บทที่ 1

บทนำ

1.1 ความสำคัญและที่มาของหัวข้อวิจัย

ปัจจุบันเครือข่ายอินเทอร์เน็ตได้ขยายตัวอย่างรวดเร็ว รวมถึงการเพิ่มขึ้นของช่องทางในการติดต่อสื่อสารระหว่างกันและกันในเครือข่าย ทำให้ผู้ใช้สามารถติดต่อสื่อสารกันได้สะดวกขึ้น แต่อย่างไรก็ตามสิ่งเหล่านี้ก็ส่งผลถึงค่าใช้จ่ายในการดูแลระบบคอมพิวเตอร์เพิ่มขึ้นด้วย โดยเฉพาะอย่างยิ่งค่าใช้จ่ายในเรื่องการรักษาความปลอดภัย เนื่องจากเครือข่ายและช่องทางในการสื่อสารมีมากขึ้นเท่าใด ผู้บุกรุกก็จะอาศัยสิ่งเหล่านั้นมาใช้ในการบุกรุกระบบได้มากขึ้นด้วยเช่นกัน จึงส่งผลให้ภัยคุกคามและการบุกรุกต่าง ๆ บนระบบคอมพิวเตอร์มีแนวโน้มที่เพิ่มสูงขึ้นมากในปัจจุบัน

ปัญหาการรักษาความปลอดภัยจึงเป็นปัญหาสำคัญมากในปัจจุบัน ดังนั้นแต่ละองค์กรควรจะมีมาตรการในการรักษาความปลอดภัยของทรัพยากรคอมพิวเตอร์และเครือข่าย ซึ่งเป็นกระบวนการที่เกี่ยวข้องกับการป้องกันและตรวจสอบการเข้าใช้งานโดยไม่ได้รับอนุญาต โดยการป้องกันจะช่วยสกัดกั้นไม่ให้ผู้ที่ไม่ได้รับอนุญาตซึ่งมักเรียกว่า ผู้บุกรุก เข้าถึงระบบไม่ว่าจะเป็นส่วนใดก็ตาม ส่วนการตรวจสอบจะทำให้ทราบได้ว่ามีใครพยายามบุกรุกเข้ามาในระบบหรือไม่ การบุกรุกสำเร็จหรือไม่และผู้บุกรุกทำอะไรกับระบบบ้าง

ดังนั้นจึงมีแนวความคิดในการสร้างระบบที่เป็นเครื่องมือเพื่อใช้ในการตรวจจับเหตุการณ์การบุกรุกที่เรียกว่าระบบตรวจจับการบุกรุก (Intrusion Detection System) หรือที่เรียกย่อว่า IDS ซึ่งเป็นระบบที่ใช้ในการตรวจสอบการใช้งานและความพยายามในการใช้งานคอมพิวเตอร์และเครือข่ายที่ขัดกับข้อบังคับและวัตถุประสงค์การใช้งานที่ได้ระบุไว้ในนโยบายการรักษาความปลอดภัยขององค์กร

โดยทั่วไปแล้วระบบตรวจจับการบุกรุกจะเก็บรวบรวมข้อมูลต่าง ๆ แล้วนำวิเคราะห์เพื่อตรวจจับการบุกรุก โดยข้อมูลที่นำมาใช้สำหรับการวิเคราะห์อาจจะเป็นแพ็กเก็ต (packet) ในเครือข่าย โดยระบบตรวจจับการบุกรุกที่ใช้ข้อมูลประเภทนี้ในการวิเคราะห์เพื่อตรวจจับการบุกรุกจะเรียกว่า Network-Based Intrusion Detection System (NIDS) ส่วนข้อมูลอีกประเภทหนึ่ง คือบันทึกการทำงาน (Audit Log) ที่ได้จากระบบปฏิบัติการและโปรแกรมประยุกต์ ซึ่งระบบตรวจจับการบุกรุกที่ใช้ข้อมูลนี้ในการวิเคราะห์จะเรียกว่า Host-Based Intrusion Detection System (HIDS) แนวทางและวิธีการในการตรวจสอบการบุกรุกนั้นทำได้หลายวิธี โดยในการศึกษาครั้งนี้จะอาศัยข้อมูลบันทึกการทำงานที่มีการบันทึกผ่านกลไกของ syslog ของระบบยูนิกซ์ ที่เก็บอยู่ในล็อกไฟล์ต่าง ๆ ในการวิเคราะห์เพื่อตรวจจับการบุกรุก ปัญหาที่สำคัญสำหรับ

