ระบบตอบสนองเมื่อเกิดการละเมิดความปลอดภัย

Incident Response System

นายพรชัย กอประเสริฐถาวร

นายลาภบุญเอก กมลพิมุกต์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2548

ระบบตอบสนองเมื่อเกิดการละเมิดความปลอดภัย

Incident Response System

นายพรชัย กอประเสริฐถาวร

นายลาภบุญเอก คมลพิมุกต์

อาจารย์ที่ปรึกษา

อ.อัครเดช วัชระภูพงษ์

ผศ.ธนา หงษ์สุวรรณ

อ.ธนัญชัย ตรีภาค

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2548

ปริญญานิพนธ์ปีการศึกษา 2548

ภาควิชา วิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบตอบสนองเมื่อเกิดการละเมิดความปลอดภัย

Incident Response System

ผู้จัดทำ

1. นายพรชัย กอประเสริฐถาวร รหัสประจำตัว 45010495
2. นายลาภบุญเอก กมลพิมุกต์ รหัสประจำตัว 45010496

_____ อาจารย์ที่ปรึกษา

(อาจารย์อัครเดช วัชระภูพงษ์)

_____ อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ธนา หงษ์สุวรรณ)

_____ อาจารย์ที่ปรึกษา

(อาจารย์ธนัญชัย ตรีภาค)

ระบบตอบสนองเมื่อเกิดการละเมิดความปลอดภัย

นายพรชัย กอประเสริฐถาวร	45010495
นายลาภบุญเอก กมลพิมุกต์	45010496
อาจารย์อัครเดช วัชระภูพงษ์	อาจารย์ที่ปรึกษา
ผศ.ธนา หงษ์สุวรรณ	อาจารย์ที่ปรึกษาร่วม
อาจารย์ธนัญชัย ตรีภาค	อาจารย์ที่ปรึกษาร่วม
ปีการศึกษา 2548	

บทคัดย่อ

ถึงแม้ระบบรักษาความปลอดภัยทางคอมพิวเตอร์จะดีเลิศเพียงใด ก็ยังมีโอกาสเกิดการละเมิดได้ ฉะนั้นระบบรักษาความปลอดภัยทางคอมพิวเตอร์ที่ดีจึงต้องเตรียมความพร้อมต่อเหตุการณ์ดังกล่าว ทั้งก่อนหน้า ระหว่าง และหลังเกิดการละเมิดความปลอดภัย เพื่อทราบได้ว่าเกิดการละเมิดขึ้นแล้ว การทำอะไรไปบ้าง กระทบต่อสิ่งใดบ้าง และจะทำการกู้คืนระบบให้สามารถทำงานเช่นเดิมได้อย่างไร รวมถึงการรวบรวมหลักฐานเพื่อเอาผิดต่อผู้ละเมิดความปลอดภัย

โครงงานนี้เป็นโครงงานใหม่ที่มุ่งศึกษาแนวทางการตอบสนองเมื่อเกิดการละเมิดความปลอดภัยในทุกช่วงเหตุการณ์ โดยเน้นระบบปฏิบัติการยูนิกซ์

INCIDENT RESPONSE SYSTEM

Mr. Pornchai Korpraserttaworn	45010495
Mr. Larpboonek Kamolpimook	45010496
Mr. Akkradach Watcharapupong	Advisor
Asst. Prof. Thana Hongsuwan	Co-Advisor
Mr. Tanunchai Tripak	Co-Advisor

Academic Year 2005

ABSTACT

Eventhough the computer security system is now much more powerful than the old days. It cannot be considered the perfect system anyway. Since the problems still exist, the reliable security system has to be ready for the unexpected events to occur. The system should be able to handle those at the time intrusion taking place as well as before and after the affairs in order to be able to make an incident response to such an event. The incident response mentioned includes knowing what the intruder has done to the system, detecting the effects to the system, recovering the system and gathering the information due to the legal issue.

This project purposes presenting a new method in computer security aiming at the effective way to response when there is an intrusion. All is done under UNIX environment.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้จะไม่สามารถเสร็จสมบูรณ์ได้ถ้าไม่ได้รับคำแนะนำ คำเตือน ทั้งหลายจากอาจารย์อัครเดช วัชระภูพงษ์ ผู้ช่วยศาสตราจารย์ธนา หงษ์สุวรรณ และอาจารย์ธนัญชัย ตรีภาค คณะผู้จัดทำขอขอบพระคุณอย่างยิ่งสำหรับทุกสิ่งที่อย่างที่ได้รับจากท่านทั้งสาม

นอกจากนี้ขอขอบคุณสถาบัน ภาควิชาวิศวกรรมคอมพิวเตอร์ และห้องวิจัยและพัฒนาการรักษาความปลอดภัยข้อมูล (ISAG) ที่ได้เอื้อเฟื้อสถานที่ให้คณะผู้จัดทำได้ทำการวิจัยและศึกษา ขอขอบคุณเพื่อนๆ พี่ ๆ ห้อง ISAG ที่ได้ให้คำแนะนำและให้ความช่วยเหลือในยามที่ผู้จัดทำพบกับปัญหาได้ดีเสมอมา

สุดท้ายต้องขอขอบคุณบิดา มารดาที่ได้ให้กำเนิด คอยสั่งสอน ให้การสนับสนุนการศึกษา และเป็นกำลังใจในการศึกษาเล่าเรียนเสมอ นับเป็นพระคุณอย่างยิ่ง

นายพรชัย กอประเสริฐถาวร
นายลาภบุญเอก กมลพิมุกต์

สารบัญ

หน้า

สารบัญ

หน้า

สารบัญตาราง

สารบัญรูปภาพ

สารบัญรูปภาพ (ต่อ)

บทที่ 1
บทนำ

1.1 บทนำ

การมีเครื่องมือที่ใช้ป้องกันการละเมิดความปลอดภัยจากผู้ประสงค์ร้ายที่ดีเพียงใด ก็ยังไม่สามารถที่จะป้องกันได้สมบูรณ์ร้อยเปอร์เซ็นต์ เนื่องจากไม่มีโปรแกรมใดที่ไม่มีช่องโหว่ ทำให้ระบบทุกระบบมีโอกาสที่จะถูกละเมิดสิทธิ์หรือละเมิดความปลอดภัยได้เสมอ จึงจำเป็นที่จะต้องมีการเตรียมความพร้อมที่จะรับมือเมื่อมีการละเมิดความปลอดภัยเกิดขึ้น

โปรแกรมต้นแบบที่สร้างขึ้นนี้ เป็นโปรแกรมที่ใช้เพื่อการตอบสนองหลังจากที่ตรวจพบว่ามีการละเมิดความปลอดภัยต่อระบบ โดยในการตัดสินใจขั้นแรกจะใช้โปรแกรม Snort-Inline ซึ่งสามารถทำการตรวจสอบและแยกแยะระหว่างผู้ใช้งานทั่วไปและผู้ละเมิดความปลอดภัยได้ในระดับหนึ่ง หากผู้ละเมิดความปลอดภัยสามารถหลุดรอดจากโปรแกรม Snort-Inline มาได้ก็จะถูกบันทึกพฤติกรรม การใช้งานทุกอย่างๆ พร้อมๆ กับผู้ใช้งานปกติทั่วไปโดยใช้ Host-base IDS โดยข้อมูลที่จัดเก็บทั้งหมดจะถูกแยกไปจัดเก็บใน Log Server เพื่อเป็นการป้องกันไม่ให้ผู้ละเมิดความปลอดภัยทำการเปลี่ยนแปลงหรือลบข้อมูลที่ได้บันทึกพฤติกรรมไว้ หลังจากนั้นข้อมูลเหล่านั้นจะถูกนำไปวิเคราะห์เพื่อตรวจจับการกระทำที่เป็นการละเมิดความปลอดภัย ทำการวิเคราะห์ความเสี่ยงต่อระบบที่อาจเกิดขึ้น หากตรวจสอบพบการละเมิดความปลอดภัย ระบบจะทำการแจ้งเตือนไปยังผู้ดูแลระบบและทำการตอบสนองต่อการละเมิดความปลอดภัยนั้นๆ

ทั้งนี้ระบบสามารถทำการเก็บ Snapshot ของระบบตามที่ผู้ดูแลระบบกำหนดไว้สำหรับการกู้คืนระบบในกรณีที่ผู้ละเมิดความปลอดภัยทำความเสียหายต่อระบบในระดับที่ไม่สามารถทำการแก้ไขได้

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อศึกษาแนวทางการตอบสนองเมื่อเกิดการละเมิดความปลอดภัย

1.2.2 เพื่อสร้างต้นแบบและจัดทำเอกสารเกี่ยวกับระบบตอบสนองเมื่อเกิดการละเมิดความปลอดภัย

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 ได้รับความรู้ ความเข้าใจเกี่ยวกับกระบวนการตรวจจับผู้บุกรุก

1.3.2 ได้รับความรู้ ความเข้าใจเกี่ยวกับแนวทางในการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย

1.3.3 ได้ต้นแบบที่สามารถตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยแบบต่างๆ ได้อย่างเหมาะสม

1.4 ขอบเขตของโครงงาน

ในการพัฒนาระบบตอบสนองเมื่อเกิดการละเมิดความปลอดภัยมีขอบเขตในการพัฒนาระบบโดยรวมดังนี้คือ

1) พัฒนาระบบตอบสนองเมื่อเกิดการละเมิดความปลอดภัยบนระบบปฏิบัติการลินุกซ์ debian core 2.6.11

2) ถ้าระบบเกิดความเสียหายมากเนื่องจากถูกละเมิดความปลอดภัยจะไม่สามารถทำการ recovery และ ปิดช่องโหว่ได้

3) ระบบที่พัฒนาขึ้นนี้เป็นการใช้งานกับระบบเครือข่ายที่ความเร็ว 100 Mbps

ทั้งนี้ในการพัฒนาระบบจะใช้เวลาทั้งหมด 2 ภาคการศึกษาโดยมีขอบเขตการศึกษาหรือพัฒนาในแต่ละภาคการศึกษาดังนี้คือ

- ภาคการศึกษาที่ 1 จะเป็นการศึกษาและทดสอบเกี่ยวกับโปรแกรมที่จะนำมาใช้ในการสร้างระบบซึ่งประกอบไปด้วยโปรแกรมสำหรับตรวจจับการบุกรุกทั้ง Network-base IDS และ Host-base IDS การ Forensic
- ภาคการศึกษาที่ 2 จะเป็นการศึกษาเกี่ยวกับการปรับแต่งให้ Network-base IDS และ Host-base IDS ทำงานอย่างมีประสิทธิภาพมากขึ้น และเขียนโปรแกรมสำหรับทำการวิเคราะห์ข้อมูลที่ได้ทั้งหมดเพื่อตรวจสอบหาการบุกรุกหรือการละเมิดความปลอดภัย

1.5 เนื้อหาของรายงาน

เนื้อหาของรายงานฉบับนี้ประกอบด้วยส่วนต่างๆ คือ ส่วนที่หนึ่งเป็นทฤษฎีซึ่งจะนำเสนอทฤษฎีต่างๆ ที่จำเป็นในการสร้างระบบต้นแบบที่ได้ทำการศึกษา ส่วนที่สองเป็นการออกแบบทั้งฮาร์ดแวร์และซอฟท์แวร์ ส่วนที่สามเป็นการทดสอบระบบที่ได้สร้างขึ้น พร้อมการจำลองการใช้งานระบบในสถานการณ์จริงพร้อมผลการทดสอบ ส่วนสุดท้ายจะเป็นการวิเคราะห์ผลการทดสอบแล้วรวบรวมเป็นข้อสรุป

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 บทนำ

ในการที่จะสร้างระบบต้นแบบซึ่งเป็นระบบตอบสนองต่อผู้ละเมิดความปลอดภัย การศึกษาทฤษฎีที่เกี่ยวข้องเป็นเรื่องที่สำคัญเป็นอย่างยิ่งโดยเฉพาะทฤษฎีในเรื่องของขั้นตอน แนวความคิดในการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย ทฤษฎีการตรวจจับผู้บุกรุกหรือผู้ละเมิดความปลอดภัย และการใช้โปรแกรมต่างๆ ในการเก็บข้อมูลเพื่อนำไปใช้ในการวิเคราะห์ต่อไป

2.2 ทฤษฎีการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย (Incident Response)

2.2.1 นิยามและความหมาย

Incident หมายถึง เหตุการณ์ที่เป็นภัยคุกคามต่อความปลอดภัยของระบบคอมพิวเตอร์และระบบเครือข่าย เช่น คอมพิวเตอร์หรือระบบเครือข่ายหยุดทำงาน การสั่งให้โปรแกรมที่ประสงค์ร้าย (malicious code) ทำงาน การใช้งาน Account ของผู้อื่นโดยไม่ได้รับอนุญาต

ทั้งนี้เหตุการณ์ที่เป็นภัยคุกคามต่อความปลอดภัยของระบบคอมพิวเตอร์และระบบเครือข่าย จะไม่รวมถึงเหตุการณ์ที่เป็นภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ ไฟตก เป็นต้น

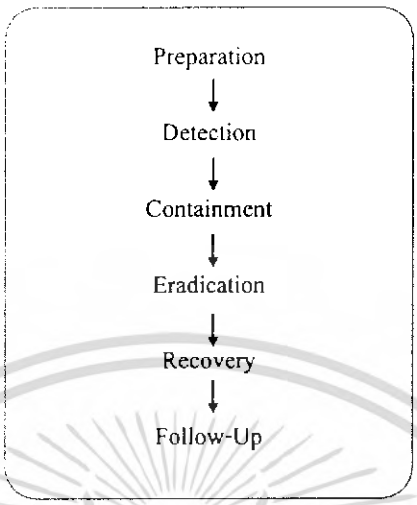
Incident Response หมายถึง การดำเนินการกับเหตุการณ์ละเมิดความปลอดภัยที่เกิดขึ้น การดำเนินการนี้มีจุดประสงค์เพื่อกำจัดหรือลดผลกระทบที่อาจเกิดขึ้นกับระบบ

2.2.2 เป้าหมายหรือวัตถุประสงค์ของการรับมือและการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย

1. เพื่อหาข้อมูลว่าเหตุการณ์นั้นเกิดขึ้นได้อย่างไร
2. หาวิธีป้องกันไม่ให้เกิดเหตุการณ์ประเภทนี้อีก
3. ป้องกันไม่ให้เหตุการณ์ลุกลามจนนำมาสู่ความเสียหายต่อระบบ
4. ประเมินผลกระทบและความเสียหายจากเหตุการณ์
5. ฟื้นฟูระบบจากเหตุการณ์
6. แก้ไขนโยบายและระเบียบปฏิบัติให้เหมาะสมขึ้น
7. ค้นหาผู้ก่อเหตุ (หากเหมาะสมและเป็นไปได้)

2.2.3 การตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย

แนวคิดในการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย 6 ขั้นตอนดังนี้คือ



รูปที่ 2.1 ขั้นตอนการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย

2.2.4 ขั้นตอนที่ 1 การเตรียมการ (Preparation)

ขั้นตอนการเตรียมการเป็นการเตรียมความพร้อมเพื่อที่จะรับมือกับเหตุการณ์ที่จะเกิดขึ้น ขั้นตอนนี้ถือได้ว่าเป็นขั้นตอนที่สำคัญ เป็นขั้นตอนที่มีความซับซ้อนและต้องใช้เวลาในการตระเตรียมสิ่งที่จำเป็น ในขั้นตอนการเตรียมการประกอบด้วย 4 กระบวนการพื้นฐานดังนี้คือ

1) ติดตั้งระบบป้องกันและควบคุมต่อเหตุการณ์ที่อาจเกิดขึ้น
2) เตรียมแผนการปฏิบัติที่จะดำเนินการกับเหตุการณ์ที่จะเกิดขึ้นอย่างมีประสิทธิภาพ

แผนการปฏิบัติสำหรับการดำเนินการกับเหตุการณ์ละเมิดความปลอดภัยควรมีวิธีการอย่างน้อยดังต่อไปนี้

- วางแผนการและระบุขั้นตอนการดำเนินการต่อเหตุการณ์ละเมิดความปลอดภัยภายใต้สภาพแวดล้อมที่กำหนด
- บุคคลที่ควรจะต้องแจ้งหรือติดต่อเมื่อเกิดเหตุการณ์ละเมิดความปลอดภัยขึ้น
- ระบุประเภทของข้อมูลที่สามารถเปิดเผยและข้อมูลที่ไม่สามารถเปิดเผยต่อบุคคลภายนอกได้
- จัดลำดับความสำคัญของขั้นตอนการตอบสนองเมื่อเกิดการละเมิดความปลอดภัย
- ระบุหน้าที่และบทบาทของแต่ละบุคคลที่เป็นส่วนหนึ่งของการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย

- จัดทำเอกสารที่ระบุถึงระดับความเสี่ยงที่สามารถยอมรับได้ และเอกสารนโยบายด้านความปลอดภัยขององค์กรเพื่อใช้เป็นแนวทางในการดำเนินการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย

3) จัดหาทรัพยากรทุกอย่างที่จำเป็นทั้งทรัพยากรทางด้านวัตถุ และทรัพยากรบุคคล

ทรัพยากรในที่นี้เป็นทุกสิ่งที่จำเป็นต้องใช้เพื่อความสำเร็จของการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยไม่ว่าจะเป็นฮาร์ดแวร์ ซอฟแวร์ หรือแม้แต่การฝึกอบรม

สำหรับซอฟแวร์ที่จำเป็นต้องใช้ตัวอย่างเช่น ซอฟแวร์ตรวจจับผู้บุกรุก (Intrusion detection software) เครื่องมือในการทำรีเวิร์สเอ็นจิเนียริง (Reverse engineering tool) ซอฟแวร์สำหรับการสืบค้นและวิเคราะห์ (Forensic analysis software) ซอฟแวร์ระบบฐานข้อมูล (Database server software) เป็นต้น

4) จัดเตรียมโครงสร้างพื้นฐานที่สนับสนุนการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

การที่จะตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยได้อย่างเสร็จสมบูรณ์จะต้องมีการจัดเตรียมโครงสร้างพื้นฐานขององค์กรที่สนับสนุนกระบวนการ โดยโครงสร้างพื้นฐานเหล่านั้นจะต้องมีความเป็นเอกภาพสอดคล้องกันทั้งองค์กร เช่น การใช้ระบบป้องกันและควบคุมที่เหมาะสมกับระบบ อุปกรณ์เครือข่าย ระบบฐานข้อมูล หรือแม้แต่โปรแกรมต่างๆ การแบ่งหน้าที่ให้กับแต่ละบุคคลที่เกี่ยวข้องกับการดำเนินการ การดูแลทรัพยากรที่จำเป็นไม่ว่าจะเป็นฮาร์ดแวร์หรือซอฟท์แวร์ให้อยู่ในสภาพที่ใช้งานได้ การเตรียมคอนแทกท์ลิสต์สำหรับติดต่อบุคคลที่เกี่ยวข้อง การเก็บหลักฐาน และการศึกษาหรือเตรียมการด้านกฎหมาย เป็นต้น

นอกจากนี้ส่วนที่สำคัญของการเตรียมการบางอย่างอาจเป็นหน้าที่ของผู้ดูแลระบบเองที่จะต้องจัดการดูแลอย่างมีประสิทธิภาพโดยอาจมีวิธีการดังต่อไปนี้

- ใช้นโยบายหรือกฎในการตั้งรหัสผ่านต่างๆ
- ลบบัญชีผู้ใช้ที่ไม่ได้ใช้งานทั้งหมดหรือระงับสิทธิ์การใช้งาน
- ติดตั้งเครื่องมือหรือโปรแกรมที่จำเป็นต้องใช้ เช่น เครื่องมือในการตรวจจับการบุกรุก เครื่องมือสำหรับการสืบหลักฐานหรือร่องรอยของการละเมิดความปลอดภัย
- เก็บรักษาล็อกไฟล์ของระบบ
- ลงส่วนเพิ่มเติมของโปรแกรม (patch) เพื่อลดจุดอ่อนหรือช่องโหว่ของโปรแกรมต่างๆ ในระบบ
- ตรวจสอบความถูกต้อง (integrity) ของระบบไฟล์
- สำรองข้อมูลของระบบเท่าที่จำเป็น
- สำรวจสิ่งที่น่าสงสัยที่เกิดขึ้นในระบบ ซึ่งโดยปกติแล้วจะถือเป็น เหตุการณ์ที่ไม่ปกติ

2.2.5 ขั้นตอนที่ 2 การตรวจสอบ (Detection)

การตรวจสอบคือการพยายามตรวจหาความผิดปกติหรือตรวจหาเหตุการณ์ที่อาจเป็นการละเมิดความปลอดภัยต่อระบบ โดยในการตรวจสอบนี้มักใช้เครื่องมือหรือโปรแกรมประเภทระบบตรวจจับการบุกรุก (Intrusion Detection System : IDS) เข้ามาช่วยในการตรวจสอบ โดยหลักๆ แล้วโปรแกรมเหล่านี้อาจแบ่งเป็น Host-base IDS และ Network-base IDS ซึ่งมีคุณสมบัติในการทำงานต่างกัน

เหตุการณ์บางประเภทไม่จำเป็นต้องใช้โปรแกรมในการตรวจสอบ แต่อาจใช้วิธีการสังเกตจากอาการและข้อมูลที่อยู่ในระบบ เช่น ล็อกไฟล์ของระบบ ล็อกไฟล์ของไฟร์วอล ตัวอย่างเหตุการณ์เช่น

- การพยายามทำการล็อกอินเข้าสู่ระบบและไม่สามารถเข้าสู่ระบบได้หลายๆ ครั้ง
- การล็อกอินเข้าสู่ระบบด้วยบัญชีผู้ใช้ (Account) ที่ถูกระงับสิทธิ์หรือบัญชีผู้ใช้ที่ระบบสร้างให้เป็นค่าเริ่มต้น ผู้ดูแลระบบสามารถตรวจสอบการล็อกอินเข้าสู่ระบบของผู้ใช้งานและควรจะสังเกตการใช้งานที่น่าสงสัยเช่น การล็อกอินเข้าระบบในช่วงเวลาที่ไม่ได้กำหนดการใช้งาน
- กิจกรรมบางอย่างที่เกิดขึ้นในช่วงเวลาที่ไม่มีการทำงาน ตัวอย่างเช่น การล็อกอินเข้าสู่ระบบในช่วงเวลาที่ไม่มีใครทำงานหรือใช้ระบบแล้ว
- การเกิดบัญชีผู้ใช้ใหม่โดยที่ไม่ได้เป็นการสร้างจากผู้ดูแลระบบ
- การมีไฟล์หรือโปรแกรมที่แปลกปลอมในระบบ
- การเปลี่ยนแปลงสิทธิ์การใช้งานของไดเรกทอรีหรือไฟล์ต่างๆ
- การเปลี่ยนหน้าของเว็บเพจที่เก็บอยู่ในเครื่องให้บริการเว็บ
- การปรากฏรูปอนาจารในระบบ
- การใช้คำสั่งที่ไม่เกี่ยวข้องกับงานที่ทำของผู้ใช้นั้นๆ
- การเกิดช่องว่างในล็อกไฟล์เนื่องจากโดนลบข้อมูล
- การเปลี่ยนแปลงค่าการทำงานของระบบ DNS หรือการทำงานของเราเตอร์ หรือการเปลี่ยนกฎของไฟล์วอล
- ประสิทธิภาพการทำงานของระบบลดลงอย่างผิดปกติ
- ระบบไม่สามารถให้บริการได้ (system crash)

2.2.6 ขั้นตอนที่ 3 การยับยั้ง (Containment)

จุดมุ่งหมายของขั้นตอนนี้คือ การยับยั้งหรือหยุดการโจมตีและการทำความเสียหาย ขั้นตอนนี้จะเริ่มขึ้นเมื่อมีการตรวจสอบพบเหตุการณ์ละเมิดความปลอดภัยแล้ว

หลังจากได้รับการยืนยันแล้วว่ามีการละเมิดความปลอดภัยเกิดขึ้นก็ควรจะมีการดำเนินการกับสิ่งที่เกิดขึ้นอย่างทันท่วงที การดำเนินการที่สามารถกระทำได้อย่างรวดเร็วและไม่ยุ่งยากคือ การยับยั้ง ตัวอย่างเช่น การระงับสิทธิ์การล็อกอินของบัญชีผู้ใช้ชั่วคราวหากตรวจสอบพบว่ามีการพยายามจะล็อกอินเข้าระบบด้วยรหัสผ่านที่ผิดหลายครั้งติดต่อกัน

สิ่งสำคัญสำหรับการยับยั้งคือ การทำให้การยับยั้งนั้นมีความเข้มแข็ง เพราะมีหลายเหตุการณ์ที่สามารถหลุดรอดออกไปได้อย่างรวดเร็ว ซึ่งอาจทำความเสียหายต่อระบบ เช่น กา กระจายตัวของโค๊ดหนอน ผู้ดูแลจะต้องจำกัดหรือยับยั้งการแพร่กระจายของโค๊ดหนอนในเครือข่ายให้เร็วที่สุดเท่าที่จะเป็นไปได้

ก่อนที่จะมีการกระทำหรือดำเนินการใดๆ ในขั้นตอนนี้จะต้องมีการตัดสินใจก่อนว่าจะเลือกใช้วิธีการใดระหว่างการยับยั้งเหตุการณ์ในทันที หรือปล่อยให้ผู้ละเมิดความปลอดภัยดำเนินการต่อไปเพื่อที่ผู้ดูแลระบบสามารถทำการเก็บรวบรวมข้อมูลหรือหลักฐานต่างๆ ซึ่งอาจสามารถนำไปใช้ในการดำเนินการทางกฎหมายได้ แต่ทั้งนี้การที่จะตัดสินใจเลือกวิธีการใดจะต้องพิจารณาถึงความเสี่ยงที่ได้รับ ซึ่งแต่ละองค์กรมีระดับความเสี่ยงที่ยอมรับได้ต่างกัน หรือระดับความสำคัญหรือความลับของข้อมูลต่างกัน

สิ่งสำคัญพื้นฐานอีกประการของการยับยั้งคือ การตรวจสอบว่ามีการโจมตีใดบ้าง มีการติดตั้งโปรแกรมหรือโค๊ดที่ไม่ประสงค์ดีอะไรบ้าง มีการดิดตั้งโปรแกรมที่สร้างช่องทางสำหรับใช้ในการเข้าระบบอย่างไม่ถูกต้อง หลังจากตรวจสอบพบแล้วก็จะต้องพิจารณาต่อไปว่าจะดำเนินการอย่างไรกับสิ่งที่ตรวจสอบพบเช่น ยังไม่ทำการลบหรือถอนออกจากระบบเนื่องจากต้องการเก็บไว้เป็นหลักฐานสำหรับดำเนินการทางด้านกฎหมายหรือ ทำการลบออกจากระบบทันทีและทำการเปลี่ยนรหัสผ่านของผู้ดูแลระบบเพื่อป้องกันมิให้ผู้โจมตีที่อาจรู้รหัสผ่านทำการเปลี่ยนรหัสผ่านนั้น

2.2.7 ขั้นตอนที่ 4 การกำจัด (Eradication)

จุดมุ่งหมายของขั้นตอนนี้คือ เพื่อทำการกำจัดสิ่งที่เป็นต้นเหตุของการละเมิดความปลอดภัย ในขั้นตอนนี้อาจใช้โปรแกรมเข้ามาช่วยได้เช่น การกำจัดไวรัสที่แพร่กระจายในระบบด้วยโปรแกรมจำพวก antivirus หากมีโปรแกรมจำพวกม้าโทรจัน โปรแกรมหรือโค้ดที่สร้างช่องทางสำหรับการเข้าระบบซึ่งควรจะถูกกำจัดตั้งแต่ขั้นตอนการจำกัดขอบเขตหลงเหลืออยู่ในระบบ จะต้องทำการกำจัดในขั้นตอนนี้ ในบางกรณีหากไม่สามารถกำจัดโปรแกรมหรือโค๊ดที่ไม่ประสงค์ดีเหล่านี้ได้อาจต้องทำการฟอร์แมท (Format) ฮาร์ดดิสก์ใหม่ซึ่งจะต้องทำการสำรองข้อมูลทั้งหมดไว้ก่อน สิ่งที่น่าสนใจคือ จะต้องแน่ใจว่าข้อมูลที่สำรองไว้นั้นปราศจากไวรัส หรือโปรแกรมที่ไม่ประสงค์ดีก่อนที่จะนำข้อมูลนั้นกลับมาใช้งาน

ตัวอย่างวิธีการในการกำจัดสิ่งที่ทำให้เกิดช่องโหว่ต่อระบบ หรือโปรแกรมที่ทำอันตรายต่อระบบปฏิบัติการยูนิกซ์ หรือลินุกซ์ มีดังนี้คือ

1) ตรวจสอบความผิดปกติในไฟล์ที่มีนามสกุลเป็น .forward
2) ใช้คำสั่ง ps เพื่อตรวจสอบรายชื่อโปรเซสที่กำลังทำงานและตรวจหาโปรเซสที่ผิดปกติหรือน่าสงสัย
3) ตรวจสอบการเปลี่ยนแปลงในไฟล์เหล่านี้คือ
   - /etc/dfs/dfstab (หรือ /etc/exports)
   - .login
   - .logout
   - .profile
   - /etc/profile
   - .cshc
   - ทุกๆ ไฟล์ที่อยู่ในไดเรกทอรี /etc/rc
   - .rhosts
   - /etc/hosts.equiv
4) ตรวจสอบการตั้งค่าการทำงานหรือการแก้ไขโปรแกรมให้ทำงานผิดปกติไปจากเดิมในโปรแกรมหรือไฟล์ดังต่อไปนี้
   - netstat
   - ls
   - sum
   - find
   - diff
   - /etc/nsswitch.conf
   - /etc/resolv.conf
   - /var/spool/cron
   - /var/spool/cron/crontabs
   - kerb.conf
5) ตรวจสอบวันเวลาของการแก้ไขไฟล์ด้วยคำสั่ง ls –lac
6) ตรวจสอบ suid ของโปรแกรมโดยใช้คำสั่ง

   find / -type f –perm -4000 –ls หรือ

   find / -type f –perm -4000 –print
7) ตรวจสอบการแก้ไขเปลี่ยนแปลงไฟล์ต่อไปนี้
   - /etc/passwd
   - shadow password file
   - /etc/group
   - yppasswd
8) ตรวจสอบการเพิ่มสิทธิ์ที่ไม่ได้รับการอนุญาตในไฟล์ .rhosts และไฟล์ /etc/hosts.equiv โดยใช้คำสั่งต่อไปนี้

   find / -name .rhosts –ls –o –name .forward –ls

   find / -name .rhosts –print –o –name .forward -print

9) ตรวจสอบการเปิดบริการ (service) ที่แปลกปลอมในไฟล์ต่อไปนี้ คือ

- /etc/inetd.conf
- /etc/inittab
- /etc/services
- /etc/hosts.allow
- /etc/hosts.deny

