บทที่ 5
วิเคราะห์ผลการทดลองและสรุป

5.1 บทสรุป

การใช้งานระบบเครือข่ายคอมพิวเตอร์ (Computer Network) เป็นที่นิยมอย่างแพร่หลาย ดังจะเห็นได้จากปริมาณการใช้งานเครือข่ายและจำนวนผู้ใช้ที่เพิ่มมากขึ้นตลอดเวลาขึ้น ทำให้เกิดความพยายามในสร้างโปรแกรมที่จะนำมาตรวจสอบและวัดตัวแปรสำคัญทั้ง 2 เพื่อนำข้อมูลที่ได้ไปวิเคราะห์ซึ่งนำไปสู่การจัดการและดูแลระบบเครือข่ายให้มีประสิทธิภาพสูงสุดโดยโปรแกรมเหล่านี้ได้แก่ โปรแกรมจัดการระบบเครือข่าย (Network Management Program) หรือ โปรแกรมตรวจสอบระบบเครือข่าย (Network Viewer Program) และโปรแกรมตรวจสอบเครื่องคอมพิวเตอร์ในเครือข่าย (Host Investigate Program) แต่เนื่องด้วยความเปลี่ยนแปลงของสภาพแวดล้อมในเครือข่ายปัจจุบันที่มุ่งเน้นความปลอดภัยมากขึ้นทำให้โปรแกรมเหล่านั้นไม่สามารถทำงานได้อย่างเต็มประสิทธิภาพและถึงแม้โปรแกรมบางโปรแกรมยังคงสามารถทำงานได้แต่ก็มีราคาแพงหรือไม่ก็สามารถแสดงข้อมูลได้เพียงบางส่วนทำให้เป็นหน้าที่ของผู้ดูแลระบบ (Network Administrator) ต้องนำข้อมูลจากโปรแกรมหลายโปรแกรมมาวิเคราะห์ด้วยตนเองก่อให้เกิดความเสียเวลาและอาจเกิดความผิดพลาดได้ ดังนั้น จึงต้องสร้างโปรแกรมที่มีความสามารถในการแสดงข้อมูลที่มีประโยชน์ต่อการดูแลและจัดการเครือข่ายรวมทั้งประมวลผลข้อมูล

โปรโตคอลเอสเอ็มเอ็นพี (SNMP Protocol) เป็นหนึ่งในโปรโตคอลที่มีมานานและอุปกรณ์ทางด้านระบบเครือข่ายเกือบทั้งหมดรองรับซึ่งสามารถบอกถึงปริมาณข้อมูลที่วิ่งผ่านอุปกรณ์ระบบเครือข่ายนั้นๆได้อย่างแน่นอน และการวิธีการพอร์ตแสกน (Port Scan) นอกจากจะสามารถตรวจสอบบริการทางระบบเครือข่าย (Network Service) ได้แล้วยังสามารถนำมาใช้แทนการPing ในการตรวจสอบสถานะของเครื่องคอมพิวเตอร์ในเครือข่ายได้อย่างมีประสิทธิภาพ ดังนั้นการนำวิธีการทั้งสองนี้มารวมไว้ในโปรแกรมเดียวกันและให้ภาระหน้าที่ในการประมวลผลไปถึงการวิเคราะห์ข้อมูลเบื้องต้นเป็นหน้าที่ของโปรแกรมแล้วย่อมลดภาระและความผิดพลาดของผู้ดูแลระบบได้

5.2 วิเคราะห์ผลการทดลอง

ความสามารถเกี่ยวกับระบบเครือข่าย

- สามารถตรวจสอบปริมาณ Traffic ของระบบเครือข่ายย่อยที่กำหนดและบันทึกสถิติได้

- สามารถตรวจสอบสถานะการเชื่อมต่อออกไปยัง Internet และเก็บสถิติไว้ได้

ความสามารถเกี่ยวกับเครื่องคอมพิวเตอร์ในเครือข่าย

- สามารถตรวจสอบสถานะเปิดปิดและเก็บสถิติได้
- สามารถตรวจสอบบริการทางเครือข่ายที่มีการเปิดใช้ได้
- สามารถตรวจสอบได้ว่ามีการติด Trojan หรือไม่