การตรวจจับการบุกรุกด้วยวิธีการวิเคราะห์ข้อมูลในล็อกไฟล์ คือปริมาณของข้อมูลที่เก็บรวบรวมได้นั้นมีปริมาณมาก จึงเกิดปัญหาในเรื่องของพื้นที่ที่จะต้องมีการจัดเตรียมไว้สำหรับการจัดเก็บรวมทั้งความยุ่งยากในการตรวจสอบข้อมูลเหล่านั้นเพื่อตรวจจับการบุกรุก ซึ่งในสภาวะแวดล้อมการใช้งานระบบที่ต่างกัน ข้อกำหนดในการเก็บรวบรวมข้อมูลก็จะแตกต่างกันด้วย ดังนั้นในการศึกษาครั้งนี้จะใช้สภาวะแวดล้อมของการใช้ระบบคอมพิวเตอร์ของศูนย์คอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ เป็นกรณีศึกษา

1.2 การตรวจเอกสาร

ในการศึกษาเกี่ยวกับเรื่อง ระบบตรวจจับการบุกรุก ซึ่งหมายถึง ระบบที่ประกอบด้วยฮาร์ดแวร์หรือซอฟต์แวร์สำหรับทำงานในกระบวนการตรวจสอบเหตุการณ์ต่าง ๆที่เกิดขึ้นในระบบคอมพิวเตอร์และเครือข่ายเพื่อวิเคราะห์หาร่องรอยของการบุกรุกโดยอัตโนมัติและการบุกรุก(Intrusion) คือ ความพยายามหรือการกระทำที่ส่งผลต่อความบูรณภาพ (Integrity) ความลับ (Confidentiality) และความพร้อมใช้งาน (Availability) ของทรัพยากรในระบบหรือข้ามผ่านมาตรการในการควบคุมความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย [Bace and Mell, 2001] โดยงานวิจัยที่สำคัญและเป็นรากฐานของการศึกษาและพัฒนาระบบตรวจจับการบุกรุกเสนอโดย James Anderson [Anderson, 1980] เรื่อง "Computer Security Threat Monitoring and Surveillance" โดยได้เสนอแนวความคิดพื้นฐานว่าพฤติกรรมปกติของผู้ใช้สามารถอธิบายได้โดยการวิเคราะห์กิจกรรมต่าง ๆ ในล็อกไฟล์และการบุกรุกระบบคอมพิวเตอร์สามารถตรวจจับโดยการใช้ข้อมูลที่ได้มาจากลักษณะของพฤติกรรมทั่วไป ดังนั้นประโยชน์ของล็อกไฟล์คือสามารถนำมาใช้ติดตามพฤติกรรมของผู้ใช้เพื่อที่จะตรวจจับการบุกรุกระบบ ซึ่งมีลักษณะการทำงานแบบ Misuse Detection คือการตรวจจับจากการใช้งานที่ไม่ได้รับอนุญาต โดยระบบจะทำการตรวจสอบการกระทำที่อาจจะส่อได้ว่าเป็นการทำงานที่ไม่น่าไว้วางใจตามรูปแบบของการเจาะเข้าสู่ระบบที่ได้บันทึกไว้ ซึ่งต่อมา Dorothy Denning และ Peter Neumann [Denning and Neumann, 1985] ได้วิจัยและพัฒนาต้นแบบระบบตรวจจับการบุกรุกแบบ Real-Time ชื่อว่า Intrusion Detection Expert System (IDES) ที่ทำงานในแบบอิงกฎ (Rule-Based) และต่อมาได้มีการปรับปรุงและขยายความสามารถเพิ่มเติมภายใต้ชื่อ Next-Generation Intrusion Detection Expert System (NIDES) [SRI International] และนำไปสู่การพัฒนาแนวทางและวิธีการในการตรวจจับการบุกรุกอีกหลายวิธีในลำดับต่อมา ซึ่งจะกล่าวถึงรายละเอียดของระบบตรวจจับการบุกรุกในบทที่ 3 โดยในส่วนการตรวจจับการบุกรุกโดยการวิเคราะห์ล็อกไฟล์นั้น ได้มีงานวิจัยของ Stephen Hansen และ Todd Atkins เรื่อง Centralized System Monitoring With Swatch [Hansen and Atkins, 1993] โดยได้พัฒนาเครื่องมือในการวิเคราะห์ข้อมูลในล็อกไฟล์ที่ชื่อว่า SWATCH (The Simple