10) ค้นหาไฟล์ที่อาจถูกสร้างขึ้นในช่วงเวลาที่ระบบถูกโจมตีโดยใช้คำสั่งดังนี้

find / -ctime -1 –ls หรือ

find / -ctime -1 –print

หากตรวจสอบพบไฟล์ที่น่าสงสัยอาจทำการลบได้ตามความจำเป็น

11) ค้นหาไฟล์ที่อาจถูกเปลี่ยนแปลงในช่วงเวลาที่ระบบถูกโจมตีโดยใช้คำสั่งดังนี้

find / -mtime -1 –ls หรือ

find / -mtime -1 –print

หากตรวจสอบพบไฟล์ที่น่าสงสัยอาจดำเนินการใดๆได้ตามความจำเป็น

2.2.8 ขั้นตอนที่ 5 การกู้คืนระบบ (Recovery)

จุดมุ่งหมายของขั้นตอนนี้คือ เพื่อทำให้ระบบที่ถูกละเมิดความปลอดภัยกลับมาใช้งานได้อย่างเป็นปกติ ความจำเป็นหรือระดับของการกู้คืนระบบนั้นแตกต่างกันตามแต่ละองค์กร เนื่องจากแต่ละองค์กรอาจมีข้อมูลที่มีความสำคัญไม่เท่ากัน องค์กรใดที่ไม่จำเป็นต้องรักษาข้อมูลหรือข้อมูลที่สูญเสียไปอาจไม่มีผลกระทบต่อองค์กรมากนักก็อาจจะใช้วิธีการฟื้นคืนระบบ (restore) ใหม่ทั้งหมด ทั้งนี้วิธีการนี้จะต้องแน่ใจว่าข้อมูลที่สูญเสียไปนั้นจะไม่นำมาซึ่งความเสียหายต่อองค์กร นอกจากนี้อาจใช้วิธีการฟื้นคืนระบบกลับไปยังช่วงเวลาก่อนที่ระบบจะถูกละเมิดความปลอดภัยจนเกิดความเสียหายซึ่งวิธีนี้จะต้องอาศัยกลไกในการสำรองข้อมูลแบบอินครีเมนทอล (Incremental backup) ข้อดีของวิธีการนี้คือ ช่วยลดจำนวนข้อมูลที่สูญเสียไปและบรรเทาความเสียหายอันเนื่องมาจากการสูญเสียข้อมูลนั้น

สิ่งที่สำคัญที่อาจต้องนำมาพิจารณาคือ การฟื้นคืนระบบนั้นหากเป็นระบบที่มีความซับซ้อนมากอาจต้องใช้เวลาในการฟื้นคืนระบบมาก ดังนั้นการที่จะเลือกใช้วิธีการกู้คืนระบบแบบใดควรจะต้องพิจารณาตามนโยบายขององค์กร

2.2.9 ขั้นตอนที่ 6 การติดตามผล (Follow – up)

ในขั้นตอนนี้ถือเป็นขั้นตอนสุดท้ายซึ่งมีจุดมุ่งหมายเพื่อรวบรวมข้อมูลที่เกี่ยวข้องกับเหตุการณ์ละเมิดความปลอดภัยที่เกิดขึ้น และแก้ไขระบบในส่วนที่เคยถูกละเมิดความปลอดภัย

ปรับปรุงให้มีความปลอดภัยมากขึ้นเพื่อป้องกันเหตุการณ์เดิมที่อาจเกิดขึ้นอีกครั้ง บางครั้งการติดตามผลอาจถูกมองข้ามไปทำให้การตอบสนองต่อการละเมิดความปลอดภัยนั้นไม่สมบูรณ์

ข้อมูลที่จะต้องทำการรวบรวมในขั้นตอนนี้ประกอบไปด้วยข้อมูลที่บ่งบอกถึง

- เกิดเหตุการณ์อะไรขึ้นกับระบบ
- ใครเป็นสาเหตุของเหตุการณ์นั้น
- เหตุการณ์นั้นทำให้ระบบเกิดการเปลี่ยนแปลงอย่างไร
- เหตุการณ์นั้นทำความเสียหายกับส่วนใดของระบบ

2.3 รูปแบบและพฤติกรรมของผู้บุกรุก

พฤติกรรมทั่วไปของผู้บุกรุก

อันดับแรกผู้บุกรุกพยายามหาข้อมูลของเครื่องเป้าหมายให้ได้มากที่สุดเท่าที่จะหาได้ ผู้บุกรุกอาจเข้าระบบโดยได้สิทธิ์ของผู้ใช้ปกติ แล้วเรียกใช้โปรแกรม เช่น whois (เป็นโปรแกรมที่ใช้หาข้อมูลว่ามีใครใช้งานอยู่ในระบบบ้าง) ดูโดเมนเนมของระบบ และค้นหาค่ากำหนดของเครื่องที่ทำงานอยู่ในเน็ตเวิร์ก เช่น ชื่อเครื่อง รุ่นของระบบปฏิบัติการ ชื่อผู้ใช้ทั้งหมดในระบบ

สำหรับภายในระบบ ผู้บุกรุกมักสแกนข้อมูลต่างๆ เพื่อหาช่องโหว่ เช่น เข้าไปตรวจสอบการใช้ CGI ในเว็บเพจ หรือใช้โปรแกรม ping หรือโปรแกรมที่ใช้โพรโตคอลคล้ายกัน เช่น SNMP ในการค้นหาว่ามีเครื่องใดที่ยังเปิดให้บริการ หรือสแกนพอร์ตที่มีเซอร์วิสที่ใช้โพรโตคอล TCP หรือ UDP เพื่อค้นหาว่ามีเซอร์วิสอะไรที่เปิดให้บริการบ้าง ซึ่งข้อมูลเหล่านี้ใช้สำหรับการบุกรุกระบบ

หลังจากนั้น เมื่อผู้บุกรุกพยายามล้ำเส้นเข้ามาในเครื่องเป้าหมาย โดยอาจใช้ช่องโหว่ในสคริปต์ซีจีไอ (CGI script) แล้วส่งคำสั่งหรือให้เรียกโปรแกรมใดๆ ส่งค่าไปเป็นอินพุตโดยผ่านทางคำสั่งเชลล์ หรือผู้บุกรุกพยายามหารหัสผ่านที่เดาได้ง่ายๆ หรือการเข้าใช้งานระบบโดยล็อกอินที่ไม่มีรหัสผ่าน เมื่อผู้บุกรุกสามารถเข้าไปเป็นผู้ใช้ทั่วไปแล้วก็สามารถหาช่องทางที่จะทำให้ได้สิทธิ์ของผู้ดูแลระบบ

เมื่อผู้บุกรุกได้ข้อมูลที่ต้องการหรือได้ใช้ทรัพยากรใดๆ แล้ว สิ่งที่ทำต่อไปคือ การพยายามกลบเกลื่อนหลักฐานทั้งหมดในการบุกรุก หรือสร้างช่องทางให้สามารถกลับไปใช้ระบบนั้นๆ อีก โดยการสร้างประตูหลัง (Back door) หรือทำความเสียหายให้แก่ระบบนั้นโดยการวางโปรแกรมของข้อมูลในระบบ เพื่อตรวจสอบว่ามีการเปลี่ยนแปลงใดๆ ในไฟล์หรือองค์ประกอบอื่นในระบบหรือไม่ อีกพฤติกรรมหนึ่งของผู้บุกรุกคือ เมื่อบุกรุกระบบใดระบบหนึ่งได้ จะใช้เป็นช่องทางในการบุกรุกระบบอื่นๆ ต่อไป

ประเภทของการบุกรุก

การบุกรุกเข้าสู่ระบบแบ่งออกเป็นประเภทหลักๆ 3 ประเภทดังนี้

1. การบุกรุกทางกายภาพ (Physical Intrusion) ผู้บุกรุกพยายามบุกรุกที่เครื่องคอมพิวเตอร์โดยตรง โดยอาจมาใช้สิทธิ์พิเศษจากการทำงานที่คอนโซล หรือถอดย้ายอุปกรณ์ เช่น ฮาร์ดดิสก์ ซึ่งอาจนำไปเขียนหรืออ่านภายหลัง หรือบายพาสไบออสได้

2. การบุกรุกทางระบบ (System Intrusion) ผู้บุกรุกเข้ามาในระบบ โดยปกติมักเป็นผู้ใช้ที่มีสิทธิ์ต่ำ ถ้าระบบไม่ได้ทำการใส่แพตช์ (Patch) ที่สามารถแก้ข้อบกพร่องของโปรแกรมแล้ว จุดนี้ก็เป็นช่องโหว่ที่ทำให้ผู้ใช้คนนั้นสร้างสิทธิ์ของตัวเองให้มากขึ้น จนเทียบเท่าผู้ดูแลระบบได้ เนื่องจากโปรแกรมที่ใช้งานเกือบทุกโปรแกรมยังมีข้อบกพร่องอยู่ ถ้ายังไม่สามารถทำให้ข้อบกพร่องนั้นหมดไปหรือลดลงไปได้ จุดนี้ก็เป็นช่องทางสำหรับการบุกรุกระบบ

3. การบุกรุกระยะไกล (Remote Intrusion) ผู้บุกรุกติดต่อผ่านทางเน็ตเวิร์ก มีหลายเทคนิคในการบุกรุกระบบแบบนี้ ปัจจุบันมีโปรแกรมประเภทไฟล์วอล (Firewall) ทำหน้าที่เป็นด่านแรกในการป้องกันการบุกรุกทางเน็ตเวิร์ก

ขั้นตอนหลักของการบุกรุกเข้าสู่ระบบ

ขั้นที่ 1 การตรวจสอบระบบจากภายนอก

ผู้บุกรุกจะพยายามปลอมแปลงตัวเองเพื่อไม่ให้รู้ว่าตัวเองคือใครและมีเจตนาอะไร โดยการปรากฏตัวเป็นผู้ใช้ทั่วไป ซึ่งในขั้นนี้เราไม่สามารถตรวจพบได้ ผู้บุกรุกอาจใช้คำสั่ง whois เพื่อค้นหาข้อมูลของเครือข่าย หลังจากนั้นผู้บุกรุกจะเข้าดูตาราง DNS ของเครือข่ายโดยใช้คำสั่ง nslookup หรือ dig เพื่อหาชื่อของคอมพิวเตอร์ในเครือข่าย

ขั้นที่ 2 การตรวจสอบระบบจากภายใน

ผู้บุกรุกใช้วิธีการบุกรุกต่างๆ เพื่อจะค้นหาข้อมูลของเครือข่าย โดยอาจเข้าเว็บเพจของระบบและค้นหา สคริปต์ซีจีไอ (CGI scripts) หรืออาจใช้วิธีการ ping กวาดไปทั่วระบบเพื่อดูว่ามีเครื่องไหนที่ทำงานอยู่ หรืออาจจะทำการใช้การสแกน ทีซีพี/ยูดีพี (TCP/UDP scan) ไปยังเครื่องเป้าหมาย เพื่อดูว่ามีบริการอะไรที่เปิดรับอยู่ ณ จุดนี้สิ่งที่ผู้บุกรุกทำดูเหมือนเป็นพฤติกรรมที่ปกติที่เกิดขึ้นบนเครือข่ายและยังไม่มีสิ่งใดที่จะระบุได้ว่าเป็นการบุกรุก แต่ว่าระบบตรวจสอบผู้บุกรุกทางเครือข่ายจะสามารถบอกได้ว่า มีบางคนกำลังตรวจสอบระบบของเราอยู่ แต่ว่ายังไม่ได้ทำอะไร

ขั้นที่ 3 การเจาะระบบ

ผู้บุกรุกจะเริ่มเจาะระบบผ่านทางช่องโหว่ของระบบ โดยผู้บุกรุกอาจจะพยายามส่งสคริปต์ซีจีไอที่มีคำสั่งเชลล์ (shell) ในฟิลด์อินพุต (input fields) หรืออาจพยายามส่งข้อมูลจำนวนมากเพื่อทำให้เกิดบัฟเฟอร์โอเวอร์รัน (buffer-overrun) หรืออาจจะทำการหาล็อกอินที่ง่ายต่อการ

คาดเดาพาสเวิร์ด เมื่อได้แอคเคาน์แล้วก็พยายามที่จะได้สิทธิ์เป็น root/admin หรือหาทางเข้ามาจากช่องโหว่ของโปรแกรมต่างๆที่ให้บริการอยู่บนเครื่องเป้าหมาย

ขั้นที่ 4 สร้างช่องทางลับและลบหลักฐาน

ณ จุดนี้ผู้บุกรุกจะสร้างช่องทางลับในระบบ โดยเจาะเข้าเครื่องคอมพิวเตอร์ในระบบนั้น เป้าหมายหลักเพื่อลบหลักฐานของการบุกรุกและทำให้แน่ใจว่าสามารถที่จะกลับเข้ามาอีกได้ โดยผู้บุกรุกจะติดตั้ง toolkit เพื่อให้สามารถเข้าระบบได้ หรือส่งม้าโทรจันไปฝังตัวไว้เพื่อสร้างพาสเวิร์ดแบ็กดอร์ (backdoor password) หรือสร้างแอคเคาน์ขึ้นใหม่เลย ทำให้สามารถเข้ามาอีกเมื่อไหร่ก็ได้

ขั้นที่ 5 แสวงหาผลประโยชน์

ผู้บุกรุกจะแสวงหาผลประโยชน์จากสิทธิ์ที่ตนได้รับโดยอาจขโมยข้อมูลลับ เช่น รหัสบัตรเครดิต หรือทำให้ระบบทำงานผิดพลาด หรืออาจใช้ระบบนี้เพื่อเป็นทางผ่านไปยังระบบอื่นหรือโจมตีระบบอื่นเพื่อไม่ให้รู้ตัวตนที่แท้จริงของผู้บุกรุก

2.4 ระบบตรวจจับผู้บุกรุก

ความหมายของระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์

ระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์ (Intrusion Detection System: IDS) เป็นส่วนให้ความช่วยเหลือระบบคอมพิวเตอร์ ในการเตรียมการรับมือกับการบุกรุก ระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์รวบรวมข้อมูลจากแหล่งข้อมูลหลายๆ แหล่งทั้งจากภายในระบบและจากเครือข่ายคอมพิวเตอร์ แล้วทำการวิเคราะห์ข้อมูลเหล่านั้นเพื่อหาลักษณะการที่บ่งบอกว่ามีการบุกรุกระบบเกิดขึ้น ในบางกรณีระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์อาจอนุญาตให้ผู้ใช้กำหนดวิธีการตอบสนองต่อการบุกรุกเองได้

กล่าวโดยสรุปแล้วระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์ คือ ระบบที่ทำหน้าที่ติดตามดูการทำงานที่เกิดขึ้นบนระบบคอมพิวเตอร์ เพื่อค้นหาร่องรอยที่บอกว่ามีผู้กำลังพยายามบุกรุกระบบคอมพิวเตอร์ หรือค้นหาการกระทำที่เกินขอบเขตสิทธิ์ของผู้ใช้ระบบ

ผู้บุกรุกระบบคอมพิวเตอร์หรือ Intruder หมายถึง บุคคลที่พยายามบุกรุกหรือได้บุกรุกเข้ามาในระบบโดยที่ไม่ได้รับอนุญาต หมายความถึงบุคคลที่เรียกว่า แฮ็กเกอร์ (Hacker) คือผู้ที่ชอบเข้าไปศึกษาบางสิ่งบางอย่างในระบบ เช่น เข้าไปศึกษาหลักการทำงานของระบบและโปรแกรม

ความจำเป็นของระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์

ผู้ดูและระบบอาจคิดว่าในระบบที่ตนดูแลอยู่ไม่มีข้อมูลสำคัญ ถึงแม้มีผู้บุกรุกเข้ามาก็ไม่เป็นไร แต่ความเป็นจริงแล้วสามารถเกิดกรณีที่มีผู้บุกรุกเข้ามายังระบบ แล้วใช้เป็นทางผ่านในการเจาะระบบของธนาคาร หรือหน่วยงานที่มีข้อมูลสำคัญ และเข้าไปทำความเสียหายให้กับระบบ

นั้นๆ ถ้ามีการตรวจสอบกลับมา เจ้าของระบบต้องเป็นผู้รับผิดชอบกับเหตุการณ์ที่เกิดขึ้น ดังนั้น การรักษาความปลอดภัยของระบบจึงเป็นเรื่องจำเป็นที่ละเลยไม่ได้

การบุกรุกถ้าแบ่งจากสถานที่ที่ติดต่อเข้ามาของผู้บุกรุก สามารถแบ่งได้เป็น 2 ประเภทคือ การบุกรุกจากภายในเครือข่ายเอง และบุกรุกจากภายนอกเครือข่าย

การบุกรุกจากภายนอกเป็นการบุกรุกที่มาจากภายนอกเครือข่ายของระบบ และเข้ามาทำความเสียหายให้แก่ระบบ เช่น เข้ามาเปลี่ยนข้อมูลในโฮมเพจ หรือส่งสแปมเมลล์ไปให้ผู้อื่น โดยผ่านระบบของหรือพยายามบุกรุกผ่านไฟร์วอลล์เข้ามาทำความเสียหายให้กับเครื่องที่อยู่ภายในเน็ตเวิร์ก ผู้บุกรุกจากภายนอกสามารถเข้ามาโดยผ่านบริการ (Service) ของระบบ หรือติดต่อผ่านโมเด็มเข้ามา

การบุกรุกจากภายในเป็นการบุกรุกโดยผู้ที่มีสิทธิ์อันชอบธรรมที่เข้ามาใช้ทรัพยากรในระบบ แต่ใช้งานทรัพยากรอย่างไม่ถูกต้อง หรือพยายามแอบอ้างไปใช้สิทธิ์ของผู้อื่นที่มีสิทธิ์ในการใช้งานเหนือกว่า

ชนิดของระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์

ระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์สามารถแบ่งได้เป็น 2 ชนิด คือ

1. ระบบตรวจจับผู้บุกรุกในโฮสต์ (Host-based Intrusion Detection System)
2. ระบบตรวจจับผู้บุกรุกเครือข่าย (Network Intrusion Detection System)

2.4.1 Host based IDS

เป็นโปรแกรมที่จะตรวจสอบข้อมูลจากเครื่องหรือจากระบบ โดยมีข้อดีกว่า network-base คือเราสามารถรู้ได้ว่าเกิดการเปลี่ยนแปลงอะไรบ้างที่เครื่องเรา

โดยส่วนมากโปรแกรมประเภท host-base IDS จะตรวจสอบค่าหรือข้อมูลที่เก็บอยู่ใน log file และตรวจสอบค่า integrity checksum โดยจะตรวจสอบหาการกระทำที่ผิดปกติอย่างเช่น มีการปรับเปลี่ยนข้อมูล มีการลบข้อมูล มีการเข้าถึงข้อมูล มีการเปลี่ยนแปลงระบบ มีการลงโปรแกรม มีการหลีกเลี่ยงการตรวจจับหรือการตรวจสอบ เป็นต้น

การใช้ค่า logs ในการตรวจสอบนั้นโดยส่วนมากจะไม่ใช้เพียงไฟล์ใดไฟล์เดียวแต่จะเป็นการเอาค่า logs ต่างๆมาทำการ cross-check เพื่อตรวจสอบ โดย host-base IDS ที่ดีนั้นจะทำการ cross-check ค่า logs และ system activity

ในการเก็บล็อกจะต้องพิจารณาถึง ลักษณะการเก็บ ปริมาณจะเก็บ พื้นที่ที่ต้องใช้ในการเก็บล็อก รวมไปถึงเวลาที่ต้องเสียไปในการตรวจสอบ

2.4.1.1 Unix logs (syslogd)

โปรแกรม syslogd เป็นกลไกที่ใช้ในการเก็บข้อมูลต่างๆ ของ kernel และ application บนระบบยูนิกซ์และลินุกซ์ลงล็อกไฟล์ โดยโปรแกรม syslogd นี้จะเป็น daemon ที่ถูกติดตั้งมาให้พร้อมกับระบบปฏิบัติการในเกือบทุกระบบ โดยผู้ดูแลระบบสามารถปรับแต่งไฟล์ configuration เพื่อปรับแต่งลักษณะการทำงานของ syslogd ได้ เช่น ให้ syslogd เก็บข้อมูลไปไว้ที่ไฟล์ใด หรือให้ส่งข้อมูลล็อกนี้ไปเก็บไว้ยังเครื่องอื่นในเครือข่าย

ข้อมูลล็อกที่ควบคุมโดย syslogd นั้น จะถูกกำหนดให้มีค่า facility และ priority โดยส่วนของ facility นั้น เป็นข้อมูลที่อธิบายถึงแหล่งกำเนิดของข้อมูลล็อกนั้นๆ เช่น ข้อมูลล็อกที่ส่งมาจากระบบเมลล์ก็จะมี facility เป็น mail ส่วน priority นั้น จะแสดงถึงระดับความสำคัญของเหตุการณ์ที่เกิดสำหรับแต่ละ facility ทั้งนี้ข้อมูลล็อกทุกอันจำเป็นต้องมี facility และ priority เสมอ

ตารางที่ 2.1 แสดงค่า facility และความหมาย

Facility	คำอธิบาย
auth	เกี่ยวข้องกับการทำ authentication
authpriv	การทำ private authentication เท่านั้น
cron	cron daemon
daemon	system daemons
kern	ส่วนของ kernel
lpr	line printer spooling system
mail	sendmail และซอฟท์แวร์อื่นที่เกี่ยวกับเมล์
mark	ให้บันทึกเวลาขณะเกิดเหตุการณ์ด้วย
news	usenet news system
security	เหมือนกับ auth
syslog	ข้อมูลล็อกภายในของ syslogd
user	ส่วนของโปรเซสของ user
uucp	สำรองไว้สำหรับ UUCP
local0 - local7	local messages

ตารางที่ 2.2 แสดงค่า priority และความหมาย

Priority	คำอธิบาย
emerg	ภาวะฉุกเฉิน
alert	แจ้งเตือนเร่งด่วน
crit	ล่อแหลม
err	มีข้อผิดพลาด
warning	คำเตือน
notice	ข้อสังเกตุ
info	ข้อมูลทั่วไป
debug	สำหรับใช้ดีบักเท่านั้น

การทำงานของ syslogd นั้น จะขึ้นอยู่กับไฟล์ /etc/syslog.conf เป็นหลัก การแก้ไขใดๆ ที่เกิดขึ้นกับไฟล์นี้นั้น จะยังไม่มีผลต่อการทำงานของ syslogd ในทันที จะต้องทำการ restart syslogd service ใหม่เสียก่อน รูปแบบคำสั่งในไฟล์ /etc/syslog.conf นั้นมีรูปแบบดังนี้

facility.level action

facility1, facility2.level action

facility1.level1; facility2.level2 action

*.level action

*.level;badfacility.none action

หมายความว่า เมื่อมีข้อมูลล็อกที่มี facility และ level ที่ตรงหรือมากกว่ากับที่ตั้งไว้ ก็จะกระทำ action ตามที่กำหนดไว้ ทั้งนี้เพราะ level ที่ตั้งไว้นั้น เป็นค่า minimum ซึ่งหมายความว่าถ้าเราตั้ง level เป็น debug ก็จะคลอบคุลมทุก level ของ facility นั้นๆ เลย ทั้งนี้เราสามารถใช้เครื่องหมาย * แทนทุกๆ ค่าใน facility หรือ priority level นั้นๆ ได้ เช่น mail.* /var/log/mail หมายความว่าให้ syslogd เก็บข้อมูลล็อกของ mail ทุก level ไปไว้ยังไฟล์ /var/log/mail

ในขณะที่ level ที่เป็น none นั้น หมายความว่าไม่ให้สนใจ facility ที่บ่ระกาศค่า level เป็น none เช่น*.emerg;mail.none /var/log/emer.log คือให้เก็บข้อมูลล็อกที่มี level เป็น emerg สำหรับทุก facility ยกเว้น mail facility

สำหรับ action นั้นสามารถเลือกได้ดังนี้คือ

- filename : เก็บข้อมูลล็อกนั้นลงในไฟล์ที่กำหนด
- @hostname : ส่งต่อข้อมูลล็อกไปยัง syslogd บน host ที่กำหนด
- @ipaddress : ส่งต่อข้อมูลล็อกไปยัง host ที่มี ip address ตามที่กำหนด
- user1, user2 : ส่งข้อมูลล็อกไปยังหน้าจอของ user ที่กำหนด ถ้า user เหล่านั้นยังล็อกอินอยู่ในระบบ
- * : ส่งข้อมูลล็อกไปยังทุกๆ user ที่ยังล็อกอินอยู่ในระบบ
- /dev/console เพื่อส่งข้อมูลล็อกไปยัง console device หรือ device อื่นๆ ตามที่ต้องการ สำหรับ Red Hat นั้นได้ขยายความสามารถของ syslogd เพิ่มเติม โดยอนุญาตให้ข้อมูลล็อกสามารถถูกส่งแบบ pipe ไปยังไฟล์ได้ โดยแก้ไขใน syslog.conf และยังสามารถใช้เครื่องหมาย = และ ! ใน syslog.conf ได้โดย
  - เครื่องหมาย = หมายถึง priority ที่กำหนดเท่านั้น
  - เครื่องหมาย ! หมายถึง priority อื่นที่ไม่ใช่ priority นี้และสูงกว่า

ตัวอย่าง เช่น

- mail.info ความหมายคือ ข้อมูลล็อกที่เกี่ยวข้องกับเมลล์และมี priority เป็น info และสูงกว่า
- mail.=info ความหมายคือ ข้อมูลล็อกที่เกี่ยวข้องกับเมลล์และมี priority เป็น info เท่านั้น
- mail.info;mail.!err ความหมายคือ ข้อมูลล็อกที่เกี่ยวข้องกับเมลล์และมี priority เป็น info , notice และ warning
- mail.debug;mail.!=warning ความหมายคือ ข้อมูลล็อกที่เกี่ยวข้องกับเมลล์และมี priority ทุกระดับที่ไม่ใช่ warning

โดยปกติ Red Hat จะเก็บข้อมูลล็อกไว้ในไฟล์ซึ่ง อยู่ภายใต้โฟลเดอร์ /var/log และถูกติดตั้งมาพร้อมกับ logrotate ซึ่งเป็นเครื่องมือที่ช่วยจัดการล็อกไฟล์ได้อย่างมีประสิทธิภาพ ปกติแล้วจะ rotate ล็อกไฟล์อาทิตย์ละครั้ง และจะเก็บล็อกไว้ 4 รอบ หรือ 1 เดือน ผู้ดูแลระบบสามารถปรับเปลี่ยนค่าเหล่านี้ได้ที่ /etc/logrotate.conf

ตัวอย่างของไฟล์ configuration สำหรับ stand-alone machine

- *.emerg *

  ความหมาย ในกรณีฉุกเฉินให้แจ้งเตือน user ทุกคนที่ล็อกอินอยู่

- *.warning;daemon,auth.info,user.none /var/log/messages

  ความหมาย เก็บข้อมูลล็อกที่สำคัญไว้ในไฟล์

- lpr.debug /var/log/lpd-errs

  ความหมาย printer errors

ตัวอย่างของไฟล์ configuration สำหรับ network client

- *.emerg;user.none*

  ความหมาย ในกรณีฉุกเฉินให้แจ้งเตือน user ทุกคนที่ล็อกอินอยู่

- *.warning;lpr,local1.none @netloghost

  daemon,auth.info @netloghost

  ความหมาย ส่งข้อมูลล็อกที่สำคัญไปยังเครื่องที่ทำหน้าที่เก็บล็อก

- local2.info;local0,local7.debug @netloghost

  ความหมาย ส่งข้อมูลล็อกของ local ไปยังเครื่องที่ทำหน้าที่เก็บล็อก

- lpr.debug /var/log/lpd-errs

  ความหมาย printer errors

- local2.info /var/log/sudo-logs

  ความหมาย ข้อมูลของ sudo ที่ local2 ให้เก็บไว้ในไฟล์

- kern.info /var/log/kern.log

  ความหมาย ข้อมูลของ kernel ให้เก็บไว้ในไฟล์

ในกรณีนี้ข้อมูลส่วนใหญ่จะถูกส่งไปยังเครื่องที่ทำหน้าที่เก็บล็อก ซึ่งหมายความว่าถ้าเครื่องนั้นไม่สามารถให้บริการได้ข้อมูลล็อกก็จะสูญไป ดังนั้นจึงควรเก็บข้อมูลล็อกบางส่วนไว้ที่เครื่องของตัวเองด้วย

*ตัวอย่างของไฟล์ **configuration** สำหรับ **central logging host***

- *.emerg /dev/console

  *.err;kern,mark.debug;auth.notice /dev/console

  *.err;kern,mark.debug;user.none /var/log/console.log

  auth.notice /var/log/console.log

  ความหมาย ในกรณีฉุกเฉินให้ส่งข้อมูลไปยัง console และล็อกไฟล์โดยมีเวลากำหนดด้วย

- *.err;user.none;kern.debug /var/log/messages

  daemon,auth.notice;mail.crit /var/log/messages

  lpr.debug /var/log/lpd-errs

  mail.debug /var/log/mail.log

  ความหมาย ส่งข้อมูลล็อกที่ไม่ใช่ข้อมูลฉุกเฉินไปยังไฟล์ธรรมดา

- local2.debug /var/log/sudo.log

  local2.alert /var/log/sudo-errs.log

  auth.info /var/log/auth.log

  ความหมาย เก็บข้อมูลที่เกี่ยวข้องกับการทำ authorization เช่น sudo

- local7.debug /var/log/tcp.log

  ความหมาย และข้อมูลอื่นๆ

- user.info /var/log/user.log

  ความหมาย ข้อมูลของ user

ข้อควรระวังคือ ในกรณีที่เวลาของแต่ละเครื่องไม่ตรงกันนั้นอาจจะก่อให้เกิดความยุ่งยากมากทีเดียว เพราะเวลาที่เขียนลงในล็อกไฟล์นั้นเป็นเวลาของเครื่องที่ทำหน้าที่บันทึกข้อมูลล็อก ไม่ได้ดึงมาจาก เครื่องที่ส่งข้อมูลล็อกมาให้แต่อย่างใด ดังนั้นจึงควรทำ clock synchronize ในทุกๆ เครื่องเพื่อให้เวลาที่บันทึกข้อมูลลงล็อกไฟล์นั้นตรงกัน

