ระบบรักษาความปลอดภัยสำหรับเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์

COMPUTER ENGINEERING NETWORK SECURITY SYSTEM

เจตณัฐ ตฤณตียะกูล

ณรงค์ศักดิ์ เวสารัชกร

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2558

ระบบรักษาความปลอดภัยสำหรับเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์

COMPUTER ENGINEERING NETWORK SECURITY SYSTEM

เจตณัฐ ตฤณตียะกูล
ณรงค์ศักดิ์ เวสารัชกร

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2558

ปริญญานิพนธ์ปีการศึกษา 2558

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบรักษาความปลอดภัยสำหรับเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์

COMPUTER ENGINEERING NETWORK SECURITY SYSTEM

ผู้จัดทำ

1. นายเจตณัฐ ตฤณตียะกูล รหัสนักศึกษา 55010190

2. นายณรงค์ศักดิ์ เวสารัชกร รหัสนักศึกษา 55010327

..... อาจารย์ที่ปรึกษา

(อาจารย์อัครเดช วัชระภูพงษ์)

ระบบรักษาความปลอดภัยสำหรับเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์

นายเจตณัฐ ตฤณตียะกูล 55010190
นายณรงค์ศักดิ์ เวสารัชกร 55010327
อาจารย์อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษา
ปีการศึกษา 2558

บทคัดย่อ

ในปัจจุบันความปลอดภัยสำหรับเครือข่ายสารสนเทศนั้นเป็นสิ่งที่จำเป็นอย่างยิ่งที่จะต้องรักษาไว้ เพื่อให้ระบบสารสนเทศต่างๆ นั้นสามารถดำเนินการให้บริการได้อย่างราบรื่น และไม่เกิดเหตุขัดข้องในการให้บริการ และความปลอดภัยของเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ ก็เช่นเดียวกัน โครงงานนี้จึงจัดทำขึ้นเพื่อประเมิน ออกแบบ ตั้งค่า ติดตั้ง ปรับปรุง และพัฒนาองค์ประกอบ ให้เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ และบริการหลักที่เกี่ยวเนื่องให้มีความปลอดภัยยิ่งขึ้น ไม่ว่าปัจจัย CIA และกลไก AAA โดยต้องให้เหมาะสมสอดคล้องกับพันธกิจของภาควิชาฯ คือการเรียนการสอน การวิจัยและพัฒนาการให้บริการแก่สังคม

Computer Engineering Network Security System

Mr. Jettanat Trinteeyakul 55010190

Mr. Narongsak Wesaratchakorn 55010327

Mr. Akkradach Watcharapupong Advisor

Academic Year 2015

ABSTRACT

Nowadays, the information system security is very important. All of the service should be always online. And computer Engineer's network also. So this project was made to setup, configure, maintain, expand configuration of network and main service to increase security by refer AAA and CIA standards. However, it should be depend on usage of Department of Computer Engineering. We monitored the services and recorded the result to administrator by analysis result from syslog system, IDS, and user behavior. Our project focus on protection from attacker and availability of services.

กิตติกรรมประกาศ

โครงงาน และปริญญานิพนธ์ฉบับนี้เสร็จสมบูรณ์ได้ เนื่องจากได้รับคำแนะนำ และคำปรึกษาที่ดีจากท่านอาจารย์ที่ปรึกษาคือ อาจารย์อัครเดช วัชระภูพงษ์ ที่คอยให้ความรู้ และอธิบายองค์ความรู้ต่างๆ ที่จำเป็นต้องใช้เพื่อทำโครงงาน รวมไปถึงแนะนำแนวทางเพื่อให้โครงงานนี้บรรลุเป้าหมาย ซึ่งทางคณะผู้จัดทำขอขอบคุณอาจารย์ที่ปรึกษาเป็นอย่างสูง

ขอขอบคุณนายวรภพ บุญประไพ ที่ให้คำปรึกษาเกี่ยวกับคำสั่งในการตั้งค่าต่างๆ ในระบบปฏิบัติการ Linux

ขอขอบคุณห้องวิจัย ISAG ที่เอื้อเฟื้อสถานที่ในการทำงานวิจัย และเครื่องคอมพิวเตอร์ที่ใช้ในการทดลอง

ขอขอบคุณบิดา และมารดาของคณะผู้จัดทำที่ให้การสนับสนุนสิ่งต่างๆ และคอยเป็นกำลังใจให้คณะผู้จัดทำตลอดการทำโครงงาน

ขอขอบคุณรุ่นพี่ เพื่อนๆ และรุ่นน้องจากห้องแล็บทุกๆ ห้องวิจัย ที่ได้ให้ข้อมูลต่างๆ เพื่อเป็นข้อมูลในการทำโครงงานนี้

เจตณัฐ ตฤณตียะกูล

ณรงค์ศักดิ์ เวสารัชกร

สารบัญ (ต่อ)

หน้า

บทที่ 4 การทดลองและผลการทดลอง 19
4.1 การทดลองเปลี่ยนการตั้งค่าการเข้าถึงสวิตช์จากเทลเน็ตเป็นซีเคียวเชลล์ 19
4.2 ทดลองการรวบรวมบันทึกกิจกรรมมาที่ส่วนกลาง 20
4.3 ทดลองติดตั้งและทดสอบโปรแกรมดักจับผู้บุกรุกที่เข้ามาโจมตีเว็บไซต์ของภาควิชาวิศวกรรมคอมพิวเตอร์ (Snort) บนระบบปฏิบัติการ Ubuntu 22
4.4 ทดลองติดตั้งโปรแกรมที่ตรวจสอบสถานะของเครื่อง (Zabbix) บนระบบปฏิบัติการ Ubuntu 38
4.5 ทดลองติดตั้งโปรแกรมตรวจสอบการใช้งานอินเทอร์เน็ตในระบบเครือข่ายของภาควิชาวิศวกรรมคอมพิวเตอร์ (ntop) บนระบบปฏิบัติการ Ubuntu 40

บทที่ 5 บทสรุปและข้อเสนอแนะ 42
5.1 สรุป 42
5.2 ปัญหาและอุปสรรค 43
5.3 แนวทางการแก้ไข 43
5.4 แนวทางการพัฒนาต่อ 43

บรรณานุกรม 44

สารบัญรูป

รูป หน้า

2.1 ปัจจัยของความปลอดภัยข้อมูล 4
2.2 เส้นทางการรับส่งข้อมูลเมื่อมีการใช้ฟังก์ชัน Port Forward ในอุปกรณ์ Router 6
2.3 รูปแบบการโจมตีประเภท DoS 6
2.4 รูปแบบการโจมตีประเภท DDoS 7
2.5 ตัวอย่างการทำ Centralized Logging 10
3.1 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์โดยรวม 14
3.2 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 5 15
3.3 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 6 15
3.4 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 7 16
3.5 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 8 16
3.6 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 9 17
4.1 ผลการทดสอบสำเร็จจากการติดตั้ง Snort 24
4.2 ผลการทดสอบสำเร็จจากการตั้งค่าไฟล์ snort.conf 26
4.3 การรัน Snort และรอการโจมตี 29
4.4 การโดนโจมตีการจากรันโปรแกรม barnyard2 29
4.5 การติดตั้งโปรแกรม Pulled Pork เสร็จสมบูรณ์ 31
4.6 ผลการรรันคำสั่งของโปรแกรม Pulled Pork 32
4.7 การติดตั้งโปรแกรม Image Graph 34
4.8 การทดสอบโปรแกรม BASE 36
4.9 การแจ้งเตือนเมื่อมีการโจมตีโดยส่ง TCP Packet จำนวนมาก 37
4.10 การแจ้งเตือนเมื่อมีการโจมตีด้วย SSH Brute Force Attack 38

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของโครงงาน

เนื่องจากในปัจจุบันความปลอดภัยของระบบเครือข่ายนั้นเป็นสิ่งสำคัญอย่างยิ่งสำหรับการให้บริการระบบสารสนเทศ เช่นเดียวกับเครือข่ายของภาควิชาฯ ที่ต้องให้บริการระบบสารสนเทศแก่บุคลากรอยู่ตลอดเวลา อาทิเช่น การให้บริการเครือข่ายอินเทอร์เน็ต เว็บไซต์ภาควิชาฯ เป็นต้น

ดังนั้นความปลอดภัยสำหรับเครือข่ายภาควิชาฯ จึงเป็นสิ่งที่จำเป็นที่ต้องรักษาไว้ เพื่อทำให้การบริการต่างๆ นั้นไม่เกิดข้อขัดข้องขึ้น แต่หากมีข้อขัดข้องเกิดขึ้น อาทิเช่น ระบบเครือข่ายอินเทอร์เน็ตของภาควิชาฯใช้การไม่ได้ เว็บไซต์ของภาควิชาฯไม่สามารถเข้าได้ เป็นต้น ก็ควรที่จะมีระบบที่สามารถตรวจสอบข้อผิดพลาดของเครือข่ายและระบบต่างๆ ได้ เพื่อทำให้ผู้ดูแลระบบสามารถแก้ไขปัญหาได้ถูกจุด

ในปัจจุบันสิ่งที่ทำให้เครือข่ายหรือระบบต่างๆ ที่ให้บริการใช้การไม่ได้ หรือเกิดเหตุขัดข้องนั้นไม่ได้มีแค่การทำงานผิดพลาดของระบบภายในเท่านั้น แต่ยังมีผู้ที่ไม่ประสงค์ดีที่ต้องการโจมตีระบบเครือข่ายหรือก่อกวนการให้บริการของระบบ ทำให้ระบบต่างๆ นั้นไม่สามารถให้บริการได้ อาทิเช่น การโจมตีโดยวิธี Distributed Denial of Service (DDoS Attack) เป็นต้น

ด้วยปัจจัยต่างๆ ที่ได้กล่าวในข้างต้น จึงเป็นที่น่าสนใจที่จะมีการประเมิน ออกแบบ ตั้งค่าต่างๆ และพัฒนาเครือข่ายภาควิชาฯ ให้มีความปลอดภัยมากยิ่งขึ้น รวมถึงมีระบบที่สามารถระบุและบันทึกสาเหตุของปัญหาที่เกิดขึ้นได้

1.2 วัตถุประสงค์ของโครงงาน

1) เพื่อประเมินและออกแบบให้เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ และบริการหลักที่เกี่ยวเนื่องให้มีความปลอดภัยยิ่งขึ้น
2) เพื่อตั้งค่า ติดตั้ง ปรับปรุง และพัฒนาองค์ประกอบให้เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ และบริการหลักที่เกี่ยวข้องให้มีความปลอดภัยยิ่งขึ้น

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1) ทำให้เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ มีความปลอดภัยมากยิ่งขึ้น
2) ทำให้สามารถแก้ไขปัญหาเมื่อระบบเครือข่ายภาควิชาฯ เกิดเหตุขัดข้องได้เร็วยิ่งขึ้น

1.4 ขอบเขตของโครงงาน

1) เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 องค์ประกอบหลักของความปลอดภัยข้อมูล

การที่จะบอกได้ว่าข้อมูลนั้นมีความปลอดภัยหรือไม่นั้นต้องวิเคราะห์ปัจจัยทั้ง 3 ด้านคือ ความลับ ความถูกต้อง และความพร้อมใช้งานว่ามีครบหรือไม่ ถ้าขาดปัจจัยด้านใดไปก็แสดงว่าข้อมูลนั้นไม่มีความปลอดภัย ดังนั้นการรักษาความปลอดภัยของข้อมูลจึงเป็นการปกป้องรักษาปัจจัยทั้ง 3 ด้านดังต่อไปนี้

2.1.1 ความลับ (Confidentiality)

