คู่มือประกอบการฝึกอบรมเชิงปฏิบัติการ

การติดตั้งระบบเก็บข้อมูลจราจร (Traffic Data) ตามพรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน) สมาคมอุตสาหกรรมซอฟต์แวร์ไทย

คำนำ

ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้ตั้งแต่วันที่ 22 สิงหาคม 2550 นั้น มีผลทำให้หน่วยงานต่างๆซึ่งเป็นผู้ให้บริการเข้าถึงระบบเครือข่ายอินเตอร์เน็ตจำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ไว้อย่างน้อย 90 วัน ปรากฏว่าหน่วยงานต่างๆส่วนใหญ่ยังขาดความรู้ความเข้าใจในเจตนารมณ์ของกฎหมาย และวิธีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ที่ถูกต้องและครบถ้วนตามที่กฎหมายกำหนด

ดังนั้นเพื่อให้หน่วยงานต่างๆ สามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์(Traffic Data)ได้ถูกต้องและครบถ้วนตามที่กฎหมายกำหนด และสามารถประหยัดงบประมาณในการจัดซื้อซอฟต์แวร์จากต่างชาติ **โดยการนำซอฟต์แวร์** Open Source ไปใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน) จึงเห็นควรให้มีการจัดจ้างทำคู่มือ พร้อมชุดติดตั้ง (Software package), Slideบรรยายประกอบ**การฝึกอบรมปฏิบัติการ, Courseware สำหรับใช้ทบทวนหรือศึกษาด้วยตนเอง** ให้กับผู้ประกอบการและผู้ดูแลระบบของหน่วยงานภาครัฐ นอกจากนั้นจัดให้มีการสนับสนุนภายหลังการอบรมผ่านทางเว็บไซต์ และทางโทรศัพท์ ให้กับผู้เข้าร่วมโครงการ โดยในการจัดจ้างในครั้งนี้ จะเป็นประโยชน์ต่อ ผู้ประกอบการและผู้ดูแลระบบของหน่วยงานภาครัฐหน่วยงานต่างๆ ในการที่จะนำไปใช้ นอกจากนี้แล้วสำนักงานฯ จะกำหนดให้คู่มือและชุดติดตั้งต่างๆ มีการกำหนดสิทธิในการเผยแพร่แบบโอเพนซอร์ส ซึ่งจะทำให้หน่วยงานต่างๆ สามารถนำเอาคู่มือและชุดติดตั้งประกอบ**การฝึกอบรม** ไปแก้ไขหรือพัฒนาต่อได้ ในกรณีที่มีการเปลี่ยน version ซึ่งจะเป็นการทำให้บุคลากรของผู้ประกอบการ และหน่วยงานต่างๆ ในประเทศไทยทันต่อการเปลี่ยนแปลงเทคโนโลยีอยู่เสมอ

เอกสารฉบับนี้เป็นคู่มือโครงการฝึกอบรมผู้ประกอบการในการติดตั้งและให้บริการคำปรึกษาระบบเก็บข้อมูลจราจร (Traffic Data) ตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ด้วยซอฟต์แวร์โอเพนซอร์ส สนับสนุนโดย สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน) ซึ่งต่อไปนี้เป็นการสรุปวัตถุประสงค์ ผลที่คาดว่าได้รับ โครงสร้างของหลักสูตร และหลักสูตรการฝึกอบรมของโครงการ

วัตถุประสงค์

1. เพื่อช่วยให้ผู้ประกอบการและผู้ดูแลระบบเข้าใจวัตถุประสงค์ที่แท้จริงของการเก็บข้อมูลจราจร (Traffic Data) ตาม มาตรา 26 ของ พรบ. การกระทำผิดด้วยคอมพิวเตอร์ พ.ศ. 2550
2. เพื่อให้ผู้ประกอบการและผู้ดูแลระบบเข้าใจวิธีการเก็บข้อมูลจราจร (Traffic Data) ที่ถูกต้องตามมาตรา 26 ของพรบ. การกระทำผิดด้วยคอมพิวเตอร์ พ.ศ. 2550
3. เพื่อให้ผู้ประกอบการและผู้ดูแลระบบสามารถเก็บข้อมูลจราจร (Traffic Data) ได้ด้วยซอฟต์แวร์โอเพนซอร์ส อย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด
4. เพื่อให้ผู้ประกอบการสามารถให้คำปรึกษาแก่ผู้รับบริการอย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด
5. เพื่อให้ผู้ประกอบการลดค่าใช้จ่ายในการจัดเก็บข้อมูลจราจร (Traffic Data)

ผลที่คาดว่าจะได้รับ

1. ได้หลักสูตร และระบบต้นแบบนำซอฟต์แวร์โอเพนซอร์สไปใช้เก็บข้อมูลจราจร (Traffic Data)
2. ประกอบการสามารถนำความรู้ที่ได้รับไปให้บริการให้คำปรึกษาและติดตั้งระบบเก็บข้อมูลจราจร (Traffic Data) ด้วยซอฟต์แวร์โอเพนซอร์สอย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด
3. System Admin ของหน่วยงานภาครัฐสามารถนำซอฟต์แวร์โอเพนซอร์สไปใช้เก็บข้อมูลจราจร (Traffic Data) ได้อย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด

หลักสูตรการฝึกอบรม

ชื่อหลักสูตร **หลักสูตรการติดตั้งระบบเก็บข้อมูลจราจร (Traffic Data) ตามพรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับด้วยคอมพิวเตอร์ พ.ศ. 2550 ด้วยซอฟต์แวร์โอเพนซอร์ส**

วัตถุประสงค์ ฝึกอบรมโดยการบรรยาย สาธิต และฝึก Hands-on ตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ด้วยซอฟต์แวร์โอเพนซอร์ส

จำนวนวัน 5 วัน

คุณสมบัติผู้เข้าฝึกอบรม

1. มีความรู้ทางด้านคอมพิวเตอร์และ Open Source
2. เป็นผู้ที่ดูแลระบบคอมพิวเตอร์ให้กับหน่วยงาน
3. เป็นผู้ที่สนใจในระบบการติดตั้ง ระบบเก็บข้อมูลจราจร (Traffic Data) ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับด้วยคอมพิวเตอร์ พ.ศ. 2550 ด้วยซอฟต์แวร์โอเพนซอร์ส

ลักษณะการฝึกอบรม : บรรยาย สาธิต ฝึกปฏิบัติ แลกเปลี่ยนประสบการณ์

โครงสร้างหลักสูตร

วันที่ 1 Syslog-NG

เป็นการอธิบายถึง พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับด้วยคอมพิวเตอร์ พ.ศ. 2550 อธิบายถึงสถาปัตยกรรมของระบบให้ถูกต้องตาม พรบ. อธิบายถึงสถาปัตยกรรมของ Syslog-NG และวิธีการติดตั้ง

เป็นหลักสูตรที่ตรงกับข้อ 8 ของประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

วันที่ 2 ปฏิบัติการการติดตั้งซอฟต์แวร์ Syslog-NG

เป็นการฝึกการปฏิบัติการติดตั้ง Syslog-NG โดยการสาธิต และให้ผู้เข้ารับการอบรมติดตั้ง มีผู้ช่วยฝึกให้การช่วยเหลือ

วันที่ 3 NTP Server และ NTP Client

ปฏิบัติการการติดตั้งซอฟต์แวร์ NTP Server และ NTP Client

เป็นการอธิบายถึงสถาปัตยกรรมของ NTP ทั้ง Server และ Client รวมทั้งเป็นการฝึกการปฏิบัติการติดตั้ง NTP Server และ NTP Client โดยการสาธิต และให้ผู้เข้ารับการอบรมติดตั้ง มีผู้ช่วยฝึกให้การช่วยเหลือ

เป็นหลักสูตรที่ตรงกับข้อ 9 ของประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

วันที่ 4 Authentication

เป็นการอธิบายถึงสถาปัตยกรรมของ Authentication รวมทั้งเป็นการฝึกการปฏิบัติการติดตั้ง Authentication โดยการสาธิต และให้ผู้เข้ารับการอบรมติดตั้ง มีผู้ช่วยฝึกให้การช่วยเหลือ

เป็นหลักสูตรที่ตรงกับข้อ 2 ภาคผนวก ข แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

วันที่ 5 ปฏิบัติการการนำ Syslog-NG, NTP Server, NTP Client และ Authentication ทำงานร่วมกัน

ให้ผู้เข้ารับการอบรมทำการติดตั้ง Syslog-NG, NTP Server, NTP Client และ Authentication ทำงานร่วมกัน มีผู้ช่วยฝึกให้การช่วยเหลือ

การวัดผล : ผู้เข้าอบรมจะต้องสามารถทำ**การติดตั้ง Syslog-NG, NTP Server, NTP Client และ Authentication ได้**

ประกาศนียบัตร : ผู้ที่ผ่านหลักสูตรตามเงื่อนไขการวัดผล จะได้ Certificate of Completion จาก SIPA หรือ จาก ATSI หรือ SIPA ร่วมกับ ATSI

คู่มือประกอบการฝึกอบรมเชิงปฏิบัติการ
การติดตั้งระบบเก็บข้อมูลจราจร (Traffic Data)
ตาม พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ลิขสิทธิ์โดย สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน)
89/2 หมู่ 3 อาคาร 9 ชั้น 11 บมจ. ทีโอที ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 0-2554-0400
โทรสาร 0-2554-0401

ผู้ดำเนินการ สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
99/30 หมู่ 4 ชั้น 5 อาคารซอฟต์แวร์พาร์ค ถ.แจ้งวัฒนะ ข.ปากเกร็ด ต.คลองเกลือ จ.นนทบุรี 11120
โทรศัพท์ 0-2583-9992,0-2962-2900ต่อ 1501 หรือ สายตรง 0-2962-1348
โทรสาร. 0-2962-1349
E-mail: info@atsi.or.th

ผู้บริหารโครงการ บริษัท เบนซ์มาร์ค วิชั่น จำกัด
Mobile : 089 797 8262
e-mail: bv2551@gmail.com

สารบัญ

บทที่ 1 ความเป็นมา.....1
บทที่ 2 การติดตั้ง Log Server.....8
บทที่ 3 การปรับแต่งหลังติดตั้ง.....29
บทที่ 4 การติดตั้ง NTP Server.....41
บทที่ 5 การติดตั้ง Syslog Server.....49
บทที่ 6 การทำ kernel Harden.....82
บทที่ 7 การทำ Firewall.....108
บทที่ 8 การทำ Backup and Restore.....134
ภาคผนวก ก.
บรรณานุกรม

บทที่ 1
ความเป็นมา

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ
พ.ศ. 2550

ข้อ 8 การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(1) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(2) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่ เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

(3) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้การส่งมอบข้อมูลนั้นเป็นไปด้วยความรวดเร็ว

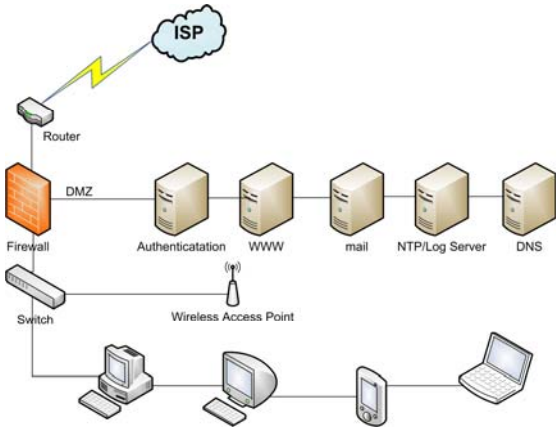
(4) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้(Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

ข้อ 9 เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการ ต้องตั้งนาฬิกา ของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาด**ไม่เกิน 10 มิลลิวินาที**

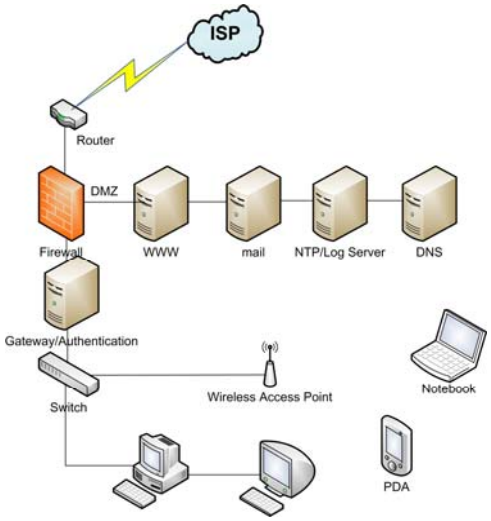
ข้อความข้างต้นคัดลอกมาจากส่วนหนึ่งของ พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ สำหรับคู่มือเล่มนี้เป็นการแนะนำวิธีการติดตั้ง Log Server ตามกฎหมายอย่างประหยัดด้วย Open source ที่มีมาให้ใช้บน Linux ไม่ต้องไปเสียค่าลิขสิทธิ์ใด ๆ เพราะ Linux ทุกค่ายออกแบบมาให้ใช้เป็น Network Operating System (NOS) มีการบันทึก Log file ให้เป็นปกติเพื่อให้ผู้ดูแลระบบสามารถวิเคราะห์ปัญหาหรือควบคุมดูแลระบบได้อย่างดีและครบถ้วนอยู่แล้ว เพียงแต่ผู้ดูแลระบบต้องปรับวิธีการวางแผนติดตั้งเสียใหม่ให้ตรงตามกฎหมาย สำหรับกฎหมายฉบับนี้ไม่อนุญาตให้ผู้ดูแลระบบ (System Administrator) เข้าถึง Log file ได้ ดังนั้นผู้ดูแลคงต้องทำการวางแผนติดตั้งและทำการกำหนดเรื่อง Security ให้ระบบรวมถึงการทำ Data hashing และ Data Archiving ในการเข้าถึงข้อมูลต้องให้ IT Auditor หรือผู้ที่ได้รับมอบหมายจากผู้บริหารระดับสูงให้ดูแล

คู่มือเล่มนี้ ไม่ได้มีเฉพาะการติดตั้ง NTP และ Log Server เท่านั้น ผู้ที่ได้รับการแต่งตั้งให้ดูแลรักษาข้อมูลจราจรเครือข่ายคอมพิวเตอร์ต้องมีการทำเรื่องความปลอดภัยให้กับ Log Server ดังนั้น รายละเอียดการป้องกัน Linux Server ได้นำมาแนบในภาคผนวกเพื่อให้สามารถรองรับการสร้างระบบความปลอดภัยให้มากขึ้น

ตัวอย่างผังการวางตำแหน่ง Authentication, NTP/Log Server

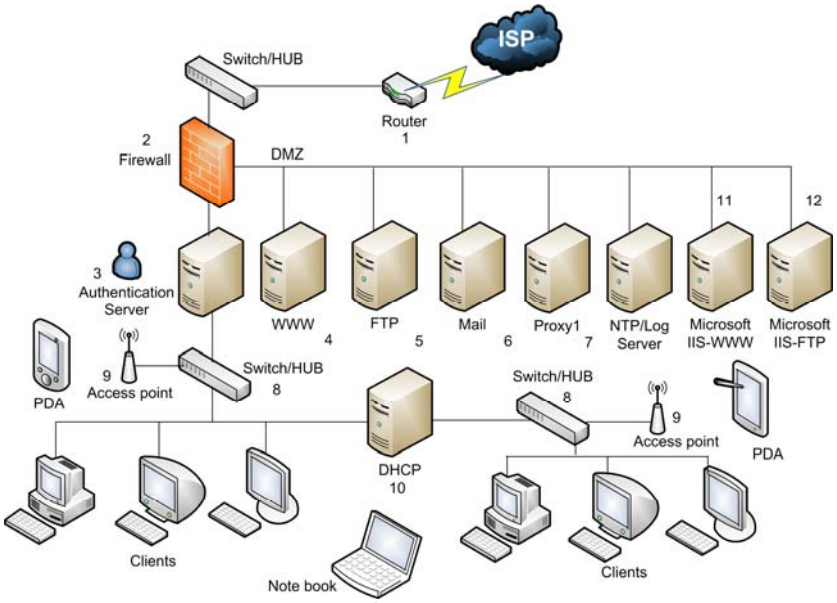


การวาง Authentication server และ Log server ไว้ที่ DMZ



การวาง Authentication server เป็น Gateway

แผนผังการนำ configuration syslog-ng ไปใช้งาน



ให้สังเกตภาพข้างบนว่ามีหมายเลขกำกับที่อุปกรณ์ต่าง ๆ (โปรดสังเกตว่าถ้าหมายเลขซ้ำกันหมายถึงอุปกรณ์ชนิดเดียวกันไม่ใช่พิมพ์ผิด) **ไม่ว่าระบบจริงจะจัดรูปแบบใดให้นำ configuration ไปใส่ให้ตรงก็ใช้งานได้** ในการนำไปใช้งานเพียงแต่ Copy file ที่อยู่ใน MyBooks ใน CD ชุดติดตั้ง Syslog-NGจะเป็น syslog-ng.conf ของเครื่อง Client ทั้งหมด ตัวอย่างเช่น

หมายเลข 1 หมายถึง เครื่อง Router ให้ทำการแก้ไขค่า Configuration ที่ตัวอุปกรณ์ให้ส่งค่า log ไปยัง remote log server ตามตัวอย่าง

ตัวอย่าง Cisco router

#conf t

#logging buffered notice

#logging buffered 64000

#logging history size 250

#logging <host or ip addr> ใส่ ip address ของ log server

#logging trap informational

#logging source-interface Loopback 0

#logging facility local2

#wr

หมายเลข 2 หมายถึง เครื่อง Firewall ที่ใช้โปรแกรม IPTABLES สำหรับดักจับการรับส่ง Packet ประเภท IM ตามภาคผนวก ฉ ให้ทำการแก้ไขค่า Configuration ตามตัวอย่างในบทที่ 7 เพื่อให้ส่งค่า log ไปยัง remote log server เพื่อตรวจจับการใช้งาน IM เช่น (MSN, ICQ, YAHOO และโปรแกรมอื่น ๆ ให้ทำเพิ่มตามหมายเลข port ที่แต่ละโปรแกรมใช้งาน) เก็บ log ส่วนนี้ไว้เปรียบเทียบกับ Authentication log และ Proxy access.log อีกชั้นหนึ่ง

หมายเลข 3 หมายถึง เครื่อง Authentication Server อาจต้องทำการ แก้ไขค่า ldap.conf หรือค่า radiusd.conf แล้วแต่จะใช้โปรแกรมอะไรทำหน้าที่ Authenticate เพื่อตรวจสอบว่ามีการส่ง log file เข้าสู่ syslog หรือไม่ ส่วนใหญ่จะส่งค่าไปเก็บที่ message อยู่แล้ว จากนั้นให้ทำการ copy file ldap_syslog-ng.conf หรือไฟล์ radius_syslog-ng.conf ไปทับไฟล์เดิมที่ /etc/syslog-ng/syslog-ng.conf จากนั้นให้สั่ง Restart syslog-ng เสร็จแล้วให้ restart service ก็จะได้การส่ง log file จากเครื่อง Authication Server ที่สมบูรณ์

หมายเลข 4 หมายถึง เครื่อง Web Server ให้ทำการ copy file www_syslog-ng.conf ไปทับไฟล์เดิมที่ /etc/syslog-ng/syslog-ng.conf จากนั้นให้สั่ง Restart syslog-ng แล้วทำการแก้ไขค่า httpd.conf ตามตัวอย่างในบทที่ 5 หลังสั่ง Restart httpd ก็จะได้การส่ง log file จากเครื่อง Web Server ที่สมบูรณ์

หมายเลข 5 หมายถึง เครื่อง FTP Server ให้ทำการ copy file ftp_syslog-ng.conf ไปทับไฟล์เดิมที่ /etc/syslog-ng/syslog-ng.conf จากนั้นให้สั่ง Restart syslog-ng แล้วทำการแก้ไขค่า vsftpd.conf ตามตัวอย่างในบทที่ 5 หลังสั่ง Restart vsftpd ก็จะได้การส่ง log file จากเครื่อง FTP Server ที่สมบูรณ์

หมายเลข 6 หมายถึง เครื่อง Mail Server ให้ทำการ copy file mail_syslog-ng.conf ไปทับไฟล์เดิมที่ /etc/syslog-ng/syslog-ng.conf จากนั้นให้สั่ง Restart syslog-ng แล้วทำการแก้ไขค่า dovecot.conf ตามตัวอย่างในบทที่ 5 หลังสั่ง Restart dovecot ก็จะได้การส่ง log file จากเครื่อง Mail Server ที่สมบูรณ์

หมายเลข 7 หมายถึง เครื่อง Proxy Server ให้ทำการ copy file squid_syslog-ng.conf ไปทับไฟล์เดิมที่ /etc/syslog-ng/syslog-ng.conf จากนั้นให้สั่ง Restart syslog-ng แล้วทำการแก้ไขค่า squid.conf ตามตัวอย่างในบทที่ 5 หลังสั่ง Reconfigure squid ก็จะได้การส่ง log file จากเครื่อง Proxy Server ที่สมบูรณ์

หมายเลข 8 หมายถึง เครื่อง Manage Switch ให้ทำการแก้ไขค่า Configuration ที่ตัวอุปกรณ์ให้ส่งค่า log ไปยัง remote log server ตามตัวอย่าง

<u>Catalyst CAT Switches running CATOS</u>

set logging server enable

set logging server 192.168.1.12

set logging level all 3 (local 3 ตรงกับค่า syslog-ng รอรับ)

set logging server severity 6 (เป็น information)

<u>กรณีเป็นรุ่นหรือยี่ห้ออื่นให้ดูคำสั่งจากคู่มือและกำหนดคาให้มี facility local 3</u>

หมายเลข 9 หมายถึง เครื่อง Wireless Access Point ให้ทำการ ตั้งค่า log ให้ส่งค่าไปยัง remote log server ส่วนมากจะมีเมนูให้กรอกค่า IP Address และให้เลือกค่า Facility ก็ให้เลือก Facility เป็น 7

หมายเลข 10 หมายถึง เครื่อง DHCP Server ให้ทำการ copy file dhcp syslog-ng.conf ไปทับไฟล์เดิมที่ /etc/syslog-ng/syslog-ng.conf จากนั้นให้สั่ง Restart syslog-ng แล้วทำการแก้ไขค่า dhcpd.conf ตามตัวอย่างในบทที่ 5 หลังสั่ง Restart dhcpd ก็จะได้การส่ง log file จากเครื่อง DHCP Server ที่สมบูรณ์

หมายเลข 11 หมายถึง เครื่อง Microsoft Windows 2xxx Server ที่ติดตั้ง IIS เพื่อให้บริการ Web Server ให้อ่านวิธีการติดตั้งโปรแกรมส่ง log ได้จากบทที่ 5 ก็จะสามารถเก็บบันทึก log file ของ web server ได้ครบถ้วน

หมายเลข 12 หมายถึง เครื่อง Microsoft Windows 2xxx Server ที่ติดตั้ง IIS เพื่อให้บริการ FTP Server ให้อ่านวิธีการติดตั้งโปรแกรมส่ง log ได้จากบทที่ 5 ก็จะสามารถเก็บบันทึก log file ของ FTP server ได้ครบถ้วน

บทสรุป

ทั้งนี้ต้องไม่ลืมว่ามีบางเรื่องที่ผู้เขียนไม่สามารถทราบถึงข้อมูลได้เช่นอุปกรณ์เครือข่าย (Network device) ที่แต่ละองค์กรหรือหน่วยงานมีใช้กัน จึงต้องรบกวนให้แต่ละแห่งศึกษาคำสั่งจากคู่มือของโรงงาน เพื่อทำการแก้ไข Configure ให้สามารถส่ง log ไปเก็บยัง Log Server ได้ และที่สำคัญที่สุดควรคำนึงเรื่องการเก็บค่าที่จำเป็นเท่านั้นเช่นถ้าพบว่ามีการส่ง log ไปเก็บมากเกินไป กรณีตัวอย่างการส่ง log จาก Authentication server ไปด้วยค่าที่ไม่จำเป็นต่าง ๆ ที่ระบบแจ้งออกไปเช่นค่า facility level 1 ถึง 7 บางครั้งต้องทำการ filter เพื่อกรองให้ส่งไปเฉพาะข้อมูลที่ต้องการเช่น user account, ip address, วัน เวลา ที่มีการร้องขอเข้าใช้ระบบเป็นต้น และในส่วนการส่งค่าของ Hardware ต้องเปิดไฟล์ของเครื่อง Log Server ที่ /etc/syslog-ng/syslog-ng.conf ดูก่อนว่าผู้เขียนรอรับค่า facility level อะไร จะได้ส่งค่าไปให้เครื่องรับได้ถูกต้อง ที่ต้องดูเป็นพิเศษสำหรับองค์กรขนาดใหญ่อาจมีอุปกรณ์เครือข่ายจำนวนมาก ให้ใช้วิธีการ filter เป็นชื่อ host และค่า local level เช่น host("3com_6") and facility (local6)

บทที่ 2

การติดตั้ง Log & Time Server

ในคู่มือนี้จะใช้ Log Server 2.0 ซึ่งปรับปรุงจาก Fedora release 8 ที่ Update ล่าสุด ณ วันที่สร้างแผ่น (วันที่ 3 มิถุนายน 2551) โดยผู้เขียนได้เลือกเฉพาะ Packages ที่ทำงานใน Server Mode และเป็นแบบ Text เท่านั้น ทำให้มีขนาดไฟล์เล็กและกินทรัพยากรน้อย เหมาะสำหรับทำงาน 2 หน้าที่เท่านั้น ทำให้เสี่ยงต่อความปลอดภัย ในการดูแลรักษาข้อมูล Log file เพื่อไม่ให้เสียเวลา คงต้องมาเตรียมจัดหาเครื่องที่จะทำงานกันคือ Log Server และ Time Server ในแผ่นนี้โปรแกรมที่ใช้ทำ Log Server คือ syslog-ng (ng = New Generation) ส่วน Time Server ใช้โปรแกรม ntp (Network Time Protocol) และเมื่อนำ Fedora release 8 ซึ่งถือว่า Stable ที่สุดในขณะนั้นมาพัฒนาใช้งาน เพราะ Release 9 เพิ่งออกยังไม่ได้ทดลองใช้งาน ไม่รู้ว่ามีจุดอ่อนส่วนใดบ้างเลย เพราะน่าเป็นห่วงมากเรื่องที่ คนทั่วไปมักใช้ PC มาทำ Server ซึ่งมีปัญหาเรื่องการเปิดใช้งานตลอด 24 ชั่วโมงแล้วมักเสียเร็วกว่าปกติ เพราะอายุการใช้งานของภาคจ่ายไฟ รวมไปถึงอุณหภูมิสะสมมีมากเกินไป เพราะเครื่อง PC ไม่ได้ออกแบบมาให้ทำงานหนักแบบนี้ ดังนั้นผู้เขียนขอแนะนำให้ จัดซื้อเครื่อง Server แท้ ที่มีรายละเอียดดังนี้

1. เป็นเครื่องที่มีสถาปัตยกรรมเป็น Server โดยเฉพาะ
2. หน่วยความจำหลักไม่น้อยกว่า 512 MB
3. ความจุ Hard disk ไม่น้อยกว่า 250 GB ประมาณจากการเก็บ log file ต่อวัน แล้วคูณด้วย 90 ถึง 365 ถึงจะเพียงพอ แต่ถ้าไม่สามารถซื้อความจุมาก ได้ก็ให้ทำการจัดเก็บลง CD/DVD ก็ได้
4. มีเครื่องบันทึก CD/DVD อย่างน้อย 1 เครื่อง
5. มี Network Interface 100/1000 Mbps 1 port

ส่วนประกอบอื่น ๆ ไม่ค่อยจำเป็น เช่น CPU เอา spec ต่ำ ๆ จะได้ไม่เสียเงินมากเกินไป และที่สำคัญคือ OS ทำงานบน Text Mode จึงไม่เน้นจอภาพและ Mouse ดูเรื่องระบบความปลอดภัยของ BIOS ให้มีมาก ๆ เข้าไว้จะดีมาก

โดยหลักการที่ถูกต้อง ผู้ดูแลระบบจะต้องเป็นผู้คิดและวางแผนการทำงานทั้งหมดไว้ในผังงาน ที่ถูกกำหนดโดยผู้รับผิดชอบงานแต่ละด้าน อาจเขียนเป็นแบบแปลนลงในกระดาษหรือสมุด สำหรับให้ผู้อื่นสามารถดูแลระบบ และขยายงานในอนาคตต่อไปได้ สิ่งที่จำเป็นในการทำระบบมีดังต่อไปนี้

1. กำหนดผังระบบ Network ของหน่วยงานหรือองค์กรโดยละเอียด
2. ตรวจสอบว่าเครื่องที่ทำ Server ตามกฎหมายมีกี่เครื่อง
3. ตรวจสอบอุปกรณ์ Network เช่น Manage Switch อุปกรณ์ที่มีการทำ Configuration แจก IP Address ให้กับลูกข่าย รวมไปถึง Wi-Fi ประเภท Access point ที่วางไว้แต่ละจุดโดยละเอียด
4. หากมีการทำระบบ Remote Access หรือ Terminal Server ต้องเก็บ Log ด้วย

สรุป..... ขั้นตอนการติดตั้งโดยสังเขป

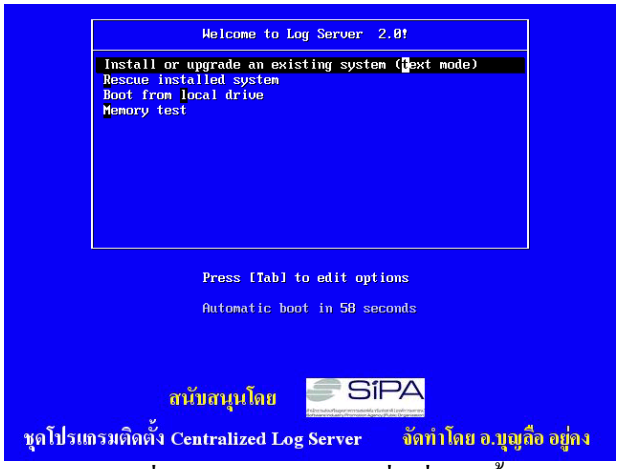
1. Boot ด้วยแผ่น CD Log Server 2.0

2. ติดตั้งตามขั้นตอนในบทที่ 2 นี้
3. ปรับแต่งหลังติดตั้งให้พร้อมใช้ในบทที่ 3
4. ทำ Firewall ให้ Log Server ในบทที่ 7

ขั้นตอนการติดตั้ง Log และ Time Server

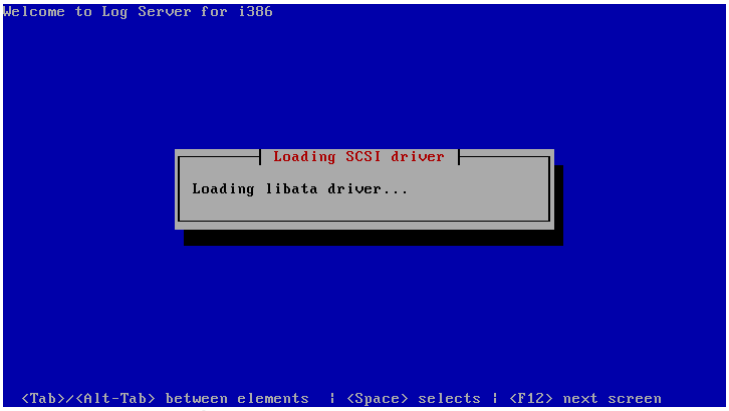
สำหรับการติดตั้ง Log server ก็ไม่ต่างจากการติดตั้ง Linux Server เพราะส่วนของการติดตั้งนำมาจาก Linux Server ทั้งหมดต่างกันตรงเมนูหรือรายการที่เลือกแต่ละ Service จะลดลงเหลือเพียง 3 รายการ คือ NTP Server, Log Server และ C++ Compiler ที่ต้องมีส่วนของภาษา C ก็เพราะบางคนถนัดที่จะไปหา Download โปรแกรมที่เป็น Source Code ภาษาซี มาทำการ Compile และทำการติดตั้งด้วยตนเอง เพราะโปรแกรมแบบนี้มักมีการปรับปรุงรุ่นให้ใหม่เสมอแต่พวก Distributor ค่ายต่าง ๆ มักจะ Update ช้า ผู้เขียนแนะนำว่าถ้าไม่จำเป็นต้องใช้ก็อย่าเลือกติดตั้งภาษาซี เพราะจะทำให้ระบบไม่ปลอดภัยจากผู้บุกรุก หรือถ้าใช้งานเสร็จก็ควรลบออกจากระบบให้เรียบร้อยก่อนเสมอ เพื่อไม่ให้สับสนและเสียเวลามากเกินไป ลองมาดูวิธีการติดตั้งเป็นลำดับ (Step-by-Step) ดังต่อไปนี้

ขั้นที่ 1 เริ่มต้นติดตั้ง Log Server



รูปที่ 2.1 แสดงจอภาพเมื่อเริ่มติดตั้ง

หลังจาก Boot จาก CD จะพบว่ามีเมนูสวยงาม รอให้เลือกว่าจะทำอะไรมีทั้งหมดสี่เมนู ในส่วนที่จะทำงานก็ต้องเลือกรายการแรก แล้วให้กด Enter ได้เลย จากนั้นโปรแกรมจะทำการ Load Module driver ของ Hardware ที่จำเป็นในการทำงานเช่น Hard disk controller Driver เพื่อให้สามารถเห็น Hard disk ที่อยู่ในเครื่องเพื่อทำการติดตั้งต่อไป



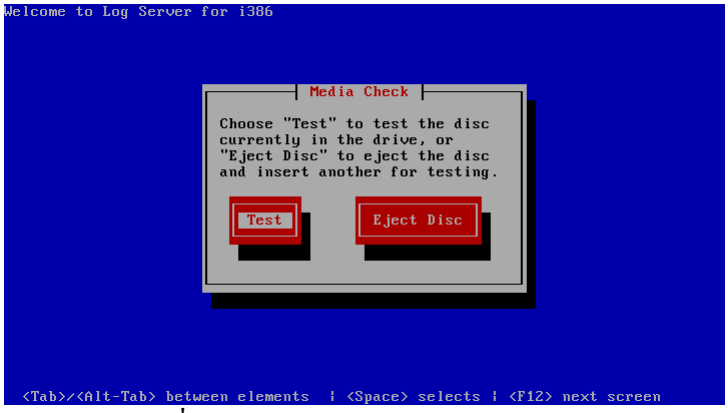
รูปที่ 2.2 แสดงการ Load SCSI driver

หลังจาก Load Driver เสร็จเครื่องพร้อมทำงานต่อไปก็จะตรวจสอบว่ามี Hard disk และ CD drive อยู่ในระบบหรือไม่ เพื่อจะได้เลือกว่าจะทำการติดตั้งโปรแกรมจากแหล่งข้อมูลใด หากไม่พบ CD มันจะถามว่าจะให้ติดตั้งจากที่ไหน แต่ถ้าพบ CD drive มันจะแสดงรายการในหน้าจอถัดไป

ขั้นที่ 2 ในขณะนี้ Linux ตรวจพบว่าคุณกำลังติดตั้งจาก CD ROM จะทำการตรวจสอบแผ่นให้ว่าแผ่น CD สมบูรณ์หรือไม่ ควรเลือก OK เพื่อทำการทดสอบว่า Package ต่าง ๆ ที่บรรจุอยู่บนแผ่น CD ทำงานได้ครบถ้วนหรือไม่ แต่ถ้ามั่นใจว่า CD ปกติหรือเคยทดสอบมาแล้ว พร้อมติดตั้งให้เลือก Skip ได้

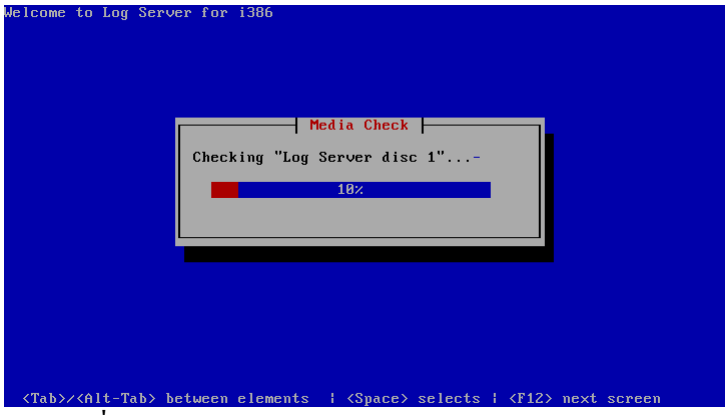
รูปที่ 2.3 แสดงการตรวจพบว่าใช้แผ่น CD ในการติดตั้ง

หลังเลือก OK ก็จะปรากฏหน้าจอภาพใหม่ให้ทำการเลือกว่า Test หรือจะเลือก Eject Disc ดังนี้



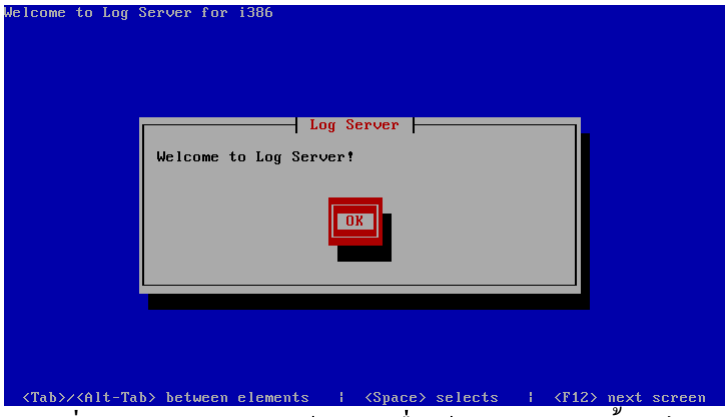
รูปที่ 2.4 แสดงเมนูเลือกทดสอบแผ่น CD

ผู้เขียนแนะนำว่าถ้ายังไม่เคย Test ให้เลือกเมนู Test จะได้ไม่ต้องเสียเวลาติดตั้งหากแผ่นไม่สมบูรณ์หรือมี Package บางตัวไม่สมบูรณ์ทำให้ติดตั้งไม่ผ่าน เมื่อเลือก Test ก็รอผลไม่นานจะมีภาพการทดสอบดังนี้



รูปที่ 2.5 แสดงความก้าวหน้าในการตรวจสอบแผ่น CD

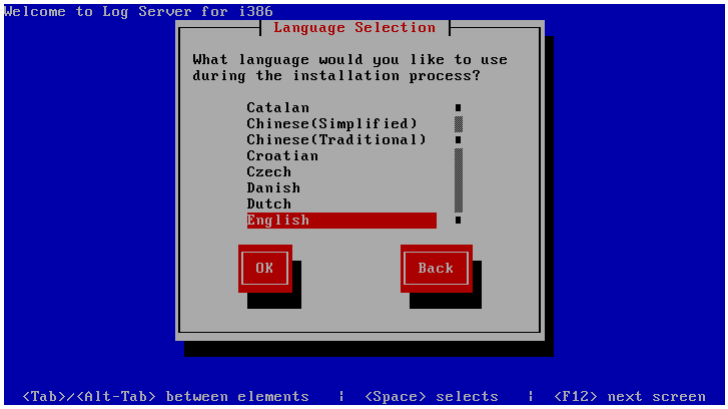
หลังจากเสร็จสิ้นจากการตรวจสอบแผ่น CD หรือเลือก Skip แล้วจะปรากฏข้อความยินดีต้อนรับสู่ Log Server 2.0 ดังรูป



รูปที่ 2.6 แสดงภาพยินดีต้อนรับเพื่อเข้าสู่รายการติดตั้งต่อไป

ถึงหน้าจอนี้คงไม่ต้องถามอะไรอีกเพราะไม่มีเมนูอะไรให้เลือกนอกจาก OK หากมั่นใจว่าจะทำการติดตั้งต่อไปก็ให้เลือก OK แล้วทำขั้นตอนต่อไป

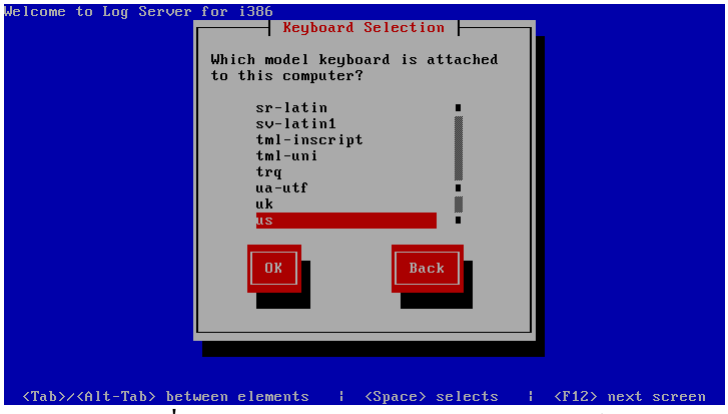
ขั้นที่ 3 เลือกภาษา ใน Text Mode จะมีเมนูสำหรับการติดตั้ง ให้ใช้คีย์บอร์ดในการเลือกเมนู และให้ใช้คีย์บอร์ดที่แป้นลูกศรขึ้น ลูกศรลง เพื่อเลือกรายการ หรือกด TAB เพื่อกระโดดไปยังรายการที่ต้องการ



รูปที่ 2.7 แสดงจอภาพสำหรับการเลือกภาษา

ค่าหลักของโปรแกรมจะเลือกมาให้เป็น English ซึ่งการทำงานเป็น Server แบบ Text Mode ก็ไม่มีภาษาไทยอยู่แล้วคงไม่ต้องเลือกภาษาอื่นให้เสียเวลาให้เลือก OK แล้วกด Enter จะปรากฏตามรูป 2.4

ขั้นที่ 4 เลือกแป้นพิมพ์ เพื่อกำหนดลักษณะของแป้นพิมพ์โดยปกติเราใช้ OS ที่มาจากต่างประเทศค่าหลักเป็นภาษาอังกฤษ ส่วนแป้นพิมพ์ก็ตั้งค่าหลักมาให้เป็นแบบ us

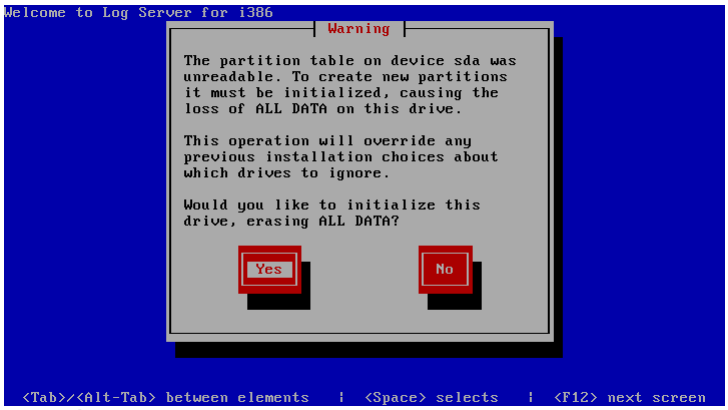


รูปที่ 2.8 แสดงจอภาพการเลือกแป้นพิมพ์

หน้าจอนี้คุณไม่ต้องเลือกเป็นอย่างอื่นเพราะคุณยังใช้งานแบบ Text Mode จึงไม่ต้องเลือกให้เป็นแป้นภาษาไทยให้ใช้ค่า Default เป็น US ให้กด TAB ไปที่ OK แล้วกดแป้น Enter จะปรากฏ ดังรูป 2.9

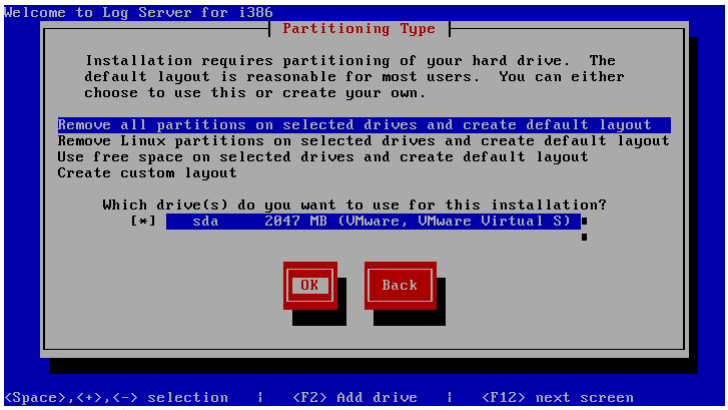
ขั้นที่ 5 คำเตือน

ในหน้าจอนี้เป็นสิ่งที่ควรระมัดระวังเพราะเป็นการเตือนว่า Linux ไม่สามารถอ่านข้อมูลที่มีอยู่เดิมได้หรือ Hard disk เป็นของใหม่จึงมีการเตือนว่าข้อมูลเก่าที่อยู่ใน Hard disk ทั้งหมดอาจถูกลบได้ เพื่อป้องกันการ



รูปที่ 2.9 คำเตือนให้ระวังข้อมูลเดิมใน Hard disk จะถูกลบ

หลังจากกด Yes แล้วจะพบว่าหน้าจอจะแสดงเมนูให้ทั้งหมด 4 รายการให้เลือกใช้งานตามความเป็นจริงควรอ่านรายละเอียดว่าคุณต้องการทำรายการใดถึงจะสามารถกำหนด Partition ที่ต้องการติดตั้ง Log Server แนะนำให้เลือกเมนูแรก หมายถึงลบข้อมูลเดิมทุก Partition แล้วให้สร้าง Partition ให้แบบอัตโนมัติ ตามค่า Default ที่โปรแกรมกำหนดมาให้ ดังภาพ



รูปที่ 2.10 แสดงรายการสำหรับเลือก Partition Type

ความหมายแต่ละรายการมีดังนี้

1. รายการแรกหมายถึง การลบข้อมูลเดิมใน Hard disk ทิ้งทั้งหมดแล้วทำการสร้าง Partition ตามค่าที่ Linux กำหนดค่า Default มาให้

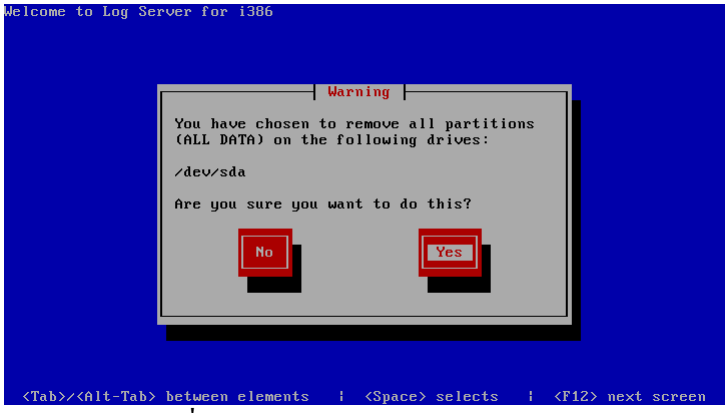
2. รายการที่สองหมายถึง การที่โปรแกรมจะทำการลบเฉพาะ Partition ที่เป็น Linux ทั้งหมดแล้วทำการสร้าง Partition ตามค่าที่ Linux กำหนดค่า Default มาให้

3. เป็นรายการที่โปรแกรมจะไปหาพื้นที่ว่างบน Hard disk แล้วสร้างให้มี Partition ตามค่า Default ของโปรแกรม

4. รายการสุดท้ายหมายถึง รายการที่ให้ผู้ใช้กำหนดค่า Partition ด้วยตนเอง

5. ในส่วนของรายการถัดลงมาจะเป็นรายการแสดงให้ผู้ติดตั้งรู้ว่าในเครื่อง Server มี Hard disk อยู่กี่ตัว แล้วเราต้องการติดตั้ง OS ลงใน Hard disk ตัวไหนก็ให้ทำเครื่องหมาย [*] หน้ารายการนั้นเช่นในภาพมี Hard disk ตัวเดียวก็แสดงเป็น sda ถ้ามีสองตัวก็จะมี sdb เพิ่มอีกหนึ่งรายการ

