# บทที่ 3

# การวิเคราะห์และออกแบบระบบ

ในบทนี้จะกล่าวถึงขั้นตอนการวิเคราะห์และออกแบบต้นแบบระบบตรวจจับการบุกรุกแบบผสมเพื่อใช้ในงานวิจัยนี้ เนื้อหาของบทนี้ประกอบด้วยภาพรวมของระบบตรวจจับการบุกรุกที่ได้รับการพัฒนา ข้อมูลนำเข้าเพื่อใช้ตรวจสอบการบุกรุก สถาปัตยกรรมของระบบตรวจจับการบุกรุก การออกแบบข้อมูลฝึกสอนระบบเพื่อใช้ดำเนินการแยกประเภทการทำงานในระบบ ออกแบบขั้นตอนการทำงานของระบบตรวจจับการบุกรุก และแผนภาพกระแสข้อมูลการทำงานของระบบตรวจจับการบุกรุก

## 3.1 ภาพรวมของระบบตรวจจับการบุกรุก

จากลักษณะที่สำคัญของโปรเซสบนระบบปฏิบัติการลินุกซ์ที่ได้กล่าวไว้ในหัวข้อ 2.4 ของบทที่ 2 นำไปสู่การตั้งสมมติฐานในการทำวิจัยคือ หากคำสั่งหรือโปรแกรมของระบบถูกเปลี่ยนแปลงหรือมีการแทรกแซงการทำงานของโปรเซสจะส่งผลต่อการเรียกใช้งานซิสเท็มคอลของโปรเซสนั้น ดังนั้นหากสามารถเก็บรวบรวมพฤติกรรมการทำงานของโปรเซสได้อย่างละเอียดจะสามารถตรวจจับการบุกรุกระบบได้ ในงานวิจัยนี้ใช้ความถี่ของซิสเท็มคอลที่ได้จากการทำงานของโปรเซสมาใช้ในการตรวจสอบการบุกรุก

ระบบตรวจจับการบุกรุกที่พัฒนาขึ้นมานั้นเป็นต้นแบบของเครื่องมือที่ผู้ดูแลระบบสามารถนำไปใช้งานเพื่อตรวจจับการบุกรุกของผู้ไม่หวังดีต่อระบบ การตรวจจับการบุกรุกเริ่มตรวจสอบตั้งแต่ผู้ใช้งานเข้าสู่ระบบและได้รับเชลล์ (shell) เพื่อเรียกใช้งานคำสั่งหรือโปรแกรมบนระบบปฏิบัติการเรียบร้อยแล้ว ระบบตรวจจับการบุกรุกจะคอยติดตามการทำงานต่าง ๆ ของผู้ใช้งานภายใต้เชลล์ที่ผู้ใช้งานได้รับ ลักษณะของระบบตรวจจับการบุกรุกจะพิจารณาความถี่ของซิสเท็มคอลที่ถูกเรียกใช้งานจากการทำงานของโปรเซสซึ่งเป็นคำสั่งหรือโปรแกรมของผู้ใช้งานเปรียบเทียบกับข้อมูลฝึกสอนระบบที่ถูกสร้างขึ้น หากผลการพิจารณาพบว่าโปรเซสนั้นเป็นการทำงานที่เข้าข่ายการบุกรุกระบบปฏิบัติการที่ใช้งานอยู่ ระบบตรวจจับการบุกรุกจะหยุดการทำงานของโปรเซสนั้นรวมทั้งโปรเซสอื่น ๆ ของผู้บุกรุกตลอดจนตัดการเชื่อมต่อของผู้บุกรุกออกจากการติดต่อกับระบบปฏิบัติการเพื่อป้องกันการโจมตีระบบปฏิบัติการจากโปร-เซสอื่น ๆ ของผู้บุกรุก นอกจากนี้ระบบตรวจจับการบุกรุกจะบันทึกข้อมูลรายละเอียดการบุกรุกนี้เก็บไว้ในแฟ้มข้อมูลหลักฐานการบุกรุก และเก็บหลักฐานที่เป็นพฤติกรรมการทำงานของโปรเซส

ซึ่งเป็นการบุกรุกระบบเพื่อให้ผู้ดูแลระบบสามารถตรวจสอบการกระทำย้อนหลังได้ ทั้งนี้เพื่อเป็นการยืนยันการบุกรุกและเพื่อนำข้อมูลที่เกี่ยวข้องกับการบุกรุกไปปรับปรุงข้อมูลฝึกสอนระบบให้มีความทันสมัยมากยิ่งขึ้น

## 3.2 ข้อมูลนำเข้า

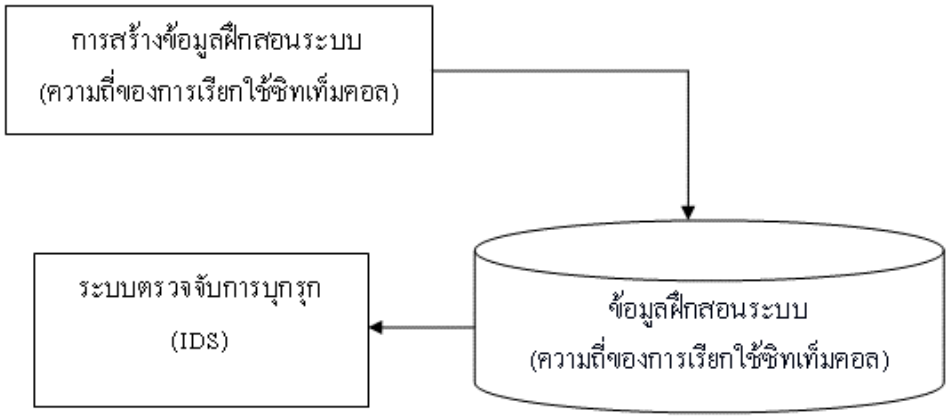
ข้อมูลนำเข้าเพื่อใช้ตรวจสอบการบุกรุกประกอบด้วย ความถี่ของการเรียกใช้งานซิสเท็มคอลจากการทำงานของโปรเซสที่ถูกติดตาม พารามิเตอร์ของซิสเท็มคอลคือชื่อโปรแกรมหรือคำสั่งของระบบปฏิบัติการแต่จะไม่สนใจพารามิเตอร์อื่น ๆ รวมทั้งค่าที่ส่งกลับมาหลังจากที่ซิสเท็มคอลทำงานเสร็จแล้ว โดยที่วิธีการติดตามลำดับการทำงานของโปรเซสต่าง ๆ บนระบบปฏิบัติการลินุกซ์เรดแฮ็ทสามารถทำได้โดยใช้คำสั่ง “strace” ดังที่ได้กล่าวถึงแล้วในหัวข้อ 2.4 ของบทที่ 2 ข้อมูลอื่น ๆ ที่นำมาใช้ในกระบวนการตรวจจับการบุกรุกคือ หมายเลขเชลล์ของผู้ใช้งาน หมายเลขโปรเซสที่ได้รับจากการสร้างโปรเซสของระบบปฏิบัติการ ข้อมูลที่กล่าวมานี้นำมาจากแฟ้มข้อมูลที่เกิดขึ้นจากการทำงานของคำสั่ง strace นอกจากนี้ยังมีชื่อและหมายเลขประจำตัวของผู้ใช้งานซึ่งได้มาจากการทำงานของคำสั่ง “ps” และข้อมูลจากแฟ้ม “/etc/passwd” ของระบบปฏิบัติการลินุกซ์เรดแฮ็ท และแฟ้มข้อมูลที่เก็บความถี่ของซิสเท็มคอลซึ่งเป็นตัวแทนของพฤติกรรมการทำงานของโปรเซสเพื่อใช้ในการแยกประเภทคลาสโดยโปรแกรม TiMBL ดังนั้นข้อมูลนำเข้าสำหรับใช้ในการตรวจจับการบุกรุกมีดังนี้คือ