ตารางที่ 2.3 แสดงรายชื่อซอฟต์แวร์ที่ใช้ syslog

Program	Facility	Levels	Description
amd	daemon	err-info	NFS automounter
date	auth	notice	Set the time and date
ftpd	daemon	err-debug	FTP daemon
gated	daemon	alert-info	Routing daemon
halt/reboot	auth	crit	Shutdown programs
inetd	daemon	crr, warning	Internet super-daemon
login/rlogind	auth	crit-info	Login programs
lpd	lpr	er-info	BSD line printer daemon
named	daemon	err-info	Name server (DNS)
nnrpd	news	crit-notice	INN news reader
ntpd	daemon, user	crit-info	Network time daemon

Program	Facility	Levels	Description
passwd	auth	err	Password-setting program
popper	local0	notice, debug	Mac/PC mail system
sendmail	mail	alert-debug	Mail transport system
su	auth	crit, notice	Switches UIDs
sudo	local2	alert, notice	Limited su program
syslogd	syslog, mark	err-info	Internal errors, timestamps
tcpd	local7	err-debug	TCP wrapper for inetd
cron	cron, daemon	info	System task-scheduling daemon
vmunix	kern	*varies*	The kernel

สำหรับการดีบักหรือทดสอบการทำงานของ syslog ว่าทำงานหรือไม่นั้น สามารถทำได้โดยไม่ยากนัก เช่นเพิ่มบรรทัดด้านล่างนี้ใน syslog.conf

local5.warning /var/log/test.log

จากนั้นให้ restart syslogd ใหม่ แล้วจึงรันคำสั่ง #logger -p local5.warning "test" ซึ่งถ้าเป็นไปตามปกติแล้ว ในไฟล์ /var/log/test.log ก็จะมีคำว่า test ปรากฏอยู่ด้วย

สำหรับ Red Hat ที่ต้องการทำหน้าที่เป็นเครื่องที่ทำหน้าที่เก็บข้อมูลล็อกสำหรับเครื่องอื่นๆ ภายในเครือข่าย สามารถแก้ไขได้โดยเพิ่ม -r ใน startup options ของ syslog daemon โดยแก้ไขได้ที่ /etc/sysconfig/syslog หรือที่ /etc/rc.d/init.d/syslog

ข้อสังเกต

syslog นั้นเป็นมาตรฐานสำหรับการทำ logging ของยูนิกซ์และลินุกซ์ แต่ syslog กำลังจะถูกแทนที่โดย syslog-ng (syslog new generation) ซึ่งมีความยืดหยุ่นมากกว่า standard syslog และสามารถเก็บข้อมูลล็อกบนพื้นฐานของ regular expression ได้

สำหรับการตรวจสอบล็อกไฟล์นั้น โดยปกติควรจะตรวจสอบอย่างน้อยวันละหนึ่งครั้ง แต่เนื่องจาก ล็อกไฟล์โดยส่วนใหญ่มักจะมีขนาดใหญ่ บางครั้งผู้ดูแลระบบเองอาจจะเผอเรอ หรือมองข้าม ในบางจุดไป ซึ่งอาจจะก่อให้เกิดความเสียหาย ต่อระบบได้ การนำ Swatch และ Logwatch มาใช้งาน จะช่วยลดปัญหาเรื่องการสูญเสียเวลาได้ สำหรับ Swatch นั้น เป็น daemon ที่ทำหน้าที่ตรวจสอบรูปแบบ (pattern matching) ของล็อกไฟล์ เมื่อเจอข้อมูลที่ต้องการก็สามารถ

รัน script หรือโปรแกรมอื่นได้ เช่นอาจจะสั่งให้ส่งอีเมลล์ ส่งเสียงบี๊บ ส่วน Logwatch นั้นทำงานบน cron job มีหน้าที่ในการตัดข้อมูลล็อก แล้วส่งผ่านอีเมลล์ไปยังผู้ดูแลระบบ เนื่องจากการส่งข้อมูล ล็อกไปยังเครื่องที่ทำหน้าที่เก็บข้อมูลล็อกอื่นนั้น ไม่มีกระบวนการของการตรวจสอบและยืนยันตัวตน และทำงานโดยใช้ UDP port 514 (user datagram protocol) ซึ่งเป็นโพรโตคอลที่ไม่มีการรับประกันการส่งข้อมูล และยังสามารถปลอมแปลง header ได้โดยง่าย ดังนั้นผู้ดูแลระบบควรดิดตั้งไฟร์วอลล์เพื่อป้องกันไม่ให้เครื่องจากภายนอกส่งข้อมูลล็อกมายังเครื่องที่ทำหน้าที่เก็บข้อมูลล็อกดังกล่าว

ข้อเสียของ syslogd

1) เนื่องจาก syslog เป็นการส่งข้อมูลแบบ udp ทำให้ผู้ส่งไม่ได้รับความมั่นใจว่าข้อมูลที่ส่งไปให้เครื่อง server นั้น จะไปถึงหรือไม่
2) การที่ไม่มีการทำ authentication ก่อนว่าใครคือคนส่ง ก็อาจจะนำไปสู่การส่งข้อมูลแปลกปลอมปนเข้าไปยังเครื่อง log server เพื่อไปชักนำให้การตามรอยผู้บุกรุก เกิดหักเหไปสู่ทิศทางที่ไม่ถูกต้อง และยังอาจจะทำให้เกิด DoS ได้
3) การส่งข้อมูล plaintext โดยไม่มีการเข้ารหัสก่อนที่จะส่ง อาจจะทำให้ผู้ไม่หวังดีสามารถดักจับข้อมูลไปดู และอาจจะทำให้รู้ได้ว่าระบบเราลงโปรแกรมอะไรบ้าง มีช่องโหว่หรือจุดอ่อน อะไรซึ่งอาจจะนำไปสู่การโจมตีหรือละเมิดความปลอดภัยได้

2.4.1.2 syslog-ng

เป็นโปรแกรมที่ปรับปรุงมาจาก syslogd โดยมีความสามารถที่เพิ่มเติมเข้ามาคือ

- สามารถทำการรับส่งข้อมูลผ่าน protocol TCP ซึ่งมีการรับประกันความถูกต้องของข้อมูล ทำให้น่าเชื่อถือ แทนที่จะเป็นการส่งโดยผ่าน protocol UDP ซึ่งไม่มีการรับประกันความถูกต้องของข้อมูล ทำให้การส่งข้อมูลนั้นไม่น่าเชื่อถือและไม่ปลอดภัย การที่ใช้การเชื่อมต่อแบบ TCP ทำให้สามารถที่จะทำการเข้ารหัสและตรวจสอบ cert เพิ่มขึ้นมาได้ ซึ่งจะมีประโยชน์ในการตรวจสอบฝั่งที่ส่งและฝั่งที่รับได้
- สามารถที่จะใช้ตัวกรองเพื่อกรองข้อมูลได้ โดยสามารถกรองจาก regular expression
- สามารถปรับแต่งการทำงานได้ยืดหยุ่นมากกว่า ซึ่งเป็นประโยชน์ต่อการนำไปใช้
- สามารถกำหนดให้มีการไว้วางใจในชื่อ hostname ที่ส่งมาได้ ซึ่งโดยปกติค่าเริ่มต้นจะตั้งค่าไว้ว่าไม่ให้ไว้วางใจ โดยจะไปทำการ resolve จาก source IP ของ แพ็กเกต ที่เข้ามาแทน เพื่อป้องกันการปลอม hostname ซึ่งใน syslogd จะเชื่อค่า hostname ที่ส่งเข้ามา
- สามารถกำหนด queue ที่จะให้รับข้อมูลได้ว่าจะให้มากขนาดไหน
- สามารถกำหนด จำนวน connection ต่อ port ที่ให้รับนั้นได้ เพื่อป้องกันการคับคั่งของข้อมูล

ปัญหาของ syslog-ng คือ

1) ไม่มีการเข้ารหัสในการรับส่งข้อมูล

2) ไม่มีการทำ authentication ในระหว่างการรับส่งข้อมูล

2.4.1.3 Tripwire

เป็นโปรแกรมในยุคเริ่มต้นของโปรแกรมประเภท host-based IDS ซึ่งภายหลังตัวโปรแกรม tripwire นี้ก็ถูกนำมาพัฒนาต่อกลายเป็นโปรแกรม host-based IDS ตัวอื่นๆ

การทำงาน

การทำงานของตัวโปรแกรม tripwire เริ่มจากการคำนวณหาค่า message digest ของแต่ละไฟล์ เก็บไว้ใน database เป็นค่าเริ่มต้น โดยค่าที่เก็บครั้งแรกนั้นเป็นค่าที่เก็บเมื่อระบบยังไม่ถูกละเมิดสิทธิ์ เป็นค่าที่ระบบยังปกติอยู่ ในการตรวจสอบระบบแต่ละครั้ง ตัวโปรแกรมก็จะทำการคำนวณค่า message digest ออกมาใหม่เพื่อเอาไปเปรียบเทียบกับค่าที่เก็บไว้ในตอนแรก ถ้าค่า message digest แตกต่างจากค่าที่เก็บไว้เมื่อตอนเริ่มต้นก็แสดงว่า มีการเปลี่ยนแปลงเกิดขึ้นกับไฟล์นั้น

Message digest คือไฟล์ชนิดพิเศษที่ผ่านกระบวนการเข้ารหัส โดยค่าที่ได้นี้ขึ้นอยู่กับข้อมูลภายในไฟล์นั้นๆ message digest ถูกออกแบบมาให้ยากมากที่จะคำนวณค่าออกมาเหมือนเดิมหรือที่จะคำนวณข้อมูล 2 ชุดได้ค่า message digest เหมือนกัน และยังมีคุณสมบัติในการป้องกันไม่ให้พิจารณาไปถึงค่าเริ่มต้นของข้อมูลได้ (ไม่สามารถถอดรหัส message digest ได้)

โดยปกติสำหรับ unix,linux จะใช้ md5sum ในการคำนวณหาค่า message digest ออกมา ซึ่งสามารถทดสอบได้โดยการใช้คำสั่ง md5sum ตามด้วยชื่อไฟล์ การเปลี่ยนค่าเพียงแค่ 1 บิทก็จะทำให้ค่า message digest มีค่าที่ไม่เหมือนเดิม ซึ่งมันเป็นไปไม่ได้ที่มีคนเปลี่ยนค่าในไฟล์แล้วจะได้ค่า message digest เป็นค่าเดิม

จากคุณสมบัติดังกล่าวทำให้ โปรแกรม tripwire เหมาะสำหรับการตรวจสอบไฟล์ที่มีความเสี่ยง โดยเราสามารถเข้าไปกำหนดค่าว่าจะให้ทำการตรวจสอบไฟล์ใดบ้างได้ที่ tw.pol

ข้อแนะนำ ในการเก็บค่า message digest ในครั้งแรกควรเก็บเอาไว้ที่ floppy disk หรือควรเก็บเอาไว้ที่แผ่น CD-ROM โดยไปทำการแก้ค่าได้ในไฟล์ configure

```
phantomb@Isag27:~/tmpS md5sum server.pem
914822e263459a98b3d3c9a39887d09e server.pem
phantomb@Isag27:~/tmp$ md5sum server.pem
914822e263459a98b3d3c9a39887d09e server.pem
phantomb@Isag27:~/tmp$ nano server.pem
phantomb@Isag27:~/tmp$ md5sum server.pem
022a86914feb6608858cfdb3276772a1 server.pem
```

รูปที่ 2.2 แสดงตัวอย่างการหา checksum

จากรูปตัวอย่าง ได้ทำการเอาไฟล์ server.pem มาเข้า checksum โดย ครั้งแรกได้ค่าเก็บไว้แล้วลอง ทำอีกครั้งโดยไม่เปลี่ยนค่าใดๆในไฟล์ ส่วนครั้งสุดท้ายทำการลบตัวอักษรออก 1 ตัว ก็จะได้ค่าไม่เหมือนเดิม

2.4.1.4 Samhain

เป็นโปรแกรมตรวจสอบความถูกต้องของข้อมูล เช่นเดียวกันกับ tripwire แต่ว่าตัวโปรแกรม samhain เป็นโปรแกรมที่พัฒนาอย่างต่อเนื่อง และทันสมัยมากกว่า โปรแกรม tripwire ที่หยุดการพัฒนาไปตั้งแต่ปี 2001 ทำให้สามารถตรวจสอบได้มากกว่า ป้องกันการหลีกเลี่ยงได้มากกว่า และ มีการเพิ่มเติมในส่วน interface มากขึ้นเพื่อให้สามารถใช้งานได้มากกว่า

คุณสมบัติหลักที่สำคัญของโปรแกรม samhain มีดังนี้คือ

1) สามารถตรวจสอบไฟล์ประเภท suid และ sgid ได้
2) โปรแกรมทำงานที่ระดับ kernel ทำให้สามารถตรวจสอบโปรแกรม ประเภท rootkit ที่อาจจะถูกติดตั้งที่ kernel ของระบบได้
3) สามารถซ่อน process ให้มองไม่เห็นได้
4) สามารถสั่งให้โปรแกรมทำงานแบบ background ได้ (daemond) เพื่อให้โปรแกรมคอยตรวจสอบความถูกต้องอยู่ตลอดเวลา
5) สามารถเก็บข้อมูลการตรวจสอบ และไฟล์ฐานข้อมูลสำหรับเปรียบเทียบไว้ที่เครื่องกลางได้
6) สามารถเก็บข้อมูลการตรวจสอบลงฐานข้อมูล ได้เพื่อให้ง่ายต่อการตรวจสอบ
7) มีการ sign ฐานข้อมูลเพื่อเป็นการยืนยันความถูกต้องของฐานข้อมูล
8) มีการ sign ข้อมูล output (ข้อมูลที่ตรวจสอบมา) และ มีการเข้ารหัสเมื่อส่งเข้าไปที่เครื่องกลาง

9) สามารถตรวจสอบการ mount file system ได้

10) สามารถเลือกวิธีที่จะใช้ในการหาค่า checksum ได้ โดยมีวิธีการ 3 อย่างให้เลือกคือ tiger192, md5 และ sha-1

11) มีการฝัง password ตอน compile เพื่อเอาไปใช้ตอน connect กับ ตัว server

12) สามารถใช้ server ควบคุมและตรวจสอบการทำงานของ client ได้

2.4.2 Network based IDS and IPS

หลักการทำงานพื้นฐานของระบบตรวจจับผู้บุกรุกทางเครือข่ายก็คือ การดักจับแพ็กเก็ตที่ผ่านเข้ามายังเครือข่ายและนำข้อมูลจากแพ็กเก็ตนั้นมาวิเคราะห์ เพื่อตรวจสอบว่ามีลักษณะตรงกับรูปแบบการบุกรุกหรือไม่ เมื่อตรวจพบลักษณะที่ตรงกับการบุกรุกก็อาจจะทำการ แจ้งเตือนผู้ดูแลระบบ หรือทำการส่งข้อมูลไปเก็บลงระบบเก็บล็อกต่อไป แต่ถ้าเป็น IPS ก็สามารถที่จะทำการ drop หรือ block แพ็กเก็ตนั้นทิ้งไปได้เลย โดยถ้าต้องการให้เครื่องของเรารับข้อมูลแพ็กเก็ตเข้ามาพิจารณาก่อน โดยไม่สนว่าเป็นของใคร จะเรียกว่า โพรมิสคูอัส โหมด (promiscuous mode) เป็นโหมดที่อนุญาตให้ฮาร์ดแวร์รับข้อมูลดิบทั้งหมดบนเน็ตเวิร์กที่เข้ามาในเครื่องคอมพิวเตอร์ของตนเอง โดยที่ไม่สนใจว่าจะเป็นของใคร ส่งให้ใคร และเป็นการละเมิดข้อบังคับของโพรโตคอลหรือไม่

ลักษณะของซิกเนเจอร์ที่ใช้ในการตรวจสอบ

การวิเคราะห์แพ็กเก็ตนั้นจะสนใจแพ็กเก็ตที่มีลักษณะซิกเนเจอร์ตรงกับที่มีข้อมูลอยู่ ซิกเนเจอร์แบ่งออกได้เป็น 3 ประเภทดังนี้คือ

1. สตริงซิกเนเจอร์ (String signatures) จะสนใจส่วนของข้อมูลในแพ็กเก็ต โดยหาส่วนของสตริงที่อาจบ่งถึงว่าเป็นการบุกรุกได้ ตัวอย่างของสตริงซิกเนเจอร์สำหรับระบบยูนิกซ์ เช่น “cat”++”>/.rhosts” ซึ่งถ้าเจอในแพ็กเก็ตใด ก็อาจสรุปได้ว่าเป็นแพ็กเก็ตของการโจมตี
2. พอร์ตซิกเนเจอร์ (Port signatures) ตรวจดูการเชื่อมต่อไปยังพอร์ตที่นิยมใช้ในการโจมตี ตัวอย่างของพอร์ตเหล่านี้ได้แก่ telnet (ทีซีพี พอร์ต 23) FTP (ทีซีพี พอร์ต 21/20) SUNRPC (ทีซีพี/ยูดีพี พอร์ต 111) และ IMAP (ทีซีพี พอร์ต 143) ซึ่งถ้าพอร์ตเหล่านี้ไม่ได้ถูกใช้โดยไซต์นั้นแล้ว แพ็กเก็ตที่เข้ามายังพอร์ตเหล่านี้ก็จะจัดได้ว่าเป็นที่น่าสงสัยที่จะเป็นการบุกรุก
3. เฮดเดอร์ซิกเนเจอร์ (Header signatures) ตรวจสอบส่วนหัวของแพ็กเก็ตว่ามีส่วนประกอบที่ผิดปกติ ไม่สมเหตุสมผลหรือไม่ ตัวอย่างที่รู้จักกันดีที่สุดคือ Winnuke หรืออีกตัวอย่างก็คือ แพ็กเก็ตที่มีทั้งแฟล็ก SYN และ FIN ตั้งไว้ซึ่งหมายความว่าผู้ส่งต้องการที่จะเริ่มและหยุดการติดต่อในเวลาเดียวกัน

ข้อดีของ Network-base IDS ก็คือ สามารถตรวจพบการบุกรุกหรือการละเมิดความปลอดภัยและทำการป้องกัน ก่อนที่จะเกิดการโจมตีได้ โดยสามารถทำการตรวจสอบได้ตั้งแต่ที่แพ็กเก็ตยังเข้ามาไม่ถึงระบบ และสามารถดูถึงเจตนาที่มุ่งร้ายได้

ตัวอย่างโปรแกรมทางด้าน NIDS ก็คือ โปรแกรม snort ซึ่งเป็นโปรแกรมที่นิยมใช้กันมากเนื่องจากเป็นโปรแกรม opensource และสามารถประยุกต์ใช้เป็นโปรแกรม IPS ได้ คือ สามารถป้องกันได้โดยไม่ใช่แค่ตรวจสอบอย่างเดียวเท่านั้น

2.4.2.1 Snort และ Snort-Inline

Snort เป็นเครื่องมือที่ใช้ตรวจจับการบุกรุกทางเครือข่าย (network intrusion detection) โดยการทำงานของ Snort จะใช้ไลบรารี (library) พื้นฐานชื่อ libpcab ซึ่งใช้กันโดยทั่วไปในบรรดา network sniffer และ network analyzer ทั้งหลาย สำหรับ Snort นั้นสามารถทำ protocol analysis, content searching/matching, ตรวจจับการบุกรุกและ probe เช่น buffer overflow, stealth port scan, CGI attack, SMB probe, OS Fingerprint และอื่นๆ

นอกจากนี้โปรแกรม Snort ยังมีคุณสมบัติในการทำ real-time alerting อีกด้วย นอกเหนือจากการเก็บล็อกไปที่ syslog หรือเก็บแยกไฟล์ต่างหาก และยังสามารถ alert ผ่าน winpopup ผ่านทาง Samba's client ได้อีกด้วย

ปัญหาที่สำคัญที่สุดของ IDS ก็คือ โดยส่วนใหญ่แล้ว IDS ไม่สามารถป้องกันการบุกรุกในลักษณะ "Real Time" ได้ เช่นการจู่โจมแบบ DoS (Denial of Services) หรือ DDoS (Distributed Denial of Services) Attack จากปัญหานี้ จึงมีคนคิดค้นเทคโนโลยีใหม่ขึ้นมา เรียกว่า "IPS" (Intrusion Prevention System) ซึ่งเราอาจจะให้คำจำกัดความง่ายๆ ว่า "IPS" = "IDS"+ "Active Response" หมายถึง IPS สามารถป้องกันการบุกรุกและหยุดการบุกรุกได้ทันท่วงที

IPS นั้น แบ่งออกเป็น 2 Generations ใน Generation แรกนั้น การหยุดการบุกรุกทำได้โดยการส่งสัญญาณ TCP Reset จัดการกับ TCP Session ที่ IPS คิดว่าเป็นการบุกรุกหรืออาจจะเข้าไปเปลี่ยนแปลงแก้ไข Rules Based ใน Firewall แบบอัตโนมัติ ซึ่งบางครั้งอาจเกิดความผิดพลาดได้ สำหรับ IPS ใน Generation ที่ 2 นั้น ได้มีการปรับปรุงให้เป็นลักษณะ "Intelligent Network Element" ซึ่งสามารถรู้จักเทคนิคของพวก Hacker เช่น IDS Evasion หรือ Anomaly IP Packet โดยมีลารวิเคราะห์ IP Packet Traffic อย่างละเอียด

IPS รุ่นใหม่ที่มีความฉลาดมากขึ้นนั้น มีการใช้เทคโนโลยีขั้นสูงในการวิเคราะห์ข้อมูล เช่น Neutral Network และ Fuzzy Logic ซึ่งจะทำให้ลดปัญหา Fault Positive และ Fault Negative ลงได้อย่างมาก ตลอดจน เนื่องจาก IPS ใช้หลักการเปรียบเทียบข้อมูล แปลกปลอมจากการปรับแต่ง IP Packet โดยใช้มาตรฐาน RFC ของ IETF ในการตัดสินใจ ทำให้ IPS บางรุ่น สามารถป้องกันการ โจมตีแบบ DoS หรือ DDoS Attack ได้ด้วย

ปัญหาของ IPS ก็มีเหมือนกัน ที่ชัดเจนเลยก็คือ ยังมีราคาค่อนข้างแพงมาก เมื่อเปรียบเทียบกับ IDS ส่วนใหญ่แล้ว IPS ที่มาใน ลักษณะของ Network Appliance นั้นจะมีราคาในหลักล้านบาทขึ้นไป และ การทำงานของ IPS จะใช้หลักการที่เรียกว่า "Inline" หรือ บางตำราเรียกว่า"Gateway IDS" คือ มีการนำ IPS ไปกั้นกลางระหว่าง ต้นทาง กับ ปลายทาง ของเส้นทางการส่งข้อมูล โดยไม่ต้องมีการกำหนด IP address ให้กับตัว IPS ปัญหาก็คือ หากตัว IPS เกิดเสีย ถ้า IPS ไม่สามารถ Bypass ตัวเองได้ ก็จะทำให้เกิดปัญหาในการรับส่งข้อมูลระหว่างต้นทางกับปลายทาง ตลอดจนถ้า IPS ตัดสินใจผิด การ "Block" IP Packet ที่ IPS คิดว่าเป็นการบุกรุก แต่จริงๆ แล้วเป็น Traffic การใช้งานธรรมดา ก็จะเกิดปัญหากับผู้ใช้งานทั่วไปได้เช่นกัน

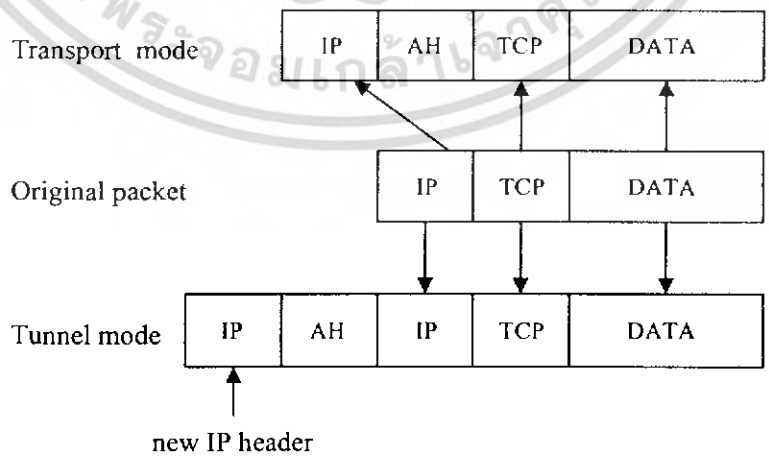
ต่อมาจึงมีการพัฒนาโปรแกรม Snort โดยมีการพยายามนำ Snort Engine มาแก้ไขให้เพิ่มความสามารถป้องกัน (drop) การโจมตีของบุกรุกได้ โดยไม่เพียงแต่แจ้งเตือน (alert) อย่างเดียว โดยนำ Snort Engine, iptables มาทำงานร่วมกันโดยดักจับ Packet ที่ Layer2 (Data-Link Layer) ซึ่งมีลักษณะการทำงานแบบ Bridge และตั้งชื่อใหม่ว่า "Snort Inline" ซึ่งมีคุณสมบัติเป็น IPS ที่สามารถป้องกันการโจมตีของ Hacker อย่างได้ผลและมีประสิทธิภาพ

2.5 Internet Protocol Security (IPsec)

IPsec เป็นส่วนเพิ่มขยายของ Internet Protocol (IP) ในชุดโพรโตคอล TCP/IP พัฒนาเพื่อเป็นส่วนหนึ่งของมาตรฐานของ IPv6 ซึ่งเป็นโพรโตคอลที่พัฒนาเพื่อใช้แทน IPv4 ที่ใช้ในปัจจุบันและกำหนดหมายเลข RFC เป็น RFC2401

IPsec ใช้โพรโตคอล 2 ชุดคือ Authentication Header (AH) และ Encapsulated Security Payload (ESP) เพื่อรองรับการพิสูจน์ตัวตน(Authentication) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความลับ (Confidentiality) ในระดับชั้นของ IP

โดยการใช้งานสามารถเลือกใช้ได้สองรูปแบบดามรูป



รูปที่ 2.3 รูปแบบการใช้งาน IPsec

- Tunnel mode เป็นการนำส่วนแพ็กเก็ตเดิมทั้งหมดมาครอบด้วย IP โพรโตคอลชุดใหม่ที่เป็นไปตามชุดโพรโตคอล IPsec สังเกตได้จากมีการเพิ่มเฮดเดอร์ IP และ AH เข้าไปข้างหน้าแพ็กเก็ตชุดเดิม
- Transport mode นำเฉพาะข้อมูลของโพรโตคอล IP ซึ่งจะประกอบด้วยข้อมูลของชั้น Transport (TCP หรือ UDP) และชั้นแอพพลิเคชัน โดยเพิ่มโพรโตคอล AH และเพิ่มข้อมูลใน IP เดิมให้เหมาะสมตามมาตรฐาน IPsec

การรักษาความถูกต้องของข้อมูลของ IP ดาตาแกรม (IP Datagram) ในชุดโพรโตคอล IPsec ใช้ Hash Message Authentication Codes หรือ HMAC ด้วยฟังก์ชันแฮชเช่น MD5 หรือ SHA-1 ทุกครั้งที่มีการส่งแพ็กเก็ตจะมีการสร้าง HMAC และใช้การเข้ารหัสไปด้วยทุกครั้ง เพื่อให้ปลายทางสามารถตรวจสอบได้ตามหลักการลายเซ็นดิจิตอลว่าต้นทางเป็นผู้ส่งแพ็กเก็ตนั้นมาจริง

ส่วนการรักษาความลับของข้อมูลนั้น จะใช้การเข้ารหัส IP ดาตาแกรมด้วยวิธีการเข้ารหัสด้วยกุญแจสมมาตร ด้วยวิธีการมาตรฐานที่เป็นรู้จักกันดีเช่น 3DES AES หรือ Blowfish เป็นต้น

ปัญหาหนึ่งของ IPsec คือการส่งกุญแจที่ใช้ในการเข้ารหัสไปกับแพ็กเก็ต ซึ่งจัดว่าไม่ปลอดภัย นอกจากนี้การแลกเปลี่ยนกุญแจนำไปสู่ปัญหาของการดูแลระบบที่ใช้ IPsec เพราะทั้งระบบต้องสนับสนุนการใช้งานโพรโตคอล IPsec เดียวกัน จะทำอย่างไรให้สามารถส่งกุญแจในการเข้ารหัสไปกับแพ็กเก็ตถ้าไม่มีการเข้ารหัสแพ็กเก็ตแต่อย่างใด เพื่อแก้ปัญหาจึงได้พัฒนาโพรโตคอลในการแลกเปลี่ยนกุญแจหรือ Internet Key Exchange Protocol (IKE)

IKE จะทำการพิสูจน์ตัวตนของปลายทางก่อนการสื่อสาร ในขั้นตอนถัดมาจึงสามารถแลกเปลี่ยนและตกลง Security Association และกุญแจในการเข้ารหัสได้ด้วยวิธีการแลกเปลี่ยนกุญแจตามวิธีการแลกเปลี่ยนกุญแจด้วยการใช้กุญแจสาธารณะเช่น Diffie-Hellmann เป็นต้น ซึ่งชุดโพรโตคอล IKE จะตรวจสอบกุญแจที่ใช้ในการเข้ารหัสระหว่างการติดต่อสื่อสารเป็นระยะตลอดการสื่อสารข้อมูลที่เกิดขึ้นแต่ละครั้ง

ชุดโพรโตคอล IPsec ประกอบด้วยโพรโตคอลหลักสองโพรโตคอลคือ Authentication Header (AH) และ Encapsulated Security Payload (ESP)

AH หรือ Authentication Header ทำหน้าที่รักษาความถูกต้องของ IP ดาตาแกรม โดยการคำนวณ HMAC กับทุก IP ดาตาแกรมดามรูป