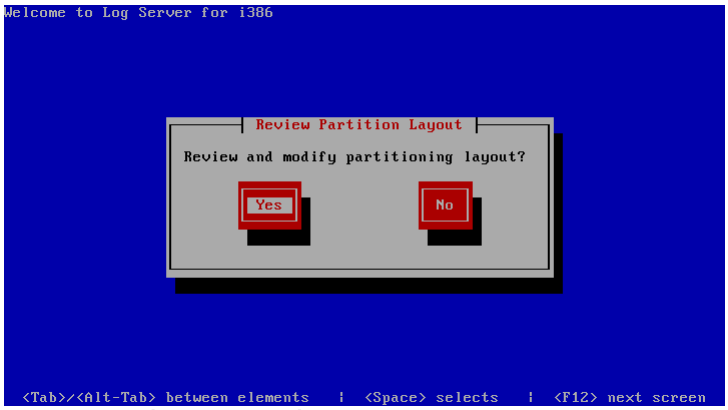
ผู้ที่มีความชำนาญในการใช้ Linux อาจแบ่งด้วยตนเองตามเมนูที่ 4 ก็ได้แต่ต้องแบ่ง /var ให้มากพอที่จะเก็บ Log File ขนาดใหญ่ หลังจากเลือกรายการที่ 1 เนื่องจากจะรวดเร็วและมีการจัดการขนาดของ Partition ให้สูงสุดที่มีบน Hard disk ทำให้เพียงพอต่อการจัดเก็บ Log File จะปรากฏ คำเตือนในส่วนของการที่ข้อมูลบน Hard disk ทั้งหมดจะถูกลบอย่างถาวร คุณแน่ใจหรือไม่ที่จะทำต่อไป ก็มีเมนูให้เลือกอยู่สองรายการคือ No และ Yes ผู้ที่ซื้อเครื่อง Server ใหม่ หรือ Hard disk ตัวใหม่ หรือ ยินดีที่จะลบข้อมูลเดิมเพื่อใช้ทำ Log server อยู่แล้วก็ให้เลือกรายการโดยกดแป้น TAB ไปที่ Yes ดังภาพ



รูปที่ 2.11 แสดงคำเตือนข้อมูลจะถูกลบ

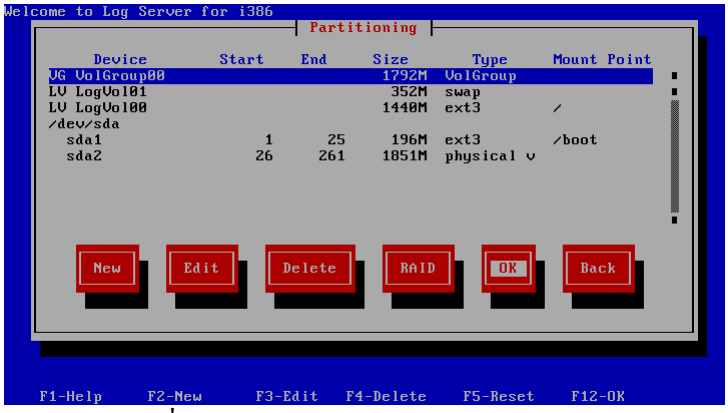
ให้กดแป้น TAB ไปที่ Yes แล้วกด Enter ได้เลยจะได้ทำขั้นตอนต่อไป

ขั้นที่ 6 การแบ่ง Partition สำหรับ Log Server



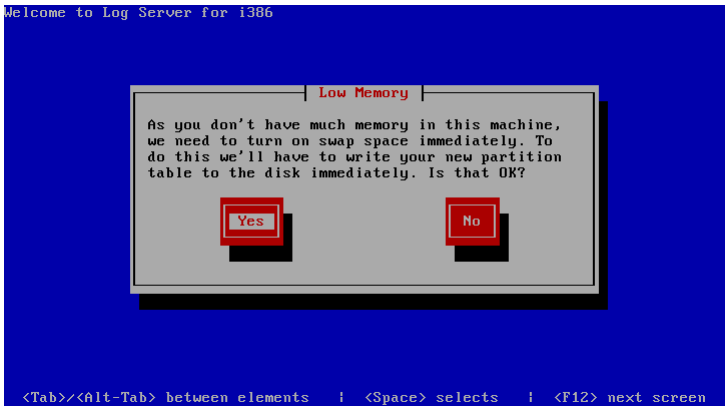
รูปที่ 2.12 ภาพที่จะให้แสดง Partition Layout

ในส่วนนี้เป็นสิ่งที่ควรทำคือต้องเลือก Yes เพื่อตรวจสอบดูว่า Default Partition ที่โปรแกรมสร้างให้นั้นใช้พื้นที่ครบถ้วนหรือทั้งหมดบน Hard disk หรือไม่ ถ้ามีข้อผิดพลาดจะได้ย้อนกลับไปทำใหม่ ดังนั้นให้ กดแป้น TAB เลือก Yes แล้วกดแป้น Enter



รูปที่ 2.13 แสดงการสร้าง Default Partition

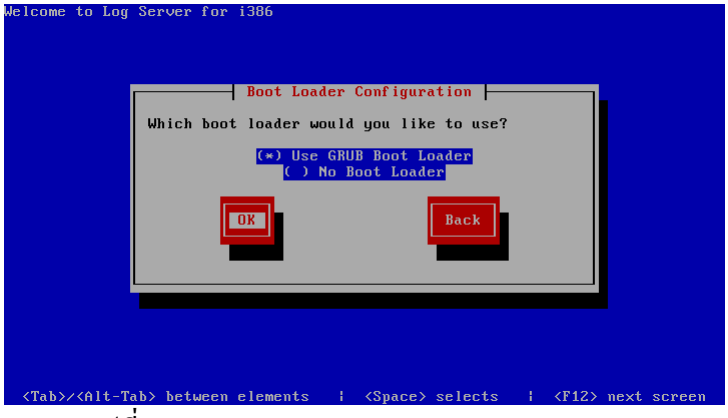
เมื่อเครื่องแสดงการสร้าง Default Partition ควรตรวจดูว่ามีการใช้งานพื้นที่หมดหรือไม่ ถ้าใช้งานหมดครบถ้วนให้เลือกไปที่ OK กดแป้น Enter จากนั้นถ้าเครื่อง Server มีหน่วยความจำน้อยเกินไป ไม่พอในการติดตั้งเครื่องจะถูกเตือนอีกว่าหน่วยความจำไม่พอต้องใช้พื้นที่ swap ใน hard disk เพื่อเขียนข้อมูลในขณะทำการ Unpack file ที่จะนำไปติดตั้ง หากยินยอมให้ใช้พื้นที่ได้ให้กด Yes หากไม่ได้กด No (ถ้ากด No เวลาในการติดตั้งจะนานมากเพราะต้องสร้าง RAM disk เพื่อใช้อ่านโปรแกรมไปเตรียมติดตั้งจำนวนมาก)



รูปที่ 2.14 แสดงการเตือนเรื่องหน่วยความจำเครื่องน้อย (Low Memory)

ขั้นที่ 7 การเลือก Boot Loader

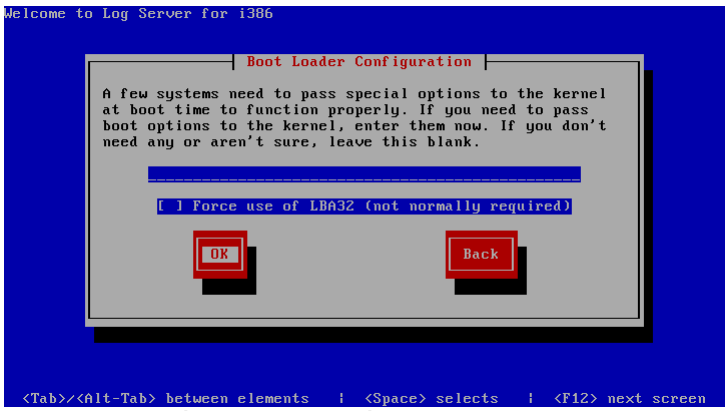
ใน Log Server 2.0 นี้ได้ตัด Linux Loader (LILO) ออกเหลือแต่ GRUB (GRand Unified Bootloader) ซึ่งมีความยืดหยุ่นในการใช้งานที่มากกว่าและปลอดภัยกว่า ในปัจจุบันจะไม่พบการใช้งาน Lilo บน Linux Version ใหม่ ๆ ในขั้นตอนนี้คุณคงไม่มีทางเลือกเป็นอย่างอื่นเพราะมีรายการมาให้เพียง 2 รายการคือเลือก Use GRUB Boot Loader และรายการ No Boot Loader ถ้าไปเลือกรายการที่ 2 เครื่อง Server ก็จะ Boot ด้วยตัวมันเองไม่ได้ ต้องอาศัยการ Boot จากที่อื่น อาจจะเป็นการ Boot จาก USB Flash Drive หรือการ Boot จาก Network อื่น ๆ ที่มีการทำงานอยู่ในระบบเดียวกัน (มืออาชีพเขาใช้กัน)



รูปที่ 2.15 ภาพของ Boot Loader Configuration

ในที่นี้จะเห็นว่าค่า default เลือกแบบ GRUB และอีกตัวเลือกคือไม่มี Boot Loader ให้สังเกตว่าค่า Default ของโปรแกรมจะมีเครื่องหมาย (*) ข้างหน้า Use GRUB Boot Loader ให้กดแป้น TAB ไปที่ [OK] กด Enter

การเพิ่มเติมค่า Parameter ของ Hardware (ถ้ามี)



รูปที่ 2.16 ภาพการเพิ่มเติม kernel option

ตามปกติ kernel 2.6 ก็รู้จัก Hardware ใหม่ ๆ มากพออยู่แล้วแต่คงไม่ทันการพัฒนารายวันของบริษัทต่าง ๆ ดังนั้นการเตรียมค่า parameter หรือ option ต่าง ๆ ไว้ให้กับ kernel จึงอาจไม่ครอบคลุม Hardware ทุกตัว แต่ความสามารถในการ Detect new hardware ของ Linux ก็สามารถที่จะไปอ่านค่า parameter มาให้และแสดงมาในช่องแรกให้ทันที คุณไม่ต้องพิมพ์อะไรเพิ่มเติมแต่อย่างใด อาจใช้ในกรณีเครื่อง Server พันธ์แท้บางยี่ห้อที่ตอน boot ต้องใส่ option เพื่อให้ boot ได้ โดยทั่วไปก็ให้กดแป้น TAB เลือก [OK] กด Enter

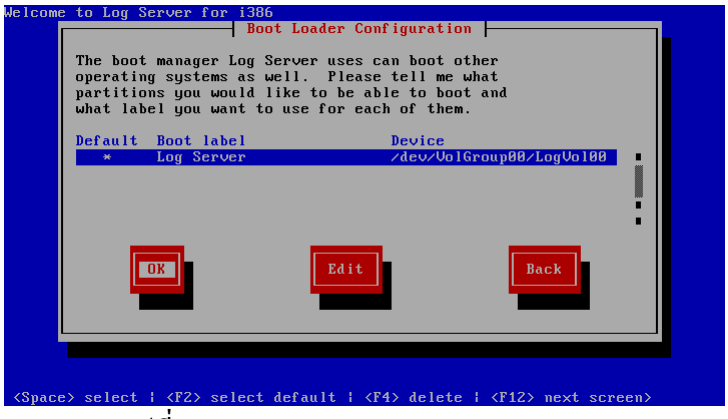
การกำหนด GRUB Password

ในส่วนนี้เป็นเรื่องของความปลอดภัยถ้าผู้ดูแลระบบมีประสบการณ์ในการจัดการระบบความปลอดภัยให้กับ Server ในแต่ละส่วนจะมีความสำคัญทั้งสิ้นเริ่มตั้งแต่การ Boot เครื่องจนไปถึงการดูแลป้องกันผู้บุกรุก

รูปที่ 2.17 หน้าต่างสำหรับใส่ค่า Password ให้ GRUB

การกำหนดค่าเริ่มต้น (Default) Boot

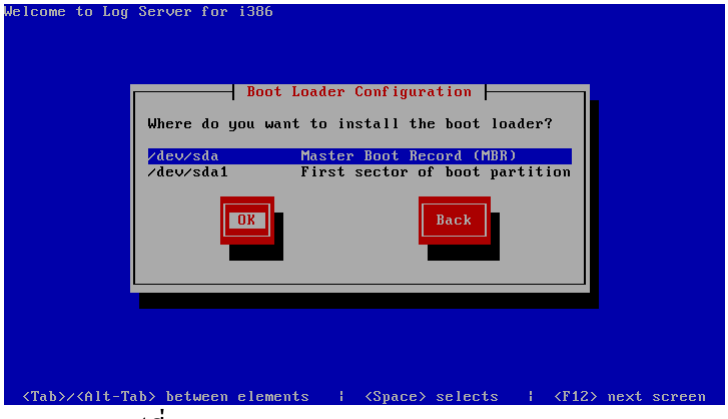
ในกรณีมี OS หลายตัวในเครื่องเดียวกันโปรแกรม GRUB สามารถกำหนดให้เลือก Boot OS ได้หลายตัวตามรายการที่เราติดตั้งไว้ ผู้เขียนไม่แนะนำให้ไปเลือก Boot จาก OS อื่น เพราะ GRUB จะไม่ทำงานและจะย้อนกลับมาที่ Linux หรือ OS ตัวอื่นไม่ได้ ในคู่มือนี้เป็นการทำ Log Server เพียงอย่างเดียวไม่มีการลง OS ตัวอื่น ๆ อีก จึงปรากฏค่า Default มาเป็น Log Server เพียงอย่างเดียวให้กดแป้น TAB ไปที่ OK แล้วกด Enter



รูปที่ 2.18 ภาพ Boot Loader Configuration

การเลือกตำแหน่งที่อยู่ของโปรแกรม Boot Loader

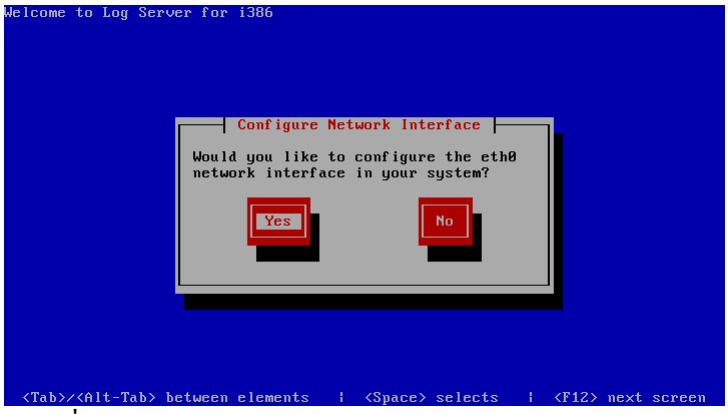
ในที่นี้ให้เลือก MBR แต่ถ้าต้องการให้โปรแกรมตัวอื่นจัดการ Boot เป็นตัวหลักในกรณีที่มี OS หลายตัวให้โปรแกรมนั้นอยู่ที่ MBR แล้ว GRUB อยู่ที่ Partition Boot หรือให้ GRUB เป็นตัวจัดการทั้งหมดให้ก็ได้



รูปที่ 2.19 ภาพ Boot Loader Configuration

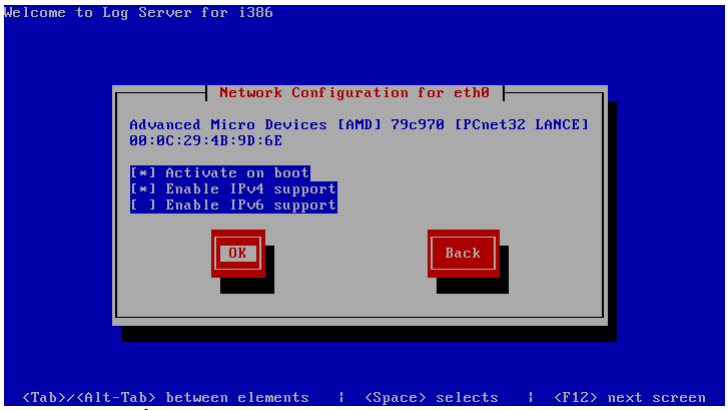
ขั้นที่ 8 การกำหนดค่า Network

สำหรับ Log Server ให้กรอกรายละเอียดเกี่ยวกับ IP Address, Netmask, Default gateway, Primary DNS และ Secondary DNS ซึ่งได้มาจากการซื้อสัญญาณหรือจากของระบบในองค์กร เลือก Yes กด Enter



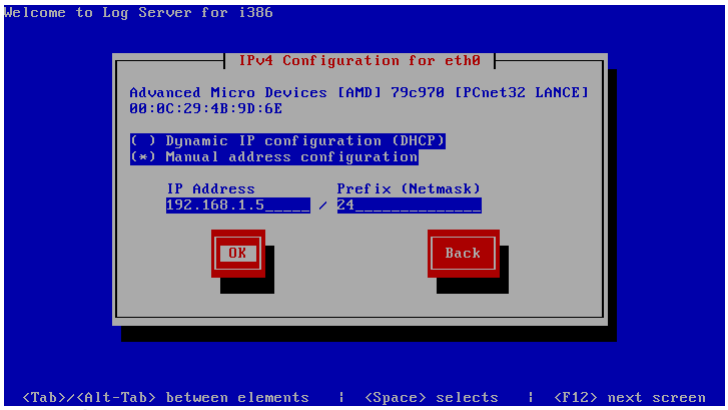
รูปที่ 2.20 แสดงการทำ Configuration ให้ Network Interface

พบ 3 รายการมีรายการแรกเลือกไว้แล้วให้เลือกว่าจะกรอกค่า IP Address เป็น IPv4 หรือ IPv6 โดยเคาะ Spacebar เพื่อให้มีเครื่องหมาย [*] หน้าบรรทัดที่ต้องการ กด แป้น TAB เลือก OK แล้วกด Enter



รูปที่ 2.21 แสดงรายการให้เลือก IPv4 และ IPv6

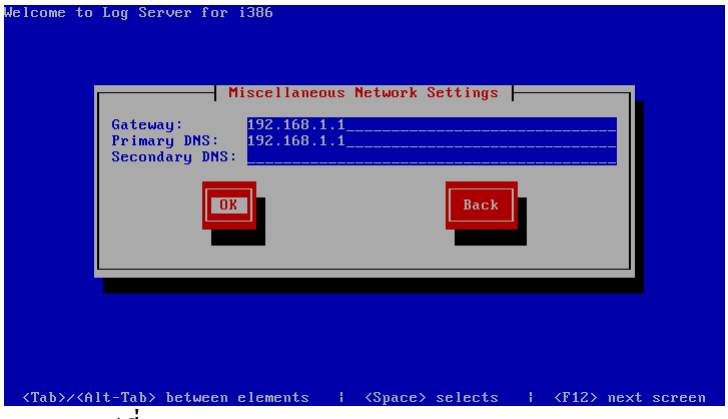
จะได้ภาพให้เลือกว่าจะรับแจก IP Address อัตโนมัติจาก DHCP Server จากภายนอกหรือจะเลือกกำหนดค่าเอง ในที่นี้ให้กำหนดเอง (Manual)



รูปที่ 2.22 แสดงรายการกรอกค่า IP Address และ Netmask

IP address คือ หมายเลข IP Address ของเครื่อง Server ที่กำลังติดตั้ง

Prefix (Netmask) คือ ค่าของ Network ที่ได้รับมาจาก ISP อาจใส่เป็นตัวย่อที่เป็นจำนวนบิทก็ได้ เช่น 255.255.255.0 = 24



รูปที่ 2.23 แสดงรายการกรอก gateway และ DNS

Gateway คือ IP Address ของ Router

Primary DNS คือ IP Address ของเครื่องที่ทำหน้าที่เป็น DNS Server ตัวแรก

Secondary DNS คือ IP Address ของเครื่องที่ทำหน้าที่เป็น DNS Server ตัวที่สอง

ข้อเสนอแนะ

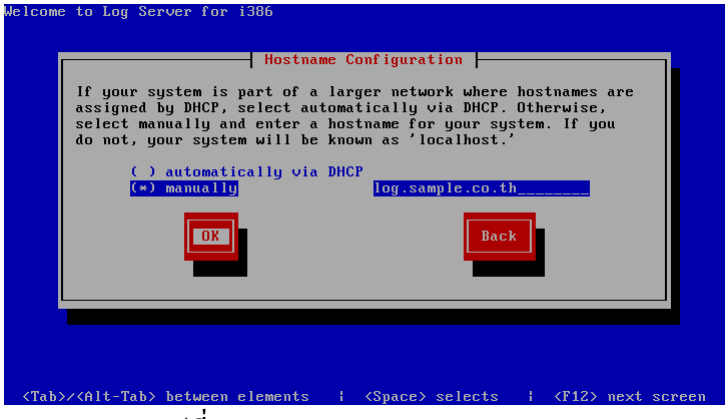
ถ้าขณะติดตั้ง ไม่ปรากฏรูปที่ 2.20 โดยข้ามไปยังขั้นตอนอื่นทันที หมายความว่าไม่มี LAN Card หรือเครื่องไม่สามารถตรวจสอบ LAN Card ได้ แต่ถ้ามี Driver ของ LAN Card อาจติดตั้งภายหลังได้ตามคู่มือผู้ผลิต

ขั้นที่ 9 การตั้งชื่อ Hostname

ซึ่งขั้นตอนต่อไปนี้สำคัญมาก ถ้ากรอกรายละเอียด ผิดพลาดจะนำไปใช้งานจริงไม่ได้ เพราะคนทั่วไปมักใส่ชื่อเครื่องสำหรับใช้งานคนเดียว (Hostname) ถ้าเรากำลังทำ Internet Server สิ่งที่จำเป็นต้องการกรอกลง

คำแนะนำ

ถ้าท่านทำ Server เป็น Intranet ใช้ภายในยังไม่จดทะเบียน Domain Name ท่านสามารถตั้งชื่อ Host name ได้ตามอิสระ ถึงแม้ว่าชาวโลก จะไม่เห็นเครื่องท่านเป็น Internet Server ก็ตามที แต่ท่านสามารถใช้ Internet ได้ โดยมีกฎง่าย ๆ คือ ข้อความตัวหน้าสุดคือชื่อเครื่อง หลังจุดแรกทั้งหมดคือ Domain แม้ว่าจะยังไม่จดโดเมนจริง ๆ มาก็แนะนำให้ตั้งให้เป็นสากลไปก่อนเพื่อส่งค่าไปยังส่วนต่าง ๆ ภายใน Server ให้ทำงานได้สมบูรณ์

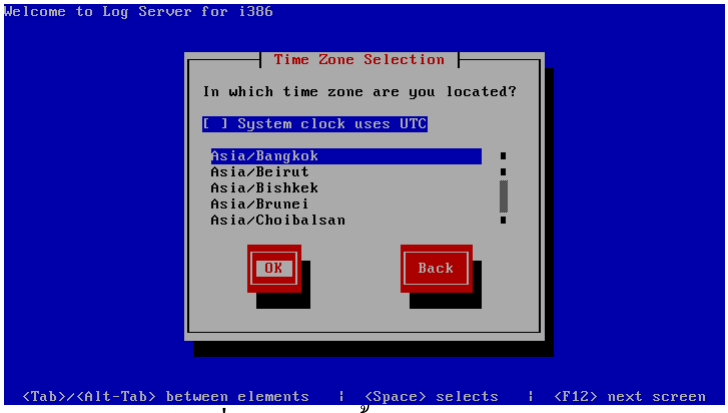


รูปที่ 2.24 Hostname Configuration

สำหรับผู้ที่จะทำ Log Server การกรอกชื่อ Host name ก็ควรอ้างอิงสากลเพื่อให้ระบบสามารถมองเห็นกันได้ด้วยค่าทาง Network ถ้าผิดอาจต้องส่งค่าถึงกันด้วยเลข IP Address เพราะผู้ดูแลระบบอาจไม่จำเป็นต้อง Add ชื่อไปที่ DNS Server ก็ได้ ในตัวอย่างตั้งเป็น log.sample.co.th เมื่อพิมพ์ชื่อ Host name ถูกต้องแล้วแล้วกด TAB ไปที่ [OK] แล้วกด Enter จะปรากฏ

ขั้นที่ 10 กำหนดฐานเวลาให้ Server

เลือกเวลาให้ตรงกับประเทศไทย จะใช้อ้างอิงในการให้บริการลูกข่ายทั่วโลก เพื่อให้เวลาของเครื่อง Server ส่งไปใช้ในการติดต่อกันในระบบ Internet เป็นไปตามจริง ในภาพค่า Default ของโปรแกรมจะกำหนดมาเป็นเวลาท้องถิ่นถ้า จะเทียบกับเวลาสากลต้อง +7 ชั่วโมง ถ้าเคาะแป้น Space bar เอาเครื่องหมาย [*] ออกจากบรรทัด [ ] System clock uses UTC (Universal Time Co-ordinated) จะได้ไม่ต้องบวก 7 ใช้ประโยชน์ในการบันทึกค่า Log file เวลานี้จะถูกบันทึกไว้ให้อ่านค่า log file ตรงกับความเป็นจริง แต่ในส่วนนี้ตั้งผิดหรือถูกก็ไม่เป็นไรเพราะ**ต้องทำการอ้างอิงจาก NTP Server** อยู่แล้ว

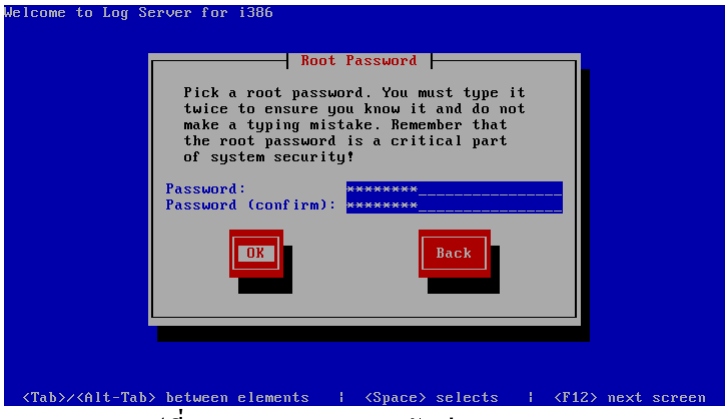


รูปที่ 2.25 การตั้งฐานเวลาอ้างอิง

ให้กดแป้นลูกศรลง เลื่อนมาที่ Asia/Bangkok กด TAB ไปที่ OK กด Enter

ขั้นที่ 11 การใส่รหัสผ่านของ Root

ขั้นตอนนี้สำคัญมากสำหรับผู้ดูแลระบบเครือข่ายเพราะการใช้งานที่มีการเชื่อมโยงกันและมีผู้ใช้หลายคนสามารถเข้าถึง Server ได้จะต้องมีรหัสผ่าน (Password) สำหรับผู้ดูแลระบบจะมี User Account มาให้คือ root ดังนั้นในการติดตั้งจึงต้องให้ใส่รหัสผ่านสำหรับ root ผู้ได้รับการแต่งตั้งให้เก็บรักษา Log ต้องเปลี่ยนรหัสผ่านเป็นของตนเองเพื่อมิให้ Admin เข้าระบบได้



รูปที่ 2.26 การกำหนดรหัสผ่านของ Root

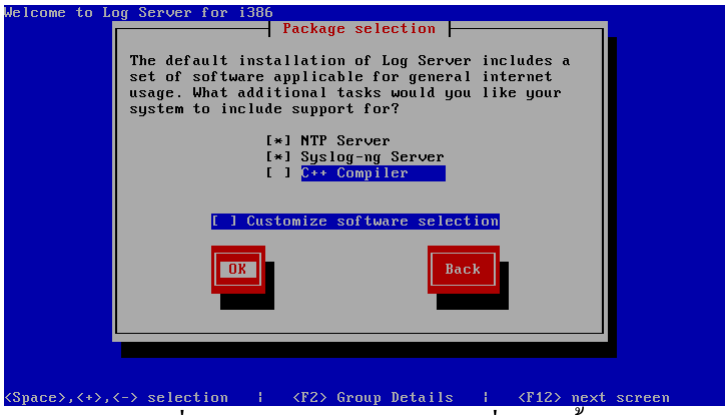
ควรตั้งให้ยาก ๆ หน่อยไม่ควรน้อยกว่า 6 ตัวอักษรเอาแบบสุ่ม ๆ ตัวใหญ่บ้าง เล็กบ้าง มีเลขปนก็ได้ (แต่ต้องจำให้ได้) ป้อน 2 ครั้งให้เหมือนกัน แล้วกด TAB ไปที่ OK กด Enter

หมายเหตุ

สำหรับผู้ที่เริ่มใช้งานระบบปฏิบัติการ Linux อาจไม่คุ้นเคยกับ account ที่มีความสำคัญสูงสุด หากเคยใช้ค่าย Microsoft จะคุ้นเคยกับ Administrator ซึ่งเป็น account ที่ผู้ดูแลมีไว้ทำงานกับ Server ในทำนองเดียวกัน Linux จะมี account ชื่อ root

ขั้นที่ 12 การเลือก Package

ใน CD Log Server Version 1.0 นี้ผู้เขียนได้จัดการกับเมนูให้ง่ายและตรงกับความต้องการใช้งานเท่านั้น รายการอื่น ๆ ที่ไม่จำเป็นถูกตัดออก จึงสามารถเลือกเท่าที่จะใช้งานจริง คือให้มีแต่ NTP Server เพื่อทำฐานเวลาอ้างอิงให้กับระบบ และ Syslog Server เพื่อทำการเก็บ Log file ตามกฎหมายกำหนด ส่วนเมนูสุดท้ายเป็น C Compiler เพื่อให้ผู้ที่ต้องการ Download โปรแกรมจาก Source มาทำการ compile และติดตั้งด้วยตนเอง



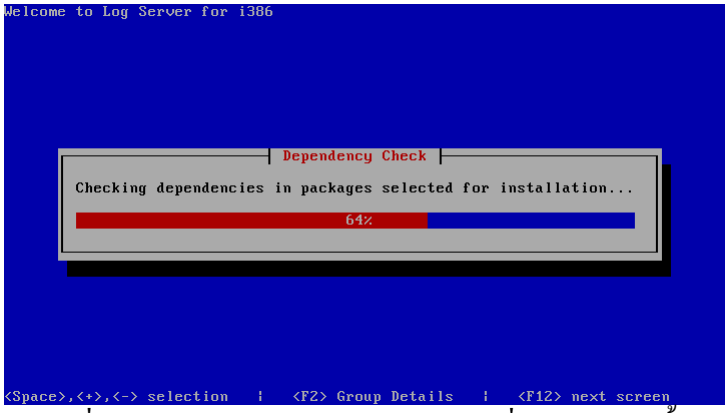
รูปที่ 2.27 การเลือก Package ที่จะติดตั้ง

กดแป้นลูกศรลงหรือลูกศรขึ้น เลือกรายการที่ต้องการ โดยเคาะ Space Bar ให้มีเครื่องหมาย [*] อยู่หน้าบรรทัดที่ต้องการ กด TAB ไปที่ OK กด Enter

การเลือกโปรแกรมที่จะติดตั้ง

NTP Server	เครื่องจะติดตั้งโปรแกรม ntp ทำหน้าที่เป็น Time Server ทำงานด้วย Network Time Protocol
Syslog-ng Server	เครื่องจะติดตั้งโปแกรม syslog-ng เพื่อเปิดบริการเก็บ Log file ที่ส่งมาจากระบบเครือข่ายทั้งหมด
C++ Compiler	เครื่องจะติดตั้งโปรแกรม gcc, C++ ทำหน้าที่เป็น C Compiler เพื่อใช้ compile และติดตั้งโปรกรม

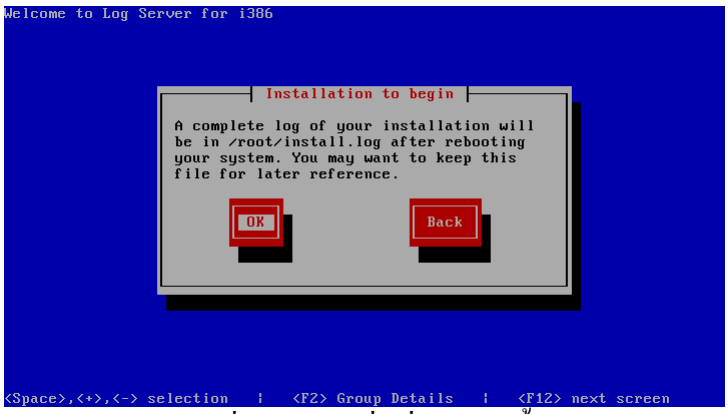
จากรายการในเมนูที่ผู้เขียนได้สร้างไว้ให้นี้คุณสามารถเลือกแล้วค่อยไปทำการแก้ไขค่า Configuration ต่างๆ เพื่อเปิดการทำงานให้บริการให้ตรงกับจุดประสงค์การใช้งานในระบบของแต่ละองค์กร ซึ่งมีรายละเอียดในการทำในบทต่อไป หลังจากเลือกรายการจากเมนูที่ต้องการจนครบถ้วนแล้ว โปรแกรมจะทำการตรวจสอบส่วนประกอบของ File ต่างๆ ที่ใช้ในการติดตั้งว่ามีอยู่ในแผ่น CD ครบสมบูรณ์ทุกรายการตามที่เลือกหรือไม่จะปรากฏภาพดังนี้



รูปที่ 2.28 แสดงการตรวจสอบโปรแกรมที่ใช้ในการติดตั้ง

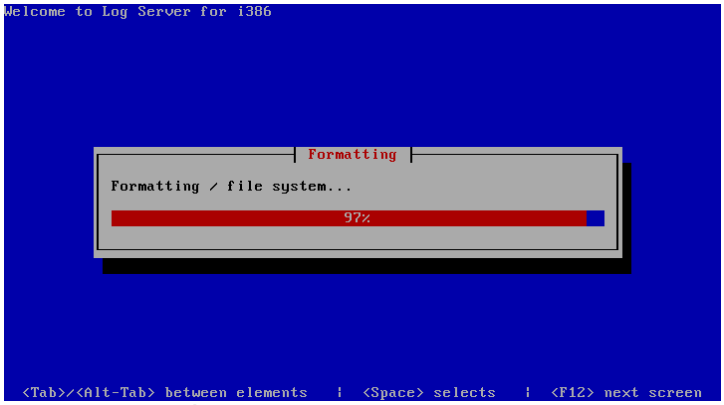
ขั้นที่ 13 เริ่มทำการติดตั้ง

ในขั้นตอนนี้คงไม่ต้องอ่านและคิดอะไรมากอีกแล้วเพียงแต่ต้องเสียเวลารอ อาจต้องไปชงกาแฟร้อน ๆ มานั่งดูความก้าวหน้าในการติดตั้งก็จะเป็นการผ่อนคลาย แต่ไม่นานแบบติดตั้ง OS ของค่ายยักษ์ใหญ่นะครับ ประมาณห้าหกนาทีก็เสร็จแล้วแต่ความเร็วของ Hardware ครับ



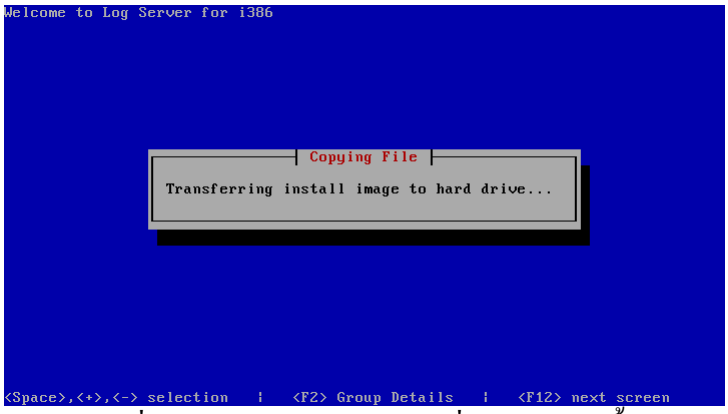
รูปที่ 2.29 ภาพเมื่อเริ่มการติดตั้ง

โปรแกรมเลือกให้เป็น OK กด Enter ได้เลย จากนั้นเครื่องจะทำการ Format Hard disk ตามค่า Partition ต่างๆ ตามที่เราสร้างมาก่อนหน้านี้ ดังภาพ



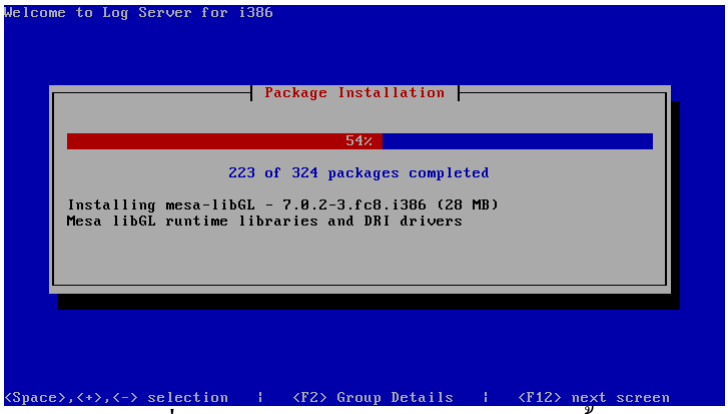
รูปที่ 2.30 แสดงการ Format Hard disk

หลังจาก Format เสร็จครบถ้วนแล้วจะทำการ Copy โปรแกรมต่างๆ ที่เกี่ยวข้องกับการติดตั้งทั้งหมดลงบน Harddisk ดังภาพ



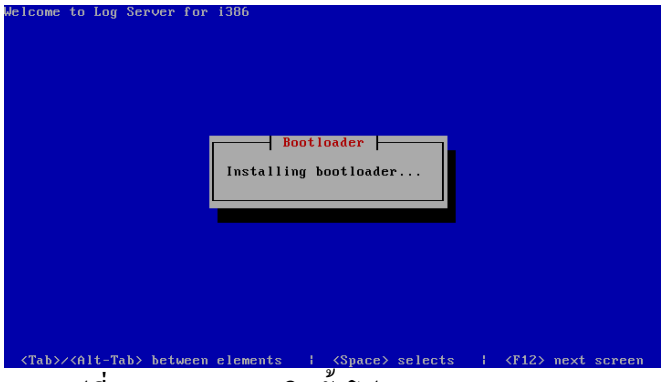
รูปที่ 2.31 แสดงการ Copy ไฟล์ที่ใช้ในการติดตั้ง

เมื่อ Copy package ต่าง ๆ ที่ใช้ในการติดตั้งครบแล้วจึงเริ่มทำการติดตั้ง Package ต่าง ๆ จนครบ 100% โปรแกรมจะมีการคำนวณเวลาที่ใช้ในการติดตั้งทั้งหมด ทั้งนี้ความเร็วจะขึ้นกับคุณสมบัติของเครื่อง Server เช่น ความเร็วในการอ่านของ CD ROM Drive ขนาดของ RAM และความเร็วในการเขียนของ Harddisk เป็นต้น



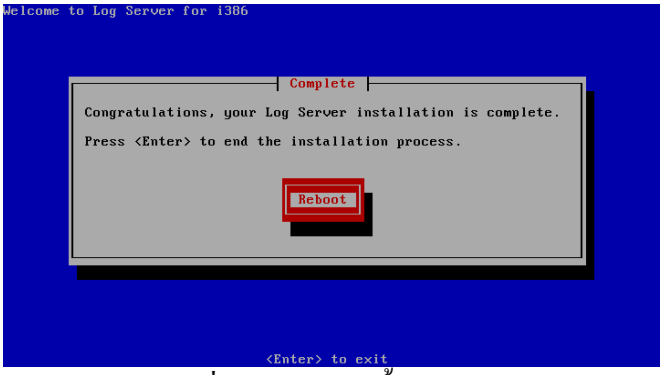
รูปที่ 2.32 แสดงความก้าวหน้าในการติดตั้ง

หลังจากนั้นเครื่องจะทำการติดตั้งส่วนของการทำหน้าที่ Boot ตามที่เลือกไว้คือ GRUB ลงใน MBR (Master Boot Record) หน้าจอภาพจะปรากฏข้อความกำลังติดตั้ง Boot Loader



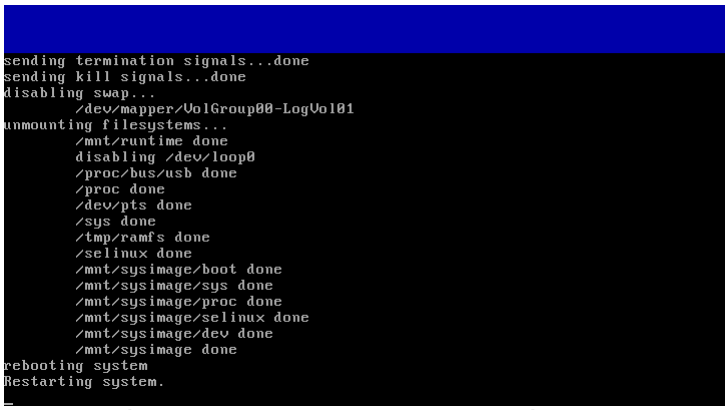
รูปที่ 2.33 แสดงการติดตั้งโปรแกรม Boot Loader

รอสักครู่เครื่องจะแจ้งว่าได้ทำการติดตั้งเสร็จสมบูรณ์แล้ว จอภาพจะแสดงข้อความ Complete และจะให้คุณทำการ Reboot เพื่อเริ่มใช้งานได้เป็นอันเสร็จสิ้นการติดตั้ง Log Server 2.0 เพื่อให้ทดลองใช้งานตามที่กำหนดไว้ในแผนที่วางไว้ โดยการอ่านและทำตามบทต่อ ๆ ไปให้ดีนะครับ



รูปที่ 2.34 การติดตั้งสมบูรณ์

เมื่อติดตั้งเสร็จเรียบร้อย เครื่องจะ Eject CD ออกมาเองโดยอัตโนมัติ ควรรีบหยิบ CD ออกก่อน เพื่อป้องกันการ Boot จาก CD ติดตั้งซ้ำอีก กดแป้น Enter เพื่อทำการ Reboot

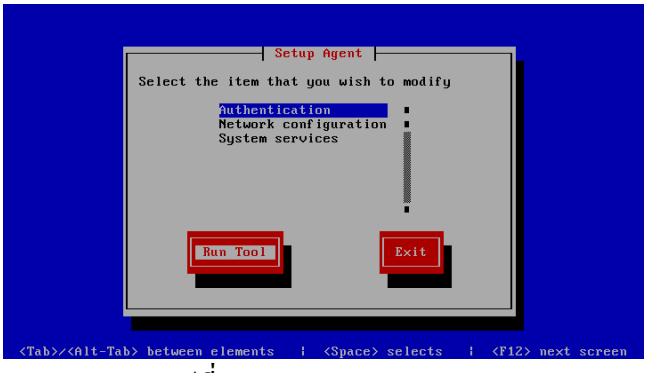


รูปที่ 2.35 แสดงการคืนแผ่น CD พร้อมที่จะ reboot

หลังจากเครื่อง Boot ใหม่จะปรากฏภาพดังนี้

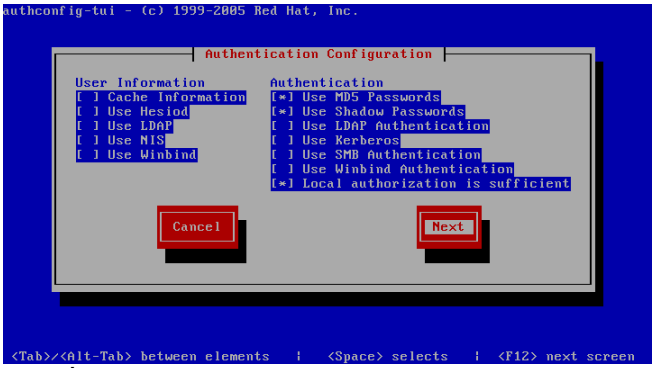
รูปที่ 2.36 แสดงภาพเมื่อเริ่มต้นทำงาน

หลังจาก boot ครั้งแรกจะปรากฏภาพ Setup Agent รอการสั่งให้ทำงานต่อไป ถ้าลืมหรือไม่สนใจมันจะผ่านการทำงานนี้ไปที่หน้า login ดังนั้นต้องรีบกดแป้น TAB เลือก Run Tool ดังภาพ



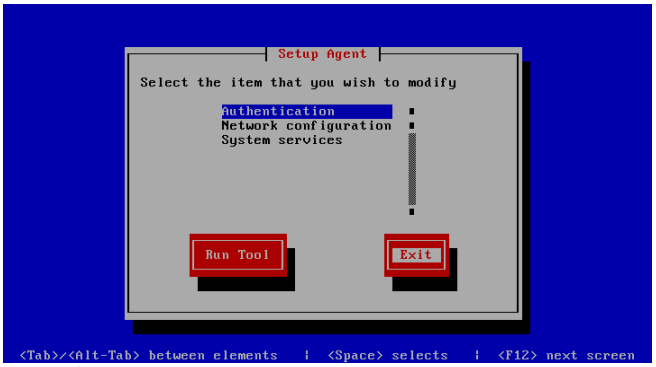
รูปที่ 2.37 แสดงรายการ Setup Agent

จะได้หน้าจอ Authentication Configuration ซึ่งมีการเลือกโดยมีเครื่องหมาย * ไว้ให้ตามที่ OS ได้ติดตั้งการ Authentication ไว้แล้วให้กดแป้น TAB ไปที่ Next แล้วกด Enter ดังภาพ



รูปที่ 2.38 แสดงรายการ Authentication Configuration

เป็นอันเสร็จสิ้นการทำ Authentication ให้กับ Linux Server มันจะกลับมาหน้าจอหลักตามเดิมให้กดแป้น TAB ไปที่ Exit กด Enter ดังภาพ



รูปที่ 2.39 หลังทำ Authentication เสร็จกลับหน้าหลัก

สำหรับขั้นตอนนี้บางครั้งอาจทำไม่ทันเพราะไม่ได้ดูหน้าจอขณะที่เครื่อง Boot ครั้งแรกเนื่องจากเมนูจะตั้งเวลานับถอยหลังไว้และจะทำงานต่อไปที่หน้าจอ login ทันที ให้ทำการ reboot ใหม่ก็จะกลับมาที่หน้าจอนี้ได้อีกครั้งเพื่อทำการ authentication ใหม่แล้วถึงจะเข้าสู่หน้าจอหลักให้ login เข้าระบบต่อไป

รูปที่ 2.40 แสดงภาพเครื่องพร้อมใช้งานได้

คำเตือน

เกือบลืมบอกไปว่าผู้เขียนได้ทำการทดลองติดตั้งทดลองหลายร้อยครั้งเพื่อให้ทราบปัญหา พบว่าการติดตั้งไม่ผ่านมี 2 กรณีคือ มีคำเตือนจากโปรแกรมว่า anaconda error และไม่สามารถอ่าน package บางตัวได้ อาการพวกนี้เกิดจากการแบ่ง partition ด้วยตนเองผิดพลาดพื้นที่น้อยเกินไปทำให้ติดตั้งไม่ได้ครับ

Tip & Trick
ในบางกรณีคุณอาจต้องติดตั้ง Linux กับเครื่อง Server พันธุ์

บทที่ 3
การปรับแต่งหลังติดตั้ง

สำหรับบทนี้จะเป็นการแนะนำให้ทำระบบความปลอดภัยให้กับ Log Server ซึ่งจัดอยู่ในมาตรการรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ตามกฎหมายด้วย และที่สำคัญคือต้องไม่ประมาท เพราะ การระวังในเรื่องความปลอดภัยของ Server นั่นมิได้หมายความถึงเฉพาะข้อมูลจราจรที่อยู่ภายใน Server เท่านั้น แต่ยังหมายรวมถึงความมีเสถียรภาพของระบบ และค่า Configuration ต่างๆ ที่กว่าเราจะติดตั้งให้ครบสมบูรณ์จนทำงานได้ หากมีผู้ไม่ประสงค์ดีบุกรุกเข้ามา อาจทำให้สิ่งที่เราไม่ต้องการ เช่น การเปลี่ยนแปลงข้อมูลจราจรที่เป็นความลับในส่วนต่างๆ และยังมีโอกาสลบ หรือเพิ่มเติมในส่วนที่ทำให้ระบบ ไม่สามารถให้บริการ ให้เหมือนเดิมได้ ดังนั้นเราจึงต้องพยายามหาทางป้องกันระบบในเบื้องต้นไว้ก่อน หลังจากติดตั้งระบบปฏิบัติการลงบน Server เสร็จ สำหรับ Log Server นี้มีวิธีการป้องกันอยู่ 4 วิธีคือ

- SELinux

- tcp wrappers
- secure shell
- Portsentry

การติดตั้งระบบรักษาความปลอดภัยนี้ แนะนำให้ทำทันทีที่ติดตั้งเสร็จก่อนต่อสายสัญญาณเชื่อมต่อเข้าสู่ระบบ Internet และก่อนที่จะเปิด Firewall เพื่อให้คนนอกสามารถเข้าถึง eth0 ได้ ต้องทำให้ครบทั้ง 4 อย่างให้ครบเพื่อป้องกัน Hacker จากภายนอก ที่มีอยู่มากมายใน Internet ที่มีทั้งเป็น Hacker ตัวจริง และ Hacker สมัครเล่นที่เปิดทำตามหนังสือ Hacker ที่มีวางขายอยู่ทั่วไป แต่ถ้าเลือกวิธีการป้องกันหลายๆ อย่างในระบบของท่านแล้ว ผู้ดูแลระบบจะต้องไม่สับสนเองว่าเวลาใช้งานบางอย่างแล้วไม่ได้เกิดจากการปิดบริการใดไว้ที่จุดใดบ้าง (เผื่อตัวเองเข้าไม่ได้จะได้แก้ไขได้ถูกจุด)

