บทที่ 10
การพัฒนาโปรแกรม Tartarus Management

10.1 แนวคิด

โปรแกรม Tartarus Management (TM) เป็นโปรแกรม Front-end ที่สร้างขึ้นเพื่อแก้ปัญหาความยุ่งยากในการดูแลและจัดการระบบจำแนกผู้บุกรุกที่อยู่ในส่วนไฟร์สกรีน การจัดการกับเครื่องกับดักของระบบไฟร์แทรป รวมถึงการแสดงล็อกไฟล์จากระบบตรวจจับผู้บุกรุก และล็อกไฟล์จากการบันทึกพฤติกรรมของผู้บุกรุกในเครื่องกับดัก

10.2 ขอบเขตและความสามารถ

โปรแกรม Tartarus Management (TM) สามารถควบคุม และกำหนดค่าการทำงานของเครื่องมือต่าง ๆ ได้ เช่น สามารถดูสถานะการทำงานของระบบจำแนกผู้บุกรุกส่วนไฟร์สกรีน , สั่งเริ่มหรือยกเลิกการทำงานของระบบ , ดูสถานะการทำงานของเครื่องกับดักในระบบไฟร์แทรป , สร้าง แก้ไข สั่งแช่แข็งหรือลบเครื่องกับดักได้ รวมทั้งยังสามารถเลือกใช้ สร้างหรืออัพเดตกฎของสนอร์ตอินไลน์ได้ พร้อมทั้งแสดงข้อมูลต่าง ๆ ที่อยู่ในดาต้าเบสเซิร์ฟเวอร์ (LogServer) ได้