การรักษาความลับของข้อมูล หมายถึง การอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้ หรืออาจหมายถึง การปกป้องข้อมูลไม่ให้ผู้ไม่ได้รับอนุญาตเข้าถึงข้อมูลได้ ข้อมูลบางอย่างนั้นอาจมีความสำคัญ และจำเป็นต้องเก็บไว้เป็นความลับ เพราะถ้าถูกเปิดเผยอาจมีผลเสียหรือเป็นอันตรายต่อเจ้าของได้ ซึ่งกลไกที่ใช้รักษาความลับคือ การเข้ารหัสข้อมูล (Cryptography หรือ Encryption) ซึ่งเป็นการจัดข้อมูลให้อยู่ในรูปที่ไม่สามารถอ่านหรือเข้าใจได้ถ้าไม่รู้วิธีการและคีย์ในการเข้ารหัสและถอดรหัสคีย์ (Key) หรือรหัสผ่าน (Password) เป็นกุญแจที่จะใช้สำหรับการเข้ารหัสและถอดรหัสข้อมูลได้

2.1.2 ความถูกต้อง (Integrity)

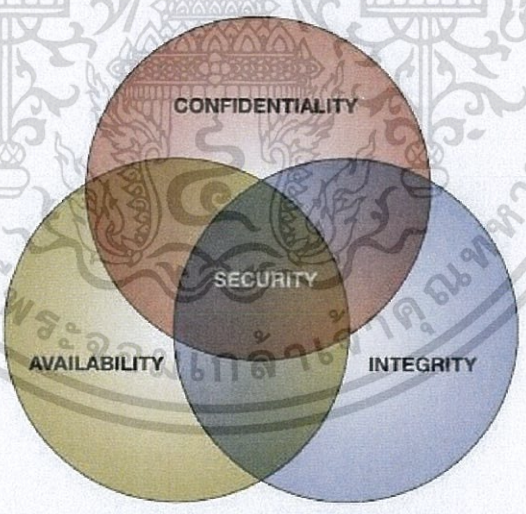
ความถูกต้องข้องข้อมูล หมายถึง ความเชื่อถือได้ของข้อมูลและทำให้สารสนเทศที่อ่อนไหว และ/หรือมีคุณค่า ไม่ถูกเปิดเผยโดยคนที่ไม่ได้รับอนุญาต ซึ่งการรักษาความถูกต้องของข้อมูลนั้นประกอบด้วยสองส่วนคือ ความถูกต้องของเนื้อหาข้อมูล และความถูกต้องของแหล่งที่มาของข้อมูล แหล่งที่มาของข้อมูลอาจมีผลต่อความถูกต้องและความน่าเชื่อถือของข้อมูล กลไกในการรักษาความถูกต้องของข้อมูลนั้นประกอบด้วย 2 ส่วนคือ การป้องกัน (Prevention) และการตรวจสอบ (Detection)

กลไกในการป้องกัน (Prevention) มีจุดมุ่งหมายเพื่อรักษาความถูกต้องของข้อมูล ซึ่งทำได้โดยการป้องกันการพยายามที่จะเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือพยายามที่จะเปลี่ยนแปลงข้อมูลในรูปแบบที่ไม่ถูกต้องหรือได้รับอนุญาต โดยในความพยายามข้อแรกนั้นเป็นความพยายามที่จะแก้ไข หรือเปลี่ยนแปลงข้อมูลโดยผู้ที่พยายามนั้นไม่ได้รับอนุญาต แต่ความพยายามอีกข้อหนึ่งนั้นเกิดจากการที่ผู้ได้รับอนุญาตพยายามที่จะแก้ไขข้อมูลนอกเหนือขอบเขตที่ตนเองมีสิทธิ์

กลไกในการตรวจสอบความถูกต้องของข้อมูล (Detection) นั้นไม่ใช่กลไกในการรักษาให้ข้อมูลคงสภาพเดิม แต่เป็นกลไกที่ตรวจสอบว่าข้อมูลยังคงมีความน่าเชื่อถืออยู่หรือไม่ กล่าวคือ การตรวจเช็คและวิเคราะห์เหตุการณ์ต่างๆ ที่เกิดขึ้นในระบบ รวมถึงเหตุการณ์ที่เกิดขึ้นโดยระบบหรือผู้ใช้เอง เพื่อตรวจว่ามีปัญหาเกิดขึ้นหรือไม่ หรืออาจตรวจสอบและวิเคราะห์ข้อมูลว่าคุณสมบัติที่สำคัญหรือที่คาดหวังไว้ยังคงสภาพเดิมอยู่หรือไม่ กลไกนี้อาจรายงานว่าส่วนไหนของข้อมูลมีการแก้ไขหรือถูกเปลี่ยนแปลงไปจากเดิมโดยสิ้นเชิง

2.1.3 ความพร้อมใช้งาน (Availability)

ความพร้อมใช้งานของข้อมูล หมายถึง ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ ความพร้อมใช้งานเป็นส่วนหนึ่งของความมั่นคงของระบบ (Reliability) ส่วนหนึ่งของความพร้อมใช้งานที่เกี่ยวข้องกับการรักษาความปลอดภัยคือ อาจมีผู้ไม่ประสงค์ดีพยายามที่จะทำให้ไม่สามารถเข้าถึงข้อมูลได้โดยการทำให้ระบบไม่สามารถใช้งานได้ การออกแบบระบบนั้นส่วนมากจะใช้ข้อมูลทางสถิติเกี่ยวกับรูปแบบและพฤติกรรมในการใช้งานระบบของผู้ใช้ เพื่อออกแบบให้ระบบเหมาะกับสภาพแวดล้อมดังกล่าว ดังนั้น กลไกในการรักษาความพร้อมใช้งานนั้นจะทำในกรณีที่ระบบไม่ได้ทำงานในสภาพที่ปกติหรือออกแบบไว้ ซึ่งถ้ากลไกนี้ไม่ทำงานส่วนมากระบบจะล่มหรือไม่พร้อมใช้งาน



รูป 2.1 ปัจจัยของความปลอดภัยข้อมูล

2.2 หลักการเกี่ยวกับการรักษาความปลอดภัยข้อมูล

นอกจากปัจจัยทั้ง 3 ด้านของความปลอดภัยข้อมูลแล้วยังมีหลักการอื่นๆ ที่เกี่ยวกับการรักษาความปลอดภัยข้อมูลอีก ดังนี้

2.2.1 การพิสูจน์ทราบตัวตน (Authentication)

การพิสูจน์ทราบตัวตนนั้นเกิดขึ้นเมื่อระบบควบคุมพิสูจน์ว่าผู้ใช้ใช่คนที่ผู้ใช้บอกหรือไม่ เช่น ถ้าผู้ใช้ระบุยูสเซอร์เนม (Username) แล้วก็ต้องสามารถระบุรหัสผ่านที่คู่กับยูสเซอร์นั้นได้

2.2.2 การอนุญาตใช้งาน (Authorization)

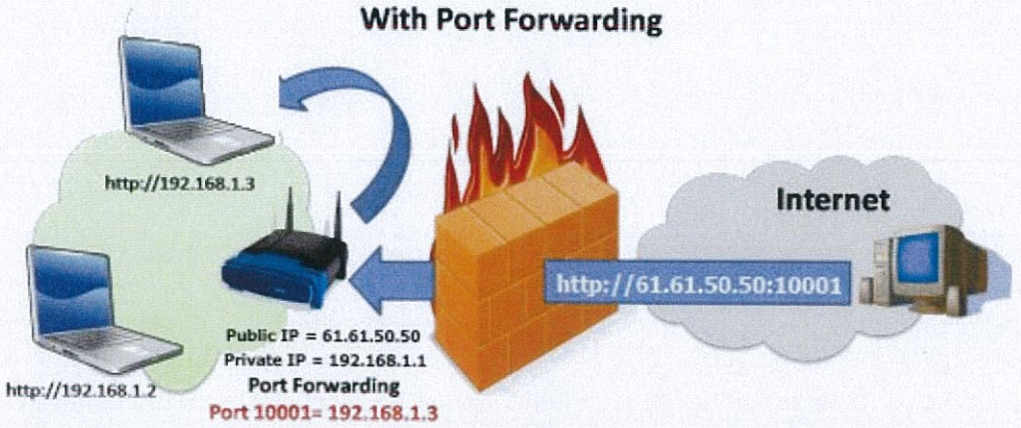
หลังจากที่สามารถพิสูจน์ทราบตัวตนแล้ว ขั้นตอนต่อไปคือ การตรวจสอบสิทธิ์ของผู้ใช้นั้นว่าได้มีการกำหนดสิทธิ์ให้ใช้งานระบบได้ในระดับไหน ซึ่งสิทธิ์นั้นประกอบด้วย การเข้าถึงหรืออ่าน การแก้ไข และการลบข้อมูล

2.2.3 การตรวจสอบได้ (Accounting)

ความสามารถในการตรวจสอบการใช้งานระบบได้ เป็นอีกส่วนที่สำคัญ เพราะเป็นการรับรองว่าทุกๆ กิจกรรมหรือเหตุการณ์ที่เกิดขึ้นสามารถตรวจสอบได้ว่าเกิดขึ้นเพราะใครหรือโพรเซสไหน เช่น การเก็บล็อก (Logs) เกี่ยวกับกิจกรรมต่างๆ ที่ผู้ใช้แต่ละคนใช้งานระบบ เป็นต้น

2.3 การเชื่อมต่ออย่างปลอดภัยด้วย SSH Tunnel

การใช้งานอินเทอร์เน็ตจากผู้ให้บริการเครือข่ายไร้สายสาธารณะ (Wi-Fi) หรือจากผู้ให้บริการร้านอินเทอร์เน็ตคาเฟ่ทั่วไป ล้วนแต่เป็นการเชื่อมต่อบนเครือข่ายที่ไม่ปลอดภัยและมีความเสี่ยงต่อการถูกผู้ไม่ประสงค์ดีหรืออาจหมายถึงผู้ให้บริการเองในการลักลอบขโมยข้อมูลการใช้งานของผู้ใช้บนเครือข่ายนั้นๆ เช่น การดักจับข้อมูลรหัสผ่านที่ผู้ใช้ส่งผ่านเครือข่ายไร้สายสาธารณะ เป็นต้น ซึ่งในเวลาต่อมาได้มีการพัฒนารูปแบบการเชื่อมต่อที่มีความสามารถในการทำให้การเข้าใช้งานระบบบนเครือข่ายใดๆ มีการรักษาความปลอดภัยในการรับส่งข้อมูล โดยหนึ่งในวิธีที่ผู้ดูแลระบบสามารถนำมาประยุกต์และปรับใช้ในการทำงาน เพื่อทำให้การรับส่งข้อมูลบนเครือข่ายมีความปลอดภัยคือ การสร้างช่องทางการรับส่งข้อมูลเฉพาะที่เรียกว่า Tunnel ผ่านโพรโทคอล SSH (Secure Shell) ที่มีรูปแบบการสื่อสารที่มีมาตรการรักษาความปลอดภัยของข้อมูลด้วยการเข้ารหัสลับข้อมูล โดย SSH Tunnel มีชื่อเรียกอีกชื่อหนึ่งว่า SSH Port Forward เนื่องจากมีการทำงานลักษณะเดียวกับ Port Forward ซึ่งใช้กำหนดเส้นทางการรับส่งข้อมูลระหว่างเครือข่ายภายนอก (WAN) กับเครือข่ายภายใน (LAN) โดยปกติการใช้งาน Port Forward จะนิยมใช้ในฟังก์ชันการทำงานของอุปกรณ์ Router เพื่อให้เครื่องคอมพิวเตอร์จากเครือข่ายอินเทอร์เน็ต สามารถเชื่อมต่อมายังเครือข่ายภายใน Router ดังกล่าว โดยสามารถระบุช่องทางการเชื่อมต่อแยกแต่ละ Port ได้ดังรูป 2.2