1. ชื่อผู้ใช้งาน
2. หมายเลขผู้ใช้งาน
3. หมายเลขเชลล์ของผู้ใช้งาน
4. หมายเลขโปรเซส
5. ชื่อโปรเซส
6. แฟ้มข้อมูลในการทดสอบซึ่งเก็บความถี่ของซิสเท็มคอลจากการทำงานของโปรเซสเพื่อนำไปใช้ในการแยกประเภทคลาสโดยโปรแกรม TiMBL
7. เวลาที่พบแฟ้มข้อมูลที่จะนำไปตรวจสอบการทำงาน

ข้อมูลนำเข้าทั้งหมดนี้เกิดขึ้นต่อเนื่องกันในระหว่างการทำงานตรวจจับการบุกรุก โดยมีข้อมูลนำเข้าแรกสุดคือ แฟ้มข้อมูลที่เกิดขึ้นจากการติดตามเชลล์ในระบบด้วยคำสั่ง strace ในหัวข้อถัดไปจะกล่าวถึงสถาปัตยกรรมของระบบตรวจจับการบุกรุก การออกแบบข้อมูลฝึกสอนระบบ และการออกแบบการทำงานของระบบตรวจจับการบุกรุก

## 3.3 สถาปัตยกรรมของระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุกที่ออกแบบไว้มีส่วนประกอบที่สำคัญ 2 ส่วนคือ ส่วนของระบบตรวจจับการบุกรุก และส่วนของข้อมูลฝึกสอนระบบตรวจจับการบุกรุก ในส่วนของข้อมูลฝึกสอนระบบนี้เป็นการรวบรวมพฤติกรรมการทำงานของโปรเซสที่เกิดจากคำสั่งของระบบปฏิบัติการลินุกซ์เรดแฮ็ทและเครื่องมือบุกรุกระบบที่สามารถหาได้จากอินเทอร์เน็ต และสำหรับในส่วนของระบบตรวจจับการบุกรุกคือ โปรแกรมที่สร้างขึ้นเพื่อทำงานตรวจสอบพฤติกรรมการทำงานของโปรเซสที่เกิดขึ้นบนระบบปฏิบัติการที่ระบบตรวจจับการบุกรุกกำลังทำงานอยู่ โดยระบบตรวจจับการบุกรุกจะใช้ข้อมูลฝึกสอนระบบเพื่อตรวจสอบพฤติกรรมการทำงานของโปรเซสว่าเป็นกิจกรรมที่เข้าข่ายการบุกรุกหรือไม่




ภาพประกอบ 3.1 สถาปัตยกรรมของระบบตรวจจับการบุกรุก

## 3.4 ออกแบบข้อมูลฝึกสอนระบบ

ข้อมูลฝึกสอนระบบเป็นส่วนประกอบที่สำคัญอย่างหนึ่งในงานวิจัยนี้ เนื่องจากข้อมูลฝึกสอนระบบคือส่วนที่เก็บรวบรวมพฤติกรรมการทำงานและคลาสของโปรเซสซึ่งใช้สำหรับการเรียนรู้เพื่อทำนายคลาสที่เหมาะสมให้กับพฤติกรรมของโปรเซสที่นำมาแยกประเภทคลาส การสร้างข้อมูลฝึกสอนระบบมีขั้นตอนที่สำคัญ 2 อย่างคือ การเลือกคำสั่งของระบบปฏิบัติการเพื่อกำหนดคลาส และกระบวนการเก็บรวบรวมพฤติกรรมของโปรเซสที่เกิดขึ้นจากคำสั่งของระบบปฏิบัติการที่ได้เลือกไว้แล้วและจากโปรแกรมบุกรุกระบบที่สามารถหาได้จากอินเทอร์เน็ต

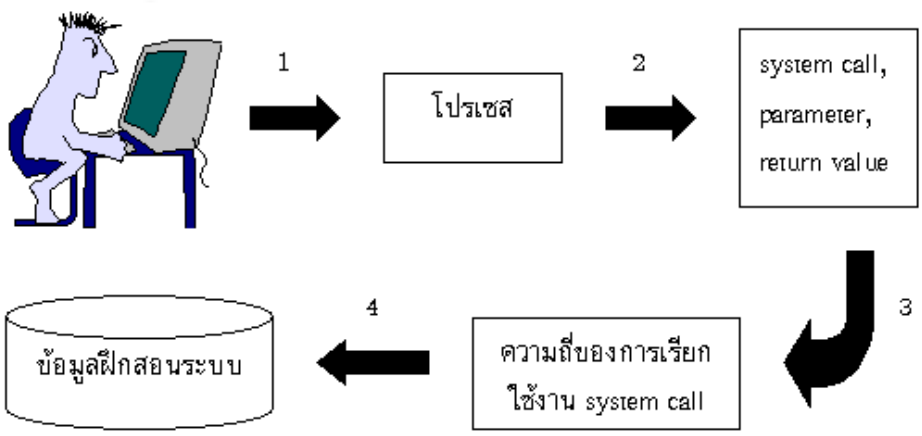
**การเลือกคำสั่งของระบบปฏิบัติการเพื่อกำหนดคลาส** ระบบปฏิบัติการที่เลือกใช้เพื่อพัฒนาระบบตรวจจับการบุกรุกในงานวิจัยนี้คือ ระบบปฏิบัติการลินุกซ์เรดแฮ็ทซึ่งต้นแบบของระบบตรวจจับการบุกรุกได้พัฒนาบนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 เนื่องจากระบบตรวจจับการบุกรุกต้นแบบนี้ทำงานตรวจสอบคำสั่งและโปรแกรมที่ถูกเรียกใช้งานผ่านเชลล์ของผู้ใช้ภายในระบบ ดังนั้นคำสั่งของระบบปฏิบัติการที่เก็บรวบรวมพฤติกรรมไว้จึงเป็นคำสั่งพื้นฐานของลินุกซ์เรดแฮ็ทที่ผู้ใช้งานส่วนใหญ่ภายในระบบจะเรียกใช้งานดังนี้คือ bash, bc, cal, cat, cc, chgrp, chmod, chown, clear, cp, csh, date, du, gcc, grep, groff, grotty, gtbl, gunzip, hostname, id, kill, ktop, login, ls, man, mkdir, more, mv, netstat, last, less, ln, ps, rm, rmdir, sh, sshd, su, syslogd, tar, top, touch, troff, uname, useradd, vi, wc, whereis, which, who และ whoami พฤติกรรมการทำงานของโปรเซสจากคำสั่งเหล่านี้จะเก็บรวบรวมไว้ในแฟ้มข้อมูลฝึกสอนระบบโดยกำหนดให้มีชื่อคลาสอย่างเดียวกันคือ “normal” เพื่อแสดงถึงการทำงานปกติที่เกิดขึ้นภายในระบบ หลังจากเลือกคำสั่งของลินุกซ์เรดแฮ็ทที่ต้องการได้เรียบร้อยแล้ว ขั้นตอนต่อไปจะดำเนินการรวบรวมพฤติกรรมการทำงานของโปรเซสที่เกิดขึ้นจากคำสั่งเหล่านี้ไว้ในแฟ้มข้อมูลฝึกสอนระบบ

**การรวบรวมพฤติกรรมการทำงานของโปรเซส** ก่อนที่จะเก็บรวบรวมพฤติ-กรรมการทำงานของโปรเซสลงในแฟ้มข้อมูลฝึกสอนระบบนั้นจะต้องมั่นใจได้ว่าระบบปฏิบัติการที่ใช้เก็บรวบรวมพฤติกรรมต้องไม่เป็นระบบที่ถูกคุกคามมาแล้ว นั่นคือระบบปฏิบัติการนั้นมาจากการติดตั้งโดยใช้สื่อเก็บข้อมูลที่เชื่อถือได้ และในระหว่างที่เก็บรวบรวมพฤติกรรมอยู่จะตัดการติดต่อผ่านทางเครือข่ายและไม่อนุญาตให้ผู้ใช้งานคนอื่น ๆ เข้ามาใช้งานคอมพิวเตอร์เครื่องนั้น ขั้นตอนของการรวบรวมพฤติกรรมการทำงานของโปรเซสจากคำสั่งที่เลือกไว้เป็นดังนี้