10.3 การทำงานของโปรแกรม

โปรแกรม Tartarus Management มีรายละเอียดดังนี้

- **หน้าต่าง Login** เพื่อพิสูจน์ตัวตนก่อนใช้โปรแกรม

รูปที่ 10.1 แสดงหน้าจอล็อกอินเข้าโปรแกรม

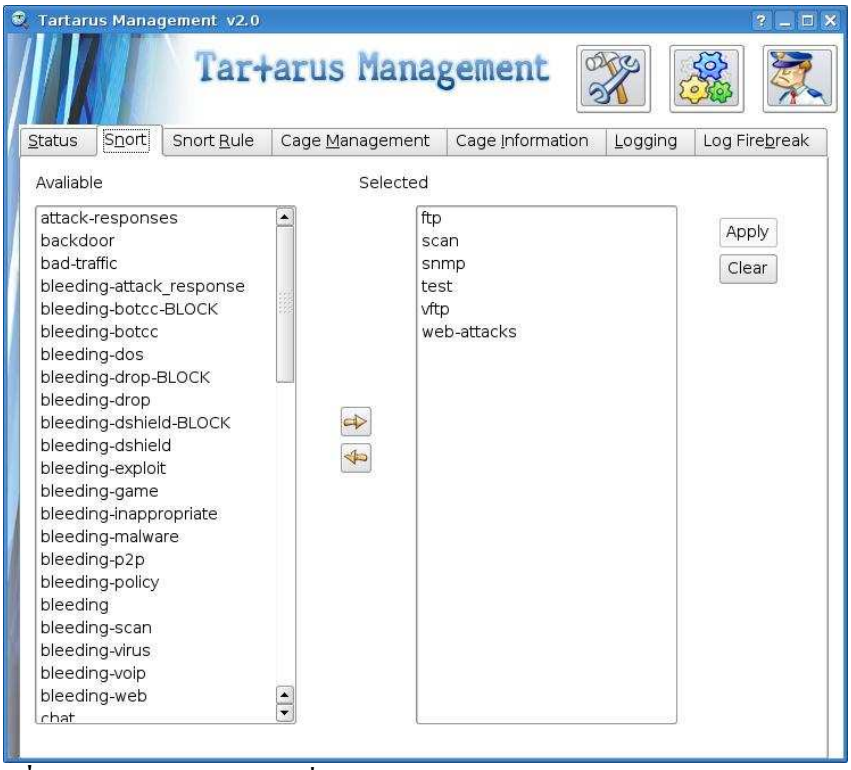
- **หน้า Status**

เป็นหน้าที่บอกถึงสถานะของเครื่องไฟร์สกรีนและเครื่องกับดักไฟร์แทรป ว่าทำงานอยู่หรือไม่ โดยสำหรับเครื่องกับดักนั้นจะแสดงถึงชื่อและประเภทของเครื่องกับดักด้วย อีกทั้งยังสามารถสั่งเริ่มหรือหยุดการทำงานของโปรแกรมสนอร์ตอินไลน์ในเครื่องไฟร์สกรีน สามารถทำการอัพเดต Signature ของสนอร์ตอินไลน์ที่อยู่ในไฟร์สกรีนและไฟร์เบรกได้ และยังสามารถสั่งเริ่มหรือหยุดการทำงานของเครื่องกับดักได้โดยการกดปุ่ม Start หรือ Suspend ซึ่งจะมีลักษณะดังในรูปถัดไป

รูปที่ 10.2 แสดงหน้า Status ของโปรแกรม Tartarus Management

- **หน้า Snort**

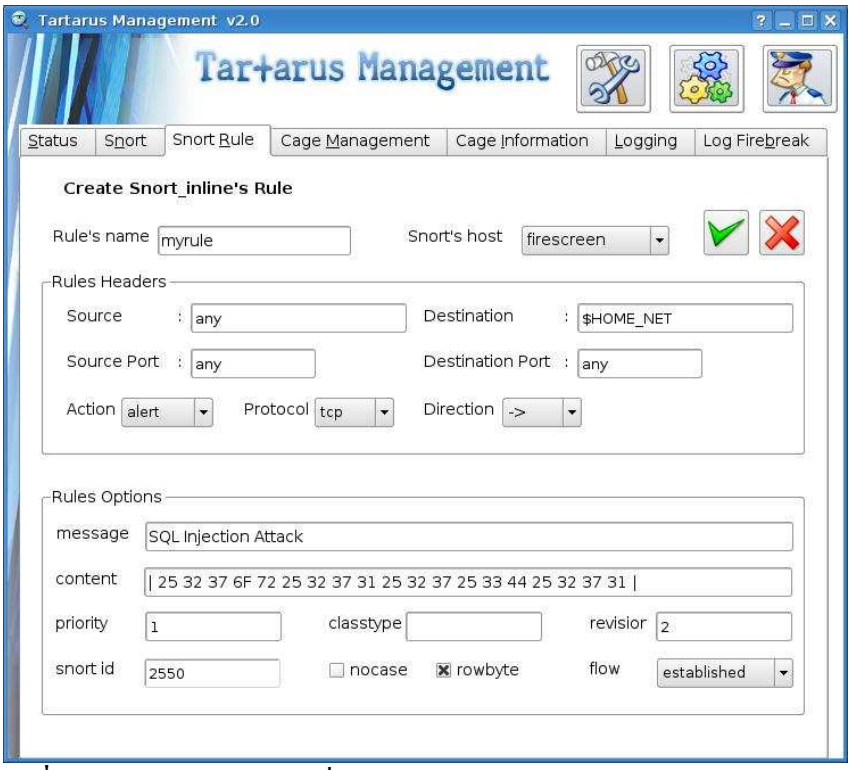
เป็นส่วนที่ใช้ในการเพิ่มหรือลดกฎของโปรแกรมสนอร์ตอินไลน์ที่เครื่องไฟร์สกรีนรวมถึงการอัพเดต Signature ของสนอร์ตอินไลน์โดยวิธีการเพิ่มกฎที่จะใช้จำแนกผู้บุกรุกสามารถทำได้โดยเลือกจากรายชื่อที่อยู่ด้านในกรอบAvaliable (กรอบด้านซ้าย) แล้วคลิ๊กที่ปุ่มลูกศร ⟶ แล้วกดปุ่ม Apply