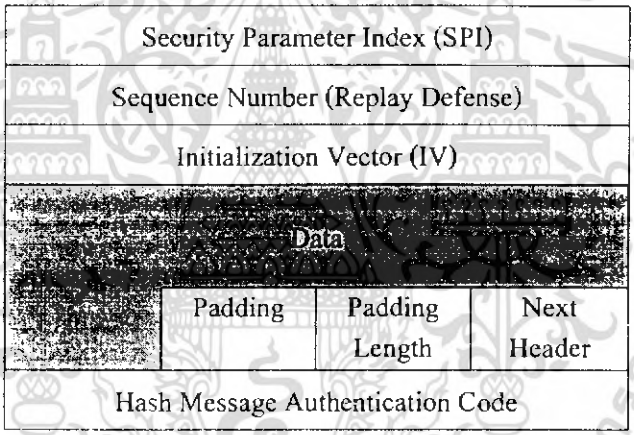
Next Header	Payload Length	Reserved
Security Parameter Index (SPI)		
Sequence Number (Replay Defense)		
Hash Message Authentication Code		

รูปที่ 2.4 Authentication Header

เฮดเดอร์ของ AH มีขนาด 24 ไบต์ อธิบายได้ดังนี้

- Next Header ใช้เพื่อบอกให้ทราบว่ากำลังใช้รูปแบบใดในการใช้งาน IPsec ระหว่าง Tunnel mode ค่าจะเป็น 4 ส่วน Transport mode ค่าจะเป็น 6
- Payload length บอกความยาวของข้อมูลที่ต่อท้ายเฮดเดอร์ ตามด้วย Reserved จำนวน 2 ไบต์
- Security Parameter Index (SPI) กำหนด Security Association สำหรับใช้ในการถอดรหัสแพ็กเก็ตเมื่อถึงปลายทาง
- Sequence Number ขนาด 32 บิตใช้บอกลำดับของแพ็กเก็ต
- Hash Message Authentication Code (HMAC) เป็นค่าที่เกิดจากฟังก์ชันแฮชเช่น MD5 หรือ SHA-1 เป็นต้น

ESP หรือ Encapsulated Security Payload ใช้สำหรับรักษาความถูกต้องของแพ็กเก็ตโดยใช้ HMAC และการเข้ารหัสร่วมด้วย



รูปที่ 2.5 Encapsulated Security Payload

- Security Parameter Index (SPI) กำหนด Security Association (SA) ระบุ ESP ที่สอดคล้องกัน
- Sequence Number ระบุลำดับของแพ็กเก็ต
- Initialization Vector (IV) ใช้ในกระบวนการเข้ารหัสข้อมูล ป้องกันไม่ให้สองแพ็กเก็ตมีการเข้ารหัสที่ซ้ำกันเกิดขึ้น
- Data คือข้อมูลที่เข้ารหัส
- Padding เป็นการเติม Data เพื่อให้ครบจำนวนไบต์ที่เข้ารหัสได้
- Padding Length บอกความยาวของ Padding ที่เพิ่ม
- Next Header กำหนดเฮดเดอร์ถัดไป
- HMAC ค่าที่เกิดจากฟังก์ชันแฮชขนาด 96 บิต

2.6 Forensics

2.6.1 Computer Forensics

2.6.1.1 พื้นฐานสำคัญที่ใช้ในการ ตรวจสอบการละเมิดสิทธิ์ และหาข้อมูล **start-up**

ตามพฤติกรรมของผู้บุกรุก หลังจากที่เข้ามาในเครื่องเราได้แล้ว ผู้บุกรุกมักจะทิ้งช่องทางเอาไว้เพื่อที่จะได้สามารถกลับเข้ามาในเครื่องเราได้อีกครั้ง และตามปกตินั้น ก็จะทำการลงโปรแกรมจะพวก rootkit หรือ อาจจะมีชุดคำสั่งที่เอาไปใส่ไว้เพื่อให้ทำงานทุกครั้งที่เปิดเครื่องขึ้นมา

โพรเซสแรกที่จะทำงานหลังจาก boot ก็คือ init โดยปกติแล้วสำหรับ ลินุกซ์นั้น init จะไปทำการอ่านค่าต่างๆ ที่ตั้งเอาไว้ที่ไฟล์ /etc/inittab ก่อน ซึ่งภายในไฟล์ก็จะกำหนดค่าที่ใช้ในการเริ่มต้นโพรเซส หลังจาก boot ระบบ และค่า ระดับการทำงานต่างๆเอาไว้ ซึ่งชี้มาจากไฟล์ /etc/rc*.d

สำหรับ /etc/rcS.d นั้นภายในโฟลเดอร์ จะเก็บไฟล์ที่จะให้ทำงานทุกครั้งเมื่อเปิดเครื่องไม่ว่าจะกำหนดค่าให้ทำงานที่ระดับใดก็ตาม โดยที่ไฟล์ที่กำหนดให้รันเมื่อเปิดเครื่องทุกครั้งจะขึ้นต้นด้วย S ส่วน ที่จะให้ทำทุกครั้งเวลาปิดเครื่อง ต้องขึ้นต้นด้วย K และ ที่ระดับต่างๆก็จะมีการกำหนดค่าให้เริ่มทำงานโปรแกรมตามที่กำหนดอีกที่ อย่างเช่นใน folder /etc/rc2.d/ ก็จะเก็บไฟล์ที่จะทำงานเมื่อระบบเริ่มต้นที กำหนดให้ใช้ระดับ2 โดยการตั้งชื่อนั้นก็จะเหมือนกันกับ rcS.d

โดยปกติแล้วไฟล์ที่ทำงานจริงๆจะเก็บเอาไว้ที่ /etc/init.d/ แต่ว่าจะทำ symbolic link เข้าไปที่ rc*.d ต่างๆแทน

Kernel Modules

จะเตรียมฟังก์ชั่นการทำงานต่างๆ เอาไว้ที่ kernel และมักจะถูกผู้บุกรุกนำไปใช้ในการควบคุมระบบของเรา โดย kernel module สามารถโหลดในตอน เริ่มเปิดเครื่องโดยใช้คำสั่ง insmod หรือ modprobe หรืออีกวิธีก็คือการใช้ kerneld ซึ่งคำสั่งหรือ modules ที่จะถูกโหลดเข้ามาตอนเปิดเครื่องนั้นโดยปกติแล้วจะถูกเก็บเอาไว้ที่ โฟลเดอร์ /lib/module/ชื่อkernel/ โดยที่ไฟล์ modules.dep จะเก็บ ว่าโมดูลใดขึ้นต่อกันบ้าง และโมดูลใดที่ต้องโหลดเข้ามาเพิ่มอีก

Data hiding

เมื่อผู้บุกรุกเข้ามาพัวพันระบบ เป็นเรื่องปกติที่จะต้องทำการสร้างไฟล์ใหม่ขึ้นมาบนระบบ แต่ว่าผู้บุกรุกนั้นก็ไม่ต้องการที่จะให้คนอื่นสามารถพบเห็นได้ง่ายๆ จึงต้องมีการใช้เทคนิคต่างๆ เพื่อช่วยในการซ่อนไฟล์

วิธีการ 2 วิธีที่ผู้บุกรุกมักใช้เป็นประจำก็คือ

1. ทำการซ่อนไฟล์ เอาไว้ในที่ ที่ผู้ใช้ปกตินั้นไม่ค่อยสนใจ และไม่สังเกต ซึ่งในระบบยูนิกซ์ นั้นที่ๆหนึ่งที่มีคุณสมบัติดังนี้ก็คือ ที่โฟลเดอร์ /dev/ ซึ่งเป็นโฟลเดอร์ที่เก็บไฟล์ไว้มากมายและหลากหลายชนิด และมีการสร้างหรือลบอยู่เกือบตลอดเวลา

2. คือเทคนิค ที่ใช้การตั้งชื่อด้วย "." ซึ่งปกติแล้วไฟล์ที่มีการตั้งชื่อด้วย "." นั้นจะไม่สามารถมองเห็นได้ถ้ามีการใช้คำสั่ง ls แบบปกติ หรืออีกทางก็คือการตั้งชื่อไฟล์ด้วยช่องว่าง

Inode

คือ โครงสร้างข้อมูล ของระบบไฟล์ ที่จะเก็บข้อมูลทั่วๆไปของไฟล์ ไดเร็คทอรี่ และอื่นๆ ซึ่งจะต้องประกอบด้วยส่วนต่างๆอย่างน้อยดังนี้

- ความยาวของไฟล์ที่มีขนาดเป็น ไบต์
- Device ID คือค่าที่ระบุบว่า อุปกรณ์ตัวไหนที่เป็นตัวเก็บไฟล์นั้นอยู่
- User ID
- Group ID
- หมายเลข inode เอาไว้ใช้ในการจำแนกแยกแยะ ไฟล์ ภายในระบบไฟล์ เมื่อไหร่ก็ตามที่โปรแกรม อ้างถึงไฟล์โดยชื่อ ระบบจะใช้ชื่อของไฟล์เพื่อไปดูค่า inode ที่เกี่ยวข้องกับไฟล์นั้น ซึ่งจะให้ข้อมูลที่ต้องการเกี่ยวกับไฟล์
- file mode เอาไว้พิจารณาว่าผู้ใช้สามารถใช้อ่าน เขียน หรือ execute ได้
- Timestamp สำหรับไฟล์ชนิดที่เป็น ext3 นั้นจะเก็บเวลาทั้งหมด 4 ชนิดคือ Modified time, Accessed, changed และ delete time ค่าที่เก็บจะเป็นค่าครั้งสุดท้ายของสิ่งนั้นๆ

- modified time เป็นเวลาครั้งสุดท้ายที่ไฟล์นั้นโดนแก้ไข ถ้ามีการเพิ่มหรือลดขนาดของไฟล์ ค่าเวลานี้ก็จะโดนแก้ไข
- accessed time คือเวลาครั้งสุดท้ายที่ ข้อมูลของไฟล์ถูกเข้าถึง อย่างเช่น ไฟล์ถูกอ่านด้วยคำสั่ง cat
- change time เป็นเวลาครั้งสุดท้าย ที่มีการเปลี่ยนแปลง inode อย่างเช่นมีการเปลี่ยนแปลง permission หรือ ขนาดของไฟล์
- delete time คือ เวลาครั้งสุดท้ายที่ไฟล์โดนลบ หรือ กลายเป็น 0 ถ้ามันไม่ได้โดนลบ

– reference count เพื่อบอกว่ามี hard link เท่าไหร่

inode สามารถใช้อ้างถึงโครงสร้างข้อมูลและ device block ที่มันจัดการอยู่ (สำหรับไฟล์ทั่วๆ ไปนั้น block ถูกสร้างขึ้นเป็น ตัวของไฟล์)

inode โดยปกติแล้วมักจะถูกอ้างถึง inode บน block device ซึ่งจัดการกับไฟล์ทั่วๆ ไป , directory และ symbolic link ซึ่งมีส่วนสำคัญในการกู้คืนไฟล์ที่เสียหายในระบบ

Delete File

สำหรับระบบเดิมอย่างเช่น ext2 นั้นเมื่อผู้ใช้ทำการลบไฟล์ ค่า inode จะยังถูกเก็บอยู่ เพียงแต่มีการตั้งค่าให้เป็นพื้นที่ ที่ไม่ได้ใช้เท่านั้นทำให้สามารถกู้คืนได้เมื่อมีการลบไป

ไฟล์ประเภท ext3 นั้นถ้ามีการลบจะทำการ เคลียร์ค่า inode และ block ทิ้งไปทั้งหมดทำให้ไม่สามารถกู้คืนกลับมาได้

Process

โดยปกติเราจะใช้คำสั่ง ps แล้วตามด้วย option ต่างๆ อย่างเช่น ps aux เพื่อใช้ในการตรวจสอบว่า มี process ใดบ้างที่กำลังทำงานอยู่บนระบบขณะนั้น เพื่อที่จะได้ตรวจสอบหาว่า มี process แปลกๆ จาก user คนไหนบ้าง แต่ว่า การใช้คำสั่งนี้ก็ยังไม่น่าเชื่อถือมากเท่าที่ควรเพราะว่าผู้บุกรุก สามารถทำให้โปรแกรมหลบซ่อนจากคำสั่ง ps ได้ โดยที่เราสามารถเข้าไปตรวจสอบที่ /proc ได้เพราะว่าคำสั่ง ps จะเป็นการไปดึงข้อมูลจาก /proc เพื่อเอาออกมาแสดง ดังนั้นเราควรตรวจสอบว่า จำนวน process ใน /proc มีจำนวนเท่ากับ คำสั่ง ps aux หรือไม่

การจัดเก็บข้อมูลใน /proc

เก็บข้อมูลเกี่ยวกับ process ตามหมายเลขที่กำหนดไว้ เช่น /proc/1234 ภายใน directory นี้จะเก็บข้อมูลเกี่ยวกับ process ที่มีหมายเลข process เป็น 1234 ไว้ ซึ่งภายในมีรายละเอียดดังนี้

1. ไฟล์ cmdline จะเก็บคำสั่งที่ process นั้นประมวลผล
2. ไฟล์ environ เก็บค่าตัวแปรสภาพแวดล้อมของ process นั้น
3. ไดเรกทอรี่ fd เก็บ symbolic link ของ file descriptor ของไฟล์ที่ process นั้นเรียกทำงาน
4. cwd Symbolic link เป็นลิงค์ที่ชี้ไปยังไดเรกทอรีที่ process ทำงานอยู่
5. exe Symbolic link เป็นลิงค์ที่ชี้ไปยัง process ที่กำลังประมวลผลอยู่
6. ไฟล์ maps เก็บส่วน memory map ของ process ซึ่งประกอบด้วยช่วงตำแหน่ง permission หรือ offset เป็นต้น
7. root Symbolic link เป็นลิงค์ที่ชี้ไปยัง root directory
8. ไฟล์ statm เก็บข้อมูลการใช้งานหน่วยความจำของ process
9. ไฟล์ stat เก็บข้อมูลรายละเอียดเกี่ยวกับ process ซึ่งมีรายละเอียดมากที่สุด
10. ไฟล์ status เก็บข้อมูลเช่นเดียวกับ stat แต่ว่าจะเข้าใจง่ายกว่า

Port

การตรวจสอบว่าเรา เปิด port อะไรอยู่บ้างนั้น ปกติแล้วเราใช้คำสั่ง netstat เพื่อตรวจสอบดู แต่บ่อยครั้งก็โดนซ่อนเช่นกัน โดยผู้บุกรุกอาจจะทำการเปิด port บาง port เพื่อเป็น backdoor เอาไว้และซ่อนจากการใช้คำสั่ง netstat ซึ่งเราก็อาจจะตรวจสอบได้โดยการใช้โปรแกรม scan port เพื่อตรวจสอบ port ที่เครื่องเปิดเอาไว้ได้

Suid,Sgid

คือไฟล์ที่มีการเซ็ตค่า sticky bit เอาไว้โดยที่ เมื่อไฟล์ใดที่มีการเซ็ตค่านี้ไว้ เมื่อมี ผู้ใช้คนอื่นที่ไม่ใช่เจ้าของไฟล์มาใช้งานไฟล์นั้น ก็จะได้สิทธิ์ เท่ากับ uid ของเจ้าของไฟล์ (โดยปกติ เมื่อเราทำการเรียกใช้โปรแกรม อะไรก็ตาม process ที่ถูกเรียกขึ้นมาจะได้ euid ซึ่งมีค่าเท่ากับ uid ของผู้เรียกไฟล์นั้น แต่เมื่อ มีการเซ็ตค่า sticky bit เข้าไป euid จะมีค่าเท่ากับ uid ของเจ้าของไฟล์) จากความสามารถดังกล่าว อาจจะทำให้ผู้บุกรุกนำไฟล์ของ root ที่มีการเซ็ตค่า sticky bit นี้ไปใช้ในการ exploit ระบบ ซึ่งเราต้องคอยตรวจสอบการเปลี่ยนแปลงของไฟล์เหล่านี้อยู่อย่างสม่ำเสมอ

ไฟล์ /etc/passwd , /etc/shadow

ทั้ง 2 ไฟล์นี้มีความสำคัญมากและควรตรวจสอบอยู่อย่างสม่ำเสมอ โดยที่ ต้องคอยดูว่ามี user เพิ่มขึ้นมาหรือมีการเปลี่ยน user id ให้มีความสามารถสูงขึ้นหรือไม่

/etc/init.d , /etc/rc*.d

ทั้ง 2 ไดเรกทอรี่นี้ จะเก็บไฟล์โปรแกรมที่จะเริ่มทำงานเมื่อเรา start เครื่อง โดยที่ผู้บุกรุกอาจจะเอาโปรแกรมไปซ่อนไว้ที่ ไดเรกทอรี่เหล่านี้ได้

crontab

คือโปรแกรมที่ใช้ตั้งเวลาการทำงานของโปรแกรมต่างๆ โดย ผู้บุกรุกอาจจะเข้าไปตั้งค่าเหล่านี้ได้เรียกให้บางโปรแกรมทำงานตามเวลาที่กำหนด

2.6.2 Network Forensics

สำหรับ การสืบหาหลักฐานทางเครือข่ายจะเป็นการหาคำตอบของคำถามต่อไปนี้

- เป็นการละเมิดสิทธิ์ หรือเป็นเพียงแค่การแจ้งเตือนที่ผิดพลาด
- ใครเป็นคนละเมิดสิทธิ์หรือใครที่เข้ามาพัวพันด้วย
- การละเมิดสิทธิ์เกิดขึ้นเมื่อเวลาใด
- อะไรคือ traffic ระหว่าง เครื่องผู้บุกรุก และเครื่องที่โดนบุกรุก
- เป็นเวลานานเท่าใดที่ผู้บุกรุกอยู่ภายในเครื่องเป้าหมาย
- รูปแบบของการกระทำการละเมิดสิทธิ์ เป็นไปในรูปแบบใด
- คำสั่งอะไรที่ ผู้ละเมิดสิทธิ์ใช้
- ผู้บุกรุกได้ทำการติดตั้งโปรแกรมประเภท rootkit หรือ backdoor ไว้หรือไม่
- อะไรเป็นสัญญาณที่บ่งบอกถึงการละเมิดสิทธิ์เริ่มแรก

Network Traffic

เมื่อมีเครื่อง 2 เครื่องที่ทำการแลกเปลี่ยนข้อมูลกันผ่านทางเครือข่าย ก็จะต้องมีการสื่อสารกันโดยผ่านทางสิ่งที่เรียกว่า โปรโตคอล เพื่อที่จะได้กำหนดค่าต่างๆของ แพ็กเก็ตที่จะแลกเปลี่ยนกันนั้น เป็นไปในรูปแบบเดียวกัน และสื่อสารกันได้อย่างเข้าใจ โดยปกติแล้ว โปรโตคอลที่นิยมใช้กันอย่างแพร่หลาย ก็คือ TCP/IP

TCP/IP ประกอบด้วย 2 โปรโตคอล คือ IP ซึ่งจะเป็นตัวที่ใช้กำหนดว่า แพ็กเก็ตนั้นมาจากที่ไหน และจะส่งไปที่ไหน ส่วน TCP นั้น เป็นตัวที่กำหนดเพื่อให้มั่นใจได้ว่าข้อมูลที่ได้รับทางปลายทางนั้น มีความถูกต้องตามลำดับ โดยที่ทั้ง 2 โปรโตคอลที่กล่าวมานั้นกระทำโดยการเพิ่มส่วนของ เฮดเดอร์ เข้าไปที่ข้อมูลที่ได้รับมาจากโปรแกรมแอปพลิเคชั่นต่างๆ

การที่จะวิเคราะห์ว่าข้อมูลที่ส่งมานั้นถูกต้องหรือไม่ ก็จำเป็นจะต้องเข้าใจ ว่า ผู้บุกรุกนั้นจะกระทำอย่างไรต่อ เฮดเดอร์ และเข้าใจ ส่วนต่างๆของเฮดเดอร์ว่ามีอะไรบ้าง

ตัวอย่างการตรวจสอบจาก header ของ โปรโตคอล

การตั้งค่าให้มีการ flagmentation ที่โปรโตคอล IP เพื่อหลีกเลี่ยงการตรวจจับของโปรแกรมที่ทำหน้าที่ป้องกันต่างๆ เพราะฉะนั้น แพ็กเก็ตที่มีขนานเล็กมาก ก็ถือว่าเป็น แพ็กเก็ตที่น่าสงสัย ซึ่งปกติแล้วขนาดของแพ็กเก็ต ไม่น่าจะต่ำกว่าครึ่งหนึ่ง ของขนาดใหญ่ที่สุดที่รับได้

การตรวจสอบค่า ttl ของแพ็กเก็ตเพื่อตรวจสอบว่าแพ็กเก็ตนั้นถูกส่งมาไกลเพียงใดและน่าจะเป็น เครื่อง ปฏิบัติการชนิดไหน โดยปกติ ระบบปฏิบัติการวินโดว์ จะใช้ค่า ttl เริ่มต้นเป็น 255 ส่วนระบบปฏิบัติการจำพวก ยูนิกซ์ จะใช้ค่า ttl เริ่มต้นเป็น 128

ค่า sequence ใช้ในการพิจารณาว่ามีการสร้าง แพ็กเก็ตของเซสชั่น นั้นใหม่หรือไม่

ค่า Header length ของโปรโตคอล ทีซีพี นั้น ปกติแล้วจะถูกสงวนเอาไว้เพื่อใช้ในอนาคต แต่ว่า บ่อยครั้งที่ถูกผู้บุกรุกนำมาใช้ในการ ติดต่อสื่อสารอย่างซ่อนเร้นกันระหว่างเครื่อง ที่โดนบุกรุก กับเครื่องของผู้บุกรุก อาจจะเป็นช่องทางที่ถูกติดตั้งไว้โดย โปรแกรม รูทคิต ต่างๆ

การจำแนก การสแกนพอร์ต

สแกนพอร์ต เป็นวิธีที่ใช้ในการตรวจสอบว่า เครื่องปลายทางนั้นเปิด พอร์ตอะไรไว้บ้าง ซึ่งมี เทคนิคมากมายในการใช้ เพื่อ สแกนพอร์ต

ตัวอย่างที่ใช้ในการ สแกนพอร์ต

SYN scan: ผู้บุกรุกสามารถตรวจสอบ พอร์ตที่เปิดอยู่ด้วยการส่ง SYN แพ็กเก็ต เข้าไปยังพอร์ตต่างๆ ถ้ามีการเปิดพอร์ตนั้นอยู่ ก็จะได้รับ SYN-ACK ตอบกลับมา ส่วน พอร์ตที่ปิดก็จะส่ง RST มาแทน ถ้าพอร์ตเปิด ผู้บุกรุกก็จะทำการส่ง RST เพื่อยกเลิกการติดต่อ

Connect scan: ผู้บุกรุกจะใช้การเชื่อมต่อ แบบสมบูรณ์เพื่อตรวจสอบ พอร์ตที่เปิดอยู่

Fin scan: เป็นการใช้ fin flag เพื่อตรวจสอบพอร์ตที่เปิดอยู่ โดยปกติไฟร์วอลล์บางชนิดจะไม่ได้ทำการปิดกั้น Fin แพ็กเก็ต ถ้าพอร์ตปิดมันจะส่ง RST กลับไป แต่ถ้าพอร์ตนั้นเปิดอยู่ เครื่องปลายทางก็จะละเลยต่อ แพ็กเก็ต Fin นั้นและไม่ตอบอะไรกลับมา

Ack scan: ใช้เพื่อค้นหา พอร์ตที่โดนตรวจสอบโดยไฟร์วอลล์ ไฟล์วอลล์บางตัวในอดีตไม่ได้ทำการปิดกั้นแพ็กเก็ต Ack ซึ่งทำให้สามารถใช้ในการแยกความแตกต่างระหว่างพอร์ตที่โดนตรวจสอบ กับไม่โดนได้ โดยที่ถ้าเป็น พอร์ตที่เปิด หรือ ปิดทั่วๆไป ยังตอบ RST กลับมา แต่ถ้าเป็น พอร์ตที่โดนกันโดยไฟร์วอลล์ จะไม่ส่งอะไรกลับมา ซึ่งอาจจะเป็น ไฟร์วอลล์ที่ไม่ใช่แบบ stateful

Passive Fingerprint

passive fingerprint เป็นวิธีที่ใช้เพื่อหาข้อมูลของเครื่องที่เราติดต่อด้วย โดยที่มีความเสี่ยงน้อยกว่าที่ผู้โดนตรวจสอบจะรู้ตัว โดยสามารถตรวจสอบ ระบบปฏิบัติการ service หรือ โปรแกรม ที่เครื่องปลายทางนั้นๆ ใช้อยู่ โดยใช้เพียงแค่การ ดักจับแพ็กเก็ตเท่านั้น

โดยปกติแล้ว fingerprint นั้นจะเป็นวิธี active ในการตรวจสอบข้อมูลของเครื่องปลายทาง อย่างเช่น การใช้โปรแกรม nmap เป็นต้น

ตัวอย่างของ TCP Passive Fingerprint

- IP Time-To-Live เป็นจำนวน hop ที่กำหนดไว้เพื่อจำกัดระยะจากต้นทางไปยังปลายทาง
- Window Size เป็นค่ากำหนดการไหลของข้อมูล ซึ่งจะแตกต่างกันตามระบบปฏิบัติการ
- DE บางระบบปฏิบัติการจะกำหนดเอาไว้ว่าไม่ให้มีการ แตกข้อมูล
- TOS การกำหนดว่าจะใช้ ชนิดไหน ขึ้นอยู่กับ ระบบปฏิบัติการ

จากด้านบนเป็นเพียงชนิดของข้อมูลจาก header ของแพ็กเก็ตที่นิยมนำมาใช้ในการพิจารณา และไม่ได้จำกัดว่าจะต้องใช้เพียงแค่ 4 ฟิลด์นี้เท่านั้น และผลที่ได้จากการพิจารณา ชนิดของระบบปฏิบัติการที่ได้มานั้นไม่อาจจะบอกได้ 100 เปอร์เซ็นต์ ว่าเป็นระบบปฏิบัติการนั้นจริงหรือไม่ ไม่มีสัญลักษณ์ใด(อย่างเดียว)ที่จะสามารถบอกได้อย่างแน่นอน แต่อย่างไรก็ตามการที่นำข้อมูลหลายๆ อย่างมารวมกันในการพิจารณา ก็สามารถเพิ่มความแม่นยำ ในการจำแนกได้

ตัวอย่างการวิเคราะห์ โดย พิจารณาจาก Icmp

โดยส่วนมากแล้ว icmp echo request จะแตกต่างกันในแต่ละระบบปฏิบัติการ โปรแกรมประเภท ping ที่ใช้กันทั่วไปใช้การสร้าง ICMP echo request ซึ่งสามารถใช้แบ่งกันได้อย่างชัดเจนระหว่าง ตระกูลยูนิกซ์ และตระกูลวินโดว์

ตัวอย่างที่ได้มาจากการวิเคราะห์

ICMP Echo Request Datagram Size: ในส่วนของระบบปฏิบัติการวินโดว์ จะใช้ขนาดความยาวเท่ากับ 60 ไบต์ ส่วนทางด้านระบบปฏิบัติการประเภท ยูนิกซ์นั้นจะใช้ขนาดเท่ากับ 84 ไบต์

ICMP Echo Request Data Payload Content: ในส่วนของระบบปฏิบัติการวินโดว์ จะส่งตัวอักษรเข้ามาใน ส่วนของ data payload ส่วนในระบบปฏิบัติการจำพวก ยูนิกซ์ นั้นจะส่งตัวเลขและอักขระพิเศษเข้ามาแทน

ICMP Echo Request Timestamp: ในผลของการ ping นั้น โดยปกติจะแสดงค่า RTT ซึ่งเป็นค่าเวลาที่คำนวณเวลาที่ใช้ไปกลับในการส่ง แพ็กเก็ต ในระบบปฏิบัติการจำพวก ยูนิกซ์ 8 ไบต์แรกของ data payload จะเป็นค่า timestamp ซึ่งช่วยเราในการหา RTT ส่วนในระบบปฏิบัติการ

จำพวกวินโดว์นั้นจะไม่มีการส่งข้อมูล timestamp มาด้วยข้อมูลจะเริ่มด้วยตัวอักษรเลย แต่ค่า timestamp นั้นจะเก็บไว้ที่ส่วนของ หน่วยความจำหลัก

ICMP Identification Number Used: ในระบบปฏิบัติการจำพวกวินโดว์นั้นใช้ค่าคงที่ 256,512 และ 768 สำหรับฟิลด์นี้ โดยค่าจะไม่มีการเปลี่ยน แต่ในระบบปฏิบัติการประเภท ยูนิกซ์นั้น ค่าที่เก็บในฟิลด์นี้จะเป็นค่าที่ถูกตั้งขึ้นมาตาม หมายเลขของโพเซสที่ ping ซึ่งจะเปลี่ยนแปลงไม่คงที่

ICMP Sequence Number ในระบบปฏิบัติการจำพวกยูนิกซ์นั้นจะเริ่มต้นค่า sequence number ด้วย ส่วนในระบบปฏิบัติการจำพวกวินโดว์นั้นจะให้ค่าเริ่มต้นเท่ากับค่าที่ใช้ครั้งล่าสุดบวกด้วย 256 และค่าจะกลับไปเริ่มที่ 0 เมื่อมีการ reboot ระบบ

ถึงแม้การตรวจสอบโดย icmp นั้นค่อนข้างจะแบ่งกันได้อย่างชัดเจนใน ตระกูลวินโดว์และยูนิกซ์ แต่ว่าก็ยังมีวิธีการที่จะใช้หลบหลีกได้เช่นกัน อย่างเช่นการใช้ hping เพื่อ ping แบบที่ไม่ให้ ระบบปฏิบัติการเป็นตัวสร้างแพ็กเก็ตให้

ในการใช้ hping2 นั้นจะไม่มีการใส่ในส่วนของข้อมูลเข้ามา ทำให้ขนาดของแพ็กเก็ตมีค่าเท่ากับ 28 ไบต์ และ ค่า ID number นั้นจะขึ้นอยู่กับหมายเลขของโพรเซสที่รันเหมือนกับ ระบบยูนิกซ์