1. ผู้ใช้งานได้รับเชลล์ที่สามารถเรียกใช้งานคำสั่งของระบบหรือโปรแกรมที่ผู้ใช้ต้องการ เมื่อโปรแกรมหรือคำสั่งถูกเรียกใช้งานระบบปฏิบัติการลินุกซ์เรด-แฮ็ทจะเปลี่ยนโปรแกรมหรือคำสั่งนั้นให้เป็นโปรเซส ในขั้นตอนนี้จะตรงกับหมายเลข 1 ในภาพประกอบ 3.2
2. โปรเซสที่เกิดขึ้นจะถูกติดตามการทำงานด้วยคำสั่ง strace ซึ่งมีอยู่ในระบบปฏิบัติการลินุกซ์เรดแฮ็ท การติดตามการทำงานของโปรเซสจะทำให้ได้รับชื่อ พารามิเตอร์ และค่าที่ถูกส่งกลับมาของซิสเท็มคอลตามลำดับทั้งหมด ในขั้นตอนนี้จะตรงกับหมายเลข 2 ในภาพประกอบ 3.2
3. ชื่อของซิสเท็มคอลจะถูกสกัดออกมาเพื่อนับความถี่ของการเรียกใช้งานโดยไม่สนใจพารามิเตอร์และค่าที่ถูกส่งกลับมาของซิสเท็มคอล โดยจะเปลี่ยนชื่อของซิสเท็มคอลเป็นหมายเลขที่ได้กำหนดไว้ในระบบปฏิบัติการเวอร์ชันนั้น หลังจากนั้นจะเลือกหมายเลขซิสเท็มคอลที่เหมาะสมมาใช้เป็นตัวแทน

พฤติกรรมการทำงานของโปรเซสซึ่งวิธีการเลือกจะกล่าวถึงในบทที่ 4 ในขั้นตอนนี้จะตรงกับหมายเลข 3 ของภาพประกอบ 3.2

4. กำหนดคลาสให้กับพฤติกรรมการทำงานของโปรเซสแล้วจัดเก็บลงไปในแฟ้มข้อมูลฝึกสอนระบบ ขั้นตอนนี้เป็นลำดับสุดท้ายสำหรับการจัดเก็บพฤติกรรมการทำงานของโปรเซสแต่ละอย่างไว้ในแฟ้มข้อมูลฝึกสอนระบบ ซึ่งตรงกับหมายเลข 4 ของภาพประกอบ 3.2




ภาพประกอบ 3.2 แนวคิดการสร้างข้อมูลฝึกสอนระบบ

การรวบรวมพฤติกรรมการทำงานของโปรเซสที่เกิดจากโปรแกรมบุกรุกระบบที่หาได้จากอินเทอร์เน็ตเป็นไปตามภาพประกอบ 3.2 เช่นเดียวกันกับการเก็บรวบรวมพฤติ-กรรมการทำงานของโปรเซสที่เกิดจากคำสั่งของระบบปฏิบัติการ แต่กำหนดให้มีชื่อคลาสเป็นอีกชื่อหนึ่งคือ “abnormal” เพื่อแสดงถึงการทำงานที่ผิดปกติหรือการคุกคามระบบ

## 3.5 ออกแบบโปรแกรมตรวจจับการบุกรุก

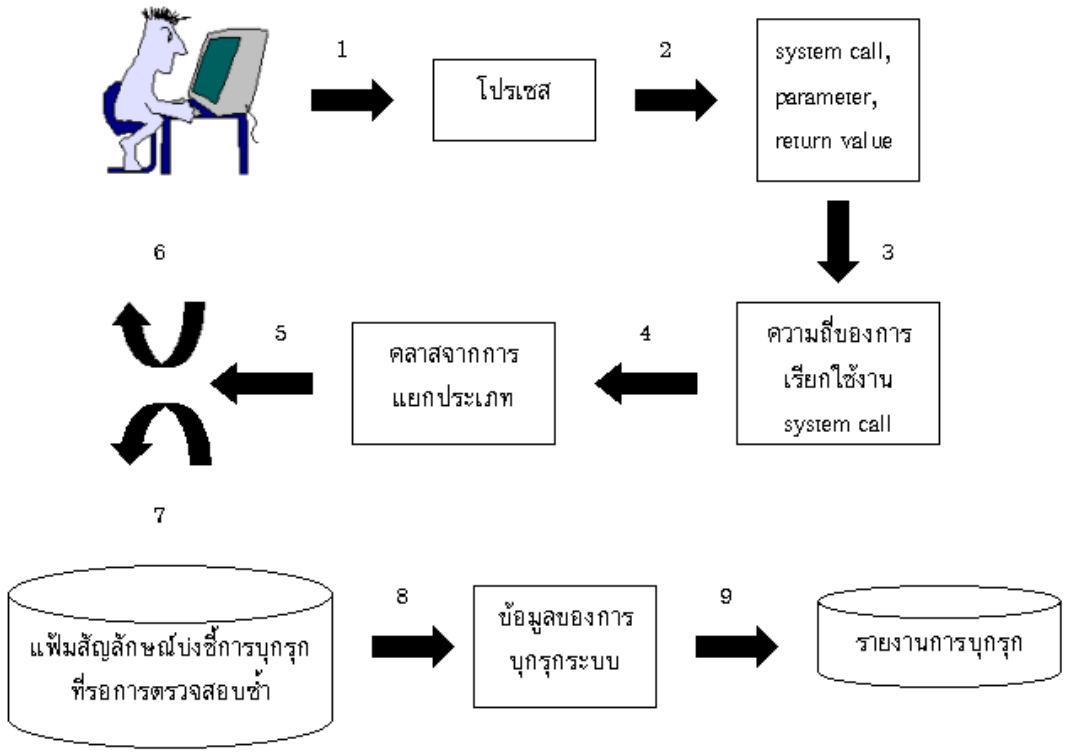
กระบวนการทำงานของระบบตรวจจับการบุกรุกมีความคล้ายคลึงกับการเก็บพฤติกรรมการทำงานของโปรเซสตามภาพประกอบ 3.2 ขั้นตอนการทำงานโดยรวมของระบบตรวจจับการบุกรุกเป็นดังนี้

1. เมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบเรียบร้อยแล้ว ผู้ใช้งานจะได้รับเชลล์จากระบบเพื่อให้สามารถทำงานต่าง ๆ ได้ เมื่อผู้ใช้เรียกโปรแกรมหรือคำสั่งให้ทำงานผ่านเชลล์ ระบบปฏิบัติการลินุกซ์เรดแฮ็ทจะเปลี่ยนโปรแกรมหรือ