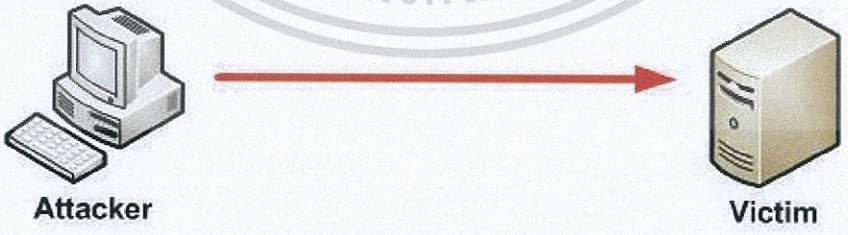
รูป 2.2 เส้นทางการรับส่งข้อมูลเมื่อมีการใช้ฟังก์ชัน Port Forward ในอุปกรณ์ Router

รูปแบบการสร้างการเชื่อมต่อของ SSH Tunnel สามารถทำได้ 2 แบบคือ Local Port Forward และ Remote Port Forward โดยการใช้งาน SSH Tunnel ผู้ใช้จะต้องติดตั้งโปรแกรม SSH Client ลงในเครื่องคอมพิวเตอร์ ซึ่งในระบบปฏิบัติการลินุกซ์ส่วนใหญ่ จะมีการติดตั้งโปรแกรม OpenSSH-Client มาพร้อมกับระบบอยู่แล้ว ส่วนในระบบปฏิบัติการวินโดวส์ ผู้ใช้สามารถดาวน์โหลดและติดตั้งโปรแกรมชื่อ PuTTY ซึ่งทำงานในลักษณะ SSH Client เช่นกัน

2.4 ประเภทของการโจมตีระบบเครือข่าย

2.4.1 Denial of Service Attack

การโจมตีแบบ Denial of Service (DoS) เป็นรูปแบบการโจมตีที่ขัดขวางหรือก่อกวนระบบเครือข่ายหรือ Server จนทำให้เครื่อง Server หรือเครือข่ายนั้นๆไม่สามารถทำงานได้ตามปกติ ซึ่งการโจมตีด้วยวิธีการ DoS Attack นั้นโดยทั่วไปนั้นจะกระทำโดยการใช้ทรัพยากรของ Server ไปจนหมด

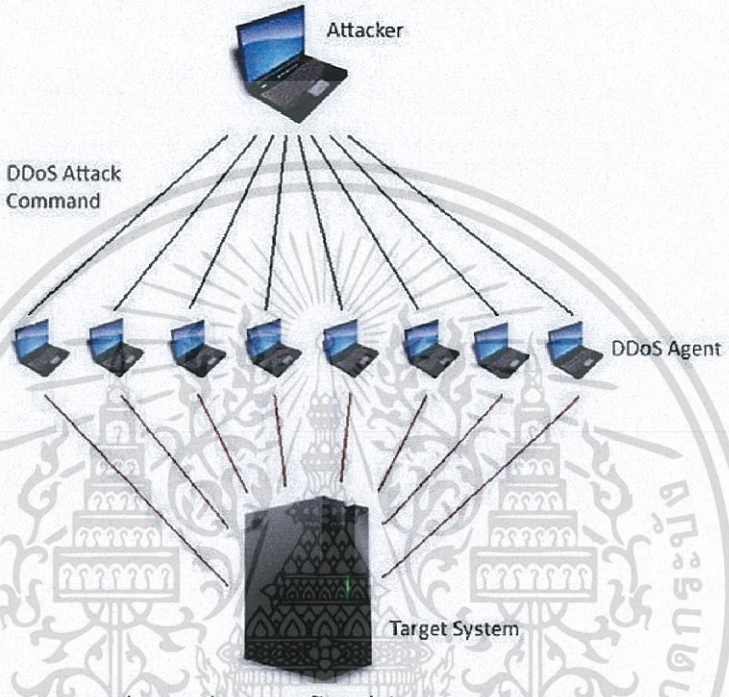


รูป 2.3 รูปแบบการโจมตีประเภท DoS

2.4.2 Distributed Denial of Service Attack

การโจมตีแบบ Distributed Denial of Service (DDoS) คือการโจมตีในรูปแบบเดียวกันกับ DoS แต่จะต่างกันตรงที่ DDoS จะใช้หลายๆ เครื่องช่วยในการโจมตี ซึ่งจะให้ผลลัพธ์ที่เป็น

อันตรายและรวดเร็วมากกว่าการทำโดยใช้เครื่องเดียวมาก การโจมตีด้วยวิธีการ DDoS นี้นั้นการป้องกันเป็นไปได้ยากเพราะเกิดขึ้นจากหลายๆ ที่และหลายๆ จุดซึ่งการโจมตีด้วยวิธีการ DDoS จะเกิดขึ้นจากการที่ใช้ Bots ซึ่งเป็นโปรแกรมที่ทำหน้าที่บางอย่างโดยอัตโนมัติ เข้าไปฝังตัวอยู่ที่เครื่องคอมพิวเตอร์ของเหยื่อโดยจะเปลี่ยนให้คอมพิวเตอร์เครื่องนั้นกลายเป็น Zombies เพื่อที่จะรอรับคำสั่งต่างๆ จากผู้โจมตีโดยผ่านช่องทางต่างๆ เช่น IRC เป็นต้น



รูป 2.4 รูปแบบการโจมตีประเภท DDoS

รูปแบบการโจมตีและการป้องกัน DDoS

เครื่องมือที่ใช้โจมตีแบบ DDoS มีใช้กันอย่างแพร่หลาย และผู้ผลิตเองต่างก็มีวิธีป้องกันการโจมตีเช่นเดียวกัน รูปแบบการโจมตีที่นิยมใช้ เช่น SYN flood, UDP flood, ICMP flood, Smurf, Fraggle เป็นต้น

2.4.2.1 การโจมตีแบบ SYN Flood

เป็นการโจมตีโดยการส่งแพ็คเก็ต TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ Source Address ได้) เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายัง Source IP Address ที่ระบุไว้ ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน Source IP Address ไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิดสภาวะ half-open ขึ้นที่เครื่องเป้าหมาย หากมีการส่ง SYN flood จำนวนมาก ก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม ทำให้ไม่สามารถให้บริการตามปกติได้ นอกจากนี้ SYN flood ที่ส่งไปจำนวนมาก ยังอาจจะทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่อีกด้วย

2.4.2.2 การโจมตีแบบ Ping of Death

เป็นการส่งแพ็คเก็ต ICMP ขนาดใหญ่จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่

2.4.2.3 การโจมตีแบบ UDP Flood

เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่ และ/หรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด โดยจะส่ง UDP packet ไปยัง port ที่กำหนดไว้

2.4.2.4 การโจมตีแบบ Teardrop

โดยปกติเราเตอร์ (Router) จะไม่ยอมให้แพ็กเก็ตขนาดใหญ่ผ่านได้ จะต้องทำการ Fragment เสียก่อนจึงจะยอมให้ผ่านได้ และเมื่อผ่านไปแล้วเครื่องของผู้รับปลายทางจะนำแพ็กเก็ตที่ถูกแบ่งออกเป็นชิ้นส่วนต่าง ๆ ด้วยวิธีการ Fragment มารวมเข้าด้วยกันเป็นแพ็กเก็ตที่สมบูรณ์ การที่สามารถนำมารวมกันได้นี้จะต้องอาศัยค่า Offset ที่ปรากฏอยู่ในแพ็กเก็ตแรกและแพ็กเก็ตต่อๆ ไป สำหรับการโจมตีแบบ Teardrop นี้ ผู้โจมตีจะส่งค่า Offset ในแพ็กเก็ตที่สองและต่อๆ ไปที่จะทำให้เครื่องรับปลายทางเกิดความสับสน หากระบบปฏิบัติการไม่สามารถรับมือกับปัญหานี้ก็จะทำให้ระบบหยุดการทำงานในทันที

2.4.2.5 การโจมตีแบบ Land Attack

ลักษณะการโจมตีประเภทนี้เป็นการส่ง SYN ไปที่เครื่องเป้าหมายเพื่อขอสถาปนาการเชื่อมต่อ ซึ่งเครื่องที่เป็นเป้าหมายจะต้องตอบรับคำขอการเชื่อมต่อด้วย SYN ACK ไปที่เครื่องคอมพิวเตอร์ต้นทางเสมอ แต่เนื่องจากว่า IP Address ของเครื่องต้นทางกับเครื่องที่เป็นเป้าหมายนี้มี IP Address เดียวกัน โดยการใช้วิธีการสร้าง IP Address ลวง (โดยข้อเท็จจริงแล้วเครื่องของ Hacker จะมี IP Address ที่ต่างกับเครื่องเป้าหมายอยู่แล้ว แต่จะใช้วิธีการทางซอฟต์แวร์ในการส่งแพ็กเก็ตที่ประกอบด้วยคำขอการเชื่อมต่อ พร้อมด้วย IP Address ปลอม) ซึ่งโปรโตคอลของเครื่องเป้าหมายไม่สามารถแยกแยะได้ว่า IP Address ที่เข้ามาเป็นเครื่องปัจจุบันหรือไม่ ก็จะทำการตอบสนองด้วย SYN ACK ออกไป หากแอดเดรสที่ขอเชื่อมต่อเข้ามาเป็นแอดเดรสเดียวกับเครื่องเป้าหมาย ผลก็คือ SYN ACK นี้จะย้อนเข้าหาตนเอง และเช่นกันที่การปล่อย SYN ACK แต่ละครั้งจะต้องมีการปันส่วนของหน่วยความจำเพื่อการนี้จำนวนหนึ่ง ซึ่งหากผู้โจมตีส่งคำขอเชื่อมต่อออกมาอย่างต่อเนื่องก็จะเกิดปัญหาการจัดสรรหน่วยความจำ

2.4.2.6 Smurf

ผู้โจมตีจะส่ง ICMP Echo Request ไปยัง Broadcast Address ในเครือข่ายที่เป็นตัวกลาง (Amplifier) โดยปลอม Source IP Address เป็น IP Address ของระบบที่ต้องการโจมตี ซึ่ง

จะทำให้เครือข่ายที่เป็นตัวกลางส่ง ICMP Echo Reply กลับไปยัง IP Address ของเป้าหมายทันที ซึ่งทำให้มีการใช้งานแบนด์วิดธ์ (Bandwidth) อย่างเต็มที่

2.4.2.7 การป้องกัน DDoS

1) การโจมตีที่เกิดขึ้นมักจะทำให้เกิดการใช้งานแบนด์วิดธ์จนเต็มที่ เช่น SYN flood ถ้าหากทำการกรองแพ็คเก็ตที่ ISP ได้ ก็จะสามารถลดผลกระทบที่จะเกิดขึ้นได้
2) ติดตั้ง hardware ที่มีขีดความสามารถสูงไว้ระหว่างเครือข่ายของท่านกับของระบบที่ต้องการป้องกัน เช่น การติดตั้งอุปกรณ์สวิทช์หรือเราเตอร์ประสิทธิภาพสูงที่สามารถทำ filtering รวมไปถึงการมีฟังก์ชั่น DoS Attack Protection ได้
3) โดยปกติการโจมตีแบบ DoS ผู้โจมตีมักจะโจมตีไปยังเป้าหมายโดยระบุเป็น IP Address โดยตรง ไม่ได้ผ่านการทำ DNS Lookup มาก่อน ดังนั้นเมื่อเกิดการโจมตีขึ้น ยังสามารถหาหนทางหลบหลีกการโจมตีดังกล่าวได้ 2 วิธีคือ 1. เปลี่ยน IP Address เมื่อเกิดการโจมตี 2. เปลี่ยน IP Address ไปเรื่อยๆ แม้จะไม่มีการโจมตี ซึ่งการกระทำทั้งสองรูปแบบก็มีข้อดีข้อเสียต่างกัน ในรูปแบบแรกจะต้องมีระบบตรวจจับที่ดี สามารถแจ้งเตือนผู้ดูแลระบบให้สามารถปรับเปลี่ยน IP Address ได้อย่างรวดเร็ว จะเห็นว่ามีช่องว่างระหว่างการดำเนินงานอยู่ แต่ก็มียังมีข้อดีที่ผู้โจมตีจะไม่สามารถรู้แทกติกนี้จนกว่าจะเริ่มโจมตี ในขณะที่วิธีที่สองจะมีความยากลำบากในการเริ่มโจมตีมากกว่า