บทที่ 3

การออกแบบและพัฒนา

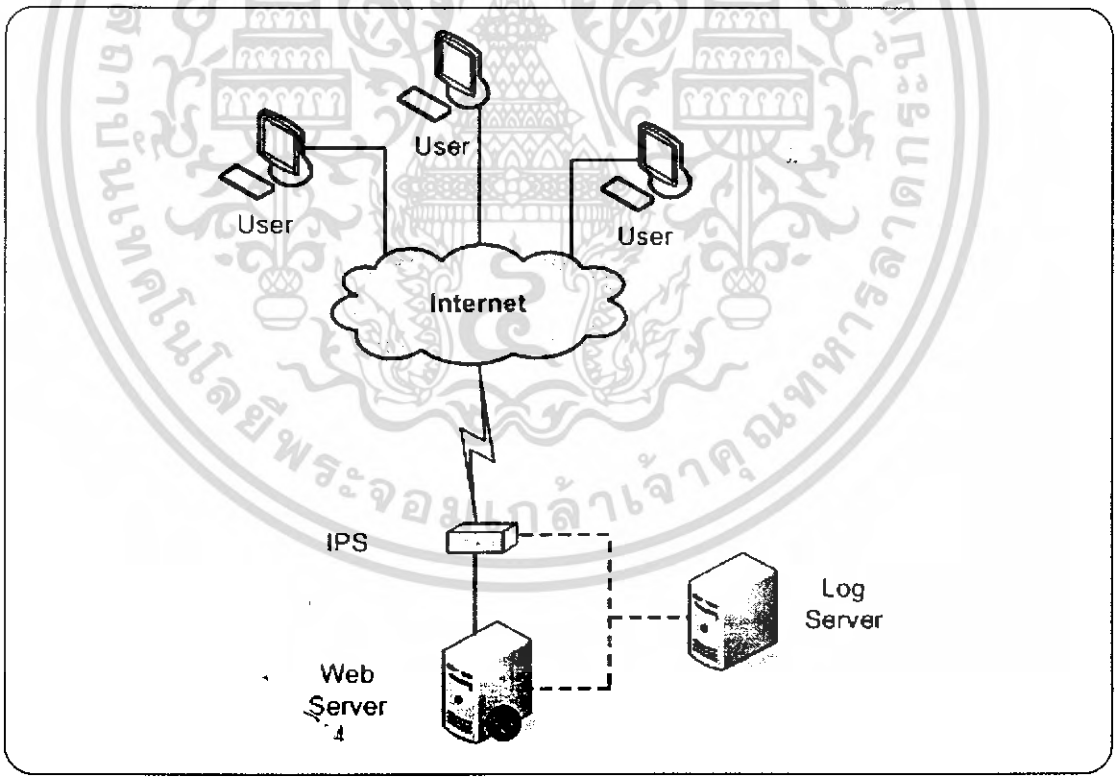
3.1 บทนำ

ในส่วนของการออกแบบและพัฒนานั้นจะต้องมีการพิจารณาถึงองค์ประกอบต่างๆ ที่จะนำมารวมและสร้างเป็นระบบขึ้น เพื่อให้ทำงานได้ตามเป้าหมายที่วางไว้ โดยในส่วนต่างๆ นั้นได้มีการพิจารณาอย่างเหมาะสม

นอกจากนั้นสิ่งสำคัญที่จะต้องนำมาพิจารณาคือ ความปลอดภัยของระบบ ทั้งนี้ระบบที่สร้างขึ้นจะต้องมีความปลอดภัยในตัวเองในระดับหนึ่ง ดังนั้นการออกแบบจึงต้องมีความรัดกุมและรอบคอบมากที่สุด โดยรายละเอียดของการออกแบบในแต่ละส่วนนั้นจะอธิบายในหัวข้อถัดไปซึ่งแยกเป็น การออกแบบฮาร์ดแวร์ และการออกแบบซอฟต์แวร์

3.2 การออกแบบฮาร์ดแวร์

โครงสร้างของระบบมีการออกแบบดังรูปภาพ



รูปที่ 3.1 แสดงโครงสร้างของระบบที่ได้ทำการออกแบบไว้

จากรูปภาพแสดงให้เห็นส่วนประกอบต่างๆ ของระบบ โดยประกอบไปด้วย

- IPS ทำหน้าที่ตรวจจับการบุกรุกและทำหน้าที่ในการตอบสนองเบื้องต้น
- Web Server เป็น Server ที่ให้บริการเว็บ
- Log Server เป็น Server สำหรับเก็บ log file ทั้งหมดที่ได้จาก IPS และ Log Server

3.3 การออกแบบซอฟต์แวร์

ในการออกแบบซอฟต์แวร์จะแบ่งออกเป็น 3 ส่วนดังนี้คือ Sensor and Audit , Forensic และ Recovery

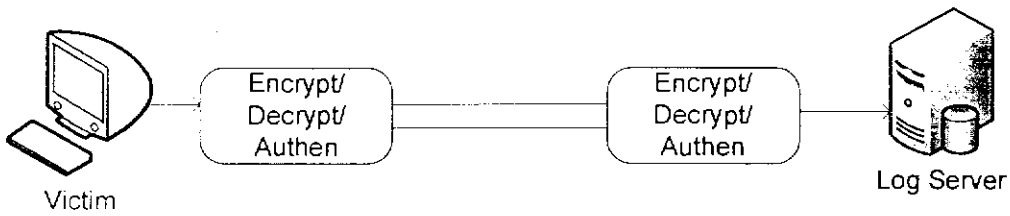
3.1.1 Sensor and Audit

การเก็บข้อมูล

เนื่องจากโดยปกติของพฤติกรรม ผู้บุกรุกนั้น เมื่อทำการละเมิดสิทธิ์ หรือ บุกรุกเข้ามาสู่เครื่องเราได้แล้วสิ่งที่จะทำต่อไปก็คือ สำรวจเก็บข้อมูล วางช่องทางเอาไว้เพื่อที่จะได้กลับเข้ามาสู่เครื่องเราอีกได้ตามที่ต้องการ และสิ่งสุดท้ายที่ผู้บุกรุกจะทำก็คือการทำลายหลักฐานเพื่อไม่ให้เจ้าของเครื่องหรือระบบรับรู้ถึงความผิดปกติ และ ถึงจะรู้ถึงสิ่งผิดปกติก็ไม่สามารถที่จะ สืบหาข้อมูล ได้ว่าเกิดอะไรขึ้นกับเครื่องบ้าง ใครเข้ามาทำอะไรเครื่องเรา และยากที่จะตัดสินใจได้ว่าควรจะแก้ไขอย่างไรจากสิ่งต่างๆดังที่ได้กล่าวมานี้จึงทำให้เกิด ระบบ centralize หรือการเก็บข้อมูลไว้ที่เครื่องกลางที่ทำหน้าที่ในการเก็บหลักฐานต่างที่ส่งมาจากเครื่องอื่นๆ เพื่อหลีกเลี่ยงการทำลายหลักฐานต่างๆ จึงได้ออกแบบให้มีการส่งข้อมูล ล็อกไฟล์ และข้อมูลทาง network หรือแม้กระทั่งข้อมูลภายในของเครื่องไปเก็บไว้ที่เครื่องกลาง ข้อมูลสำคัญต่างๆ ที่ถูกส่งไปเก็บที่เครื่องกลาง ก็เพื่อใช้ในการพิจารณาถึงการเปลี่ยนแปลงที่เกิดขึ้น และ ใช้ในการกู้คืนระบบ เมื่อระบบเกิดความเสียหาย

Secure Tunnel

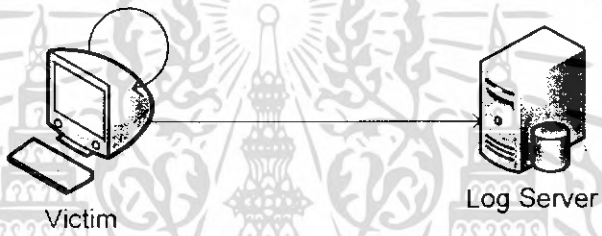
ได้ออกแบบช่องทางเพื่อใช้ในการรับส่งข้อมูล เพื่อเป็นการรองรับ CIA คือ ความถูกต้องของข้อมูลที่ส่งว่าไม่โดนแก้ไขข้อมูล มีการยืนยันทั้งทาง ผู้รับและ ผู้ส่ง ว่าเป็นผู้รับผู้ส่งที่เราต้องการจะรับส่งข้อมูลจริงๆ และมีการเข้ารหัสในช่วงที่ทำการรับส่งข้อมูล เพื่อให้เป็นความลับโดยที่ไม่โดนดักจับข้อมูลไปดูได้โดยง่าย ซึ่งจาก ความต้องการดังกล่าว จึงได้นำ IPsec เข้ามาใช้ในการรับส่งข้อมูลระหว่างเครื่องทั้ง 2 เนื่องจาก IPsec นั้นครอบคลุมทั้ง CIA คือ ความลับ และความถูกต้องของข้อมูล และมีการยืนยันว่าเป็นผู้รับ ผู้ส่ง ที่เราต้องการส่งและรับข้อมูลจริงๆ โดยมีทั้งการ เข้ารหัสข้อมูล และมาการหา HMAC เพื่อใช้ในการตรวจสอบความถูกต้องของข้อมูล และยืนยันตัวด้วยการใช้ password ที่ทั้ง 2 เครื่อง



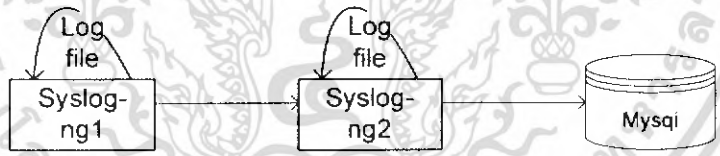
รูปที่ 3.2 แสดงการรับส่งข้อมูลผ่าน IPsec

Audit & Sensor Syslog-ng

ได้ทำการ อัพเกรด จากระบบ syslogd ที่ระบบมีให้มาเป็น syslog-ng ที่มีความสามารถที่หลากหลายกว่า เนื่องจากต้องการที่จะเก็บข้อมูลต่างๆลงฐานข้อมูล เพื่อให้ง่ายต่อการค้นหา หรือสืบหาข้อมูล ต่อไป



รูปที่ 3.3 แสดงการเก็บข้อมูลจากโปรแกรม Syslog



รูปที่ 3.4 แสดงการเก็บข้อมูลลงฐานข้อมูล

ในการทำงานนั้น จากระบบ syslog เดิมที่จะเก็บข้อมูลลง Log file ที่เครื่องตัวเองอย่างเดียวก็ให้ทำการส่งข้อมูลไปเก็บที่เครื่อง Log Server ด้วย โดยการส่งที่ผ่าน IPsec เพื่อเป็นการยืนยันผู้ส่ง ผู้รับ ข้อมูลถูกต้อง และข้อมูลที่ได้นั้นเป็นความลับ เพื่อที่จะป้องกันข้อเสียของที่ระบบเดิมๆมี และเมื่อข้อมูลเข้ามาถึงเครื่อง Log Server แล้วตัว Syslog-ng ที่เครื่อง Log Server ก็จะมารับและทำการส่งข้อมูลเข้าไปเก็บที่ใน Log file และเก็บลงฐานข้อมูล

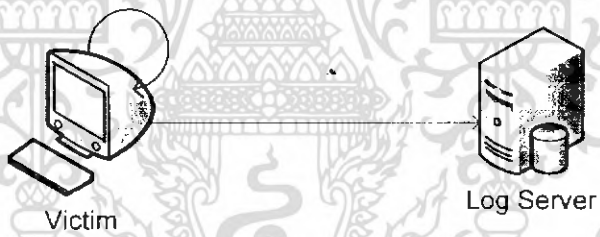
ได้ทำการออกแบบฐานข้อมูลเพื่อใช้ในการเก็บข้อมูลที่ได้มาจากโปรแกรม syslog-ng ดังนี้

```
CREATE TABLE logs ( host varchar(32) default NULL, facility varchar(10) default NULL,
        priority varchar(10) default NULL, level varchar(10) default NULL,
        tag varchar(10) default NULL, date datetime default NULL,
        program varchar(15) default NULL, msg text,
        seq int(10) unsigned NOT NULL auto_increment, PRIMARY KEY (seq),
        KEY host (host), KEY seq (seq),
        KEY program (program), KEY date(date),
        KEY priority (priority), KEY facility (facility)
        ) TYPE=MyISAM;
```

โดยที่ ตัว Sensor ที่บ่งบอกถึงความรุนแรงของเหตุการณ์ต่างๆนั้นสามารถดูได้ที่ ค่า level ต่างๆ ซึ่งได้อธิบายเอาไว้แล้วในเรื่องของ Host based IDS

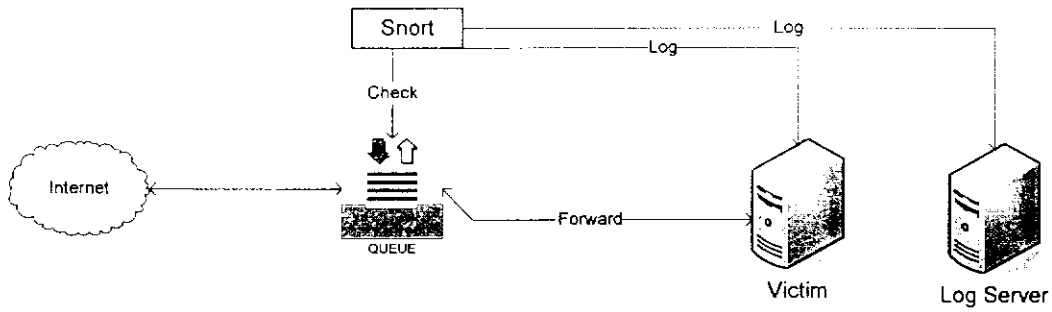
Host Integrity

สำหรับการตรวจสอบความถูกต้องของไฟล์ที่เครื่องนั้น ได้เลือกโปรแกรม samhain มาใช้ในการตรวจสอบความถูกต้องของข้อมูลที่เครื่องก่อนที่จะเก็บข้อมูลลง Log File ที่เครื่องตัวเอง และส่งไปเก็บลงฐานข้อมูลที่เครื่อง Log Server อีกทีโดยผ่าน IPsec



รูปที่ 3.5 แสดงการส่งข้อมูลไปเก็บยังเครื่อง Log Server

Audit && Sensor Network



รูปที่ 3.6 แสดงขั้นตอนการทำงานของโปรแกรม Iptables และโปรแกรม Snort

เมื่อมี packet เข้ามายังเครื่อง เซิร์ฟเวอร์ Iptables ก็จะส่งไปเข้า คิว ก่อน ไม่ว่าจะเป็นการเข้าหรือออกจากเครื่อง เพื่อให้โปรแกรม snort เข้ามาทำการตรวจสอบตัว packet นั้นๆว่า ตรงกับรูปแบบการบุกรุกหรือไม่ ถ้าตรงกับรูปแบบการบุกรุกที่เราตั้งค่าให้ drop ทิ้ง และแจ้งเตือนไปยังระบบ หรือว่าอาจจะตรงกับรูปแบบที่กำหนดให้แจ้งเตือนไปยังระบบเท่านั้น และก็ปล่อยให้ผ่านไปได้ หรือถ้าไม่ตรงกับรูปแบบการบุกรุกเลยก็คือจะปล่อยให้ผ่านไปเลย สำหรับ packet ที่ไม่ตรงกับรูปแบบใดเลยนั้น จะไม่เก็บ ข้อมูลลง Log ไฟล์ เนื่องจากข้อมูลจะมากเกินความจำเป็น

การเก็บข้อมูลที่สำคัญของเครื่อง

การเก็บข้อมูลที่สำคัญของเครื่องจะทำการเก็บไฟล์ที่สำคัญในไดเร็กทอรี่ต่อไปนี้คือ

- /etc เป็นที่เก็บรวมรวบไฟล์คอนฟิกต่างๆของระบบ
- /lib/module เป็นที่เก็บรวมรวบโมดูลที่จะถูกโหลดเข้าเคอร์เนลตอนเริ่มการทำงานของระบบปฏิบัติการ
- /bin , /usr/bin เป็นที่เก็บรวมรวมโปรแกรมสำหรับผู้ใช้งานทั่วไป
- /sbin เป็นที่เก็บรวบรวมโปรแกรมสำหรับ Super User

3.1.2 Forensic

Monitor & Forensics

สำหรับการเฝ้าดูและตรวจสอบระบบนั้นเราสามารถตรวจสอบได้จาก 3 ส่วนหลักๆ ด้วยกันคือ การดูข้อมูล จาก Host-base IDS , Network-base IDS และ Syslog-ng โดยที่แต่ละตัวจะบอกถึงความรุนแรงของเหตุการณ์ที่เกิดขึ้น และจากจุดนี้เองที่จะเป็นเหมือนจุดที่ให้เราเริ่มตรวจสอบและค้นหาหลักฐาน เมื่อเราพบว่ามีการละเมิดสิทธิ์เกิดขึ้น เราสามารถสืบหาหลักฐานได้โดยเริ่มจากโปรแกรมใดก็ได้ที่แสดงให้เห็นถึงจุดที่น่าสงสัย แต่จุดที่น่าสนใจ ที่จะแนะนำคือข้อมูลจาก Host-base IDS ที่เมื่อเรากำหนด policies ไว้ดีแล้วเราจะสามารถตรวจสอบได้ค่อนข้าง

แน่นอนว่าเกิดเหตุการณ์ที่น่าสงสัยขึ้น และค่อนข้างชัดเจนว่าเครื่องเราโดนละเมิดสิทธิ์ไปมากเพียงใดแล้ว เพราะในการตรวจสอบจากส่วนนี้ จะไม่มีข้อยกเว้นเหมือน Network-base ที่ไม่สามารถตรวจสอบเมื่อการสื่อสารระหว่างเครื่องมีการเข้ารหัสอยู่ แต่ว่าจากข้อมูลของ Host-base IDS เพียงอย่างเดียวก็ไม่สามารถบอกเราได้ว่าเกิดอะไรขึ้น และ ใครมาทำอะไร อย่างไร จึงได้มีการเปลี่ยนแปลงเกิดขึ้นกับไฟล์นั้นๆ เราจึงต้องมีการนำข้อมูล และหลักฐานที่ได้รวบรวมจากที่ต่างๆมาช่วยในการสืบหาหลักฐานต่อ คือเมื่อ ทราบว่าไฟล์มีการละเมิดสิทธิ์ โดยที่เราไม่รู้ว่าใครเป็นคนกระทำ แต่ว่าเรามีเวลาที่เกิดเหตุการณ์นั้นๆขึ้น เราสามารถเอาเวลาที่ได้มา ไปตรวจสอบว่าในช่วงเวลานี้มีใครบ้างที่ ล็อกอินอยู่ภายในระบบเรา และ เป็นการล็อกอินมาจาก เครื่องอื่น หรือว่ามีการ ล็อกอินเข้ามาผ่านเครื่องๆนั้นเอง ถ้าเป็นการล็อกอินเข้ามาจากเครื่องอื่น ก็ต้องดูต่อไปได้ว่า เครื่องนั้นมีการติดต่อกันอย่างไรบ้างกับเครื่องเรา และผู้ใช้คนนั้นมีการใช้คำสั่งอะไรบ้างในช่วงเวลาที่เค้าล็อกอินอยู่บนระบบ โดยรูปแบบการดูและค้นหาข้อมูลจะมีดังนี้

NIDS(Snort)

ส่วนแสดงผลของ จากการตรวจจับผู้บุกรุกจะมีการแสดงผลออกมาดังนี้

| Index | Signature | Priority | Timestamp | IP_src | IP_dst | Type |

โดย Signature จะบอกว่า Packet นี้เป็นรูปแบบการบุกรุกรูปแบบใด

priority จะบอกถึงความรุนแรงของรูปแบบนั้น

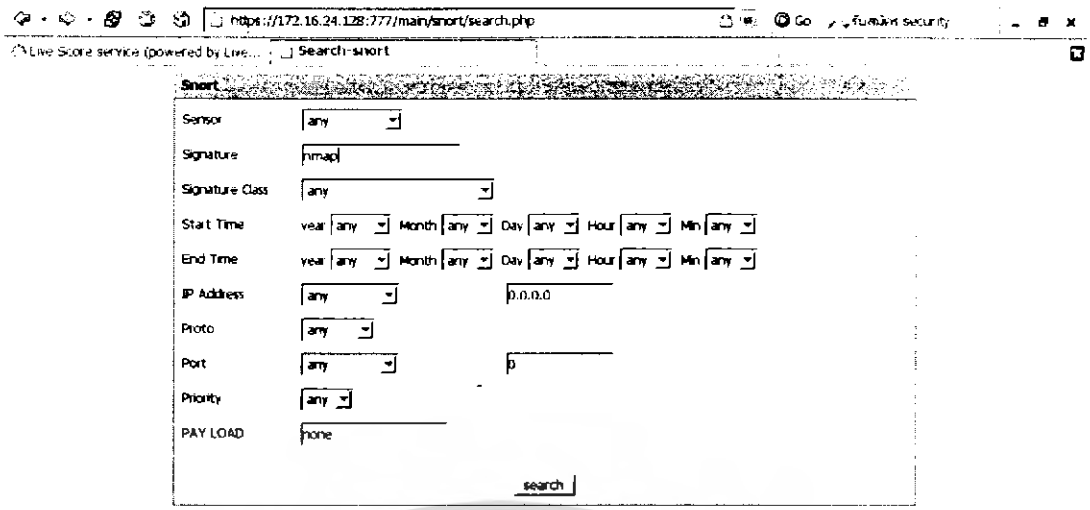
IP_src บอก IP ต้นทาง

IP_dst บอก IP ปลายทาง

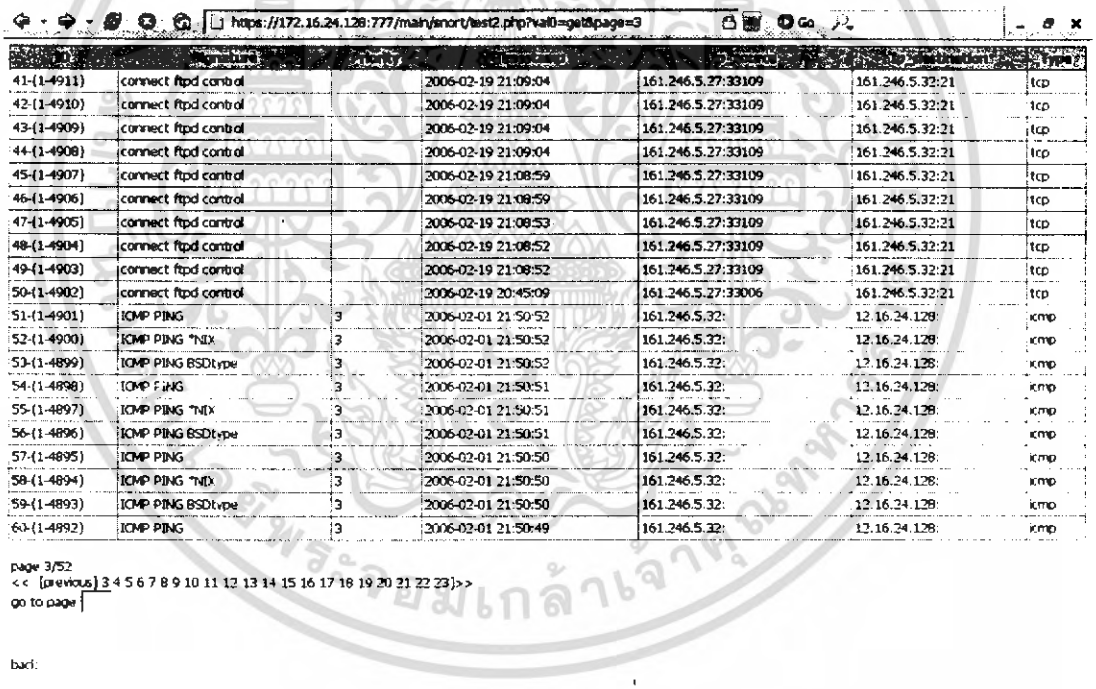
Type บอก Protocol ของแพ็กเก็ตที่ใช้ในการสื่อสาร

และสามารถดูข้อมูล data payload ได้โดยการ คลิ๊กไปที่ index

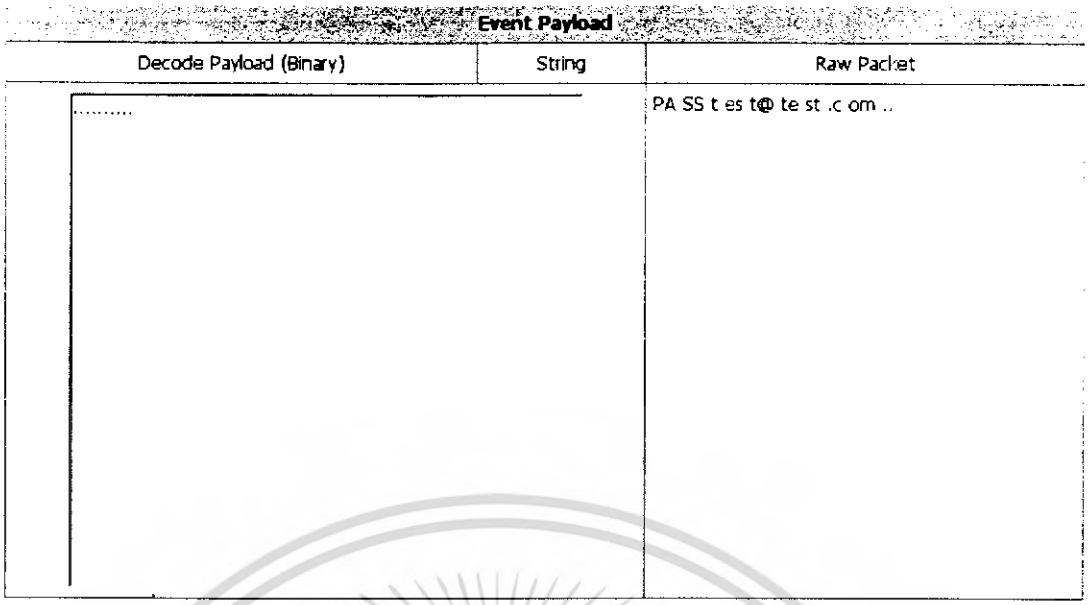
สามารถค้นหาข้อมูลจากส่วนนี้โดย query จาก sensor, signature, signature class, start time, end time, IP source, IP destination, protocol, source port, destination port, priority และ payload



รูปที่ 3.7 แสดงหน้าค้นหาข้อมูลของเครือข่าย



รูปที่ 3.8 แสดงข้อมูลทางเครือข่าย



รูปที่ 3.9 แสดงข้อมูล data payload

FILE INTEGRITY

ส่วนที่ใช้แสดงผล จากการตรวจจับการละเมิดสิทธิ์ของไฟล์ ที่เราได้กำหนดไว้มี ดังนี้

| Index | File | Policies | Owner | Severity |

โดยที่ File คือ ชื่อไฟล์ path เต็มที่โดนละเมิดสิทธิ์

Policies คือ policies ที่ไฟล์นั้นโดนละเมิดสิทธิ์

Owner คือ เจ้าของไฟล์นั้นๆ

Severity คือ ความรุนแรงในการละเมิดสิทธิ์

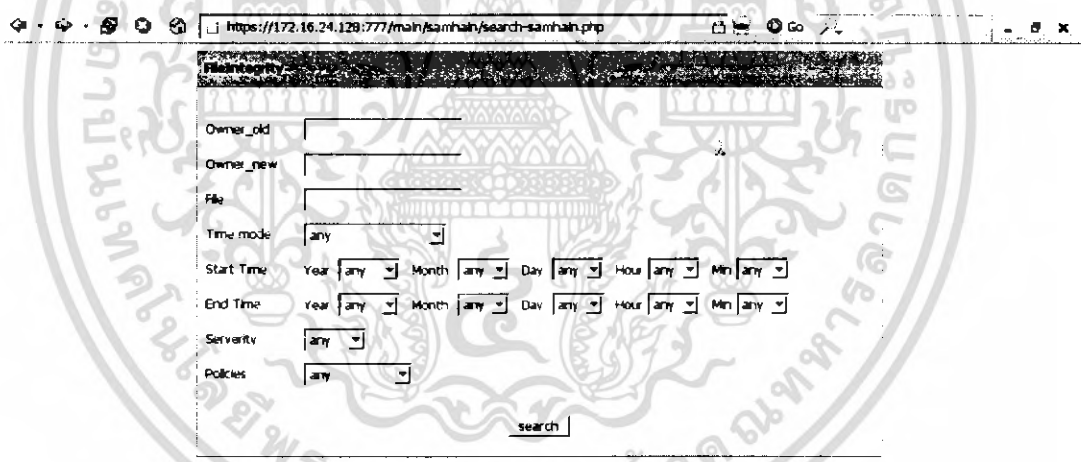
สามารถค้นหาข้อมูลจากส่วนนี้โดย query จาก File, Owner Old, Owner new, Access Time New, Access Time Old, Change Time Old, Change Time New, Modify Time Old, Modify Time New, Severity และ Policies และจากหน้าผลการค้นหาของ File Integrity สามารถเลือกให้แสดงข้อมูลของไฟล์ที่กำหนดได้ โดยหน้าแสดงข้อมูลของไฟล์จะแสดงข้อมูลดังนี้

File	**ชื่อไฟล์**
Msg	มีการละเมิดไฟล์อย่างไร
CTime-old	เวลาที่ content เปลี่ยนก่อนการละเมิด
CTime-new	เวลาที่ content เปลี่ยนหลังการละเมิด
MTime-old	เวลาที่ค่า Attribute เปลี่ยนก่อนการละเมิด
MTime-new	เวลาที่ค่า Attribute ก่อนการละเมิด

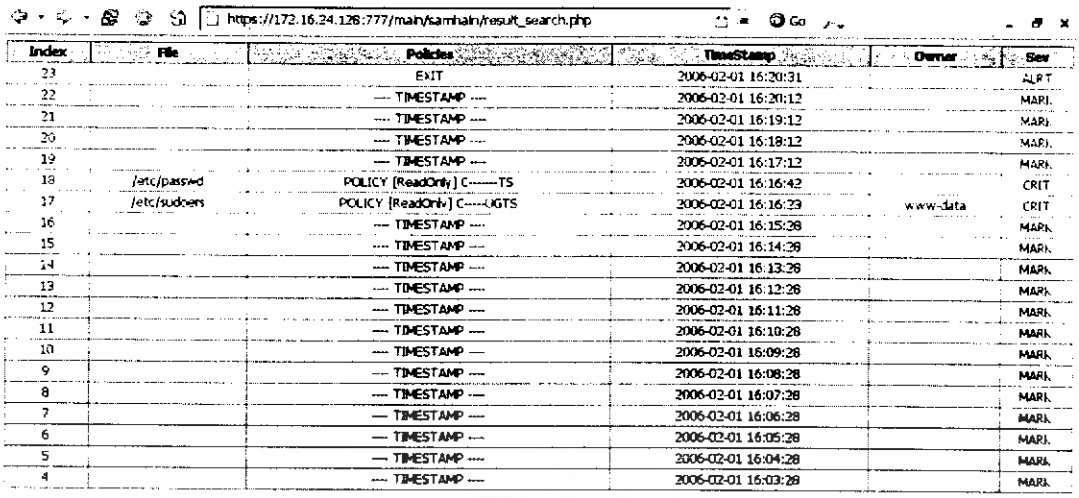
Owner-old	สิทธิ์ก่อนโดนละเมิดสิทธิ์
Owner-new	สิทธิ์หลังโดนละเมิดสิทธิ์
Attr-old	ค่าสิทธ์การเข้าถึงก่อนโดนละเมิดสิทธิ์
Attr-new	ค่าสิทธ์การเข้าถึงหลังโดนละเมิดสิทธิ์
Mode-old	ชนิดของไฟล์ก่อนโดนละเมิดสิทธิ์
Mode-new	ชนิดของไฟล์หลังโดนละเมิดสิทธิ์
Size-old	ขนาดไฟล์ก่อนโดนละเมิดสิทธิ์
Size-new	ขนาดไฟล์หลังโดนละเมิดสิทธิ์