คำสั่งนั้นไปเป็นโปรเซส ขั้นตอนนี้ตรงกับหมายเลข 1 ของภาพประกอบ 3.3

2. โปรเซสที่ถูกสร้างขึ้นจะถูกติดตามการทำงานตั้งแต่เริ่มต้นจนกระทั่งจบการทำงานด้วยคำสั่ง strace ของลินุกซ์เรดแฮ็ท ผลที่ได้จากการทำงานของคำสั่ง strace คือ ได้รับชื่อ พารามิเตอร์ และค่าที่ถูกส่งกลับมาของซิสเท็มคอล ตามลำดับการเรียกใช้งานซิสเท็มคอลของโปรเซสนั้น ขั้นตอนนี้ตรงกับหมายเลข 2 ของภาพประกอบ 3.3
3. ส่วนอื่น ๆ ของซิสเท็มคอลจะถูกสกัดทิ้งไปเหลือไว้เพียงชื่อของซิสเท็มคอล จากนั้นจะเปลี่ยนชื่อของซิสเท็มคอลไปเป็นหมายเลขที่ได้กำหนดไว้ในระบบปฏิบัติการเวอร์ชันนั้น แล้วนับความถี่ของซิสเท็มคอลที่ถูกเรียกใช้งานตามหมายเลขที่ได้เลือกไว้เพื่อให้มีรูปแบบข้อมูลตรงกันกับข้อมูลฝึกสอนระบบ แล้วจึงเก็บข้อมูลที่ได้นี้ลงไปในแฟ้มข้อมูลใหม่เพื่อนำไปหาคลาสของการทำงาน ในขั้นตอนนี้ตรงกับหมายเลข 3 ของภาพประกอบ 3.3
4. แฟ้มข้อมูลที่ได้จากข้อ 3 จะถูกนำไปแยกประเภทข้อมูลโดยใช้โปรแกรม TiMBL ในขั้นตอนนี้แฟ้มข้อมูลฝึกสอนระบบที่ได้สร้างเก็บไว้ก่อนจะถูกนำมาใช้เรียนรู้เพื่อทำนายคลาสของโปรเซสว่าเป็นการทำงานปกติภายในระบบหรือเป็นการคุกคามระบบ ขั้นตอนนี้ตรงกับหมายเลข 4 ของภาพประกอบ 3.3
5. คลาสที่ได้จากการแยกประเภทจะถูกตรวจสอบแล้วดำเนินการอย่างเหมาะสมต่อไป ขั้นตอนนี้ตรงกับหมายเลข 5 ของภาพประกอบ 3.3
6. จากขั้นตอนที่ 5 เมื่อตรวจสอบการแยกประเภทข้อมูลแล้วพบว่าเป็นการทำงานแบบปกติจะอนุญาตให้ผู้ใช้งานทำงานอื่น ๆ ภายในระบบต่อไปได้ แต่ทุก ๆ การทำงานจะถูกตรวจสอบเช่นเดียวกันกับการทำงานที่เกิดขึ้นแล้ว ขั้นตอนนี้ตรงกับหมายเลข 6 ของภาพประกอบ 3.3
7. จากขั้นตอนที่ 5 หากตรวจสอบการแยกประเภทข้อมูลแล้วพบว่าเป็นการทำงานในเชิงบุกรุกระบบ และถ้าการทำงานนั้นเกิดจากคำสั่งของระบบปฏิบัติการลินุกซ์เรดแฮ็ทจะดำเนินการเก็บชื่อคำสั่งของระบบปฏิบัติการที่แสดงพฤติกรรมการทำงานในเชิงคุกคามระบบลงไปในแฟ้มข้อมูลสัญลักษณ์บ่งชี้การบุกรุกเพื่อให้ผู้ดูแลระบบสามารถตรวจสอบการทำงานของคำสั่งนั้นได้ต่อไปในภายหลัง แต่ถ้าการทำงานนั้นไม่ใช่การทำงานที่เกิดจากคำสั่งของระบบปฏิบัติการจะข้ามขั้นตอนนี้ไป สำหรับขั้นตอนนี้ตรงกับหมายเลข 7 ของภาพประกอบ 3.3

8. ดำเนินการเก็บข้อมูลประกอบการบุกรุกระบบไว้ในรูปแบบที่พร้อมจะบันทึกลงในแฟ้มข้อมูลซึ่งเป็นรายงานการบุกรุกระบบที่ตรวจสอบพบ ในขั้นตอนนี้ตรงกับหมายเลข 8 ของภาพประกอบ 3.3
9. ขั้นตอนสุดท้ายของการตรวจสอบแล้วพบว่าเป็นการบุกรุกระบบจะเป็นการบันทึกข้อมูลที่รวบรวมได้ไว้ในแฟ้มข้อมูลรายงานผล และเก็บหลักฐานการบุกรุกระบบไว้ในสารบบเพื่อให้ผู้ดูแลระบบสามารถตรวจสอบซ้ำได้ และตัดการเชื่อมต่อระหว่างผู้บุกรุกกับระบบปฏิบัติการเพื่อไม่ให้ผู้บุกรุกสามารถทำงานอื่น ๆ บนระบบได้อีกต่อไป ขั้นตอนนี้ตรงกับหมายเลข 8 ของภาพประกอบ 3.3