รูปที่ 10.3 แสดงรูปในส่วนที่ใช้ในการกำหนดกฎ ให้กับระบบตรวจจับผู้บุกรุก

- **หน้า Create Snort Rule**

เป็นส่วนที่ให้ผู้ใช้สามารถทำการสร้างกฎสำหรับสนอร์ตอินไลน์ที่ใช้ในระบบได้ โดยผู้ใช้สามารถกำหนดส่วนเฮดเดอร์และออปชั่นต่าง ๆ ให้กับกฎของสนอร์ตอินไลน์ตามความต้องการ และเมื่อทำการกรอกข้อมูลเป็นที่เรียบร้อย ให้กฎปุ่ม ✓ จากนั้นโปรแกรมจะทำการอัพเดตกฎที่สร้างใหม่ไปยังเครื่องไฟร์สกรีนหรือไฟร์เบรกในระบบ เพื่อใช้งานต่อไป



รูปที่ 10.4 แสดงรูปในส่วนที่ใช้ในการสร้างกฎให้กับระบบตรวจจับผู้บุกรุก

- **หน้า Cage Management**

เป็นส่วนที่ใช้ในการจัดการกับเครื่องกับดักทั้งในส่วนของการสร้างเครื่องกับดักใหม่หรือลบเครื่องกับดักเก่า และกำหนดเงื่อนไขในการตรวจสอบสภาพของเครื่องกับดัก ซึ่งจะช่วยให้ผู้ดูแลระบบไม่จำเป็นต้องเข้าไปตรวจสอบด้วยตัวเอง เพราะโปรแกรมจะทำการตรวจสอบให้โดยอัตโนมัติอยู่ตลอดเวลาในการใช้งาน โดยสามารถสร้างเครื่องกับดักใหม่ได้จากเครื่องกับดักต้นแบบที่เก็บไว้ใน Cage Path (กำหนดพาธ ได้ในหน้าการ Configuration) ส่วนพาธที่เก็บเครื่องกับดักใหม่ที่สร้างขึ้นสามารถกำหนดได้ในช่อง Path ของหน้าต่างนี้

เงื่อนไขในการตรวจสอบสภาพเครื่องกับดักที่ผู้ใช้สามารเลือกให้โปรแกรมตรวจสอบได้แก่ จำนวนผู้ใช้ปัจจุบัน, จำนวนผู้ใช้ในกรุ๊ปรูท, เจ้าของไฟล์ /etc/passwd, password root ว่ามีการเปลี่ยนแปลงหรือไม่, และโหมดของไฟล์ /etc/passwd