Security-Enhanced Linux (SELinux)

โปรแกรม SELinux ได้ถูกออกแบบมาให้สามารถดูแลระบบความปลอดภัยให้กับ kernel ของ Linux ที่มีความยืดหยุ่นสูงและมีความละเอียดในการจัดการได้เป็นอย่างดีในแต่ละส่วนที่ OS กำลังทำงาน (Flexible and fine-rained mandatory access control : MAC) จึงถูกเรียกอีกอย่างหนึ่งว่า Flask in the Linux Kernel การนำ SELinux มาใช้งานนั้นผู้ดูแลระบบสามารถที่จะบังคับควบคุมความปลอดภัยให้กับทุก Process และทุก Object ด้วยการกำหนด Policy ให้กับแต่ละงานในระบบได้เอง ทำให้ผู้ควบคุมระบบได้ตัดสินใจในการแก้ปัญหาที่เกิดขึ้นอย่างอิสระ สถาปัตยกรรมของโปรแกรมได้ถูกออกแบบให้มีความยืดหยุ่นสูงโดยการแยกการตัดสินใจในแต่ละ policy ในลักษณะ logic คือบังคับให้ทำงานเป็นสองสถานะคือ จริง (True) หรือเท็จ (False) ได้ และที่สำคัญคือผู้ดูแลสามารถสร้าง policy แต่ละเรื่องที่ต้องการทำระบบ Security ให้กับ Server โดยไม่มีส่วนใดส่วนหนึ่งไปมีส่วนในการเปลี่ยนแปลงการทำงานใด ๆ ของระบบทั้งสิ้น

หลักการทำงานจะมีรูปแบบเป็นลักษณะโมเดล (Security Model) ที่ประกอบไปด้วย

1. Type Enforcement (TE) Model
2. Role-Based Access Control (RBAC) Model
3. MultiLevel Security (MLS) Model

ข้อมูลโดยละเอียดสามารถหาอ่านได้จากหนังสือ Security-Enhanced Linux ซึ่งในบทนี้ผู้เขียนจะไม่เน้นทฤษฎีที่ยุ่งยาก จะเน้นการนำไปใช้งานจริงเท่านั้นเพื่อให้ง่ายต่อการนำไปดูแลและควบคุม Internet Server ที่มีค่าของคุณ เริ่มกันเลยดีกว่านะครับ

ในขณะที่ติดตั้งระบบปฏิบัติการจากแผ่น CD ชุดติดตั้งซอฟต์แวร์ Syslog-NG ลงไปเสร็จเรียบร้อยแล้ว จะได้รับการติดตั้งส่วนของโปรแกรม SELinux ที่มีมาในแผ่นเพื่อระบบความปลอดภัย และจะทำงานทันทีที่เครื่อง Boot ค่าต่าง ๆ ใน Configuration ที่โปแกรมกำหนดมาให้เป็นค่า Default นั้นจะทำงานในลักษณะปิดทุก

```
# vi /etc/selinux/config
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=enforcing
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted
```

ในเว็บของ Fedora มีการตอบปัญหาของผู้ใช้งานเกี่ยวกับการใช้งาน HTTPD Server เมื่อกำหนดให้ลูกข่ายสามารถใช้ Home directory สร้างที่เก็บเว็บส่วนตัวใน public_html จะใช้งานไม่ได้เพราะมี SELinux ป้องกันไม่ให้ผู้อื่นเข้าถึง Home directory ของลูกข่ายแม้ว่าจะเปิดบริการจาก HTTPD เรียบร้อยทุกประการเหมือนกับ Version ก่อนหน้านี้ก็ตาม ในการตอบคำถามของบริษัท Fedora RedHat เป็นการแนะนำเพียงว่าหากต้องการใช้งานได้ต้องไปยกเลิก Configuration ในส่วนของ **SELINUX= enforcing** ให้แก้ไขเป็น **SELINUX = disabled** เพียงเท่านี้ SELinux ก็จะไม่ไปคอยป้องกัน Server ให้อีกก็สามารถใช้งานได้ตามปกติเหมือนกับ Version ที่ผ่านมา ผู้เขียนเห็นว่าหากทำตามแบบที่ว่าก็สามารถใช้งานได้จริงและไม่มีปัญหาอะไร แต่พอมาคิดอีกทีคงจะไม่ใช่เรื่องที่ถูกต้องนักเพราะปัจจุบันหาก NOS ของบริษัทใดผลิตออกมาแล้วถูกผู้ไม่หวังดีหรือที่ชอบเรียกกันว่า Hacker สามารถบุกรุกเข้าทำการใดๆ ได้อย่างง่ายดาย NOS นั้นก็จะขาดความน่าเชื่อถือแล้วจะไม่มีใครเลือกใช้งานอีกต่อไป ดังนั้นในฐานะที่ Linux เป็น NOS ที่มีความแข็งแรงมากไม่น้อยหน้า UNIX ผู้พัฒนาจึงพยายามหาสิ่งดี ๆ มาใส่ไว้เพื่อเสริมความแกร่งให้สมบูรณ์มากขึ้น บริษัท RedHat เลิกพัฒนา RedHat Linux ไว้เพียง Version 9 ที่เป็น Freeware ก็เพราะมีความยุ่งยากในการที่จะนำเอาเทคโนโลยีด้าน Security มาทำงานร่วมกับ Kernel 2.4.x จึงได้หันไปพัฒนาความปลอดภัยบนตัว Enterprise ขึ้นมาขายและทำตัว Freeware โดยใช้ชื่อว่า Fedora ปัจจุบันขณะที่ผู้เขียนกำลังทำคู่มือเล่มนี้ Fedora ได้พัฒนาถึง Version 9 แล้วครับแต่ยังไม่ Stable ผู้เขียนจึงได้ใช้ Fedora Release 8 (FC8) ที่ Stable มากกว่าและได้ Update Kernel 2.6.25 ที่ใหม่กว่า FC8 ต้นฉบับ มาทำการ Compile ลงในแผ่น CD ชุดติดตั้งซอฟต์แวร์ Syslog-NG เพื่อรองรับการทำงานของระบบความปลอดภัยต่าง ๆ ที่ค่อนข้างสมบูรณ์มาให้ผู้ดูแลระบบได้ใช้งานกัน ลืมบอกไปว่าการแก้ไขค่า policy ต่าง ๆ ของ selinux ใน **Text Mode** ทำได้หลายวิธี ซึ่งแต่ละวิธีมีความยุ่งยากสับสนและเข้าใจยากมาก บางคนไม่อยากปวดหัวเลยไป

เนื่องจากแผ่น CD ชุดติดตั้งซอฟต์แวร์ Syslog-NG ได้ติดตั้งโปรแกรม seedit ซึ่งจะเป็นโปรแกรมสำหรับปรับแต่งค่า policy ใน Text Modeแบบสำเร็จรูป ติดตั้งให้เสร็จทั้งสองโปรแกรมแล้วให้ทำการเรียกคำสั่ง

seedit-init กด Enter

reboot กด Enter

จากนั้นก็รอให้โปรแกรม seedit ไปทำการอ่านค่า policy ต่างๆ ที่โปรแกรม selinux ตั้งค่ามาตอนติดตั้งเสร็จ จนหมดในขณะที่อ่านค่าจะมีรายงานทางจอภาพทุกขั้นตอนแต่อาจเลื่อนเร็วมากอ่านไม่ทันก็ไม่ต้องตกใจ เพราะมันจะทำงานอัตโนมัติ ครั้งแรกจะมีตัวอักษรแดง fail ปนออกมาบนจอภาพนั่งรอดูจนเครื่อง Reboot ใหม่เองเป็นครั้งที่สองเพื่อแก้ค่า policy ที่มี error จากนั้น seedit ก็ทำซ้ำในการค้นหา policy ที่ยังมีปัญหาเพิ่มอีกจนครบถ้วน เครื่องก็จะทำการ Reboot ใหม่เป็นครั้งสุดท้าย จึงจะคืนหน้าจอให้คุณ login เหมือนเดิม คราวนี้คุณสามารถใช้งาน Server ได้ตามปกติ ถ้ามีการเปิด Service ใช้งานเพิ่มเติมจากเดิมแล้วพบว่า audit แจ้ง error ก็ให้ทำซ้ำขั้นตอนเดิมคือ ให้สั่ง seedit -init ใหม่ง่ายกว่าที่จะไปแก้ policy แล้วสั่ง seedit-load หรือใช้ seedit-restorecon ผู้เขียนแนะนำว่าถ้าอยากแก้ไข policy เองก็ต้องไป download คู่มือการใช้ seedit จะทำให้ใช้งานง่ายขึ้นครับ และไม่ควรใช้หลายวิธีในเครื่องเดียวกัน ต้องไม่ลืมเด็ดขาดว่าเครื่องมือที่คุณใช้ในการแก้ไข policy หรือเพื่อความปลอดภัยอื่น ๆ ต้องทำการลบทิ้งหรือถอนการติดตั้งออกจากระบบให้หมดหลังเลิกใช้งาน

TCP Wrappers

เป็นวิธีการเริ่มต้นที่สามารถกำหนดค่าป้องกันให้ใครที่จะมีสิทธิเข้ามาภายใน Server ของเราได้บ้างและใครบ้าง ที่ไม่มีสิทธิเข้าภายใน Server แม้จะเป็นการป้องกันระบบอย่างง่ายก็สามารถทำให้ผู้บุกรุกที่มีความรู้ไม่มากพอที่จะทะลุทะลวงในวิธีอื่น ๆ เข้ามาใน Server ของเราได้ บริการนี้มีมาให้ใน CD ROM แล้ว ถ้าเราติดตั้งโดยเลือกแบบ Server TCP Wrapper จะทำการติดตั้งให้มาพร้อมเลย เพียงแต่เราสามารถแก้ไขค่า Configuration ให้ทำงานตามที่เราต้องการเท่านั้น

การสร้าง Configuration ทำได้โดย ไปแก้ไขไฟล์ชื่อ hosts.allow และ hosts.deny เริ่มต้นให้ทำดังนี้

```
[root@ns ~]#  vi  /etc/hosts.deny
```

ให้พิมพ์เพิ่มต่อท้ายไฟล์ด้วยข้อความ ดังนี้

```
ALL: ALL
```

หมายความว่า service ทุกอย่างที่เครื่อง Server เปิดหลังติดตั้งส่วนใหญ่จะเปิด sshd ตามด้วยหลังเครื่องหมาย : (colon) หมายถึงทุก Domain หรือทุก IP Address ไม่อนุญาตให้เข้าใช้บริการที่ host นี้ได้เลย ภายหลังบันทึกไฟล์แล้วจะมีผลทันที

เสร็จแล้วให้ไปแก้ไขไฟล์ /etc/hosts.allow

```
[root@ns ~]#  vi /etc/hosts.allow            กด Enter
```

ให้พิมพ์เพิ่มต่อท้ายไฟล์ด้วยข้อความดังนี้

```
sshd:  192.168.
syslog-ng: 192.168.
```

เพิ่มสองบรรทัดนี้ เป็นการอนุญาตให้เฉพาะลูกข่ายที่มี IP Address 192.168.x.x เข้าใช้บริการที่ Host ได้ ในคู่มือเล่มนี้ให้เข้าใช้ได้เพียง Secure Shell และการเปิดรอรับการส่ง Log file จากเครื่อง Client ในระบบเท่านั้น

Secure Shell (Openssh)

การรักษาความปลอดภัยให้ระบบอินเตอร์เน็ต มีด้วยกันหลากหลายวิธี ผู้ดูแลระบบที่ดีควรศึกษาการทำงานของ OS ที่ใช้งานว่า มีช่องทางที่ผู้บุกรุกจะโจมตี ทำให้เกิดความเสียหายไม่ว่าจะเป็นข้อมูล หรือการสร้างความวุ่นวาย ทำให้บริการต่างๆ ทำงานผิดพลาด อาจเป็นเพราะการทดลองหรือทำโดยตั้งใจ ดังนั้นระบบที่มีเสถียรภาพย่อมที่จะนำมาซึ่ง ระบบที่ดี ผู้ดูแลไม่ต้องเหนื่อย หรือกังวลกับการที่ต้องมาคอยเฝ้าระวัง ตรวจนับผู้บุกรุก ในบทนี้ก็เป็นอีกวิธีการหนึ่งเท่านั้น ซึ่งแม้จะไม่ใช่วิธีการที่ดีที่สุด แต่ก็เป็นระบบที่ทั่วโลกนิยมใช้กัน ในระดับความเชื่อมั่นสูงพอ เช่น การทำการค้าบน Web site หรือ E-commerce สามารถใช้เพื่อความปลอดภัยในการป้องกันผู้ที่คอยดักจับ Password ระหว่างทางได้ดี เพราะมีการทำงานที่มีลักษณะการตรวจสอบรหัสกุญแจของผู้ที่จะเข้าถึง Server ทำให้มีการเข้ารหัสที่ซับซ้อนขึ้นถึง 1024 bits ทำให้ผู้บุกรุกคาดเดารหัสกุญแจนี้ได้ยากขึ้น เราก็สามารถนำระบบนี้มาใช้กับ Server ของเราได้เช่นกัน ซึ่งถ้าท่านได้ติดตั้งจากแผ่น CD ชุดติดตั้งซอฟต์แวร์ Syslog-NG นี้และในการติดตั้งเป็น Log Server ตามขั้นตอนในคู่มือเล่มนี้อย่างถูกต้องแล้ว จะได้รับการติดตั้ง openssh ให้สมบูรณ์แล้ว

ต่อไปนี้ให้ผู้ดูแลระบบทำการแก้ไขค่า Configuration ใหม่เพราะค่าเดิม (Default) ที่โปรแกรมติดมาให้มีปัญหาในเรื่องการอนุญาตให้ root สามารถ login เข้าระบบได้ซึ่งไม่ปลอดภัยอย่างยิ่งเพราะ root เป็น user ที่สามารถทำลายระบบได้ ให้ทำตามขั้นตอนต่อไปนี้

1. ทำการ Add user ที่จะทำหน้าที่ login เข้าระบบแทน root

```
# useradd admin
# passwd admin
```

2. แก้ไขไฟล์ sshd_config ดังนี้

```
# vi  /etc/ssh/sshd_config
# แก้ค่าให้ตรงกับระบบที่ใช้งานจริงตามต้องการ
# สำหรับไฟล์นี้ตัวอักษรตัวพิมพ์ใหญ่-เล็ก มีผลกับการทำงานให้ดูจาก
```

ค่าตัวอย่าง

Port 22

#Protocol 2,1

Protocol 2

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

HostKey for protocol version 1

#HostKey /etc/ssh/ssh_host_key

HostKeys for protocol version 2

HostKey /etc/ssh/ssh_host_rsa_key

HostKey /etc/ssh/ssh_host_dsa_key

Lifetime and size of ephemeral version 1 server key

KeyRegenerationInterval 1h

ServerKeyBits 1024

Logging

obsoletes QuietMode and FascistLogging

#SyslogFacility AUTH

SyslogFacility AUTHPRIV

LogLevel INFO

Authentication:

LoginGraceTime 30s

PermitRootLogin no

#StrictModes yes

MaxAuthTries 4

#RSAAuthentication yes

#PubkeyAuthentication yes

#AuthorizedKeysFile .ssh/authorized_keys

For this to work you will also need host keys in /etc/ssh/ssh_known_hosts

#RhostsRSAAuthentication no

similar for protocol version 2

#HostbasedAuthentication no

Change to yes if you don't trust ~/.ssh/known_hosts for

RhostsRSAAuthentication and HostbasedAuthentication

#IgnoreUserKnownHosts no

Don't read the user's ~/.rhosts and ~/.shosts files

#IgnoreRhosts yes

To disable tunneled clear text passwords, change to no here!

PasswordAuthentication yes

PermitEmptyPasswords no

Change to no to disable s/key passwords

#ChallengeResponseAuthentication yes

ChallengeResponseAuthentication no

Kerberos options

#KerberosAuthentication no

#KerberosOrLocalPasswd yes

#KerberosTicketCleanup yes

#KerberosGetAFSToken no

GSSAPI options

#GSSAPIAuthentication no

GSSAPIAuthentication yes

#GSSAPICleanupCredentials yes

GSSAPICleanupCredentials yes

Set this to 'yes' to enable PAM authentication, account processing,

and session processing. If this is enabled, PAM authentication will

be allowed through the ChallengeResponseAuthentication mechanism.

Depending on your PAM configuration, this may bypass the setting of

PasswordAuthentication, PermitEmptyPasswords, and

"PermitRootLogin without-password". If you just want the PAM account and

session checks to run without PAM authentication, then enable this but set

ChallengeResponseAuthentication=no

#UsePAM no

UsePAM yes

Accept locale-related environment variables

AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES

AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT

AcceptEnv LC_IDENTIFICATION LC_ALL

#AllowTcpForwarding yes

#GatewayPorts no

#X11Forwarding no

#X11Forwarding yes

#X11DisplayOffset 10

#X11UseLocalhost yes

PrintMotd yes

#PrintLastLog yes

#TCPKeepAlive yes

#UseLogin no

#UsePrivilegeSeparation yes

#PermitUserEnvironment no

#Compression delayed

#ClientAliveInterval 0

#ClientAliveCountMax 3

#ShowPatchLevel no

#UseDNS yes

#PidFile /var/run/sshd.pid

#MaxStartups 10

#PermitTunnel no

no default banner path

#Banner /some/path

override default of no subsystems

Subsystem sftp /usr/libexec/openssh/sftp-server

AllowUsers admin

AllowGroups admin

บันทึกและออกจาก vi กด :wq กด Enter

จากนั้นให้ทำการสร้าง Server key ขึ้นใหม่เพราะค่า default ของโปรแกรมกำหนดให้มีค่า ServerKeyBits 768 เมื่อแก้เป็น 1024 บิท (ค่าต่ำสุดคือ 512 bit สามารถกำหนดให้สูงตามต้องการได้แต่แนะนำถ้ามากเกินไปจะทำให้ถอดรหัสช้ามาก ไม่ควรเกิน 1024 bit) ต้องทำการสร้าง key ใหม่ทั้งหมด 2 ไฟล์ (เฉพาะโปรโตคอลเวอร์ชั่น 2) ทำตามขั้นตอนต่อไปนี้

```
# ssh-keygen -t rsa -b 1024 -f /etc/ssh/ssh_host_rsa_key
Generating public/private rsa key pair.
/etc/ssh/ssh_host_rsa_key already exists.
Overwrite (y/n)? y                          <- พิมพ์ y กด Enter
Enter passphrase (empty for no passphrase):      <- ไม่ต้องเติมกด Enter
Enter same passphrase again:     <- ไม่ต้องเติมกด Enter
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
83:c2:40:f2:0a:a5:76:41:ab:e1:4b:5c:3b:f0:b8:a0 root@log.sample.co.th
#
```

จากนั้นให้ทำการ gen dsa key ดังนี้

```
# ssh-keygen -t dsa -b 1024 -f /etc/ssh/ssh_host_dsa_key
Generating public/private dsa key pair.
/etc/ssh/ssh_host_dsa_key already exists.
Overwrite (y/n)? y                                  <- พิมพ์ y กด Enter
Enter passphrase (empty for no passphrase):      <- ไม่ต้องเติมกด Enter
Enter same passphrase again:     <- ไม่ต้องเติมกด Enter
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
fb:7c:f0:b3:d3:b6:9b:b5:ef:07:f7:27:d2:9d:29:43 root@log.sample.co.th
#
```

3. แก้ไขไฟล์ su

```
# vi +6 /etc/pam.d/su
```

ของเดิม

```
#auth    required        pam_wheel.so  use_uid
```

แก้ไขเพียงลบเครื่องหมาย # ออก เป็น

auth required pam_wheel.so use_uid

บันทึกและออกจาก vi กด :wq กด Enter

4. กำหนดให้ admin อยู่ใน wheel group ด้วยคำสั่ง

usermod -G10 admin

5. การสั่ง Start sshd พิมพ์

```
[root@ns ~]# /etc/init.d/sshd restart กด Enter
```

เพียงเท่านี้เวลาผู้ดูแลระบบต้องการ Remote Login จากที่อื่นก็สามารถใช้ User ชื่อ admin แทน root และเมื่อ Login ได้สำเร็จก็สามารถใช้คำสั่ง su - เพื่อทำหน้าที่ต่าง ๆ แทน root ได้เพียงคนเดียวครับ สำหรับ user อื่น ๆ จะไม่สามารถเข้าทาง ssh port 22 ได้เลย (ถ้าอยากให้ user อื่นสามารถใช้บริการ ssh ได้เพิ่ม user ที่ AllowUsers ครับให้คั่นด้วยเครื่องหมาย comma ให้กับ user แต่ละคนและผู้ที่ไม่ใช่ admin ก็ไม่สามารถใช้คำสั่ง su ได้อีกด้วย)

6. กำหนดให้ทำงานทุกครั้งที่ Boot เครื่อง พิมพ์คำสั่งที่ command line ดังนี้

chkconfig sshd on

หรือใช้เมนู ntsysv ที่คุ้นเคยก็ได้

```
[root@ns ~]# ntsysv กด Enter
```

เลือกให้มีเครื่องหมาย * หน้า [*] sshd ตัวอื่นคงเดิม กด OK ออกจากเมนู

สำหรับเครื่อง Client ซึ่งใช้ OS ทั้ง Linux และ MS Windows ถ้าคุณต้องการควบคุม Server จากเครื่องอื่นที่ใช้ MS Windows สามารถ Download Secure Shell Client ได้ที่ http://www.ssh.com แบบนี้ผู้ดูแลระบบก็สามารถ login ด้วย admin หรือ user ที่ทำหน้าที่เป็นผู้ดูแลระบบได้จากที่อื่น ๆ ได้และสามารถใช้ ftp ส่งไฟล์จากที่อื่นเข้า Server ได้เลยทั้งที่คุณปิดบริการ ftp และ telnet แล้วก็ตามอย่าลืมอนุญาตที่ไฟล์ hosts.allow เปิด sshd: ALL ด้วยมิฉะนั้นจะเข้า Server ไม่ได้

Portsentry

การป้องกันผู้บุกรุกอีกวิธีหนึ่งคือ ป้องกันมิให้ผู้บุกรุกทำการ Scan Port ที่เรากำลังเปิดทิ้งไว้ หรือเปิดให้บริการในสภาวะปกติอยู่ โดยมิได้ทำการป้องกัน ส่วนใหญ่ผู้ดูแลระบบจะละเลย หรือไม่ทราบว่าในขณะที่เราติดตั้ง NOS (Network Operating System) ค่าหลัก (Default) ที่โปรแกรมได้ตั้งค่าให้ Port ไหนเปิดทันทีหลังจากติดตั้งเสร็จ และบางครั้งอาจมีผู้ดูแบลางคนไม่ทราบว่า Port ใดใช้หรือไม่ใช้ในการให้บริการสำหรับการติดตั้งในเครื่องนี้ จึงเป็นช่องโหว่ที่ผู้บุกรุกสามารถใช้ความสามารถในการ Scan Port สำหรับตรวจดูเครื่องที่จะโจมตี ในปัจจุบันมี Hacker หลายคนที่สามารถเจาะระบบผ่าน Port 80, 21, 23 หรือ Port ที่เป็นบริการปกติสำหรับ Server โดยที่ผู้ดูแลไม่สามารถดูจาก Log File ได้เลย และยังสามารถแฝงตัวเข้ามาเป็น root ได้อีกด้วย มีสิทธิในการทำลายเท่าเทียมกับผู้ดูแลระบบ ในบทนี้เป็นเรื่องที่ท่านสามารถติดตั้งโปรแกรมที่ใช้ในการดัก หรือ

```
# mount /dev/cdrom /mnt/cdrom
# rpm -ivh /mnt/cdrom/MyBooks/portsentry กด TAB กด Enter
# eject
```

ถ้าติดตั้งจาก CD ที่แถมมากับคู่มือนี้ไม่ต้องแก้ไขใด ๆ ก็สามารถสั่งเริ่มใช้งานได้ทันทีแต่มีสิ่งที่ควรศึกษาว่าโปรแกรมตรวจจับผู้บุกรุกจากการ Scan Port ใดบ้างถ้าพบแล้วจะเก็บค่าไว้ที่ไหนและมีวิธีจัดการกับผู้บุกรุกอย่างไร เวลามีปัญหาจะแก้ไขให้ Server ทำงานต่อได้ตามปกติ ผู้เขียนเคยสังเกตการณ์ทำงานของโปรแกรมใน Version ที่ผ่านมาพบว่าหากผู้ใช้งานไม่ศึกษาว่าโปรแกรมได้ทำการ Block หรือไม่อนุญาตให้ผู้บุกรุก IP Address หมายเลขใดเข้า Server ได้ จะรู้ได้อย่างไรและถ้าผู้ที่ถูก Block ดันเป็นลูกข่ายที่ชอบลองของบังอาจทดสอบความสามารถของผู้ดูแลระบบเครื่องลูกข่ายเครื่องที่ถูก Block ก็จะไม่สามารถเข้าใช้บริการใด ๆ ใน Server ได้อีกเลยครับ บางคนใช้วิธีแก้ไขด้วยการ Reboot Server ใหม่เพื่อให้ลูกข่ายตัวเองเล่นได้แต่ลืมไปว่าโปรแกรม Portsentry ได้ Block ผู้บุกรุกอื่น ๆ ไว้อีกเพียบถ้ายกเลิกไป ก็ต้องรอให้มีการบุกเข้ามาใหม่ถึงจะถูกโปรแกรม Block นะครับ เรามาดู Configuration กันก่อน

```
[root@ns ~]# vi /etc/portsentry/portsentry.conf
```

1. บรรทัดที่ 35-36 เป็นหมายเลข Port ที่ป้องกันไม่ให้ถูก Scan ครับ ป้องกันทั้ง Protocol TCP และ UDP ถ้าอยากป้องกัน Port ใดเพิ่มอีกก็ให้พิมพ์ต่อท้ายบรรทัดอย่าลืมคั่นด้วยเครื่องหมาย Comma ด้วยนะครับ

2. บรรทัดที่ 73,75 เป็นหมายเลข Port ที่ยกเว้นหรืออนุญาตให้ Scan ได้เพราะเป็น Port ของการบริการตามปกติของ Server หากต้องการให้โปรแกรมยอมให้ Scan Port ใดเพิ่มอีกก็พิมพ์ต่อท้ายบรรทัดคั่นด้วยเครื่องหมาย Comma ได้เลยครับ

3. บรรทัดที่ 85 เป็นการบันทึกการ Block ผู้บุกรุกทั้งหมด มีรายละเอียดให้ดูว่ามาจาก IP Address ใด วัน เดือน ปี เวลา ที่บุกเข้ามาและมาด้วย Protocol ใด ลองเข้าไปดูเองครับตามที่อยู่ของไฟล์คือ /etc/portsentry/portsentry.history

4. สำหรับ Version นี้จะใช้วิธีจัดการกับผู้บุกรุกด้วยการใช้คำสั่ง iptables ดังนี้

KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP"

วิธียกเลิกหาก IP Address ที่ถูก DROP เป็นลูกข่ายเราเองไม่ต้อง Reboot ครับหรือห้ามสั่ง restart iptables ให้ใช้คำสั่งเดิมแก้ไขด้วยการสั่งที่ terminal ได้ดังนี้

iptables -D INPUT -s <IP Address> -j DROP"

<IP Address> คือหมายเลข IP ที่ถูก DROP ครับเพียงเท่านี้เครื่องที่ถูก Block ก็จะเข้าใช้บริการ Server ได้เหมือนเดิมครับ คงต้องมีการไปตักเตือนกันบ้างว่าทีหลังถ้าทดลองบุกเข้ามาอีกจะไม่ปลดให้เล่นอะไรกับเขาได้เลยเพราะตอนนี้กฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์บังคับแล้ว

5. บรรทัดที่ 229 หรือ 236 เป็นเรื่องเดียวกันนะครับ ต้องเลือกเอาบรรทัดใดบรรทัดหนึ่ง ใน Version เดิมจะเปิดใช้คือจะไม่มีเครื่องหมาย # อยู่หน้าบรรทัดที่ 229 เป็นการสั่งให้โปรแกรม tcp-wrappers เขียนข้อมูลเพิ่มในไฟล์ hosts.deny ว่า

ALL: <IP Address ที่บุกรุก>

ส่วนบรรทัดที่ 236 เป็นรูปแบบใหม่ของไฟล์ hosts.deny ใน tcp-wrappers version ใหม่ครับเขาจะเขียนเพิ่มว่า

ALL: <IP Address> : DENY

เลือกใช้เอาเองครับ ถ้าอยากใช้ผมแนะนำให้ลบเครื่องหมาย # หน้าบรรทัดที่ 236 ออกเพียงบรรทัดเดียวนะครับ

เป็นอันว่าอธิบายกันละเอียดขนาดนี้ถ้ายังใช้ไม่เป็นละก็ โดนดีแน่ ผู้เขียนลองใช้โปรแกรมนี้มานานหลายปีแล้วมันช่วยทำให้เราทิ้ง Server ได้เลยครับ วันไหนว่าง ๆ ก็ลองไปสั่งคำสั่งนี้ดู

iptables -L INPUT

ก็จะพบว่ามีการ DROP IP แปลกปลอมไว้เพียบ ถ้าจัดการกับ Configuration เสร็จก่อน restart service ให้ดูแลความปลอดภัยไฟล์ที่จำเป็นก่อนครับ ให้ทำตามนี้

```
# chmod  600   /etc/portsentry/portsentry.conf
# chmod  600   /etc/portsentry/portsentry.ignore
```

6. สั่งให้โปรแกรมทำงาน

```
#    /etc/init.d/portsentry      restart
```

เพื่อให้ทำงานทุกครั้งที่ Boot เครื่องใหม่ ให้ตรวจสอบโดยพิมพ์ ntsysv ต้องมีเครื่องหมาย [*] ที่หน้าบรรทัด portsentry ตอนติดตั้งเสร็จจะทำเครื่องหมาย * ให้แล้วครับไม่ต้องทำเองหรือชอบใช้ command line ก็ให้สั่ง

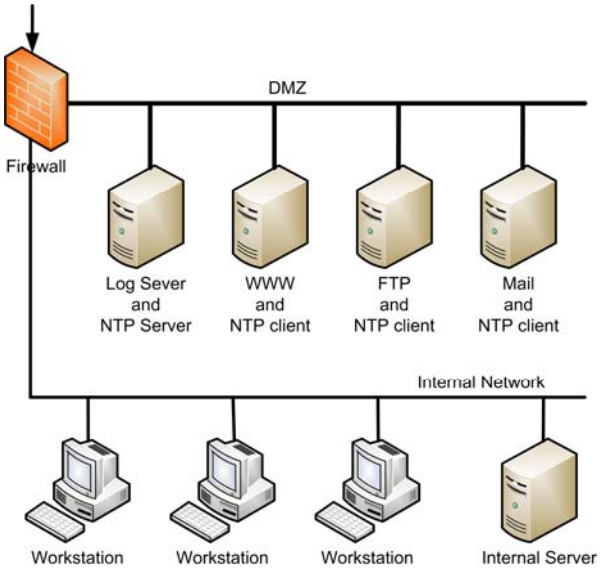
chkconfig portsentry on

บทสรุป

สำหรับท่านที่เคยติดตั้ง Linux Server บน Network ที่ใช้ IP Address จริง(Public IP) อาจพบปัญหาว่าติดตั้งโปรแกรม เสร็จใหม่ๆ ยังไม่ทันปรับแต่ง Configuration เลย Hacker จากที่ไหนก็ไม่รู้ เข้ามายึดระบบไปเรียบร้อยแล้ว มานั่งอมยิ้มอยู่ในเครื่องเราเสียแล้ว โดยเฉพาะหน่วยงานด้านการศึกษามีพวกชอบลองของเยอะ มีทั้งพวก Hacker ตัวจริง ตัวปลอม ทดลองทำตามหนังสือที่วางขายทั่วไป และในปัจจุบัน มีวิชาเรียนในโรงเรียนบางแห่ง นักศึกษาเลยพากัน Hack แข่งขันกันทำแต้มก็มีดังนั้น Server ที่เพิ่งจะติดตั้ง เสร็จใหม่ ๆ เหมือนเด็กแรกเกิดยังอ่อนโลก จึงเป็นเหมือนหมูหวานในระบบ ไม่ได้หมายความว่า Server ไม่แข็งแรง เพียงแต่เขี้ยวเล็บยังไม่งอก และกระดองยังไม่แข็งแรงพอที่จะรับมือ กับผู้ที่จ้องจะจู่โจมได้

บทที่ 4
การติดตั้ง NTP Server

ขั้นตอนการติดตั้ง NTP Server (Network Time Protocol) ก่อนอื่นต้องดูหลักเกณฑ์ในข้อ 9 ตรงข้อความที่ว่า ต้องตั้งนาฬิกา ของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้าง อิงสากล (Stratum 0) แนะนำให้ใช้วิธีการติดตั้ง NTP Server ไว้ในระบบหนึ่งเครื่องน่าจะเอาไว้ที่เครื่อง Log Server เพื่อจ่ายสัญญาณนาฬิกาให้กับเครื่อง Server และเครื่อง Workstation และอุปกรณ์เครือข่ายในระบบทั้งหมดในระบบเป็นลำดับที่ 1 ส่วนลำดับที่ 2 และ 3 ให้อ้างอิงไปยังฐานเวลาภายนอก เพราะถ้าให้ Server แต่ละตัวไปร้องขอ sync สัญญาณนาฬิกาจากภายนอกเวลาอาจมีปัญหาได้เพราะระบบ Network ในบ้านเราการให้บริการยังมีปัญหาติดขัดเป็นประจำที่แน่ ๆ คือเวลาคนใช้งานกันมาก ๆ แทบจะวิ่งออกไปท่องใน Internet กันไม่ได้เลยอาจเป็นปัญหาในการอ้างอิงเวลาให้กับ Server และ Workstation แต่ละตัวได้ สำหรับโปรแกรม ntp สามารถกำหนดค่า Configure ให้เป็นได้ทั้ง Server และ Client ตัวอย่างต่อไปนี้จะติดตั้ง Server เพียงเครื่องเดียว นอกนั้นทั้ง Server และ Workstation ในระบบทั้งหมดจะทำ configuration ให้เป็น NTP Client เพื่อร้องขอเทียบฐานเวลาจาก Server นอกจากนี้เครื่องลูกข่ายและอุปกรณ์เครือข่าย (Network Device) ทุกตัวที่ติดตั้งอยู่ต้องทำการตั้งค่าฐานเวลาอ้างอิงจาก NTP Server เพื่อให้เวลาตรงกันหมดทั้งระบบ ดังตัวอย่างในภาพจะแสดงผังการวางเครื่อง Log และ NTP Server ไว้ในเครื่องเดียวกันและติดตั้งไว้ในส่วนของ DMZ หรือในกลุ่มเดียวกันกับ Server ของระบบในหน่วยงาน ผู้เขียนจะมุ่งเน้นว่าไม่ต้องการให้ผู้ดูแลระบบต้องไปรื้อระบบหรือสร้างงานเพิ่มขึ้น อยากให้มองว่าการทำ Log Server ตามกฎหมายเป็นเพียงการตั้ง Server เพิ่มขึ้นจากเดิมซึ่งถ้าระบบมี Authentication Server อยู่แล้วก็ตั้งเพียง Log/NTP Server อีกหนึ่งเครื่องก็สามารถทำงานได้แล้ว



รูปที่ 4-1 แสดงการอ้างอิงฐานเวลาและ Log Server

ขั้นที่ 1 ให้ติดตั้งโปรแกรม ntp บน Server (ในภาพเป็นการติดตั้งไว้บนเครื่อง Log Server) ดังนี้

กรณีค่าย RedHat, Fedora ใช้คำสั่ง

 # rpm -ivh ntp-4*

ตามปกติในการติดตั้ง Linux OS ทั้ง Server และ Client โปรแกรม NTP จะถูกติดลงไปแล้วลองตรวจสอบดูก่อนด้วยคำสั่ง

 # rpm -q ntp

กรณีเป็น debian/Ubuntu ให้ติดตั้งด้วยคำสั่ง

 # sudo apt-get install ntp

คงไม่ต้องอธิบายรายละเอียดมากเกินไปเพราะผู้ดูแลระบบที่จะทำขั้นต้อนนี้ได้คงไม่ต้องบอกวิธีการ mount cd หรือการติดตั้งผ่าน Internet และก่อนที่จะทำการแก้ไข Configuration ให้ทำการตรวจสอบวันเวลาที่ server ที่อ้างอิงในประเทศไทยตามตาราง NTP Server ที่แนะนำตามตาราง

NTP Server Address	หน่วยงาน	Clock Strata	อุปกรณ์อ้างอิง
203.185.69.60	สถาบันมาตรวิทยาแห่งชาติ	Stratum-1	นาฬิกาซีเซียม Stratum-0 เทียบด้วยค่า TAI โดย BIPM (precision ~50 nSec)
time.navy.mi.th	กรมอุทกศาสตร์ กองทัพเรือ	Stratum-1	นาฬิกาซีเซียม Stratum-0 ทำ MOU กับสถาบันมาตรฯ เพื่อส่งค่าเทียบกับ BIPM
time.nist.gov	National Institute of Standards and TechnoLogy, US	Stratum-1	นาฬิกาซีเซียม Stratum-0 เทียบด้วยค่า TAI โดย BIPM

ตารางที่ 4-1 NTP Server ในประเทศไทย

จากตารางที่ 4-1 จะเห็นได้ว่าฐานเวลาที่ตามกฎหมายกำหนดเป็นค่า stratum 0 หมายถึงตัวนาฬิกาที่มีความเที่ยงตรงสูง เมื่อเครื่อง Server ตั้งเวลาอ้างอิงก็จะถือว่าเป็นลำดับชั้น (stratum 1) ส่วนที่เครื่องตัวลูกข่ายในระบบที่อ้างอิงจะเป็น Stratum 3 ตามลำดับ

ขั้นที่ 2 ตรวจสอบ Remote Server ที่ต้องการใช้อ้างอิงฐานเวลา ใช้คำสั่งดังนี้

 # ntpdate -b 203.185.69.60

 # ntpdate -b time.navy.mi.th

 # ntpdate -b time.nist.gov

28 Jan 14:28:20 ntpdate[2693]: step time server 192.43.244.18 **offset -0.092687 sec**

ตัวอย่าง NTP Server ของ Nectec

 # ntpdate -b clock.nectec.or.th

 # ntpdate -b clock2.nectec.or.th

 # ntpdate -b clock.thaicert.nectec.or.th

ที่ต้องให้ทำการทดสอบค่าเวลาระหว่างเครื่องของเรากับ Server ภายนอกเพื่อให้เลือกหา Server ที่เวลาอ้างอิงใกล้เคียงกันมากที่สุด (ดูผลค่า **offset** ต้องมีค่าน้อยที่สุดถ้าเป็นไปได้ควรเลือก Server ในประเทศไทยเลือกมาจัดอันดับที่ 1, 2, 3 ใน configuration) และต้องไม่พบปัญหา no server suitable for synchronization found เพราะถ้าไม่มี host ที่อ้างถึงก็จะไม่สามารถใช้เป็นมาตรฐานเวลาได้

ขั้นที่ 3 หลังจากทำการตรวจสอบเรียบร้อยแล้ว ให้ไปแก้ไขค่า configure ให้มีค่าดังนี้

 # cp /etc/ntp.conf /etc/ntp.conf.bak

 # vi /etc/ntp.conf

……

restrict default kod nomodify notrap noquery nopeer

restrict 127.0.0.1

อนุญาตให้ internal network เข้าใช้

restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

server time.nist.gov dynamic

server clock.nectec.or.th dynamic

server clock2.nectec.or.th dynamic

server 127.127.1.0 # local clock

fudge 127.127.1.0 stratum 10

driftfile /var/lib/ntp/drift

keys /etc/ntp/keys

เมื่อตรวจสอบแก้ไขค่าให้มีตามนี้แล้วบันทึก

:wq

ขั้นที่ 4 ก่อนสั่ง restart service ให้ตรวจสอบ server อ้างอิงอีกครั้ง

 # ntpdate -b 203.185.69.60

สั่ง restart service

 # /etc/init.d/ntpd restart

 # chkconfig ntpd on

หลังจาก start ntpd แล้วต้องรอเวลาให้ server sync เวลากับ server ที่อ้างอิงสามารถใช้คำสั่งตรวจสอบได้ดังนี้

ntpstate

ถ้าต้องการที่จะดูข้อมูลของ ntp server ให้ใช้คำสั่ง

ntpdc

ntpdc> sysinfo

ขั้นที่ 5 ตรวจสอบการทำงานจาก Log file

 # grep ntpd /var/log/messages จะได้ค่าคล้าย ๆ กับตัวอย่างข้างล่าง

Jan 28 15:47:49 ns1 ntpd[3838]: ntpd 4.2.4p2@1.1495-o Thu Jun 21 12:57:41 UTC 2007 (1)

Jan 28 15:47:49 ns1 ntpd[3839]: precision = 2.000 usec

Jan 28 15:47:49 ns1 ntpd[3839]: Listening on interface #2 lo, ::1#123 Enabled

Jan 28 15:47:49 ns1 ntpd[3839]: Listening on interface #5 eth0, 192.168.1.10#123 Enabled

Jan 28 15:47:49 ns1 ntpd[3839]: kernel time sync status 0040

Jan 28 15:47:50 ns1 ntpd[3839]: frequency initialized 80.586 PPM from /var/lib/ntp/drift

สามารถที่จะเปลี่ยนที่เก็บ log จากเดิม /var/log/message ไปไว้ที่ใหม่โดยกำหนดค่า ntp.conf ให้มีค่าเป็น

logfile /var/log/ntp.log

ขั้นที่ 6 หลังจาก Server ทำงานปกติไม่มีการแจ้ง Error ใด ๆ สามารถตรวจสอบตารางการทำงานของ Server ได้ด้วยคำสั่ง

 # ntpq -pn

remote refid st t when poll reach delay offset jitter

==========

203.185.69.60 .PPS. 1 u 49 64 3 49.263 577.356 40.539

122.154.11.67 .GPS. 1 u 50 64 3 50.387 568.011 4.886

192.43.244.18 .ACTS. 1 u 111 64 2 607.213 463.669 0.002

127.127.1.0 .LOCL. 10 1 48 64 3 0.000 0.000 0.002

สามารถใช้เครื่อง Linux เครื่องอื่นในระบบทดสอบการทำงานของ Server ได้ด้วยคำสั่ง

 # ntpdate <ip address> ใส่ ip address ของเครื่อง NTP Server

ขั้นที่ 7 สำหรับเครื่อง **Server Linux** ที่เหลือทั้งหมดของระบบให้ทำการแก้ไขค่า configuration ของโปรแกรม ntp ให้ร้องขอเวลาจาก NTP Server ดังนี้

 # vi /etc/ntp.conf

server **192.168.1.1** <- ip address ของ NTP Server

restrict default ignore

restrict 127.0.0.1

กรอก ip address เครื่อง Client ที่รอรับค่าเวลาจาก server (x)

restrict **192.168.1.x** mask 255.255.255.255 nomodify notrap noquery

driftfile /var/lib/ntp/drift

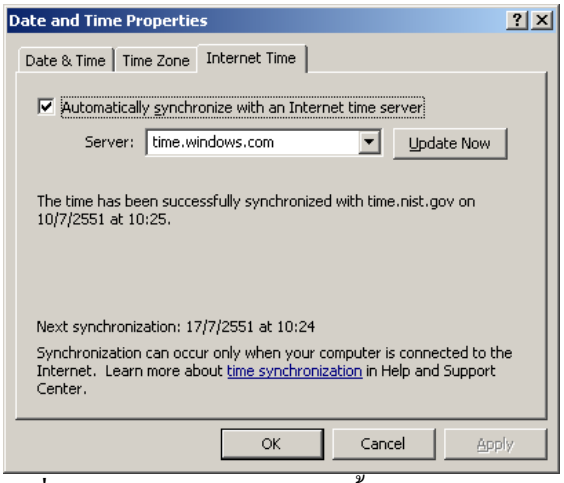
:wq

 # /etc/init.d/ntpd restart

 # chkconfig ntpd on

ใช้คำสั่งตรวจสอบการทำงานเหมือนกับการตั้ง NTP Server ตามตัวอย่างข้างบนที่ผ่านมาแล้วเพื่อให้แน่ใจว่ามีการอ้างอิงเวลาจาก NTP Server ของเราหรือยัง

ขั้นที่ 8 ต่อไปให้จัดการกับเครื่องลูกข่ายในองค์กรหรือหน่วยงาน ซึ่งผู้เขียนจะยกตัวอย่างเฉพาะลูกข่ายที่เป็น Microsoft Windows เพราะเป็นผู้ใช้ส่วนใหญ่ของประเทศ ถ้าเป็น OS ค่ายอื่นต้องศึกษาจากคู่มือของค่ายนั้น ๆ ขั้นตอนนี้ให้ไปแก้ไขค่า Internet time ของเครื่องลูกข่ายโดยไปดับเบิ้ลคลิกที่ นาฬิกาด้านล่างขวาของ Task bar จะได้หน้าจอดังนี้



รูปที่ 4-2 แสดงหน้าต่างสำหรับตั้งค่า Internet Time

จากภาพจะเห็นว่าที่เครื่องลูกข่ายจะมีส่วนของการตั้งเวลาอัตโนมัติ นั่นคือมีการให้กรอกค่า Network Time Server (NTP) เพื่อให้เครื่องสามารถตั้งเวลาตรงกับเวลาสากลได้อย่างถูกต้อง แต่ค่าหลัก (Default) ที่ Microsoft Windows XP กำหนดให้มาเป็นการ Update เวลาทุก ๆ 7 วัน ทำให้เวลาที่ตั้งไว้อาจไม่ตรงหรือคลาดเคลื่อนได้เมื่อเครื่องลูกข่ายมีเวลาไม่ตรงกับเวลามาตรฐานทำให้การบันทึก Log file การใช้งานคลาดเคลื่อนไม่เป็นไปตามกฎหมาย คงไม่สามารถไปบังคับลูกข่ายว่าก่อนเล่นต้องคลิกที่ Update Now คงไม่มีใครยอมทำตามเป็นแน่ให้จัดการกับเครื่องลูกข่ายทุกเครื่องโดยการไปแก้ไข Registry (คิดเองว่าจะใช้วิธีอะไรแก้ไขทุกเครื่อง) ดังนี้

ไปที่เมนู Start -> Run -> regedit กด Enter เข้าไปแก้ที่ตำแหน่ง

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w32time\TimeProviders\NtpClient]

จอภาพด้านขวามือจะมีคำว่า SpecialPollInterval เมื่อดับเบิลคลิกจะปรากฏค่าเป็นเลขฐานสิบหก (Hex) "SpecialPollInterval"=dword:000**93a80** ให้เลือกเป็น decimal จะเปลี่ยนจาก **93a80** เป็น **604800** ค่านี้มีหน่วยเป็นวินาทีมีค่าเท่ากับ 7 วัน (1 วัน = 86400 วินาที) ต้องการให้มีการ Update กี่วินาที กี่นาที หรือกี่ชั่วโมง ก็ให้แก้ไขเลขนี้ได้เลยตามต้องการและที่สำคัญคือให้พิมพ์ลงไปในช่อง Server ของเดิมเป็น time.windows.com เปลี่ยนเป็นเลข IP Address ของเครื่อง NTP Server ที่ตั้งขึ้นเองแล้วทดลองคลิก Update Now ถ้าทำสำเร็จบรรทัดต่อลงมาจะเป็นรายงานว่าเวลาได้ Sync กับ Server เรียบร้อยแล้ว และต้องไม่ลืมเป็นสิ่งสุดท้ายคือต้องตั้งให้ Windows Time Service อยู่ที่ Automatic เพื่อให้ start service ทุกครั้งที่เครื่อง Boot