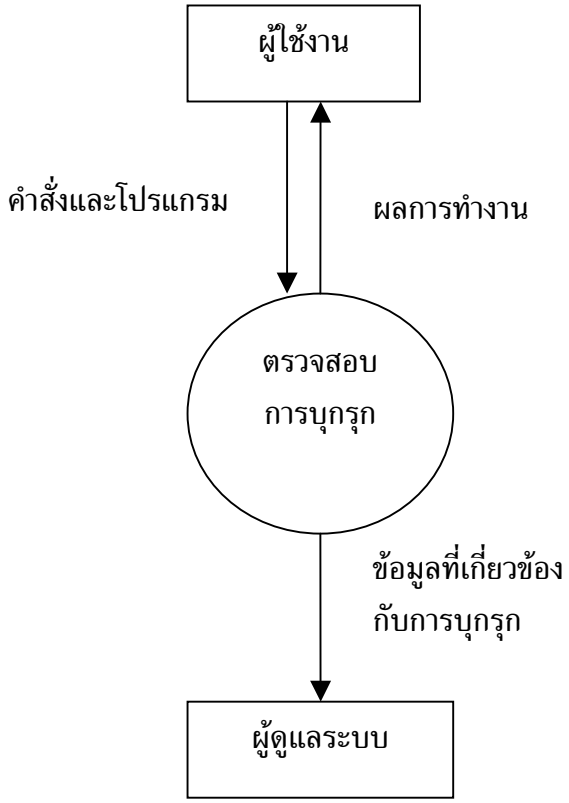



ภาพประกอบ 3.3 แนวคิดการทำงานของโปรแกรมตรวจจับการบุกรุก

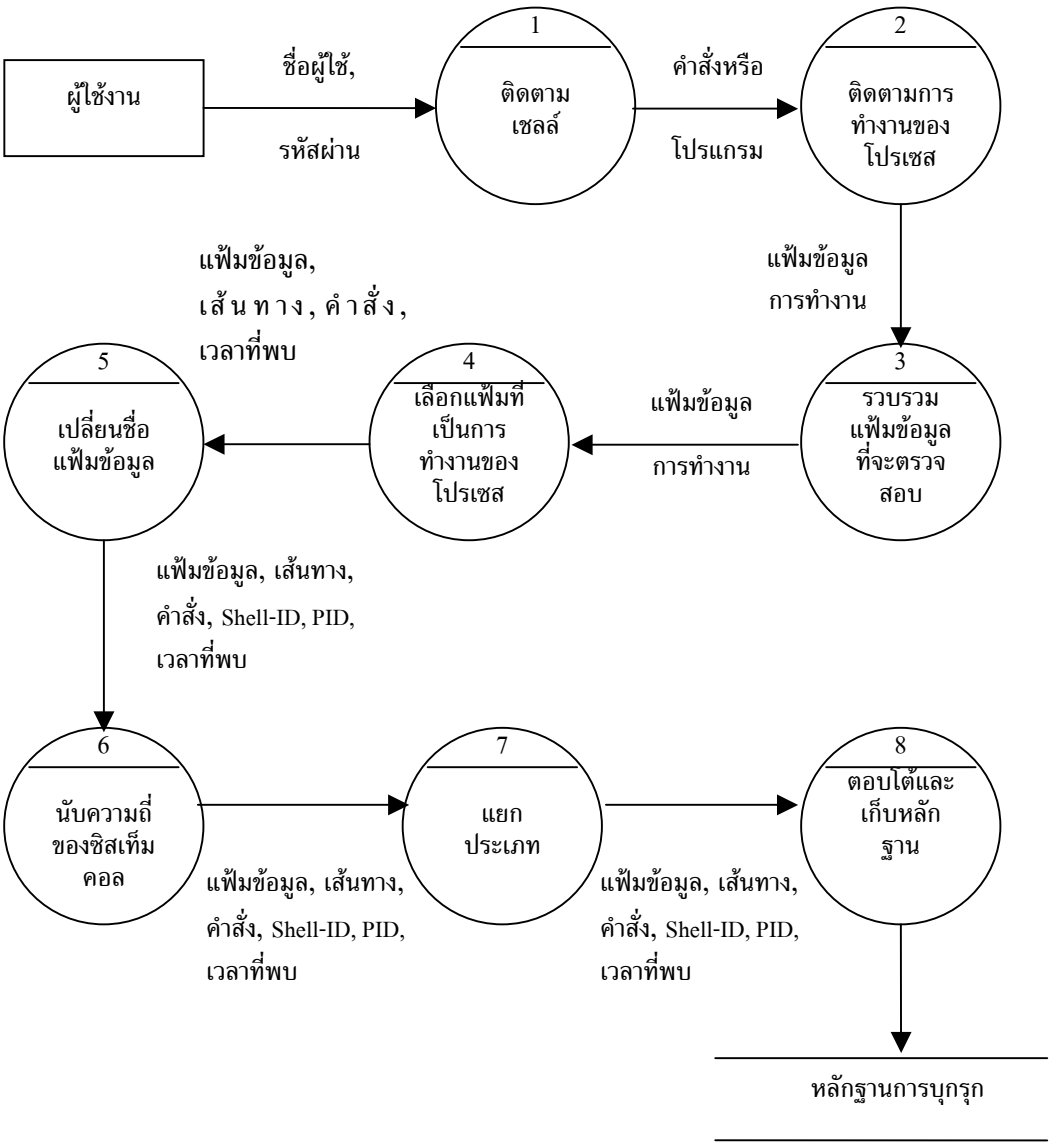
## 3.6 แผนภาพกระแสข้อมูลการทำงานของระบบตรวจจับการบุกรุก

ขั้นตอนการดำเนินงานของระบบตรวจจับการบุกรุกสามารถอธิบายโดยการเขียนให้อยู่ในรูปของแผนภาพกระแสข้อมูล (data flow diagram (DFD)) ซึ่งช่วยให้เข้าใจกระบวนการดำเนินงานต่าง ๆ และการไหลเวียนของข้อมูลที่เกิดขึ้นในโปรแกรม สำหรับแผนภาพกระแสข้อ

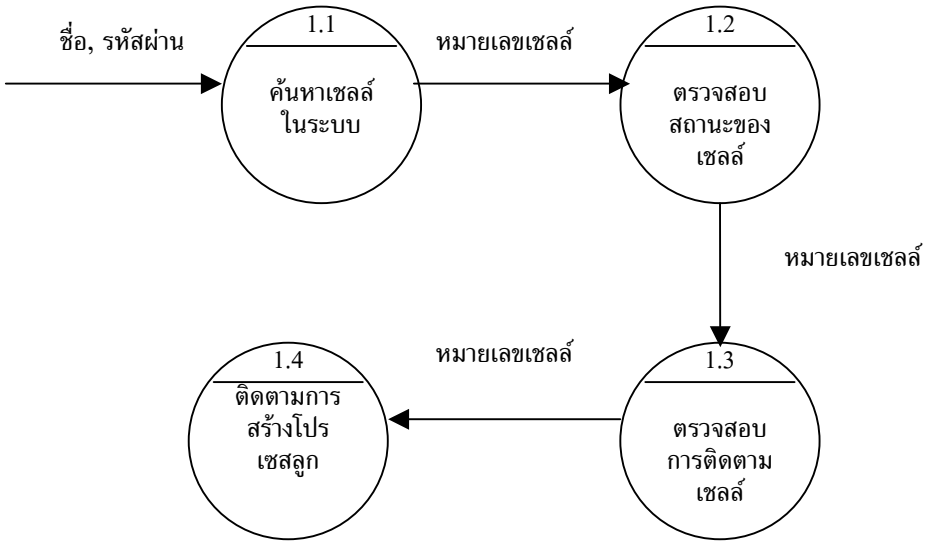
มูลของกระบวนการที่สำคัญของระบบตรวจจับการบุกรุกแสดงเริ่มจาก DFD ระดับสูงสุด (context level data flow diagram) ของระบบตรวจจับการบุกรุก และ DFD ระดับย่อยซึ่งแสดงแผนภาพกระแสข้อมูลในกระบวนการย่อยของระบบเรียงลำดับจากภาพประกอบ 3.4 ถึงภาพประกอบ 3.12 ส่วนคำอธิบายรายละเอียดการทำงานของกระบวนการต่าง ๆ จากแผนภาพกระแสข้อมูลแสดงไว้ในตาราง 3.1 ถึงตาราง 3.8 ตามลำดับ