จากหน้านี้สามารถแสดงข้อมูลที่เกี่ยวข้องดังนี้

1. ผู้ใช้ที่กำลังใช้งานระบบอยู่ในช่วงเวลานั้น
2. การตรวจสอบ directory ที่เก็บไฟล์ และสามารถเข้าไปทำการตรวจสอบไฟล์ก่อนและหลังถูกละเมิดความปลอดภัย
3. การกู้คืนเฉพาะไฟล์ที่ถูกละเมิดความปลอดภัยให้เป็นไฟล์ก่อนถูกละเมิดความปลอดภัยได้



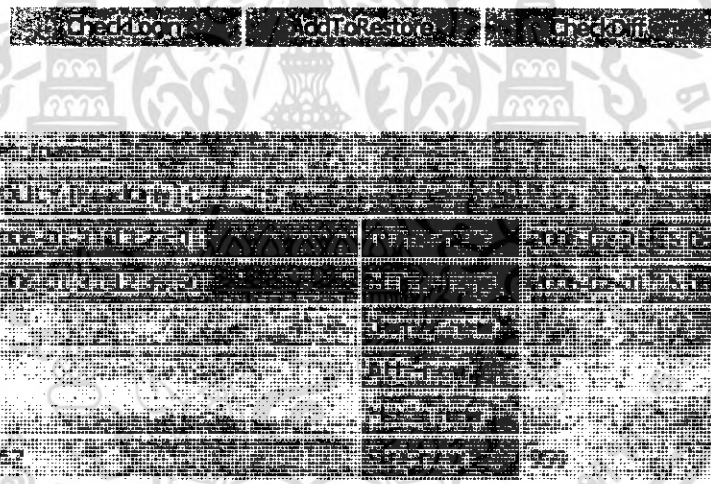
รูปที่ 3.10 แสดงหน้าค้นหาไฟล์ที่โดนละเมิดความปลอดภัย



Index	File	Policies	TimeStamp	Owner	Sev
23		EXIT	2006-02-01 16:20:31		ALRT
22		--- TIMESTAMP ---	2006-02-01 16:20:12		MARK
21		--- TIMESTAMP ---	2006-02-01 16:19:12		MARK
20		--- TIMESTAMP ---	2006-02-01 16:18:12		MARK
19		--- TIMESTAMP ---	2006-02-01 16:17:12		MARK
18	/etc/passwd	POLICY [ReadOnly] C-------TS	2006-02-01 16:16:42		CRIT
17	/etc/sudoers	POLICY [ReadOnly] C-----UGTS	2006-02-01 16:16:29	www-data	CRIT
16		--- TIMESTAMP ---	2006-02-01 16:15:28		MARK
15		--- TIMESTAMP ---	2006-02-01 16:14:28		MARK
14		--- TIMESTAMP ---	2006-02-01 16:13:28		MARK
13		--- TIMESTAMP ---	2006-02-01 16:12:28		MARK
12		--- TIMESTAMP ---	2006-02-01 16:11:28		MARK
11		--- TIMESTAMP ---	2006-02-01 16:10:28		MARK
10		--- TIMESTAMP ---	2006-02-01 16:09:28		MARK
9		--- TIMESTAMP ---	2006-02-01 16:08:28		MARK
8		--- TIMESTAMP ---	2006-02-01 16:07:28		MARK
7		--- TIMESTAMP ---	2006-02-01 16:06:28		MARK
6		--- TIMESTAMP ---	2006-02-01 16:05:28		MARK
5		--- TIMESTAMP ---	2006-02-01 16:04:28		MARK
4		--- TIMESTAMP ---	2006-02-01 16:03:28		MARK

รูปที่ 3.11 แสดงผลรายชื่อไฟล์ทั้งหมดที่โดนละเมิดความปลอดภัย

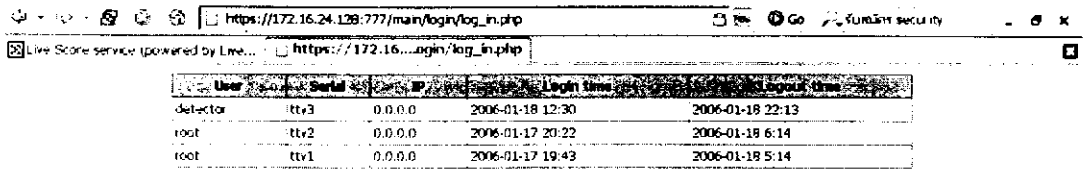
จากรูปที่ 3.11 เมื่อคลิ้กที่ Index ของไฟล์ที่ถูกละเมิดความปลอดภัยจะเป็นการแสดงข้อมูลต่างๆ ของไฟล์ที่โดนละเมิดความปลอดภัย



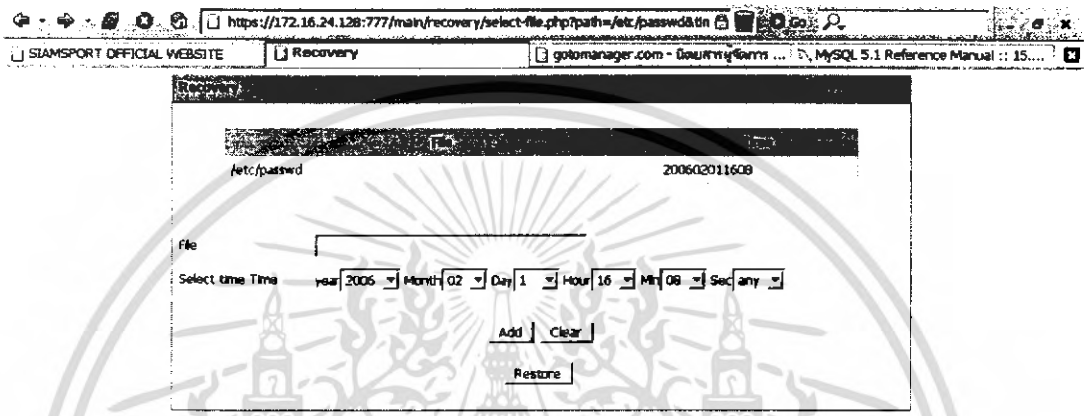
รูปที่ 3.12 แสดงข้อมูลของไฟล์ที่โดนละเมิดความปลอดภัย

จากรูปที่ 3.12 สามารถตรวจสอบข้อมูลที่มีความสัมพันธ์กับไฟล์ที่ถูกละเมิดความปลอดภัย และตอบสนองต่อการละเมิดความปลอดภัยได้ดังนี้คือ

1. CheckLogin จะทำการค้นหาผู้ใช้ที่ใช้งานระบบอยู่ในช่วงเวลาที่ไฟล์มีการเปลี่ยนแปลง
2. AddToRestore เพื่อทำการ กู้คืนไฟล์ให้เป็นค่าเดิม
3. CheckDiff เพื่อตรวจสอบโฟลเดอร์ที่เก็บไฟล์ก่อนถูกละเมิดความปลอดภัยและหลังถูกละเมิดความปลอดภัย



รูปที่ 3.13 แสดงรายชื่อผู้ใช้ที่ใช้งานระบบอยู่ในเวลาเดียวกันกับเวลาที่ไฟล์ /etc/passwd โดนละเมิดความปลอดภัย



รูปที่ 3.14 แสดงการกู้คืนไฟล์ที่โดนละเมิดความปลอดภัย

Syslog-ng

ส่วนที่ใช้แสดงผลที่ได้จากการเก็บข้อมูลของระบบ มีดังนี้

| Prog | Msg | Time | Priority | Host Facility |

โดยที่ Prog คือ ชื่อโปรแกรมที่ส่งข้อความแจ้งมายังระบบ

Msg คือ ข้อความที่แจ้งมา

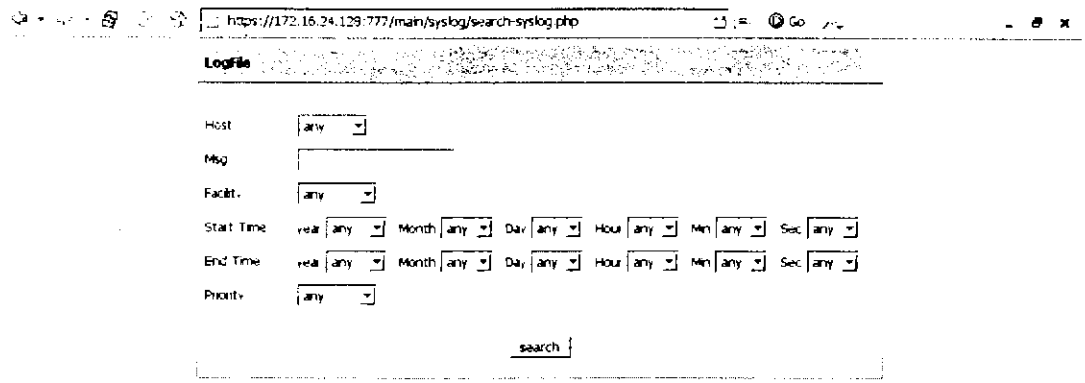
Time คือ เวลาที่ส่งเข้ามา

Priority คือ ความรุนแรงของข้อความที่แจ้งเตือนมา

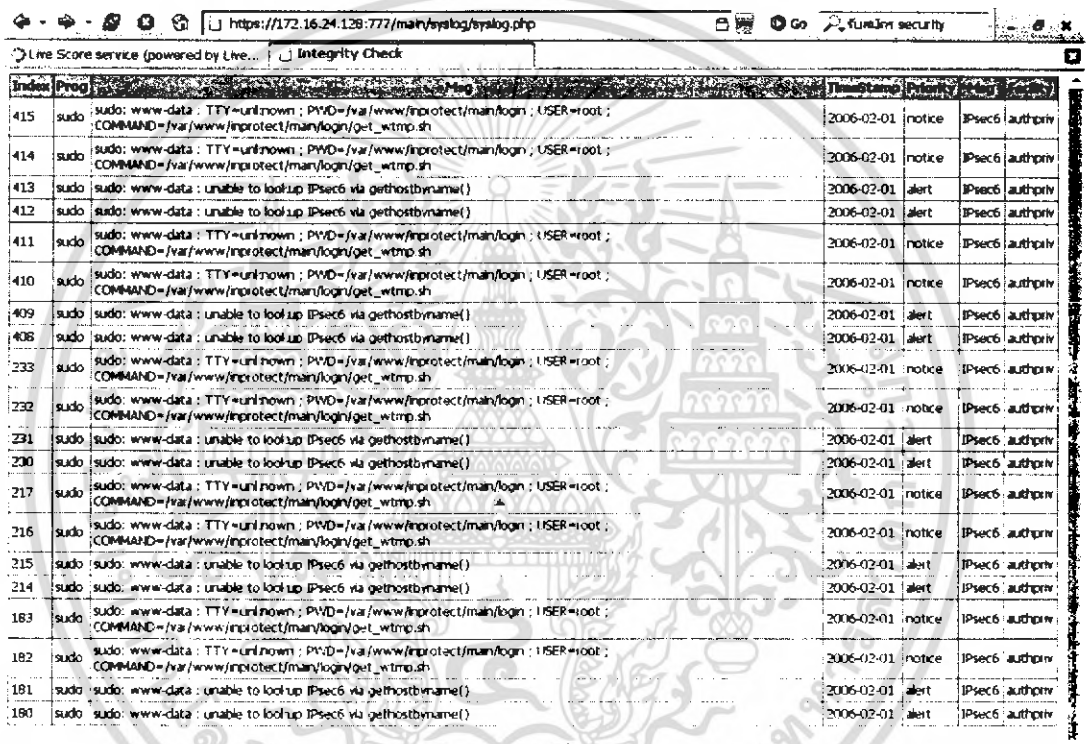
Host คือ เครื่องที่ส่งเข้ามาเก็บยัง Log Server

Facility คือ ระดับหรือชนิดอย่างเช่น kernel auth เป็นต้น

ส่วนข้อมูลเกี่ยวกับการ login และ command ที่ผู้ใช้ได้ใช้งานจะถูกแสดงแยกอีกที่สามารถค้นหาข้อมูลได้จาก Host, Msg, Facility, Start time, End time และ priority



รูปที่ 3.15 แสดงหน้าสำหรับค้นหาข้อมูลจากล็อกไฟล์



รูปที่ 3.16 แสดงข้อมูลทั้งหมดจาก ล็อกไฟล์

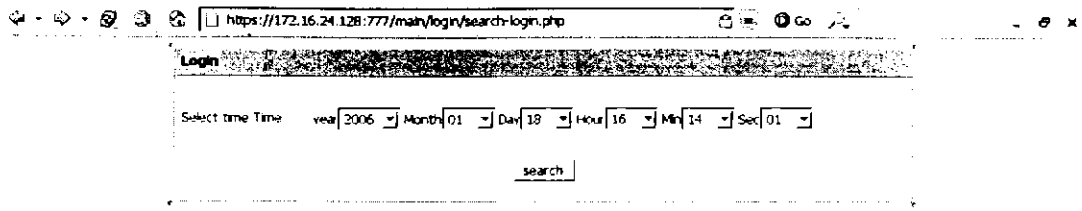
Login

- **ส่วนที่แสดงให้ดูคือ**

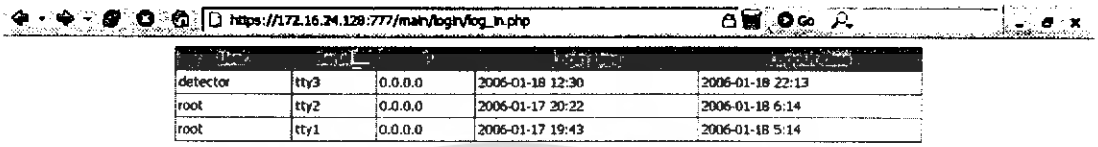
  | User | serial | Login Time | Logout Time |

ในส่วนนี้เราต้องกำหนดเวลาที่เราต้องการดู เมื่อป้อนเวลา ก็จะได้ผลลัพธ์เป็นผู้ใช้ที่ล็อกอินอยู่ในช่วงเวลานั้นๆ และสามารถแสดงข้อมูลที่เกี่ยวข้องดังนี้ได้

1. **สามารถดูข้อมูลการใช้คำสั่งของผู้ใช้แต่ละคน ในช่วงเวลาที่ใช้งานระบบ จาก เทอร์มินอล นั้นๆได้**
2. **สามารถดู แพ็กเก็ต ที่เข้า หรือ ออก จากเครื่องนั้นๆ ได้**



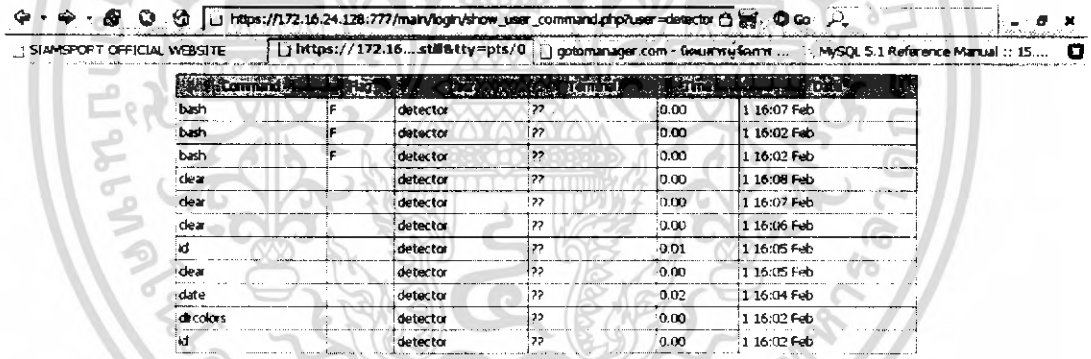
รูปที่ 3.17 แสดงการค้นหาผู้ใช้งานที่ใช้ระบบในช่วงเวลาที่กำหนด



รูปที่ 3.18 แสดงรายชื่อผู้ใช้งานที่ใช้งานระบบในเวลาที่กำหนด

จากรูปด้านบน สามารถตรวจสอบข้อมูลที่เกี่ยวข้องกันได้ดังนี้

1. คำสั่งที่ผู้ใช้งานใช้ในขณะที่เข้าใช้งานระบบ สามารถทำการตรวจสอบต่อได้โดยคลิ๊กที่ชื่อผู้ใช้
2. ข้อมูลทางเครือข่ายของเครื่องนั้น สามารถทำการตรวจสอบต่อได้โดยคลิ๊กที่ IP Address



รูปที่ 3.19 แสดงคำสั่งของผู้ใช้ detector ในช่วงเวลาที่กำหนด

3.1.3 Recovery

ในส่วนของการเตรียมการเพื่อทำการกู้คืนระบบนั้นได้ออกแบบการทำงานของระบบออกเป็น 2 ส่วนคือ

ส่วนที่ 1 เป็นส่วนที่ทำการเก็บ snapshot ของ directory ต่างๆ

ในส่วนนี้ได้เลือกใช้โปรแกรม Rsync มาเป็นเครื่องมือสำหรับทำการถ่ายโอนข้อมูลจากเครื่อง Response Wall มาเก็บยังเครื่อง Log Server และทำการบีบอัดด้วยโปรแกรม BZip2 ซึ่งจะทำให้ไฟล์ Snapshot มีขนาดเล็กลงเพื่อเป็นการประหยัดเนื้อที่

คุณสมบัติของโปรแกรม Rsync

- มี Difference Search Algorithm ทำให้สามารถทำ Incremental Backup ได้
- Owner group และ modify time ของไฟล์ต้นฉบับไม่เปลี่ยนแปลง
- มีการบีบอัดไฟล์ก่อนที่จะทำการส่งผ่านเครือข่าย ทำให้สามารถลดความหนาแน่นเนื่องจากปริมาณข้อมูลของเครือข่ายได้

ในการเก็บ Snapshot ได้ออกแบบให้ผู้ดูแลระบบสามารถเลือกระยะเวลาของการเก็บ Snapshot โดยแบ่งเป็นการเก็บแบบหยาบ (Main step) และการเก็บแบบละเอียด (Sub step)

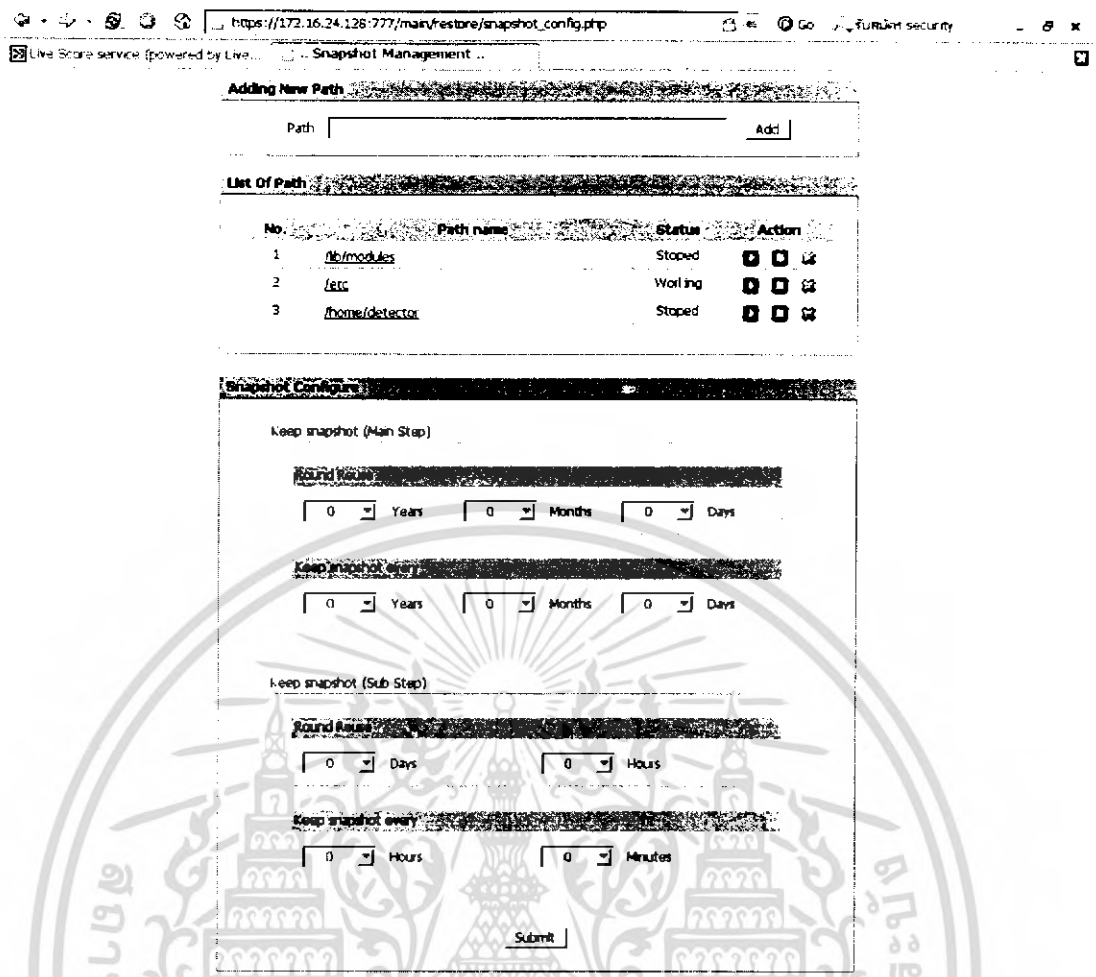
ข้อดีของการเก็บแบบหยาบคือ ประหยัดเนื้อที่ ลด traffic และงานของเครื่อง Response Wall และ Log Server

ข้อดีของการเก็บแบบละเอียดคือ สามารถจัดเก็บไฟล์ที่ใกล้เคียงกับระบบเดิมมากที่สุด โดยเฉพาะในช่วงวิกฤติซึ่งเป็นช่วงเวลาที่ตรวจพบการเริ่มการบุกรุกหรือละเมิดความปลอดภัย จะช่วยทำให้ลดผลกระทบที่อาจเกิดขึ้นกับผู้ใช้ระบบคนอื่นๆ เนื่องจากการกู้คืนระบบ

ในการเลือกหรือปรับแต่งค่าการเก็บ Snapshot นั้นจะอยู่ในรูปของระยะเวลาโดยผู้ดูแลระบบสามารถเลือกได้ว่า จะให้เก็บ Snapshot เป็นระยะเวลาเท่าใด และเก็บทุกๆ ช่วงเวลาเท่าไหร่ ซึ่งโปรแกรมที่ได้ทำการออกแบบไว้จะทำการคำนวณจำนวนของไฟล์ Snapshot ที่จะเก็บให้โดยอัตโนมัติ

ส่วนที่ 2 เป็นส่วนของการกู้คืนระบบ

ในส่วนนี้ได้ทำการออกแบบให้ระบบสามารถทำการวิเคราะห์และค้นหาไฟล์ต้นฉบับที่เหมาะสมจาก Snapshot ที่ได้จัดเก็บไว้ และนำมาเสนอให้กับผู้ดูแลระบบเพื่อการตัดสินใจต่อไป ทั้งนี้จุดเด่นของระบบที่ได้ทำการออกแบบก็คือ การกู้คืนระบบแบบ Selective Restore โดยผู้ดูแลระบบสามารถที่จะเลือกไฟล์ที่ต้องการจะ Restore ได้ จึงไม่มีความจำเป็นที่จะต้องทำการกู้คืนระบบใหม่ทั้งหมด ทำให้สามารถประหยัดเวลา ลดปริมาณข้อมูลที่ต้องผ่านเครือข่าย และลดผลกระทบที่อาจจะเกิดขึ้นกับผู้ใช้งานระบบอื่นๆ



รูปที่ 3.20 แสดงหน้า Snapshot Management

จากรูปที่ 3.20 แสดงในส่วนของการบริหารจัดการการเก็บ Sanpshot ซึ่งแบ่งการทำงานเป็นส่วนๆ โดยแต่ละส่วนมีคุณสมบัติดังนี้คือ

1. Adding New Path เป็นส่วนสำหรับการเพิ่ม Path ที่จะให้ระบบทำการเก็บ Snapshot
2. List Of Path เป็นส่วนที่แสดงรายชื่อและสถานะการเก็บ Snapshot ของ Path ที่กำหนด โดยในส่วนนี้สามารถควบคุมการเก็บ Snapshot ดังนี้คือ
   - ปุ่ม Start สำหรับการสั่งให้เริ่มเก็บ Snapshot
   - ปุ่ม Stop สำหรับการสั่งให้หยุดการเก็บ Snapshot
   - ปุ่ม Remove สำหรับการยกเลิกการเก็บ Snapshot และลบไฟล์ Snapshot
3. Snapshot Configure เป็นส่วนที่กำหนดการเก็บ Snapshot
   - Keep Snapshot (Main Step) เป็นการกำหนดการเก็บ Snapshot แบบหยาบโดยมีรายละเอียดดังนี้คือ
     - Round Reuse เป็นการกำหนดช่วงเวลาของไฟล์ Snapshot ที่จะวนทับไฟล์เดิม
     - Keep Snapshot Every เป็นการกำหนดวงรอบการเก็บ Snapshot โดยวงรอบต่ำสุดคือ 1 วัน

- Keep Snapshot (Sub Step) เป็นการกำหนดการเก็บ Snapshot แบบละเอียดโดยมีรายละเอียดดังนี้คือ
  - Round Reuse เป็นการกำหนดช่วงเวลาของไฟล์ Snapshot ที่จะวนทับไฟล์เดิม
  - Keep Snapshot Every เป็นการกำหนดวงรอบการเก็บ Snapshot โดยวงรอบต่ำสุดคือ 1 นาที

หลังจากที่ได้ทำการปรับแต่งค่าการทำงานของการเก็บ Snapshot และกดปุ่ม Submit แล้ว การเปลี่ยนแปลงดังกล่าวจะมีผลกับการทำงานของระบบการเก็บ Snapshot ในทันทีโดยไม่ต้องสั่งให้หยุดแล้วเริ่มการเก็บ Snapshot ใหม่

บทที่ 4

การทดลองและผลการทดลอง

4.1 บทนำ

ในการทดลองจะเป็นการทดสอบระบบที่ได้สร้างขึ้นโดยแยกการทดสอบออกเป็น 4 การทดสอบ คือ

1. ทดสอบการเก็บข้อมูลทางด้านเครือข่าย
2. ทดสอบการเก็บข้อมูลจากเครื่องคอมพิวเตอร์
3. ทดสอบการแจ้งเตือนและวิเคราะห์
4. ทดสอบการกู้คืนระบบ
5. ทดสอบระบบโดยการจำลองสถานการณ์จริง

4.2 การทดสอบที่ 1 การเก็บข้อมูลทางด้านเครือข่าย

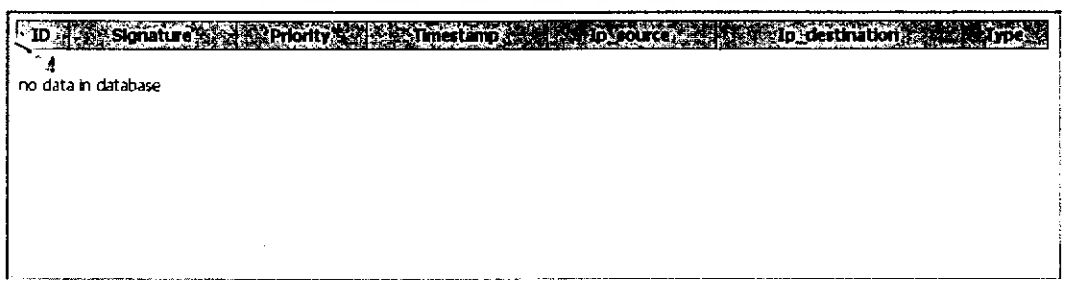
4.2.1 วิธีการทดสอบ

1) ทำการติดตั้งโปรแกรม Snort-Inline หลังจากนั้นปรับแต่งค่าคอนฟิกต่างๆ เพื่อให้โปรแกรมทำงานมีประสิทธิภาพมากขึ้นโดยการเพิ่มกฎ (rule) ต่างๆ ปรับแต่งให้โปรแกรมทำการส่งข้อมูลไปเก็บยังเครื่อง Log Server ปรับแต่งให้มีการแจ้งเตือนเมื่อพบแพ็กเก็ตที่น่าสงสัยว่าจะเป็นการละเมิดความปลอดภัยหรือการบุกรุก
2) เปิดระบบและเริ่มเก็บข้อมูลจากเครือข่าย และส่งข้อมูลทั้งหมดไปเก็บในฐานข้อมูลที่อยู่บนเครื่อง Log Server ผ่าน IPsec
3) ตรวจสอบการทำงานโดยใช้ส่วนแสดงผล สังเกตผลที่เกิดขึ้นและเปรียบเทียบระหว่างก่อนเริ่มเก็บข้อมูลและหลังจากทำการเก็บข้อมูลแล้ว

4.2.2 ผลการทดสอบ

จากการทดสอบพบว่า

1) ในฐานข้อมูลที่เครื่อง Log Server มีข้อมูลที่ได้จากโปรแกรม Snort-Inline
2) ปริมาณข้อมูลในฐานข้อมูลมีการเพิ่มขึ้นในขณะที่ทำการเปิดระบบค้างไว้



รูปที่ 4.1 แสดงการแสดงผลโดยที่ยังไม่มีการเริ่มเก็บข้อมูล

ID	Signature	Priority	Timestamp	Ip_source	Ip_destination	Type
41-(1-4911)	connect ftpd control		2006-02-19 21:09:04	161.246.5.27:33109	161.246.5.32:21	tcp
42-(1-4910)	connect ftpd control		2006-02-19 21:09:04	161.246.5.27:33109	161.246.5.32:21	tcp
43-(1-4909)	connect ftpd control		2006-02-19 21:09:04	161.246.5.27:33109	161.246.5.32:21	tcp
44-(1-4908)	connect ftpd control		2006-02-19 21:09:04	161.246.5.27:33109	161.246.5.32:21	tcp
45-(1-4907)	connect ftpd control		2006-02-19 21:08:59	161.246.5.27:33109	161.246.5.32:21	tcp
46-(1-4906)	connect ftpd control		2006-02-19 21:08:59	161.246.5.27:33109	161.246.5.32:21	tcp
47-(1-4905)	connect ftpd control		2006-02-19 21:08:53	161.246.5.27:33109	161.246.5.32:21	tcp
48-(1-4904)	connect ftpd control		2006-02-19 21:08:52	161.246.5.27:33109	161.246.5.32:21	tcp
49-(1-4903)	connect ftpd control		2006-02-19 21:08:52	161.246.5.27:33109	161.246.5.32:21	tcp
50-(1-4902)	connect ftpd control		2006-02-19 20:45:09	161.246.5.27:33006	161.246.5.32:21	tcp
51-(1-4901)	ICMP PING	3	2006-02-01 21:50:52	161.246.5.32:	12.16.24.128:	icmp
52-(1-4900)	ICMP PING *NIX	3	2006-02-01 21:50:52	161.246.5.32:	12.16.24.128:	icmp
53-(1-4899)	ICMP PING BSDtype	3	2006-02-01 21:50:52	161.246.5.32:	12.16.24.128:	icmp
54-(1-4898)	ICMP PING	3	2006-02-01 21:50:51	161.246.5.32:	12.16.24.128:	icmp
55-(1-4897)	ICMP PING *NIX	3	2006-02-01 21:50:51	161.246.5.32:	12.16.24.128:	icmp
56-(1-4896)	ICMP PING BSDtype	3	2006-02-01 21:50:51	161.246.5.32:	12.16.24.128:	icmp
57-(1-4895)	ICMP PING	3	2006-02-01 21:50:50	161.246.5.32:	12.16.24.128:	icmp
58-(1-4894)	ICMP PING *NIX	3	2006-02-01 21:50:50	161.246.5.32:	12.16.24.128:	icmp
59-(1-4893)	ICMP PING BSDtype	3	2006-02-01 21:50:50	161.246.5.32:	12.16.24.128:	icmp
60-(1-4892)	ICMP PING	3	2006-02-01 21:50:49	161.246.5.32:	12.16.24.128:	icmp

Event Payload

Decode Payload (Binary)	String	Raw Packet
.....		PA SS t es t@ te st .c om ..

