vsyslog() function.
CVE-2000-1044	Format string vulnerability in ypbind-mt in SuSE SuSE-6.2, and possibly other Linux operating systems, allows an attacker to gain root privileges.
CVE-2000-1059	The default configuration of the Xsession file in Mandrake Linux 7.1 and 7.0 bypasses the Xauthority access control mechanism with an "xhost + localhost" command, which allows local users to sniff X Windows events and gain privileges.
CVE-2000-1095	modprobe in the modutils 2.3.x package on Linux systems allows a local user to execute arbitrary commands via shell metacharacters.
CVE-2000-1107	in.identd ident server in SuSE Linux 6.x and 7.0 allows remote attackers to cause a denial of service via a long request, which causes the server to access a NULL pointer and crash.
CVE-2000-1135	fshd (fsh daemon) in Debian Linux allows local users to overwrite files of other users via a symlink attack.
CVE-2000-1136	elvis-tiny before 1.4-10 in Debian Linux, and possibly other Linux operating systems, allows local users to overwrite files of other users via a symlink attack.
CVE-2000-1189	Buffer overflow in pam_localuser PAM module in Red Hat Linux 7.x and 6.x allows attackers to gain privileges.
CVE-2000-1195	telnet daemon (telnetd) from the Linux netkit package before netkit-telnet-0.16 allows remote attackers to bypass authentication when telnetd is running with the -L command line option.
CVE-2001-0069	dialog before 0.9a-20000118-3bis in Debian Linux allows local users to overwrite arbitrary files via a symlink attack.

CVE Number	Description
CVE-2001-0109	rctab in SuSE 7.0 and earlier allows local users to create or overwrite arbitrary files via a symlink attack on the rctmp temporary file.
CVE-2001-0111	Format string vulnerability in splitvt before 1.6.5 allows local users to execute arbitrary commands via the -rcfile command line argument.
CVE-2001-0116	gpm 1.19.3 allows local users to overwrite arbitrary files via a symlink attack.
CVE-2001-0117	sdiff 2.7 in the diffutils package allows local users to overwrite files via a symlink attack.
CVE-2001-0118	rdist 6.1.5 allows local users to overwrite arbitrary files via a symlink attack.
CVE-2001-0119	getty_ps 2.0.7j allows local users to overwrite arbitrary files via a symlink attack.
CVE-2001-0120	useradd program in shadow-utils program may allow local users to overwrite arbitrary files via a symlink attack.
CVE-2001-0125	exmh 2.2 and earlier allows local users to overwrite arbitrary files via a symlink attack on the exmhErrorMsg temporary file.
CVE-2001-0169	When using the LD_PRELOAD environmental variable in SUID or SGID applications, glibc does not verify that preloaded libraries in /etc/ld.so.cache are also SUID/SGID, which could allow a local user to overwrite arbitrary files by loading a library from
CVE-2001-0170	glibc 2.1.9x and earlier does not properly clear the RESOLV_HOST_CONF, HOSTALIASES, or RES_OPTIONS environmental variables when executing setuid/setgid programs, which could allow local users to read arbitrary files.
CVE-2001-0178	kdesu program in KDE2 (KDE before 2.2.0-6) does not properly verify the owner of a UNIX socket that is used to send a password, which allows local users to steal passwords and gain privileges.
CVE-2001-0193	Format string vulnerability in man in some Linux distributions allows local users to gain privileges via a malformed -l parameter.
CVE-2001-0195	sash before 3.4-4 in Debian Linux does not properly clone /etc/shadow, which makes it world-readable and could allow local users to gain privileges via password cracking.
CVE-2001-0309	inetd in Red Hat 6.2 does not properly close sockets for internal services such as chargen, daytime, echo, etc., which allows remote attackers to cause a denial of service via a series of connections to the internal services.
CVE-2001-0316	Linux kernel 2.4 and 2.2 allows local users to read kernel memory and possibly gain privileges via a negative argument to the sysctl call.