ขั้นที่ 9 กรณีที่เครื่อง NTP Server ไม่ sync เวลากับฐานเวลาอ้างอิงให้เขียน script แล้วทำการตั้งเวลาด้วย crontab เพื่อตั้งเวลาให้ตรงดังนี้

```
# vi /etc/cron.daily/ntp
#!/bin/bash
/usr/sbin/ntpdate -s -b -u clock.nectec.or.th
/sbin/hwclock --adjust
/sbin/hwclock --systohc
```

:wq

chmod 700 /etc/cron.daily/ntp

ในบรรทัดคำสั่ง ntpdate สามารถระบุชื่อของ server อ้างอิงได้มากกว่าหนึ่งชื่อ แต่ต้องกำหนดค่า option ให้คำสั่งนี้เพิ่มเติมอีกให้ลองใช้คำสั่ง

man ntpdate

เพื่อดูรายละเอียดและเพิ่ม option ให้ครบและแยกชื่อ server แต่ละแห่งด้วยการเว้นหนึ่งเคาะ (space) ก็ใช้งานได้ตามปกติ

Tip & Trick

สำหรับการทำ NTP Server จะมีการใช้งานโปรโตคอล UDP หมายเลข **Port = 123** ต้องไปดูเรื่อง **Firewall** อนุญาตให้ลูกข่ายสามารถเข้าใช้ Port และ Protocol ให้ตรงกันจึงจะใช้งานได้ ในส่วนนี้ตามปกติผู้ดูแลระบบมักจะไม่ได้เปิดไว้สังเกตได้จากเครื่องลูกข่ายบางหน่วยงานที่ไม่สามารถ Update software ได้เลยเพราะติด Firewall ให้ผู้ดูแลระบบตรวจสอบและทำให้สามารถ Update ฐานเวลาเพื่อปฏิบัติตามกฎหมายต่อไป ตัวอย่าง firewall

/sbin/iptables -A INPUT -p udp --dport 123 -j ACCEPT

/sbin/iptables -A OUTPUT -p udp --sport 123 -j ACCEPT

บทสรุป

การที่ผู้เขียนจำเป็นต้องแนะนำให้ทำ Time Server ด้วยโปรแกรม NTP ก็ด้วยเหตุผลว่าต้องการให้เครื่องลูกข่ายและอุปกรณ์เครือข่ายในระบบทั้งองค์กร สามารถที่จะตั้งค่าหรือชี้ไปที่ Time Server ของระบบตนเองดีกว่าที่จะต้องวิ่งออกไปติดต่อกับ Server ภายนอก จะทำให้ลด Traffic และลดปัญหาเรื่องของ Network หลุดๆ ติดๆ ของประเทศไทย จึงฝากให้ผู้ดูแลระบบทั้งหลายคิดถึงองค์ประกอบนี้ด้วย บางคนอาจมองว่าทำไมต้องทำทั้งที่แค่อ้างไปยังหน่วยงานมาตรฐานต่าง ๆ เช่น Nectec หรือตามตารางตัวอย่างข้างบนที่ผ่านมาก็เพียงพอแล้ว นอกจากเหตุผลที่กล่าวมาแล้วยังมีเรื่องที่น่าสนใจอีกต่อไปว่า ตามปกติใน Server แต่ละเครื่องที่ใช้งานกันอยู่ถ้าเป็น NOS (UNIX/Linux) มักมีการติดตั้งตัวโปรแกรม NTP ลงมาด้วยอยู่แล้ว เพียงแต่ไปตั้งค่า Configure ตามตัวอย่างในบทนี้ก็เสร็จแล้วไม่ได้เป็นการเพิ่มงานหรือภาระของ Server แต่อย่างใด จึงควรมองเรื่องนี้ไว้ประกอบกับการทำตามกฎหมายด้วยนะครับ

บทที่ 5

การติดตั้ง Syslog-NG

<u>การติดตั้ง Centralize Log Server</u> ปัจจุบัน Linux ก็ยังคงใช้โปรแกรม syslog ในการบันทึกข้อมูลการทำงานต่าง ๆ บน Server ซึ่งใช้งานกันแพร่หลายมาเป็นเวลานานแล้วและได้มีการปรับเปลี่ยนให้มีความยืดหยุ่นในการใช้งาน ให้สะดวกในการกำหนดค่าต่างๆ เพิ่มขึ้นโดยได้พัฒนาเป็น syslog-ng (New Generation) ต่อไปนี้จะเป็นเนื้อหาการติดตั้งโปรแกรม syslog-ng ทั้งในเครื่องที่ทำหน้าที่เป็น Centralize Log Server และเครื่องให้บริการต่างๆ ภายในองค์กรที่ต้องทำการส่งค่า Log file ไปไว้ที่เดียวกันทั้งหมดใน Centralize Log เพื่อให้ผู้รับผิดชอบในหน่วยงานหรือองค์กรที่ได้รับมอบหมายให้ทำหน้าที่ IT Auditor มีรหัสผ่านเพื่อเข้าระบบได้แต่เพียงผู้เดียวแม้แต่ admin ก็ไม่สามารถเข้าไปดู แก้ไขและเปลี่ยนแปลงข้อมูลใน Log Server ได้ เริ่มทำการติดตั้งใช้งานดังนี้

<u>ขั้นที่ 1</u> ถ้าต้องการติดตั้งบน Linux ค่ายอื่นให้ไปทำการ Download source codeโปรแกรม syslog-ng เพื่อนำมาทำการ Compile และติดตั้งตามรูปแบบที่เป็น source code ภาษาซีได้จาก

http://www.balabit.com/downloads/files/syslog-ng/sources/stable/src/

กรณีที่มีการติดตั้ง syslogd, sysklogd เดิมอยู่แล้วให้ทำการถอนการติดตั้ง (uninstall) ออกก่อนแล้วจึงติดตั้ง (install) syslog-ng ลงไป ตัวอย่าง

```
# rpm -e sysklogd                    กด Enter
```

ถ้าเป็นค่ายที่ใช้ apt-get ให้สั่ง

```
# sudo apt-get --purge remove sysklogd          กด Enter
```

ถ้าต้องการติดตั้งบนค่าย debian สามารถติดตั้งด้วยคำสั่ง

```
# sudo apt-get install syslog-ng
```

ติดตั้งบนค่าย RedHat, Fedora ติดตั้งด้วยคำสั่ง

```
# yum install syslog-ng
```

ในการติดตั้งใช้งานจริงต้องเลือก Version ให้ดีเพราะจากการทดลองพบว่าเมื่อนำค่า Configuration ของ Version 2 ไปใส่กับ version 1.x มันไม่ทำงานหรือทำงานไม่เป็นไปตามที่กำหนด ตัวอย่างต่อไปนี้เป็นการใช้งาน syslog-ng version 2.0.8 ที่อยู่ใน FC8 นำมาใช้ทดลอง (ใน Fedora 6 สามารถกำหนดค่า tcp port ได้ตามต้องการ แต่ใน FC8, FC9 ทำไม่ได้ต้องใช้หมายเลข port เป็น 514 เหมือนกันถึงทำงานได้)

<u>ขั้นที่ 2</u> ทำการแก้ไข Configuration ซึ่งหากต้องการให้มีรูปแบบการจัดเก็บที่แตกต่างจากตัวอย่างก็สามารถทำได้โดยไปศึกษาเพิ่มเติมจากคู่มือของโปรแกรม syslog-ng โดยตรง

ตัวอย่างCentralize Log Server Configuration

 # /etc/syslog-ng/syslog-ng.conf

```
options {
   sync (0);
   time_reopen (10);
   log_fifo_size (1000);
   long_hostnames (off);
   use_dns (no);
   use_fqdn (no);
   create_dirs (no);
   keep_hostname (yes);
};

source s_sys {
   file ("/proc/kmsg" log_prefix("kernel: "));
   unix-stream ("/dev/log");
   internal();
   # udp(ip(0.0.0.0) port(514));
   # tcp(ip(0.0.0.0) port(514));
};

destination d_cons { file("/dev/console"); };
destination d_mesg { file("/var/log/messages"); };
destination d_auth { file("/var/log/secure"); };
destination d_mail { file("/var/log/maillog" sync(10)); };
destination d_spol { file("/var/log/spooler"); };
destination d_boot { file("/var/log/boot.log"); };
destination d_cron { file("/var/log/cron"); };
destination d_mlal { usertty("*"); };
#filter f_filter1   { facility(kern); };
filter f_filter2   { level(info..emerg) and
                     not facility(mail,authpriv,cron); };
```

```
filter f_filter3   { facility(authpriv); };
filter f_filter4   { facility(mail); };
filter f_filter5   { level(emerg); };
filter f_filter6   { facility(uucp) or
                (facility(news) and level(crit..emerg)); };
filter f_filter7   { facility(local7); };
filter f_filter8   { facility(cron); };

#log { source(s_sys); filter(f_filter1); destination(d_cons); };
log { source(s_sys); filter(f_filter2); destination(d_mesg); };
log { source(s_sys); filter(f_filter3); destination(d_auth); };
log { source(s_sys); filter(f_filter4); destination(d_mail); };
log { source(s_sys); filter(f_filter5); destination(d_mlal); };
log { source(s_sys); filter(f_filter6); destination(d_spol); };
log { source(s_sys); filter(f_filter7); destination(d_boot); };
log { source(s_sys); filter(f_filter8); destination(d_cron); };

# Source from remote client
source s_client {
        tcp(ip(0.0.0.0) port(514) keep-alive(yes) max-connections(300));
        udp(ip(0.0.0.0) port(514));
        };

#
# Edit by : Boonlue Yookong, Phitsanulok Thailand.
# Test OK. base on FC8 2 April 2008.
#
# Log from squid (proxy) server kept access.log from LAN.
#
filter f_squid { program("squid") and facility(user); };

destination d_squid {
```

```
  file("/var/log/$HOST/$YEAR/$MONTH/squid.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_squid); destination(d_squid); };

#
# Log mail server from pop3 service.
#
filter f_pop3 { match("pop3"); };

destination d_pop3 {
  file("/var/log/$HOST/$YEAR/$MONTH/pop3.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_pop3); destination(d_pop3); };

#
# Log mail server from imap service.
#
filter f_imap { match("imap|courier"); };

destination d_imap {
  file("/var/log/$HOST/$YEAR/$MONTH/imap.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_imap); destination(d_imap); };
```

```
#
# Log mail server use smtp or sendmail service.
#
filter f_smtp { match("sendmail|smtp"); };

destination d_smtp {
 file("/var/log/$HOST/$YEAR/$MONTH/smtp.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_smtp); destination(d_smtp); };

#
# Log mail server use postfix service.
#
filter f_postfix { program("^postfix/"); };

destination d_postfix {
 file("/var/log/$HOST/$YEAR/$MONTH/postfix.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_postfix); destination(d_postfix); };

#
# Log IM used iptable check MSN,ICQ,... service.
#
filter f_im1 { level(warn..emerg); };
filter f_im2 { program("iptables"); };
```

```
destination d_im {
  file("/var/log/$HOST/$YEAR/$MONTH/msn.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_im1); filter(f_im2); destination(d_im); };

#
# Log dhcp server.
#
filter f_dhcp { program("dhcpd") and facility(daemon); };

destination d_dhcp {
  file("/var/log/$HOST/$YEAR/$MONTH/dhcp.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_dhcp); destination(d_dhcp); };
#
# Log ssh server.
#
filter f_ssh   { program("sshd") and facility(auth, authpriv); };

destination d_ssh {
  file("/var/log/$HOST/$YEAR/$MONTH/ssh.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
```

```
log { source(s_client); filter(f_ssh); destination(d_ssh); };

#
# Log ftp server.
#
filter f_ftp { program("vsftpd"); };

destination d_ftp {
  file("/var/log/$HOST/$YEAR/$MONTH/ftp.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_ftp); destination(d_ftp); };

#
# Log apache (httpd) web server.
#
filter f_www { program("logger"); };
filter f_www1 { program("apache"); };

destination d_www {
  file("/var/log/$HOST/$YEAR/$MONTH/www.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_www); filter(f_www1); destination(d_www); };

#
# Log Samba File server.
#
```

```
filter f_samba   { level(info..emerg) and program("smbd"); };

destination d_samba {
 file("/var/log/$HOST/$YEAR/$MONTH/samba.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_samba); destination(d_samba); };

#
# Log ldap server.
#
filter f_ldap { program("slapd"); };

destination d_ldap {
 file("/var/log/$HOST/$YEAR/$MONTH/ldap.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_ldap); destination(d_ldap); flags(final); };

#
# Log radius server.
#
filter f_radius { program("radiusd"); };
#
destination d_radius {
 file("/var/log/$HOST/$YEAR/$MONTH/radius.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
```

```
};

log { source(s_client); filter(f_radius); destination(d_radius); };

#
# Log Microsoft windows IIS6 www  server
#
filter windows_www { facility(local6) and match(W3SVC1); };

destination windows_www {
file("/var/log/$HOST/$YEAR/$MONTH/windows_www.$YEAR-$MONTH-$DAY"
template("$ISODATE <$FACILITY.$PRIORITY> $HOST $MSG\n")
template_escape(no)
owner(root) group(root) perm(665)
create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(windows_www); destination(windows_www); flags(final); };

#
# Log Microsoft windows IIS6 FTP server
#
filter windows_ftp { facility(local6) and match(FTPSvcLog); };

destination windows_ftp {
file("/var/log/$HOST/$YEAR/$MONTH/windows_ftp.$YEAR-$MONTH-$DAY"
template("$ISODATE <$FACILITY.$PRIORITY> $HOST $MSG\n")
template_escape(no)
owner(root) group(root) perm(665)
create_dirs(yes) dir_perm(0775));
};
```

```
log { source(s_client); filter(windows_ftp); destination(windows_ftp); flags(final); };

filter f_router { facility(local2); };

destination d_router {
 file("/var/log/$HOST/$YEAR/$MONTH/router.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_router); destination(d_router); };

filter f_switch { facility(local3); };
destination d_switch {
 file("/var/log/$HOST/$YEAR/$MONTH/switch.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_switch); destination(d_switch); };

filter f_firewall { facility(local4); };

destination d_firewall {
 file("/var/log/$HOST/$YEAR/$MONTH/firewall.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_firewall); destination(d_firewall); };

filter f_vpnbox { facility(local5); };
```

```
destination d_vpnbox {
  file("/var/log/$HOST/$YEAR/$MONTH/vpnbox.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_client); filter(f_vpnbox); destination(d_vpnbox); };
```

จากตัวอย่างข้างบนเป็น Configuration ที่ทำไว้ให้สำเร็จรูปใน CD ชุดติดตั้งซอฟต์แวร์ Syslog-NG แล้ว ถ้าต้องการให้เก็บมากกว่านี้หรือต้องการระบุเจาะจงไปยังเครื่องหรืออุปกรณ์ก็สามารถใช้การ **filter** ด้วยค่า **host** ได้เช่น

filter windows_ftp { **host("FTP_Server")** and facility(local6) and match(FTPSvcLog); };

แต่ต้องไม่ลืมว่าค่าของ host ต้องเป็นข้อความได้เท่านั้นไม่สามารถใช้ค่า IP Address ของเครื่องนั้น ๆ ได้

จากนั้นให้ไปทำ**Configuration เครื่องลูก** (server) **ที่จะส่ง log ไปเก็บที่ Centralized Log Server** ต้องมีการทำ **Configuration** ให้ตรงกับแต่ละ Service เพื่อมิให้มีค่า log ที่ไม่เกี่ยวข้องตามกฎหมายถูกส่งออกไปด้วย โดยจะแยกทำตัวอย่างให้เป็นเรื่อง ๆ ดังต่อไปนี้

 # /etc/syslog-ng/syslog-ng.conf

```
options {
   sync (0);
   time_reopen (10);
   log_fifo_size (1000);
   long_hostnames (off);
   use_dns (no);
   use_fqdn (no);
   create_dirs (no);
   keep_hostname (yes);
};
```

```
source s_sys {
   file ("/proc/kmsg" log_prefix("kernel: "));
   unix-stream ("/dev/log");
   internal();
   # udp(ip(0.0.0.0) port(514));
   # tcp(ip(0.0.0.0) port(514));
};

destination d_cons { file("/dev/console"); };
destination d_mesg { file("/var/log/messages"); };
destination d_auth { file("/var/log/secure"); };
destination d_mail { file("/var/log/maillog" sync(10)); };
destination d_spol { file("/var/log/spooler"); };
destination d_boot { file("/var/log/boot.log"); };
destination d_cron { file("/var/log/cron"); };
destination d_mlal { usertty("*"); };

#filter f_filter1   { facility(kern); };
filter f_filter2   { level(info..emerg) and
                     not facility(mail,authpriv,cron); };
filter f_filter3   { facility(authpriv); };
filter f_filter4   { facility(mail); };
filter f_filter5   { level(emerg); };
filter f_filter6   { facility(uucp) or
                     (facility(news) and level(crit..emerg)); };
filter f_filter7   { facility(local7); };
filter f_filter8   { facility(cron); };

#log { source(s_sys); filter(f_filter1); destination(d_cons); };
log { source(s_sys); filter(f_filter2); destination(d_mesg); };
log { source(s_sys); filter(f_filter3); destination(d_auth); };
log { source(s_sys); filter(f_filter4); destination(d_mail); };
```

```
log { source(s_sys); filter(f_filter5); destination(d_mlal); };
log { source(s_sys); filter(f_filter6); destination(d_spol); };
log { source(s_sys); filter(f_filter7); destination(d_boot); };
log { source(s_sys); filter(f_filter8); destination(d_cron); };
```

จากตัวอย่างข้างบนเป็นค่า default ของ syslog-ng.conf อยู่แล้วให้เพิ่มเติมเฉพาะส่วนของการระบุ ip address, protocol และ port ที่เครื่อง Log server

destination logserver { tcp("192.168.1.12" port(514)); };

*** 192.168.1.12 เป็น IP ตัวอย่างที่สมมุติให้เป็น Log server ***

ต่อไปนี้ให้พิมพ์เพิ่มเติมต่อท้ายไฟล์เฉพาะ Service ให้ตรงกับการให้บริการในระบบ และถ้าระบบใครที่เครื่อง Server เครื่องเดียวให้บริการหลายอย่าง ก็ให้คัดลอก script แต่ละเรื่องไปต่อกันที่ท้ายไฟล์ syslog-ng.conf ได้เลย ดังตัวอย่างต่อไปนี้

ตัวอย่างการส่ง log ของ ftp server

```
#
# Log ftp server.
#
filter f_ftp { program("vsftpd"); };

destination d_ftp {
  file("/var/log/$HOST/$YEAR/$MONTH/ftp.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_sys); filter(f_ftp); destination(logserver); };
```

ตัวอย่างการส่ง log ของ dhcp server

```
#
```

```
# Log dhcp server.
#
filter f_dhcp { program("dhcpd") and facility(daemon); };


destination d_dhcp {
 file("/var/log/$HOST/$YEAR/$MONTH/dhcp.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_sys); filter(f_dhcp); destination(logserver); };
```

ตัวอย่างการส่ง log ของ Samba Windows File server

```
#
# Log Samba File server.
#
filter f_samba   { level(info..emerg) and program("smbd"); };

destination d_samba {
 file("/var/log/$HOST/$YEAR/$MONTH/samba.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_sys); filter(f_samba); destination(logserver); };
```

ตัวอย่างการส่ง log ของ ldap server

```
#
# Log ldap server.
#
filter f_ldap { program("slapd"); };
```

```
destination d_ldap {
  file("/var/log/$HOST/$YEAR/$MONTH/ldap.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_sys); filter(f_ldap); destination(logserver); flags(final); };
```

ตัวอย่างการส่ง log ของ Mail server

```
#
# Log mail server from pop3 service.
#
filter f_pop3 { match("pop3"); };

destination d_pop3 {
  file("/var/log/$HOST/$YEAR/$MONTH/pop3.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_sys); filter(f_pop3); destination(logserver); };

#
# Log mail server from imap service.
#
filter f_imap { match("imap|courier"); };

destination d_imap {
  file("/var/log/$HOST/$YEAR/$MONTH/imap.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
```

```
};

log { source(s_sys); filter(f_imap); destination(logserver); };
#
# Log mail server use smtp or sendmail service.
#
filter f_smtp { match("sendmail|smtp"); };

destination d_smtp {
 file("/var/log/$HOST/$YEAR/$MONTH/smtp.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_sys); filter(f_smtp); destination(logserver); };

#
# Log mail server use postfix service.
#
filter f_postfix { program("^postfix/"); };

destination d_postfix {
 file("/var/log/$HOST/$YEAR/$MONTH/postfix.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};
log { source(s_sys); filter(f_postfix); destination(logserver); };
```

ตัวอย่างการส่ง log ของ squid server

```
#
#  Log squid server (access.log)
#
```

```
filter f_squid { program("squid") and facility(user); };

destination d_squid {
  file("/var/log/$HOST/$YEAR/$MONTH/squid.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_sys); filter(f_squid); destination(logserver); };
```

ตัวอย่างการส่ง log ของ Secure Shell server

```
#
# Log ssh server.
#
filter f_ssh   { program("sshd") and facility(auth, authpriv); };

destination d_ssh {
  file("/var/log/$HOST/$YEAR/$MONTH/ssh.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};

log { source(s_sys); filter(f_ssh); destination(logserver); };
```

ตัวอย่างการส่ง log ของการใช้งาน IM เก็บจาก iptables

```
#
# Log IM used iptable check MSN,ICQ,... service.
#
filter f_im1 { level(warn..emerg); };
filter f_im2 { program("iptables"); };

destination d_im {
```

```
 file("/var/log/$HOST/$YEAR/$MONTH/msn.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};

log { source(s_sys); filter(f_im1); filter(f_im); destination(logserver); };
```

ขั้นที่ 3 แก้ไขค่าที่เครื่อง Server ในที่นี้ hosts.deny ได้สั่ง ALL: ALL ไว้แล้ว

 # vi /etc/hosts.allow

….

syslog-ng: 192.168.1. <- IP Address ที่ต้องการให้ส่ง Log เข้ามา

:wq

เพิ่มค่าลงใน Firewall iptables ดูตัวอย่างได้จากบทที่ 7 หรือถ้าไม่ได้ทำบทที่ 7 ให้เพิ่มscript ในส่วนของ filter ดังนี้

 # vi /etc/sysconfig/iptables

…ต้องกำหนดกลุ่ม ip address เฉพาะในระบบของเราเท่านั้น

-A INPUT -s 192.168.1.0/255.255.255.0 -p tcp -m state --state NEW -m tcp --dport 514 -j ACCEPT

:wq

 # /etc/init.d/iptables restart

หรือถ้าใช้ lokkit ก็ให้เพิ่มลงในช่องอื่น ๆ 514:tcp ก็สามารถรับค่า Log ได้เช่นกัน **แต่ lokkit จะไม่ระบุ ip address ที่จะส่ง log มีผลให้เครื่องที่อื่น ๆ สามารถส่งเข้ามารบกวนได้**แนะนำให้ปิดทุก port ให้เปิดเฉพาะ Log จะได้ปลอดภัยจากการบุกรุก

ขั้นที่ 4 สั่งให้โปรแกรมเริ่มทำงาน

 # /etc/init.d/syslog-ng start

 # chkconfig syslog off

 # chkconfig syslog-ng on

ตรวจสอบการทำงานด้วยคำสั่ง

 # ps ax |grep syslog-ng

สำหรับตัวอย่าง syslog-ng.conf มีการกำหนดค่าแบ่งเป็น 3 ส่วนคือ source, filter และ destination การที่จะเก็บส่วนใดหรือไม่เก็บส่วนใด ให้เลือกจาก filter เป็นตัวกำหนดเพื่อให้ได้เฉพาะเนื้อหาตรงกับความต้องการ

```
filter f_filter1   { facility(kern); };
filter f_filter2   { level(info..emerg) and
            not (facility(mail)
            or facility(authpriv)
            or facility(cron)); };
filter f_filter3   { facility(authpriv); };
filter f_filter4   { facility(mail); };
filter f_filter5   { level(emerg); };
filter f_filter6   { facility(uucp) or
                (facility(news)
                 and level(crit..emerg)); };
filter f_filter7   { facility(local7); };
filter f_filter8   { facility(cron); };
```

จะเห็นว่าบางเรื่องไม่เกี่ยวข้องกับที่กฎหมายกำหนดก็ไม่ต้องเก็บรวมไปไว้ที่ Centralize Log ด้วยการใช้ Operator and, or, not เข้าไปช่วย เช่น

```
filter notdebug {
            level(info...emerg);
}
filter notmail {
            not facility(mail);
}
```

เมื่อมีการกำหนดค่า filter ตามต้องการแล้วจึงนำไปสั่งให้จัดเก็บในส่วนของคำสั่ง log ดังตัวอย่างนี้

```
log {
            source(local);
            filter(notdebug);
            filter(notmail);
            destination(logserver);
};
```

ส่วนที่ไม่ได้จัดส่งไปยัง Centralize Log Server ก็ยังคงให้จัดเก็บไว้บน Server แต่ละเครื่องตามปกติ เพื่อให้ admin มีไว้วิเคราะห์หรือแก้ปัญหาระบบได้ตามปกติหรือรวมไปถึงการที่ admin ต้องการจัดเก็บค่า log ทุกอย่างไว้ใน server ตัวเองด้วยอีกส่วนหนึ่งก็ได้แต่ไม่สามารถนำส่งตามกฎหมายเพื่อใช้ดำเนินคดีได้

คำเตือน

ให้จำไว้ว่าการเก็บ Log file **ต้องทำการเก็บทั้งสองส่วน**คือ ให้เก็บไว้ที่เครื่อง Server แต่ละ Service ที่ผู้ดูแลระบบต้องทำเป็นปกติอยู่แล้ว และอีกส่วนหนึ่งคือการทำ Configuration ให้ส่งค่า Log file ไปเก็บยัง Centralized Log Server ห้ามละเลยเด็ดขาดเพราะบางคนคิดว่าส่งไปเก็บที่ Log server แล้วไม่ต้องเก็บไว้ที่เครื่องตัวเอง จะมีผลด้านการคัดค้านเมื่อพบว่าข้อมูล Log file ที่นำส่งพนักงานเจ้าหน้าที่มีข้อสงสัยว่ามีข้อผิดพลาดหรือน่าเชื่อว่ามีการแก้ไขข้อมูลหากผู้ดูแลระบบนำข้อมูลของตนเองในเครื่องไปร้องคัดค้านก็จะสามารถเป็นข้อมูลที่ใช้อ้างอิงหรือถ่วงดุลกันระหว่างผู้ดูแลระบบกับผู้ดูแลรักษาข้อมูล Log file ตามกฎหมาย

3. การเก็บ Log ตามที่กฎหมายกำหนด แบ่งได้ 6 หัวข้อตามตารางในภาคผนวก ข ข้อ 2 ท้ายหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ดังนี้

ก. ข้อมูลอินเตอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย ข้อนี้เป็นการให้บริการเข้าถึงระบบระยะไกล (Remote Access) ถ้าหน่วยงานหรือองค์กรใดมีการเปิดบริการ ส่วนมากจะนิยมนำโปรแกรม Freeradius มาติดตั้งใช้งาน ให้ทำการแก้ไข Configuration ของ Freeradius ให้ส่งค่า Log ไปที่ syslog และติดตั้งโปรแกรม syslog-ng ลงไปเพื่อส่งค่า Log file ไปเก็บยัง Centralize Log ดังตัวอย่าง

 # vi /etc/raddb/radiusd.conf

logdir = syslog

log_destination = syslog

:wq

จากนั้นให้แก้ startup script ให้ตามด้วย -l syslog และ -g <facility>

ถ้าเป็นกรณีในข้อ 8 (4) ที่ให้ระบุข้อมูลจราจรเป็นรายบุคคลเช่น Proxy Server ตามปกติระบบที่ใช้กันอยู่มักเป็น Gateway server ที่ทำ Proxy รวมไว้ด้วย เพียงแต่ต้องทำการ Authentication เพื่อให้ user ทุกคนต้องทำการ Log on เข้าระบบ โปรแกรมที่ใช้กันอยู่อย่างแพร่หลายคือ Squid ซึ่งมีการจัดการเรื่อง Log file อย่างดีอยู่แล้ว เพียงแต่ไปแก้ Configuration ให้ชี้ไปเก็บที่ Log กลาง ดังนี้

 # vi /etc/squid/squid.conf

…ของเดิมถ้า logformat เป็น squid ต้องแก้เป็น **combined**

access_log /var/log/squid/access.log **combined**

คัดลอกเพิ่มอีกหนึ่งบรรทัดและแก้ไขเป็น

access_log syslog combined

อย่าลืมลบเครื่องหมาย # หน้าบรรทัดLogformat combined ออกด้วย

:wq

 # squid -k reconfigure

สำหรับระบบที่ยุ่งยากหรือซับซ้อน หน่วยงานที่มีงบประมาณมากอาจมีการวางระบบเครือข่ายที่ใช้อุปกรณ์ **Hardware ราคาแพง**เช่นการวาง **Core Switch, Manage Switch** การทำ **VLAN** การทำ **NAT** ที่อุปกรณ์ต่าง ๆ รวมไปถึงการวางอุปกรณ์ประเภท **WiFi Hotspot** หรือที่รู้จักกันตามหน่วยงานว่า Access Point (AP) เช่นระบบเครือข่ายของมหาวิทยาลัยต่าง ๆ แบบนี้ต้องดูคู่มือของอุปกรณ์ประกอบในเรื่องการเก็บ Log และการทำ Forward Log ไปยัง Log กลางเพื่อเป็นข้อมูลประกอบกับ user account ในการระบุหมายเลขเครื่องหรือชื่อ host ที่ใช้งานในขณะนั้น

ข. ข้อมูลอินเตอร์เน็ตบนเครื่องที่ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers) ปัจจุบันหน่วยงานต่าง ๆ ก็เริ่มสนใจที่จะทำ Mail Server ของตนเองก็จะเข้าข่ายเป็นเครื่องให้บริการ จำเป็นต้องทำการเก็บ Log ตามที่กฎหมายกำหนด ในส่วนนี้ไม่มีปัญหาอะไรเพราะ Mail Server ที่มีใช้งานกันอยู่เป็น Protocol มาตรฐานเช่น pop, imap และ smtp ซึ่งถือว่าเป็นส่วนหนึ่งของระบบมีการบันทึก Log อยู่แล้วสามารถที่จะติดตั้ง syslog-ng ในส่วน client ก็จะส่ง Mail Log ไปเก็บยัง Log กลางได้ทันที แต่ถ้าเป็นกรณีการใช้ Free e-mail ที่มีให้บริการในเว็บต่าง ๆ ข้อมูลก็จะไปอยู่ที่ Log ของผู้ให้บริการ mail นั้น ๆ ระบบของเราเพียงเก็บรายละเอียดการใช้งานผ่านเว็บได้จาก Access Log ที่ proxy ก็จะรู้ว่าใครออกไปใช้บริการ mail ข้างนอกหากมีการเก็บข้อมูลไม่ครบเช่น user account เจ้าพนักงานก็สามารถร้องขอ Log ไปยัง Server ที่ให้บริการเพื่อนำมาเปรียบเทียบระบุตัวตนได้

ค. ข้อมูลอินเตอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล สำหรับหน่วยงานที่ทำ FTP Server โดยตรงหรือเพียงเปิดบริการโอนแฟ้มข้อมูลในการทำเว็บก็ตามจัดได้ว่ามีการให้บริการโอนแฟ้มข้อมูลเช่นกัน ต้องทำการเก็บ Log file ส่วนใหญ่การเปิดบริการ FTP จะเป็นโปรแกรมที่มีมาให้กับ Linux ทุกค่ายอยู่แล้วหรือบางแห่งอาจไป download มาใช้เองก็ตาม ในส่วนของ Configuration จะมีการสั่งให้จัดเก็บ Log ไว้อยู่แล้ว ตัวอย่างเช่นโปรแกรม vsftpd ก็ต้องไปแก้ไขส่วนของ Log ดังนี้

 # vi /etc/vsftpd/vsftpd.conf

….. ส่วนที่เป็น Log อื่น ๆ ปิดให้หมดแล้วเพิ่ม syslog ลงไป

Activate Logging of uploads/downloads.

xferlog_enable=YES

#log_ftp_protocol=YES

เพิ่มลงไปอีกสองบรรทัด

log_ftp_protocol=YES

syslog_enable=YES

:wq

 # /etc/init.d/vsftpd restart

หลังจากติดตั้ง syslog-ng เสร็จเรียบร้อย ค่าการใช้งาน FTP Server ก็จะถูกส่งไปเก็บยัง Log กลางทันที มีข้อควรระวังอีกอย่างคือสำหรับผู้ดูแลระบบที่ชอบใช้ Secure Shell (ssh) เป็นการเข้าถึง Server ระยะไกลที่ปลอดภัย ใน Configuration ของ sshd จะมีการนำเอา sftp server มารวมไว้ให้ทำงานแบบ Subsystem ตัวนี้เป็นการอำนวยความสะดวกให้ผู้ดูแลระบบแต่ server จะเก็บ Log ให้เฉพาะ sshd เท่านั้นในส่วนของ sftp-server เป็น child process ใน Log จะเก็บเพียงมีการร้องขอบริการ sftp แต่ไม่เก็บรายละเอียดตามกฎหมาย ถ้าไม่อยากให้เกิดปัญหาควรยกเลิกการบริการ sftp-server แล้วไปใช้ FTP server หลักของระบบแทน จะได้ Log ที่มีข้อมูลครบถ้วนต่อไป

ง. ข้อมูลอินเตอร์เน็ตบนเครื่องให้บริการเว็บ ระบบโดยทั่วไปสำหรับหน่วยงานต่าง ๆ ที่มีการเปิดให้บริการเว็บถ้าเป็น Linux หรือ Software ประเภท Open source แล้วจะนิยมใช้โปรแกรม Apache หรือในชื่อ httpd ซึ่งเป็นโปรแกรมระดับมืออาชีพ มีการเก็บบันทึกการใช้งานของผู้ชมไว้อย่างละเอียดในรูปของ access_log อยู่แล้วและยังสามารถจัดการเกี่ยวกับรูปแบบ (Log format) ให้จัดเก็บได้ตรงตามกฎหมายอีกด้วย สิ่งที่ต้องทำคือการเข้าไปแก้ค่า Configuration ให้ส่ง Log file ไปไว้ยัง Log กลางเท่านั้น ทำดังนี้

 # vi /etc/httpd/conf/httpd.conf

….. ของเดิม

LogLevel warn

แก้ไขเป็น

LogLevel notice

ของเดิม

CustomLog logs/access_log combined

คัดลอกเพิ่มอีกหนึ่งบรรทัดและแก้ไขเป็น

CustomLog "|/usr/bin/logger -p local1.info" combined

:wq

 # /etc/init.d/httpd restart

กรณีเปิดให้บริการ Secure Socket Layer (SSL) ก็ไปแก้ไขที่

 # vi /etc/httpd/conf.d/ssl.conf

<VirtualHost _default_:443>

พิมพ์เพิ่ม 1 บรรทัด

CustomLog "|/usr/bin/logger -p local1.info" combined

:wq

 # /etc/init.d/httpd reload

หรือจะใช้วิธีการเขียน Script เพื่อส่งค่า log ดังนี้

```
#!/usr/bin/perl
use Sys::Syslog qw( :DEFAULT setlogsock );

setlogsock('unix');
openlog('apache', 'cons', 'pid', 'local1');

while ($log = <STDIN>) {
        syslog('notice', $log);
}
closelog
```

บันทึก script ไว้ที่ **/usr/bin/httpd_log**

ให้ไปแก้ค่าใน httpd.conf ดังนี้

vi /etc/httpd/conf/httpd.conf

CustomLog logs/access_log combined

คัดลอกเพิ่มอีกหนึ่งบรรทัดและแก้ไขเป็น

CustomLog |/usr/bin/httpd_log combined

:wq

 # /etc/init.d/httpd reload

และถ้าใช้ SSL ก็ให้ไปแก้ค่าใน ssl.conf ดังนี้

vi /etc/httpd/conf./ssl.conf

<VirtualHost _default_:443>

พิมพ์เพิ่ม 1 บรรทัด

CustomLog |/usr/bin/httpd_log combined

:wq

 # /etc/init.d/httpd reload

หลังจากติดตั้ง syslog-ng เรียบร้อยแล้ว Log จาก Web Server จะถูกส่งไปเก็บยัง Log กลางตามรูปแบบที่กำหนดใน Log format ครบถ้วน

จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet) หัวข้อนี้ไม่มีเปิดให้บริการในหน่วยงานบ้านเราจึงไม่มีตัวอย่างการเก็บ Log File ตามปกติจะใช้การทำงานแบบ NNTP (Usenet News Transfer Protocol) port 119 ทั้ง tcp และ udp

ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเตอร์เน็ตเช่น Internet Relay Chat (IRC) หรือ Instant Messaging (IM) เป็นต้น คงจะหนีไม่พ้นเรื่องของการติดต่อสื่อสารกันระหว่างบุคคลของสมาชิกในองค์กรต่าง ๆ มักนิยมใช้การสนทนาด้วยโปรแกรมที่มีไว้บริการฟรี ๆ กันอย่างแพร่หลายเช่น MSN, Yahoo, ICQ ซึ่งมีโอกาสที่จะใช้กระทำความผิดได้จึงต้องมีการเก็บข้อมูลระหว่างผู้ที่กำลังสนทนาไว้ใน Log file เช่นกัน รวมไปถึงประเภทในการติดต่อเช่นพิมพ์ข้อความ ใช้กล้องหรือส่งไฟล์ ระบบต้องจัดเก็บเฉพาะในส่วนที่กฎหมายกำหนดคือ user account ของผู้สนทนา หมายเลขเครื่อง วันเดือนปีเวลาที่ใช้ติดต่อและประเภทในการติดต่อ สามารถทำได้ง่ายโดยอาศัยหลักการ Transparent Proxy เหมือนกับเรื่อง Web Proxy Server แต่หัวข้อนี้ต้องเป็น IM Transparent Proxy นั่นคือให้ไป download โปรแกรม imspector เป็นโปรแกรมประเภท Open source มาติดตั้งไว้บนเครื่อง Gateway ที่จ่ายสัญญาณอินเตอร์เน็ตให้ลูกข่าย จากนั้นก็แก้ไข Configuration ให้ทำการส่ง Log file ไปเก็บยัง Log กลางเหมือนเรื่องอื่น ๆ แต่ต้องพึงระวังเพราะ software ที่ทำหน้าที่ Transparent Proxy จะเก็บข้อมูลที่กำลังสนทนาได้อาจผิดกฎหมายละเมิดสิทธิ์ส่วนบุคคลได้

ตัวอย่างการเขียน Firewall

เพื่อส่งค่า Log ของ IM ไปเก็บเพื่อใช้เปรียบเทียบกับ imspector

*nat

-A POSTROUTING -p tcp --dport 1863 -m limit --limit 5/min -j LOG --log-prefix "MSN: " --log-level WARN

-A POSTROUTING -p tcp --dport 5190 -m limit --limit 5/min -j LOG --log-prefix "ICQ/AIM: " --log-level WARN

-A POSTROUTING -p tcp --dport 5050 -m limit --limit 5/min -j LOG --log-prefix "Yahoo: " --log-level WARN

-A POSTROUTING -p tcp --dport 6667 -m limit --limit 5/min -j LOG --log-prefix "IRC: " --log-level WARN

ตัวอย่างการเขียน Firewall เพื่อ Redirect IM ไปยัง Transparent proxy

MSN: iptables -t nat -A PREROUTING -p tcp --destination-port 1863 -j REDIRECT

--to-ports 16667

ICQ/AIM: iptables -t nat -A PREROUTING -p tcp --destination-port 5190 -j REDIRECT

--to-ports 16667

Yahoo: iptables -t nat -A PREROUTING -p tcp --destination-port 5050 -j REDIRECT

--to-ports 16667

IRC: iptables -t nat -A PREROUTING -p tcp --destination-port 6667 -j REDIRECT

--to-ports 16667

แต่จุดอ่อนของโปรแกรมนี้คือไม่ได้เก็บเลข IP หรือชื่อเครื่องที่เล่นไว้ ถ้าต้องการให้ได้เลข IP ของเครื่องที่กำลังสนทนาต้องไปเก็บที่ Firewall ในแต่ละ port ข้างต้นลง Log file เพื่อนำไปเปรียบเทียบกับ IM Log ก็สามารถระบุตัวตนพร้อมเครื่องที่ใช้กระทำความผิดได้

4. การทำระบบรักษาความปลอดภัยให้ Log Server หากจะปฏิบัติตามที่กฎหมายกำหนดให้ครบถ้วนสมบูรณ์ที่ระบุว่าต้องทำ Data hashing, Data archiving และต้องไม่ให้ admin เข้าระบบ Log Server ได้เลย น่าจะต้องให้ผู้ที่ได้รับมอบหมายหรือ IT Auditor เป็นผู้ถือรหัสผ่านของเครื่อง Log Server จากนั้นในการปฏิบัติงานจริงข้อมูล Log จะมีปริมาณมากมายมหาศาล สิ่งที่ต้องทำคือ

ก. ทำ Rotation ให้กับ Log Server ผู้ดูแลระบบบางคนอาจคิดที่จะทำการ rotate Log ที่บันทึกใน server ผู้เขียนแนะนำว่า ใน script ของ syslog-ng.conf ได้ทำการจัดเก็บแยก Log ที่ส่งมาจาก server แต่ละตัว เช่น /var/log/webserver/… และใน Directory ย่อยของแต่ละ server จะเป็นการบอก ปี เดือน ในรายการย่อยแต่ละไฟล์ยังระบุชื่อไฟล์พร้อมนามสกุลเป็น ปี-เดือน-วัน ให้อีกเพื่อสะดวกในตอนค้นหาข้อมูลในแต่ละวัน เช่นส่งจาก webserver จะได้ไฟล์ /var/log/webserver/2008/02/kernel.2008-02-14 เป็นต้น ดังนั้นจึงไม่จำเป็นต้องทำการ rotate ไฟล์เพราะจะเก็บให้ไฟล์ละวันอยู่แล้ว

ข. ทำการบีบอัดข้อมูล Log (Compress) เพื่อให้ขนาดไฟล์เล็กลง ให้ใช้คำสั่ง tar เหมือนกับเรื่อง Backup ในบทที่ 8 ดังตัวอย่าง

 # tar cvfz webserver.tar.gz /var/log/webserver

 # ls

webserver.tar.gz

ค. ทำการเข้ารหัสไฟล์ที่บีบอัดไว้แล้ว ก็ให้ใช้หลักการเดียวกับบทที่ 8 เช่น

 # openssl des -in webserver.tar.gz -out webserver.sec

 # ls

webserver.tar.gz webserver.sec

กรณีบีบอัดไฟล์และทำการเข้ารหัสไฟล์แล้วต้องการสำรอง (backup) ส่งไปยัง CD ต้องทำการจัดเก็บค่าสำหรับตรวจสอบความถูกต้องของไฟล์ต้นทางไว้ด้วย ดังนี้

md5sum webserver.sec > MD5SUM

ให้ส่งไฟล์ MD5SUM ไปเก็บพร้อมกับไฟล์ webserver.sec ด้วย เวลาจะนำมาใช้ต้องตรวจสอบความถูกต้องของไฟล์ด้วยคำสั่ง

md5sum -c MD5SUM

จะต้องปรากฏข้อความว่า

webserver.sec: OK

ถึงจะได้ไฟล์ที่ถูกต้องเหมือนต้นฉบับที่ไม่มีการนำไปแก้ไขดัดแปลง

หรือใช้ SHAxxxSUM เพื่อเพิ่มจำนวนบิทให้มากตามต้องการเช่น

sha1sum webserver.sec > SHA1SUM

ให้ส่งไฟล์ SHA1SUM ไปเก็บพร้อมกับไฟล์ webserver.sec ด้วย เวลาจะนำมาใช้ต้องตรวจสอบความถูกต้องของไฟล์ด้วยคำสั่ง

sha1sum -c SHA1SUM

จะต้องปรากฏข้อความว่า

webserver.sec: OK

ข้อดีของการใช้ SHAxxxSUM คือสามารถเลือกจำนวนบิทได้ ถ้าต้องการให้มีความปลอดภัยสูงก็สามารถใช้คำสั่ง

sha224sum filename > SHA224sum

sha256sum filename > SHA256sum

sha384sum filename > SHA384sum

sha512sum filename > SHA512sum

เมื่อต้องการนำส่งข้อมูลต้องทำการถอดรหัสไฟล์ก่อนหรือถ้าทำไม่เป็นก็ต้องส่งมอบพร้อมรหัสผ่านและวิธีการเข้ารหัสไฟล์ให้พนักงานเจ้าหน้าที่ ถึงจะได้ไฟล์ที่ถูกต้องเหมือนต้นฉบับที่ไม่มีการนำไปแก้ไขดัดแปลง จึงค่อยทำการถอดรหัสไฟล์ด้วยคำสั่ง

 # openssl des -d -in webserver.sec -out webserver.tar.gz

ง. จัดเก็บหรือ Backup ลงบนสื่อที่มีอายุการใช้งานครอบคลุมในการจัดเก็บ ให้ดูวิธีการบันทึกลงสื่อ เช่น CD ได้จากบทที่ 8 ผู้ที่รับผิดชอบข้อมูล Log ต้องจัดลำดับงาน เช่น

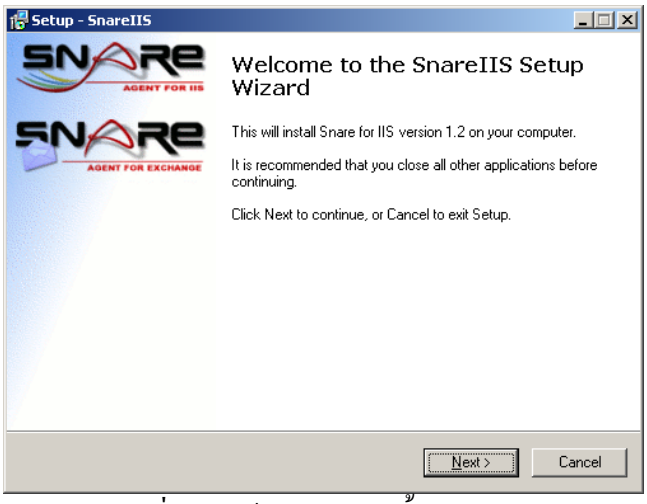
- หลังจากทำการบีบอัดไฟล์ตามข้อ ข เสร็จแล้วต้องลบต้นฉบับทิ้ง
- หลังจากเข้ารหัสไฟล์ตามข้อ ค แล้วให้ลบไฟล์ .gz ทิ้ง
- สร้างรหัสเพื่อตรวจสอบความถูกต้องของไฟล์ข้อมูล (Check Sum)
- ส่งไฟล์ที่เข้ารหัสแล้วและไฟล์ check sum ไปยัง media ที่ใช้สำหรับ Backup เช่น CD ROM หลังจาก backup ลง CD แล้วให้ลบไฟล์ .sec ใน Server ทิ้ง

งานที่ต้องทำก็คือควรเขียนเป็น script ไว้เพื่อสะดวกในการทำงานดีกว่าที่จะไปนั่งสั่งทาง command line อาจเขียน script ไว้ที่ crontab ให้ทำการบีบอัดไฟล์และเข้ารหัสทุกเที่ยงคืนพร้อมลบไฟล์ข้อมูลดิบทิ้งแล้วสั่ง reload syslog-ng ใหม่เพื่อรองรับการทำงานสร้าง Log ใหม่ต่อไป สำหรับข้อนี้เป็นเพียงการแนะนำ ถ้า Hard disk มีพื้นที่เก็บ Log มากก็ไม่ต้องเก็บลง CD ก็ได้เพียงแต่ควรสั่งให้มีการลบทิ้งเมื่อได้ระยะเวลาหนึ่งเช่น 3 เดือนหรือไม่เกิน 1 ปีตามกฎหมายกำหนด หรืออาจใช้วิธีทำ Log rotate เพื่อให้การจัดเก็บวนไปตามจำนวนตามต้องการแล้วมันจะลบตัวเองเมื่อครบกำหนดที่สั่ง rotate ไว้เป็นอัตโนมัติก็ได้ เพราะเป็นไปไม่ได้ที่ความจุจะมากจนรับการทำงานได้ตลอดไป