WATCHer) ซึ่งพัฒนาด้วยภาษา Perl เป็นโปรแกรมที่ถูกออกแบบมาเพื่อให้ค้นหาสิ่งผิดปกติที่เกิดขึ้นในล็อกไฟล์และแจ้งเตือนผู้ดูแลระบบด้วยวิธีต่าง ๆ เช่น ส่งอี-เมล์ ส่งเสียงบิ๊บ(beep)หรือสั่งให้โปรแกรมที่เขียนเตรียมไว้แล้ว สามารถทำงานได้ทั้งแบบ Real-Time และแบบ Batch และหลังจากนั้นก็ได้มีการพัฒนาเครื่องมือในการวิเคราะห์ล็อกไฟล์ที่มีลักษณะการทำงานตามแนวทางเดียวกันกับ SWATCH คือ Logsurfer ซึ่งพัฒนาด้วยภาษา C โดย Wolfgang Ley and Uwe Ellermanis [Ley and Ellerman, 2004] ซึ่งได้เพิ่มเติมความสามารถในการเก็บข้อมูลล็อกได้หลายบรรทัด ทำให้สามารถบันทึกข้อมูลการบุกรุกได้ตั้งแต่ต้นจนจบการบุกรุก และสามารถปรับเปลี่ยนกฎได้แบบ Dynamic นอกจากนี้ก็ยังมีเครื่องมือในการวิเคราะห์ล็อกไฟล์ตัวอื่น ๆ ที่ทำงานในโหมด Batch เพียงอย่างเดียว เช่น

- Logwatch [Bauer, 2003] พัฒนาโดยการใช้ภาษา Perl ทำการวิเคราะห์ข้อมูลในล็อกไฟล์ในช่วงเวลาที่กำหนดและผู้ใช้สามารถกำหนดช่วงเวลาการทำงานได้ผ่านโปรแกรม cron
- Logcheck [Rowland, 2003] พัฒนาด้วยใช้ Shell Script และภาษา C ซึ่งเริ่มต้นพัฒนาโดย Craig H. Rowland และปัจจุบันเป็นโปรแกรมประเภท open source

1.3 วัตถุประสงค์

1. พัฒนาแบบจำลองที่ทำการวิเคราะห์ข้อมูลของกิจกรรมของระบบและเหตุการณ์ที่ได้บันทึกไว้ เพื่อตรวจจับการบุกรุก พร้อมทั้งวิธีการรายงานแจ้งปัญหาไปยังผู้รับผิดชอบหรือผู้ดูแลระบบ
2. จัดหากลไกหรือเครื่องมือเพิ่มเติมในการบันทึกกิจกรรมต่าง ๆ ของระบบ เพื่อให้ได้ข้อมูลล็อกที่สามารถนำมาใช้ในการวิเคราะห์เพื่อตรวจจับการบุกรุก
3. ศึกษาวิเคราะห์และนำเสนอระดับของการบันทึกเหตุการณ์ของ syslog เพื่อให้ได้ข้อมูลที่มีประโยชน์กับการวิเคราะห์เพื่อตรวจจับการบุกรุกสูงสุดและใช้เนื้อที่ในการเก็บเหมาะสมที่สุด