CVE Number	Description
CVE-2001-0317	Race condition in ptrace in Linux kernel 2.4 and 2.2 allows local users to gain privileges by using ptrace to track and modify a running setuid process.
CVE-2001-0366	saposcol in SAP R/3 Web Application Server Demo before 1.5 trusts the PATH environmental variable to find and execute the expand program, which allows local users to obtain root access by modifying the PATH to point to a Trojan horse expand program.
CVE-2001-0405	ip_conntrack_ftp in the IPTables firewall for Linux 2.4 allows remote attackers to bypass access restrictions for an FTP server via a PORT command that lists an arbitrary IP address and port number, which is added to the RELATED table and allowed by th
CVE-2001-0474	Utah-glx in Mesa before 3.3-14 on Mandrake Linux 7.2 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/glxmemory file.
CVE-2001-0481	Vulnerability in rpmdrake in Mandrake Linux 8.0 related to insecure temporary file handling.
CVE-2001-0525	dsh program in dqs version 3.2.7 in SuSE Linux 7.0 and earlier, and possibly other operating systems, allows a local attacker to gain privileges via a buffer overflow in the first command line argument.
CVE-2001-0625	ftpdownload in Computer Associates InoculateIT 6.0 allows a local attacker to overwrite arbitrary files via a symlink attack on /tmp/ftpdownload.log .
CVE-2001-0635	Red Hat Linux 7.1 sets insecure permissions on swap files created during installation, which can allow a local attacker to gain additional privileges by reading sensitive information from the swap file, such as passwords.
CVE-2001-0641	Buffer overflow in man program in various distributions of Linux allows local user to execute arbitrary code as group man via a long -S option.
CVE-2001-0738	LogLine function in klogd in sysklogd 1.3 in various Linux distributions allows an attacker to cause a denial of service (hang) by causing null bytes to be placed in log messages.
CVE-2001-0739	Guardian Digital WebTool in EnGarde Secure Linux 1.0.1 allows restarted services to inherit some environmental variables, which could allow local users to gain root privileges.
CVE-2001-0787	LPRng in Red Hat Linux 7.0 and 7.1 does not properly drop memberships in supplemental groups when lowering privileges, which could allow a local user to elevate privileges.

CVE Number	Description
CVE-2001-0797	Buffer overflow in login in various System V based operating systems allows remote attackers to execute arbitrary commands via a large number of arguments through services such as telnet and rlogin.
CVE-2001-0819	A buffer overflow in Linux fetchmail before 5.8.6 allows remote attackers to execute arbitrary code via a large 'To:' field in an email header.
CVE-2001-0822	FPF kernel module 1.0 allows a remote attacker to cause a denial of service via fragmented packets.
CVE-2001-0850	A configuration error in the libdb1 package in OpenLinux 3.1 uses insecure versions of the snprintf and vsnprintf functions, which could allow local or remote users to exploit those functions with a buffer overflow.
CVE-2001-0851	Linux kernel 2.0, 2.2 and 2.4 with syncookies enabled allows remote attackers to bypass firewall rules by brute force guessing the cookie.
CVE-2001-0852	TUX HTTP server 2.1.0-2 in Red Hat Linux allows remote attackers to cause a denial of service via sending a malformed header.
CVE-2001-0859	2.4.3-12 kernel in Red Hat Linux 7.1 Korean installation program sets the setting default umask for init to 000, which installs files with world-writeable permissions.
CVE-2001-0869	Format string vulnerability in the default logging callback function in Cyrus SASL library (cyrus-sasl) may allow remote attackers to execute arbitrary commands.
CVE-2001-0872	OpenSSH 3.0.1 and earlier with UseLogin enabled does not properly cleanse critical environment variables such as LD_PRELOAD, which allows local users to gain root privileges.
CVE-2001-0886	Buffer overflow in glob function of glibc for Red Hat Linux 6.2 through 7.2, and other operating systems, allows attackers to cause a denial of service (crash) and possibly execute arbitrary code via a glob pattern that ends in a brace "{" character.
CVE-2001-0912	Packaging error for expect 8.3.3 in Mandrake Linux 8.1 causes expect to search for its libraries in the /home/snailtalk directory before other directories, which could allow a local user to gain root privileges.
CVE-2001-0918	Vulnerabilities in CGI scripts in susehelp in SuSE 7.2 and 7.3 allow remote attackers to execute arbitrary commands by not opening files securely.