สำหรับกรณี Microsoft .. server

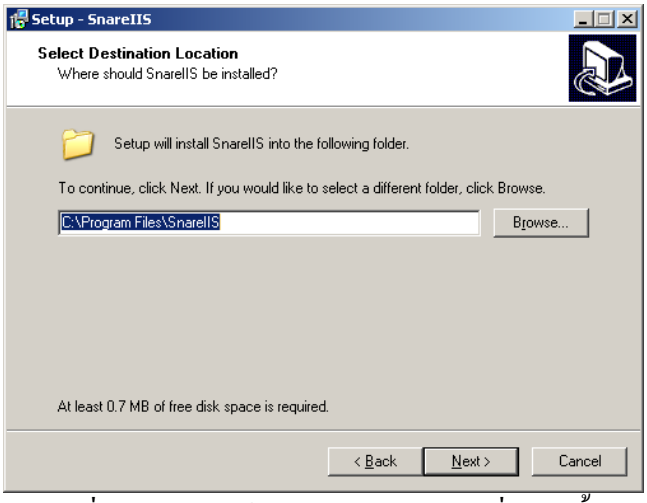
กรณีที่ในระบบมีการติดตั้ง Server ด้วย Microsoft Windows 2xxx Server มีการเปิดบริการ Web server และ FTP serverซึ่งตรงกับที่กฎหมายกำหนด ก็สามารถที่จะส่ง log จาก MS Windows Server ไปยัง Log กลางที่ติดตั้ง Syslog-NG ไว้ได้เช่นกัน ผู้ดูแลต้องไปหา download โปรแกรมมีทั้งฟรีและต้องเสียเงินซื้อในบทนี้จะขอยกตัวอย่างโปรแกรมฟรีชื่อ snare จากเว็บ http://www.intersectalliance.com/ เพื่อนำไปติดตั้งบน Server แล้วทำการ Configuration ให้ส่ง log ทั้ง Web server และ FTP serverไปเก็บยัง Log กลาง วิธีติดตั้งให้ทำดังนี้ (ตัวอย่างนี้เป็นการติดตั้ง snare for IIS)

ขั้นที่ 1 หลังจาก Download ได้ File ชื่อ SnareIISSetup-1.2.exe มาแล้วให้ให้ติดตั้งโปรแกรมลงบน Microsoft Windows 2xxx Server จะปรากฏภาพดังนี้



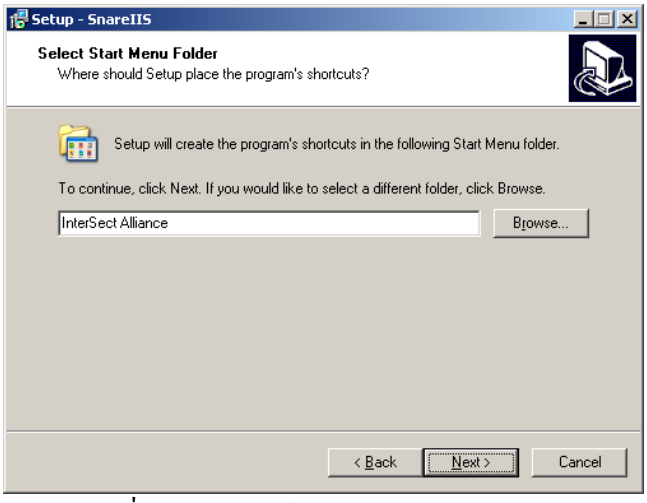
รูปที่ 5.1 หน้าแรกการติดตั้ง SnareIIS

ขั้นที่ 2 ให้คลิกที่ Next เพื่อทำงานต่อไป จะปรากฏหน้าจอให้เลือก Directory ที่จะทำการติดตั้งโปรแกรม ดังภาพ



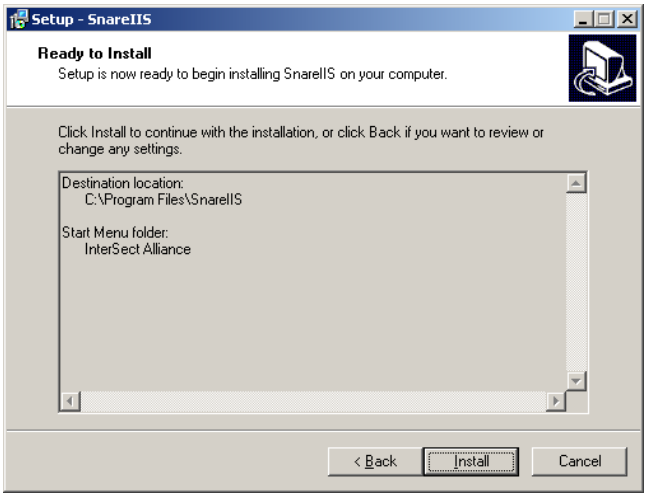
รูปที่ 5.2 แสดงหน้าต่างเลือก Directory ที่จะติดตั้ง

ขั้นที่ 3 โปรแกรมจะแสดง Start Menu Folder เพื่อให้เลือกชื่อที่ต้องการให้ปรากฏในเมนูซึ่งโปรแกรมจะสร้าง Shotcuts มีชื่อตามที่กำหนด



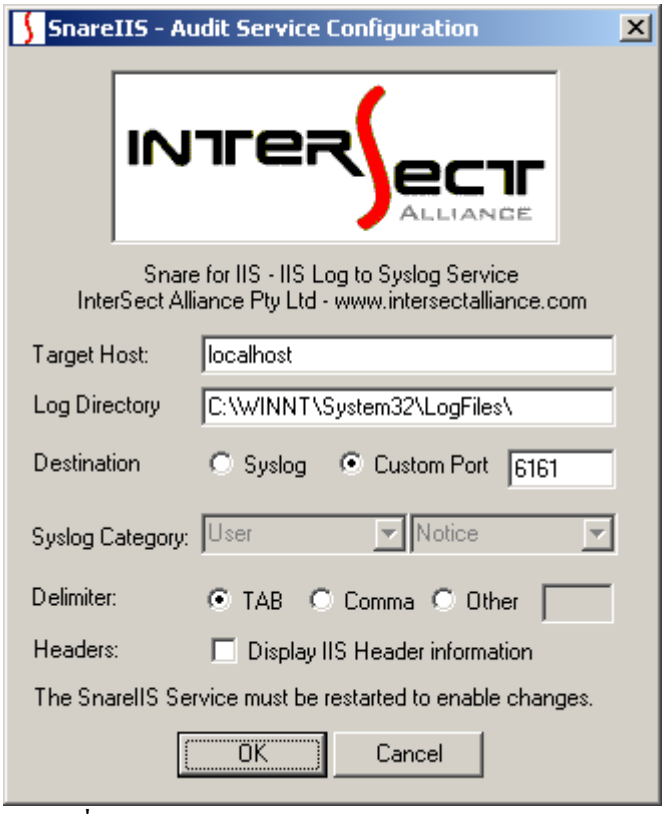
รูปที่ 5.3 แสดงหน้าต่าง Start Menu Folder

ขั้นที่ 4 เริ่มติดตั้งโปรแกรม ให้คลิกที่ Install



รูปที่ 5.4 แสดงภาพเริ่มติดตั้งโปรแกรม

ขั้นที่ 5 ให้ทำการกำหนดค่า Configuration ให้กับโปรแกรมให้ตรงกับความต้องการที่จะใช้งานดังภาพ



รูปที่ 5.5 แสดงหน้าต่างการกำหนดค่า Configuration

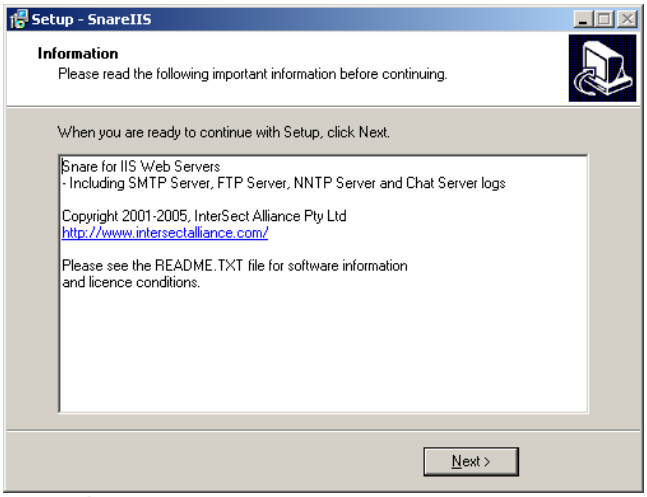
Target Host: ให้ใส่ค่า IP Address เครื่อง Centralize Log

Log Directory ให้ใส่ค่าให้ตรงกับในเครื่องเช่นถ้าเป็น Windows 2003 Server ต้องใส่เป็น **C:\WINDOWS\System32\LogFiles**

Destination ให้เลือกเป็น Syslog

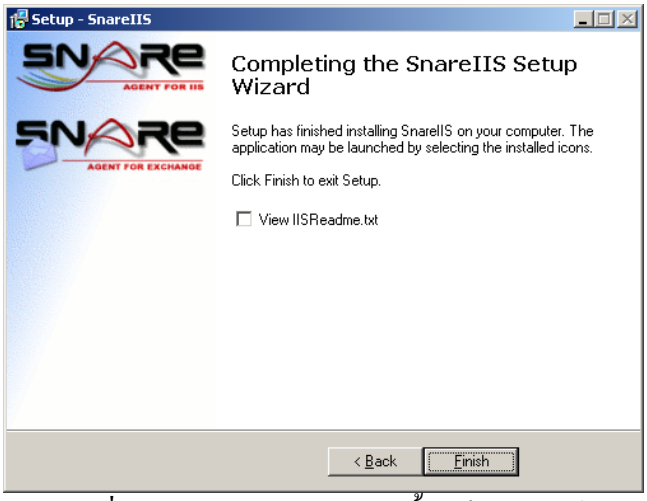
Headers: ถ้าไม่ต้องการให้แสดง IIS Header ก็ไม่ต้องเลือก

หลังจากทำการใส่ค่า Configuration เสร็จสมบูรณ์ก็จะปรากฏภาพแสดงข้อมูลของโปรแกรม



รูปที่ 5.6 แสดงข้อมูล (Information) ของโปรแกรม

เมื่อคลิก Next ก็จะแสดงหน้าต่างการติดตั้งเสร็จสมบูรณ์และมี Check Box ว่าจะให้แสดงไฟล์ Readme.txt หรือไม่ค่า Default มีเลือกไว้ถ้าไม่ต้องการอ่านก็คลิกเครื่องหมายถูกออก แล้วคลิกที่ Finish



รูปที่ 5.7 แสดงหน้าต่างการติดตั้งเสร็จสมบูรณ์

เพียงเท่านี้เครื่อง Microsoft Windows 2xxx Server ที่มีการติดตั้ง IIS ทำหน้าที่ Web Server และ FTP Server ก็จะสามารถส่ง Log file ไปยังเครื่อง Centralize Log Server ได้ตามต้องการ

<u>บทสรุป</u>

ในส่วนของการทำ Centralize Log Server ตามที่ได้รวบรวมสรุปวิธีการทำอย่างง่ายแต่ครอบคลุมตามที่กฎหมายกำหนดโดยไม่ต้องลงทุนหรือจัดสรรงบประมาณจำนวนมากมายนัก ระบบที่แนะนำต้องการเพียงเครื่อง Log Server ที่ไม่มีการให้บริการอื่น ๆ ทำงานเพียงหน้าที่เดียว มีผู้ดูแลคนเดียวและที่สำคัญผู้ที่ได้รับมอบหมายต้องสามารถอ่าน Log file เป็นสามารถนำส่วนที่ถูกร้องขอส่งเจ้าพนักงานเพื่อใช้เป็นข้อมูลในชั้นศาลได้อย่างครบถ้วนเพื่อลดขั้นตอนตั้งแต่การสืบสวนไปจนถึงลดขั้นตอนการโต้แย้งต่าง ๆ หากมีการระบุตัวตน สถานที่ วันเวลาที่กระทำความผิดได้ แต่กฎหมายก็เปิดทางไว้ว่าให้เก็บเฉพาะส่วนที่ให้บริการเท่าที่ทำได้ ผู้ดูแลระบบก็คงไม่ต้องกังวลจนลาออก หรือไม่กล้าที่จะรับภาระในการดูแล Log ให้กับหน่วยงานของตนเอง เพราะการเตรียมการที่ดี การจัดการที่ดีจะส่งผลดีในตอนที่เกิดเหตุการณ์กระทำความผิดเท่านั้น จนบางหน่วยงานอาจมองว่ายังไม่ต้องทำก็ได้คงไม่มีปัญหาอะไร ใช้งานมาตั้งนานแล้วยังไม่เกิดปัญหาเลยแบบนี้ก็แล้วแต่จะคิด เพราะกฎระเบียบเป็นเพียงการกำหนดให้ประชาชนปฏิบัติตาม แต่ก็เป็นปกติธรรมดาที่ต้องมีผู้ปฏิบัติบ้าง ไม่ปฏิบัติบ้าง แล้วแต่นโยบายหรือการบริหารจัดการของหน่วยงานนั้นๆ หวังว่าขั้นตอนและข้อแนะนำในภาคผนวกนี้คงจะได้นำไปใช้ประโยชน์กับหน่วยงานหรือองค์กรแต่ละแห่งของประเทศไทย (ที่มีเงินงบประมาณน้อยไม่มีเงินจ้างผู้อื่นทำให้)

ที่จำเป็นและสำคัญมากคือต้องมีการทำระบบความปลอดภัยให้กับ Log Server เป็นอย่างดีไม่ใช่เป็น Server ที่เปิดทุก Service หรือเปิดหลาย port ควรทำหน้าที่เดียวและทำ Secure พร้อม Firewall ของตนเองอย่า

บทที่ 6

Kernel Harden

การปรับแต่งค่าต่าง ๆ ให้กับ kernel

ในที่นี้จะกล่าวให้เห็นภาพของการดูแล Server ในส่วนของผู้ดูแลระบบ (Administrator) ควรทำการวางแผนการป้องกันภัยที่จะมาคุกคามระบบเครือข่ายทั้งหมด ตั้งแต่ Router ไปจนถึงเครื่องลูกข่าย ดังนั้นในคู่มือเล่มนี้จะเน้นให้ผู้ดูแลทำเป็นขั้นตอน เพื่อให้ระบบมีเสถียรภาพมากที่สุดเท่าที่จะทำได้ แต่ต้องไม่ลืมว่าสิ่งที่เราทำได้ฝ่ายตรงข้ามก็ย่อมทำได้เช่นกัน ดังนั้นการติดตามข้อมูลข่าวสารเกี่ยวกับความปลอดภัยของระบบน่าจะเป็นสิ่งที่ดีที่สุด มากกว่าที่จะมั่นใจว่าเราได้ทำแล้วและคงจะป้องกันได้ตลอดไป เลยเกิดความประมาท ทิ้งเครื่อง Server ไว้โดยไม่ดูแลและปรับปรุงอะไรเลย อาจทำให้เกิดความเสียหายได้มากถึงขั้นไม่สามารถกู้คืนได้ บางกรณีถึงกับต้อง format และติดตั้ง OS ใหม่เลยก็มี

เริ่มด้วยการป้องกันตั้งแต่ตัว Case

ในกฎหมายระบุไว้ชัดเจนว่าผู้ดูแลระบบหรือ Admin ต้องไม่สามารถเข้าถึงข้อมูลจราจรเครือข่ายคอมพิวเตอร์ได้ ซึ่งในทางปฏิบัติเมื่อเครื่อง Log Server ถูกติดตั้งอยู่รวมกับ Server อื่น ๆ ในระบบที่มี Admin ดูแลอยู่จะเป็นการทำงานที่ไม่ครอบคลุมตามที่กฎหมายบอกไว้ จึงควรจัดหา Spec ของเครื่อง Log Server ที่มีการป้องกันการเปิดเข้าถึงตัวเครื่องได้เช่นอาจมีที่ใส่กุญแจป้องกันการเปิด Case เพื่อ Clear BIOS หรือนำข้อมูลออกจากแหล่งบันทึกข้อมูลได้โดยง่าย หรืออาจมีวิธีการอื่นใดที่ป้องกันได้ดีกว่านี้ก็ควรต้องทำ

ป้องกันที่ BIOS

สิ่งที่ไม่ควรมองข้ามก็คือการตั้งค่าที่ BIOS ให้ไม่สามารถ Boot จาก Floppy Disk, USB, CD ROM หรือ Remove media อื่น ๆ ได้และต้องไม่ลืมใส่ password ให้กับ BIOS เพื่อป้องกันไม่ให้ผู้อื่นสามารถเข้าไปแก้ไขค่าที่ตั้งไว้ได้ คำแนะนำนี้ผู้อ่านต้องเปิดคู่มือการตั้งค่า BIOS จากเครื่องที่ใช้งานเองนะครับ ควรอ่านให้ละเอียดในคู่มือว่านอกจากตั้งค่าไม่อนุญาตให้ Boot จากอุปกรณ์ต่าง ๆ ที่กล่าวมาได้แล้วยังมีเมนูส่วนของ Security อื่น ๆ ให้ตั้ง Password อีกหรือไม่จากนั้นควรกำหนดบุคคลที่มีสิทธิในการรับรู้ Password นี้ได้เป็นบางคนเท่านั้น การป้องกันนี้จะถูกบุกรุกได้วิธีเดียวคือเปิดเครื่องเพื่อปลด Battery Backup ออกหรือใช้ Reset CMOS Switch จะมีผลทำให้ BIOS ถูก Reset กลับเป็นค่าเริ่มต้นใหม่ทันที ในข้อนี้ถือได้ว่าเป็นความรับผิดชอบของผู้ที่ได้รับมอบหมายให้ดูแลรักษาความลับของข้อมูลจราจรเครือข่ายคอมพิวเตอร์ตามกฎหมายด้วย

ควรหยุดการทำงานของ Network ก่อนขณะแก้ไขค่าต่างๆ

ควรอย่างยิ่งที่ผู้ดูแลระบบต้องพึงระวัง อย่าใช้ความเคยชินในการทำงานมาเป็นมาตรวัดความเสี่ยงของระบบ ในขณะที่คุณกำลังติดตั้งระบบปฏิบัติการให้ระบบเครือข่าย ไม่ควรต่อสายสัญญาณเข้าที่ NIC เพราะจะทำให้ระบบทั่วโลกหรือที่ต่อเชื่อมกับ Server คุณสามารถ Access เข้ามาในขณะที่คุณกำลังจะเริ่มจัดการระบบรักษา

ifdown eth0 กด Enter เมื่อต้องการสั่งให้ทำงานต่อก็สั่ง

ifup eth0 กด Enter หรือ

/etc/rc.d/init.d/network stop เมื่อต้องการสั่งให้ทำงานต่อก็สั่ง

/etc/rc.d/init.d/network start

เพียงเล็กน้อยแค่นี้คงไม่ทำให้คุณเสียเวลามากมาย ดีเสียกว่าต้องมานั่งปวดหัวเพราะผู้ไม่ประสงค์ดีได้บุกเข้ามาฝากข้อมูลเพื่อเปิดประตูหลังบ้าน (Back Door) ได้เรียบร้อยตั้งแต่เริ่มติดตั้ง คราวนี้ต่อให้คุณปิดประตูลงกลอนกี่ชั้น มีคนร้ายแอบอยู่ในบ้าน เขาก็สามารถเข้าออกได้อย่างสบาย จริงไหมครับ

การเลือกปิดหรือเปิด Service ที่จำเป็น

หลังติดตั้งเสร็จเรียบร้อยอาจมี Service บางตัวที่ไม่ได้ใช้งาน ถ้าปล่อยไว้นอกจากจะสิ้นเปลืองทรัพยากรในการทำงานแล้ว ยังอาจมีการเปิด Port ที่ไม่ปลอดภัยเพราะไม่ได้มีการป้องกันใด ๆ ทำให้ผู้ไม่หวังดีแอบเจาะเข้าระบบได้ง่าย ให้ลองดูตัวอย่าง service ต่าง ๆ ดังนี้

ตรวจสอบดูว่ามี Service อะไรบ้างที่กำลังทำงานอยู่ (ใน mode 3)

 # chkconfig --list | awk '/3:on/ { print $1}'

anacron

auditd

cpuspeed

crond

firstboot

haldaemon

iptables

irqbalance

mdmonitor

messagebus

microcode_ctl

network

ntpd

portsentry

restorecond

sendmail

sshd

syslog-ng

udev-post

ให้ทำการลบ service ที่นอกเหนือจากตัวอย่างข้างบนโดยใช้คำสั่ง

 # /etc/init.d/<ชื่อ service> stop

 # chkconfig <ชื่อ service> off

และอย่าเผลอไปลบ service ที่สำคัญที่ระบบต้องใช้เช่น

crond, anacron, haldaemon, messagebus, network, restorecond, syslog-ng

และทุก service ที่ใช้งานต้องสั่งให้ทำงานใน Mode 3 เท่านั้นอีกด้วย

การกำหนดรหัสผ่าน (Password) อย่างปลอดภัย

ผู้ดูแลระบบที่ดีต้องพยายามไปหา Download โปรแกรมที่ Hacker ใช้ในการโจมตี Server และที่ขาดไม่ได้คือต้องไปหาโปรแกรมที่ใช้ในการ Crack Password มาทำการ Crack password ดูสัปดาห์ละครั้ง หากพบว่า password ของใครมีความง่ายต่อการเดาหรือมีอายุการใช้งานเกินครึ่งของเวลาที่กำหนดให้ทำการเปลี่ยนรหัสผ่านให้คนนั้นใหม่ทันที ควรเลือกเครื่องมือหรือโปรแกรมที่มีความสามารถตั้งค่าในการตรวจเช็คว่า password ใครเก่าหรือง่าย ตรงตามคำในพจนานุกรม จะเปลี่ยน password ให้ใหม่แต่ต้องไม่ลืมว่าเครื่องมือนั้นต้องยอมรับการผสมตัวเลขและอักษรสัญลักษณ์พิเศษปนอยู่ในจำนวนแปดตัวหรือแปดหลักนั้นได้ด้วย

วางแผนในการออกรหัสผ่านที่ดี

1. ควรมีความยาวรหัสผ่าน (Password Length) ไม่น้อยกว่า 6 ตัว ถ้าจะให้ดีควรให้มีความยาว 8 ตัวอักขระโดยให้มีตัวอักษร ตัวเลขหรือสัญลักษณ์พิเศษรวมอยู่ด้วยอย่างน้อยหนึ่งตัว ปัจจุบัน PAM กำหนดค่าหลักให้ไม่น้อยกว่า 8 ตัว
2. ไม่ควรกำหนดให้มีความง่ายต่อการเดาและเป็นคำที่มีใช้กันปกติ เช่น ชื่อบุคคล ครอบครัว อาชีพการงาน ทะเบียนรถ หมายเลขโทรศัพท์ หรือบุคลิกลักษณะของคนพิเศษ
3. ควรมีการกำหนดอายุของรหัสผ่านให้มีการเปลี่ยนรหัสผ่านใหม่ตามกำหนดเวลาที่ตั้งไว้
4. ควรมีการ Lock รหัสไม่ให้ใช้งาน และถ้ามีการป้อนรหัสผิดครบตามจำนวนครั้งที่ตั้งไว้

วิธีการกำหนดความยาวของรหัสผ่าน (Password Length)

ใน Version เก่า ๆ ที่การจัดการเรื่องรหัสผ่านยังไม่แข็งแรงเช่นไฟล์ที่ใช้เก็บ password มีการเก็บทั้ง User name และ password ไว้ด้วยกันต่อมาก็มีการพัฒนาให้แยกไฟล์ password ไปไว้ที่ shadow เพื่อให้ปลอดภัยมากขึ้น ในอดีตผู้ดูแลระบบสามารถกำหนดค่าตัวแปรสำหรับลูกข่ายที่จะ login เข้าระบบได้โดยการไปแก้ไข

/etc/login.defs	PASS_MAX_DAYS	60	Maximum number of days a password is valid.
/etc/login.defs	PASS_MIN_DAYS	7	Minimum number of days before a user can change the password since the last change.
/etc/login.defs	PASS_MIN_LEN	n/a	This parameter does not work. It is superseded by the PAM module "pam_cracklib"
/etc/login.defs	PASS_WARN_AGE	7	Number of days when the password change reminder starts.
/etc/default/useradd	INACTIVE	14	Number of days after password expiration that account is disabled.
/etc/default/useradd	EXPIRE		Account expiration date in the format YYYY-MM-DD.

ปัจจุบันการดูแลระบบความปลอดภัยในการเข้ารหัสให้กับไฟล์ shadow ต้องทำงานผ่าน PAM (Pluggable Authentication Module) ดังนั้นผู้ที่ต้องการจะปรับเปลี่ยนค่าตัวแปรให้กับเรื่องรหัสผ่านของลูกข่าย ให้เปลี่ยนไปทำที่ไฟล์ /etc/pam.d/system_auth ซึ่งค่าตัวแปรที่จะใช้งานได้จะเป็น module ที่ชื่อว่า pam_cracklib ดูคำอธิบายค่าตัวแปรที่จะใช้งานดังนี้

pam_cracklib.so	minlen=8	Minimum length of password is 8
pam_cracklib.so	lcredit=-1	Minimum number of lower case letters is 1

pam_cracklib.so	ucredit=-1	Minimum number of upper case letters is 1
pam_cracklib.so	dcredit=-1	Minimum number of digits is 1
pam_cracklib.so	ocredit=-1	Minimum number of other characters is 1

จากค่าต่างๆ ตามตารางให้นำไปเพิ่มเติมลงในไฟล์ system_auth เพื่อให้การทำงานเป็นไปตามที่ต้องการได้โดยไปแก้ไขตามตัวอย่างนี้

 # vi /etc/pam.d/system_auth

#%PAM-1.0

This file is auto-generated.

User changes will be destroyed the next time authconfig is run.

auth required pam_env.so

auth sufficient pam_unix.so nullok try_first_pass

auth requisite pam_succeed_if.so uid >= 500 quiet

auth required pam_deny.so

account required pam_unix.so

account sufficient pam_localuser.so

account sufficient pam_succeed_if.so uid < 500 quiet

account required pam_permit.so

password requisite pam_cracklib.so try_first_pass retry=3 <- พิมพ์ต่อตรงบรรทัดนี้

minlen=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1

ตามตัวอย่างจะส่งผลให้การเปลี่ยน password ของลูกข่ายด้วยคำสั่ง passwd ถูกบังคับให้มีค่าตามที่อธิบายไว้ในตารางข้างบน แต่จะไม่มีผลกับการ login ด้วย root นอกจากนี้ควรมีการห้ามใช้ password ซ้ำกับค่าเดิมที่เคยใช้ไปแล้วต่อไปนี้ให้ดูเทียบกับค่า PASS_MIN_DAYS = 7 ในไฟล์ /etc/login.defs เป็นการกำหนดจำนวนวันต่ำสุดที่ต้องทำการเปลี่ยน password = 7 วัน ถ้าต้องการให้เครื่องจำ password เดิมไว้ 26 ครั้งก็ให้กำหนดค่า remember=26 และสามารถกำหนดให้การเปลี่ยน password ใหม่ต้องมีอักขระต่างกันกับใน password เดิมจำนวน 3 ตัวให้เพิ่ม difok=3 เพิ่มทั้งสองค่านี้ลงไปในไฟล์เดิมดังนี้

 # vi /etc/pam.d/system_auth

…….

password requisite pam_cracklib.so try_first_pass retry=3

minlen=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1 **difok=3** <- พิมพ์เพิ่ม

password sufficient pam_unix.so nullok use_authtok md5 shadow **remember=26**

จากนั้นให้ตรวจดูว่ามีไฟล์ /etc/security/opasswd อยู่หรือไม่เป็นไฟล์ที่ใช้เก็บค่า password เก่าถ้าไม่มีต้องสร้างขึ้นใหม่ด้วยคำสั่ง touch แล้วกำหนด permission = 600

ls -l /etc/security/opasswd

-rw------- 1 root root 0 Dec 8 06:54 /etc/security/opasswd

ความปลอดภัยเกี่ยวกับ root account

Root เป็น account ที่มีสิทธิสูงสุดของ OS ตระกูล UNIX ดังนั้นมันจึงไม่มีความปลอดภัยในทุก ๆ ด้าน ถ้าคุณ log in ด้วย root ทิ้งไว้ คุณอาจเสียใจเพราะผู้ไม่ประสงค์ดีจะทำการใด ๆ ด้วยสิทธิสูงสุดโดยไม่มีคำเตือนจากระบบเลย ไม่ว่าจะเป็นการสั่งปิดเปิดบริการใด ๆ หรือการลบข้อมูล ลบไฟล์หรือไดเรกทอรี ระบบจะยินยอมให้ทำการได้ทุกอย่าง หากคุณไม่ได้อยู่หน้าเครื่องคงต้องขอบอกด้วยความห่วงใยว่าอย่า log in ทิ้งไว้เด็ดขาดนะครับ ฝรั่งเขาเตือนว่ามันเป็นสิ่งที่แย่มาก ๆ ๆ ๆ สำหรับการกระทำเช่นนั้นเลยทีเดียว

กำหนดเวลาให้ root login

ผู้ดูแลระบบต้องทำการแก้ไขค่า login timeout ให้กับ root กรณีที่ผู้ดูแลระบบบางคนนั่งทำงานหน้าเครื่องมัก login ด้วย root ควรตั้งเวลากรณีไม่มีการทำงานให้ login ทิ้งไว้ได้เป็นเวลาเท่าไร ให้เครื่อง logout กลับออกไปเองเพื่อความปลอดภัยให้ไปแก้ไขไฟล์ **profile** ดังนี้

 # vi /etc/profile

….

HISTSIZE=1000

TMOUT = 3600

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE **TMOUT** INPUTRC

**** การแก้ไขไฟล์นี้จะมีผลก็ต่อเมื่อได้ทำการ logout แล้ว login ด้วย root กลับเข้ามาใหม่ ****

ค่า 3600 วินาที หมายความว่าให้ login ด้วย root account ทิ้งไว้โดยไม่มีการทำงานใด ๆได้นาน 1 ชั่วโมง (60 x 60 = 3600 วินาที) หากไม่มีการทำงานใด ๆ linux จะ logout ตัวเองทันที ถ้าต้องการให้เร็วหรือช้ากว่านี้ก็เปลี่ยนเลขได้ตามต้องการ หลังจากเปลี่ยนค่าเสร็จให้ logout เมื่อทำการ login ด้วย root ใหม่จะรับค่า profile ใหม่มาทำงานทันที

ป้องกัน Boot loader (GRUB)

ปัจจุบัน Boot loader ของ Linux นิยมใช้ GRUB (GRand Unified Bootloader) แทน LILO (Linux Loader) ซึ่งมีรูปแบบการใช้งานในลักษณะที่เป็นเมนูให้เลือกแก้ไขเปลี่ยนแปลงค่าในการ boot ได้ด้วยการกดแป้นพิมพ์เช่นต้องการแก้ไขกด e ต้องการ boot กดแป้น b เป็นต้นอย่างนี้ถือว่าสะดวกสำหรับผู้ใช้งานเป็นอย่างมาก ถ้าต้องการ boot แบบ single mode ก็ทำได้ง่ายเพียงเข้าเมนูแล้วเลื่อนแถบไปยังบรรทัดที่มีคำว่า kernel แล้วกดแป้น e พิมพ์คำว่า single ต่อท้าย

kernel /vmlinuz-2.6.25.9-40.fc8 ro root=LABEL=/ **single**

เสร็จแล้วกด enter แล้วกดแป้น b เพื่อทำการ boot เพียงง่าย ๆ แบบนี้ก็จะเข้าทำงานแบบ single user เพื่อเข้าไปแก้ไข root password (ใช้กรณีลืม root password) ก็เลยเป็นช่องทางในการเข้าระบบที่หน้าเครื่องโดยผู้ไม่หวังดีได้ จึงต้องทำการป้องกันไม่ให้ผู้อื่นสามารถเข้าเมนูของ GRUB ได้หากต้องการเข้าไปแก้ไขเปลี่ยนแปลงค่าใด ๆ ต้องมีการกรอกรหัสผ่าน (password) เสียก่อน มีขั้นตอนดังต่อไปนี้

 # grub-md5-crypt

Password: <พิมพ์รหัสผ่านที่ต้องการ>

$1$0WXVJ$siSTEUxO.X7qx56RIwggD1 <- รหัสผ่านถูกเข้ารหัสแล้ว

หลังจากใช้คำสั่ง grub-md5-crypt เสร็จแล้วจะมีการเข้ารหัสให้กับรหัสผ่านที่เราพิมพ์ลงไป เป็นรูปแบบ MD5 ที่ไม่สามารถเดาได้ว่าค่ารหัสผ่านที่แท้จริงคือคำว่าอะไร เมื่อทำขั้นตอนเข้ารหัสเสร็จดังตัวอย่างแล้วจะส่งผลให้ค่าดังกล่าวไปแทนที่ในไฟล์ grub.conf ดังนี้

 # vi /boot/grub/grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol00
#          initrd /initrd-version.img
```

```
#boot=/dev/sda
password --md5 $1$0WXVJ$siSTEUxO.X7qx56RIwggD1
default=0
timeout=5 <- แก้ให้เป็น 0 ถ้าไม่รอเวลาให้เข้าเมนูหรือให้ boot ทันที
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Log Server 2.0 (2.6.25.9-40.fc8)
        root (hd0,0)
        kernel /vmlinuz-2.6.25.9-40.fc8 ro root=/dev/VolGroup00/LogVol00
        initrd /initrd-2.6.25.9-40.fc8.img
```

เสร็จแล้วให้ทดลองสั่ง reboot แล้วเข้าเมนูเพื่อแก้ไขข้อมูลในการ boot ดูว่ามีการถามรหัสผ่านหรือไม่ สังเกตดูว่าถ้าอยู่ในเมนูหลัก รายการข้อความที่มีให้เลือกด้านล่างจะมีเพียงอนุญาตให้กดแป้น p เพื่อกรอกรหัสผ่านเท่านั้นจะไม่มีตัว e หรือตัวอักษรอื่นให้เลือกเหมือนเดิม หลังกดแป้น p จะมีการให้กรอกรหัสผ่าน ให้กรอกให้ตรงกับตอนที่สร้างด้วย grub-md5-crypt ถ้าเข้าเมนูหลักได้แสดงว่าได้ทำการป้องกันในส่วนของ GRUB เสร็จเรียบร้อย

ยกเลิกการกดแป้น Ctrl+Alt+Del เพื่อ reboot

บางครั้งคนใช้งานคอมพิวเตอร์อาจสงสัยว่าวิธีนี้จะเอามาแนะนำกันทำไม มันก็ดีอยู่แล้วว่าสามารถที่จะ Reboot เครื่องแบบ cold start ทำให้เครื่องพังช้าลงตามทฤษฎี แต่สำหรับผู้ดูแลระบบที่ใช้ Server จริง ๆ ราคาแพง ๆ คงจะรู้นะครับว่าหน้าเครื่อง Server จะไม่มีปุ่ม Reset มีแต่ปุ่มกด Power เท่านั้นยกเว้นผู้ที่เอาเครื่อง PC มาทำ Server มีปุ่มกดหน้าเครื่องเพียบ ถ้าคุณทำ Internet Server คงต้องเปิดบริการ 24 ชั่วโมง แม้แต่จอภาพยังไม่ต้องการ ในระบบที่ต้องแข็งแรงคงมีแต่ UPS และ Server เท่านั้น ตัวอย่างนี้จึงต้องการให้คุณเห็นว่า หากมีใครสักคนเข้ามาเยี่ยมเยียนห้อง server อาจเป็นนักเล่นคอมพิวเตอร์ตัวยง พอเห็นเครื่องคอมพิวเตอร์ทีไรก็จะเข้าไปนั่งหน้าจอ พิมพ์โน่นบ้างขยับเมาส์บ้างเพื่อให้คนที่มาด้วยเห็นว่าเขาคนนั้นใช้คอมพิวเตอร์เป็นทำนองนั้น พอเปิดจอ ขยับเมาส์ มันไม่มีอะไรเกิดขึ้นก็เล่นบทใบ้ว่าเครื่องคง Hang มองหาปุ่ม Reset ไม่พบก็จะกดสามนิ้วพิฆาต Ctrl+Alt+Del ตามเคยเพื่อให้เครื่อง Reboot จะได้เห็นหน้าตาที่คุ้นเคย คิดออกหรือยังครับอาการนี้แหละน่าเป็นห่วงมากเครื่อง Server ของคุณจะหยุดบริการและ Reboot ใหม่ทันที ขอแนะนำให้ปลดหรือยกเลิกการใช้ Key อันตรายนี้ด้วยการแก้ไขไฟล์ **inittab** ดังนี้

```
# vi /etc/inittab
```

ค้นหาบรรทัดที่มีข้อความ ตามตัวอย่างข้างล่าง

ca::ctrlaltdel:/sbin/shutdown -t3 -r now

ให้ยกเลิกด้วยการแทรกเครื่องหมาย # ข้างหน้าบรรทัด

 # ca::ctrlaltdel:/sbin/shutdown -t3 -r now

บันทึกไฟล์แล้วสั่ง

 # /sbin/init q

<u>จำกัดจำนวน terminal ที่ใช้งานบน Server</u>

หลังจากติดตั้ง Log Server เสร็จโปรแกรมจะยอมให้ใช้ virtual console (ttys) บน keyboard ได้รวมทั้งหมด 6 ttys ซึ่งเป็นจำนวนที่มากเกินไป ส่วนมากผู้ดูแลระบบมีความจำเป็นต้องใช้เพียง 2 ttys เท่านั้นคือเมื่อ tty1 มีปัญหาก็จะ login ผ่านทาง tty2 เพื่อจัดการปัญหา ตัวอย่างนี้ใช้เฉพาะผู้ดูแลระบบที่นั่งหน้าเครื่องเท่านั้น ถ้าต้องการให้ปลอดภัยที่สุดควรให้ทำงานได้เพียง tty เดียวเท่านั้น โดยให้ไปแก้ไขค่าจำนวน ttys ได้ที่ไฟล์ /etc/inittab ดังนี้

 # vi /etc/inittab

….. ไม่ใช้ ttys ไหนให้ปิดด้วยเครื่องหมาย # หน้าบรรทัด

Run gettys in standard runlevels

1:2345:respawn:/sbin/mingetty tty1

2:2345:respawn:/sbin/mingetty tty2

 # 3:2345:respawn:/sbin/mingetty tty3

 # 4:2345:respawn:/sbin/mingetty tty4

 # 5:2345:respawn:/sbin/mingetty tty5

 # 6:2345:respawn:/sbin/mingetty tty6

บันทึกไฟล์แล้วสั่ง

 # /sbin/init q

สิ่งที่ต้องทำคู่กันในการควบคุมการ login เข้าใช้งานทาง virtual console (vc or ttys)มีการควบคุมอีกไฟล์หนึ่งซึ่งจะถูกเรียกใช้เมื่อมีการใช้งานคำสั่ง login นั่นก็คือไฟล์ /etc/securetty ให้ไปแก้ไขดังนี้

 # vi /etc/securetty

 # console

vc/1

 # vc/2

 # vc/3

 # vc/4

 # vc/5

 # vc/6

 # vc/7

 # vc/8

 # vc/9

 # vc/10

 # vc/11

tty1

 # tty2

 # tty3

 # tty4

 # tty5

 # tty6

 # tty7

 # tty8

 # tty9

<u>ป้องกัน user เรียกใช้โปรแกรมบางอย่างผ่าน Console</u>

หากมีการสั่งให้โปรแกรมทำงานผ่าน Console ได้ก็จะเป็นช่องทางที่ Hacker หรือ user ทั่วไปสามารถเข้ามาสั่งคำสั่งต่าง ๆ ที่สำคัญของระบบเช่น poweroff, reboot และ halt จะทำให้เกิดความเสียหายเนื่องจากเครื่อง Server กำลังให้บริการลูกข่ายอยู่แต่กลับมีลูกข่ายบางคน login เข้ามาใช้งานแล้วเผลอไปสั่ง reboot หรือ poweroff เครื่องจะปิดตัวเองโดยไม่รู้สาเหตุ Linux OS บางค่ายได้ป้องกันจุดนี้ไว้แล้วบางค่ายยังปล่อยไว้ให้ดำเนินการป้องกันทั้งสองแห่งคือลบไฟล์และเขียน script เพื่อยกเลิกการสั่งงานผ่าน console ที่มีการ Authenticate ผ่านโปรแกรม PAM ทั้งหมดด้วย ทำดังนี้

rm -f /etc/security/console.apps/halt

rm -f /etc/security/console.apps/poweroff

rm -f /etc/security/console.apps/reboot

<u>ยกเลิกการเข้าถึงระบบผ่าน Console ทั้งหมดใน pam.d</u>

หลังจากติดตั้ง Linux ทำ Internet Server เรียบร้อยแล้ว linux จะติดตั้ง Linux-PAM library เพื่อรอรับการ authenticate user, password ของ user เพื่อให้เข้าถึง Server เพื่อดูแลระบบ จัดการบริหารผู้ใช้ เข้าถึงโปรแกรมและระดับไฟล์ ผ่านทาง console ซึ่งพบว่าเกิดความไม่ปลอดภัยกับระบบเป็นอย่างมาก จึงควรยกเลิก

สร้าง script ไว้ที่ /root ดังนี้

 # vi disable

 # !/bin/sh

cd /etc/pam.d

for i in * ; do

sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i

done

หลังจากบันทึกแล้วให้ทำการ

chmod 700 disable

สั่งให้ script ทำงานโดย

./disable

ต้องการรู้ว่า script ทำงานได้สำเร็จหรือไม่ ให้ใช้คำสั่ง

 # grep pam_console.so /etc/pam.d/*

ปลอดภัยด้วย TCP Wrappers

Linux OS ทุกค่ายได้ติดตั้งโปรแกรม tcp wrappers มาด้วย เพื่อใช้เป็นระบบความปลอดภัยเบื้องต้น โดยมีไฟล์ที่สำคัญในการกำหนดค่าที่จะให้เข้ามาใช้ Host ได้หรือไม่อยู่ 2 ไฟล์ คือ hosts.deny และ hosts.allow โดยมีหลักการทำงานดังนี้

- อนุญาตให้ daemon, client ที่ตรงกับค่าที่กำหนดใน hosts.allow เข้า Server ได้
- ไม่อนุญาตให้ daemon, client ที่ตรงกับค่าที่กำหนดใน hosts.deny เข้า Server
- ที่เหลือนอกนั้นจะถูกอนุญาตทั้งหมด

วิธีกำหนดค่าทำดังนี้

 # vi /etc/hosts.deny

ALL: ALL

ในส่วนการอนุญาตให้ผู้อื่นสามารถเข้าถึง Server ได้นั้นให้ไปกำหนดค่าไว้ในไฟล์ hosts.allow ดังตัวอย่างต่อไปนี้

 # vi /etc/hosts.allow

#

 # hosts.allow This file describes the names of the hosts which are

 # allowed to use the local INET services, as decided

 # by the '/usr/sbin/tcpd' server.

#

syslog-ng: 192.168.

sshd: 203. 192.168. : spawn (echo -e "Login from %c to %s" | /bin/mail -s "Login Info for %s" root) &

ในตัวอย่างข้างบน sshd เป็นการอนุญาตให้ client ที่มี ip address 203.xxx.xxx.xxx 192.168.xxx.xxx สามารถเข้าใช้บริการ sshd ได้ และให้ mail ไปแจ้ง root ด้วยว่าเข้ามาจาก %c (client) ถึง %s (server) สามารถตรวจสอบการเข้าใช้บริการได้จาก mail ของ root หรืออีกตัวอย่างทั้งเก็บที่ log file และส่ง mail แจ้งไปที่ root ด้วย (%p = process id)

sshd: 192.168.1. : spawn (echo -e "Illegal connection attempt from %c to %s %d %p at `date`" >> /var/log/unauthorized.log | /bin/mail -s "SSH Info from %c to %s %d %p `date`" root) &

<u>จัดการเรื่องการตรวจสอบค่าใน host</u>

หลังติดตั้ง Internet Server เสร็จ ผู้ดูแลระบบต้องเลือกวิธีการที่จะตรวจสอบหาค่า ip address .ให้กับการใช้งานภายใน host โดยไปกำหนดที่ไฟล์ /etc/host.conf ว่าจะให้ตรวจชื่อ host ว่ามีหมายเลข ip address อะไรถ้าตรวจแล้วไม่ทราบค่า ก็ให้ไปถาม dns แต่ถ้าต้องการให้ระบบไปถาม dns ก่อนก็ให้สลับที่กันระหว่าง hosts กับ bind ซึ่งถ้ากำหนดไม่ดีจะทำให้ระบบได้หมายเลข ip address ช้าการให้บริการอื่น ๆ จะช้าตามไปด้วย ดังตัวอย่าง

 # vi /etc/host.conf

order hosts, bind

nospoofon

(สั่ง nospoof on : ห้ามไม่ให้ ip address แปลกปลอมอื่น ๆ เข้ามาใช้ host)

<u>ป้องกันการแก้ไขค่ามาตรฐาน</u>

ค่ามาตรฐานของชื่อบริการ (Service Name) หมายเลข port และ protocol ตามมาตรฐาน RFC 1700 ในเรื่องการ Assigned Number ให้กับบริการต่าง ๆ บน Server เพื่อให้ client ที่ร้องขอบริการต่าง ๆ ตามชื่อบริการจะได้รับหมายเลข port และ protocol ที่ถูกต้อง ถูกเก็บอยู่ในไฟล์ /etc/services คุณควรป้องกันไม่ให้ผู้บุกรุกเข้ามาเปลี่ยนค่าในไฟล์นี้เพื่อการบุกรุก หรือประสงค์ร้ายกับระบบด้วยการ

 # chattr +i /etc/services

ควรลบ account ที่ไม่ได้ใช้งาน

ในการติดตั้ง Linux ทำ Internet Server นั้น เป็นระบบที่พยายามที่จะให้ผู้ใช้สามารถทำการติดตั้งใช้งานได้ง่ายกว่าการติดตั้งในระบบ UNIX จึงเป็นสาเหตุใหญ่ที่ทำให้บางเรื่องเกิดอาการที่เรียกว่าเกินความจำเป็น หมายความว่า บางอย่างไม่ได้ใช้ก็ติดลงไปให้ด้วย ทำให้เป็นช่องทางหรือเปิดทางให้ผู้ไม่ประสงค์ดีบุกโจมตีระบบได้ง่าย โดยที่ผู้ดูแลไม่ทันระวังตัวเนื่องมาจากไม่เข้าใจ OS ว่าเขาทำอะไรมาให้บ้าง ในหัวข้อนี้จะแนะนำการกำจัด special user account ที่เกินความจำเป็นให้หมดเพื่อลดปัญหามือที่สามแอบเอาไปใช้เพื่อ login เข้าระบบโดยมีสิทธิสูงกว่า user ธรรมดาเสียอีก ให้คุณจัดการลบทั้ง user และ group ที่ไม่จำเป็นต้องใช้งานด้วยคำสั่ง

 # userdel username

 # groupdel groupname

ให้ลบตามนี้ได้เลยเพราะไม่ได้ใช้ประโยชน์หรือจะเลือกลบเฉพาะกลุ่ม ที่เหลือยังคงเอาไว้บ้างก็ตามสะดวก

userdel adm

userdel lp

userdel shutdown

userdel halt

userdel news

userdel operator

 # userdel mailnull

 # userdel games

userdel gopher

userdel ftp

 # userdel vcsa

การใช้คำสั่ง userdel จะไม่ลบ home directory ให้กับระบบ ถ้าต้องการลบ home directory ให้ใช้ parameter **-r** ร่วมด้วย เป็น **userdel -r username** หลังจากนั้นให้ลบ group ดังนี้

groupdel adm

groupdel lp

groupdel news

groupdel games

groupdel dip

groupdel pppusers

groupdel popusers

groupdel slipusers

หากเป็น Version อื่นให้ลองตรวจสอบดูว่ามี User หรือ Group ใดไม่ใช้งานตรงตามตัวอย่างก็ให้ลบทิ้งได้เลย หลังจากนั้นควรสร้าง user account ที่ทำหน้าที่แทน root เพื่อใช้ login เข้าระบบแทนการใช้ root login จะทำให้ปลอดภัยมากขึ้น (ปกติก็คือ user คนแรกตอนติดตั้ง) ให้ทำดังนี้

 # useradd admin

 # passwd admin

<u>ควรป้องกันการใช้ su เป็น root</u>

เมื่อ linux ไม่อนุญาตให้ root ทำการ login เข้าระบบด้วย tty อื่น ๆ รวมถึงไม่สามารถ remote login จากภายนอกได้ด้วย ผู้บุกรุกมักจะ login ด้วย user อื่น ๆ แล้วทำการเปลี่ยนสิทธิด้วยการใช้ su เป็น root เข้าปฏิบัติการโจมตี คุณควรป้องกันการใช้ su เป็น root ก่อนที่จะสายเกินแก้ ทำได้ดังนี้

 # vi /etc/pam.d/su

#%PAM-1.0

auth sufficient pam_rootok.so

Uncomment the following line to implicitly trust users in the "wheel" group.

#auth sufficient pam_wheel.so trust use_uid

Uncomment the following line to require a user to be in the "wheel" group.