<u>วิธีการสร้างไฟล์ config ของเครื่องกับดัก</u>

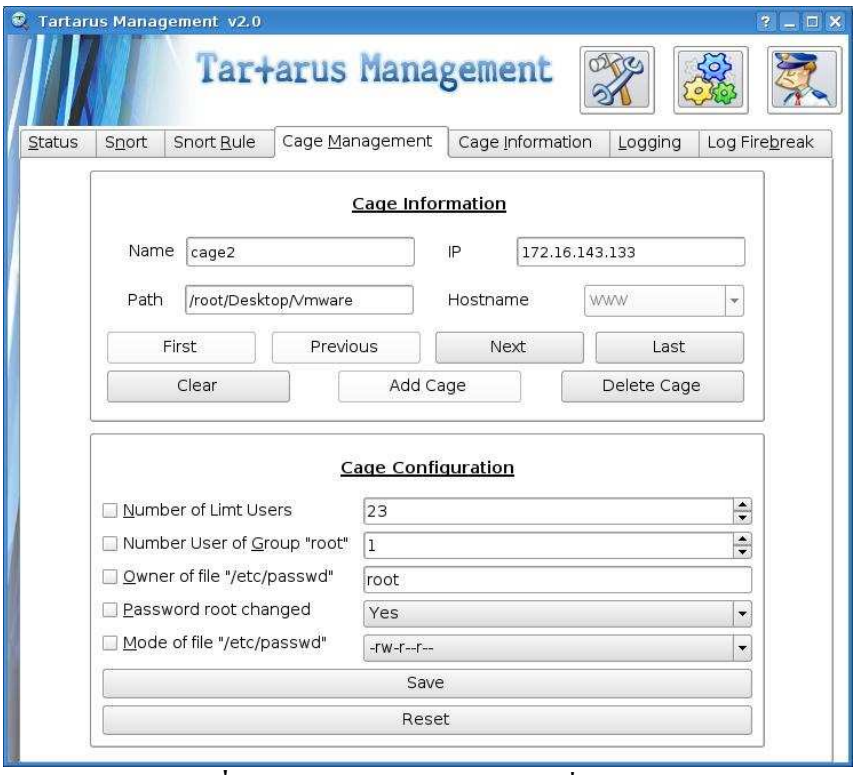
สามารถทำได้โดยเลือกเครื่องกับดักที่ต้องการโดยกดปุ่ม Next หรือ Previous แล้วเลือกเงื่อนไขที่ต้องการให้ตรวจสอบ จากนั้นกดปุ่ม save โปรแกรมก็จะทำการสร้างไฟล์ cage.conf ให้ โดยไฟล์นี้จะเก็บอยู่ในไดเรกทอรี่เดียวกับที่เก็บตัวอิมเมจของเครื่องกับดัก

<u>การสร้างเครื่องกับดักใหม่</u>

การสร้างเครื่องกับดักใหม่ สามารถทำได้โดยในขั้นแรกให้กดปุ่ม Clear จากนั้นให้พิมพ์ข้อมูลลงในช่องต่างๆ แล้วกดปุ่ม Add Cage

<u>การลบเครื่องกับดัก</u>

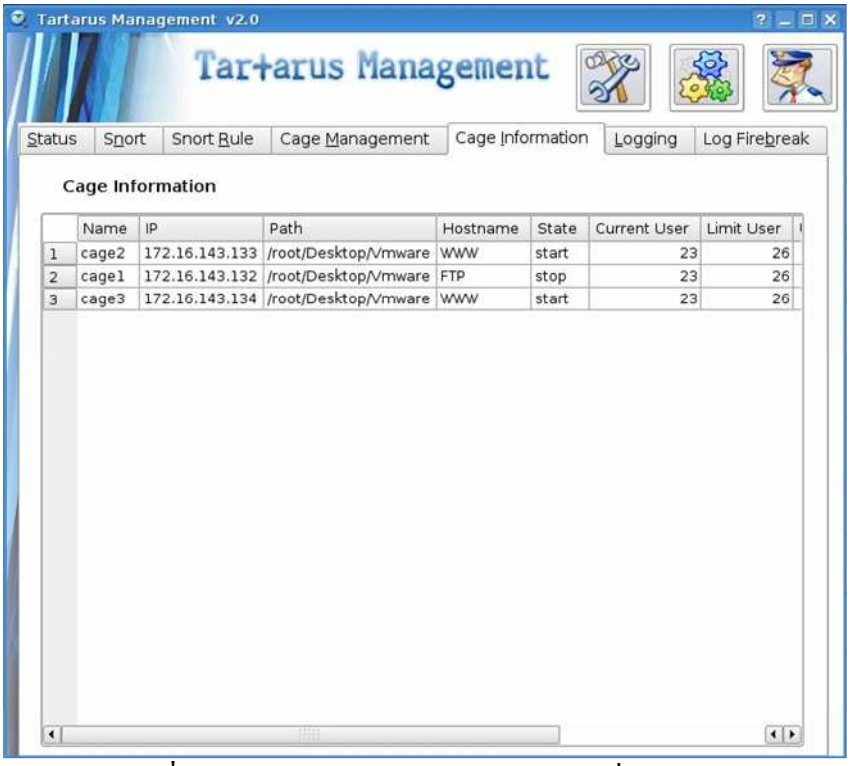
การลบเครื่องกับดักสามารถทำได้โดยการเลือกเครื่องกับดักที่ต้องการลบโดยกดปุ่ม next หรือปุ่ม Previous แล้วกดปุ่ม Delete Cage