CVE Number	Description
CVE-2001-0946	apmscript in Apmd in Red Hat 7.2 "Enigma" allows local users to create or change the modification dates of arbitrary files via a symlink attack on the LOW_POWER temporary file, which could be used to cause a denial of service, e.g. by creating /etc/nol
CVE-2001-0977	slapd in OpenLDAP 1.x before 1.2.12, and 2.x before 2.0.8, allows remote attackers to cause a denial of service (crash) via an invalid Basic Encoding Rules (BER) length field.
CVE-2001-0980	docview before 1.0-15 allows remote attackers to execute arbitrary commands via shell metacharacters that are processed when converting a man page to a web page.
CVE-2001-1002	The default configuration of the DVI print filter (dvips) in Red Hat Linux 7.0 and earlier does not run dvips in secure mode when dvips is executed by lpd, which could allow remote attackers to gain privileges by printing a DVI file that contains malic
CVE-2001-1056	IRC DCC helper in the ip_masq_irc IP masquerading module 2.2 allows remote attackers to bypass intended firewall restrictions by causing the target system to send a "DCC SEND" request to a malicious server which listens on port 6667, which may cause th
CVE-2001-1119	cda in xmcd 3.0.2 and 2.6 in SuSE Linux allows local users to overwrite arbitrary files via a symlink attack.
CVE-2001-1130	Sdbsearch.cgi in SuSE Linux 6.0-7.2 could allow remote attackers to execute arbitrary commands by uploading a keylist.txt file that contains filenames with shell metacharacters, then causing the file to be searched using a .. in the HTTP referer (from the
CVE-2001-1146	AllCommerce with debugging enabled in EnGarde Secure Linux 1.0.1 creates teporary files with predictable names, which allows local users to modify files via a symlink attack.
CVE-2001-1177	ml85p in Samsung ML-85G GDI printer driver allows local users to overwrite arbitrary files via a symlink attack on temporary files.
CVE-2001-1180	FreeBSD 4.3 does not properly clear shared signal handlers when executing a process, which allows local users to gain privileges by calling rfork with a shared signal handler, having the child process execute a setuid program, and sending a signal to the

CVE Number	Description
CVE-2001-1240	The default configuration of sudo in Engarde Secure Linux 1.0.1 allows any user in the admin group to run certain commands that could be leveraged to gain full root access.
CVE-2001-1345	bctool in Jetico BestCrypt 0.7 and earlier trusts the user-supplied PATH to find and execute an fsck utility program, which allows local users to gain privileges by modifying the PATH to point to a Trojan horse program.
CVE-2002-0004	Heap corruption vulnerability in the "at" program allows local users to execute arbitrary code via a malformed execution time, which causes at to free the same memory twice.
CVE-2002-0044	Enscript 1.6.1 and earlier allows local users to overwrite arbitrary files of the Enscript user via a symlink attack on temporary files.
CVE-2002-0045	slapd in OpenLDAP 2.0 through 2.0.19 allows local users, and anonymous users before 2.0.8, to conduct a "replace" action on access controls without any values, which causes OpenLDAP to delete non-mandatory attributes which would otherwise be protected by
CVE-2002-0046	Linux kernel, and possibly other operating systems, allows remote attackers to read portions of memory via a series of fragmented ICMP packets that generate an ICMP TTL Exceeded response, which includes portions of the memory in the response packet.
CVE-2002-0060	IRC connection tracking helper module in the netfilter subsystem for Linux 2.4.18-pre9 and earlier does not properly set the mask for conntrack expectations for incoming DCC connections, which could allow remote attackers to bypass intended firewall restr
CVE-2002-0080	rsync does not properly call setgroups before dropping privileges, which could provide supplemental group privileges to local users, who could then read certain files that would otherwise be disallowed.
CVE-2002-0083	Off-by-one error in the channel code of OpenSSH 2.0 through 3.0.2 allows local users or remote malicious servers to gain privileges.
CVE-2002-0207	Buffer overflow in Real Networks RealPlayer 8.0 and earlier allows remote attackers to execute arbitrary code via a header length value that exceeds the actual length of the header.

