บทที่ 4
รายงานผลการศึกษา

การสร้างระบบตรวจสอบการบุกรุกเครือข่ายภายในมหาวิทยาลัยราชภัฏเชียงราย โดยดำเนินการสร้างตามโครงสร้างที่ได้ออกแบบไว้ในบทที่ 3 มีองค์ประกอบของระบบดังต่อไปนี้

4.1 ระบบเครือข่ายที่ใช้ในการสร้างและทดสอบผล

ระบบเครือข่ายภายในมหาวิทยาลัยประกอบด้วยเครื่องแม่ข่ายที่ให้บริการจำนวน 22 เครื่อง ดังต่อไปนี้

(1) เครื่องให้บริการจดหมายอิเล็กทรอนิกส์ (Mail Server) .ใช้ระบบปฏิบัติการ Linux Fedora Core 3 จำนวน 3 เครื่องสำหรับ domain .ricr.ac.th,.stu.ricr.ac.th,.cru.in.th

(2) เครื่องให้บริการสำหรับเว็บไซต์สำหรับมหาวิทยาลัยใช้ ระบบปฏิบัติการ Microsoft Windows 2003 Server จำนวน 1 เครื่อง

(3) เครื่องให้บริการพื้นที่โฮมเพจของ หน่วยงาน อาจารย์ เจ้าหน้าที่และนักศึกษาใช้ ระบบปฏิบัติการ Microsoft Windows 2000 Advance Server จำนวน 2 เครื่อง

(4) เครื่องให้บริการ DNS ใช้ระบบปฏิบัติการ Microsoft Windows 2000 Advance Server จำนวน 1 เครื่อง

(5) เครื่องให้บริการ Gateway ติดตั้งระบบปฏิบัติการ Linux Fedora Core 2 จำนวน 1 เครื่อง

(6) เครื่องให้บริการ Radius ติดตั้งระบบปฏิบัติการ Redhat Linux 9 จำนวน 1 เครื่อง

(7) เครื่องให้บริการระบบการเงิน ติดตั้งระบบปฏิบัติการ Microsoft Windows 2000 Advance Server จำนวน 1 เครื่อง

(8) เครื่องให้บริการระบบ E-Learning ติดตั้งระบบปฏิบัติการ Microsoft Windows 2000 Advance Server จำนวน 1 เครื่อง

(9) เครื่องให้บริการพื้นที่เว็บไซต์ของคณะ ติดตั้งระบบปฏิบัติการ Microsoft Windows 2000 Advance Server จำนวน 11 เครื่อง

4.2 ส่วนประกอบของระบบตรวจจับการบุกรุกเครือข่าย

ในการสร้างระบบตรวจจับการบุกรุกภายในมหาวิทยาลัยราชภัฏเชียงรายนั้นได้ติดตั้งระบบดังต่อไปนี้

(1) เครื่องคอมพิวเตอร์ที่ทำหน้าที่ตรวจจับการบุกรุกใช้ระบบปฏิบัติ Linux Fedora core 3 ทำการติดตั้ง Snort 2.2.0

(2) เครื่องคอมพิวเตอร์ที่ทำหน้าที่รับข้อมูลจากเครื่องตรวจจับและจัดการเกี่ยวกับกฎของเครื่องตรวจจับ ทำการติดตั้ง โปรแกรมฐานข้อมูล MySQL version 4.1.10a โปรแกรม Apache Webserver version 2.0.53 โปรแกรมจัดการเรื่องกฎและเก็บสถิติการโจมตีของ snort ที่ได้ทำการพัฒนาขึ้นมา

ข้อมูลที่จัดเก็บนั้นจะถูกส่งมาจากเครื่องเซ็นเซอร์ของที่มีแต่ละจุดในเครือข่าย โดยเมื่อเซ็นเซอร์ตรวจพบการละเมิดกฎที่ได้เลือกใช้ในการตรวจสอบ จะทำการส่งข้อมูลผ่านเครือข่ายมายังเครื่องแม่ข่ายที่ติดตั้งฐานข้อมูล MySQL โดยข้อมูลนั้นจะส่งมาเก็บทันทีที่เหตุการณ์ถูกตรวจพบ

4.3 รายละเอียดและข้อมูลการบุกรุกที่ตรวจจับได้

ปริมาณการบุกรุกแยกตามโปรโตคอล

TCP (34%)

UDP (4%)

ICMP (63%)

Portscan Traffic (0%)