ความสามารถเกี่ยวกับการวิเคราะห์และแสดงผล

- สามารถแบ่งการตรวจสอบออกเป็นระบบเครือข่ายย่อยในช่วง IP Range ที่กำหนด และให้แต่ละช่วงมีการเก็บข้อมูล SNMP จากอุปกรณ์เครือข่ายคนละตัวได้
- สามารถแสดงปริมาณ Traffic ของระบบเครือข่ายทั้งการ Download หรือ Upload หรือทั้ง 2 อย่างในรูปแบบกราฟ 3 มิติตามวันที่กำหนดเพื่อง่ายต่อการเปรียบเทียบระหว่างระบบเครือข่ายย่อยได้
- สามารถแสดงปริมาณ Traffic ทั้งหมดตั้งแต่เริ่มตรวจสอบของระบบเครือข่ายย่อยทั้งการ Download หรือ Upload หรือทั้ง 2 อย่างในรูปแบบกราฟ 3 มิติตามวันที่กำหนดเพื่อง่ายต่อการเปรียบเทียบระหว่างระบบเครือข่ายย่อยได้
- สามารถแสดงปริมาณ Traffic เฉลี่ยของของระบบเครือข่ายทั้งการ Download หรือ Upload หรือทั้ง 2 อย่างในรูปแบบกราฟ 3 มิติเพื่อง่ายต่อการเปรียบเทียบระหว่างระบบเครือข่ายย่อยได้
- สามารถแสดงปริมาณเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายในรูปแบบกราฟ 3 มิติเพื่อง่ายต่อการเปรียบเทียบระหว่างระบบเครือข่ายย่อยได้
- สามารถแสดงเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบและปริมาณ Traffic ของระบบเครือข่ายย่อยในช่วงเวลาที่กำหนดได้
- สามารถจัดลำดับเครื่องคอมพิวเตอร์ในระบบเครือข่ายย่อยที่มีปริมาณ Traffic เฉลี่ยสูงสุด 5 ลำดับทั้งการ Download และ Upload และทั้ง 2 อย่าง
- สามารถ Save ข้อมูลทีได้จากการตรวจสอบระบบเครือข่ายเพื่อถ่ายโอนไปแสดงผลโดยนำไป Open กับตัวโปรแกรมที่เครื่องอื่นได้ง่าย
- สามารถแสดง System Log ของโปรแกรมได้

ความสามารถเฉพาะของโปรแกรม

- สามารถทำงานทั้งหมดที่กล่าวมาแม้ในสภาพแวดล้อมที่เครื่องคอมพิวเตอร์ในเครือข่ายมี
- การติดตั้ง Personal Firewall ก็ตาม
- สามารถถ่ายโอนโปรเจ็คการตรวจสอบระบบไปยังเครื่องคอมพิวเตอร์อื่นได้

5.3 ปัญหาอุปสรรคและแนวทางในการแก้ไข

1. อุปกรณ์ในเครือข่ายโดยส่วนใหญ่จะมีการรองรับ SNMP ในระดับพื้นฐานเหมือนกันแต่หากเป็นความสามารถของ SNMP อื่นๆจะรองรับแตกต่างกันขึ้นกับระดับของอุปกรณ์รวมไปถึงยี่ห้อของอุปกรณ์ด้วย จึงไม่สามารถนำความสามารถระดับสูงของ SNMP เช่น การดึงสถิติของการเชื่อมต่อระหว่าง Host, การดึงสถิติของ Traffic ในระดับ Port มาใช้ได้เพราะจะทำให้กลายเป็นโปรแกรมเฉพาะอุปกรณ์รวมไปถึงความที่ SNMP นั้นไม่ค่อยถูกใช้ทำให้มีผู้เข้าใจจริงน้อย การแก้ไขคือมีการดึงสถิติมาเฉพาะในส่วนของ SNMP พื้นฐานและทำให้ในส่วนของ การตั้งค่า SNMP น้อยที่สุดและมีเฉพาะส่วนที่จำเป็นจริงๆ