รูปที่ 4.2 แสดงข้อมูลที่ได้หลังจากทำการเก็บข้อมูลจากเครือข่าย

```
 ESP(spi=0x000022b8,seq=0x4d83), length 88
06:30:24.549151 IP 172.16.24.128 > 172.16.24.130: AH(spi=0x00000457,seq=0x4603):
 ESP(spi=0x00001e61,seq=0x4603), length 88
06:30:24.551636 IP 172.16.24.130 > 172.16.24.128: AH(spi=0x000008ae,seq=0x4d84):
 ESP(spi=0x000022b8,seq=0x4d84), length 88
06:30:25.560984 IP 172.16.24.128 > 172.16.24.130: AH(spi=0x00000457,seq=0x4604):
 ESP(spi=0x00001e61,seq=0x4604), length 88
06:30:25.561480 IP 172.16.24.130 > 172.16.24.128: AH(spi=0x000008ae,seq=0x4d85):
 ESP(spi=0x000022b8,seq=0x4d85), length 88
06:30:26.548844 IP 172.16.24.128 > 172.16.24.130: AH(spi=0x00000457,seq=0x4606):
 ESP(spi=0x00001e61,seq=0x4605), length 88
06:30:26.549261 IP 172.16.24.130 > 172.16.24.128: AH(spi=0x000008ae,seq=0x4d87):
 ESP(spi=0x000022b8,seq=0x4d87), length 88
06:30:28.568329 IP 172.16.24.128 > 172.16.24.130: AH(spi=0x00000457,seq=0x4607):
 ESP(spi=0x00001e61,seq=0x4607), length 88
06:30:28.568441 IP 172.16.24.130 > 172.16.24.128: AH(spi=0x000008ae,seq=0x4d88):
 ESP(spi=0x000022b8,seq=0x4d88), length 88
06:30:29.587340 IP 172.16.24.128 > 172.16.24.130: AH(spi=0x00000457,seq=0x4608):
 ESP(spi=0x00001e61,seq=0x4608), length 88
06:30:29.587916 IP 172.16.24.130 > 172.16.24.128: AH(spi=0x000008ae,seq=0x4d89):
 ESP(spi=0x000022b8,seq=0x4d89), length 88
06:30:30.564213 IP 172.16.24.128 > 172.16.24.130: AH(spi=0x00000457,seq=0x4609):
 ESP(spi=0x00001e61,seq=0x4609), length 88
06:30:30.565060 IP 172.16.24.130 > 172.16.24.128: AH(spi=0x000008ae,seq=0x4d8a):
 ESP(spi=0x000022b8,seq=0x4d8a), length 88
06:30:31.505128 IP 172.16.24.128 > 172.16.24.130: AH(spi=0x00000457,seq=0x460a):
 ESP(spi=0x00001e61,seq=0x460a), length 88
06:30:31.505648 IP 172.16.24.130 > 172.16.24.128: AH(spi=0x000008ae,seq=0x4d8b):
 ESP(spi=0x000022b8,seq=0x4d8b), length 88
```

รูปที่ 4.3 แสดงการเข้ารหัสและตรวจสอบความถูกต้องของข้อมูลโดยผ่าน IPsec

4.3 การทดสอบที่ 2 การเก็บข้อมูลจากเครื่องคอมพิวเตอร์

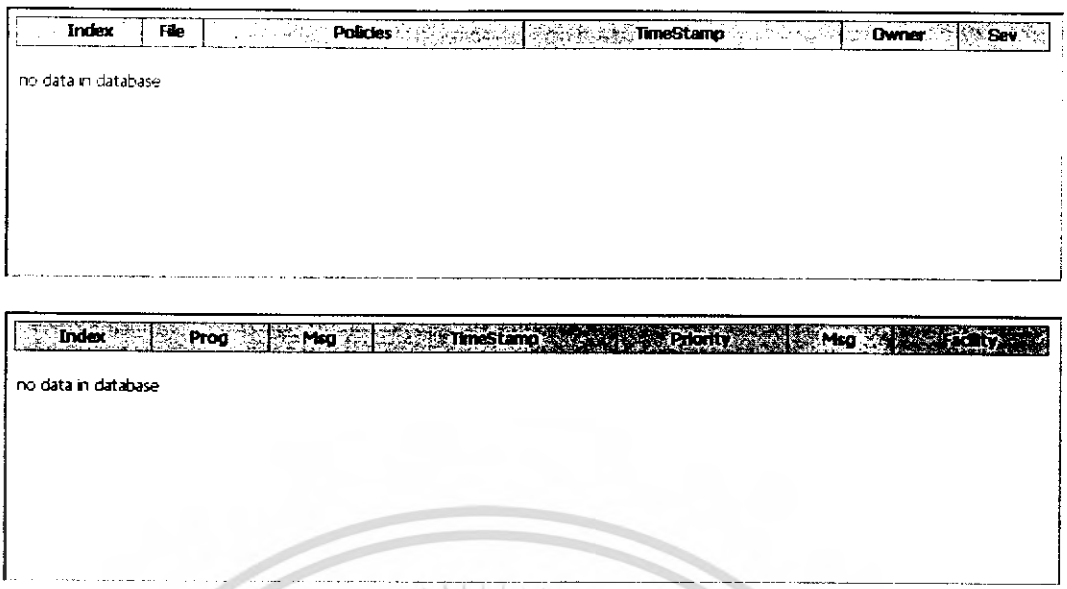
4.3.1 วิธีการทดสอบ

1) ทำการติดตั้งโปรแกรม Syslog-ng และโปรแกรม Samhain หลังจากนั้นปรับแต่งค่าคอนฟิกต่างๆ เพื่อให้โปรแกรมทำงานมีประสิทธิภาพมากขึ้น ปรับแต่งให้โปรแกรมทำการส่งข้อมูลไปเก็บยังเครื่อง Log Server ปรับแต่งให้มีการตรวจสอบไฟล์ต่างๆ ตามที่กำหนด
2) เปิดระบบและเริ่มเก็บข้อมูลจากเครื่อง Response wall และส่งข้อมูลทั้งหมดไปเก็บในฐานข้อมูลที่อยู่บนเครื่อง Log Server ผ่าน IPsec
3) ตรวจสอบการทำงานโดยใช้ส่วนแสดงผล สังเกตผลที่เกิดขึ้นและเปรียบเทียบระหว่างก่อนเริ่มเก็บข้อมูลและหลังจากทำการเก็บข้อมูลแล้ว

4.3.2 ผลการทดสอบ

จากการทดสอบพบว่า

1) ในฐานข้อมูลที่เครื่อง Log Server มีข้อมูลที่ได้จากโปรแกรม Syslog-ng และโปรแกรม Samhain
2) ปริมาณข้อมูลในฐานข้อมูลมีการเพิ่มขึ้นในขณะที่ทำการเปิดระบบไว้



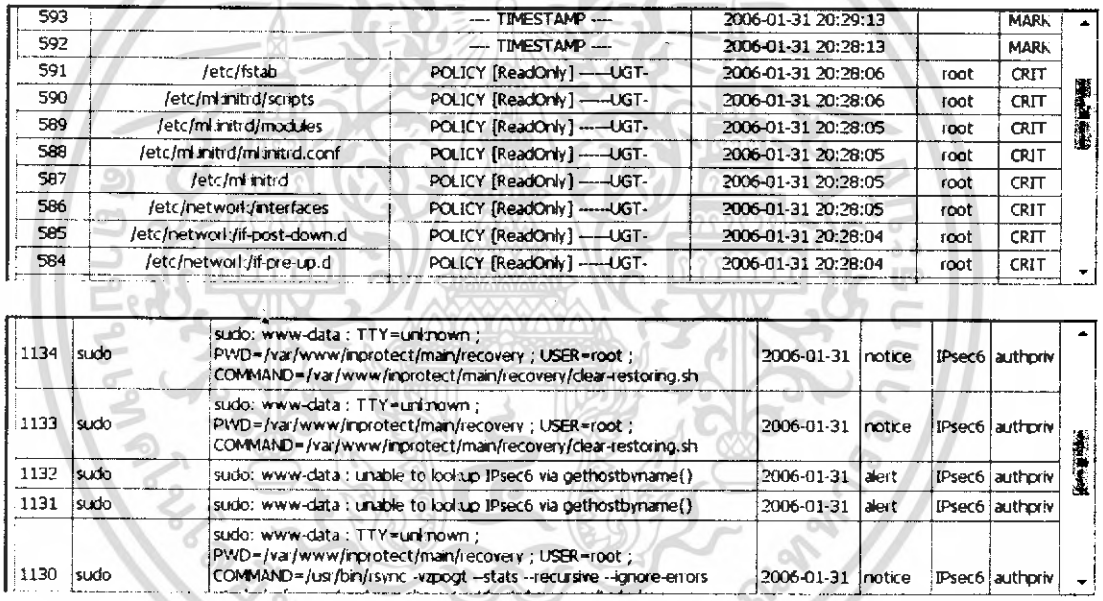
Index	File	Policies	TimeStamp	Owner	Sev

no data in database

Index	Prog	Msg	TimeStamp	Priority	Msg	Facility

no data in database

รูปที่ 4.4 แสดงการแสดงผลโดยที่ยังไม่มีการเริ่มเก็บข้อมูล



593		--- TIMESTAMP ---	2006-01-31 20:29:13		MARK
592		--- TIMESTAMP ---	2006-01-31 20:28:13		MARK
591	/etc/fstab	POLICY [ReadOnly] ------UGT-	2006-01-31 20:28:06	root	CRIT
590	/etc/mkinitrd/scripts	POLICY [ReadOnly] ------UGT-	2006-01-31 20:28:06	root	CRIT
589	/etc/mkinitrd/modules	POLICY [ReadOnly] ------UGT-	2006-01-31 20:28:05	root	CRIT
588	/etc/mkinitrd/mkinitrd.conf	POLICY [ReadOnly] ------UGT-	2006-01-31 20:28:05	root	CRIT
587	/etc/mkinitrd	POLICY [ReadOnly] ------UGT-	2006-01-31 20:28:05	root	CRIT
586	/etc/network/interfaces	POLICY [ReadOnly] ------UGT-	2006-01-31 20:28:05	root	CRIT
585	/etc/network/if-post-down.d	POLICY [ReadOnly] ------UGT-	2006-01-31 20:28:04	root	CRIT
584	/etc/network/if-pre-up.d	POLICY [ReadOnly] ------UGT-	2006-01-31 20:28:04	root	CRIT

1134	sudo	sudo: www-data : TTY=unknown ; PWD=/var/www/inprotect/main/recovery ; USER=root ; COMMAND=/var/www/inprotect/main/recovery/clear-restoring.sh	2006-01-31	notice	IPsec6	authpriv
1133	sudo	sudo: www-data : TTY=unknown ; PWD=/var/www/inprotect/main/recovery ; USER=root ; COMMAND=/var/www/inprotect/main/recovery/clear-restoring.sh	2006-01-31	notice	IPsec6	authpriv
1132	sudo	sudo: www-data : unable to lookup IPsec6 via gethostbyname()	2006-01-31	alert	IPsec6	authpriv
1131	sudo	sudo: www-data : unable to lookup IPsec6 via gethostbyname()	2006-01-31	alert	IPsec6	authpriv
1130	sudo	sudo: www-data : TTY=unknown ; PWD=/var/www/inprotect/main/recovery ; USER=root ; COMMAND=/usr/bin/rsync -vzpogt --stats --recursive --ignore-errors	2006-01-31	notice	IPsec6	authpriv

รูปที่ 4.5 แสดงข้อมูลที่ได้หลังจากทำการเก็บข้อมูลจากเครื่อง Response wall

4.4 การทดสอบที่ 3 การแจ้งเตือนและการวิเคราะห์

4.4.1 วิธีการทดสอบ

1) เปิดการทำงานทั้งหมดของระบบ
2) ทำการ scan ไปยังเครื่อง Response wall ด้วยโปรแกรม NMAP
3) Remote login ด้วย Secure Shell ไปยังเครื่อง Response wall และใส่รหัสผ่านที่ไม่ถูกต้องติดต่อกัน 3 ครั้ง
4) ทำการเปลี่ยนข้อมูลที่อยู่ในไฟล์สำคัญของระบบโดย และให้ขัดกับ Policy ของเครื่อง

4.4.2 ผลการทดสอบ

จากการทดสอบพบว่า ระบบมีการเก็บข้อมูลและแจ้งเตือนดังนี้คือ

1) มีการแจ้งเตือนว่า มีการ Scan โดยใช้โปรแกรม NMAP
2) มีการแจ้งเตือนว่า มีการพยายามใช้ Secure Shell ในการ Log in เข้าสู่ระบบ
3) มีการแจ้งเตือนว่า มีการเข้าไปแก้ไขหรือเปลี่ยนแปลงไฟล์สำคัญของระบบ

4.5 การทดสอบที่ 4 การกู้คืนระบบ

4.5.1 วิธีการทดสอบ

1) เปิดการทำงานทั้งหมดของระบบ
2) สร้างไฟล์ test โดยมีข้อมูล This is testing. ใน directory /etc/snort ที่เครื่อง Response wall
3) เพิ่ม path /etc/snort เข้าไปในระบบ Snapshot Management
4) ปรับแต่งค่าการเก็บ Snapshot ให้ทำงานดังนี้
   - Main Step ให้เก็บ Snapshot ในช่วงเวลา 2 เดือน โดยทำการเก็บทุกๆ 1 วัน
   - Sub Step ให้เก็บ Snapshot ในช่วงเวลา 20 นาที โดยทำการเก็บทุกๆ 1 นาที
5) ทำการเริ่มเก็บ Snapshot โดยคลิกที่ปุ่ม Start หลังจากให้ระบบได้ทำการเก็บ Snapshot เป็นเวลา 10 นาที เข้าไปตรวจสอบไฟล์ที่เกิดขึ้นใน directory /backup/snapshot/etc/snort/main และ /backup/snapshot/etc/snort/sub
6) เปลี่ยนข้อมูลที่อยู่ในไฟล์ test ใน directory /etc/snort ที่เครื่อง Response wall เป็น Content changed.
7) ตรวจสอบการเปลี่ยนแปลงจากข้อมูลที่ได้จากโปรแกรม Samhain และดำเนินการ Restore ไฟล์ test กลับไปยังเครื่อง Response wall
8) ตรวจสอบข้อมูลในไฟล์ test หลังจากการ Restore

4.5.2 ผลการทดสอบ

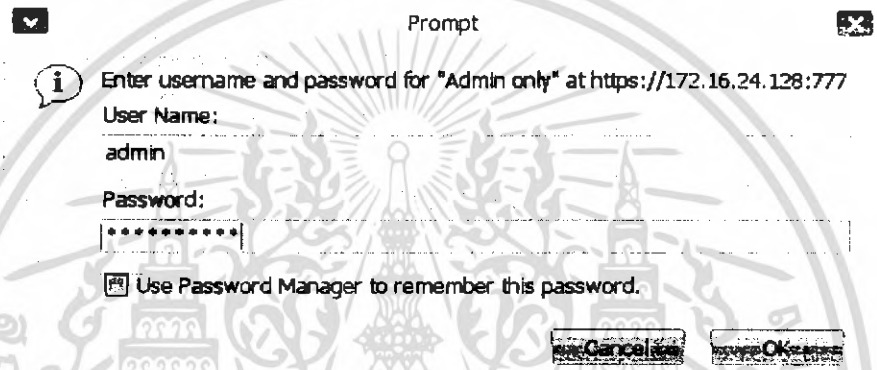
จากการทดสอบพบว่า

1) ระบบสามารถทำการเก็บ Snapshot ตาม path และช่วงเวลาที่กำหนดได้อย่างถูกต้อง
2) หลังจากทำการ restore ไฟล์ test กลับไปยังเครื่อง Response wall พบว่าข้อมูลในไฟล์กลับมาเป็น This is testing. เหมือนเดิม

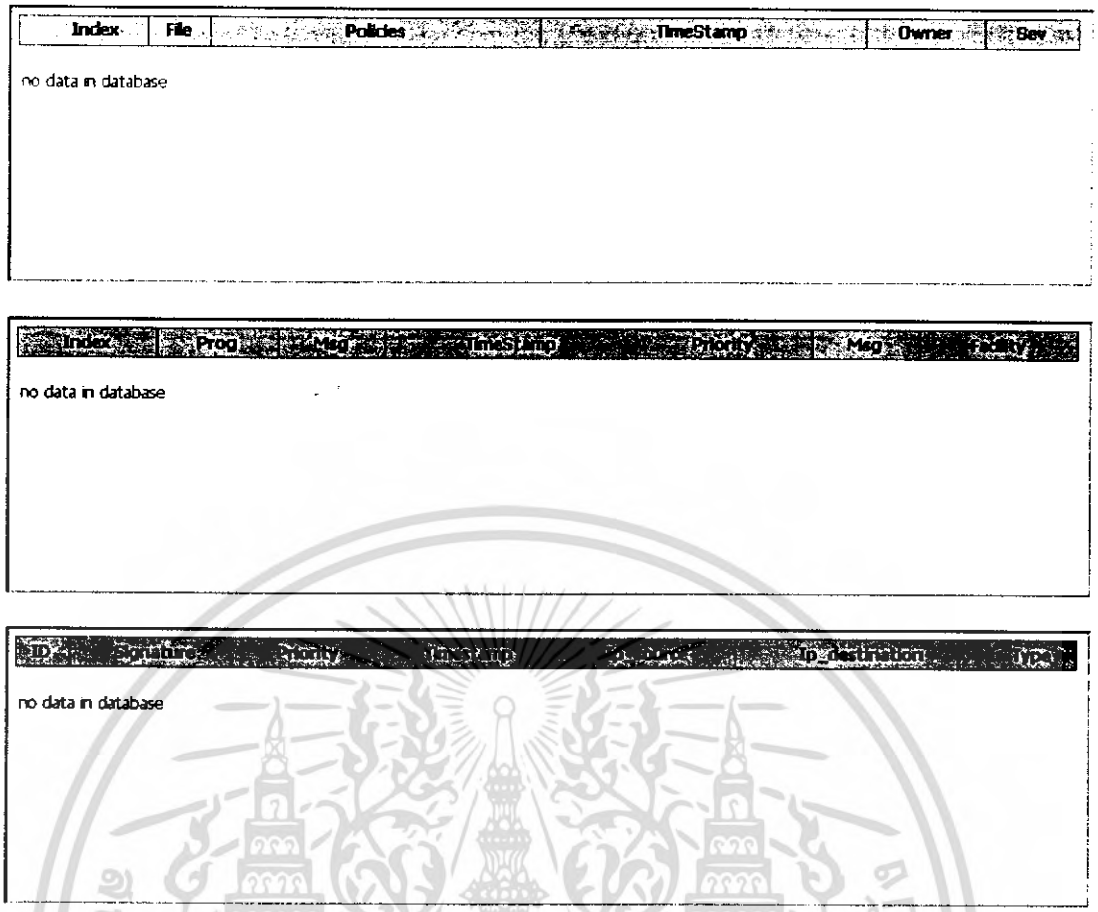
4.6 การทดสอบที่ 5 การจำลองสถานการณ์จริง

4.6.1 จำลองขั้นตอนการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย

1) เปิดการทำงานทั้งหมดของระบบและเข้าสู่ระบบแสดงผลข้อมูลที่เครื่อง Log Server



รูปที่ 4.6 แสดงการพิสูจน์ตนเพื่อเข้าสู่ระบบ



รูปที่ 4.7 แสดงข้อมูลในขณะที่ระบบยังไม่ถูกละเมิดความปลอดภัย

2) ทำการ Scan port ของเครื่อง Response wall
3) ทำการ Log in เข้าไปยังเครื่อง Response wall ผ่านทาง Secure Shell โดยใช้ Username เป็น Detector และรหัสผ่านใดๆ หลายๆ ครั้ง
4) ตรวจสอบเหตุการณ์ที่เกิดขึ้นกับ Response wall

25	sshd	::ffff:161.246.5.27 port 33427 ssh2	2006-02-21	info	IPsec4	auth
24	sshd	sshd[4871]: (pam_unix) 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=isag27.ce.kmitl.ac.th user=detector	2006-02-21	notice	IPsec4	auth
23	sshd	sshd[4871]: (pam_unix) 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=isag27.ce.kmitl.ac.th user=detector	2006-02-21	notice	IPsec4	auth
22	sshd	sshd[4871]: error: PAM: Have exhasted maximum number of retries for service. for detector from isag27.ce.kmitl.ac.th	2006-02-21	err	IPsec4	auth
21	sshd	sshd[4871]: error: PAM: Have exhasted maximum number of retries for service. for detector from isag27.ce.kmitl.ac.th	2006-02-21	err	IPsec4	auth
20	sshd	sshd[4871]: error: PAM:+Authentication failure for detector from isag27.ce.kmitl.ac.th	2006-02-21	err	IPsec4	auth

รูปที่ 4.8 แสดงข้อมูลหลังจากที่ระบบถูกละเมิดความปลอดภัย

จากภาพพบเหตุการณ์ผิดปกติ คือ โดน scan port โดยมาจาก IP 161.246.5.27 และ มีการพยายามเข้ามายังเครื่องเป้าหมายโดยการเข้ามาทาง ssh และมาจากเครื่อง 161.246.5.27 โดยที่เข้า

มาโดยใช้ชื่อผู้ใช้ว่า detector โดยมีการ ป้อนรหัสผ่านผิดเกินจำนวนที่กำหนด แต่สุดท้ายก็สามารถเข้าสู่ระบบได้

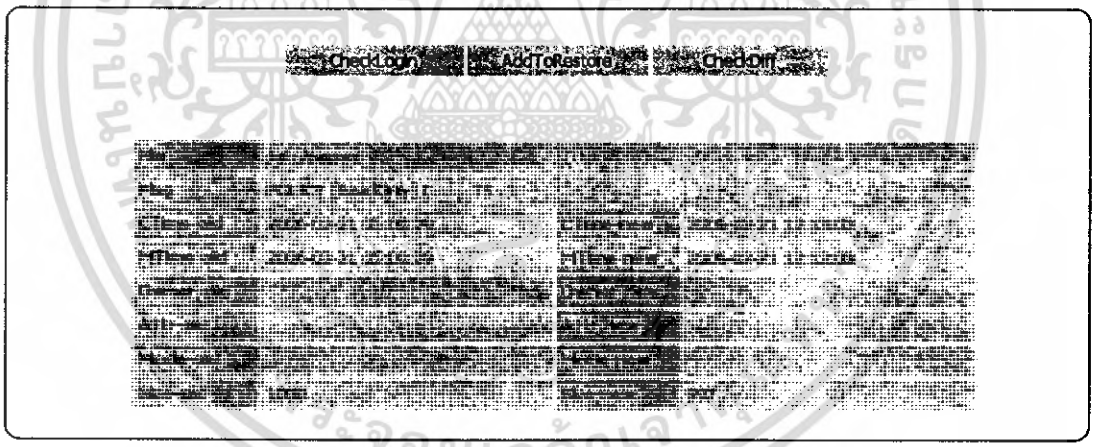
5) ทำการสืบหาร่องรอยที่น่าสงสัยจากข้อมูลที่ได้มา

Index	File	Policies	TimeStamp	Owner	Sev
16	/etc/passwd	POLICY [ReadOnly] C------TS	2006-02-21 12:21:45		CRIT
15		---- TIMESTAMP ----	2006-02-21 12:21:11		MARK
14		---- TIMESTAMP ----	2006-02-21 12:20:11		MARK
13		---- TIMESTAMP ----	2006-02-21 12:19:11		MARK
12		---- TIMESTAMP ----	2006-02-21 12:18:11		MARK
11		---- TIMESTAMP ----	2006-02-21 12:17:11		MARK
10		---- TIMESTAMP ----	2006-02-21 12:16:11		MARK
9		---- TIMESTAMP ----	2006-02-21 12:15:11		MARK
8		---- TIMESTAMP ----	2006-02-21 12:14:11		MARK

รูปที่ 4.9 แสดงข้อมูลที่บ่งบอกถึงการเปลี่ยนแปลงที่ไฟล์ /etc/passwd

จากข้อมูลที่ได้ทำให้ทราบว่า มีการแจ้งเตือนในระดับวิกฤต เนื่องจากมีการเปลี่ยนแปลงไฟล์ /etc/passwd ซึ่งเป็นไฟล์ที่เก็บชื่อผู้ใช้และ ค่าต่างๆ ของผู้ใช้ระบบ

ทำการตรวจสอบต่อไปเพื่อหาข้อมูลช่วงเวลาที่ไฟล์ /etc/passwd โดนเปลี่ยนแปลง หลังจากได้ช่วงเวลาที่แน่นอนแล้ว ขั้นตอนต่อไปคือการตรวจสอบการใช้งานระบบในช่วงนั้น เพื่อดูว่า มีผู้ใช้ระบบคนใดบ้างที่เข้าใช้งานระบบช่วงเวลานั้นๆ



รูปที่ 4.10 แสดงข้อมูลที่บ่งบอกถึงช่วงเวลาที่ไฟล์ /etc/passwd โดนเปลี่ยนแปลง

User	Serial	IP	Login time	Logout time
detector	pts/0	161.246.5.27	2006-02-21 12:09	2006-02-21 12:20
root	tty1	0.0.0.0	2006-01-31 20:21	Still log in

รูปที่ 4.11 แสดงข้อมูลที่บ่งบอกถึงการใช้งานระบบ

จากข้อมูลที่ได้ทำให้ทราบว่า ผู้ที่เข้าใช้งานระบบมีเพียงคนเดียวในช่วงเวลาที่ไฟล์ /etc/passwd โดนเปลี่ยนแปลง คือผู้ใช้ที่ชื่อ detector ที่ทำการเข้าสู่ระบบตั้งแต่เวลา 19.31 น. ถึงเวลา 19.48 น.