1.4 ขอบเขตของการวิจัย

1. พัฒนาแบบจำลองในการวิเคราะห์ล็อกของกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบ พร้อมการแจ้งเตือน/รายงานปัญหาที่เกิดขึ้นไปยังผู้ดูแลระบบผ่านทางอีเมล์ การสั่งให้โปรแกรมอื่น ๆ ทำงานและการบันทึกลงไฟล์

2. ศึกษาวิเคราะห์และนำเสนอระดับของการบันทึกเหตุการณ์ของ syslog เพื่อให้ได้ข้อมูลที่มีประโยชน์กับการวิเคราะห์เพื่อตรวจจับการบุกรุกสูงสุดและใช้เนื้อที่ในการเก็บเหมาะสมที่สุด โดยทำการศึกษาภายใต้สภาวะแวดล้อมการทำงานของศูนย์คอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

1.5 ขั้นตอนและวิธีดำเนินการวิจัย

1. ศึกษาการทำงานของระบบตรวจสอบการบุกรุกต่าง ๆที่มีอยู่ในปัจจุบันและรวมทั้งข้อดีและข้อเสีย
2. ศึกษาข้อกำหนดในการบันทึกข้อมูลลงในล็อกไฟล์ โดยใช้ syslog และเก็บรวบรวมข้อมูลล็อกต่าง ๆที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ของศูนย์คอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ และจัดหากลไก/เครื่องมือที่เพิ่มความสามารถการบันทึกข้อมูลกิจกรรมเพื่อใช้ในการตรวจสอบการบุกรุก
3. ศึกษาและทดสอบการบุกรุกแบบต่าง ๆ บนเครือข่ายที่สร้างขึ้น แล้วเก็บรวบรวมร่องรอยการบุกรุก(intrusion signature) ที่เกิดขึ้นในล็อกไฟล์
4. พัฒนาโปรแกรมที่จะใช้ในการวิเคราะห์ข้อมูลในล็อกไฟล์ โดยใช้วิธีการเปรียบเทียบการจับคู่แบบรูป (pattern matching) ในล็อกไฟล์ กับร่องรอยการบุกรุกที่มีอยู่ รวมทั้งวิธีแจ้งเตือน/รายงานปัญหาที่เกิดขึ้นไปยังผู้ดูแลระบบ
5. ทดสอบโปรแกรม วิเคราะห์ผลที่ได้และรวบรวมผลการทดสอบ
6. สรุปผล จัดทำรายงานและเอกสารประกอบการใช้งาน

1.6 ระยะเวลาการดำเนินงาน

กรกฎาคม พ.ศ.2547 – กรกฎาคม 2548

แผนการดำเนินงาน

ขั้นตอน	ก.ค 47	ส.ค 47	ก.ย 47	ต.ค 47	พ.ย 47	ธ.ค 47	ม.ค 48	ก.พ 48	มี.ค 48	เม.ย 48	พ.ค 48	มิ.ย 48	ก.ค 48
1	◄——►												
2		◄——►											
3				◄——►									
4					◄——►								
5						◄——►							
6							◄——►						

1.7 เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย

ฮาร์ดแวร์

เครื่องไมโครคอมพิวเตอร์ 1 เครื่อง

ระบบปฏิบัติการ Linux RedHat เวอร์ชั่น 7.2 หรือสูงกว่า

ระบบปฏิบัติการ Windows98

หน่วยความจำอย่างน้อย 32 MB

ฮาร์ดดิสก์อย่างน้อย 1 GB

ซอฟต์แวร์

โปรแกรมการวิเคราะห์ Audit Log เช่น SWATCH, Logsurfer, logcheck เป็นต้น

โปรแกรมการทำ Audit Log เช่น syslog เป็นต้น

ตัวแปลภาษา C บน Unix

ตัวแปลภาษา Perl บน Unix

1.8 ประโยชน์ที่คาดว่าจะได้รับ

1. ข้อกำหนดในการบันทึกเหตุการณ์หรือกิจกรรมของระบบที่เหมาะสมกับสภาวะแวดล้อมของการใช้งานระบบของศูนย์คอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่
2. แบบจำลองในการตรวจสอบการบุกรุกและเหตุการณ์ความผิดปกติโดยใช้วิธีการวิเคราะห์ล็อก