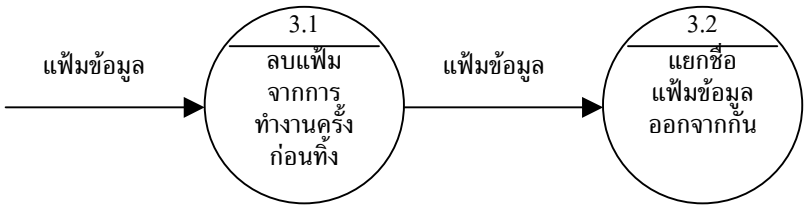

ภาพประกอบ 3.4 แผนภาพบริบทของระบบตรวจจับการบุกรุก



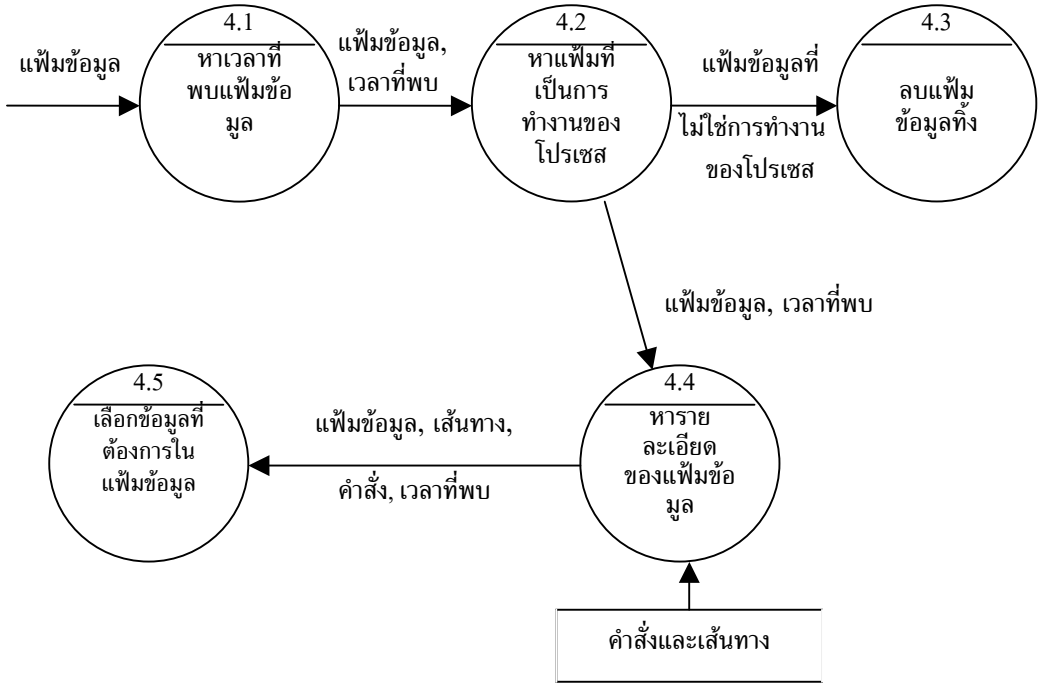

ภาพประกอบ 3.5 DFD ระดับที่ 1 ของระบบตรวจจับการบุกรุก



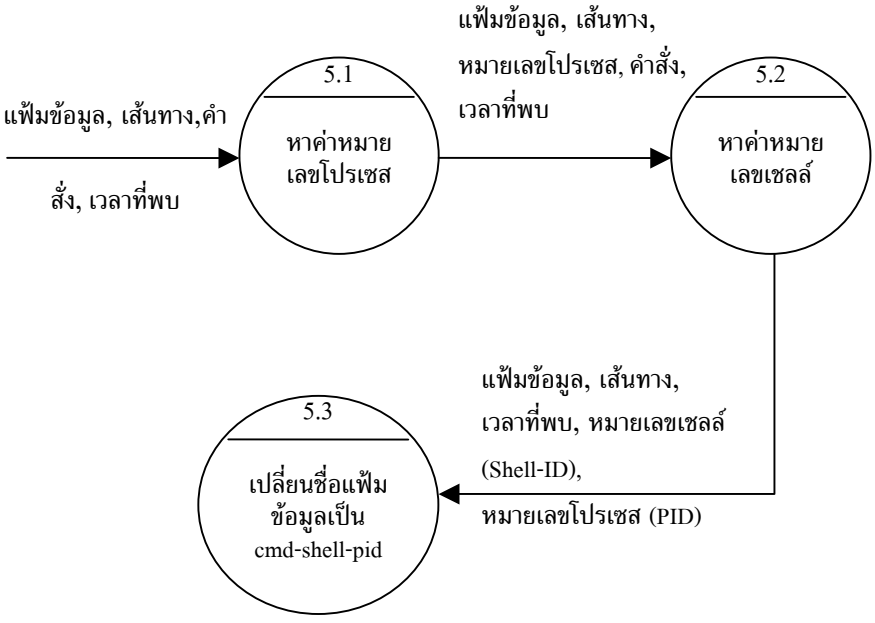

ภาพประกอบ 3.6 DFD ระดับที่ 2 ของกระบวนการที่ 1 การติดตามการทำงานของเซลล์



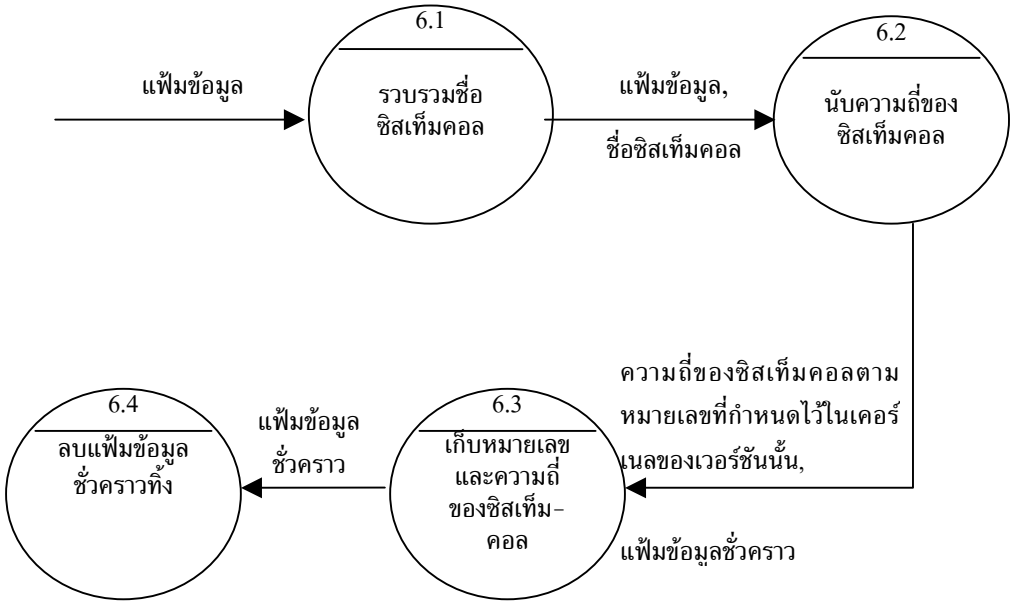

ภาพประกอบ 3.7 DFD ระดับที่ 2 ของกระบวนการที่ 3 การรวบรวมแฟ้มข้อมูลการทำงานของโปรเซส