2.4.3 Brute-force Attack

การโจมตีบางรูปแบบจะโจมตีจากทางด้านหลังของระบบ แต่การโจมตีแบบ Brute-force จะเป็นการโจมตีจากทางประตูหน้าของระบบ เป็นการพยายามทดลองและเดารหัสผ่านของระบบ ซึ่ง Brute-force Attack นั้นเป็นหนึ่งในสี่ของการโจมตีระบบเครือข่าย โดยมักจะใช้การคาดเดารหัสผ่านหลายร้อยหรือหลายพันชุดเพื่อโจมตีระบบ

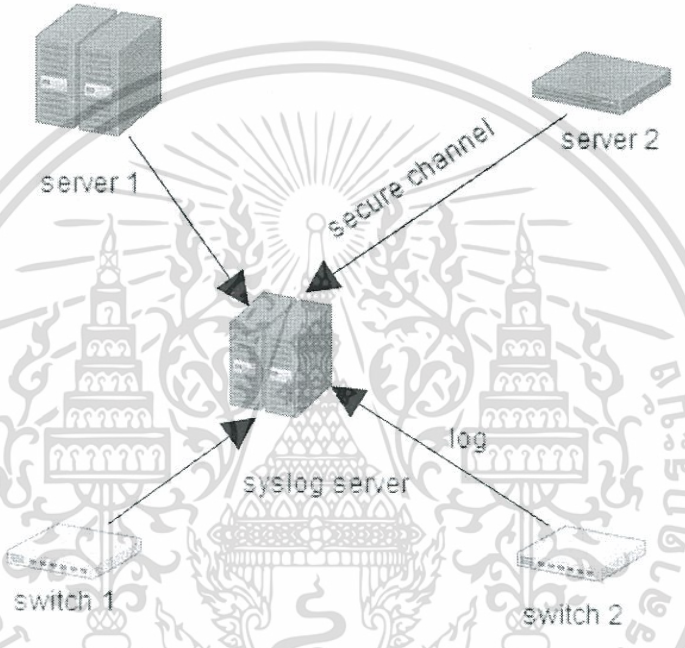
ซึ่งการป้องกันการโจมตีแบบ Brute-force ก็มีหลายวิธี หนึ่งในวิธีที่ง่าย คือการล็อคบัญชีผู้ใช้หากมีจำนวนการเข้าระบบที่มากเกินไป

2.4.4 Shellshock Attack

ช่องโหว่นี้สามารถทำการรีโมทโค้ดคำสั่งที่ทำงานได้โดยข้ามขั้นตอนการตรวจสอบ การยืนยันสิทธิ์ ซึ่งหากมีกลุ่มผู้ไม่หวังดีต้องการสร้างความเสียหาย อาจส่งโค้ดอันตรายเพื่อควบคุมระบบปฏิบัติการ สามารถเข้าถึงข้อมูลลับต่างๆ หรือแฝงตัวซุ่มโจมตีในอนาคตได้อย่างง่ายดาย

2.5 การจัดเก็บบันทึกกิจกรรมส่วนกลาง (Centralized Logging)

คือการรวบรวมบันทึกกิจกรรมไว้ที่คอมพิวเตอร์ส่วนกลาง เพื่อสะดวกต่อการนำมาวิเคราะห์และตรวจสอบเมื่อเกิดปัญหาหรือตรวจพบการโจมตีต่างๆ โดยใช้ซิสลอกเซิร์ฟเวอร์ (Syslog Server) ในการรวบรวมบันทึกกิจกรรมจากเซิร์ฟเวอร์ที่ให้บริการต่างๆ และใช้พอร์ตสำหรับแสดงผล (Monitoring Port) สำหรับส่งข้อมูลบันทึกกิจกรรมจากอุปกรณ์อื่นๆ เช่น สวิตช์ ภายในเครือข่ายผ่านช่องทางการสื่อสารแบบปลอดภัย (Secure Channel)



รูป 2.5 ตัวอย่างการทำ Centralized Logging

2.5.1 ช่องทางการสื่อสารแบบปลอดภัย (Secure Channel)

คือช่องทางการส่งข้อมูลที่มีการป้องกันการดักฟัง ทนทานต่อการปลอมแปลงข้อมูลและเช่น SSL (Secure Sockets Layer) , TLS (Transport Layer Security) โดยในการส่งข้อมูลระหว่างกันนั้นจะถูกเข้ารหัสด้วยการเข้ารหัสแบบกุญแจสมมาตร (Symmetric key Cryptography) เอาไว้ เนื่องจากการถอดรหัสลับของการเข้ารหัสลับแบบกุญแจสมมาตรนั้นจะต้องใช้กุญแจเดียวกันกับการเข้ารหัสลับทำให้ต้องส่งกุญแจไปให้อีกฝ่ายด้วยและในการส่งกุญแจสมมาตรสำหรับรหัสลับนั้น ตัวกุญแจจะถูกเข้ารหัสลับด้วยการเข้ารหัสลับแบบกุญแจไม่สมมาตร (Asymmetric key Cryptography) เอาไว้ และใช้ Certificate ที่อนุมัติโดย CA (Certificate Authority) เพื่อการยืนยันว่าผู้ส่งข้อมูลคือผู้ที่เราต้องการจะรับส่งข้อมูลด้วย

2.5.2 การเข้าและถอดรหัสลับด้วยกุญแจสมมาตร (Symmetric Key Cryptography)

คือการเข้ารหัสลับที่ใช้กุญแจในการเข้ารหัสลับและการถอดรหัสลับเป็นกุญแจเดียวกัน เช่น

2.5.2.1 Data Encryption Standard (DES)

การเข้ารหัสลับชนิดนี้ได้รับการรับรองโดยรัฐบาลสหรัฐอเมริกาในปี ค.ศ. 1977 ให้เป็นมาตรฐานการเข้ารหัสข้อมูลสำหรับหน่วยงานของรัฐทั้งหมด ในปี 1981 อัลกอริทึมยังได้รับการกำหนดให้เป็นมาตรฐานการเข้ารหัสข้อมูลในระดับนานาชาติตามมาตรฐาน ANSI (American National Standards) อีกด้วย แต่เนื่องจากขนาดความยาวของกุญแจที่มีขนาดเพียง 56 บิต ซึ่งในปัจจุบันถือว่าสั้นเกินไป ทำให้เกิดการนำ DES มาประยุกต์ใช้โดยการเข้ารหัสลับด้วย DES 3 ครั้ง เรียกว่า Triple-DES จึงเปรียบเสมือนการใช้กุญแจเข้ารหัสที่มีความยาว 168 บิต

2.5.2.2 Advanced Encryption Standard (AES)

หรือรู้จักกันในชื่อ Rijndael เป็นการเข้ารหัสลับที่ได้รับการคัดเลือกโดยหน่วยงาน National Institute of Standard and Technology (NIST) ของสหรัฐอเมริกาให้เป็นมาตรฐานในการเข้ารหัสชั้นสูงของประเทศ โดยสามารถใช้กุญแจที่มีความยาวขนาด 128, 192 และ 256 บิต

2.5.2.3 Blowfish

เป็นการเข้ารหัสลับแบบบล็อคโดยสามารถใช้กุญแจที่มีความยาวตั้งแต่ 32 บิตไปจนถึง 448 บิตทำให้เกิดความยืดหยุ่นสูงในการเลือกใช้กุญแจ

2.5.3 การเข้าและถอดรหัสลับด้วยกุญแจไม่สมมาตร (Asymmetric Key Cryptography)

คือการเข้ารหัสลับที่ใช้กุญแจในการเข้ารหัสลับและการถอดรหัสลับเป็นคนละกุญแจกัน เช่น RSA

2.6 Schedule Tasks

คือการทำให้โปรแกรมทำงานเป็นรอบตามเวลาที่เรากำหนดเช่น ให้โปรแกรมทำงานทุก ๆ 5 นาทีให้โปรแกรมทำงานในทุกวันศุกร์เวลาเที่ยงคืน เป็นต้น

2.7 IDS/IPS

2.7.1 Intrusion Detection System (IDS)

ระบบตรวจจับการบุกรุกหรือ IDS เป็นระบบตรวจจับและแจ้งเตือนภัยของเครือข่ายสัญญาณป้องกันขโมยเป็นระบบที่ใช้สำหรับตรวจจับผู้ไม่ประสงค์ดีที่พยายามจะบุกรุกเข้าสถานที่ต้องห้าม IDS ก็ทำงานคล้ายกันโดยจะแยกแยะได้ระหว่างการเข้าถึงส่วนของเครือข่ายโดยไม่ได้รับอนุญาต หรือเป็นการเข้ามาโดยผิดปกติ IDS นั้นมีหลายประเภท การเลือกใช้งานนั้นก็ขึ้นอยู่กับ

ความเสี่ยงและทรัพยากรที่มีอยู่ขององค์กร IDS อาจต้องใช้ทรัพยากรค่อนข้างมากจากฝ่ายรักษาความปลอดภัย

ระบบตรวจจับการบุกรุกที่รู้จักกันมากที่สุด คือซอร์ฟแวร์ป้องกันไวรัส ซึ่งซอร์ฟแวร์นี้ควรติดตั้งบนคอมพิวเตอร์ทุกเครื่องรวมไปถึงเครื่องเซิร์ฟเวอร์ด้วย ซอร์ฟแวร์ป้องกันไวรัสเป็น IDS ที่ใช้ทรัพยากรน้อยที่สุด

IDS แบ่งออกเป็น 2 ประเภทคือ

1) Host-based IDS : ตรวจจับการบุกรุกเข้ามาในเครื่อง
2) Network-based IDS : ตรวจจับการบุกรุกเข้ามาในเครือข่าย

การตรวจสอบล็อกไฟล์ด้วยมือนั้นเป็นวิธีที่อาจได้ผลดี แต่ก็เป็นวิธีที่ใช้เวลามากและมีโอกาสที่จะเกิดข้อผิดพลาดได้สูง โดยธรรมชาติมนุษย์จะไม่สามารถตรวจสอบล็อกไฟล์ได้อย่างมีประสิทธิภาพเท่าที่ควร เนื่องจากล็อกไฟล์อาจมีจำนวนมากเกินความสามารถของมนุษย์ที่จะตรวจสอบ ดังนั้นซอร์ฟแวร์ที่ใช้ตรวจวิเคราะห์ล็อกไฟล์แบบอัตโนมัตินั้นอาจเป็นทางออกที่ดีกว่า

2.7.2 Intrusion Prevention System (IPS)

ระบบตรวจจับและป้องกันการบุกรุก หรือ IPS คือระบบที่คอยตรวจจับการบุกรุกของผู้ที่ไม่ประสงค์ดี รวมไปถึงข้อมูลจำพวกไวรัสด้วย โดยสามารถทำการวิเคราะห์ข้อมูลทั้งหมดที่ผ่านเข้าออกภายในเครือข่ายว่า มีลักษณะการทำงานที่เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายต่อระบบเครือข่ายหรือไม่ เมื่อตรวจพบข้อมูลที่มีลักษณะการทำงานที่เป็นความเสี่ยงต่อระบบเครือข่ายก็จะทำการป้องกันข้อมูลดังกล่าวนั้น ไม่ให้เข้ามาภายในเครือข่ายได้

IPS สามารถแบ่งได้เป็น 2 ประเภทใหญ่ๆ คือ

1) แบ่งตามแพลตฟอร์ม
2) แบ่งตาม Attack timeline

2.7.2.1 แบ่งตามแพลตฟอร์ม (Network / Host based)