```
auth        required      pam_wheel.so use_uid
auth        include       system-auth
account     sufficient    pam_succeed_if.so uid = 0 use_uid quiet
account     include       system-auth
password    include       system-auth
session     include       system-auth
session     optional      pam_xauth.so
```

หากต้องการให้สมาชิกใน group wheel สามารถ su เป็น root โดยไม่ต้องใส่ password (กรณีนี้ไม่แนะนำให้ทำ) ให้ลบเครื่องหมาย # หน้าบรรทัด

```
auth      sufficient      pam_wheel.so trust use_uid
```

ต่อไปให้สร้าง admin user เข้าไปใน wheel group เพื่อให้สามารถใช้คำสั่ง su ได้

```
# usermod  -G10  admin
```

ทำแบบนี้แล้ว user คนอื่น ๆ ไม่สามารถ login เข้าระบบแล้วใช้คำสั่ง su เป็น root ได้ ยกเว้นคุณเข้าระบบด้วย admin ทำไว้ให้ผู้ดูแลระบบใช้นะครับ ไม่ใช่เอาไว้ให้ Hacker ใช้ ควรกำหนด password ยาก ๆ หน่อย ถ้าคุณอยากให้ผู้บุกรุกไม่สามารถเข้ามาแก้ไข user account ได้ควรจัดการกับไฟล์ต่อไปนี้

```
# chattr +i /etc/passwd
# chattr +i /etc/shadow
# chattr +i /etc/group
# chattr +i /etc/gshadow
```

จากวิธีการที่แนะนำมาทั้งหมด user account บางคนเกิดขึ้นจากการติดตั้ง package เช่น squid เวลาติดตั้งจะสร้าง user, group ชื่อ squid เข้ามาดังนั้นคุณจะเปลี่ยน attribute +i ก็ควรทำหลังจากติดตั้ง package ทุกอย่างที่ต้องการแล้วครับไม่เช่นนั้นมัน**จะ add user ไม่ได้** ถ้าจำเป็นต้องทำการติดตั้ง packet ใหม่หรือต้องการเพิ่ม แก้ไข User account ต้องสั่งยกเลิกการป้องกันด้วย -i ก่อนดังนี้

```
# chattr -i /etc/passwd
# chattr -i /etc/shadow
# chattr -i /etc/group
# chattr -i /etc/gshadow
```

เสร็จภารกิจเมื่อไรก็จัดการ +i เหมือนเดิม

ควรจำกัดการเข้าใช้ทรัพยากรของลูกข่าย

ในตัว OS linux ได้มีข้อจำกัดการใช้ทรัพยากร เพื่อความปลอดภัยของระบบด้วยการจำกัดการเข้าใช้ memory จำนวน process id หรืออื่น ๆ ที่ต้องการ คุณควรปรับปรุงระบบในส่วนนี้เพื่อป้องกันการบุกโจมตีที่เรียกกันว่า Denial of Service Attacks (DoS) การจำกัดค่าในครั้งนี้จะมีผลกับทุก ๆ User account ที่มีใน server เมื่อมีการ login เข้ามา ให้ทำดังนี้

 # vi /etc/security/limits.conf

* hard core 0

* hard rss 5000

* hard nproc 35

กำหนดค่า hard core 0 หมายถึงห้าม user เข้ามาสร้าง core file

กำหนดค่า hard rss 5000 หมายถึงอนุญาตให้ใช้ memory ได้ 5 MB

กำหนดค่า hard nproc 35 หมายถึงอนุญาตให้มี process id ได้ไม่เกิน 35

กำหนดค่า * หมายถึงทุก ๆ user ที่ login เข้า Server **ยกเว้น root**

ในการกำหนดค่าเป็น * มีปัญหากับ account ของ service ต่าง ๆ เช่น apache, mysql หรือ squid ที่มีในระบบทั้งหมดจะทำให้เปิดบริการได้ไม่สมบูรณ์เพราะบาง service ต้องการทรัพยากรมากกว่าที่กำหนดให้ จึงไม่แนะนำให้ใช้ * แต่เปลี่ยนเป็น group name (@users) แทน ดังนี้

@users hard core 0

@users hard rss 5000

@users hard nproc 35

ต้องไม่สับสนตรง users ต้องไปเอา**ชื่อ group** ที่ต้องการมาใส่ลงไปเช่น **@student**

ควรย้ายโปรแกรม RPM ไปไว้ที่ปลอดภัย

โปรแกรมใน RedHat หรือใน Linux ค่ายอื่น ๆ ที่ทำให้เราใช้งานง่ายคงไม่พ้นโปรแกรมที่ทำหน้าที่ Install, Erase หรือ Update package ต่าง ๆ ที่สะดวกและรวดเร็ว ดังนั้นผู้บุกรุกก็มีโอกาสนำความสะดวกนี้ทำการติดตั้งโปรแกรมต่าง ๆ ที่ส่งเข้ามาใน Server จึงควรอย่างยิ่งที่จะต้องเตรียมการป้องกันโดยให้ย้ายโปรแกรมที่ใช้ในการติดตั้ง รวมถึงโปรแกรมประเภท compress file ต่าง ๆ ทุกตัวด้วย เช่น

 # chmod 700 /bin/rpm

 # mount /dev/fd0

 # mv /bin/rpm /mnt/floppy

 # umount /dev/fd0

สิ่งที่เห็นเป็นการเปลี่ยน mode ให้ใช้โปรแกรม rpm ได้เฉพาะ root ไม่อนุญาตให้ user อื่น ๆ เข้ามาเรียกใช้ได้ และยังต้องย้ายที่อยู่ไปไว้ที่ /mnt/floppy ผู้บุกรุกจะไม่สามารถเรียกใช้ตามปกติได้ จากประสบการณ์ผู้เขียน พบว่า Hacker ที่ส่งไฟล์เข้ามาที่ Server มักเป็นไฟล์ประเภทที่มีนามสกุล .tar หรือ .gz มากกว่าที่จะเป็น

แก้ไขค่า Shell Logging

สำหรับผู้ที่ใช้ linux ใหม่ ๆ มักชอบมากที่จะใช้วิธีกดเรียกคำสั่งเดิมที่เคยเรียกใช้มาก่อนหน้า ด้วยการกดแป้นลูกศรขึ้น (Up arrow key) บางคนกดกันเพลินด้วยความชอบใจว่ามันจำไว้มากดี คุณรู้หรือไม่ว่า linux จำคำสั่งเดิมได้สูงถึง 1000 คำสั่งเลยเชียว แต่สิ่งที่ดูเหมือนดี อาจเป็นภัยอย่างหาตัวจับไม่ได้เลย เพราะหากคุณหรือ user ทำการใด ๆ ที่มีการส่งค่า password เข้าระบบ แล้วมีการผิดพลาดขึ้น มันก็จะจำและเก็บไว้ให้ด้วย คนที่ใช้เป็นเขาเข้ามาเปิดไฟล์ที่เก็บค่านี้ดูก็สามารถรู้ password ของคุณได้อย่างไม่ต้องเอาไปเดาให้ยาก สิ่งที่คุณชอบเก็บอยู่ที่ไฟล์ .bash_history บันทึกใน home directory ของทุก ๆ user ดังนั้นคุณควรกำหนดค่าให้จำเท่าที่จำเป็นก็พอหากเกินค่าที่กำหนด มันจะลบคำเก่าออก ทำได้ดังนี้

 # vi /etc/profile

ค้นหาคำว่า HISTSIZE แล้วเปลี่ยนค่าตามตัวหนา

HISTSIZE=**10**

HISTFILESIZE=**0**

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE **HISTFILESIZE** TMOUT INPUTRC

การแก้ไขไฟล์นี้จะมีผลก็ต่อเมื่อทำการ logout แล้ว login ด้วย root กลับเข้ามาใหม่

ควรกำหนด permission ให้กับ script file

ไฟล์ที่มีความสำคัญอย่างมากในการควบคุมการ start , stop, restart daemon ต่าง ๆ ที่มีไว้สำหรับให้ผู้ดูแลระบบเรียกใช้งานได้จะอยู่ที่ /etc/rc.d/init.d ควรเป็น script ที่ทำไว้ให้ root เรียกใช้ได้เท่านั้น ไม่ควรปล่อยให้ user ปกติเข้ามาเรียกใช้ได้ ให้สั่ง

 # chmod -R 700 /etc/rc.d/init.d/*

ควรปิดการแสดงข้อมูล OS

ในการ boot หรือขณะที่ login เข้าระบบมักจะมีคำอธิบายเรื่องของคุณสมบัติ OS เช่น เป็น Fedora Release 8.x หรือข้อมูลอื่น ๆ แล้วแต่ละ version จะกำหนด จะเป็นช่องทางให้ผู้ไม่ประสงค์ดีสามารถนำไปค้นหาทางบุกรุกเข้า Server ได้เป็นอย่างดี คุณควรทำการปิดการแสดงค่าเหล่านี้ โดย

 # rm -f /etc/issue

 # rm -f /etc/issue.net

ให้ลอง logout แล้วทำการ login เข้าระบบมาใหม่จะพบว่าหน้าจอมีแต่ข้อความ login ไม่มีการโฆษณาเกี่ยวกับ version ต่าง ๆ ให้เห็นอีก

ควรตั้งค่าให้ root เป็นเจ้าของโปรแกรมคำสั่งเท่านั้น

ในการติดตั้ง Linux ค่า permission ที่มีมาให้ในแต่ละโปรแกรม จะถูกกำหนดมาให้อย่างอัตโนมัติจากผู้เขียน Linux เพราะต้องการสร้างงานที่ง่ายและสำเร็จรูป หมายความว่าติดตั้งง่าย ใช้งานง่าย ติดแล้วใช้ได้ทุกบริการ จึงมีการกำหนดค่า permission ให้กับโปรแกรมสำคัญหรือโปรแกรมหลักบางอย่าง ให้ทุก user สามารถเรียกใช้งานได้อย่างสะดวก จึงเป็นช่องทาง หรือ Back door ให้กับผู้ไม่ประสงค์ดีบุกรุกเข้ามายัง server ได้ตลอดเวลา ค่า permission ดังกล่าวคือการตั้ง permission ให้มี bit เป็น +s ทั้ง user และ group เรียกว่า SUID และ SGID เรียกว่า root-owned program หมายถึงการตั้งค่า permission ของโปรแกรมที่ root มีไว้เรียกใช้ให้มีบาง bits มีค่าเป็น +s หรือกำหนดเป็นตัวเลขได้เป็น 04000 และ 02000 (SUID/SGID : -rwsr-xr-x, -r-xr-sr-x) คุณสามารถยกเลิกได้ด้วยการใช้คำสั่ง chmod a-s <program name> โปรแกรมต่าง ๆ ล้วนมีความสำคัญต่อการเรียกใช้งานของ root ดังนั้นคุณควรดูแล และกำหนดค่าการใช้งานอย่างระมัดระวัง ข้อจำกัดของโปรแกรมเหล่านี้ คือ

- คุณไม่เคยใช้งานโปรแกรมเหล่านี้เลย
- คุณไม่ต้องการให้ user ที่ไม่ใช่ root เรียกใช้งาน
- คุณอาจเรียกใช้บางครั้งแต่ไม่ต้องการให้ su เป็น root เข้ามาเรียกใช้งานวิธีการค้นหาและยกเลิกทำได้ดังนี้

ขั้นที่ 1 ค้นหา file ที่มี flag +s ด้วยคำสั่ง find ตามตัวอย่าง สำหรับบรรทัดที่มีตัวอักษรเข้ม หมายถึงไฟล์ที่มีความสำคัญ ควรเปิดปิด flag +s สำหรับให้ su ใช้งานด้วยความระมัดระวังอย่างมาก ถ้าไม่จำเป็นก็ควรยกเลิก เพราะเป็นโปรแกรมที่ใช้เปลี่ยนแปลงค่าต่าง ๆ ได้ทุกส่วนในระบบความปลอดภัย

find / -type f \(-perm -04000 -o -perm -02000 \) -exec ls -lg {} \;

-rwxr-sr-x 1 root root 5872 Nov 29 2006 /sbin/netreport

-rwsr-xr-x 1 root root 12280 May 30 2007 /sbin/pam_timestamp_check

-rwsr-xr-x 1 root root 18668 May 30 2007 /sbin/unix_chkpwd

-rwsr-xr-x 1 root root 38616 Aug 2 18:57 /bin/umount

-rwsr-sr-x 1 root root 24060 Apr 17 2007 /bin/su

-rwsr-xr-x 1 root root 41652 Apr 12 2007 /bin/ping

-rwsr-xr-x 1 root root 57652 Aug 2 18:57 /bin/mount

-rwsr-xr-x 1 root root 36680 Apr 12 2007 /bin/ping6

--wsr-x--- 1 root root 0 Nov 5 14:14 /media/.hal-mtab-lock

-rwsr-xr-x 1 root root 172200 Mar 31 2007 /usr/libexec/openssh/ssh-keysign

-rwx--s--x 1 root utmp 6944 Jul 28 2006 /usr/libexec/utempter/utempter

---s--x--x 2 root root 159096 Oct 2 2006 /usr/bin/sudo

-rwsr-xr-x 1 root root 24556 May 23 2007 /usr/bin/newgrp

-rwsr-xr-x 1 root root 9100 Dec 13 2006 /usr/bin/rsh

-rwsr-sr-x 1 root root 315384 Aug 6 14:16 /usr/bin/crontab

-rwx--s--x 1 root slocate 23856 Nov 26 2006 /usr/bin/locate

-rwsr-xr-x 1 root root 46748 May 23 2007 /usr/bin/chage

-rwsr-xr-x 1 root root 14388 Dec 13 2006 /usr/bin/rlogin

-rws--x--x 1 root root 19128 Aug 2 18:57 /usr/bin/chsh

-rwsr-xr-x 1 root root 22932 Jul 17 2006 /usr/bin/passwd

-rwxr-sr-x 1 root nobody 79388 Mar 31 2007 /usr/bin/ssh-agent

---s--x--x 2 root root 159096 Oct 2 2006 /usr/bin/sudoedit

-rwxr-sr-x 1 root mail 16020 Jul 13 2006 /usr/bin/lockfile

-r-xr-sr-x 1 root tty 10420 Sep 4 20:19 /usr/bin/wall

-rwsr-xr-x 1 root root 44040 Aug 23 2006 /usr/bin/at

-rws--x--x 1 root root 17900 Aug 2 18:57 /usr/bin/chfn

-rwsr-xr-x 1 root root 18736 Dec 13 2006 /usr/bin/rcp

-rwsr-xr-x 1 root root 47352 May 23 2007 /usr/bin/gpasswd

-rwxr-sr-x 1 root tty 10984 Aug 2 18:57 /usr/bin/write

-rwsr-xr-x 1 root root 7048 Nov 29 2006 /usr/sbin/usernetctl

-rwxr-sr-x 1 root lock 16572 Jul 20 2006 /usr/sbin/lockdev

-rwsr-xr-x 1 root root 312956 Jul 25 2006 /usr/sbin/pppd

-r-s--x--- 1 root apache 11740 Jul 14 22:28 /usr/sbin/suexec

-rwxr-sr-x 1 root smmsp 827324 Sep 17 22:59 /usr/sbin/sendmail.sendmail

-rws--x--x 1 root root 34796 Oct 3 2006 /usr/sbin/userhelper

-rwsr-xr-x 1 root root 6416 Aug 22 2006 /usr/sbin/ccreds_validate

-rwsr-xr-x 1 root root 144548 Sep 5 01:20 /usr/kerberos/bin/ksu

-rwsr-x--- 1 root squid 15452 Jul 14 22:31 /usr/lib/squid/pam_auth

-rwsr-x--- 1 root squid 17360 Jul 14 22:31 /usr/lib/squid/ncsa_auth

ขั้นที่ 2 ยกเลิกด้วย chmod

chmod a-s /usr/bin/chage

chmod a-s /usr/bin/gpasswd

chmod a-s /usr/bin/wall

chmod a-s /usr/bin/chfn

chmod a-s /usr/bin/chsh

chmod a-s /usr/bin/newgrp

chmod a-s /usr/bin/write

chmod a-s /usr/sbin/usernetctl

 # chmod a-s /bin/ping6

chmod a-s /bin/mount

chmod a-s /bin/umount

chmod a-s /bin/ping

chmod a-s /sbin/netreport

ปรับแต่งค่า kernel parameter ให้ปลอดภัย

ในการติดตั้งใช้งาน Log Server จาก Linux ทุกค่ายและทุก version ผู้ดูแลระบบสามารถที่จะส่งค่า parameter ต่าง ๆ ให้กับ kernel เพื่อให้เกิดความปลอดภัยในการใช้งานมากขึ้นได้โดยการส่งค่าบางอย่างเกี่ยวกับ network หรือค่าที่เกี่ยวข้องกับการจัดสรรทรัพยากรในขณะที่ OS กำลังทำงานให้บริการลูกข่ายสามารถทำได้ 2 ทาง คือสามารถส่งค่าด้วย echo เข้าไปในไฟล์ต่าง ๆ ที่อยู่ใน /proc/sys กำหนดให้ network ทำงานตามที่คุณต้องการได้ หรือถ้าต้องการให้ทำงานทุกครั้งที่เครื่อง reboot ผู้ที่ linux มักนำคำสั่งต่าง ๆ ไปฝากไว้ที่ไฟล์ /etc/rc.local วิธีที่สองที่ผู้เขียนแนะนำคือการส่งค่าอย่างถาวรให้ kernel เมื่อเครื่องมีการ reboot จะรับค่าที่คุณตั้งเข้าควบคุมระบบการทำงานตามต้องการทันทีโดยที่คุณสามารถเข้าไปเพิ่มค่าหรือแก้ไขค่า parameter ต่าง ๆ ได้ที่ไฟล์ /etc/sysctl.conf ในที่นี้จะขอแยกอธิบายและใส่ค่าเป็นเรื่อง ๆ ว่าคุณต้องการจะควบคุมอะไรบ้างเพื่อความปลอดภัยของ Server (สิ่งที่ควรรู้คือการส่งค่า Parameter ให้กับ kernel ที่ boot ไปแล้วจะมีผลทำให้ kernel รับค่า

1. วิธีป้องกันการตอบรับคำสั่ง ping

เป็นวิธีการป้องกันการส่ง package ใหญ่ ๆ มาถล่ม Server ที่เรียกกันว่า Ping of Death ซึ่งในอดีตเป็นเรื่องที่ Server กลัวกันมาก ผู้ดูแลระบบอาจไม่ชอบการเขียน Script ให้ firewall ปิดการ ping สามารถใช้วิธีนี้ได้ง่ายกว่ามาก ทำได้ดังนี้

 # vi /etc/sysctl.conf

เพิ่มต่อท้ายไฟล์ได้เลยครับ

net.ipv4.icmp_echo_ignore_all = 1

บันทึกแล้วอย่าลืมว่าต้อง

 # /etc/rc.d/init.d/network restart

กรณีไม่ต้องการ restart network ให้สั่งโดยตรงได้ดังนี้

 # sysctl -w net.ipv4.icmp_echo_ignore_all = 1

2. ขัดขวางการร้องขอการ Broadcasts

ในระบบ Network ภายในองค์กรเดียวกัน หากมีผู้ไม่ประสงค์ดีส่งสัญญาณร้องขอการ Broadcasts (ที่ ip หมายเลขสุดท้าย เช่น 192.168.1.255) เพื่อกระจาย package ไปทุก ip address ใน Network จะทำให้ระบบหยุดให้บริการได้ คุณควรป้องกันในส่วนนี้ด้วย

 # vi /etc/sysctl.conf

เพิ่มต่อท้ายไฟล์ได้เลยครับ

net.ipv4.icmp_echo_ignore_broadcasts = 1

บันทึกแล้วอย่าลืมว่าต้อง

#/etc/rc.d/init.d/network restart

กรณีไม่ต้องการ restart network ให้สั่งโดยตรงได้ดังนี้

 # sysctl -w net.ipv4.icmp_echo_ignore_broadcasts = 1

3. ป้องกัน Source route

Routing และ Routing Protocol สร้างปัญหาให้กับ Server เป็นอย่างมากเพราะ IP Source Routing ในขณะทำงานจะเป็นตัวที่บรรจุรายละเอียดเส้นทางที่จะส่ง packet ไปยังจุดหมายปลายทางใด ซึ่งเป็นอันตรายอย่างมากเพราะถ้ามีผู้ไม่ประสงค์ดีส่งค่าเพื่อการโจมตีเข้ามาพร้อมกับ source route packet ก็สามารถส่งถึงเครื่องเป้าหมายและมีการโต้ตอบทำงานตามเงื่อนไขของผู้บุกรุกได้ทันที จึงเป็นการสมควรอย่างยิ่งที่ต้องรีบยกเลิกค่า ip routing ดังนั้นจึงควรที่จะปิดเส้นทางอันตรายนี้ ดังต่อไปนี้

 # vi /etc/sysctl.conf

เพิ่มต่อท้ายไฟล์ได้เลยครับ

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

บันทึกแล้วอย่าลืมว่าต้อง

#/etc/rc.d/init.d/network restart

กรณีไม่ต้องการ restart network ให้สั่งโดยตรงได้ดังนี้

 # sysctl -w net.ipv4.conf.all.accept_source_route = 0

 # sysctl -w net.ipv4.conf.default.accept_source_route = 0

4. ป้องกัน TCP SYN Cookie Attack

คงเคยได้ยิน DoS (Denial of Service) กันบ่อย ๆ ว่ามีการส่ง package หรือยิงคำสั่งมาใน Server จำนวนมาก ๆ ในเวลาพร้อม ๆ กันทำให้ server หยุดบริการในส่วนต่าง ๆ เห็นตามหนังสือ Hacker ชอบเขียนกันมากมาย TCP SYN Cookie Attack ก็เป็นหนึ่งใน DoS เหมือนกัน เป็นวิธีการส่ง Package มาพร้อม ๆ กับข้อมูล หากใครโดนเข้าจะมีอาการ Traffic หนาแน่นจนไม่สามารถให้บริการลูกข่าย หรือถ้าหนักหน่อยเครื่องก็ Reboot ได้ จึงควรรีบปิดเสียก่อนที่จะถูกโจมตี ทำดังนี้ครับ

 # vi /etc/sysctl.conf

เพิ่มต่อท้ายไฟล์ได้เลยครับ

net.ipv4.tcp_syncookies = 1

บันทึกแล้วอย่าลืมว่าต้อง

#/etc/rc.d/init.d/network restart

กรณีไม่ต้องการ restart network ให้สั่งโดยตรงได้ดังนี้

 # sysctl -w net.ipv4.tcp_syncookies = 1

5. ป้องกันการ Redirect Package

ในขณะที่ระบบมีการใช้เส้นทางในการส่ง packet ไปยังปลายทางผิดพลาดเกิดขึ้น icmp redirect packet จะใช้วิธีย้อนกลับ (Redirect)ไปถาม router ว่าเส้นทางที่ถูกต้องอยู่ที่ไหน ถ้าผู้บุกรุกมักส่ง package แทรกเข้าระบบในขณะนี้ได้ก็สามารถที่จะทำการเปลี่ยนเส้นทาง routing table ที่จะไปตาม host ต่าง ๆ จนทำให้ระบบ

 # vi /etc/sysctl.conf

เพิ่มต่อท้ายไฟล์ได้เลยครับ

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

บันทึกแล้วอย่าลืมว่าต้อง

 # /etc/rc.d/init.d/network restart

กรณีไม่ต้องการ restart network ให้สั่งโดยตรงได้ดังนี้

 # sysctl -w net.ipv4.conf.all.accept_redirects=0

 # sysctl -w net.ipv4.conf.default.accept_redirects=0

6. Enable bad error message Protection

การใช้ Linux ที่ผ่านมาส่วนมากจะพบว่า เมื่อมีเหตุการณ์เกี่ยวกับระบบมีปัญหา linux จะไม่แจ้งข้อความเตือนให้ผู้ดูแลระบบทราบ ทำให้การค้นหาสาเหตุทำได้ยาก ดังนั้นคุณควรสั่งให้มีการแจ้งข้อความเตือนทุกครั้งที่มีเหตุผิดพลาดในระบบ Network เท่าที่ OS จะแสดงได้ ทำได้ดังนี้

 # vi /etc/sysctl.conf

เพิ่มต่อท้ายไฟล์ได้เลยครับ

net.ipv4.icmp_ignore_bogus_error_responses = 1

บันทึกแล้วอย่าลืมว่าต้อง

 # /etc/rc.d/init.d/network restart

กรณีไม่ต้องการ restart network ให้สั่งโดยตรงได้ดังนี้

 # sysctl -w net.ipv4.icmp_ignore_bogus_error_responses = 1

7. Enable IP spoofing protection

ในบางครั้งคุณอาจเคยตรวจพบ IP Address แปลก ๆ แอบบุกรุกเข้ามาใช้ทรัพยากรใน Server ได้จาก Log file แสดงว่ามีการเปิดประตูให้ผู้บุกรุกเข้าออกได้ตามใจชอบ ซึ่งเป็นช่องทางที่ทำให้เกิดปัญหาการบุกโจมตีเพื่อให้ระบบหยุดทำงาน (DoS) ได้ตลอดเวลา คุณควรป้องกันดังนี้

 # vi /etc/sysctl.conf

เพิ่มต่อท้ายไฟล์ได้เลยครับ

net.ipv4.conf.all.rp_filter = 1

บันทึกแล้วอย่าลืมว่าต้อง

#/etc/rc.d/init.d/network restart

กรณีไม่ต้องการ restart network ให้สั่งโดยตรงได้ดังนี้

 # sysctl -w net.ipv4.conf.all.rp_filter = 1

8. Enable Log Spoofed, Source Routed and Redirect Packets

หาก Server ทำงานตามปกติก็ไม่ต้องกังวลอะไรมาก แต่พอมีปัญหาผู้ดูแลระบบมักจะต้องทำการค้นหาศึกษาปัญหาที่เกิดขึ้น ดังนั้นคุณควรบันทึกการผิดพลาดต่าง ๆ ไว้ใน log file ในเรื่องต่าง ๆ ที่มีการปลอม IP เข้ามาเพื่อให้ Server ทำงานผิดปกติหรือกรณี icmp redirect packet ตามข้อ 5 ทำได้ดังนี้

 # vi /etc/sysctl.conf

เพิ่มต่อท้ายไฟล์ได้เลยครับ

net.ipv4.conf.all.log_martians = 1

บันทึกแล้วอย่าลืมว่าต้อง

 # /etc/rc.d/init.d/network restart

กรณีไม่ต้องการ restart network ให้สั่งโดยตรงได้ดังนี้

 # sysctl -w net.ipv4.conf.all.log_martians = 1

9. ค้นหาไฟล์ที่ไม่มีเจ้าของ

เมื่อใดก็ตามที่ปรากฏว่ามีไฟล์หรือ directory ที่ไม่มีเจ้าของอยู่ใน Server แสดงให้เห็นว่ามีการนำไฟล์ที่ไม่มีเจ้าของมาใส่ไว้ใน server หรือมีผู้บุกรุกจากภายนอกได้ส่งข้อมูลเข้ามาใน Server แล้ว และกำลังปฏิบัติการบางอย่างที่ไม่คาดคิด อาจทำให้ระบบเสียหายอย่างใหญ่หลวง คุณควรค้นหาไฟล์ที่ไม่มีเจ้าของและลบทิ้งหรือถ้าเป็นการนำมาใส่ไว้เองก็ต้องทำการ chown เพื่อให้รู้ว่าเป็นของ user คนใดนอกนั้นให้รีบลบทิ้งเพื่อความปลอดภัยของ Server ทำดังนี้

 # find / -nouser -o -nogroup

ให้ค้นหาซ้ำอีกครั้งถ้าหากมีไฟล์ดังกล่าวใน /dev ไม่นับรวมและไม่ต้องไปลบหรือแก้ไข ใน CD ชุดนี้ได้แก้ไขแล้วอาจมีข้อความในแจ้งว่าหาไฟล์หรือ Directory ใน /proc ไม่พบก็ไม่ต้องแก้ไขอะไร

10. ค้นหาไฟล์ ".rhosts"

ใน Server ไม่ควรปล่อยให้มีไฟล์ .rhosts อยู่เพราะเป็นไฟล์ที่เกิดจากการ Remote เข้าไปยัง server หากพบว่ามีให้ลบทิ้งเพราะจะทำให้ผู้บุกรุกใช้เป็นช่องโหว่ในการโจมตีได้ เป็นหน้าที่ประจำของผู้ดูแลระบบที่ต้องค้นหาและลบทิ้ง ทำได้ดังนี้

 # find /home -name .rhosts

คุณควรใช้ crontab ตั้งเวลาตรวจสอบไฟล์นี้จะดีกว่า จะได้ไม่ลืมค้นหาหรืออาจเขียน script ให้ส่ง mail ไปบอกคุณเมื่อมีไฟล์นี้ปรากฏขึ้นใน Server ตามตัวอย่างต่อไปนี้

 # vi /etc/cron.daily/rhosts.cron

พิมพ์ script ต่อไปนี้ลงไปเพื่อให้แจ้งกับ root ทุกวันเมื่อมีไฟล์ .rhosts

```
#!/bin/sh
/usr/bin/find /home -name .rhosts | (cat <<EOF
This is an automated report of possible existent ..rhosts files on
the server deep.openna.com, generated by the find utility command.
New detected ..rhosts. files under the ./home/. directory include:
EOF
cat
) | /bin/mail -s "Content of .rhosts file audit report" root
```

เสร็จแล้วให้เปลี่ยน mode เป็น 550

 # chmod 550 /etc/cron.daily/rhosts.cron

บทสรุป

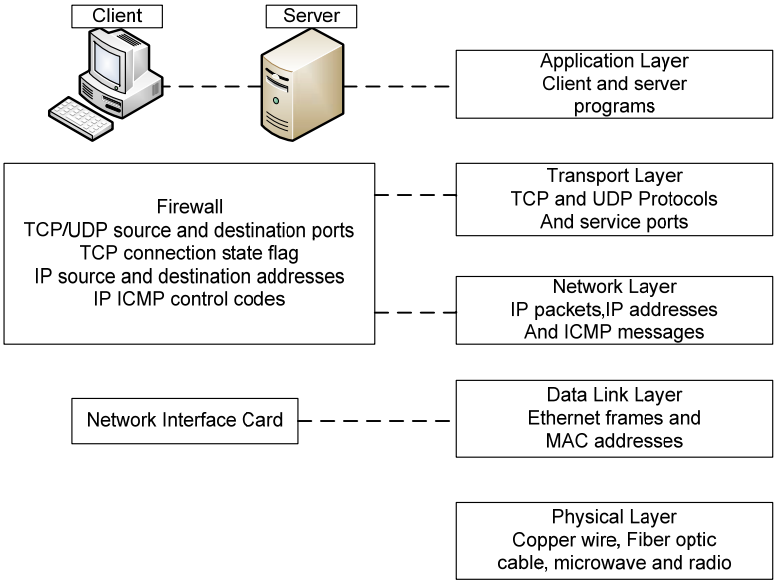
แม้ว่าจะมีการแนะนำการปรับค่าต่าง ๆ ให้กับ kernel ก็ยังไม่สามารถทำให้เกิดความปลอดภัยได้อย่างครบถ้วน 100% เนื่องมาจาก kernel แต่ละ version จะมี bug ต่าง ๆ เกิดขึ้นเมื่อมีการนำไปใช้งานแล้วเท่านั้นรวมไปถึงเมื่อมีผู้บุกรุกโจมตีเข้าถึง kernel ได้เมื่อไรก็จะมีการนำปัญหาเหล่านั้นไปสร้าง patch เพื่อให้สามารถใช้งานกันได้ต่อเนื่อง ดังนั้นหากมี Linux ค่ายไหนพบปัญหาก่อนก็มักจะ patch ให้กับ kernel ของค่ายตนเองก่อน ผู้ดูแลระบบควรติดตามข่าวสารจากเว็บของผู้ผลิตตลอดเวลา ไม่ควรไปฟังจากค่ายอื่น เพราะปัญหาของค่ายอื่นอาจไม่เกี่ยวข้องหรือไม่ใช่ปัญหาของ kernel ที่เราใช้งานอยู่ได้ ผู้เขียนแนะนำให้อ่านดูแล้วนำไปเปรียบเทียบว่าใน Server ที่กำลังปฏิบัติงานอยู่มีปัญหาที่ต้องแก้ไขปรับปรุงตรงกับหัวข้อใดบ้างจะได้ใช้งานได้อย่างมีเสถียรภาพ

บทที่ 7

Firewall

การติดตั้งและใช้งานโปรแกรม

ปัจจุบันนี้คนที่กำลังสนใจที่จะทำ Firewall จาก Free Software มักหนีไม่พ้น IPTABLES ที่มีมาให้บน Linux OS อยู่แล้ว บางคนอาจคิดว่ายากเลยเสาะแสวงหา Application ตัวอื่นมาช่วยผ่อนแรงในการทำ Configuration เช่น Openwall, IPCOP หรือตัวอื่น ๆ ที่แล้วแต่ความชอบส่วนบุคคล ทั้ง ๆ ที่แต่ละตัวที่นำมาใช้ก็ล้วนแล้วแต่ทำงานด้วย IPTABLES เกือบทั้งนั้น เพียงแต่ออกแบบเมนูหรือหน้าตาในการช่วยให้ทำ Configure ง่ายขึ้น หากพอมีเวลาควรศึกษาตัวตนของโปรแกรม IPTABLES ให้ละเอียดขึ้นอีกนิดจะได้นำความสามารถของมันไปประยุกต์ใช้งานให้คุ้มค่าเต็มพิกัด สมกับที่ผู้พัฒนาได้ออกแบบสร้างมาให้ใช้กันดีกว่าที่จะได้ยินบางคนบ่นว่า IPTABLES ไม่ดี ทั้งที่ตนเองก็ไปเอาโปรแกรมตัวอื่นที่ทำงานบน IPTABLES มาใช้งานอยู่ โดยเฉพาะปัจจุบันนี้มีการพัฒนาต่อเนื่องขึ้นไปเรื่อย ๆ เพื่อรองรับการปรับเปลี่ยนระบบ Network ที่มีความซับซ้อนและปลอดภัยมากขึ้นเช่นปัจจุบันสามารถใช้งาน IPTABLES ทำงานร่วมกับ IPV6 ซึ่งจะให้ความปลอดภัยมากกว่า IPV4 แต่อาจต้องทำการศึกษาให้ละเอียดมากขึ้นเพื่อไม่ให้การทำงานผิดพลาด และที่สำคัญคือบางคนมักคิดว่าเคยใช้งาน IPTABLES กับ Kernel 2.4 ก็ไปคัดลอกมาใช้งานบน Kernel 2.6 ทันที แบบนี้อาจมีบางส่วนที่ต้องปรับปรุงเพื่อให้มีประสิทธิภาพในการใช้งานดีขึ้นและรวดเร็วขึ้นตามขีดความสามารถของ Version ใหม่ บางคำสั่งหรือบางกฎเกณฑ์สามารถนำมาใช้ได้เพราะ Version ที่สูงกว่าย่อมเห็นการทำงานใน Version เก่าได้ทั้งหมดแต่การปรับปรุง Version นั้นหมายถึงการแก้ปัญหาต่าง ๆ และเพิ่มขีดความสามารถใหม่ ๆ เข้ามาหากคุณยังใช้วิธีคัดลอกของเดิมมาใช้ ก็จะไม่ได้รับอะไรใหม่ ๆ ที่ผู้พัฒนาทำมาให้ ในบทนี้ผู้เขียนจะนำหลักและวิธีการใหม่ ๆ ของ IPTABLES 1.3.x (ขณะที่เขียนคู่มือเล่มนี้ iptables 1.4 กำลังอยู่ระหว่าง Test)มานำเสนอเพื่อให้นำไปปรับปรุงเพิ่มเติมใช้งานให้เหมาะสมกับการใช้งานของแต่ละหน้าที่ ดังนั้นหากคุณกำลังทำ Server ที่ให้บริการอะไรควรศึกษาและทำ Firewall ให้กับเครื่อง Server นั้น ๆ ให้ตรงกับความต้องการเท่านั้น ไม่ควรลอกทั้งหมดหรือทำเหมือนกันหมดทุกเครื่องเพราะอาจไม่เกิดผลดีเท่าที่ควรหรืออาจเกิดความขัดแย้งในขณะให้บริการกับลูกข่ายก็เป็นได้ ผู้เขียนได้พยายามสรุปแต่ละขั้นตอนเพื่อให้ง่ายและสามารถนำไปใช้ได้ทันที เพียงแต่ควรอ่านให้เข้าใจก่อน จะได้ไม่เกิดการทำงานที่ผิดพลาดขึ้นแล้วหาสาเหตุไม่พบ ในอดีตรูปแบบการใช้งานอย่างง่ายที่มักพบการทำตัวอย่าง Firewall ด้วย IPTABLES มีการใช้งานง่าย ๆ คือ มีการใช้งาน 3 Policy ในการควบคุมซึ่งประยุกต์หรือดัดแปลงมาจากการใช้งาน ipchains นั่นเอง ลองดู Firewall Model กันก่อน



Firewall placement in the TCP/IP reference model

ถ้าต้องการให้ทำงานสมบูรณ์ขึ้นควรศึกษารายละเอียดที่โปรแกรมมีมาให้ และนำไปใช้ให้ตรงกับความต้องการเท่านั้น สิ่งที่ IPTABLES มีมาให้ที่เด่นก็คือการสร้าง Module ขึ้นมาเพื่อแยกการทำงานของ rule table ให้ทำงานแต่ละ packet แยกกันอิสระ และจำแนกออกเป็น 3 Table คือ filter table, nat table และ mangle table มีรายละเอียดดังนี้

Filter Table เป็น Table หลักส่วน Table อื่น ๆ จะถูกระบุเพิ่มเติมโดยการสั่ง option ทาง Command Line หน้าที่สำคัญของ filter table ที่เป็นพื้นฐานในการใช้งานมีดังนี้

1. Chain-relate operation ประกอบด้วย INPUT, OUTPUT, FORWARD และ user-defined chain
2. Target disposition ประกอบด้วย ACCEPT หรือ DROP
3. IP header field match operations แต่ละ protocol, source และ destination address, input และ output interface, และ fragment handling
4. Match operation ของ TCP, UDP และ ICMP header field

NAT table มีทั้งหมด 3 รูปแบบดังนี้

1. Unidirectional outbound NAT ใช้สำหรับ Private IP Address แบ่งได้ 2 แบบคือ

   1.1 Basic NAT ใช้ map local private source address ไปยังกลุ่มของ Public IP address

   1.2 NAPT (Network Address Port Translation) ใช้ map local private IP address ไปยัง Public IP Address 1 เบอร์ (เหมือนกับ linux masquerading แบบเดิมที่ใช้ ipchains)

2. Bidirectional NAT เป็นแบบสองทางทั้งการเชื่อมต่อแบบ inbound และ outbound และยังใช้ทำ bidirectional mapping ระหว่าง IPV4 และ IPV6 address อีกด้วย

3. Twice NAT เป็นแบบอนุญาตทั้งสองทางคือทั้ง inbound และ outbound ของ Source และ Destination

NAT ยัง support การทำงานทั้ง SNAT (Source NAT) และ DNAT (Destination NAT) ซึ่งประกอบด้วย build-in chains 3 แบบ คือ

PREROUTING ใช้ระบุการเปลี่ยนแปลงที่ destination ไปยัง incoming packet ก่อนส่ง packet ไปยัง routing function (DNAT) เปลี่ยน Address ปลายทางไปยัง localhost เช่น transparent proxy, port redirection

OUTPUT ใช้ระบุค่าการเปลี่ยนที่ปลายทางไปสร้าง packet จากตัว local ก่อนที่จะส่งออกไปภายนอก (DNAT, REDIREC)

POSTROUTING ใช้ระบุการเปลี่ยนแปลงจากต้นทางไปยัง Outgoing packet ตามที่กำหนด (SNAT, MASQUERADE)

Mangle table ยอมให้กำหนดตำแหน่ง จัดกลุ่มของค่าต่าง ๆ ของ netfilter ทำการเปลี่ยนตำแหน่งของ packet ก่อนส่งออกไปปลายทาง ประกอบด้วย build-in chain ดังนี้

- PREROUTING ใช้ระบุการเปลี่ยน packet ที่เข้ามายัง interface ก่อนทำการหาเส้นทางและตัดสินใจว่าจะส่งไปยัง local IP Address ใด
- INPUT ใช้ระบุการเปลี่ยน packet ทุก ๆ process หลังจากที่ผ่านการขัดขวางจากกฎของ PREROUTING แล้ว
- POSTROUTING ใช้ระบุการเปลี่ยนแปลง packet ที่จะออกจาก Firewall หลังจากที่ผ่านการขัดขวางจากกฎของ OUTPUT แล้ว
- FORWARD ใช้ระบุให้เปลี่ยน packet ที่จะส่งไปยัง Firewall
- OUTPUT ใช้ระบุการเปลี่ยนแปลงค่าที่ระบบภายในสร้างขึ้นก่อนส่ง packet ออกไปยังภายนอก

ในการวางติดตั้งระบบ Network ที่ดีนั้น ผู้ออกแบบควรคำนึงถึงระบบความปลอดภัยข้อมูลเป็นสำคัญ เพราะเมื่อใดก็ตามหากวางระบบให้มีช่องโหว่ อาจทำให้ข้อมูลเกิดความเสียหายได้ หรือถ้าเป็นระบบ Internet การป้องกันให้ระบบทำงานได้อย่างมีเสถียรภาพยิ่งมีความจำเป็นอย่างมาก และจะไม่สามารถที่จะกู้คืนหรือ

ก่อนอื่นควรจะทราบ Policy ที่โปแกรมสร้างมาให้ภายในแล้ว มีทั้งหมด 5 chain คุณสามารถสร้าง chain เองได้แล้วแต่จะตั้งชื่ออะไรนอกเหนือจาก chain ที่มีอยู่แล้วดังนี้

- INPUT
- OUTPUT
- FORWARD
- PREROUTING
- POSTROUTING

คุณอาจเคยใช้ใน ipchains มาแล้วใน Version ที่ผ่านมา ทุกครั้งที่อยากกำหนดค่า Firewall ด้วยตนเอง คุณต้องแจ้งให้โปรแกรมทราบว่าคุณต้องการให้แต่ละ Chain มีค่าเป็นอย่างไรเช่น

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

รูปแบบคำสั่งที่จะใช้งานมีดังนี้

iptables [-t|--table table] -*command* [chain] [-i *interface*] [-p *protocol*]

[-s *address* [*port*[:*port*]]] [-d *address* [*port*[:*port*]]] -j *policy*

ในการสั่งใช้งานตามรูปแบบที่เห็นถ้าเป็นตัวอักษรตัวเอียง แสดงว่าให้คุณกรอกค่าที่ต้องการลงไปแทนส่วนตัวที่มีเครื่องหมาย Pipe [|] ขั้นกลางแสดงว่าให้เลือกว่าจะใช้อย่างใดอย่างหนึ่งเช่น -t หรืออาจใช้ --table ก็ได้มีความหมายเช่นเดียวกัน และที่น่าจะงงคือ [port[:port]] หมายถึงให้กำหนดค่าหมายเลข port ตั้งแต่ port : จนถึง port สุดท้าย เช่น 0:1023 หมายถึง ตั้งแต่ port 0 ถึง port 1023 หรืออาจเขียนรูปแบบสั้น ๆ เช่น 1024: แบบนี้หมายถึง port 1024 เป็นต้นไปครับ ต่อไปดูค่าอื่น ๆ กันบ้างจะได้ใช้กันเป็น

table หมายถึงให้เติมค่าได้ทั้งหมด 4 ค่าตามที่อธิบายผ่านมาข้างต้น คือ

filter เป็นค่า default คือโปรแกรมจะทำงานในโหมดกรอง packet หากไม่ระบุค่าหลัง -t โปรแกรมจะถือว่าเป็นค่านี้

nat เป็นการเรียกใช้ Network Address Translation

mangle ใช้กับ QOS (Quality of Service) และการเลือกเส้นทางที่ดีที่สุด

raw ใช้เมื่อต้องการให้การทำงานดีและเร็วที่สุดโดยลดขั้นตอนการทำงานของ kernel ในขณะที่มีการเรียกใช้งาน port ที่ตรงกันจะไม่มีการแปรค่าใด ๆ

command [chain] หมายถึงคำสั่งที่ต้องการให้ทำงานให้ใช้ได้เพียงค่าเดียวเท่านั้นส่วน chain ก็คือค่า chain ที่มีมาในโปแกรมทั้ง 5 chain และรวมถึง chain ที่สร้างขึ้นเอง ดูค่า command ก่อนมีทั้งหมดดังนี้

-A หรือ --append หมายถึง การเพิ่ม rule ให้กับ chain

-D หรือ --delete หมายถึง การลบ rule ออกจาก chain

-I หรือ --insert หมายถึง การแทรก rule ตามตำแหน่งที่ต้องการ

-R หรือ --replace หมายถึง การแทนที่ rule

-F หรือ --flush หมายถึง การสั่งให้เริ่มรับค่าใหม่เพื่อทำงานพร้อมกันทั้งหมด

-L หรือ --list หมายถึง เรียกดู rule ทั้งหมด

-N หรือ --new-chain หมายถึง การสร้าง chain ใหม่

-X หรือ --delete-chain หมายถึง การลบ chain ที่สร้างขึ้นเอง

-P หรือ --policy หมายถึง การตั้งค่าหลักให้กับ chain

-E หรือ --rename-chain หมายถึง การเปลี่ยนชื่อ chain ส่วนที่ต่อจาก command ก็คือ command option มีค่าที่จำเป็นคือ

-i หมายถึง interface ที่รับ packet เข้ามา

-o หมายถึง interface ที่ส่ง packet ออกไป

-p หมายถึง protocol เช่น tcp, udp, icmp

-s หมายถึง หมายเลข IP ของ packet ต้นทาง (Source)

-d หมายถึง หมายเลข IP ของ packet ปลายทาง (Destination)

-m หมายถึง match state ในการรับส่ง packet

-j หมายถึง jump ส่ง packet ไปยังปลายทางด้วย policy อะไร พอมาถึง -j ก็ต้องตามด้วย policy ที่ต้องการส่ง packet ไปให้ มีค่าหลายค่า ดังนี้

ACCEPT หมายถึง ยอมให้ packet ผ่านไปได้

DROP หมายถึง ไม่ยอมให้ packet ผ่านไปได้โดยไม่มีการแจ้งกลับ

REJECT หมายถึง ไม่ยอมให้ packet ผ่านโดยมีการแจ้งให้ทราบ

RETURN หมายถึง ให้ไปเลือกการทำงานตามเป้าหมายที่กำหนด

MASQUERADE ใช้ร่วมกับ NAT และ DHCP

SNAT	ใช้ร่วมกับ PREROUTING
REDIRECT	ใช้ร่วมกับ NAT ในการเปลี่ยนแปลง output port
DNAT	ใช้ร่วมกับ POSTROUTING

อ้างอิงจากของต่างประเทศดูได้จากตารางข้างล่าง

Common options used in Rule Specifications

Option	Description
-s sourceIP	Match if the packet originated from sourceIP. sourceIP may be an IP address (e.g., 192.168.200.201), network address (e.g., 192.168.200.0/24), or hostname (e.g., woofgang.dogpeople.org). If not specified, defaults to 0/0 (which denotes "any").
-d destinationIP	Match if packet is destined for destinationIP. destinationIP may take the same forms as sourceIP, listed earlier in this table. If not specified, defaults to 0/0.
-i ingressInterface	Match if packet entered system on ingressInterfacee.g., eth0. Applicable only to INPUT, FORWARD, and PREROUTING chains.
-o egressInterface	Match if packet is to exit system on egressInterface. Applicable only to FORWARD, OUTPUT, and POSTROUTING chains.
-p tcp | udp | icmp | all	Match if the packet is of the specified protocol. If not specified, defaults to all.
--dport destinationPort	Match if the packet is being sent to TCP/UDP port destinationPort. Can be either a number or a service name referenced in /etc/services. If numeric, a range may be delimited by a colone.g., 137:139 to denote

Common options used in Rule Specifications

Option	Description
	ports 137-139. Must be preceded by a -p (protocol) specification.
--sport sourcePort	Match if the packet was sent from TCP/UDP sourcePort. The format of sourcePort is the same as with destinationPort, listed earlier in this table. Must be preceded by a -p [udp | tcp] specification.
--tcp-flags mask match	Look for flags listed in mask; if match is set, match the packet. Both mask and match are comma-delimited lists containing some combination of SYN, ACK, PSH, URG, RST, FIN, ALL, or NONE. Must be preceded by -p tcp.
--icmp-type type	Match if the packet is icmp-type type. type can be a numeric ICMP type or a name. Use the command iptables -p icmp -h to see a list of allowed names. Must be preceded by -p icmp.
-m state --state statespec	Load state module, and match packet if packet's state matches statespec. statespec is a comma-delimited list containing some combination of NEW, ESTABLISHED, INVALID, or RELATED.
-j accept | drop | log | reject | [chain_name]	Jump to the specified action (accept, drop, log, or reject) or to a custom chain named chain_name.

ต่อไปนี้จะเป็นตัวอย่างการป้องกันที่จะนำไปปรับปรุงแก้ไขให้ตรงกับการใช้งานจริง ซึ่งมีการนำเอากฎที่ถูกต้องในการสร้างเพื่อรองรับการส่งค่าไปกลับที่ถูกต้องตามที่ผู้เขียนโปรแกรมได้กำหนดมาให้ การทดลองแต่ละตัวอย่างให้สร้างเป็น script แล้วสั่ง Run จะดีกว่าลองแบบ Command line เพราะจะได้นำตัวอย่างถัดไปมาเพิ่มแล้วทดลองต่อได้จนครบทุกเรื่อง มาลองศึกษาดูทีละตัวอย่างดังนี้

ตัวอย่างที่ 1 การตั้งค่าเริ่มต้นที่ถูกต้อง (Initializing netfilter)

 # vi /root/test_firewall

… เริ่มพิมพ์ตั้งแต่ตรงนี้เป็นต้นไป…