รูปที่ 10.5 หน้าต่างส่วนจัดการเครื่องกับดัก

- **หน้า Cage Information**

ส่วน Cage Information เป็นส่วนที่ใช้แสดงข้อมูลของเครื่องกับดักที่เก็บอยู่ในฐานข้อมูลในเครื่องแม่ข่ายฐานข้อมูล (Log Server) ซึ่งจะแสดงถึงชื่อ, หมายเลขไอพีแอดเดรส, สถานะ, พาธที่เก็บเครื่องกับดัก และข้อกำหนดที่ใช้ตรวจสอบเครื่องกับดักนั้นๆ โดยในการติดต่อกับฐานข้อมูลภายในเครื่องแม่ข่ายฐานข้อมูลนั้นจะกระทำผ่านช่องทาง SSH ซึ่งสถานะของเครื่องกับดักที่แสดงในหน้าต่างนี้จะสอดคล้องกับสถานะของเครื่องกับดักจากหน้าต่าง Status



รูปที่ 10.6 หน้าต่างของส่วนแสดงข้อมูลเครื่องกับดัก

- **หน้า Logging**

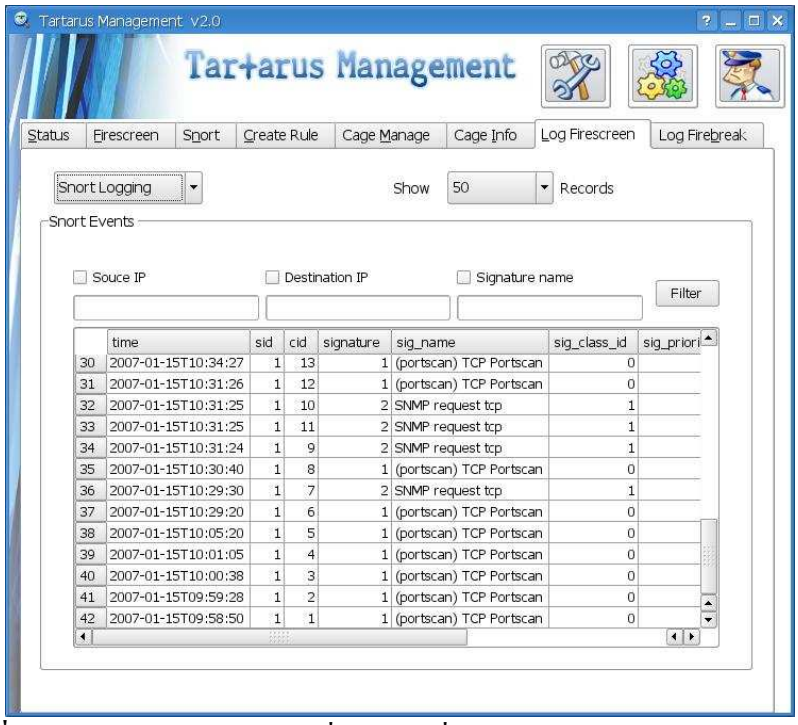
เป็นส่วนที่ใช้แสดงหน้าที่ใช้ในการดูข้อมูลล็อกไฟล์ ที่เก็บอยู่ในฐานข้อมูลภายในเครื่อง Logserver ซึ่งจะประกอบด้วยข้อมูลที่ได้จากโปรแกรมสนอร์ตอินไลน์, โปรแกรมเซมเฮน และโปรแกรมเซเบค ซึ่งทั้ง 3 โปรแกรมนี้จะทำการเก็บบันทึกที่แตกต่างกันดังนี้