การแบ่งตามประเภทของแพลตฟอร์ม จะแบ่งได้เป็น 2 ประเภท คือ Network Intrusion Prevention System (NIPS) และ Host Intrusion Prevention System (HIPS) ซึ่ง NIPS เฝ้ามอง traffic ภายในระบบเน็ตเวิร์คว่ามีการมุ่งประสงค์ร้ายจากภายนอกที่น่าสงสัยหรือไม่ หรือมีกิจกรรมภายในเน็ตเวิร์คที่น่าสงสัยหรือไม่ ถ้าพบก็จะปิดกั้นเครือข่ายที่น่าสงสัยเหล่านั้น ส่วน HIPS นั้นจะถูกติดตั้งให้อยู่ในเครื่องโฮสต์ หน้าที่ทั่วไปคือ เฝ้ามองส่วนของการร้องขอ (Request) ของระบบแล้วปิดกั้นการร้องขอที่ไม่เหมาะสม ในส่วนของ NIPS นั้นจะแจ้งเตือนปัญหาและป้องกันในส่วนของสภาพแวดล้อมของเครือข่าย ในขณะที่ HIPS จะเจาะจงไปยังเครื่องโฮสต์เครื่องใดเครื่องหนึ่งเท่านั้น

2.7.2.2 แบ่งตาม Attack timeline

เป็นการแบ่งตามความสามารถในการตรวจจับการโจมตีแบบ “zero-day” ซึ่งขึ้นอยู่กับฐานข้อมูลที่มี แต่ถ้าไม่มีการอัพเดทเพิ่มเติมนั้น ในกรณีนี้การโจมตี “zero-day” เป็นการโจมตีที่ไม่สามารถตรวจจับได้ แล้วเมื่อสามารถแยกแยะรูปแบบการโจมตีได้แล้ว จึงเรียกว่าการโจมตีที่สามารถตรวจจับได้ ดังนั้นการตรวจจับการโจมตีที่ไม่สามารถตรวจจับได้แต่เดิมจะช่วยให้ความสามารถในการป้องกันของ IPS เพิ่มมากขึ้น ในขณะที่การตรวจจับการโจมตีที่สามารถตรวจจับได้นั้น ทำให้แยกความแตกต่างของชนิดและรูปแบบการโจมตีได้แบบเฉพาะเจาะจงได้มากขึ้น

บทที่ 3

การออกแบบและพัฒนา

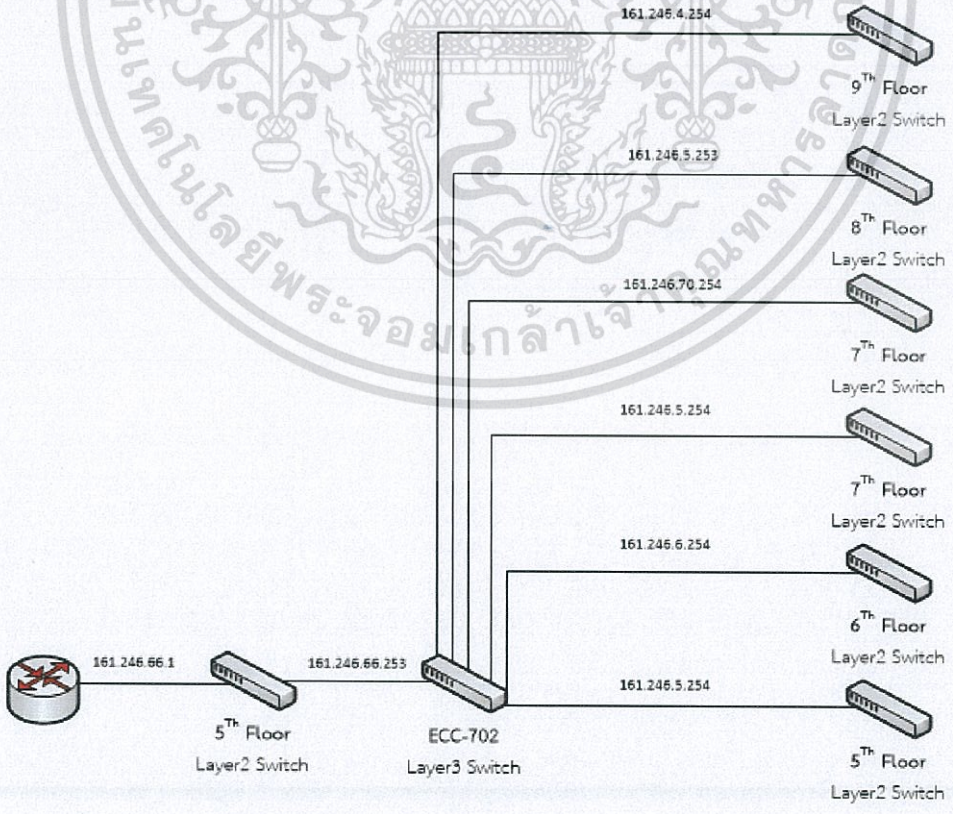
3.1 รายละเอียดของระบบที่พัฒนา

3.1.1. จัดทำตารางรวบรวมสินทรัพย์ภายในภาควิชาวิศวกรรมคอมพิวเตอร์

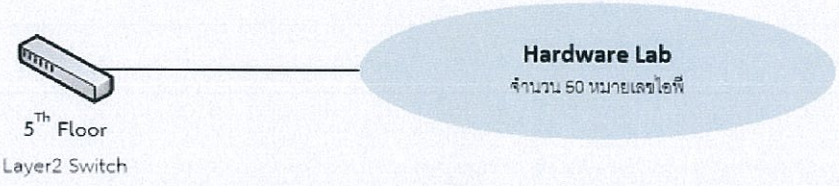
ทำการรวบรวมรายการทรัพย์สินทั้งหมดภายในภาควิชาวิศวกรรมคอมพิวเตอร์ โดยแบ่งเป็นรายการทรัพย์สินด้านอินเทอร์เน็ตโพรโทคอล (IP Device) และรายการทรัพย์สินด้านตัวอุปกรณ์และการตั้งค่าต่างๆ เพื่อนำมาเป็นข้อมูลในการประเมิน และตรวจสอบความเสี่ยงที่อาจเกิดขึ้นได้ในเครือข่ายของภาควิชาฯ

3.1.2 แผนภาพเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์

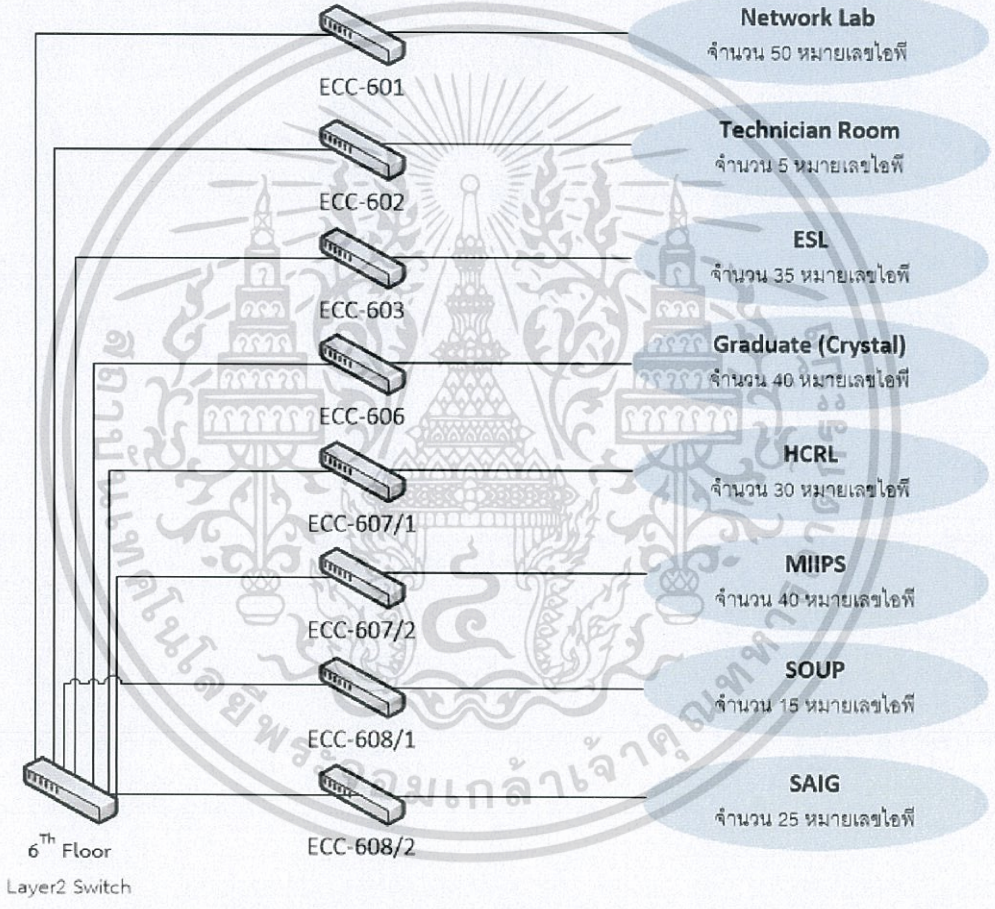
จากการรวบรวมข้อมูลรายการสินทรัพย์ด้านอินเทอร์เน็ตโพรโทคอล (IP device) จึงทราบถึงเครือข่ายในภาควิชาฯ และจัดทำแผนภาพแสดงเครือข่ายภาควิชาฯ เพื่อทำให้ง่ายกับการวิเคราะห์ การออกแบบ การแก้ไขปัญหาต่างๆที่อาจเกิดขึ้นในเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์



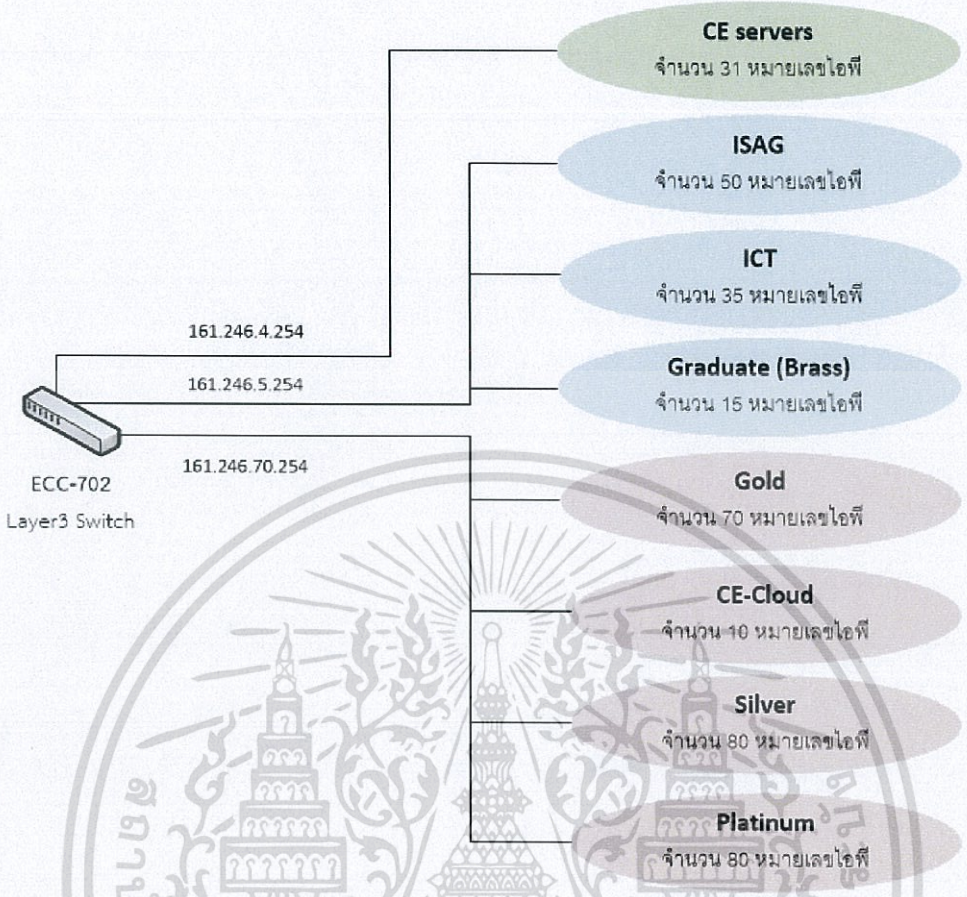
รูป 3.1 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์โดยรวม