```
#!/bin/sh
# Script Created by: Mr.Boonlue Yookong
/sbin/modprobe ip_tables
/sbin/modprobe ip_conntrack_ftp
# กำหนดค่าตัวแปรเริ่มต้น
IPTS="/sbin/iptables"
# Flush old rules, old custom tables
$IPTS -F
$IPTS -F -t nat
$IPTS -X
# Firewall ที่ดีควรปิดทุกอย่างทั้งที่เรารู้และไม่รู้จักทุก Chain
$IPTS -P INPUT DROP
$IPTS -P FORWARD DROP
$IPTS -P OUTPUT DROP
```

เสร็จแล้วให้บันทึกแล้วออกจาก vi

:wq

จากนั้นให้เปลี่ยน mode file เป็น 700

 # chmod 700 /root/test_firewall

การทดสอบให้สั่ง run script ได้โดย

 # /root/test_firewall

ลองตรวจสอบได้จาก

 # iptables -L -n

ก็จะพบว่า chain ทั้ง 3 ถูกกำหนดให้ DROP เมื่อทำงานตามที่ต้องการก็ให้ทดลองทำตัวอย่างต่อไป

ตัวอย่างที่ 2 การกำหนด Policy ให้กับ Loopback interface

```
# กำหนดให้ loopback interfaces รับ-ส่ง packet ได้อย่างอิสระ
$IPTS -A INPUT  -i lo -j ACCEPT
$IPTS -A OUTPUT -o lo -j ACCEPT
```

ตัวอย่างที่ 3 ป้องกัน IP แปลกปลอมเข้ามา (Anti-IP-spoofing rules) การทำงานของผู้ดูแลระบบควรมีการบันทึกค่าที่ได้ไว้ใน log file เพื่อตรวจสอบและปรับปรุงระบบได้ถูกต้อง ดังตัวอย่าง

```
# เป็นตัวอย่างเบื้องต้นสำหรับกลุ่ม ip address ที่แปลกปลอมเข้ามา
$IPTS -A INPUT -s 255.0.0.0/8 -j LOG --log-prefix "Spoofed source IP!"
$IPTS -A INPUT -s 255.0.0.0/8 -j DROP
$IPTS -A INPUT -s 0.0.0.0/8 -j LOG --log-prefix "Spoofed source IP!"
$IPTS -A INPUT -s 0.0.0.0/8 -j DROP
$IPTS -A INPUT -s 127.0.0.0/8 -j LOG --log-prefix "Spoofed source IP!"
$IPTS -A INPUT -s 127.0.0.0/8 -j DROP
$IPTS -A INPUT -s 192.168.0.0/16 -j LOG --log-prefix "Spoofed source IP!"
$IPTS -A INPUT -s 192.168.0.0/16 -j DROP
$IPTS -A INPUT -s 172.16.0.0/12 -j LOG --log-prefix " Spoofed source IP!"
$IPTS -A INPUT -s 172.16.0.0/12 -j DROP
$IPTS -A INPUT -s 10.0.0.0/8 -j LOG --log-prefix " Spoofed source IP!"
$IPTS -A INPUT -s 10.0.0.0/8 -j DROP
$IPTS -A INPUT -s 208.13.201.2 -j LOG --log-prefix "Spoofed Woofgang!"
$IPTS -A INPUT -s 208.13.201.2 -j DROP
```

กรณีที่รู้ว่า IP Address ใดที่ไม่ปลอดภัยก็สามารถเพิ่มลงไปจากตัวอย่างนี้ได้เช่น

```
$IPTS -A INPUT -s xxx.xxx.xxx.xxx -j DROP
```

xxx.xxx.xxx.xxx คือ IP ที่ไม่ยอมให้เข้ามา

ตัวอย่างที่ 4 ป้องกันการ scan แบบ stealth (Anti-stealth-scanning rule)

เป็นวิธีการป้องกันไม่อนุญาตให้ผู้ที่กำลัง scan มาเชื่อมต่อกับระบบได้ด้วยการใช้ TCP header syn bit ตรวจสอบ เปรียบเทียบกับ -m state เป็นการตรวจสอบสำหรับผู้ที่จะเข้ามาใหม่เท่านั้น (NEW) ส่วนผู้ที่สามารถเข้าระบบได้อยู่แล้วยกเว้น (! --syn) ตรวจสอบผลจาก log file

```
$IPTS -A INPUT -p tcp ! --syn -m state --state NEW \
-j LOG --log-prefix "Stealth scan attempt?"
$IPTS -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
```

ตัวอย่างที่ 5 การกำหนดค่า rule ให้กับ INPUT chain

ให้สังเกตรูปแบบการใช้ command option -m ในตัวอย่างว่าถ้ากรณีเป็น INPUT chain ต้องใช้ค่า state อะไรบ้างแล้วไปเปรียบเทียบกับ OUTPUT chain ว่า state ต้องเป็นค่าอะไรถึงจะทำงานสอดคล้องกันได้สมบูรณ์

```
# กำหนดให้ยอมรับ Connection ที่กำลังทำงานอยู่ก่อนหน้า rule นี้ให้ทำงานต่อไป
$IPTS -A INPUT -j ACCEPT -m state --state ESTABLISHED,RELATED
# Accept inbound packets which initiate SSH sessions
$IPTS -A INPUT -p tcp -j ACCEPT --dport 22 -m state --state NEW
# Accept inbound packets which initiate FTP sessions
$IPTS -A INPUT -p tcp -j ACCEPT --dport 21 -m state --state NEW
# Accept inbound packets which initiate HTTP sessions
$IPTS -A INPUT -p tcp -j ACCEPT --dport 80 -m state --state NEW
# Log anything not accepted above
$IPTS -A INPUT -j LOG --log-prefix "Dropped by default:"
```

ตัวอย่างข้างบนไม่ได้ระบุค่า source ip address ในระบบจริงมีการจัดการเป็นแบบ Bastion host ที่ตั้ง server อยู่ในกลุ่ม DMZ จึงควรกำหนดค่า source ip address ให้กับเครื่องที่ให้บริการในแต่ละ service เช่น server ที่เปิดบริการ Secure shell port 22 กำหนดดังนี้

```
$IPTS -A INPUT -p tcp -j ACCEPT -s xxx.xxx.xxx.xxx --dport 22 \
-m state --state NEW
```

ตัวอย่างที่ 6 การกำหนด rule ให้กับ OUTPUT chain

ให้สังเกตว่าการใช้ command option -m ใส่ค่า TCP Header bit อะไรบ้างเพื่อให้สอดรับกับ rule ที่ INPUT chain ถ้ากำหนดไม่ถูกต้องจะมีผลให้การทำงานช้าลงและอาจมีข้อผิดพลาดในการป้องกันได้ ในตัวอย่างนี้จะเห็นว่ามีการใช้ state RELATED และ ESTABLISHED กำหนดไว้ให้สำหรับกรณีที่มี connection ใดที่ผ่านการตรวจสอบจาก INPUT chain แล้วมีการ connect ได้สำเร็จและกำลังทำงานอยู่ก่อนที่จะมี rule นี้ยอมให้ส่ง packet ที่สัมพันธ์กันกับการร้องขอมาออกไปได้ ให้กำหนดดังนี้

```
$IPTS -I OUTPUT 1 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

ถ้าต้องการให้เครื่องตอบรับการใช้คำสั่ง ping ให้ระบุ protocol และ type ดังนี้

```
$IPTS -A OUTPUT -p icmp -j ACCEPT --icmp-type echo-request
```

ถ้าต้องการส่ง packet ในแต่ละ service ให้ระบุ state เป็น NEW หมายถึงให้ส่งเฉพาะ connection ที่เกิดขึ้นใหม่เท่านั้น ลองดูตัวอย่าง DNS Server ตอบรับการร้องขอ IP ให้ระบุดังนี้

```
$IPTS -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT
```

บรรทัดสุดท้ายของการกำหนด rule ของทุก chain ควรเก็บค่าที่ไม่ผ่านการตรวจสอบจาก rule ที่กำหนดมาข้างบนไว้ที่ log file เสมอ

```
$IPTS -A OUTPUT -j LOG --log-prefix "Dropped by default:"
```

กรณีที่มีผู้ดูแลระบบบางคนพยายามหลีกเลี่ยงการใช้ port มาตรฐานหรือ Privilege port แต่กลับไปใช้ Non-privileged port แทนคือ port 1024 ขึ้นไปต้องกำหนดค่าให้ INPUT และ OUTPUT chain ตรงกันด้วย เช่น

```
$IPTS -A INPUT     -p tcp --sport 1024: --dport 1024:  \
-m state --state ESTABLISHED -j ACCEPT
$IPTS -A OUTPUT -p tcp --sport 1024: --dport 1024:  \
-m state --state ESTABLISHED,RELATED -j ACCEPT
```

จากตัวอย่างที่ผ่านมาเป็นการออกแบบสร้าง Firewall ที่เน้นการควบคุมทั้ง 3 Policy แล้วมีการกำหนดให้มี chain rule ทั้งด้าน incoming และ outgoing packets ให้กับระบบที่มีการตั้ง Server ทั่วๆ ไปโดยส่วนใหญ่นอกจากจะป้องกัน Service ที่ Server ให้บริการแล้วยังเน้นการป้องกันการถูกโจมตีด้วยการ scan ในรูปแบบต่างๆ เพื่อไม่ให้ผู้ไม่หวังดีรู้ว่าเครื่อง Server เปิด port อะไรที่ไม่ได้ใช้งานทิ้งไว้บ้าง ก่อนที่จะไปศึกษาเรื่องอื่นต่อควรรู้เกี่ยวกับเครื่องมือที่ใช้ในการ Scan port กันก่อน เครื่องมือที่มีความเก่งในระดับโลกที่นิยมใช้กันก็คือ nmap ที่มีมาให้ใช้ฟรีๆ ใน Linux อยู่แล้ว ควรศึกษาวิธีการใช้คำสั่งเบื้องต้นเพื่อใช้ในการทดสอบความแข็งแรงของ Firewall สักเล็กน้อย

nmap ได้ชื่อว่าเป็น World champion port scanner สามารถใช้ scan port ได้หลายชนิดดังนี้

1. TCP Connect scan
2. TCP SYN scan
3. TCP FIN scan
4. TCP NULL scan
5. TCP Xmas Tree scan
6. UDP scan
7. RPC scan

มีรูปแบบการใช้งานดังนี้

```
nmap [-s scan-type] [-p port-range]|-F options target
```

-s ตามด้วยตัวอักษรดังนี้ T = TCP Connect scan S = TCP SYN scan

U = UDP scan (can be combined with the previous flags)

R = RPC scan (can be combined with previous flags)

F, N, X, L, W, O, V, P คือ Fin, Null, Xmas Tree, List, Window, IP Protocol, Version และ Ping scans

เวลาใช้งานสามารถใช้หลายตัวปนกันได้เช่น -sSUR หมายถึง SYN scan, UDP scan และ RPC scan ส่วนการใช้งาน -p ตามด้วย port เดียวหรือเป็นกลุ่มหรือ range ได้เช่น -p 20-23,80,53,600-1024 หมายถึง nmap จะ scan ตั้งแต่ port 20 ถึง 23, 80, 53, และ 600 ถึง 1024 ส่วนการใช้ -F หมายถึง fast scan ส่วน target คือ ip address เป้าหมายกำหนดได้หลายแบบ เช่น 192.168.1.* หมายถึงทั้งหมด 255 IP addresses หรือที่นิยมจะใช้เป็น

ตัวอย่าง การใช้ nmap อย่างง่าย (Simple scan against a bastion host)

 # nmap -sT -F -P0 -O 192.168.1.11

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2008-01-03 13:03 ICT

Insufficient responses for TCP sequencing (0), OS detection may be less accurate

Insufficient responses for TCP sequencing (0), OS detection may be less accurate

Insufficient responses for TCP sequencing (0), OS detection may be less accurate

Interesting ports on 192.168.1.11:

Not shown: 1013 closed ports, 219 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

443/tcp open https

465/tcp open smtps

993/tcp open imaps

995/tcp open pop3s

3306/tcp open mysql

MAC Address: 00:C1:28:01:9C:4E (Unknown)

Too many fingerprints match this host to give specific OS details

Nmap finished: 1 IP address (1 host up) scanned in 38.046 seconds

ตัวอย่าง การใช้ nmap ที่นิยมใช้ตรวจสอบการทำงานโดยทั่วไปให้สั่ง

 # nmap -sURT -F -P0 -O 192.168.1.11

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2008-01-03 13:05 ICT

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port

Interesting ports on 192.168.1.11:

Not shown: 1239 filtered ports, 1010 open|filtered ports

PORT STATE SERVICE VERSION

1379/udp closed dbreporter

1399/udp closed cadkey-licman

2045/udp closed cdfunc

5011/udp closed telelpathattack

32773/udp closed sometimes-rpc10

32779/udp closed sometimes-rpc22

MAC Address: 00:C1:28:01:9C:4E (Unknown)

Too many fingerprints match this host to give specific OS details

Nmap finished: 1 IP address (1 host up) scanned in 809.294 seconds

ตัวอย่าง การตรวจสอบ Version (Nmap Version Scan)

 # nmap -sV -p 80 192.168.1.10

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2008-01-06 10:40 ICT

Interesting ports on 192.168.1.10:

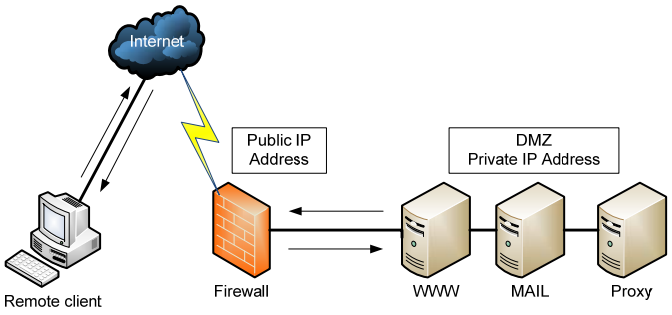
PORT STATE SERVICE VERSION

80/tcp open http **Apache httpd 2.2.4 ((Fedora))**

Nmap finished: 1 IP address (1 host up) scanned in 19.153 secondsds

หลังจากศึกษาการป้องกันด้วย iptables ตามตัวอย่างทั้งหกและยังสามารถใช้เครื่องมือในการ Scan port อย่างมืออาชีพเพื่อใช้ทดสอบ Firewall ได้แล้ว ต่อไปจะนำเสนอสิ่งที่ใกล้ตัวสำหรับผู้ดูแลระบบต้องศึกษาทดลองเพื่อนำไปสร้าง Firewall ที่เหมาะสมกับการใช้งานจริง โดยจะมุ่งเน้นรูปแบบการเขียน Script ที่ครอบคลุมการป้องกันในแต่ละส่วนมาให้ดูทั้งหมด 5 แบบ ดังต่อไปนี้

1. **Host Forwarding** Destination NAT หรือ DNAT ถูกออกแบบมาให้สำหรับทำ Host Forwarding ซึ่งในปัจจุบันได้มีการนำเอาหลักการนี้ไปใส่ในอุปกรณ์ Network ต่าง ๆ กันมากมาย วิธีการนี้เหมาะสำหรับ Site ขนาดเล็กที่ได้ Public IP Address เพียงเบอร์เดียวก็สามารถที่จะตั้ง Server ภายในหน่วยงานให้ทำงานอยู่บน Private IP Address ได้ DNAT จะอนุญาตให้มีการ connected จากภายนอกเข้ามายัง Service ภายในด้วยวิธีการที่เรียกว่า Transparent forward ไปยัง Server ที่ติดตั้งอยู่บน DMZ โดยที่ Public Service ไม่ต้องให้บริการอยู่บนเครื่องที่ทำหน้าที่ Firewall ดังภาพ



จากภาพจะเห็นว่ากรณีที่ได้ Public IP Address มา 1 IP ให้นำ IP ที่ได้ไปติดตั้งใช้งานบนเครื่อง Firewall จากนั้นให้เครื่อง Firewall แจก Private IP Address ออกมาใช้ภายในเพื่อตั้ง Server ซึ่งถือว่าเป็น Zone ที่ปลอดภัยที่สุด เมื่อมีการร้องขอใช้บริการจากลูกข่ายภายนอก (Remote Client) มายังเครื่อง Firewall ไม่ว่าจะขอใช้บริการเว็บหรือ mail ที่ได้ตั้ง Server ไว้ให้บริการภายในหน่วยงานหรือองค์กรของเรา ที่ติดตั้งอยู่บน Private IP Address ขณะที่ packet ส่งการร้องขอมายัง Firewall จะถูกเปลี่ยน Address ปลายทาง (Destination Address) ไปยัง local server ที่บริการนั้น ๆ พร้อมกับส่ง packet ไปให้ด้วย เมื่อมีการตรวจสอบตาม rule ที่ตั้งไว้ถูกต้องจะมีการส่ง packet ออกจาก local server กลับออกไปยัง Firewall จากนั้น Firewall จะทำหน้าที่เปลี่ยน Source Address ที่เป็น Private IP กลับเป็น Public IP Address ของเครื่อง Firewall แล้วส่ง packet ออกไปให้กับ Remote Client ต่อไป ทำได้โดยการสร้าง Script ด้วย iptables ตัวอย่างนี้เป็นการ forward ไปยัง web server ถ้าต้องการให้บริการอื่น ๆ ก็ให้เปลี่ยน port ให้ตรงกับการใช้งานจริง

```
iptables -t nat -A PREROUTING -i <public interface> -p tcp \
    --sport 1024:65535 -d <public address> --dport 80 \
    -j DNAT --to-destination <local web server>
```

มักมีคำถามที่ยากในการอธิบายเสมอว่า ที่บอกว่า NAT ทำหน้าที่เปลี่ยน Address นั้นเปลี่ยนในขั้นตอนไหน คำตอบก็คือ DNAT จะเริ่มทำการเปลี่ยนค่า Address ให้ตั้งแต่ก่อนจะส่ง packet ไปให้ forward chain ดังนั้นจึงต้องทำการสร้าง rule ให้กับ forward chain ให้ส่งค่าไปยัง Server ที่อยู่ใน Private IP ให้สอดคล้องกันกับ Address ของ Public IP Address บน firewall ตามตัวอย่าง

```
iptables -A FORWARD -i <public interface> -o <DMZ interface> -p tcp \
    --sport 1024:65535 -d <local web server> --dport 80 \
    -m state --state NEW -j ACCEPT
```

การที่ Server จะส่ง packet กลับออกไปสู่ Internet ได้สมบูรณ์นั้นต้องมีการกำหนด forward rule ให้ ACCEPT การเชื่อมต่อตั้งแต่ต้นเสียก่อนจึงจะทำงานได้ดังตัวอย่าง

```
iptables -A FORWARD -i <DMZ interface> -o <public interface>\
    -m state --state ESTABLISHED,RELATED -j ACCEPT
```

อย่างไรก็ตามต้องไม่ลืมในส่วนของ Remote Client ต้องทำการ forward ค่าที่สมบูรณ์ครบถ้วนไปให้ Server ด้วยเหมือนกัน ต้องกำหนดให้ ACCEPT เฉพาะ NEW state ให้ส่งต่อไปยัง rule ทั้งหมดที่เชื่อมต่อได้สำเร็จ (ESTABLISHES หรือ RELATED state) ดังตัวอย่าง

```
iptables -A FORWARD -i <public interface> -o <DMZ interface>
    -m state --state ESTABLISHED,RELATED -j ACCEPT
```

สรุปก็คือในการทำแบบที่ 1 นี้ต้องสร้าง Script ให้ครบทั้ง 5 บรรทัด จึงจะสามารถทำงานได้อย่างครบถ้วนสมบูรณ์ (เฉพาะตัวอย่างนี้เป็น Web Server อย่างเดียวเท่านั้น)

2. **Host Forwarding and Port Redirection** สำหรับแบบนี้เป็นตัวอย่างที่ DNAT ไม่สามารถทำหน้าที่เปลี่ยนแปลง Destination port ได้เหมือนกับ Address ถ้าต้องการให้ทำการเปลี่ยนทั้ง Address และ Port ปลายทาง ต้องทำการสร้าง script กำหนดให้ NAT มี 2 rules เช่น port ที่ Remote Client ร้องขอมาเป็น port 80 โดยปกติทั่วไป server จะส่งค่ากลับที่ port 80 ด้วยจะมีผลเรื่องของ traffic เมื่อมีการให้บริการเป็นจำนวนมาก จึงมีการออกแบบให้การตอบกลับหรือส่ง packet ของ server เปลี่ยนเป็นหมายเลขอื่นแทน เช่นตัวอย่างนี้ส่งค่ากลับด้วย port 81 แล้วทาง firewall จะทำการ match เพื่อเปลี่ยนเป็น port 80 ส่งให้กับ Client ต่อไปดังตัวอย่าง

```
iptables -t nat -A PREROUTING -i <public interface> -p tcp \
    -s <allowed remote host> --sport 1024:65535 \
    -d <public address> --dport 80 \
    -j DNAT --to-destination <local web server>:81
iptables -t nat -A PREROUTING -i <public interface> -p tcp \
    --sport 1024:65535 -d <public address> --dport 80 \
    -j DNAT --to-destination <local web server>
```

หลังจากทำ NAT เสร็จแล้วต้องไม่ลืมที่จะ forward packet จาก server ที่ port 81 ไปยัง firewall ที่เป็น Public IP ให้เปลี่ยนกลับเป็น port 80 ส่งค่าไปยัง client ต่อไป

```
iptables -A FORWARD -i <public interface> -o <DMZ interface> -p tcp --sport 1024:65535 -d
<local web server> --dport 81 \
    -m state --state NEW -j ACCEPT
iptables -A FORWARD -i <public interface> -o <DMZ interface> -p tcp --sport 1024:65535 -d
<local web server> --dport 80 \
    -m state --state NEW -j ACCEPT
```

อย่างไรก็ตามต้องไม่ลืมในส่วนของ Remote Client ต้องทำการ forward ค่าที่สมบูรณ์ครบถ้วนไปให้ Server ด้วยเหมือนกัน ต้องกำหนดให้ ACCEPT เฉพาะ NEW state ให้ส่งต่อไปยัง rule ทั้งหมดที่เชื่อมต่อได้สำเร็จ (ESTABLISHES หรือ RELATED state) เหมือนตัวอย่างในข้อ 1 แต่ต้องทำ 2 rule ให้ครบ ดังนี้

```
iptables -A FORWARD -i <DMZ interface> -o <public interface>\
        -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i <public interface> -o <DMZ interface>\
        -m state --state ESTABLISHED,RELATED -j ACCEPT
```

3. **Host Forwarding to a Server Farm** แบบนี้เป็นตัวอย่างในการใช้ DNAT ให้สามารถรับค่า Destination IP Address ได้หลาย IP เช่น 192.168.2.1-192.168.2.5 แบบนี้จะมีประโยชน์มากกับระบบงานที่ให้บริการลูกข่ายจำนวนมาก ๆ ในเวลาพร้อม ๆ กันเช่นการทำ e-auction หรือกรณีที่เป็นเว็บสำคัญต้องมีผู้เข้าดูพร้อม ๆ กันจำนวนมาก ๆ เพราะ server แต่ละเครื่องจะมีการจำกัดการเข้าใช้ (Max connection) ไว้ถ้าต้องการแก้ปัญหาต้องตั้ง server หลาย ๆ เครื่อง (Server Farm) ที่ทำงานและหน้าที่เดียวกันเช่นตัวอย่างนี้ตั้งไว้ 5 เครื่อง แล้วให้ใช้ความสามารถของ DNAT จัดการรับส่งค่าให้ Server แต่ละตัว บางครั้งก็เรียกวิธีการนี้ว่า Load Balance ดังตัวอย่าง

```
iptables -t nat -A PREROUTING -i <public interface> -p tcp \
        --sport 1024:65535 -d <public Web address> --dport 80 \
        -j DNAT --to-destination 192.168.2.1-192.168.2.5
iptables -A FORWARD -i <public interface> -o <DMZ interface> -p tcp --sport 1024:65535 -d
192.168.2.0/29 --dport 80 \
        -m state --state NEW -j ACCEPT
iptables -A FORWARD -i <DMZ interface> -o <public interface>\
        -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i <public interface> -o <DMZ interface>\
        -m state --state ESTABLISHED,RELATED -j ACCEPT
```

4. ตัวอย่างในข้อนี้เหมาะสำหรับหน่วยงานที่ได้จัดสรร Public IP Address 8 เบอร์ ให้นำไปออกแบบ firewall ที่ติดตั้ง server บน Private IP Address 5 IP ตามจำนวน IP ที่เหลือดังตัวอย่างในตารางต่อไปนี้

ตารางที่ 1. การออกแบบ Firewall ที่มี 8 IP Addresses	
ADDRESS BLOCK	IP ADDRESS
Network Address	203.254.25.80/29
Network Mask	255.255.255.248

ตารางที่ 1. การออกแบบ Firewall ที่มี 8 IP Addresses	
ADDRESS BLOCK	IP ADDRESS
Router Address	203.254.25.81
Firewall/DNS Address	203.254.25.82
First Host Address	203.254.25.83
Last Host Address	203.254.25.86
Broadcast Address	203.254.25.87
Total Local Hosts	5

ตารางที่ 2. Logical Mapping ระหว่าง Public and Private Server Addresses		
SERVER	PUBLIC ADDRESS	PRIVATE DMZ ADDRESS
Public Web Server(80)	203.254.25.83	192.168.1.3
Customer Web Server(443)	203.254.25.84	192.168.1.4
FTP Server(21)	203.3254.25.85	192.168.1.5
Mail Server(25)	203.254.25.86	192.168.1.6

```
iptables -t nat -A PREROUTING -i <public interface> -p tcp \
        --sport 1024:65535 -d $PUBLIC_WEB_SERVER --dport 80 \
        -j DNAT --to-destination $DMZ_PUBLIC_WEB_SERVER
iptables -t nat -A PREROUTING -i <public interface> -p tcp \
     --sport 1024:65535 -d $CUSTOMER_WEB_SERVER  \
     --dport 443 -j DNAT –to-destination \
     $DMZ_CUSTOMER_WEB_SERVER
iptables -t nat -A PREROUTING -i <public interface> -p tcp \
```

```
    --sport 1024:65535 -d $FTP_SERVER --dport 21 \
    -j DNAT --to-destination $DMZ_FTP_SERVER
iptables -t nat -A PREROUTING -i <public interface> -p tcp \
    --sport 1024:65535 -d $MAIL_SERVER --dport 25 \
    -j DNAT --to-destination $DMZ_MAIL_SERVER
iptables -A FORWARD -i <public interface> -o <DMZ interface>\
    -p tcp --sport 1024:65535 -d $DMZ_PUBLIC_WEB_SERVER \
    --dport 80 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i <public interface> -o <DMZ interface>\
-p tcp --sport 1024:65535 -d $DMZ_CUSTOMER_WEB_SERVER\
--dport 443 -m state --state NEW -j ACCEPT
iptables -A FORWARD -i <public interface> -o <DMZ interface>\ -p tcp --sport 1024:65535 -d
$DMZ_FTP_SERVER --dport 21 \
    -m state --state NEW -j ACCEPT
iptables -A FORWARD -i <public interface> -o <DMZ interface>\ -p tcp --sport 1024:65535 -d
$DMZ_MAIL_SERVER --dport 25 \
    -m state --state NEW -j ACCEPT
iptables -A FORWARD -i <DMZ interface> -o <public interface>\
    -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i <public interface> -o <DMZ interface>\
    -m state --state ESTABLISHED,RELATED -j ACCEPT
```

5. **Local Port Redirection Transparent Proxy** ตัวอย่างสุดท้ายในการใช้ nat table ทำหน้าที่ Redirect port ให้กับ Transparent Proxy ที่นิยมใช้งานกันตามหน่วยงานหรือองค์กรต่าง ๆ แต่ตัวอย่างนี้เป็นการเขียน Script ให้กับ Proxy Server ที่ติดตั้งอยู่บน Private IP Address ทำงานร่วมกับ Firewall Server ซึ่งอาจไม่เหมือนกับผู้ที่ติดตั้ง Proxy Server ไว้บน Public IP Address ดูรูปแบบ script ดังตัวอย่างต่อไปนี้

```
iptables -t nat -A PREROUTING -i <lan interface> -p tcp \
    -s <lan hosts> --sport 1024:65535 --dport 80 \
    -j REDIRECT --to-port 8080
iptables -A INPUT -i <lan interface> -p tcp \
    -s <lan hosts> --sport 1024:65535 -d <lan address> \
   --dport 8080 -m state --state NEW,ESTABLISHED,RELATED \
```

```
    -j ACCEPT
iptables -A OUTPUT -o <public interface> -p tcp \
        -s <public address> --sport 1024:65535 --dport 80 \
-m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i <public interface> -p tcp \
        --sport 80 -d <public address> --dport 1024:65535  \
        -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -o <lan interface> -p tcp \
        -s <lan address> --sport 80 --dport 1024:65535 \
        -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Tip & Tricks

ในการใช้งาน iptables เพื่อทำ Firewall นอกจากจะป้องกันแต่ละ Service ใน Server แล้วยังป้องกันกลุ่มที่ต้องการ Scan port แต่ละชนิดเพื่อหาช่องทางทำให้ Service หยุดทำงาน (Denial of Service) ด้วยการปล่อย packet ออกมาพร้อม ๆ กันทำให้ Service รองรับการทำงานของ Process ที่เกิดขึ้นในเวลาเดียวกันจำนวนมาก ๆ ไม่ได้จึงหยุดทำงานลักษณะการถูกโจมตีแบบนี้เรียกกันอีกอย่างหนึ่งว่า syn-flood ผู้ดูแลระบบสามารถใช้ iptables ป้องกันได้ดังตัวอย่างต่อไปนี้

```
EXT_IF=eth0                 <- Public IP Address
INT_IF=eth1                 <- Private IP Address
DEST_IP=xxx.xxx.xxx.xxx     <- ค่า ip address ของ server
$IPTS -t nat -N syn-flood
$IPTS -t nat -A syn-flood -m limit --limit 12/s --limit-burst 24 \
-j RETURN
$IPTS -t nat -A syn-flood -j DROP
$IPTS -t nat -A PREROUTING -I $EXT_IF -d $DEST_IP -p tcp \
--syn -j syn-flood
```

หลักการใช้ nat table จึงถูกนำไปใช้ในการทำ Transparent Proxy เพราะสามารถบังคับให้ลูกข่ายกลุ่ม Private IP Address ที่กำลังจะออกไปขอใช้บริการ Port 80 ต้องถูกเปลี่ยนทิศทาง (REDIRECT) ให้วิ่งไปที่ port 8080 ดังตัวอย่างนี้

```
$IPTS -t nat -A PREROUTING  -i $INT_IF -p tcp --dport 80 \
-j REDIRECT --to-port 8080
```

อีกรูปแบบหนึ่งที่ต้องมีการป้องกันคือ Xmas scan และการส่ง Null packet จากภายนอกซึ่งการโจมตีแบบนี้ไม่ค่อยมีใครสนใจที่จะป้องกันให้ทำตามตัวอย่างต่อไปนี้

```
$IPTS -t nat -A PREROUTING -p tcp --tcp-flag ALL ALL -j DROP
$IPTS -t nat -A PREROUTING -p tcp --tcp-flag ALL NONE \
-j DROP
```

ตรงนี้สำคัญมากเพราะเป็นการใช้งาน iptables ขั้นสูงเท่าที่ดูในการใช้งานกันทั่วๆ ไปยังไม่เคยมีใครทำกันแม้แต่ในคู่มือ iptables ก็ไม่มีแนะนำอาจเป็นเพราะต้องมีการ Patch ทั้ง kernel และในส่วนของ iptables ไปดูรายละเอียดและ Download ได้จาก http://www.netfilter.org/ ให้ทำงานร่วมกับ psd patch เมื่อมีการ patch เสร็จแล้ว iptables จะมี command option ในส่วนของ -m เพิ่มขึ้นอีกอย่างคือ -m psd ใช้ประโยชน์ในการป้องกันการ Scan port ดังตัวอย่างต่อไปนี้

```
$IPTS -t nat -A PREROUTING -i $EXT_IF -d $DEST_IP -m psd \
-j DROP
```

หรือถ้ามีการนำ iplimit patch มาใช้ก็จะเพิ่มความสามารถให้กับ iptables ในการจำกัดจำนวน IP Address ที่ยอมให้ Connected ได้พร้อม ๆ กันจำนวนเท่าใด ดังตัวอย่างต่อไปนี้อนุญาตให้ Connected ได้พร้อมกันสูงสุด 16 IP Address

```
$IPTS -t nat -A PREROUTING -i $EXT_IF -p tcp --syn \
-d $DEST_IP -m iplimit --limit-above 16 -j DROP
```

จากสองตัวอย่างข้างบนที่ใช้ psd และ iplimit คงต้องศึกษาการ compile ใหม่ที่ค่อนข้างยุ่งยาก ถ้าคอยติดตามการทดลองของ netfilter จะพบว่ามี patch ออกมาให้ใช้งานมากมายมีการปรับปรุงล่าสุดอยู่ในชื่อ patch-o-matic-ng ยกตัวอย่างเมื่อปี ค.ศ. 2004 ตอนที่ไวรัส CodeRed ระบาดผ่านเว็บ ทาง netfilter ได้ออก string-matching patch มาช่วยในการป้องกัน CodeRed และ Nimda virus ดังตัวอย่างต่อไปนี้

```
$IPTS -A INPUT -i $EXT_IF -p tcp -d DEST_IP --dport 80 \
-m string --string "/default.ida?" -j DROP
$IPTS -A INPUT -i $EXT_IF -p tcp -d DEST_IP --dport 80 \
-m string --string ".exe?/c+dir" -j DROP
$IPTS -A INPUT -i $EXT_IF -p tcp -d DEST_IP --dport 80 \
-m string --string ".exe?/c_tftp" -j DROP
```

จะเห็นได้ว่า netfilter ได้พัฒนาติดตามการเปลี่ยนแปลงการบุกรุกทุกรูปแบบมาตั้งแต่ต้นจนปัจจุบัน แต่ผู้เขียนยังไม่เห็นผู้ดูแลระบบคนไหนนำประโยชน์ต่างๆ เหล่านี้มาประยุกต์ใช้งานกันเลย iptables Version 1.3.x ขึ้นไป ก็ได้รวมเอา String-matching patch ไว้ให้ใช้เรียบร้อยแล้ว ผู้ที่ควบคุมระบบยังพยายามมองหาสิ่งอำนวยความสะดวกอย่างอื่นๆ ไปใช้งานกันอีก เช่นตัวอย่างง่ายๆ สำหรับคำถามที่พบบ่อยกับผู้ทำ Internet Server ปัจจุบันคือ "จะป้องกันการ Download พวก bit torrent ได้อย่างไร" ผู้เขียนลองคิดดูหลายครั้ง ไปอ่านดูตามเว็บบอร์ด ก็เห็นให้ไปหาโปรแกรมควบคุมการใช้งาน P2P อะไรไปติดกันบ้าง ป้องกันโดยการปิด port บ้าง ก็มีคนเขียนกันไว้ว่าใช้ไม่ได้หรือไม่ได้ผล สาเหตุต่างๆ เหล่านี้มันเกิดจากเมื่อมีการนำเอา module ที่มีผู้พัฒนาให้ในเว็บมาใส่ใน Server ของเรา บางครั้งการทำงานมันอาจไม่ตรงก็จะสั่งงานเหมือนที่เขาอธิบายไว้ไม่ได้ หรือบางครั้งโปรแกรมพวก bit torrent มีการ Random Port ได้ตลอดจึงไม่สามารถใช้วิธีปิด port ได้ แต่ถ้าลองดูความสามารถของ iptables ที่เราใช้ทำ Firewall น่าจะนำมาประยุกต์อะไรได้มากมาย ปัจจุบันได้มีการทำ patch แบบที่ไม่น่าจะทำได้มาให้ใช้กันแล้วคือ L7 หรือ Layer 7 ซึ่งเป็นการควบคุมระดับ Application Layer เช่นถ้าต้องการไม่ให้ลูกข่ายใช้ MSN ก็ไม่ต้องไปถามใครว่ามันใช้ port เบอร์อะไร ก็สามารถสั่ง DROP โปรแกรม Messenger ได้เลยแบบนี้คงถูกใจคนควบคุมระบบเป็นแน่ ดูตัวอย่างการใช้งานต่อไปนี้

```
#Block portscan กรณีมี psd patch
#-----------------------------------------
iptables -A INPUT -p tcp -m psd -j DROP
#Block MSN กรณีมี l7 patch
#-----------------------------------------
iptables -A FORWARD -m layer7 --l7proto messenger -j DROP
#Block math string แบบนี้ใช้ได้เลยใน Version ปัจจุบัน
#-----------------------------------------
iptables -A FORWARD -m string –string “.torrent” --algo bm \
-j DROP
```

เห็นตัวอย่างข้างบนกันแล้วคงมีประโยชน์กันบ้างไม่มากก็น้อยสำหรับการใช้ string matching สามารถใช้เป็นค่าตัวเลขฐานสิบหกได้โดยใช้ --hex-string เพื่อป้องกันไวรัสใหม่ๆ ที่มีการเปิดเผย Code ในเว็บ Antivirus ใครสนใจจะ Compile patch Layer7 ใช้กันเองให้ไปดูรายละเอียดได้ที่ http://under-linux.org/ หรือดูข้อมูลพร้อม download ได้ที่ http://l7-filter.sourceforge.net/ ตัวอย่างสุดท้ายคือสิ่งที่ชอบใช้กันอยู่แล้วคือเรื่องการทำ Port Forward ด้วย Command Option DNAT (Destination NAT)

```
$IPTS -t nat -A PREROUTING ! -i $INT_IF -p tcp --dport-port 80 \
-j DNAT --to 100.0.0.5:80
```

ถ้าทำ Port forward ไปยัง Server ที่เป็น Private IP เวลาจะทำการป้องกัน virus ต้องใช้ FORWARD chain แบบนี้

```
$IPTS -A FORWARD -p tcp --dport 80 -m string \
--string "/default.ida?" --algo bm -j DROP
```

ตัวอย่าง firewall สำหรับ log server

```
#/bin/sh

#chkconfig: 345 60 95
#description: Create script by Mr.Boonlue Yookong, 2008.
/sbin/modprobe ip_tables
/sbin/modprobe ip_conntrack_ftp

# Declare Variable
IPTS="/sbin/iptables"

# Flush old rules, old custom tables
$IPTS -F
$IPTS -F -t nat
$IPTS -X
$IPTS -P INPUT DROP
$IPTS -P FORWARD DROP
$IPTS -P OUTPUT DROP
$IPTS -A INPUT  -i lo -j ACCEPT
$IPTS -A OUTPUT -o lo -j ACCEPT
$IPTS -A INPUT -s 255.0.0.0/8 -j LOG --log-prefix "Spoofed source IP!"
$IPTS -A INPUT -s 255.0.0.0/8 -j DROP
$IPTS -A INPUT -s 0.0.0.0/8 -j LOG --log-prefix "Spoofed source IP!"
$IPTS -A INPUT -s 0.0.0.0/8 -j DROP
$IPTS -A INPUT -s 127.0.0.0/8 -j LOG --log-prefix "Spoofed source IP!"
$IPTS -A INPUT -s 127.0.0.0/8 -j DROP
# ถ้าไม่ใช้กลุ่ม ip 192.168 ก็ให้ลบเครื่องหมาย # หน้า 2 บรรทัดต่อไปนี้ออก
```

#$IPTS -A INPUT -s 192.168.0.0/16 -j LOG --log-prefix "Spoofed source IP!"

#$IPTS -A INPUT -s 192.168.0.0/16 -j DROP

$IPTS -A INPUT -s 172.16.0.0/12 -j LOG --log-prefix " Spoofed source IP!"

$IPTS -A INPUT -s 172.16.0.0/12 -j DROP

$IPTS -A INPUT -s 10.0.0.0/8 -j LOG --log-prefix " Spoofed source IP!"

$IPTS -A INPUT -s 10.0.0.0/8 -j DROP

$IPTS -A INPUT -s 208.13.201.2 -j LOG --log-prefix "Spoofed Woofgang!"

$IPTS -A INPUT -s 208.13.201.2 -j DROP

$IPTS -A INPUT -p tcp ! --syn -m state --state NEW \

-j LOG --log-prefix "Stealth scan attempt?"

$IPTS -A INPUT -p tcp ! --syn -m state --state NEW -j DROP

$IPTS -A INPUT -j ACCEPT -m state --state ESTABLISHED,RELATED

Accept inbound packets which initiate SSH sessions

$IPTS -A INPUT -p tcp -j ACCEPT --dport 22 -m state --state NEW

Accept client inbound packets which initiate NTP sessions

**$IPTS -A INPUT -s x.x.x.x/x.x.x.x -p udp -j ACCEPT -m state **

--state NEW -m udp --sport 123

ควรกำหนดค่า IP Address และ netmask (**x.x.x.x/x.x.x.x**) เพื่อป้องกัน IP ที่ไม่ต้องการเข้าใช้ NTP server

Accept inbound packets which initiate Syslog-ng (UDP) sessions

**$IPTS -A INPUT -s 192.168.1.0/255.255.255.0 -p udp -j ACCEPT -m state **

--state NEW -m udp --dport 514

Accept inbound packets which initiate Syslog-ng (TCP) sessions

**$IPTS -A INPUT -s 192.168.1.0/255.255.255.0 -p tcp -j ACCEPT -m state **

--state NEW -m tcp --dport 514

Log anything not accepted above

$IPTS -A INPUT -j LOG --log-prefix "Dropped by default:"

$IPTS -I OUTPUT 1 -m state --state RELATED,ESTABLISHED -j ACCEPT

```
# Accept inbound packets which ping sessions
$IPTS -A INPUT -p icmp -j ACCEPT --icmp-type echo-request
$IPTS -A OUTPUT -p icmp -j ACCEPT --icmp-type echo-request
$IPTS -A OUTPUT -j LOG --log-prefix "Dropped by default:"
```

การนำไปใช้งาน ให้ทำการสร้างหรือคัดลอก script นี้ไปไว้ใน /etc/init.d แล้วให้ทำการเปลี่ยน permission file ดังนี้

```
# chmod 700 /etc/init.d/firewall
# chkconfig firewall on
# chkconfig iptables off
# /etc/init.d/firewall
```

ตัวอย่างการเขียน Firewall

เพื่อส่งค่า Log ของ IM ไปเก็บเพื่อใช้เปรียบเทียบกับ imspector

```
*nat
-A POSTROUTING -p tcp --dport 1863 -m limit --limit 5/min -j LOG --log-prefix "MSN: " --log-level WARN
-A POSTROUTING -p tcp --dport 5190 -m limit --limit 5/min -j LOG --log-prefix "ICQ/AIM: " --log-level WARN
-A POSTROUTING -p tcp --dport 5050 -m limit --limit 5/min -j LOG --log-prefix "Yahoo: " --log-level WARN
-A POSTROUTING -p tcp --dport 6667 -m limit --limit 5/min -j LOG --log-prefix "IRC: " --log-level WARN
```

ตัวอย่างการเขียน Firewall เพื่อ Redirect IM ไปยัง Transparent proxy

MSN:

```
iptables -t nat -A PREROUTING -p tcp --destination-port 1863 \
-j REDIRECT --to-ports 16667
```

ICQ/AIM:

```
iptables -t nat -A PREROUTING -p tcp --destination-port 5190 \
-j REDIRECT --to-ports 16667
```

Yahoo:

```
iptables -t nat -A PREROUTING -p tcp --destination-port 5050 \
-j REDIRECT --to-ports 16667
```

IRC:

```
iptables -t nat -A PREROUTING -p tcp --destination-port 6667 \
-j REDIRECT --to-ports 16667
```

บทสรุป

ในการทำ Firewall ให้กับ log server มีความจำเป็นและสำคัญเป็นอย่างยิ่งเพราะจะต้องใช้เป็นหลักเกณฑ์ในการชี้แจงรายการในส่วนของการรักษาความปลอดภัยให้กับข้อมูลจราจรเครือข่ายคอมพิวเตอร์ที่เก็บใน Centralized log server ซึ่งหากมีการกำหนดค่าในการใช้งานผิดพลาดหรือไม่ครบถ้วน ก็จะส่งผลเสียคือไม่สามารถทำงานได้สมบูรณ์หรืออาจทำให้ระบบทำงานช้าลง เพราะมีการส่งค่าวนไปมาหรือหาทางออกไม่ได้ ผู้ดูแลระบบควรศึกษาเปรียบเทียบกับตัวอย่าง Script ที่มีมาให้ดูในบทนี้เพื่อประกอบการใช้งานให้เหมาะสมแต่ในส่วนท้ายบทผู้เขียนได้ทำตัวอย่าง Script เพื่อให้สามารถคัดลอกนำไปใช้งานได้ทันทีแต่ต้องไม่ลืมเปลี่ยนค่า IP Address และหมายเลข Port ของ Syslog-ng ให้ตรงกับการใช้งานจริงด้วย และที่สำคัญอย่างยิ่งต้องทำการยกเลิกการใช้งาน iptables ในระบบก่อนจากนั้นให้นำ Script ไปใส่ใน /etc/init.d ก็สามารถ chkconfig firwall on ทำให้ทำงานทุกครั้งที่เครื่อง boot เหมือน service อื่น ๆ ทั่วไป

บทที่ 8

Backup and Restore

การติดตั้งและใช้งานโปรแกรม

ปัจจุบันมีผู้เขียนหนังสือเกี่ยวกับ Server มากมายให้คนไทยได้อ่านและนำไปใช้งาน แต่ไม่เห็นผู้เขียนเหล่านั้นสนใจเรื่องการ Backup/Restore ข้อมูลใน Server ทั้ง ๆ ที่ ข้อมูลต่าง ๆ ที่เก็บอยู่ใน Server ล้วนมีความสำคัญและเป็นสาระที่หายาก บางหน่วยงานสะสมข้อมูลตามกำหนดระยะเวลา แต่กลับสนใจกันแต่จะซื้อเครื่อง Server ดี ๆ เลือก NOS ดี ๆ หรือที่ตนชอบ ไม่เห็นคิดถึงเรื่องความเสียหายเมื่อวันหนึ่ง Server มีปัญหาไม่สามารถเรียกหาข้อมูลในส่วนที่ต้องการได้ ยิ่งบางหน่วยงานให้งบประมาณมากมายในการซื้อเครื่องแม่ข่าย เครื่องลูกข่าย แต่ไม่เคยเขียนของบประมาณจัดซื้อเครื่องสำรองข้อมูล คงมองข้ามกันไปยกใหญ่ ส่วนมากผู้เขียนเห็นแต่เน้นการจัดซื้อเครื่องสำรองไฟฟ้า (UPS) กันมากกว่า

ชนิดของการ backup สามารถแบ่งออกได้ 6 ชนิดดังนี้

1. Full backup เป็นการทำ backup หมดทุกอย่าง
2. Incremental backup เป็นการทำ backup ทุกอย่างที่เปลี่ยนแปลงหลังจากทำ Full backup
3. Differential มีหลักการคล้ายกับแบบที่สองต่างกันตรงชื่อเรียก
4. Network backup ใช้สำหรับการ backup ข้อมูลจาก client ไปยัง backup server เพื่อให้ Server ทำการ backup สื่อ
5. Dump backup ไม่ใช่เป็นการ backup file ตามปกติ แต่จะทำการ backup ได้ทั้งไฟล์และรวม disk partition หรือ file system ไปด้วย
6. Level 0 to 9 backup เป็นการทำ incremental backup อย่างละเอียดทุกอย่างที่มีการเปลี่ยนแปลงเรียกอีกอย่างว่า lower lever backup

ความเร็วในการ backup และ Restore จะขึ้นอยู่กับปริมาณข้อมูลและวิธีการ backup เช่นถ้าข้อมูลมีจำนวนมาก ๆ เป็นหลายร้อย Gigabyte ก็จำเป็นต้องใช้เวลา backup นานและยิ่งถ้ามีการทำ backup ผ่าน Network ก็จะยิ่งใช้เวลามากขึ้นอีกตามขนาด Bandwidth ที่ใช้ในระบบ ในการวางแผนที่ดีสำหรับ backup ข้อมูลควรคำนึงถึงกรณีเมื่อเกิดเหตุ Hard drive failure ข้อมูลที่ใช้งานตั้งแต่ต้นจนถึงล่าสุดจะเกิดความเสียหายทั้งหมด ดังนั้นน่าจะมีการทำ backup บ่อย ๆ ให้ลองพิจารณาการวางแผนจากองค์ประกอบดังต่อไปนี้

1. ปริมาณข้อมูลที่จะทำการ backup
2. ข้อมูลมีการเปลี่ยนแปลงบ่อยด้วยวิธีการใด
3. ความเป็นไปได้ในการ Restore ข้อมูลจำนวนมาก ๆ
4. ระยะเวลาที่ Server จะหยุดให้บริการได้
5. ข้อมูลอะไรที่มีการเปลี่ยนแปลงบ่อยที่สุด

หลังจากทำการเรียบเรียงองค์ประกอบต่าง ๆ ที่เกี่ยวข้องเสร็จแล้ว ก็สรุปเป็นแนวคิดใหม่ นำมาจัดกลุ่มของข้อมูลตามลักษณะการเปลี่ยนแปลงได้เป็นสาม กลุ่ม คือ

1. ข้อมูลที่ไม่ค่อยมีการปรับปรุง
2. ข้อมูลที่มีการปรับปรุงเป็นประจำ
3. ข้อมูลที่มีการปรับปรุงตามช่วงเวลาที่กำหนด

หลังจากนั้นให้พิจารณาดูว่า Directory ใดที่ต้องมีการทำ backup ไม่จำเป็นต้อง backup หมดทั้ง hard drive เพราะจะใช้เวลามากเกินไป ไม่มีใครเขาทำกัน ให้ดูจากตัวอย่างตามนี้

/etc เป็นที่เก็บ Configuration file

/home เป็นที่เก็บข้อมูลของ User

/www เป็นที่เก็บข้อมูลเกี่ยวกับ Web file (อาจมีชื่อ dir อื่นก็ได้)

ต่อไปเป็นการพิจารณาเลือกสื่อ (Media) ที่จะใช้จัดเก็บข้อมูลที่ทำการ backup เมื่อมีการแบ่งกลุ่มตามการเปลี่ยนแปลงข้อมูลได้แล้ว สื่อที่จะใช้เก็บก็จะสามารถเลือกให้เกิดความประหยัดได้ บางหน่วยงานไม่มีงบประมาณที่จะจัดซื้ออุปกรณ์ราคาแพงเช่น Tape backup ก็สามารถใช้สื่อที่หาง่ายเช่น CD หรือ DVD ที่ปัจจุบันมีราคาถูกกว่า Floppy Disk สมัยก่อนเสียอีก โดยเฉพาะเครื่องบันทึก CD หรือ DVD ก็มีราคาถูกเกือบเท่า Floppy Drive ในอดีตอีกเช่นกัน คงเป็นทางเลือกให้กับผู้ดูแลระบบในแต่ละหน่วยงานหรือองค์กรได้นำไปใช้งานจริง ดังต่อไปนี้

กลุ่มที่ 1 ข้อมูลไม่ค่อยมีการปรับปรุง ในกลุ่มนี้ได้แก่ /etc เนื่องมาจากค่า Configure จะมีการแก้ไขเพียงหลังติดตั้งโปรแกรมเพียงครั้งเดียว แล้วให้ server ทำงานให้บริการไปเป็นระยะเวลานาน จะมีการปรับปรุงค่า Configure อีกครั้งก็ต่อเมื่อมีการ Update โปรแกรมเท่านั้น จึงควรเลือกสื่อที่ใช้บันทึกแบบความจุต่ำและมีความเร็วในการทำงานไม่สูงเช่น ZIP Disk ถ้าแพงไปอาจเก็บใน CD-R ก็ได้ การเก็บ /etc ส่วนนี้มีความสำคัญมากเพราะมีการเก็บข้อมูลของ User คือไฟล์ passwd และ shadow เป็นข้อมูลที่ต้องทำการ Restore ก่อนเป็นอันดับแรก เพราะจะมีผลกับข้อมูลในส่วนอื่น ๆ ที่ User ได้ทำการบันทึกหรือมีไว้ใช้งาน ถ้า Restore ภายหลังข้อมูลอื่นอาจส่งผลให้การทำงานของข้อมูลผิดพลาดได้

ส่วน Directory ที่ดูเหมือนจะมีการเปลี่ยนแปลงน้อยเหมือนกันแต่คนทั่วโลกไม่นิยมทำการ backup กันก็คือ /bin และ /usr เพราะเป็นส่วนของตัวโปรแกรม เมื่อมีปัญหาใช้วิธีติดตั้งใหม่เร็วกว่าการ backup/restore เพราะเราได้ทำการเก็บค่า Configuration ไว้แล้วนั่นเอง

กลุ่มที่ 2 ข้อมูลปรับปรุงบ่อย ๆ ในกลุ่มนี้คงหนีไม่พ้นข้อมูลหลักของ User และข้อมูลพวก Database ส่วนใหญ่จัดให้เก็บอยู่ใน /home เมื่อข้อมูลมีการเปลี่ยนแปลงทุกวันก็ควรมีการทำ backup ทุกวันเช่นกันและถ้าการ backup ต้องใช้เวลานาน ก็ควรเลือกเวลาในช่วงพักหรือกลางคืน ที่มีการใช้งานน้อยหรือไม่มีการใช้งาน จะ

<u>กลุ่มที่ 3</u> ข้อมูลที่มีการปรับปรุงตามช่วงเวลาที่กำหนด สำหรับข้อมูลกลุ่มนี้ควรพิจารณาให้ลึกลงไปอีกว่าเป็นข้อมูลชุดใดที่มีการปรับปรุงระบุเวลาแน่นอนก็ให้เขียน Script รองรับเฉพาะตอนที่ทำการปรับปรุงพร้อมกันกับการ backup ไปด้วยกันเลย ส่วนข้อมูลที่มีการปรับปรุงตามกำหนดเวลาจากตัวโปรแกรมที่ใช้งานต่าง ๆ ก็ให้ทำการ backup ตามระยะเวลาที่แต่ละโปรแกรมกำหนดไว้

โปรแกรมคำสั่งที่มีไว้สำหรับ backup ข้อมูลใน Linux มาตรฐานทุกค่ายมักเป็นคำสั่งอย่างง่าย ๆที่สามารถใช้ได้ทั้งการ copy และการเก็บรวบรวมข้อมูลจำนวนมาก ๆ มีด้วยกัน 4 คำสั่งคือ

- cp
- tar
- gzip
- dump

ในที่นี้จะยกตัวอย่างการใช้คำสั่ง tar เพราะใช้งานง่ายและเหมือนกับในระบบ UNIX สะดวกในการใช้งานเพียงคำสั่งเดียวสามารถเก็บได้ตั้งแต่ไฟล์เดียวจนถึงหลาย ๆ Directory ใน Linux จัดให้ tar อยู่ในประเภท Utility ที่น่าใช้ตัวหนึ่งที่มีลักษณะการใช้งานที่สามารถเพิ่ม Option ในการเก็บข้อมูลตามความต้องการและสามารถเขียน Script ให้ทำการจัดเก็บตามตารางเวลาที่กำหนดได้สะดวกรวดเร็วอีกด้วยและยังมีคุณสมบัติในการบีบอัดข้อมูล (Compress) ให้มีขนาดไฟล์เล็กลงได้ ดูตัวอย่างรูปแบบการใช้งานดังนี้

 # tar cf backup.tar directory

c = create new file

f = file or device ที่จะจัดเก็บ

เช่น ต้องการ backup /home ให้สั่ง

 # tar cf backup.tar /home

ถ้าต้องการ Restore ให้สั่ง

 # tar xPf backup.tar

ความหมายของ Option ที่จำเป็นต้องใช้มีดังนี้

v = Lists verbosely files being processed.

z = Detects and properly processes gzip archives during extraction.

p = Specifies to extract all protection information.

d = Specifies to find differences between the archive and the file system.

t = Lists the contents of the archive.

u = Specifies to append only files newer than the archive copies.

N date = Specifies to archive only files newer than the specified date.

P = Specifies not to strip the leading / character from file names. In this case, regardless of the directory, from which the extraction command is executed, the files will be extracted into their initial directories.

กรณีต้องการ backup ครั้งเดียวหลาย Directory ก็สามารทำได้ดังนี้

 # tar cf backup.tar /home /etc /www

สามารถตรวจสอบทั้งไฟล์และ Directory ที่เก็บไว้ใน backup.tar ได้ดังนี้

 # tar tvf backup.tar

กรณีต้องการ backup พร้อมกับบีบอัดไฟล์ให้มีขนาดเล็กลงสามารถทำได้โดยให้คำสั่ง tar ไปเรียกใช้คำสั่ง gzip ทำงานร่วมด้วยจะทำให้ไฟล์ที่จัดเก็บมีนามสกุลเป็น .tar.gz ดังนี้

 # tar cfz backup.tar.gz /home /etc /www

และทำการ Restore ด้วยคำสั่ง

 # tar xzPf backup.tar.gz

<u>การรักษาความปลอดภัยให้กับ Backup Media</u>

หากพิจารณาเรื่องความปลอดภัยข้อมูลคงต้องย้อนไปนึกถึงเรื่องการเข้ารหัสกุญแจ ซึ่งโปรแกรมที่ยังนิยมใช้มากที่สุดในปัจจุบันก็คือ OpenSSH มีติดตั้งใน Linux Server ทุกค่ายอยู่แล้วให้นำวิธีการเข้ารหัสกุญแจของโปรแกรมนี้มาช่วยเข้ารหัสไฟล์ที่ทำ backup ไว้ ป้องกันไม่ให้ใครนำไปใช้หรือเปิดดูได้ให้ใช้คำสั่งดังต่อไปนี้

 # openssl des -in /home/backup.tar.gz -out /home/backup.sec

ตัวอย่างนี้สร้างไฟล์ backup.sec หลังจากนั้นให้รีบบันทึกลงสื่อที่เตรียมไว้แล้วทำการลบไฟล์ทั้งสองคือ backup.tar.gz และ backup.sec ออกจากเครื่อง Server และเมื่อต้องการ Restore ก็ให้ใช้คำสั่งปลดรหัสกุญแจดังนี้

 # openssl des -d -in /home/backup.sec -out /home/backup.tar.gz

<u>การใช้คำสั่ง tar ทำการ backup ข้อมูลผ่าน ssh</u>

บางครั้งผู้ดูแลระบบมีความจำเป็นที่ต้องการทำ backup ไปไว้บนเครื่องคอมพิวเตอร์อื่นที่ทำหน้าที่รองรับไฟล์ backup แต่ไม่ได้ให้บริการอื่น ๆ ซึ่งอาจเก็บไว้ใน Hard drive หรืออาจสั่งบันทึกข้อมูลลงบนสื่อต่าง ๆ เช่น CD-R, CD-RW หรือ DVD วิธีการที่จะส่งไฟล์อาจทำได้หลายวิธี แต่ผู้เขียนมักใช้ความรู้เดิม ๆ ที่ผู้ดูแลคุ้นเคยมาประยุกต์ใช้งาน เช่นในหัวข้อนี้เมื่อเรานิยมใช้ Secure Shell ที่มีความปลอดภัยค่อนข้างสูงในการทำงานแบบ Remote Login เราก็น่าจะนำความสามารถนี้มาประยุกต์ใช้ในการ Backup ข้อมูลแล้วส่งไฟล์ไปไว้รวมกันที่เครื่องอื่นจะได้ไม่รบกวนพื้นที่บนเครื่อง Server หลักมีวิธีการที่ไม่ยุ่งยากอะไรเพียงแต่ถ้าทำผิดพลาดอาจเป็นช่องทางที่ผู้ไม่หวังดีเจาะเข้าระบบได้ ทำตามขั้นตอนดังต่อไปนี้

กรณีต้องการที่จะ backup partition /home จากเครื่อง Server ส่งไปยังเครื่อง backup สามารถใช้คำสั่ง tar ร่วมกับ gzip เพื่อบีบให้ไฟล์เล็กลง เสร็จแล้วส่งไปเก็บยังเครื่อง backup สั่งดังนี้

 # tar zcvf - /home | ssh bkuser@backup "cat > /home/bkuser/home.tar.gz"

หรือถ้าไม่ได้กำหนดชื่อ host ก็ต้องใช้เลข IP แทนดังนี้

 # tar zcvf - /home | ssh bkuser@192.168.1.20 "cat > /home/bkuser/home.tar.gz"

ตัวอย่างที่ผ่านมาเครื่อง backup มี IP address 192.168.1.20 มี user ที่รอรับการเก็บไฟล์เป็น user ธรรมดาชื่อ bkuser เพราะในการใช้งาน Secure Shell จะไม่อนุญาตให้ root สามารถ login เข้าระบบได้ เมื่อต้องการส่งไฟล์ไปก็ต้องไม่ลืมว่าส่งไปไว้ที่ home directory ของ bkuser เท่านั้น หลังจากกด Enter จะมีรายการไฟล์ที่อยู่ใน /home แสดงออกมาบนจอภาพ จากนั้นก็จะรอให้กรอก password ของ bkuser เมื่อกรอกรหัสผ่านถูกต้อง ไฟล์ก็จะถูกส่งไปยังเครื่อง backup จนเสร็จสมบูรณ์

หรือถ้าถนัดใช้คำสั่ง dd ก็ไม่ต้องใช้ cat สามารถสั่งได้ดังนี้

 # tar zcvf - /home | ssh bkuser@192.168.1.20 "dd of=/home/bkuser/home.tar.gz"

กรณีที่มีการ mount สื่ออื่นไว้บนเครื่อง backup ก็สามารถส่งไปบันทึกได้เลยเช่น ถ้า mount tape ไว้บน /dev/st0 ก็สามารถส่งไปบันทึกได้ดังนี้

 # tar cvzf - /home | ssh ssh bkuser@192.168.1.20 "cat > /dev/st0"

ถ้าต้องการสั่งหมุนเทปกลับแล้วค่อยบันทึกก็ทำได้ดังนี้

 # tar cvzf - /home | ssh ssh bkuser@192.168.1.20 $(mt -f /dev/st0 rewind; cat > /dev/st0)$

คราวนี้ถ้าต้องการ Restore กลับคืนมาเครื่อง Server ผ่าน ssh ก็ทำได้โดยสั่งดังนี้

 # cd /

 # ssh root@192.168.1.20 "cat /home/bkuser/home.tar.gz" | tar zxvf -

<u>การใช้ SSH ที่ไม่ต้องกรอกรหัสผ่าน</u>

ตัวอย่างที่ผ่านมาทุกครั้งที่ทำการ backup แล้วส่งข้ามเครื่องผ่าน ssh มีความยุ่งยากในการที่ต้องกรอกรหัสผ่านทุกครั้งที่เรียกใช้คำสั่ง ssh เครื่องปลายทางจะถามรหัสผ่านถ้ากรอกผิดก็ไม่สามารถส่งไฟล์ไปเก็บได้ ตัวอย่างในหัวข้อนี้สามารถนำไปใช้ประโยชน์ได้มากมาย สำหรับบทนี้ให้ใช้เพียงการส่งไฟล์ backup ไปเก็บโดยไม่ถามรหัสผ่าน และที่สำคัญคือผู้ดูแลระบบสามารถนำไปเขียน Script ส่งข้อมูลอื่น ๆ ไปเก็บได้อีกด้วย วิธีการทำมีง่าย ๆ ดังนี้

สิ่งแรกที่ควรคำนึงคือบนเครื่อง Server เราต้องเป็น root หรือ user ที่มีสิทธิเทียบเท่า root เพราะจะสามารถทำการใด ๆ บน Hard drive ได้ทุกส่วน ถ้าเป็น user ธรรมดาจะไม่สามารถบุกรุกเข้าในส่วนที่หวงห้ามได้ เช่นถ้าต้องการ backup /etc มีไฟล์ shadow ถ้าเป็น user ธรรมดาก็จะถูกฟ้องว่าอ่านไฟล์ไม่ได้ เริ่มกันเลยในขณะที่อยู่ใน home directory ของ root ให้สั่ง

 # ssh-keygen -t rsa

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id_rsa): <- กด Enter

Enter passphrase (empty for no passphrase): <- กด Enter

Enter same passphrase again: <- กด Enter

Your identification has been saved in /root/.ssh/id_rsa.

Your public key has been saved in /root/.ssh/id_rsa.pub.

The key fingerprint is:

25:70:8f:1e:84:52:9a:45:f6:6d:f3:f3:eb:ce:11:44 **root@sv2.sample.co.th**

#

เป็นการสร้าง rsa key หรือรหัสกุญแจของ root ที่เครื่อง server ชื่อไฟล์ id_rsa และ id_rsa.pub เก็บอยู่ใน .ssh หลังจากสร้างเสร็จให้ทำการส่งค่า id_rsa.pub (public key) ไปไว้ที่เครื่อง backup เอาไว้ตรวจสอบ key ให้ตรงกันระหว่างเครื่องต้นทางกับปลายทาง สั่งดังนี้

 # ssh-copy-id -i .ssh/id_rsa.pub bkuser@192.168.1.20

15

bkuser@192.168.1.20's password: <- กรอก password ของ bkuser

Now try logging into the machine, with "ssh 'bkuser@192.168.1.20'", and check in:

.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.

#

ขั้นตอนนี้ต้องกรอกรหัสผ่านของ bkuser ที่เครื่อง backup ให้ตรงถึงจะส่ง key ไปไว้บนเครื่อง backup ได้สำเร็จโดยจะสร้าง directory ชื่อ .ssh ใน home directory ของ bkuser แล้วบันทึกไฟล์ชื่อ authorized_keys ให้ ถ้าไม่แน่ใจลองไปดูบนเครื่อง backup อีกครั้ง ถ้าพบว่ามีไฟล์ดังกล่าวแล้วแสดงว่าขั้นตอนสร้างรหัสกุญแจทั้งสองเครื่องนี้เสร็จแล้ว ต่อไปให้ตรวจสอบเครื่อง backup ว่าในบริการ ssh มีการทำ configure อะไรไว้สามารถรองรับการส่งไฟล์จาก user ชื่อ bkuser ได้หรือไม่ ให้ไปดูและแก้ไขที่

ตรงนี้ต้อง login ด้วย root เพื่อแก้ configuration บนเครื่อง backup

 # vi /etc/ssh/sshd_config

..... ตรวจสอบดูว่า 3 บรรทัดนี้ต้องไม่มี # ปิดอยู่หน้าบรรทัด

RSAAuthentication yes

PubkeyAuthentication yes

AuthorizedKeysFile .ssh/authorized_keys

ถ้าไม่เหมือนก็จัดการให้เสร็จ บันทึกไฟล์แล้วสั่ง restart

 # /etc/init.d/sshd restart

เพียงเท่านี้ก็พร้อมใช้งานได้ให้ทดลอง login ด้วยคำสั่งนี้

[root@ns1 ~]# ssh bkuser@192.168.1.20

Last login: Tue Jan 15 11:49:28 2008 from 192.168.1.1

[bkuser@backup ~]$

ให้สังเกตดูว่าเครื่องหมาย prompt เปลี่ยนและชื่อ user@host หน้าบรรทัดเปลี่ยนแสดงว่าทำได้สำเร็จสมบูรณ์ ไปใช้คำสั่ง tar ตามตัวอย่างที่ผ่านมาส่งไฟล์ backup.tar.gz ข้ามไปเก็บยังเครื่อง backup ได้เลย ของแถมน่าใช้

ผู้ที่ต้องการทำ backup ลงบน CD-R, CD-RW หรือ DVD ดูตัวอย่างนี้แล้วนำไปทดลองดูว่าสามารถใช้ได้หรือไม่ ถ้าทำได้ก็นำไปรวมกับ Script ตัวอย่างที่เป็น tape เปลี่ยนจาก tape มาเป็น CD จะได้ราคาประหยัด ลองดูวิธีการบันทึกไฟล์ backup ลง CD

ก่อนอื่นที่เครื่อง backup ต้องติดตั้งโปรแกรม cdrecord และ mkisofs ลงไปก่อน จากนั้นย้อนกลับไปดูวิธีที่ทำ backup ด้วยคำสั่ง tar เมื่อส่งไฟล์ home.tar.gz มาที่เครื่อง backup แล้วอาจส่งมาแบบธรรมดาหรืออาจเข้ารหัสด้วย openssh มาแล้วก็ไม่เป็นไรเพราะถือว่าเป็นไฟล์เหมือนกัน ให้ทดลองสั่งดังนี้

ที่เครื่อง backup

$ mkisofs -R -l home.tar.gz | cdrecord speed=8 -

ถ้าเป็น CD-RW ต้องการลบแผ่นก่อนบันทึกให้เพิ่ม

$ mkisofs -R -l home.tar.gz | cdrecord blank=fast speed=8 -

อยากให้บันทึกแล้วดีดแผ่นออกหรือใส่ option อะไรเพิ่มตอนบันทึกให้ลอง man ดูรายละเอียดเอง เพราะเพียงเท่านี้ถ้านำไปต่อ ๆ กันตั้งแต่ต้นจะเห็นได้ว่าสามารถทำ backup ในเครื่อง server เองก็ได้ หรือทำ backup ส่งไปเก็บที่เครื่องอื่นผ่าน ssh ก็ได้แถมยังส่งไปเก็บบนสื่อตามต้องการได้อีกด้วย

การ Backup และ Restore Partition

ในบทนี้จะแนะนำเครื่องมือสำหรับ clone หรือการ copy ได้เป็น partition มีชื่อว่าโปรแกรม partimage มีลักษณะการทำงานบน text mode เป็นเมนูสำเร็จรูป โดยจะเก็บรายละเอียดทั้งหมดตั้งแต่ชนิด ขนาด และข้อมูลที่มีใน partition นั้น ๆ ซึ่งจะมีประโยชน์ในการที่ต้องการจะเปลี่ยน Hard disk ตัวใหม่ไม่ต้องติดตั้งโปรแกรมใหม่สามารถที่จะทำการ backup ได้แม้กระทั่ง MBR ที่ boot partition และที่สำคัญคือสามารถ backup ได้ทุก file system ดังนี้ ext2fs, ext3fs, fat16, fat32, hfs, hpfs, jfs, ntfs, reiserfs, ufs, xfs และยังมีข้อดีอีกอย่างคือแม้ว่า partition ที่จะทำการ restore ไม่ใช่เป็น file system ที่ตรงกันโปรแกรมจะทำการเปลี่ยนให้ตรงกับชนิดเดียวกับที่ได้ backup มาจากต้นทาง และถ้าพื้นที่ว่างไม่พอโปรแกรมจะไปหาที่ว่างส่วนอื่นบน hard disk เพื่อให้ข้อมูลติดตั้งลงได้ครบสมบูรณ์อีกด้วย โปรแกรมนี้เป็น Open source มีรองรับหลาย Distro ผู้ดูแลระบบสามารถไปหา download โปรแกรมนี้ได้ด้วยตนเองตัวอย่างเช่นที่ http://dries.ulyssis.org/rpm/packages/partimage/info.html เลือกให้ตรงกับ OS และ Version ที่กำลังใช้งาน กรณีตัวอย่างต่อไปนี้เป็นการใช้งานกับ Fedora Core 6 ไป download ไฟล์ชื่อ partimage-0.6.6-1.fc6.rf.i386.rpm มีวิธีใช้งานง่าย ๆ ตามเมนูดังต่อไปนี้

กรณีเป็น Debian ให้ติดตั้งด้วยคำสั่ง

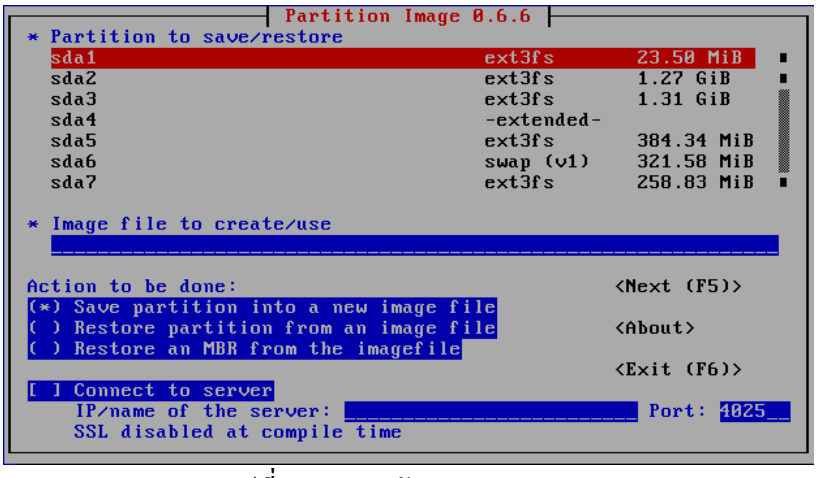
 # apt-get install partimage

ถ้าเป็น Fedora RedHat ให้ติดโดยคำสั่ง

 # rpm -ivh partimage-0.6.6-1.fc6.rf.i386.rpm

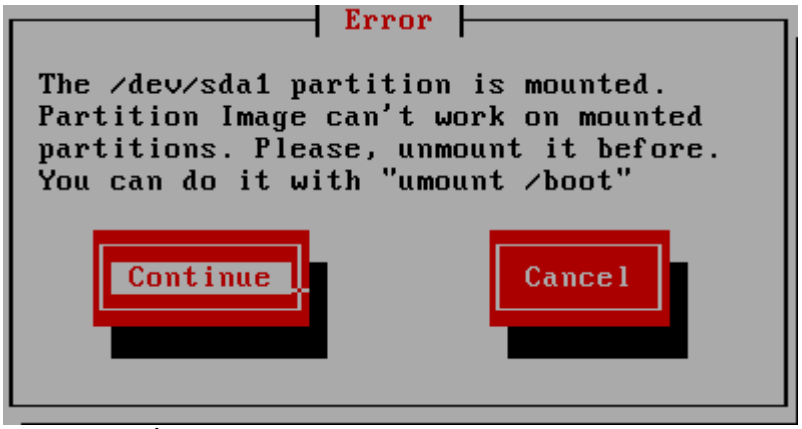
หลังติดตั้งเสร็จให้เรียกใช้งานด้วยคำสั่ง

 # partimage กด Enter จะได้เมนูดังรูป



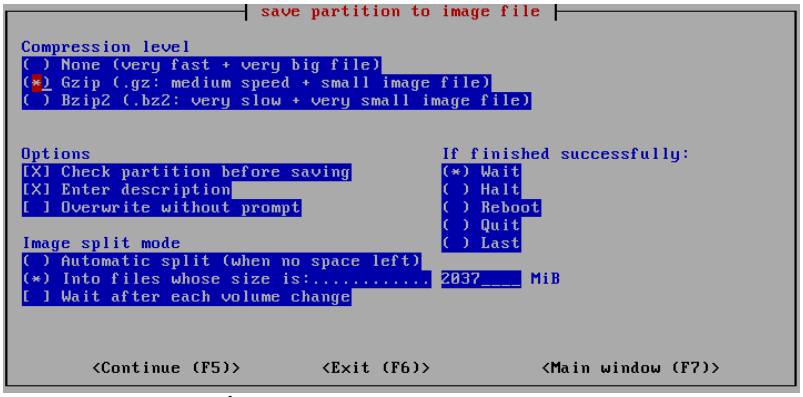
รูปที่ 8.1 เมนูหลักของ partimage

จากรูปที่ 8.1 ให้เลือก partition ที่ต้องการ backup โดยเลื่อนแป้นลูกศรขึ้นลง ตามตัวอย่างจะเป็น sda1 (boot partition) จากนั้นให้ใช้แป้น TAB มาที่ image file to create/use เพื่อกรอกชื่อไฟล์และ path ที่ต้องการเช่น ต้องการ backup ไฟล์ชื่อ boot_part เก็บไว้ที่ /backup ก็ให้กรอกลงไปเป็น /backup/boot_part เมนูถัดลงมาเป็น Action to be done: ถ้าต้องการ backup เลือกรายการแรกถ้าต้องการ Restore ให้เลือกรายการที่สองแต่ถ้าต้องการ Restore partition ที่ใช้ boot ต้องเลือก Restore an MBR จากนั้นให้กด F5 ไปยังหน้าจอถัดไป ดังภาพ



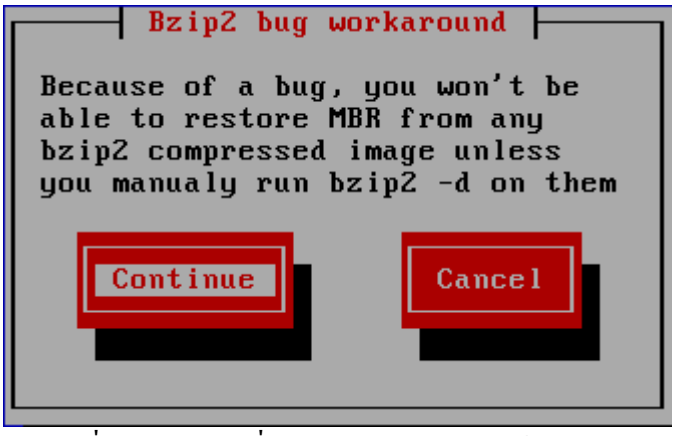
รูปที่ 8.2 แจ้ง Error กรณี partition ยังไม่ได้ unmount

จากภาพที่ 15.2 เป็นการเตือนให้ผู้ดูแลระบบทราบว่า การใช้ partimage ต้องทำการ backup partition เฉพาะที่ unmount เท่านั้น ถ้ากด Continue โปรแกรมจะทำต่อให้แต่ไม่รับประกันว่าจะได้ข้อมูลครบสมบูรณ์หรือไม่ จึงแนะนำให้ทำการ unmount ก่อนเช่น # umount /boot หลังจากนั้นจะได้เมนูหน้าจอถัดไปดังภาพ



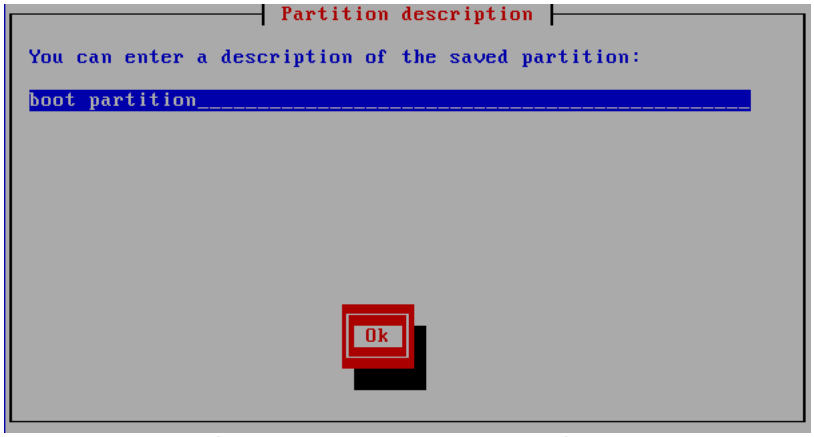
รูปที่ 8.3 หน้าต่างเลือกการบีบอัดข้อมูล

จากภาพที่ 15.3 มีระดับการเลือกบีบอัด Compression level ให้ 3 รายการ แนะนำให้ใช้รายการที่สอง เพราะได้ไฟล์เล็กและความเร็วปานกลาง ถ้าเลือกรายการที่สามได้ไฟล์เล็กที่สุดแต่ทำงานช้ามากและที่สำคัญการใช้ bzip2 ไม่รองรับการเก็บ MBR จะถูกเตือนดังภาพ



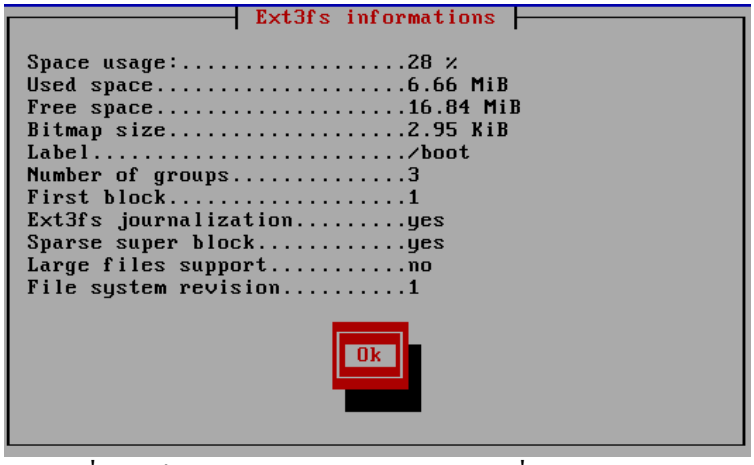
รูปที่ 8.4 คำเตือนเมื่อเลือกการบีบอัดแบบด้วย bzip2

สำหรับรายการอื่น ๆ ในภาพที่ 15.3 ก็มี Option ถูกเลือกไว้ให้อยู่แล้ว ส่วนถัดไปเป็น Image split mode สามารถกำหนดให้ Automatic split และขนาดไฟล์ได้ตามต้องการ เมนูถัดไปเป็นการเลือกว่าถ้าเสร็จแล้วจะทำอะไร โปรแกรมเลือกไว้ที่ wait ให้กดแป้น F5 จะทำงานต่อดังภาพ



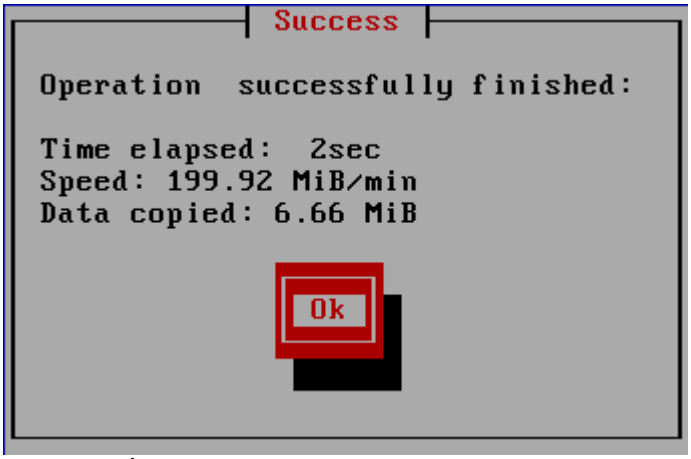
รูปที่ 8.5 ให้กรอกรายละเอียดไฟล์ที่จะเก็บ

ในภาพที่ 15.5 ให้กรอกค่ารายละเอียดของ Partition ที่กำลังจะทำการจัดเก็บ จากนั้นเลือก OK



รูปที่ 8.6 เป็นการแจ้งข้อมูลของ Partition ที่กำลังจะ Backup

เมื่ออ่านรายละเอียดในภาพที่ 15.6 แล้วให้เลือก OK เพื่อจัดเก็บได้ทันที คงต้องรอเวลาในการทำ Backup จะช้าหรือเร็วขึ้นอยู่กับขนาดของข้อมูลในแต่ละ Partition รวมถึงการเลือกแบบในการบีบอัดข้อมูลด้วย เมื่อเสร็จแล้วโปรแกรมจะรายงานให้ทราบ ดังนี้



รูปที่ 8.7 รายงานผลความสำเร็จในการ Backup

เพียงรูปแบบการทำงานผ่านเมนูง่าย ๆ แบบนี้ผู้ดูแลระบบคงพอมองออกว่าจะนำไปใช้ประโยชน์ได้อย่างไร ส่วนการ Restore ก็ทำกลับกันตามเมนูเดิม เพียงแต่บอกว่า image file อยู่ที่ไหน ชื่ออะไร ซึ่งเป็นเครื่องมือที่มีไว้อำนวยความสะดวกกับ Server ที่ต้องการเสถียรภาพของระบบควรนำไปใช้ประโยชน์ได้เป็นอย่างดี

<u>บทสรุป</u>

การทำ backup และ restore จากเนื้อหาและตัวอย่างในบทนี้ ถ้าดูแล้วเข้าใจยากก็ให้นึกถึงการใช้คำสั่ง tar cvfz และ tar xvfz แบบที่เคยใช้บีบอัดข้อมูลเหมือนกับโปรแกรม Zip และ Unzip ใน DOS หรือใน Windows นั่นเองไม่ได้มีความยุ่งยากอะไร เพียงแต่ในตัวอย่างทำให้ยาวขึ้นเพราะต้องการให้คุณบันทึกชื่อไฟล์เป็นคำอธิบายว่าเป็น Full-backup วันที่เท่าไร เดือนอะไรเท่านั้น เพื่อความสะดวกในการเรียกข้อมูลกลับคืนได้ตรงตามวัน เดือนที่ต้องการ จะได้ไม่ต้องไปค้นหากันให้วุ่นวาย เหมือนกับคนไทยใช้ Word พิมพ์งานเวลา Save ก็ตั้งชื่อ aaa bbb xyz เก็บกันไว้เต็ม Hard disk พอถึงเวลาจะเรียกใช้ก็ต้องมานั่งเปิดดูทุกไฟล์ ไม่รู้ความหมายว่า

ภาคผนวก

ตัวอย่างลำดับขั้นตอนการดูแลระบบความปลอดภัยให้ Log Server

ผู้ที่ได้รับการแต่งตั้งจากผู้อำนวยการหรือผู้มีอำนาจในองค์กรต่างๆ จำเป็นต้องเขียนบันทึกลำดับขั้นตอนการปฏิบัติหน้าที่ดูแลรักษาความลับข้อมูลจราจรเครือข่ายคอมพิวเตอร์อย่างรัดกุม รอบคอบและเป็นระบบ เพื่อให้ผู้บริหารลงนามเป็นลายลักษณ์อักษร เป็นเอกสารประกอบการปฏิบัติหน้าที่ตามกฎหมาย ผู้เขียนได้สรุปเป็นข้อ ๆ ดังนี้

1. ใส่กุญแจที่ตัวเครื่องป้องกันการเปิดเข้าถึงอุปกรณ์ Hardware ภายในได้ จะป้องกันผู้บุกรุกรวมถึงผู้ดูแลระบบ (Admin) ขององค์กรด้วย
2. ใส่ Bios password ป้องกันการแก้ไขค่าสำหรับ boot และตั้งค่าให้เครื่อง boot จาก hard disk ได้อย่างเดียวเท่านั้น ยกเลิกการ boot จากอุปกรณ์อื่น ๆ ทั้งหมด
3. ใส่รหัสผ่านที่ Boot loader (GRUB password) ป้องกันการแก้ไขค่าที่ Boot loader
4. เปลี่ยนรหัสผ่าน (Login password) หลังจากรับมอบเครื่องจากผู้ดูแลระบบ (Admin)
5. มีการจัดทำเรื่องความปลอดภัยป้องกันการ Hack เข้าระบบดังนี้
   - Update software
   - Kernel harden
   - Firewall
   - TCP_Wrappers ป้องกันการเข้าถึง host
   - ป้องกันการ scan port
   - ปิด port ที่ไม่ได้ใช้งานและ service ที่ไม่จำเป็น
6. กรณีผู้ดูแลระบบขอเปิดใช้บริการส่งข้อมูล log file ผ่านทาง ssh มีการออก User account ที่มีการจำกัดสิทธิการเข้าระบบและได้ทำการสร้าง key ใหม่โดยเข้ารหัสกุญแจไม่น้อยกว่า 1024 บิท
7. ทำการบีบอัดและเข้ารหัส log file พร้อมจัดทำระบบการตรวจสอบความถูกต้องไฟล์ข้อมูล (Checksum) ที่จัดเก็บไว้ในสื่อ CD หรือ DVD
8. มีระบบการตรวจสอบความถูกต้องของไฟล์ข้อมูล (Checksum) ที่จัดเก็บในข้อ 7 ด้วยการเข้ารหัสได้สูงถึง 512 บิท
9. ในการเข้าถึงข้อมูล log ต้องมีการตรวจสอบความถูกต้องของไฟล์และทำการถอดรหัสไฟล์ก่อนที่จะแตกไฟล์ข้อมูลเพื่อนำส่งเจ้าพนักงาน
10. สื่อหรือ Media ที่จัดเก็บ บันทึกข้อมูลเช่น CD, DVD บุคคลทั่วไปไม่สามารถเข้าถึงข้อมูลดิบได้เนื่องจากข้อมูลดังกล่าวมีการเข้ารหัสไว้ดังที่กล่าวข้างต้น โดยผู้มีหน้าที่ดูแลรักษาข้อมูลนี้เป็นผู้ถือรหัสผ่านในแต่ละขั้นตอนแต่เพียงผู้เดียว แม้แต่ผู้ดูแลระบบ (Admin) ก็ไม่สามารถเข้าถึงข้อมูลนี้ได้
11. การนำส่งข้อมูลให้กับพนักงานเจ้าหน้าที่ต้องดำเนินการจัดส่งให้ตรงกับการร้องขอและครบถ้วนสมบูรณ์ด้วยความรวดเร็ว ตัวอย่างกรณีเมื่อมีการกระทำความผิดเกิดขึ้นกับเครื่องให้บริการเว็บ (Web Server)

12. ระบบรักษาความปลอดภัยทั้งหมดเมื่อได้รับมอบจากผู้ดูแลระบบ (Admin) แล้วผู้รับผิดชอบได้ทำการเปลี่ยนรหัสทุกขั้นตอนจนครบถ้วนด้วยตนเองจนแน่ใจว่ามีความปลอดภัยตามที่กฎหมายกำหนดทุกประการ

ลงชื่อ .....

( )

ผู้รับผิดชอบดูแลรักษาข้อมูลจราจรเครือข่ายคอมพิวเตอร์

ลงชื่อ .....

( )

ตำแหน่ง .....

อาจมีการปรับปรุงเพิ่มเติมหรือลดในส่วนที่ตรงกับการทำงานในระบบของแต่ละองค์กร ตามความเหมาะสม เพื่อให้เกิดความรัดกุมและเป็นหลักฐานที่สามารถใช้ยืนยันในชั้นศาลได้ ก็จะทำให้หมดภาระหน้าที่ของผู้รับผิดชอบในการดูแลเก็บรักษาความลับของ Log file ตามกฎหมาย

คำแนะนำสำหรับผู้ดูแลระบบเครือข่าย (Administrator)

โดยทั่วไปผู้ดูแลระบบมักเป็นผู้มีความรู้ความชำนาญในด้าน Software และ Hardware เป็นอย่างดี สามารถติดตั้ง NOS และทำการเปิดให้บริการลูกข่ายได้ทั้งระบบ ทำให้หน่วยงานหรือองค์กรต่าง ๆ ไว้วางใจมอบหมายให้จัดทำ Log Server ตามกฎหมายเพิ่มขึ้นอีก 1 เครื่อง ผู้เขียนเห็นว่าหากไม่มีการแนะนำในส่วนนี้อาจทำให้เกิดความเข้าใจผิดคิดกันไปว่า ผู้ดูแลระบบเป็นคนทำและดูแล Log server ด้วยตนเองรวมถึงต้องเป็นผู้เก็บรักษาข้อมูลและนำส่งพนักงานเจ้าหน้าที่เองทั้งหมด ความจริงไม่เป็นเช่นนั้น หลังทำ Log server ให้ทำงานได้อย่างสมบูรณ์พร้อมทำระบบความปลอดภัยให้ครบถ้วนอีกด้วย เสร็จแล้วต้องส่งมอบเครื่อง Log server ให้กับผู้ที่ได้รับการแต่งตั้งจากผู้บริหารองค์กรดูแลรักษาข้อมูลจราจรเครือข่ายคอมพิวเตอร์ต่อไป จึงควรอย่างยิ่งที่ต้องมีการจัดการทุกอย่างเป็นลายลักษณ์อักษร ให้ผู้บริหารลงนามรับทราบการทำงานไว้เป็นเอกสารอ้างอิงเมื่อเกิดเหตุการณ์กระทำความผิดขึ้นในองค์กร ดังต่อไปนี้

1. เขียนแบบระบบเครือข่ายขององค์กรทั้งหมดโดยละเอียดพร้อมตำแหน่งการติดตั้ง
2. เขียนรายละเอียดประกอบแบบให้ครบถ้วนโดยเฉพาะในส่วนของการส่งค่าไปเก็บใน Log server เช่น Host name และค่า network ต่าง ๆ
3. ลำดับขั้นตอนการติดตั้ง Log server และ NTP Server
4. การติดตั้งและสร้างระบบรักษาความปลอดภัยให้ Log server
5. ในแต่ละขั้นตอนที่มีการเข้ารหัสผ่าน (Password) ต้องบันทึกส่งมอบรหัสผ่านพร้อมวิธีเปลี่ยนรหัสผ่านในแต่ละส่วนให้กับผู้ดูแล Log server เพื่อให้ทำการเปลี่ยนรหัสผ่านทั้งระบบป้องกันมิให้ผู้ใดเข้าถึงข้อมูลใน Log server ได้อีก
6. หากมีความจำเป็นต้องมีการส่ง log file บางเรื่องหรือบางกรณีผ่านทาง Secure Shell ต้องทำการส่งแบบตั้งเวลาอัตโนมัติด้วย User account ที่ถูกจำกัดสิทธิและแจ้งขั้นตอนและเวลาที่ระบบจะส่งข้อมูลให้ละเอียดชัดเจน

7. โปรแกรม Log server 2.0 ทำการติดตั้งเพื่อรอรับค่า log file จากระบบทั้งหมดไว้แล้ว เพียงให้ทำการแก้ไขค่า IP address ให้ตรงกับระบบจริงขององค์กรก็สามารถใช้งานได้ ทำงานที่ TCP/UDP port 514 ส่วน NTP server จะทำงานด้วย UDP port 123

ลงชื่อ .....

( )

ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์

ลงชื่อ .....

( )

ตำแหน่ง .....

อาจมีการปรับปรุงเพิ่มเติมหรือลดในส่วนที่ตรงกับการทำงานในระบบของแต่ละองค์กร ตามความเหมาะสม เพื่อให้เกิดความรัดกุมและเป็นหลักฐานที่สามารถใช้ยืนยันในชั้นศาลได้ ก็จะทำให้หมดภาระหน้าที่ของผู้ดูแลระบบเครือข่ายหรือ (Admin) ในกรณีเกิดการกระทำความผิดในองค์กรได้

บรรณานุกรม

บุญลือ อยู่คง. **การติดตั้ง Internet Server ด้วย Linux.** นครราชสีมา: บริษัทซายเอ็นเทค จำกัด, 2545.

บุญลือ อยู่คง. **ป้องกัน Linux Server อย่างมืออาชีพ.** เชียงใหม่: บริษัท ดวงกมลเชียงใหม่กรุ๊ป จำกัด, 2546.

บุญลือ อยู่คง. **ติดตั้ง Log Server ด้วย Linux.** พิษณุโลก: โฟกัสมาสเตอร์พรินต์, 2551.

Linux Security HOWTO, Kevin Fenzi and Dave Wreski, http://www.linuxsecurity.com/docs/LDP/Security-HOWTO/

Secure Programming for Linux and Unix HOWTO, David A. Wheeler, available at http://www.dwheeler.com/secure-programs

Securing and Optimizing Linux: The Ultimate Solution, Gerhard Mourani http://www.openna.com/products/books/sol/solus.php

Linux Security Overview, ISSA-PS 2003, Brian Hatch, http://www.ifokr.org/bri/presentations/issa-2003/

Linux: The Securable Operating System, Brian Hatch, http://www.linuxsecurity.com

http://fedoraproject.org/

http://grub.org/

http://www.balabit.com/network-security/syslog-ng/

http://www.ssh.com/