ภาคผนวก ข

รายละเอียดส่วนโปรแกรมและซอฟต์แวร์ด้านการรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์ประเภทต่าง ๆ

ในส่วนนี้จะแสดงตารางสรุปการติดตั้งส่วนโปรแกรม และโปรแกรมด้านการรักษาความปลอดภัยที่เหมาะสมและจำเป็นสำหรับเซิร์ฟเวอร์ต่าง ๆ ที่มีการแนะนำให้ใช้ ในการเสริมความแข็งแกร่งให้กับลินุกซ์ที่ทำหน้าที่เป็นเซิร์ฟเวอร์ โดยรายละเอียดของการดำเนินการติดตั้งและใช้งานโปรแกรมในตารางที่ ข.1 นี้ มีการกล่าวถึงไว้ใน [24]

รายละเอียดของตารางที่ ข.1 ประกอบด้วย

Server Type	ประเภทของเซิร์ฟเวอร์
Required Components	ส่วนโปรแกรมที่จำเป็นสำหรับเซิร์ฟเวอร์นั้น ๆ
Optional Components	ส่วนโปรแกรมเพื่อเสริมการทำงานของเซิร์ฟเวอร์
Required Security Software	โปรแกรมรักษาความปลอดภัยที่จำเป็นสำหรับการทำงานของเซิร์ฟเวอร์
Recommended Security Software	โปรแกรมรักษาความปลอดภัยที่ควรมีเพื่อเสริมความปลอดภัยให้กับเซิร์ฟเวอร์

ตารางที่ ข.1 โปรแกรมและซอฟต์แวร์ด้านการรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์

Server Type	Mail Server
Required Components	Sendmail or qmail (SMTP Server) BIND/DNS (Cache) IPTABLE Firewall IMAP/POP only for Sendmail
Optional Components	N/A
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry Quota
Server Type	Gateway Server
Required Components	BIND/DNS (Caching) qmail (Standalone) IPTABLES Firewall Squid Proxy (Server)
Optional Components	N/A
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Client & Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry

ตารางที่ ข.1โปรแกรมและซอฟต์แวร์ด้านการรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์ (ต่อ)

Server Type	FTP Server
Required Components	Wu-FTPD (Server) qmail (Standalone) BIND/DNS (Caching) IPTABLE Firewall
Optional Components	N/A
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry Quota
Server Type	Domain Name Server
Required Components	Primary BIND/DNS (Server) qmail (Standalone) IPTABLES Firewall Secondary BIND/DNS (Server)
Optional Components	N/A
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry

ตารางที่ ข.1โปรแกรมและซอฟต์แวร์ด้านการรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์ (ต่อ)

Server Type	File Sharing Server
Required Components	Samba LAN (SErver) qmail (Standalone) BIND/DNS (Caching) IPTABLES Firewall
Optional Components	N/A
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry
Server Type	Database Server
Required Components	PostgreSQL (Client & Server) qmail (Standalone) BIND/DNS (Cache) IPTABLE Firewall MySQL (Client & Server) OpenLDAP (Client & Servers)
Optional Components	N/A
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry

ตารางที่ ข.1โปรแกรมและซอฟต์แวร์ด้านการรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์ (ต่อ)

Server Type	Backup Server
Required Components	Amanda (Server) qmail (Standalone) BIND/DNS (Caching) Dump Utility IPTABLES Firewall
Optional Components	N/A
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry
Server Type	VPN Server
Required Components	FreeS/WAN VPN (Server BIND/DNS (Caching) qmail (Standalone) IPTABLES Firewall
Optional Components	N/A
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry

ตารางที่ ข.1โปรแกรมและซอฟต์แวร์ด้านการรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์ (ต่อ)

Server Type	Web Server
Required Components	Apache (Web Server) qmail (Standalone) BIND/DNS (Caching) IPTABLES Firewall
Optional Components	Mod_PHP4 Capability Mod_SSL Capability Mod-Perl Capability MM Capability Webmail Capability
Required Security Software	Secure Linux Kernel Patches OpenSSL Encryption Software OpenSSH (Server) Tripwire Integrity Tool
Recommended Security Software	GnuPG sXid Logcheck PortSentry Quota

ประวัติผู้เขียนวิทยานิพนธ์

นางสาว รัศมีทิพย์ วิตา เกิดเมื่อวันที่ 6 กันยายน พ.ศ. 2523 ที่จังหวัดลำปาง สำเร็จการศึกษาปริญญาตรี วิทยาศาสตร์บัณฑิต จากภาควิชาวิทยาการคอมพิวเตอร์ประยุกต์ คณะวิทยาศาสตร์ประยุกต์ สถาบันเทคโนโลยีพระจอมเกล้า พระนครเหนือ ในปีการศึกษา 2543 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตร์มหาบัณฑิต ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2544