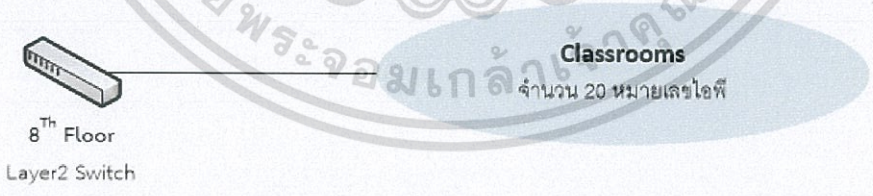
รูป 3.2 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 5



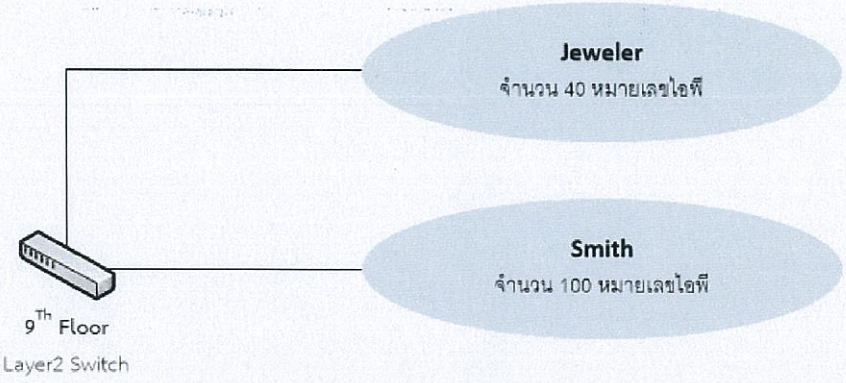
รูป 3.3 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 6



รูป 3.4 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 7



รูป 3.5 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 8



รูป 3.6 เครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ของตึก ECC ชั้นที่ 9

3.2 การวิเคราะห์ปัญหาที่เกิดขึ้นของระบบเครือข่ายภาควิชาฯ

3.2.1 ช่องโหว่ที่พบและการออกแบบวิธีการตรวจจับผู้บุกรุกจากเหตุการที่เกิดขึ้นจริง

1) พบว่าการตั้งค่าการเข้าถึงระบบปฏิบัติการของสวิตช์ในภาควิชาฯ เป็นการใช้เทลเน็ต (Telnet) ซึ่งไม่มีการเข้ารหัสลับในการเชื่อมต่อ
2) การตรวจสอบบันทึกกิจกรรมของทั้งเครือข่ายภาควิชาฯ ทำได้ยาก เนื่องจากกระจัดกระจายไปตามเครื่องต่างๆ ภายในเครือข่าย
3) เกิดเหตุการณ์ที่ไม่สามารถเข้าเว็บไซต์ภาควิชาฯ ได้ จากการวิเคราะห์ทำให้ทราบสาเหตุ ซึ่งเกิดจากมีผู้โจมตีระบบด้วยวิธีการ DDoS Attack
4) ตรวจพบว่าไม่สามารถใช้งานอินเทอร์เน็ตภายในเครือข่ายภาควิชาฯ จากการวิเคราะห์ทำให้ทราบสาเหตุของปัญหา ซึ่งสาเหตุในแต่ละครั้งก็มีที่ไม่เหมือนกัน ได้แก่
   - สวิตช์ตัวหลักของภาควิชาฯ มีการทำงานผิดปกติ
   - เครือข่ายอินเทอร์เน็ตของสำนักบริการคอมพิวเตอร์มีปัญหา
   - สายแพตช์ใยแก้วนำแสงระหว่างพาแนลไปยังสวิตช์ L2 ระหว่างตู้ของชั้น 5 เสื่อมสภาพ

3.3 ดำเนินการพัฒนาเพื่อแก้ไขปัญหา

จากปัญหาที่พบในเครือข่ายภาควิชาฯ จึงได้มีการออกแบบการแก้ไขปัญหาที่เกิดขึ้นดังนี้

3.3.1 เปลี่ยนการเข้าถึงของสวิตช์

เปลี่ยนการเข้าถึงระบบปฏิบัติการของสวิตช์เป็นการใช้ซีเคียวเชลล์ (SSH) แทนการใช้เทลเน็ต (Telnet) เพื่อให้การส่งข้อมูลมีการเข้ารหัสลับ

3.3.2 จัดทำระบบจัดเก็บบันทึกกิจกรรมส่วนกลาง

เพื่อรวบรวมบันทึกกิจกรรมที่กระจัดกระจายอยู่ตามเครื่องต่างๆ ภายในระบบเครือข่ายภาควิชาฯ นำมาเก็บรวมไว้ที่เดียวกันเพื่อให้ง่ายต่อการตรวจสอบบันทึกกิจกรรม

3.3.3 ติดตั้งโปรแกรมตรวจจับการโจมตีของผู้บุกรุก (Snort)

เพื่อดักจับการโจมตีต่างๆ จากผู้บุกรุก และแจ้งเตือนผู้ดูแลระบบให้ได้ทราบ

3.3.4 ติดตั้งโปรแกรมตรวจสอบสถานะของเครื่องที่ต้องการตรวจสอบ (Zabbix)

เพื่อตรวจสอบสถานะต่างๆ ของเครื่องที่ต้องการจะตรวจสอบว่าเครื่องๆ นั้นยังสามารถให้บริการได้อยู่หรือไม่

3.3.5 จัดทำสคริปสำหรับระบุปัญหาในการเชื่อมต่ออินเทอร์เน็ตเบื้องต้น

เพื่อทำให้ทราบว่ามีปัญหาในการเชื่อมต่ออินเทอร์เน็ตที่จุดใด เมื่อไม่สามารถใช้งานอินเทอร์เน็ตได้

3.3.6 ติดตั้งโปรแกรมตรวจสอบการใช้งานในระบบเครือข่ายอินเทอร์เน็ตของภาควิชาวิศวกรรมคอมพิวเตอร์ (ntop)

เพื่อตรวจสอบ Traffic การใช้งานของอินเทอร์เน็ตของ User แต่ละคน

3.3.7 เครื่องมือที่ใช้ในการพัฒนา

1) สภาพแวดล้อมในการพัฒนา
   - หน่วยประมวลผล Intel® Core™ i5
   - หน่วยความจำหลัก 4 GB
   - ระบบปฏิบัติการ Ubuntu

บทที่ 4

การทดลองและผลการทดลอง

4.1 การทดลองเปลี่ยนการตั้งค่าการเข้าถึงสวิตช์จากเทลเน็ต (Telnet) เป็นซีเคียวเชลล์ (SSH)

โดยการทดลองนี้ได้ทำการทดลองกับสวิตช์ของ Cisco รุ่น WS-X4013 - CatOS 6.3(3) การทดลองนี้ทำเพื่อ เตรียมการเปลี่ยนจากการเชื่อมต่อสวิตช์ด้วยการเทลเน็ต (Telnet) ซึ่งไม่มีการเข้ารหัสลับใดๆ เป็นซีเคียวเชลล์ (SSH) ที่มีการเข้ารหัสลับในการส่งข้อมูล

ตัวอย่าง 4.1 คำสั่งที่ใช้ทดลองการตั้งค่าสวิตช์รุ่น WS-X4013 - CatOS 6.3(3)

```
Router> enable
Router# configure terminal
Router(config)# ip domain-name xxx.com
Router(config)#  crypto key gen rsa
How many bits in modulus : 1024
Router(config)#  line vty 0 4
Router(config-line)# login local
Router(config-line)# transport input ssh
Router(config-line)# exit
Router(config)# username admin priv 15 secret PwD
Router(config)# line vty 0 4
Router(config)# exec-timeout 5
```

จากการทดลองสามารถเชื่อมต่อด้วยซีเคียวเชลล์ (SSH) และไม่สามารถใช้เทลเน็ต (Telnet) ในการเชื่อมต่อได้

4.2 ทดลองการรวบรวมบันทึกกิจกรรมมาที่ส่วนกลาง

ในการจัดทำบันทึกกิจกรรมส่วนกลางนั้นมีเครื่องมือให้เลือกใช้มากมาย ทางกลุ่มของผู้พัฒนาใช้เครื่องมือในการทำคือ Syslog-ng ซึ่งเป็นโปรแกรมโอเพนซอร์ซ (open source) ในระบบปฏิบัติการประเภท Linux โดยจะมีการติดตั้งแบ่งออกเป็น 2 ส่วนคือ

1) ส่วนของ syslog - server
2) ส่วนของ syslog - client

4.2.1 Syslog – server

คือ เซิร์ฟเวอร์ที่ใช้ในการรวบรวมบันทึกกิจกรรมจากเครื่องอื่นๆ ในเครื่องข่ายเอาไว้

ขั้นตอนการติดตั้งและตั้งค่าสำหรับ Syslog – server

1) ทำการติดตั้งโปรแกรม Syslog
   - ระบบปฏิบัติการ Debian/Ubuntu
     - # apt-get install syslog-ng
   - ระบบปฏิบัติการ Fedora/Centos
     - # yum install syslog-ng
   - ระบบปฏิบัติการอื่นๆ
     - โหลดโปรแกรมได้จาก https://github.com/balabit/syslog-ng แล้วใช้คำสั่ง $ ./configure && make && make install
2) เริ่มการตั้งค่าโดยเข้าไปที่ไฟล์ /etc/syslog-ng/syslog-ng.conf ตั้งค่าเลขที่อยู่ไอพี (IP Address) ของเครื่องผู้รับบริการและโพรโทคอลที่ใช้ ดังคำสั่ง ตามตัวอย่าง 4.2

ตัวอย่าง 4.2 คำสั่งตั้งค่า IP Address ของเครื่องผู้รับบริการในฝั่ง Server

```
source s_network { syslog(ip(<Client IP Address>) transport("tcp")); };
```

3) ตั้งค่าสถานที่เก็บบันทึกการสนทนาที่ได้รับ

ตัวอย่าง 4.3 คำสั่งตั้งค่าสถานที่เก็บบันทึกสนทนาในฝั่ง Server

```
destination d_local {
    file("/var/log/messages"); };
```

หรือถ้าต้องการแยกไฟล์แต่ละไฟล์ที่เก็บข้อมูลของแต่ละเครื่องที่ใช้บริการ

ตัวอย่าง 4.4 คำสั่งแยกไฟล์ที่เก็บข้อมูลของแต่ละเครื่องที่ใช้บริการในฝั่ง Server

```
destination d_local {
    file("/var/log/messages_${HOST}"); };
```

4) เริ่มการทำงานของการส่งข้อมูล

ตัวอย่าง 4.5 คำสั่งเริ่มการทำงานของการส่งข้อมูลในฝั่ง Server

```
log {
        source(s_local); source(s_network); destination(d_local); };
```

4.2.2 Syslog – client

ขั้นตอนการติดตั้งและตั้งค่าสำหรับ Syslog – client

1) ทำการติดตั้งโปรแกรม Syslog
   - ระบบปฏิบัติการ Debian/Ubuntu
     - # apt-get install syslog-ng
   - ระบบปฏิบัติการ Fedora/Centos
     - # yum install syslog-ng
   - ระบบปฏิบัติการอื่นๆ
     - โหลดโปรแกรมได้จาก https://github.com/balabit/syslog-ng แล้วใช้คำสั่ง $ ./configure && make && make install
2) เข้าไปตั้งค่าโปรแกรมที่ /etc/syslog-ng/syslog-ng.conf
3) สร้างเครือข่ายที่ปลายทางที่ติดต่อโดยตรงกับ Syslog Server เครือข่ายปลายทางนั้นจะขึ้นกับโพรโทคอลที่ใช้

ตัวอย่าง 4.6 คำสั่งสร้างเครือข่ายปลายทางของ Server

```
destination d_network { syslog(ip(<Client IP Address>))
transport("tcp")); };
```