การตรวจจับเหตุการณ์ รูปแบบดังตัวอย่างตารางที่ 4.1

จากข้อมูลปริมาณการบุกรุกที่ตรวจจับโดยใช้กฎมาตรฐานที่ติดตั้งมากับโปรแกรมสนอร์ทนั้นจะได้ข้อมูลของปริมาณการบุกรุกที่มากที่สุดคือโปรโตคอล ICMP เนื่องจากเป็นโปรโตคอลพื้นฐานที่ใช้ในการตรวจสอบการทำงานของเครื่องที่อยู่ในเครือข่าย หรือเป็นขั้นตอนพื้นฐานในการโจมตีของผู้บุกรุกในการตรวจสอบเป้าหมายก่อนเริ่มดำเนินการโจมตี ทั้งนี้คาดว่าจะมีข้อมูลบางส่วนที่เป็นการรายงานที่ผิดพลาดของโปรแกรมระบบเอง (False Positive)

ตารางที่ 4.1 แสดงผลการตรวจจับรูปแบบการบุกรุกเครือข่าย

	< Signature >	< Classification >	< รวม # >	Sensor #
1	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	ไม่ทราบกลุ่ม	579 (8%)	2
2	[snort] ICMP Destination Unreachable Communication Administratively Prohibited	misc-activity	4595 (61%)	2
3	[snort] SCAN UPnP service discover attempt	network-scan	47 (1%)	2
4	nessus[snort] MS-SQL ping attempt	misc-activity	58 (1%)	1
5	[snort] BAD-TRAFFIC tcp port 0 traffic	misc-activity	47 (1%)	2
6	[arachNIDS][snort] ICMP PING NMAP	attempted-recon	16 (0%)	2
7	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	misc-activity	75 (1%)	1
8	[snort] ATTACK-RESPONSES directory listing	bad-unknown	1 (0%)	1

โดยสามารถแยกประเภทการบุกรุกเป็น 9 กลุ่ม ดังนี้

จากตารางที่ 4.1 พบว่าข้อมูลที่รายงานการบุกรุกในช่วงเวลาที่ติดตั้งระบบนั้น มีข้อมูลที่สามารถนำไปใช้งานในการช่วยป้องกันปัญหาที่เกิดขึ้นในเครือข่ายได้จริงเช่น ข้อที่ 4 เป็นการแจ้งเตือนว่ามีการพยายามเข้าใช้ฐานข้อมูล MS-SQL Server โดยเครื่องที่เป็นแหล่งกำเนิดนั้นติดไวรัสประเภท Worm ที่พยายามจะแพร่กระจายผ่านพอร์ตสื่อสารของ MS-SQL Server

ตารางที่ 4.2 แสดงกลุ่มการแจ้งเตือนที่ตรวจพบ

< กลุ่ม >	ยอดรวมที่พบ

ไม่ทราบกลุ่ม	2443 (22%)
misc-activity	7091 (64%)
network-scan	79 (1%)
attempted-recon	825 (7%)
bad-unknown	4 (0%)
web-application-activity	490 (4%)
web-application-attack	139 (1%)
attempted-admin	3 (0%)
attempted-dos	1 (0%)

จากข้อมูลตารางที่ 4.2 นั้นพบว่ากลุ่มหรือประเภทของการแจ้งเตือนที่ไม่ทราบกลุ่มนั้นมีมากที่สุด โดยส่วนใหญ่จะเป็นการผิดกฎเกณฑ์ในเรื่องของการ ping เนื่องจากผู้ศึกษาได้ทำการเลือกใช้กฎการตรวจสอบ โปรโตคอล icmp แต่ในเครือข่ายมิได้มีการบังคับการห้ามใช้คำสั่ง ping ดังนั้นปริมาณของข้อมูลในส่วนนี้จะมีมากที่สุด

ในช่วงเวลาที่ติดตั้งระบบประมาณ 1 เดือนนั้น มียอดรวมการแจ้งเตือน: 12,141 ครั้ง แยกเป็นดังนี้

- จำนวน IP addresses จากเครื่องต้นทาง: 248 address
- จำนวน IP addresses ไปยังเครื่องปลายทาง: 690 address
- จำนวน IP ลิงค์ที่ไม่ซ้ำ 1158 address
- จำนวน Ports จากเครื่องต้นทาง: 2021 port
    - แยกเป็น TCP (1989) และเป็น UDP (79)
- จำนวน Ports ไปยังเครื่องปลายทาง: 122
    - แยกเป็น TCP (118) และเป็น UDP (4)\