Sebek จะทำการบันทึกการกระทำของผู้บุกรุก เช่น keystroke, ข้อมูลการนำเข้า หรือส่งออก, ไฟล์ที่ได้นำเข้าหรือส่งออก

Samhain จะทำการบันทึกการเปลี่ยนแปลงของไฟล์ต่างๆ ในเครื่องกับดัก ซึ่งจะทำให้ทราบผลจากคำสั่งของผู้บุกรุกว่าไปมีผลต่อไฟล์ใด หรือทำการแก้ไข หรือลบไฟล์ใด

Snort inline จะทำการบันทึกข้อมูลของชิ้นข้อมูลที่มีการตรวจพบว่าเป็นผู้บุกรุกจากเครื่องไฟร์สกรีน

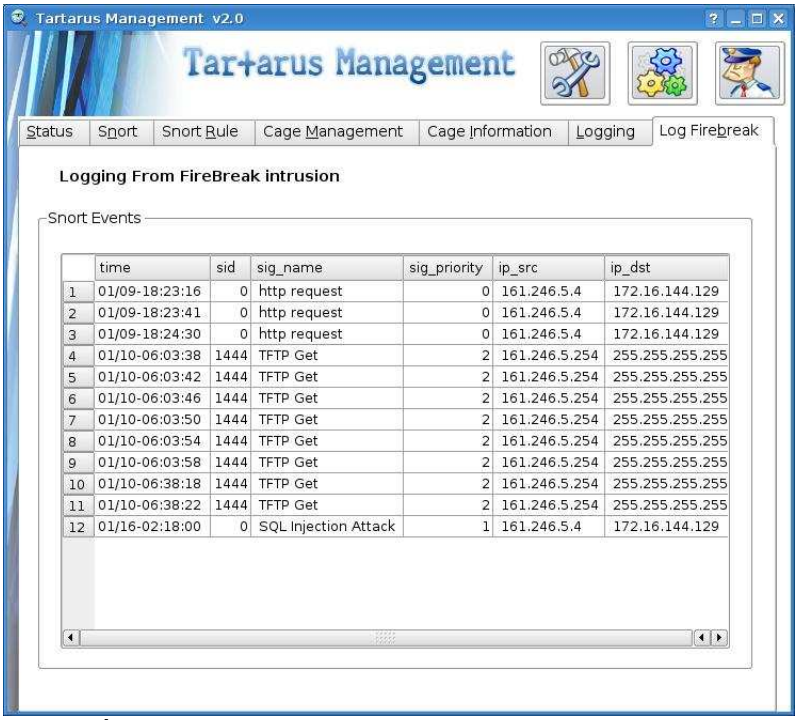
ผู้ใช้สามารถเลือกดูล็อกไฟล์จากแต่ละโปรแกรมโดยทำการเลือกที่ ComboBox ด้านบน แล้วโปรแกรมจะทำการดึงข้อมูลจากเครื่อง Logserver ออกมาแสดง นอกจากนั้นผู้ใช้สามารถค้นหาเฉพาะข้อมูลที่ต้องการโดยใส่ข้อมูลลงในช่องด้านบน แล้วกดปุ่ม Filter



รูปที่ 10.7 หน้าต่างแสดงข้อมูลที่เก็บในเครื่องดาต้าเบสเซิร์ฟเวอร์ (LogServer)

- **หน้า Log FireBreak**

แสดงล็อกไฟล์เกี่ยวกับการบุกรุกของผู้บุกรุกที่เข้ามาในระบบไฟร์เบรก โดยหลังจากที่โปรแกรมสนอร์ตอินไลน์ในไฟร์เบรกตรวจพบรูปแบบการบุกรุกที่เกิดขึ้นและทำการตัดการเชื่อมต่อนั้น ๆ โปรแกรมสนอร์ตอินไลน์จะทำการส่งล็อกไฟล์เหตุการณ์ที่เกิดขึ้นมาแสดงผล



รูปที่ 10.8 หน้าต่างแสดงข้อมูลล็อกไฟล์จากระบบไฟร์เบรก