4) สร้างคำสั่งสำหรับการติดต่อกับเซิร์ฟเวอร์ (Server)

ตัวอย่าง 4.7 คำสั่งสร้างการติดต่อกับ Server

```
log {
        source(s_local); destination(d_network); };
```

4.3 ทดลองติดตั้งและทดสอบโปรแกรมดักจับผู้บุกรุกที่เข้ามาโจมตีเว็บไซต์ของภาควิชาวิศวกรรมคอมพิวเตอร์ (Snort)

บ่อยครั้งที่เว็บไซต์ของทางภาควิชาวิศวกรรมคอมพิวเตอร์นั้นถูกโจมตีให้เว็บไซต์ไม่สามารถให้บริการได้อย่างปกติจากผู้ไม่ประสงค์ดี และทำให้ผู้ดูแลระบบนั้นต้องเข้ามาตรวจสอบระบบจากล็อคไฟล์ที่อยู่ในเครื่องเซิร์ฟเวอร์เพื่อระบุถึงสาเหตุของการหยุดให้บริการ และทำการแก้ไข

ดังนั้นการที่มีระบบดักจับการโจมตีของผู้บุกรุก และมีการแจ้งเตือนถึงสาเหตุของการหยุดให้บริการนั้นจะทำให้ผู้ดูแลระบบสามารถทราบถึงประเภทของการโจมตี และทราบว่าใครเป็นผู้ที่กระทำ ทำให้ผู้ดูแลระบบสามารถแก้ไขปัญหาได้สะดวกขึ้น

4.3.1 ขั้นตอนการติดตั้งโปรแกรมดักจับผู้บุกรุก Snort

1) ติดตั้งโปรแกรมที่เกี่ยวข้องกับ Snort ดังโปรแกรม 4.1

โปรแกรม 4.1 คำสั่งติดตั้งโปรแกรมที่เกี่ยวข้องกับ Snort

```
sudo apt-get install -y build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex
zlib1g-dev
```

2) สร้างไดเร็กทอรี่ที่จะบันทึกไฟล์ที่ดาวน์โหลด ดังโปรแกรม 4.2

โปรแกรม 4.2 คำสั่งสร้างไดเร็กทอรี่ที่จะบันทึกไฟล์ที่ดาวน์โหลด

```
mkdir ~/snort_src
cd ~/snort_src
```

3) ดาวน์โหลด DAQ ของ Snort (ควรเป็นเวอร์ชั่นล่าสุดเสมอ)

โปรแกรม 4.3 คำสั่งดาวน์โหลด DAQ ของ Snort

```
wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
tar -xvzf daq-2.0.6.tar.gz
cd daq-2.0.6
./configure
make
sudo make install
```

4) ดาวน์โหลดตัวโปรแกรม Snort (ควรเป็นเวอร์ชั่นล่าสุดเสมอ)

โปรแกรม 4.4 คำสั่งดาวน์โหลดตัวโปรแกรม Snort

```
cd ~/snort_src
wget https://www.snort.org/downloads/snort/snort-2.9.8.2.tar.gz
tar -xvzf snort-2.9.8.2.tar.gz
cd snort-2.9.8.2
./configure --enable-sourcefire
make
sudo make install
```

5) Update Libraries

โปรแกรม 4.5 คำสั่ง Update Libraries

```
sudo ldconfig
```

6) สร้าง shortcut เพื่อการเข้าถึงไฟล์ได้ง่ายและรวดเร็ว

โปรแกรม 4.6 คำสั่งสร้าง shortcut เพื่อการเข้าถึงไฟล์ได้ง่าย

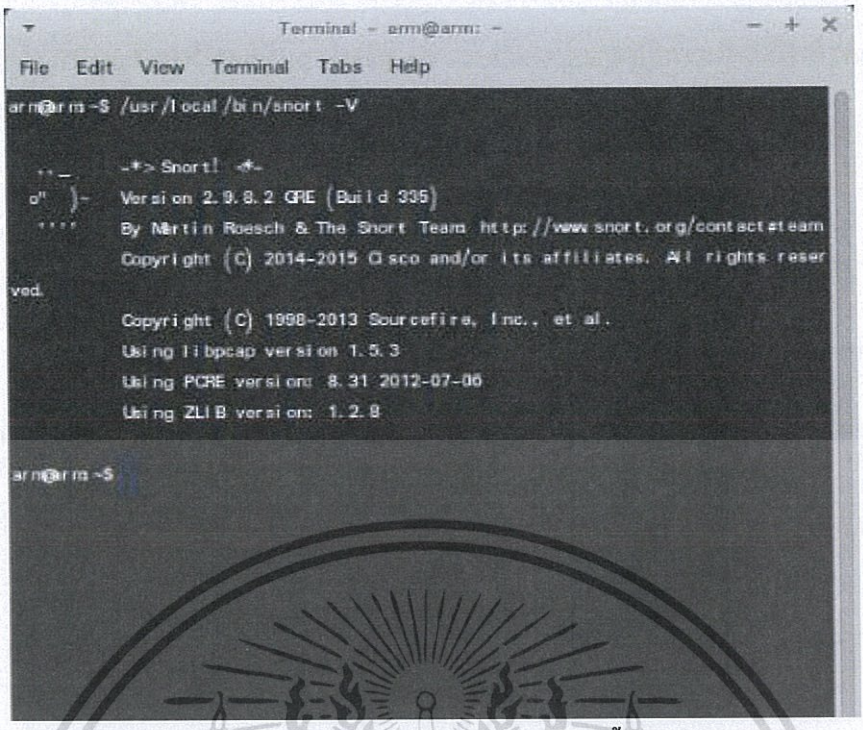
```
sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

7) ทดสอบการติดตั้ง Snort

โปรแกรม 4.7 คำสั่งทดสอบการติดตั้ง Snort

```
/usr/sbin/snort -V
```

ถ้าติดตั้งสำเร็จ จะแสดงดังรูป 4.4



รูป 4.1 ผลการทดสอบสำเร็จจากการติดตั้ง Snort

8) สร้างโฟลเดอร์ไว้รองรับไฟล์ต่างๆ ที่จำเป็น เช่น rules, preproc_rules เป็นต้น และสร้างไฟล์จำพวก blacklist และ whitelist รวมถึงกำหนดสิทธิ์เข้าถึงไฟล์

โปรแกรม 4.8 คำสั่งสร้างโฟลเดอร์ และไฟล์ต่างๆ รวมถึงกำหนดสิธิ์การเข้าถึงไฟล์

```
sudo mkdir /etc/snort
sudo mkdir /etc/snort/rules
sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules
sudo touch /etc/snort/rules/local.rules
sudo mkdir /etc/snort/preproc_rules
sudo mkdir /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrules
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
sudo chown -R snort:snort /etc/snort
```

โปรแกรม 4.8 คำสั่งสร้างโฟลเดอร์ และไฟล์ต่างๆ รวมถึงกำหนดสิทธิ์การเข้าถึงไฟล์ (ต่อ)

```
sudo chown -R snort:snort /var/log/snort
sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

9) ย้ายไฟล์มาไว้ที่ /etc/snort (จะเป็นโฟลเดอร์หลักในการแก้ไข)

โปรแกรม 4.9 คำสั่งย้ายไฟล์มาไว้ที่ /etc/snort

```
sudo cp ~/snort_src/snort-2.9.7.0/etc/*.conf* /etc/snort
sudo cp ~/snort_src/snort-2.9.7.0/etc/*.map /etc/snort
```

10) ขั้นตอนการตั้งค่าไฟล์ snort.conf

โปรแกรม 4.10 คำสั่งการตั้งค่าไฟล์ snort.conf

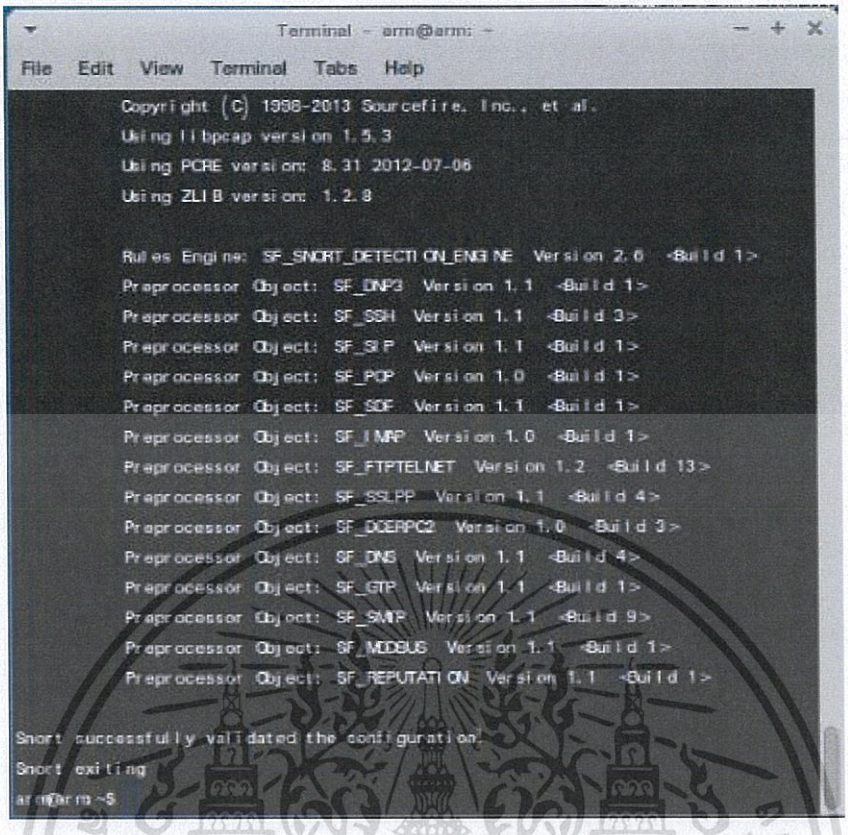
```
sudo nano /etc/snort/snort.conf
ipvar HOME_NET 10.0.0.0/24                    # (line 45) ใส่ ip address ของเครื่อง server
ipvar EXTERNAL_NET !$HOME_NET                 # (line 48)
var RULE_PATH /etc/snort/rules                # (line 104)
var SO_RULE_PATH /etc/snort/so_rules          # (line 105)
var PREPROC_RULE_PATH /etc/snort/preproc_rules  # (line 106)
var WHITE_LIST_PATH /etc/snort/rules          # (line 113)
var BLACK_LIST_PATH /etc/snort/rules          # (line 114)
include $RULE_PATH /local.rules               # (line 545)
```

11) หลังจาก Config ไฟล์เสร็จ ให้ทำการรันคำสั่งเพื่อทดสอบระบบที่เพิ่มเข้าไปใหม่ในไฟล์ snort.conf

โปรแกรม 4.11 คำสั่งรันคำสั่งเพื่อทดสอบระบบที่เพิ่มเข้าไปใหม่ในไฟล์ snort.conf

```
sudo snort -T -c /etc/snort/snort.conf
```

หากโปรแกรมสมบูรณ์ไม่มีปัญหาจะเป็นดังรูป 4.5



รูป 4.2 ผลการทดสอบสำเร็จจากการตั้งค่าไฟล์ snort.conf

12) การติดตั้ง barnyard2 ต้องดาวน์โหลดโปรแกรมที่เกี่ยวข้องกับ barnyard2 ซึ่งจะมีฐานข้อมูล mysql เข้ามาเกี่ยวด้วย

โปรแกรม 4.12 คำสั่งดาวน์โหลดโปรแกรมที่เกี่ยวข้องกับ barnyard2

```
sudo apt-get install -y mysql-server libmysqlclient-dev mysql-client autoconf libtool
```

แล้วจะได้รับการแจ้งเตือนสำหรับการกำหนดรหัสผ่าน root ของ mysql

13) ตั้งค่าที่ /etc/snort/snort.conf เพิ่มบรรทัดด้านล่างลงไปใต้บรรทัด 520 เพื่อสั่งให้โปรแกรมส่งออก logfiles