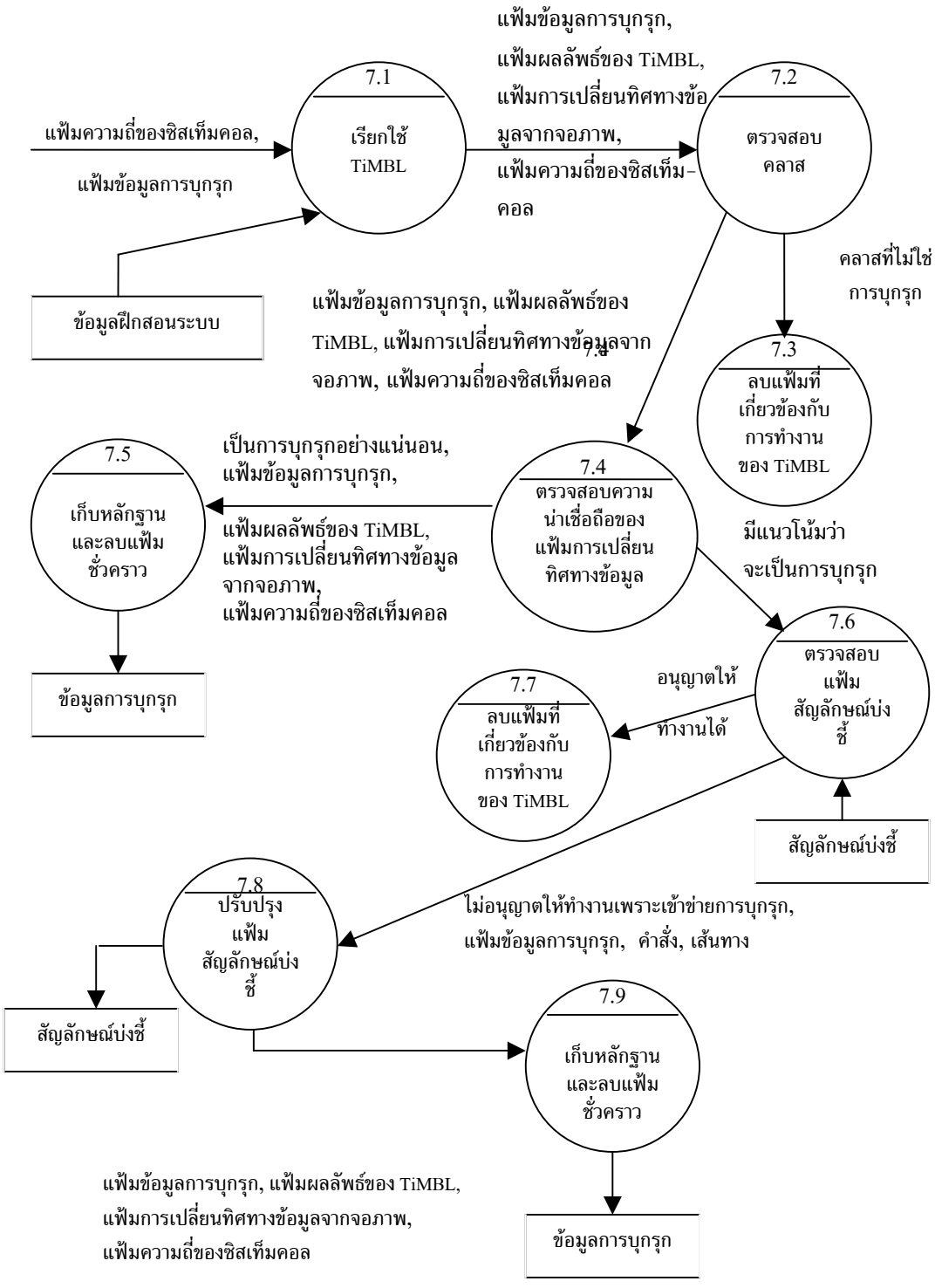

ภาพประกอบ 3.8 DFD ระดับที่ 2 ของกระบวนการที่ 4 การตรวจสอบแฟ้มข้อมูล



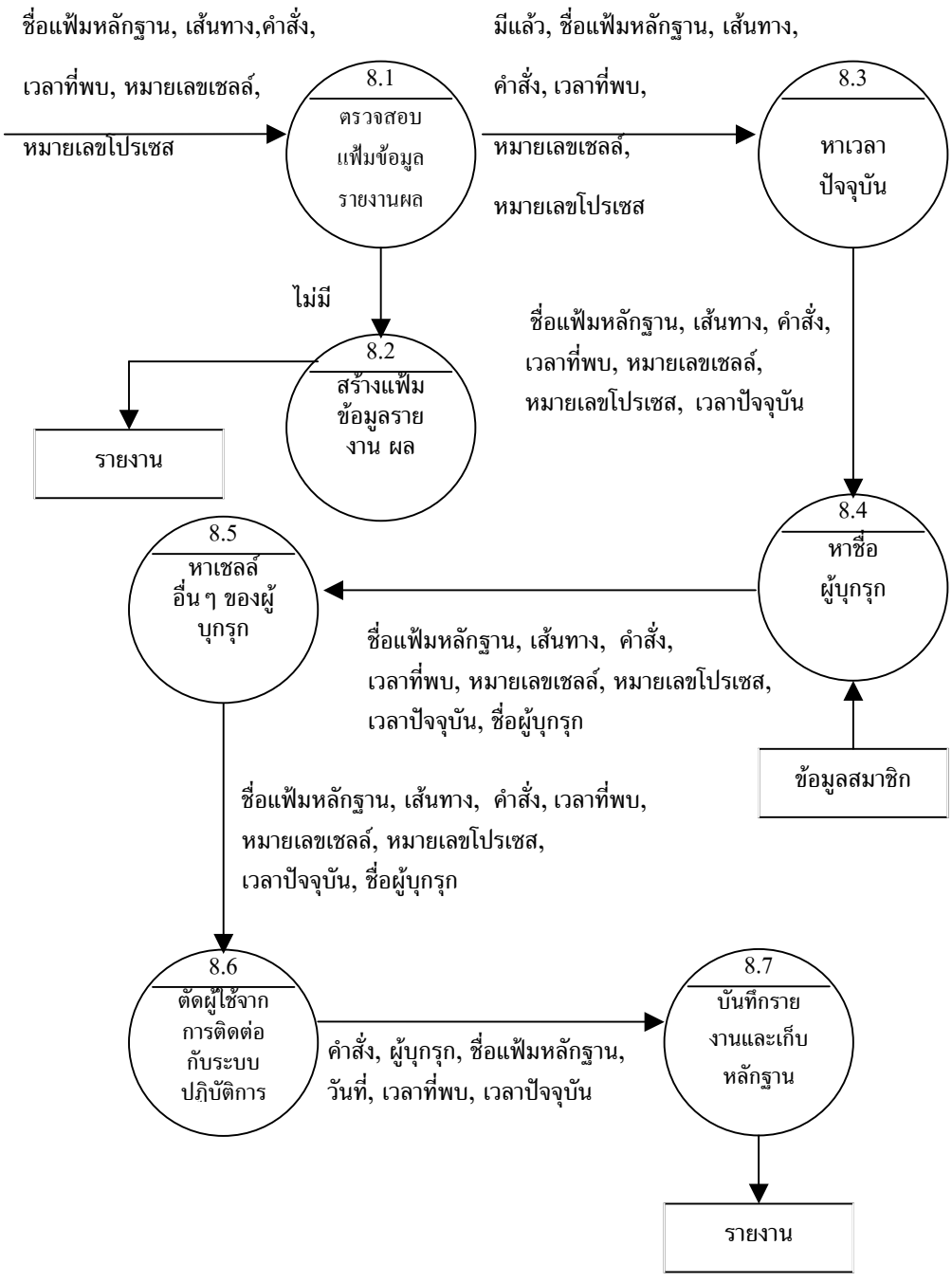

ภาพประกอบ 3.9 DFD ระดับที่ 2 ของกระบวนการที่ 5 การเปลี่ยนชื่อแฟ้มข้อมูลให้สัมพันธ์กับคำสั่งที่ถูกเรียกให้ทำงาน




ภาพประกอบ 3.10 DFD ระดับที่ 2 ของกระบวนการที่ 6 การนับความถี่ของซิสเท็มคอล




ภาพประกอบ 3.11 DFD ระดับที่ 2 ของกระบวนการที่ 7 การแยกประเภทการทำงานของโปรเซส




ภาพประกอบ 3.12 DFD ระดับที่ 2 ของกระบวนการที่ 8 การตอบโต้การบุกรุกและการรายงานผล

ตาราง 3.1 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.5

| กระบวนการที่ | การทำงานของกระบวนการ |
|---|---|
| 1 | ติดตามเชลล์ของผู้ใช้งานบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท |
| 2 | ติดตามการทำงานของโปรเซสลูกที่เกิดจากการเรียกใช้งานโปรแกรมหรือคำสั่งของระบบปฏิบัติการผ่านเชลล์ของผู้ใช้งาน |
| 3 | รวบรวมแฟ้มข้อมูลที่เกิดจากการติดตามการทำงานของโปรเซสเพื่อตรวจสอบความปลอดภัยให้กับระบบปฏิบัติการจากการทำงานของโปรเซส |
| 4 | ตรวจสอบแฟ้มข้อมูลโดยคัดเลือกเฉพาะแฟ้มข้อมูลที่เป็นการทำงานของโปรแกรมหรือคำสั่งของระบบปฏิบัติการ |
| 5 | เปลี่ยนชื่อแฟ้มข้อมูลเดิมให้สัมพันธ์กันกับการทำงานของโปรเซสโดยใช้ชื่อของโปรแกรมหรือคำสั่งที่ถูกเรียกให้ทำงาน |
| 6 | นับความถี่ของการเรียกใช้งานซิสเท็มคอลแยกตามหมายเลขของซิสเท็ม-คอล |
| 7 | แยกประเภทการทำงานของโปรเซสโดยใช้ TiMBL |
| 8 | ตัดผู้บุกรุกจากการเชื่อมต่อกับระบบปฏิบัติการและรวบรวมหลักฐานเพื่อทำรายงานประกอบการบุกรุก |

ตาราง 3.2 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.6

| กระบวนการที่ | การทำงานของกระบวนการ |
|---|---|
| 1.1 | ค้นหาเชลล์ในระบบปฏิบัติการ |
| 1.2 | ตรวจสอบสถานะเชลล์ของผู้ใช้งานในสารบบ /proc ของระบบปฏิบัติการ |
| 1.3 | ตรวจสอบเชลล์ของผู้ใช้งานว่าได้รับการติดตามด้วยคำสั่ง strace แล้วหรือยัง |
| 1.4 | ติดตามการสร้างโปรเซสลูกของเชลล์ |

ตาราง 3.3 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.7

| กระบวนการที่ | การทำงานของกระบวนการ |
|---|---|
| 3.1 | ลบแฟ้มข้อมูลที่ไม่ต้องใช้งานแล้วซึ่งอาจหลงเหลืออยู่จากการทำงานในครั้งก่อน |
| 3.2 | แยกชื่อแฟ้มข้อมูลเพื่อเตรียมพร้อมสำหรับการตรวจสอบแฟ้มข้อมูล |