2. เนื่องจากสภาพแวดล้อมของเครือข่ายมีการใช้งาน Personal Firewall ทำให้การตรวจสอบอ้างอิงอยู่บนการ Scan Port มีผลให้การตรวจสอบระบบในแต่ละครั้งใช้เวลานานและมีความเปราะบางหากมีการโปรแกรมอื่นๆเข้ามาทำงานพร้อมๆกับการตรวจสอบระบบอาจทำให้ข้อมูลผิดพลาดหรือสูญหายได้ การแก้ไขคือมีการตัดความสามารถต่างๆของโปรแกรมชั่วคราวและไม่ใช้โปรแกรมที่มีการใช้งานระบบเครือข่ายหนักๆในช่วงที่ทำการตรวจสอบระบบ

3. เนื่องจากสภาพแวดล้อมของเครือข่ายมีการใช้งาน Personal Firewall ทำให้ไม่สามารถตรวจสอบ Traffic ต่อเครื่องคอมพิวเตอร์ในระบบได้โดยตรง การแก้ไขคืออาศัยค่าเฉลี่ยระหว่าง Traffic ของเครือข่ายย่อยกับจำนวนเครื่องที่มีสถานะเชื่อมต่อกับเครือข่ายในขณะนั้นเพื่อนำมาจัดลำดับเครื่องที่มีการใช้งานระบบเครือข่ายซึ่งจะได้ความแม่นยำระดับหนึ่ง

4. เนื่องจากวิธีการจัดวางหรือระบบโครงสร้างของระบบเครือข่ายในที่ต่างๆไม่เหมือนกันจึงอาจเป็นปัญหาในการตั้งค่าต่างๆสำหรับการดึงค่า SNMP ในช่วงที่ตรวจสอบระบบได้ การแก้ไขคือมีการตั้งค่าของระบบเครือข่ายย่อยได้ถึงระดับ Port ของอุปกรณ์และมีการแสดง Port ทั้งหมดของอุปกรณ์ออกมาเพื่อป้องกันการ ตั้งค่าผิด

5.4 ข้อจำกัดของโปรแกรม

1. ลำดับที่ได้จากโปรแกรมอาจมีความผิดพลาดเนื่องจากความจำกัดทางข้อมูล
2. การตั้งค่าช่วงของการตรวจสอบระบบถูกจำกัดไว้ที่ 10 นาทีเนื่องจากระยะเวลาของการตรวจสอบระบบในแต่ละครั้งมีเวลานานและมีการใช้งานทรัพยากรของเครื่องสูง
3. จำเป็นต้องมีการตรวจสอบระบบเป็นระยะเวลาหนึ่งจึงจะได้ข้อมูลด้านสถิติที่ถูกต้องมากขึ้น
4. การตรวจสอบระบบอาจมีปัญหาหากเครื่องที่ตั้งมีโปรแกรม Personal Firewall อยู่

5. ไม่สามารถตรวจสอบเครื่องปลายทางที่ทำการปิดพอร์ต เช่น เครื่องปลายทางที่ใช้ระบบปฏิบัติการ Linux และทำการปิดเซอร์วิสทั้งหมดได้
6. ไม่สามารถตรวจสอบการเปิดโปรแกรม P2P หรือ เกมส์ที่ทำการเปลี่ยนพอร์ตพื้นฐานของโปรแกรมได้
7. หากต้องการให้โปรแกรมสามารถเข้าไปดึงข้อมูล SNMP ในสวิตซ์หรือ เราเตอร์ได้ ผู้ดูแลระบบจำเป็นที่จะต้องทำการเปิดใช้บริการ SNMP ที่สวิตซ์หรือ เราเตอร์ตัวนั้นก่อน และทราบ SNMP Parameters(Read/Write Community) ของอุปกรณ์ตัวนั้น

5.5 แนวทางการพัฒนาต่อ

1. พัฒนาในส่วนของระบบการ Scan Port ขึ้นมาเองเพื่อนำมาใช้งานในโปรแกรมโดยเฉพาะเพื่อลดความล่าช้าและความผิดพลาดที่อาจจะเกิดขึ้นจากการเรียกใช้งานโปรแกรม Nmap
2. พัฒนาในส่วนของ Database ให้มีการ Share แบบ Online และมีการนำข้อมูลจากเครื่องอื่นๆมาวิเคราะห์ร่วมกันเพื่อให้ได้ข้อมูลที่ชัดเจนยิ่งขึ้น