6) ทำการตรวจสอบต่อไปว่าผู้ใช้คนนั้นมีการใช้คำสั่งอะไรบ้างในระหว่างช่วงเวลาที่มีการ login เข้าสู่ระบบซึ่งปรากฏว่ามีการใช้คำสั่งที่น่าสงสัย คือ คำสั่ง su จึงเข้าไปตรวจสอบต่อยัง Logfile ของระบบ

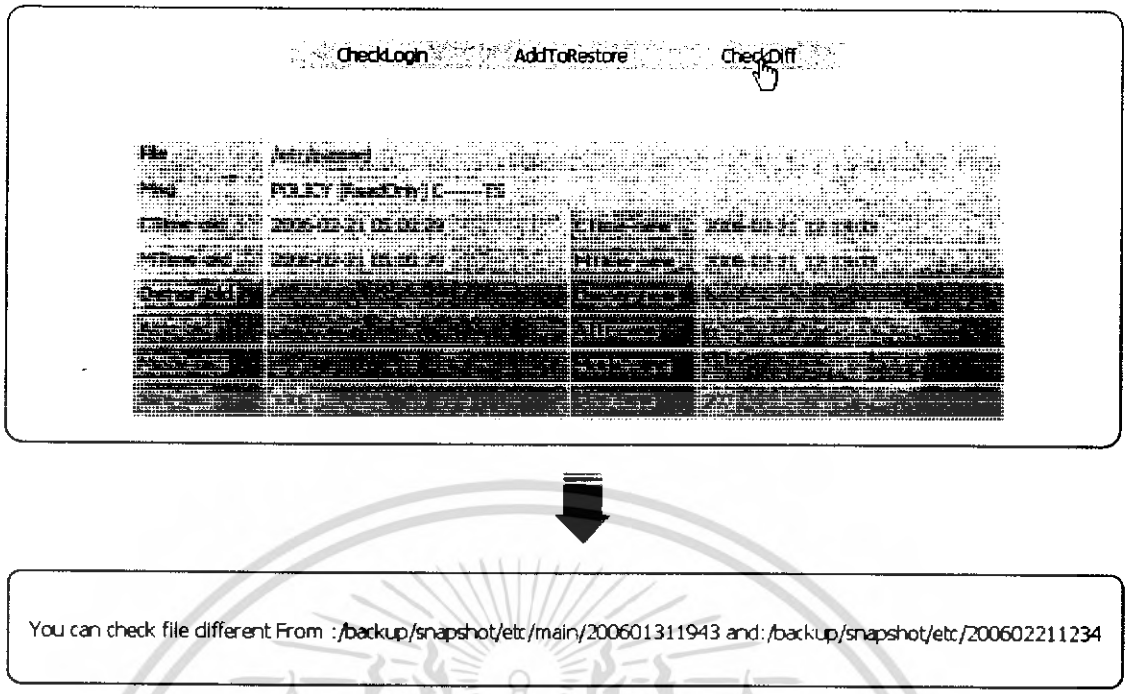
Command	Flag	User	TTY	CPU	Start
sshd	SF	detector	??	0.53	21 12:08 Feb
bash	F	detector	??	0.00	21 12:09 Feb
bash	F	detector	??	0.00	21 12:09 Feb
sshd	SF	detector	??	0.05	21 12:01 Feb
bash	F	detector	??	0.00	21 12:01 Feb
bash	F	detector	??	0.00	21 12:01 Feb
bash		detector	??	0.07	21 12:08 Feb
ls		detector	??	0.01	21 12:19 Feb
clear		detector	??	0.00	21 12:10 Feb
clear		detector	??	0.00	21 12:10 Feb
dircolors		detector	??	0.00	21 12:09 Feb
id		detector	??	0.00	21 12:09 Feb
bash		detector	??	0.07	21 12:01 Feb
clear		detector	??	0.01	21 12:07 Feb
dircolors		detector	??	0.00	21 12:01 Feb
id		detector	??	0.00	21 12:01 Feb

รูปที่ 4.12 แสดงข้อมูลที่บ่งบอกการใช้คำสั่งของผู้ใช้งานระบบ

Index	Prog	Msg	TimeStamp	Priority	Host	Facility
52	sudo	sudo: detector : TTY=pts/0 ; PWD=/home/detector ; USER=root ; COMMAND=/bin/bash	2006-02-21	notice	IPsec4	authpriv
51	sudo	sudo: detector : TTY=pts/0 ; PWD=/home/detector ; USER=root ; COMMAND=/bin/bash	2006-02-21	notice	IPsec4	authpriv
50	syslog-ng	syslog-ng[2657]: STATS: dropped 0	2006-02-21	notice	IPsec4	syslog
49	syslog-ng	syslog-ng[2657]: STATS: dropped 0	2006-02-21	notice	IPsec4	syslog
48	sudo	sudo: detector : unable to lookup IPsec4 via gethostbyname()	2006-02-21	alert	IPsec4	authpriv
47	sudo	sudo: detector : unable to lookup IPsec4 via gethostbyname()	2006-02-21	alert	IPsec4	authpriv

รูปที่ 4.13 แสดงข้อมูลที่บ่งบอกรายละเอียดของการใช้คำสั่งของผู้ใช้งานระบบ

จากข้อมูลที่ได้ทำให้ทราบว่าผู้ใช้ชื่อ detector มีการใช้คำสั่ง sudo และไม่มีข้อผิดพลาดแจ้งเตือน



รูปที่ 4.14 แสดงผลของระบบจากการหาข้อแตกต่างของไฟล์ที่พบการเปลี่ยนแปลง

7) ทำการตรวจสอบจากข้อมูลของไฟล์ว่าถ้าต้องการดูการเปลี่ยนแปลงของไฟล์ /etc/passwd ที่เครื่องเก็บล็อกสามารถเข้าไปดูได้ที่ไหน จึงได้ path 2 path ที่จะนำมาใช้ในการตรวจสอบความแตกต่าง

```
IPsec6:/backup/snapshot/etc/sub# diff 200602211319/etc/passwd ../main/200601311943/etc/passwd
23,24c23
< detector:x:0:1001:,,,:/home/detector:/bin/bash
< ftp:x:103:65534::/home/ftp:/bin/false
---
> detector:x:1001:1001:,,,:/home/detector:/bin/bash
IPsec6:/backup/snapshot/etc/sub#
```

รูปที่ 4.15 แสดงการหาข้อแตกต่างของไฟล์ที่โดนเปลี่ยนแปลง

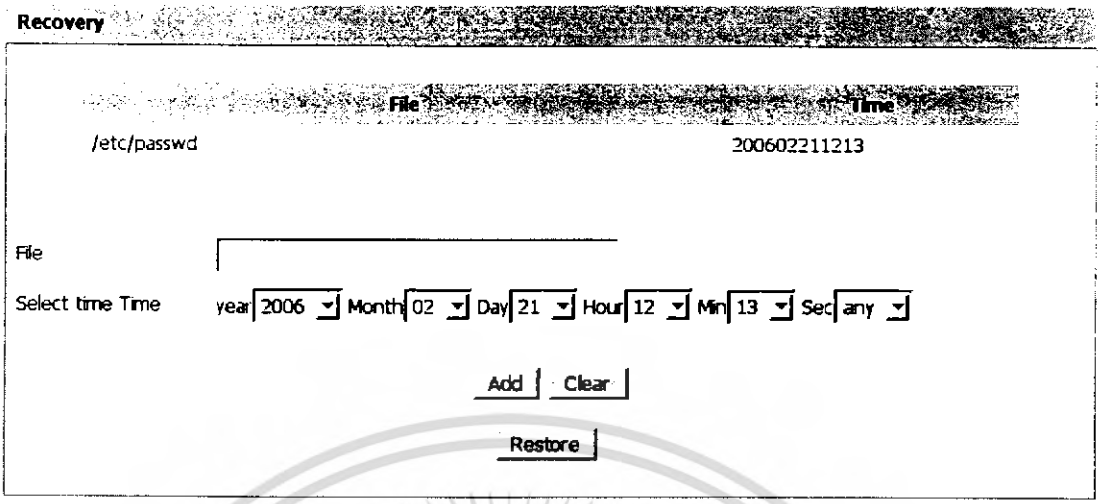
เข้าไปตรวจสอบดูความแตกต่างของไฟล์ทั้ง 2 ที่ ปรากฏว่ามีการเปลี่ยนแปลงจากไฟล์ก่อนหน้าคือ ผู้ใช้ detector มีการเปลี่ยน user id จากเดิมที่เป็น 1001 มาเป็น 0 ซึ่งทำให้ผู้ใช้คนนั้นมีสิทธิ์เทียบเท่ากับ root

รูปที่ 4.16 แสดงการตรวจสอบการเปิดพอร์ต

ทำการตรวจสอบระบบว่ามีการเปิด port หรือ backdoor ไว้หรือไม่โดยการใช้เครื่อง logserver สแกน เครื่องที่โดนบุกรุก ปรากฏว่าไม่มีการเปิด port หรือบริการใดๆเพิ่มขึ้นจากปกติ จากนั้นก็ทำการตรวจสอบว่าเวลาปัจจุบันมีใครใช้ระบบอยู่บ้าง แต่ ปรากฏว่าไม่มี จึงเข้าไปตรวจสอบ ที่เครื่องจริงว่าไฟล์นั้นมีการเปลี่ยนแปลงไปจริงหรือไม่

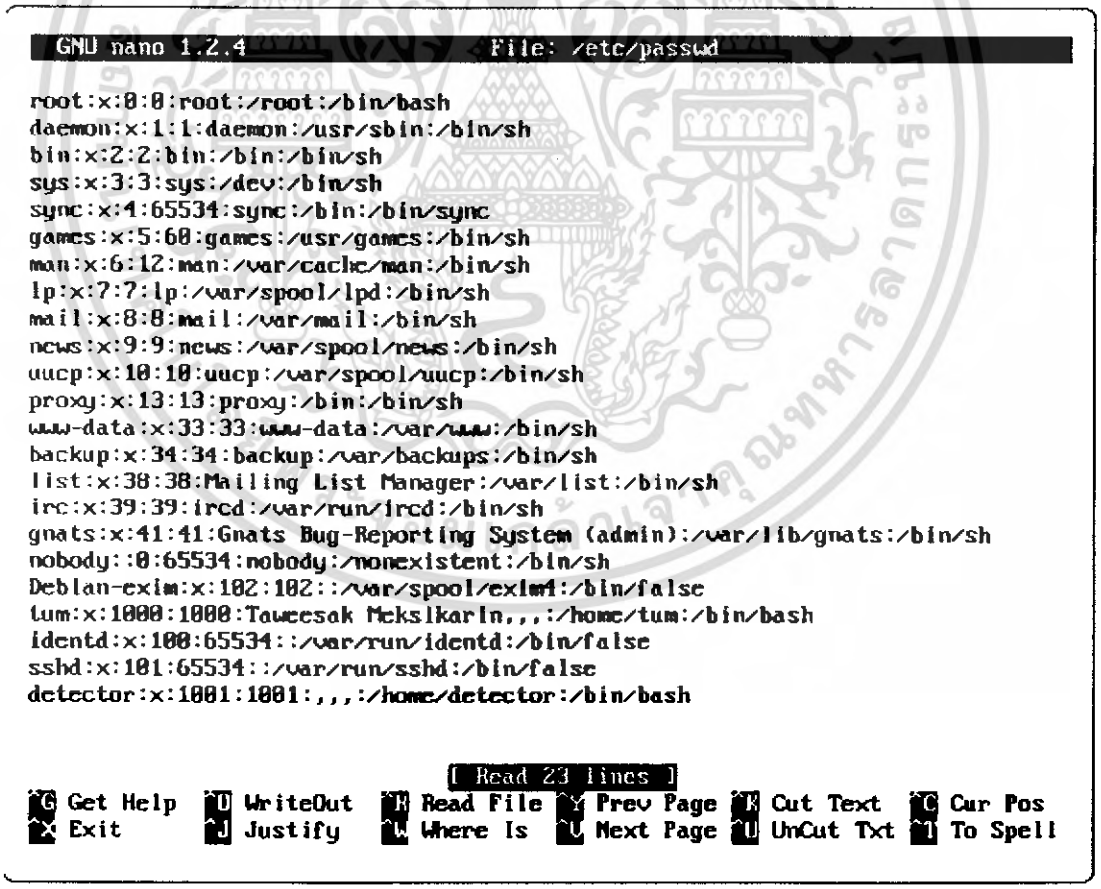
จากข้อมูลที่ได้มาทั้งหมด ทำให้ทราบได้ค่อนข้างแน่นอนว่า ผู้บุกรุกได้เข้ามาโดยใช้ชื่อผู้ใช้ว่า detector โดยที่เข้ามาทางบริการ ssh และมีการใช้ช่องโหว่จากการกำหนดขอบเขตของคำสั่ง sudo ที่ไม่ดีพอเพื่อได้สิทธิ์ของ root ไปและยังได้ทำการเปลี่ยนแปลงสิทธิ์ของตนเองเพื่อให้ได้มาซึ่งสิทธิ์ที่สูงขึ้น คือเป็น root และมีการลบค่าล็อกต่างๆ เนื่องจากมีการแจ้งเตือนว่า ไฟล์ /var/log มีขนาดเล็กลง เมื่อเข้าไปตรวจสอบค่าล็อกที่เครื่องซึ่งโดนโจมตี ปรากฏว่ามีการลบค่าต่างๆ ทิ้งไป

8) ทำการกู้คืนระบบ

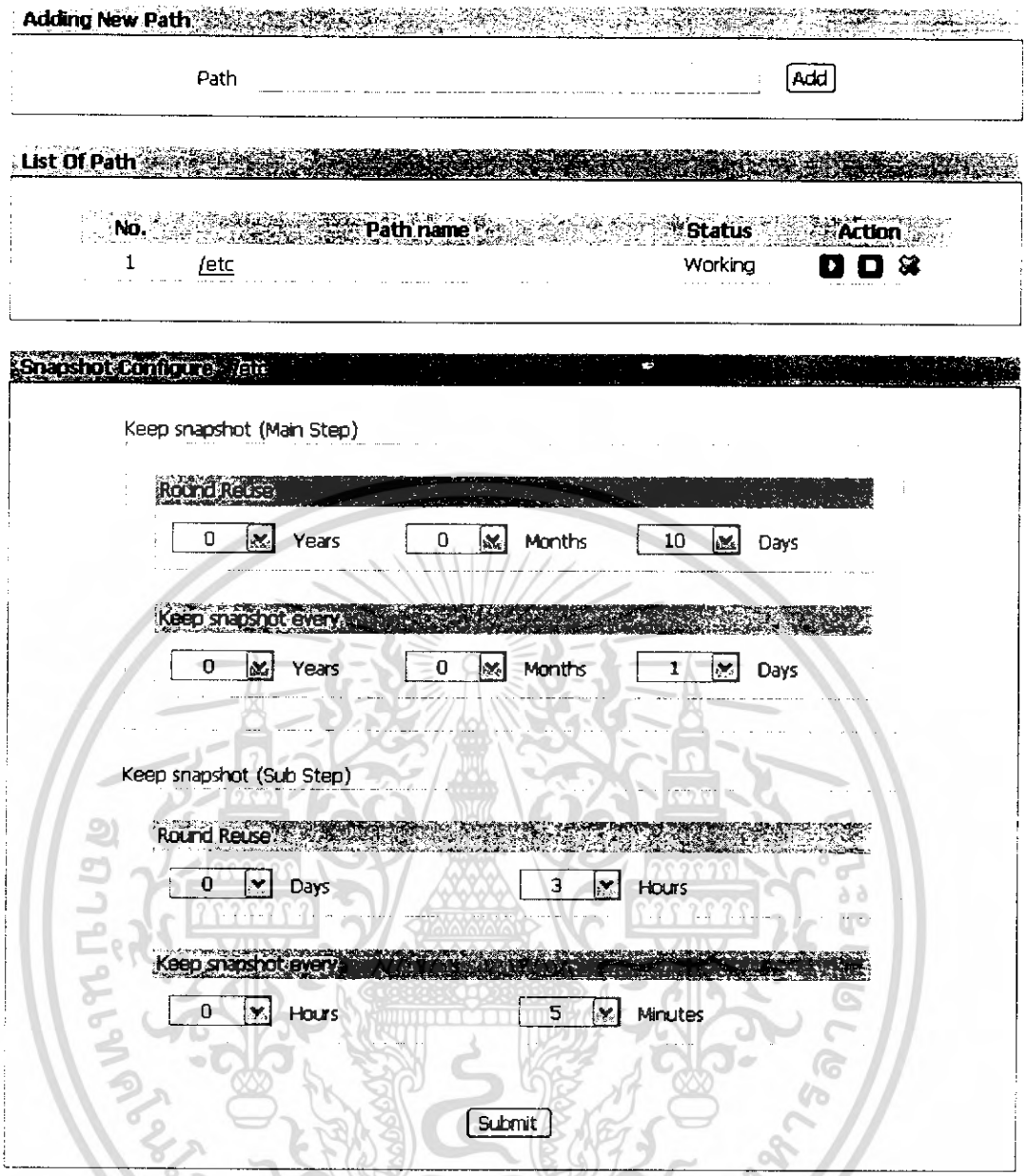


รูปที่ 4.17 แสดงการเพิ่มไฟล์เข้าไปในระบบการ Recovery

ทำการกู้คืนระบบโดยการแก้ค่าไฟล์ที่โดนเปลี่ยนแปลงให้กับเป็นค่าเหมือนกับตอนก่อนถูกเปลี่ยนแปลง



รูปที่ 4.18 แสดงการเข้าไปตรวจสอบค่าหลังจากที่ได้ทำการกู้คืนระบบ



รูปที่ 4.19 แสดงการตั้งค่าช่วงเวลาของการเก็บ Snapshot

เข้าไปเพิ่มการเก็บ Snapshot ให้ทำการเก็บเพิ่มที่ ไดเร็กทอรี่ ของผู้ใช้ detector และทำการเพิ่มความถี่ในการเก็บ Snapshot ให้ถี่ขึ้น

4.6.2 จำลองการฉะเมิดความปลอดภัย

1) ชื่อผู้ใช้คนหนึ่งของเครื่องที่ต้องการโจมตี ชื่อ detector ผู้บุกรุกจึงได้ทำการ scan เครื่องเป้าหมาย เพื่อตรวจสอบว่ามีบริการใดเปิดไว้บ้าง เพื่อที่จะเข้าไปโจมตีระบบ หลังจากทีทราบบริการที่เปิด ผู้บุกรุกก็ได้ทำการ เลือก บริการที่จะเข้า และทดสอบเดารหัสผ่าน ซึ่งอยู่ใกล้ตัวของผู้ใช้คนนั้น ปรากฏว่าสามารถเข้าสู่ระบบได้

```
Isag27:/home/phantomb# nmap 161.246.5.32

Starting Nmap 3.95 ( http://www.insecure.org/nmap/ ) at 2006-02-21 12:07 ICT
Interesting ports on isag32.ce.kmitl.ac.th (161.246.5.32):
(The 1665 ports scanned but not shown below are in state: closed)
PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  open     ssh
113/tcp open     auth
179/tcp filtered bgp
873/tcp open     rsync
MAC Address: 00:0C:29:F8:44:27 (VMware)

Nmap finished: 1 IP address (1 host up) scanned in 9.375 seconds
Isag27:/home/phantomb# ssh detector@161.246.5.32
Password:
Password:
Password:
Permission denied (publickey,keyboard-interactive).
Isag27:/home/phantomb# ssh detector@161.246.5.32
Password:
Linux IPsec4 2.6.11.7 #1 Tue Jan 17 08:22:54 ICT 2006 i686 GNU/Linux

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Tue Feb 21 12:01:10 2006 from isag27.ce.kmitl.ac.th
detector@IPsec4:~$
```

รูปที่ 4.20 แสดงการ Log in เข้าใช้บริการยังเครื่องเป้าหมาย

ผู้บุกรุกได้ทำการทดสอบดูคำสั่ง และ ดูสิ่งที่มีอยู่ ปรากฏว่าผู้บุกรุกได้เจอ คำสั่ง sudo จึงได้ทดสอบโดยลองเรียกเชลล์ของ root ดูปรากฏว่า สามารถได้เชลล์ของ root เนื่องจากมีการตั้งค่าสำหรับ คำสั่ง sudo ไว้ไม่ดี ผู้บุกรุกจึงได้เป็น root

```
detector@IPsec4:~$ su
su          sudo        sudoedit    sum         superformat  suspend
detector@IPsec4:~$ sudo -s -H
sudo: unable to lookup IPsec4 via gethostbyname()
Password:
IPsec4:/home/detector# id
uid=0(root) gid=0(root) groups=0(root)
IPsec4:/home/detector#
```

รูปที่ 4.21 แสดงการทดสอบการใช้คำสั่ง sudo

ผู้บุกรุกเข้าไปที่ ไฟล์ /etc/passwd และได้ทำการเปลี่ยน user id ของตัวเองให้เป็น 0 เพื่อให้มีสิทธิ์เท่ากับ root

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody::0:65534:nobody:/nonexistent:/bin/sh
Debian-exim:x:102:102::/var/spool/exim4:/bin/false
tum:x:1000:1000:Taweesak Meksikarin,,,:/home/tum:/bin/bash
identd:x:100:65534::/var/run/identd:/bin/false
sshd:x:101:65534::/var/run/sshd:/bin/false
detector:x:0:1001:,,,:/home/detector:/bin/bash
ftp:x:103:65534::/home/ftp:/bin/false
```

รูปที่ 4.22 แสดงการเข้าไปแก้ไขข้อมูลในไฟล์ /etc/passwd

ผู้บุกรุกเข้าไปดูที่ /var/log ซึ่งเก็บ ล็อกไฟล์ต่างๆ ของระบบ เพื่อที่จะได้ทำการแก้ไข

```
Feb 21 12:00:59 IPsec4 sshd[4850]: (pam_unix) 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=isa$
Feb 21 12:01:10 IPsec4 sshd[4855]: Accepted keyboard-interactive/pam for detector from ::ffff:161.246.5.27 port 33912 ssh2
Feb 21 12:01:10 IPsec4 sshd[4858]: (pam_unix) session opened for user detector by (uid=0)
Feb 21 12:05:01 IPsec4 CRON[4864]: (pam_unix) session opened for user root by (uid=0)
Feb 21 12:05:01 IPsec4 CRON[4864]: (pam_unix) session closed for user root
Feb 21 12:07:19 IPsec4 sshd[4858]: (pam_unix) session closed for user detector
Feb 21 12:09:07 IPsec4 sshd[4871]: (pam_unix) authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=isag27.ce.k$
Feb 21 12:09:08 IPsec4 sshd[4871]: error: PAM: Authentication failure for detector from isag27.ce.kmitl.ac.th
Feb 21 12:09:12 IPsec4 sshd[4871]: error: PAM: Authentication failure for detector from isag27.ce.kmitl.ac.th
Feb 21 12:09:15 IPsec4 sshd[4871]: error: PAM: Have exhasted maximum number of retries for service. for detector from isag27$
Feb 21 12:09:15 IPsec4 sshd[4871]: (pam_unix) 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=isa$
Feb 21 12:09:22 IPsec4 sshd[4876]: Accepted keyboard-interactive/pam for detector from ::ffff:161.246.5.27 port 33427 ssh2
Feb 21 12:09:22 IPsec4 sshd[4879]: (pam_unix) session opened for user detector by (uid=0)
Feb 21 12:10:01 IPsec4 CRON[4885]: (pam_unix) session opened for user root by (uid=0)
Feb 21 12:09:48 IPsec4 CRON[4885]: (pam_unix) session closed for user root
Feb 21 12:10:01 IPsec4 CRON[4891]: (pam_unix) session opened for user root by (uid=0)
Feb 21 12:10:00 IPsec4 CRON[4891]: (pam_unix) session closed for user root
Feb 21 12:11:05 IPsec4 sudo: detector : unable to lookup IPsec4 via gethostbyname()
Feb 21 12:11:11 IPsec4 sudo: detector : TTY=pts/0 ; PWD=/home/detector ; USER=root ; COMMAND=/bin/bash
```

รูปที่ 4.23 แสดงการเข้าไปดูข้อมูลในไฟล์ /var/log

ผู้บุกรุกทำการลบข้อมูลบรรทัดที่จะเป็นหลักฐานความผิดของตัวเอง และเหลือไว้เพียงเหตุการณ์ที่ดูเป็นปกติ

```
Feb 21 12:01:10 IPsec4 sshd[4858]: (pam_unix) session opened for user detector by (uid=0)
Feb 21 12:05:01 IPsec4 CRON[4864]: (pam_unix) session opened for user root by (uid=0)
Feb 21 12:05:01 IPsec4 CRON[4864]: (pam_unix) session closed for user root
Feb 21 12:07:19 IPsec4 sshd[4858]: (pam_unix) session closed for user detector
Feb 21 12:09:22 IPsec4 sshd[4876]: Accepted keyboard-interactive/pam for detector from ::ffff:161.246.5.27 port 39427 ssh2
Feb 21 12:09:22 IPsec4 sshd[4879]: (pam_unix) session opened for user detector by (uid=0)
Feb 21 12:10:01 IPsec4 CRON[4885]: (pam_unix) session opened for user root by (uid=0)
Feb 21 12:09:48 IPsec4 CRON[4885]: (pam_unix) session closed for user root
Feb 21 12:10:01 IPsec4 CRON[4891]: (pam_unix) session opened for user root by (uid=0)
Feb 21 12:10:00 IPsec4 CRON[4891]: (pam_unix) session closed for user root
Feb 21 12:15:01 IPsec4 CRON[4909]: (pam_unix) session opened for user root by (uid=0)
Feb 21 12:14:42 IPsec4 CRON[4909]: (pam_unix) session closed for user root
Feb 21 12:15:01 IPsec4 CRON[4915]: (pam_unix) session opened for user root by (uid=0)
Feb 21 12:15:00 IPsec4 CRON[4915]: (pam_unix) session closed for user root
Feb 21 12:17:01 IPsec4 CRON[4922]: (pam_unix) session opened for user root by (uid=0)
Feb 21 12:17:01 IPsec4 CRON[4922]: (pam_unix) session closed for user root
```

รูปที่ 4.24 แสดงข้อมูลในไฟล์ /var/log หลังจากที่โดนแก้ไขแล้ว

บทที่ 5
บทวิจารณ์และสรุป

5.1 วิเคราะห์และสรุปผลการทดสอบ

วิเคราะห์ผลการทดลอง

จากการทดลองที่ได้ทดสอบมาได้ผลเป็นที่น่าพอใจ เนื่องจากระบบที่เตรียมเอาไว้สามารถทำการเก็บข้อมูลหลักฐานได้อย่างครบถ้วนตามที่ได้ออกแบบไว้ มีการเข้ารหัส รวมทั้ง มีการตรวจสอบความถูกต้อง ของข้อมูลและผู้รับผู้ส่ง โดยที่ไม่โดนทำลายหลักฐานหรือลบร่องลอย เนื่องจากเครื่องที่ใช้ในการเก็บหลักฐาน และ ใช้ในการวิเคราะห์นั้นไม่ได้อยู่บนเครื่องที่ต้องการตรวจสอบจริงๆ ระบบสามารถแจ้งเตือนต่อเหตุการณ์ที่น่าสงสัย ได้อย่างทันท่วงที เพื่อที่จะได้ทำการตรวจสอบต่อไป ว่าเกิดอะไรขึ้นกับระบบ และใครเป็นคนกระทำ และสามารถค้นหาข้อมูลได้ตามที่ต้องการ ไม่ว่าจะเป็นตาม ช่วงเวลาที่กำหนด ตามผู้ใช้ หรือ โปรแกรม จนสามารถทั้งจะนำมารวบรวมและใช้ในการตัดสินใจว่าจะ ตอบสนองอย่างไรต่อเหตุการณ์ที่เกิดขึ้น

5.2 ปัญหาและอุปสรรค

1. การตอบสนอง นั้นจะทำได้ดีก็ต่อเมื่อ มีการเตรียมการมาดีตั้งแต่เริ่มต้น ทำให้ระบบตอบสนองนั้นประกอบด้วยส่วนต่างๆ มากมาย ตั้งแต่ขั้นตอนการวางแผน การเก็บหลักฐานและเตรียมระบบ การตรวจสอบเหตุการณ์ที่น่าสงสัย การสืบหาหลักฐาน วิเคราะห์ข้อมูล รวมไปถึงการการปิดช่องโหว่ และการกู้คืนระบบ ทำให้ยากต่อการสร้างระบบขึ้นมาเองทั้งหมด จึงต้องนำโปรแกรม opensource เข้ามาช่วยในบางส่วน

2. การทำงานวิเคราะห์ข้อมูล สืบหาหลักฐาน และการกู้คืนระบบ ไม่ได้อยู่บนเครื่องนั้นจริงๆ ทำให้การจัดการข้อมูลต่างๆ ทำได้อย่างลำบาก

3. การที่ต้องมีการส่งไฟล์สำคัญ ไม่ว่าจะเป็น ไฟล์ snapshot หรือไฟล์ที่ใช้ในการวิเคราะห์สืบหาหลักฐานจึงต้องใช้ทรัพยากรเครื่องมากจนทำให้ระบบช้า

4. การหาหลักฐานเพื่อเตรียมให้ผู้ดูและระบบสืบหาหลักฐานนั้น จำเป็นจะต้องรู้ถึงรูปแบบการโจมตีในรูปแบบต่างๆ และเทคนิคต่างๆ ที่ผู้บุกรุกจะใช้เพื่อหลบหลีกการตามรอย และต้องรู้ว่าเหตุการณ์แบบใดที่ผิดปกติ และเหตุการณ์ใด เป็นเหตุการณ์ปกติ

5. การสืบหาหลักฐานนั้นโดยปกติแล้วจะเป็นการ สืบหาหลักฐานแบบ offline คือทำจากระบบที่ปิดแล้วในการพิจารณาข้อมูล และ ในที่นี้เราได้ใช้การสืบหาหลักฐานแบบ ออนไลน์ และกระทำบนเครื่องอื่น จึงทำให้หาข้อมูลได้ยาก ต้องมีการค้นคว้า เพื่อหาวิธีที่จะเอาข้อมูลจากที่ต่างๆมาประกอบกัน เพื่อให้เข้าใจถึงเหตุการณ์ที่เกิดขึ้น

6. ในการเก็บ Snapshot หากมีการสั่งให้ระบบทำการเก็บ Snapshot พร้อมๆ กันในหลายๆ Directory อาจทำให้ซีพียูทำงานหนักจนไม่สามารถประมวลผลงานอย่างอื่นได้

5.3 แนวทางการประยุกต์และพัฒนา

1. ทำการปรับปรุง Source Code ที่ได้เขียนให้มีประสิทธิภาพและรัดกุมมากขึ้น
2. เพิ่มวิธีการเก็บหลักฐานเพื่อนำไปใช้เป็นข้อมูลสำหรับการวิเคราะห์มากขึ้น
3. ผู้บุกรุกที่มีความสามารถอาจทำการตัดการเชื่อมต่อระหว่างเครื่องที่รับและส่งข้อมูลจึงต้องเพิ่มส่วนที่ทำหน้าที่ตรวจสอบการเชื่อมต่อดังกล่าว
4. เพิ่มรูปแบบการแจ้งเตือนให้หลากหลายขึ้นเช่น การส่งการแจ้งเตือนไปทางอีเมลล์
5. ทำการ Harden ระบบให้มีความปลอดภัยมากขึ้น

บรรณานุกรม

[1] ThaiCert. "การรับมือกับเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์และเครือข่าย" : http://www.thaicert.nectec.or.th/paper/incident/handling.htm. 2543.

[2] ThaiCert. "ระบบตรวจจับการบุกรุก" : http://www.thaicert.nectec.or.th/paper/ids/ids.php

[3] ThaiCert. "การติดตั้ง Snort แบบง่าย" : http://www.thaicert.nectec.or.th/paper/ids/snort.php

[4] ThaiCert. "ความรู้เบื้องต้นเกี่ยวกับการพิสูจน์ตัวตน" : http://www.thaicert.nectec.or.th/paper/authen/authentication_guide.php

[5] ACIS. "IDS และ IPS ควรเลือกใช้แบบใด" : http://www.acisonline.net/article_prinya_ids1.htm

[6] นายอภิชน ไวท์ยางกูร และนางสาวอังสนา วงศ์รัตนวิจิตร "ระบบตรวจจับผู้บุกรุกเครือข่ายบน-ยูนิกซ์" ปริญญานิพนธ์วิศวกรรมศาสตรบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง 2544

[7] The Honeynet Project Team. 2547 **Know you enemy edition2**, Addison-Wesley, Boston

[8] Dr.E.Eugene Shultz , Russel Shumway. 2544 **Insident Response**, New Riders, Indiana