ตาราง 3.4 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.8

| กระบวนการที่ | การทำงานของกระบวนการ |
|---|---|
| 4.1 | หาเวลาขณะที่ค้นพบแฟ้มข้อมูล |
| 4.2 | ตรวจสอบว่าแฟ้มข้อมูลนั้นเป็นการทำงานของโปรเซสหรือไม่ |
| 4.3 | ลบแฟ้มข้อมูลที่ไม่ใช่การทำงานของโปรเซสทิ้งไป |
| 4.4 | หารายละเอียดที่ต้องการจากแฟ้มข้อมูลคือ เส้นทางการทำงาน คำสั่งหรือโปรแกรมที่ถูกเรียกใช้งาน |
| 4.5 | เลือกข้อมูลการทำงานของโปรเซสเริ่มต้นจากซิสเท็มคอลชื่อ execve จนกระทั่งสิ้นสุดการทำงานของโปรเซส |

ตาราง 3.5 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.9

| กระบวนการที่ | การทำงานของกระบวนการ |
|---|---|
| 5.1 | หาค่าหมายเลขโปรเซส (PID) |
| 5.2 | หาค่าหมายเลขเชลล์ (shell) |
| 5.3 | เปลี่ยนชื่อแฟ้มข้อมูลให้มีความสัมพันธ์กับการทำงานของโปรเซส โดยกำหนดให้ชื่อของแฟ้มข้อมูลมีรูปแบบคือ ชื่อคำสั่ง-หมายเลขเชลล์-หมายเลขโปรเซส (cmd-shell-PID) |

ตาราง 3.6 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.10

| กระบวนการที่ | การทำงานของกระบวนการ |
|---|---|
| 6.1 | คัดเลือกเฉพาะชื่อของซิสเท็มคอลและพารามิเตอร์คือชื่อโปรเซส โดยตัดส่วนของพารามิเตอร์อื่น ๆ และค่าที่ส่งกลับคืนออกไป และเปลี่ยนชื่อซิสเท็มคอลไปเป็นหมายเลขตามที่ระบบปฏิบัติการได้กำหนดไว้ |
| 6.2 | นับความถี่ของซิสเท็มคอลแยกตามหมายเลขของซิสเท็มคอล |
| 6.3 | จัดเก็บความถี่ของซิสเท็มคอลแยกตามหมายเลขของซิสเท็มคอลไว้ในแฟ้มข้อมูลใหม่เพื่อนำไปใช้กับการทำงานของโปรแกรม TiMBL |
| 6.4 | ลบแฟ้มข้อมูลชั่วคราวระหว่างการทำงานทิ้ง |

ตาราง 3.7 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.11

| กระบวนการที่ | การทำงานของกระบวนการ |
|---|---|
| 7.1 | เรียกใช้งานโปรแกรม TiMBL เพื่อแยกประเภทคลาสการทำงานของโปร-เซส |
| 7.2 | ตรวจสอบคลาสจากการทำงานของโปรแกรม TiMBL |
| 7.3 | หากพบว่าไม่ใช่คลาสการทำงานที่ผิดปกติ (abnormal) จะลบแฟ้มข้อมูลที่เกี่ยวข้องกับการทำงานของโปรแกรม TiMBL ทิ้ง |
| 7.4 | ถ้าเป็นคลาสการทำงานที่ผิดปกติจะตรวจสอบความน่าเชื่อถือโดยใช้แฟ้มการเปลี่ยนทิศทางของข้อมูลก่อนตัดสินใจยอมรับว่าเป็นการบุกรุกระบบ |
| 7.5 | เมื่อตรวจสอบความน่าเชื่อถือแล้วพบว่าเป็นกลุ่มการบุกรุกจริงจะเก็บหลัก-ฐานการบุกรุกแล้วลบแฟ้มข้อมูลชั่วคราวระหว่างการทำงานทิ้ง |
| 7.6 | เมื่อตรวจสอบความน่าเชื่อถือแล้วพบว่าโปรเซสที่เกิดจากคำสั่งของระบบปฏิบัติการมีแนวโน้มที่จะเป็นการทำงานบุกรุกระบบ ระบบตรวจจับการบุกรุกจะตรวจสอบแฟ้มข้อมูลซึ่งเก็บคำสั่งที่ถูกทำสัญลักษณ์การบุกรุกก่อนตัดสินใจดำเนินการ |
| 7.7 | เมื่อตรวจสอบแฟ้มเก็บคำสั่งที่ถูกทำสัญลักษณ์แล้วพบว่าคำสั่งนั้นได้รับการบันทึกไว้ในแฟ้มแล้ว ระบบตรวจจับการบุกรุกจะยอมให้คำสั่งนั้นทำงานไปก่อนเนื่องจากเป็นคำสั่งที่รอการตรวจสอบอยู่ และดำเนินการลบแฟ้มข้อมูลที่เกี่ยวข้องกับการทำงานของโปรแกรม TiMBL ทิ้ง |
| 7.8 | เมื่อตรวจสอบแฟ้มเก็บคำสั่งที่ถูกทำสัญลักษณ์แล้วพบว่าคำสั่งนั้นเป็นคำสั่งที่ยังไม่ถูกทำสัญลักษณ์เก็บไว้ ระบบตรวจจับการบุกรุกจะเก็บข้อมูลคำสั่งนั้นไว้ในแฟ้มเก็บคำสั่งที่ถูกทำสัญลักษณ์ว่าเป็นการบุกรุก |
| 7.9 | เก็บหลักฐานการบุกรุกไว้แล้วลบแฟ้มข้อมูลชั่วคราวระหว่างการทำงานทิ้ง |

ตาราง 3.8 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.12

| กระบวนการที่ | การทำงานของกระบวนการ |
|---|---|
| 8.1 | ตรวจสอบแฟ้มข้อมูลรายงานผลว่ามีแฟ้มข้อมูลนี้อยู่แล้วหรือยัง |
| 8.2 | ถ้ายังไม่มีแฟ้มข้อมูลรายงานผลจะสร้างแฟ้มข้อมูลรายงานผลขึ้นมาก่อน |
| 8.3 | หาเวลาปัจจุบัน |
| 8.4 | หาชื่อผู้บุกรุกโดยใช้รายละเอียดจากเชลล์และแฟ้ม /etc/passwd |
| 8.5 | หาเชลล์อื่น ๆ ของผู้บุกรุกเพื่อตัดการเชื่อมต่อที่มีอยู่ทั้งหมด |

ตาราง 3.8 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.12 (ต่อ)

| กระบวนการที่ | การทำงานของกระบวนการ |
|---|---|
| 8.6 | ตัดการเชื่อมต่อของผู้บุกรุกจากระบบปฏิบัติการ |
| 8.7 | บันทึกข้อมูลการบุกรุกระบบลงในแฟ้มข้อมูลรายงานผล และเก็บหลักฐาน ซึ่งเป็นแฟ้มข้อมูลที่เก็บพฤติกรรมการทำงานของโปรเซสที่ทำงานบุกรุกระบบไว้ในสารบบ /testit/evidence |

## 3.7 สรุป

ในบทนี้ได้กล่าวถึงแนวคิดการสร้างระบบตรวจจับบุกรุก การออกแบบสถาปัตยกรรมซึ่งแสดงให้เห็นส่วนประกอบต่าง ๆ ของระบบตรวจจับการบุกรุก แนวคิดของขั้น-ตอนการทำงานของระบบตรวจจับการบุกรุก และวิธีการสร้างข้อมูลฝึกสอนระบบเพื่อให้ระบบตรวจจับการบุกรุกใช้เรียนรู้และแยกประเภทพฤติกรรมการทำงานที่ต้องการทราบ ในบทต่อไปจะกล่าวถึงการพัฒนาระบบตรวจจับการบุกรุกเพื่อใช้งานบนระบบปฏิบัติการลินุกซ์เรดแฮ็ทเวอร์ชัน 6.1