โปรแกรม 4.13 คำสั่งการตั้งค่าไฟล์ snort.conf เพื่อสั่งให้โปรแกรมส่งออก logfiles

```
output unified2: filename snort.u2, limit 128
```

14) ติดตั้งโปรแกรม barnyard2

โปรแกรม 4.14 คำสั่งการติดตั้งโปรแกรม barnyard2

```
cd ~/snort_src
wget https://github.com/firnsy/barnyard2/archive/v2-1.13.tar.gz
tar zxvf barnyard2-2-1.13.tar.gz
cd barnyard2-2-1.13
autoreconf -fvi -I ./m4
```

15) เลือกที่อยู่ไฟล์ MySQL libraries ตามรุ่นของคอมพิวเตอร์ (ในที่นี้คือ 64 bit)

โปรแกรม 4.15 คำสั่งเลือกที่อยู่ของไฟล์ MySQL Libraries

```
./configure --with-mysql --with-mysql-libraries=/usr/lib/x86_64-linux-gnu
make
sudo make install
```

16) ก็อปปี้, ให้สิทธิ์, สร้างไฟล์ ที่จำเป็นไว้ในโฟลเดอร์ Snort และโฟลเดอร์ Log File เพื่อการแก้ไขที่ง่ายและสะดวก

โปรแกรม 4.16 คำสั่งก็อปปี้, ให้สิทธิ์, สร้างไฟล์ ที่จำเป็นไว้ในโฟลเดอร์ Snort และโฟลเดอร์ Log File

```
cd ~/snort_src/barnyard2-2-1.13
sudo cp etc/barnyard2.conf /etc/snort
sudo mkdir /var/log/barnyard2
sudo chown snort.snort /var/log/barnyard2
sudo touch /var/log/snort/barnyard2.waldo
sudo chown snort.snort /var/log/snort/barnyard2.waldo
sudo touch /etc/snort/sid-msg.map
```

17) สร้างฐานข้อมูลชื่อ snort

โปรแกรม 4.17 คำสั่งสร้างฐานข้อมูลชื่อ snort

```
echo "create database snort;" | mysql -u root –p
mysql -u root -p -D snort < ~/snort_src/barnyard2-2-1.13/schemas/create_mysql
echo "grant create, insert, select, delete, update on snort.* to snort@localhost identified by
'snortpassword_xxxx'" | mysql -u root -p
```

18) ตั้งค่าไฟล์ barnyard.conf

โปรแกรม 4.18 คำสั่งตั้งค่าไฟล์ barnyard.conf

```
sudo nano /etc/snort/barnyard2.conf
ให้เพิ่มบรรทัดนี้เข้าไปในบรรทัดสุดท้ายของไฟล์
output database: log, mysql, user=snort password=snortpassword_xxxx' dbname=snort
host=localhost
```

19) กำหนดสิทธิ์เพื่อป้องกันไม่ให้ผู้ใดเข้ามาอ่านไฟล์ได้

โปรแกรม 4.19 คำสั่งกำหนดสิทธิ์เพื่อป้องกันไม่ให้ผู้ใดเข้ามาอ่านไฟล์ได้

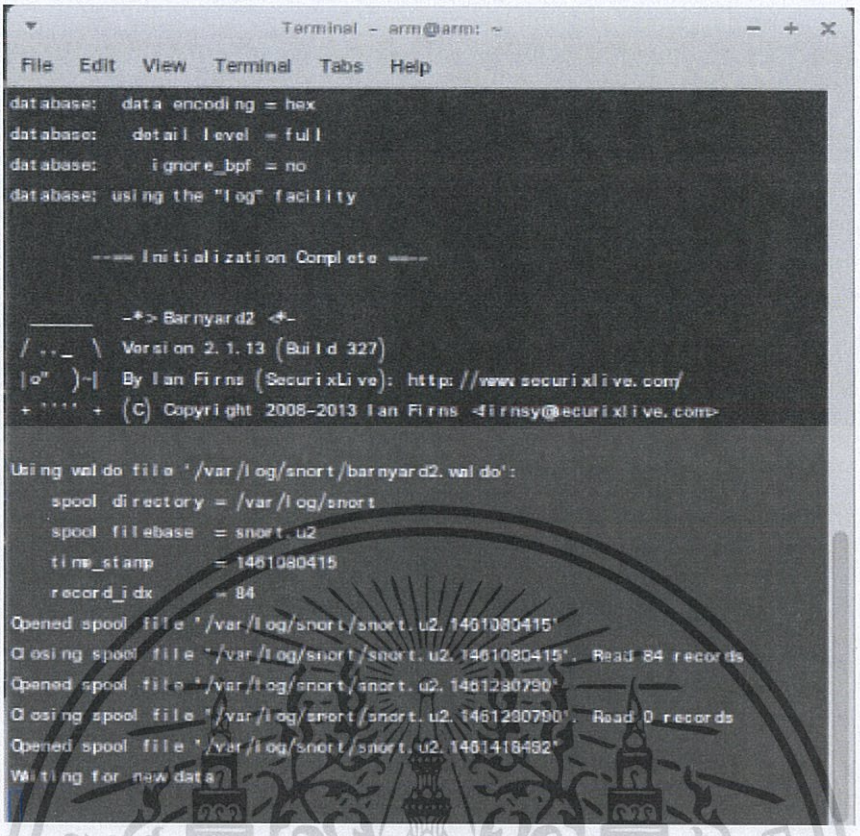
```
sudo chmod o-r /etc/snort/barnyard2.conf
```

20) เปิดใช้งาน Snort คู่กับ barnyard2 จำเป็นต้องเปิด Snort ก่อน

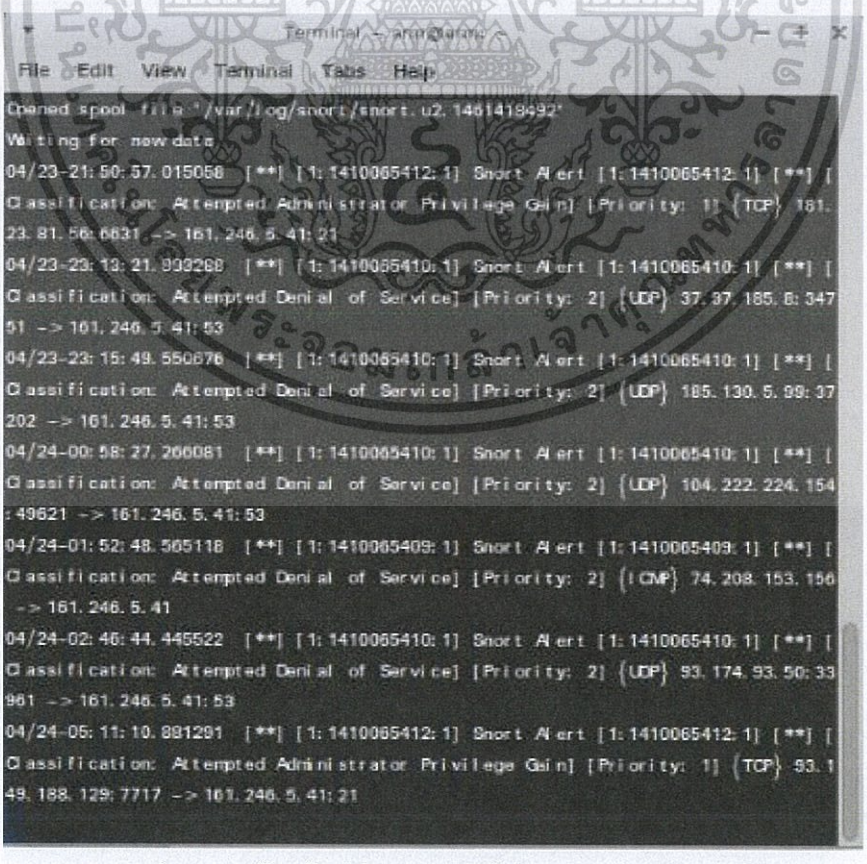
โปรแกรม 4.20 คำสั่งรันโปรแกรม Snort และ barnyard2

```
sudo /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth0
sudo barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 –w
/var/log/snort/barnyard2.waldo -g snort -u snort
```

และรอการโจมตีดังรูป 4.6 และรูป 4.7 ถ้ามีการโจมตีจะมีการแจ้งเตือน



รูป 4.3 การรัน Snort และรอการโจมตี



รูป 4.4 การโดนโจมตีการจากรันโปรแกรม barnyard2

21) ติดตั้งโปรแกรมที่เกี่ยวข้องของ Pulled Pork

โปรแกรม 4.21 ติดตั้งโปรแกรมที่เกี่ยวข้องของ Pulled Pork

```
sudo apt-get install -y libcrypt-ssleay-perl liblwp-useragent-determined-perl
```

22) ดาวน์โหลดโปรแกรม Pulled Pork และทำการติดตั้ง

โปรแกรม 4.22 คำสั่งดาวน์โหลดโปรแกรม Pulled Pork และทำการติดตั้ง

```
cd ~/snort_src
wget https://pulledpork.googlecode.com/files/pulledpork-0.7.0.tar.gz
tar xvfvz pulledpork-0.7.0.tar.gz
cd pulledpork-0.7.0/
sudo cp pulledpork.pl /usr/local/bin
sudo chmod +x /usr/local/bin/pulledpork.pl
sudo cp etc/*.conf /etc/snort
```

23) สร้างไฟล์ที่จำเป็นให้กับ Pulled Pork

โปรแกรม 4.23 คำสั่งสร้างไฟล์ที่จำเป็นให้กับ Pulled Pork

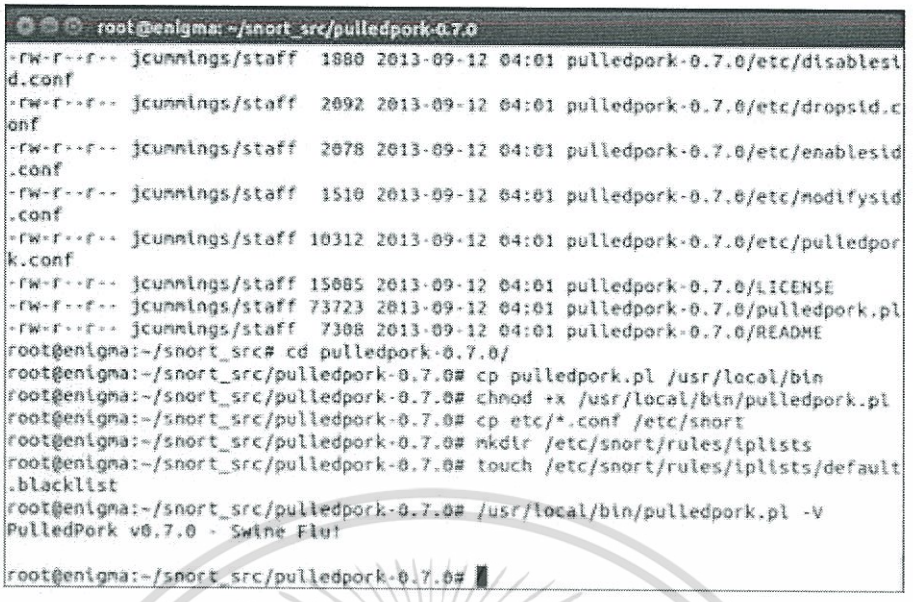
```
sudo mkdir /etc/snort/rules/iplists
sudo touch /etc/snort/rules/iplists/default.blacklist
```

24) ทดสอบโปรแกรม Pulled Pork

โปรแกรม 4.24 คำสั่งทดสอบโปรแกรม Pulled Pork

```
/usr/local/bin/pulledpork.pl -V
```

หากสำเร็จจะได้ผลดังรูป 4.8



รูป 4.5 การติดตั้งโปรแกรม Pulled Pork เสร็จสมบูรณ์

25) ดาวน์โหลดไฟล์ pulledpork.conf สำเร็จรูป

โปรแกรม 4.25 คำสั่งดาวน์โหลดไฟล์ pulledpork.conf

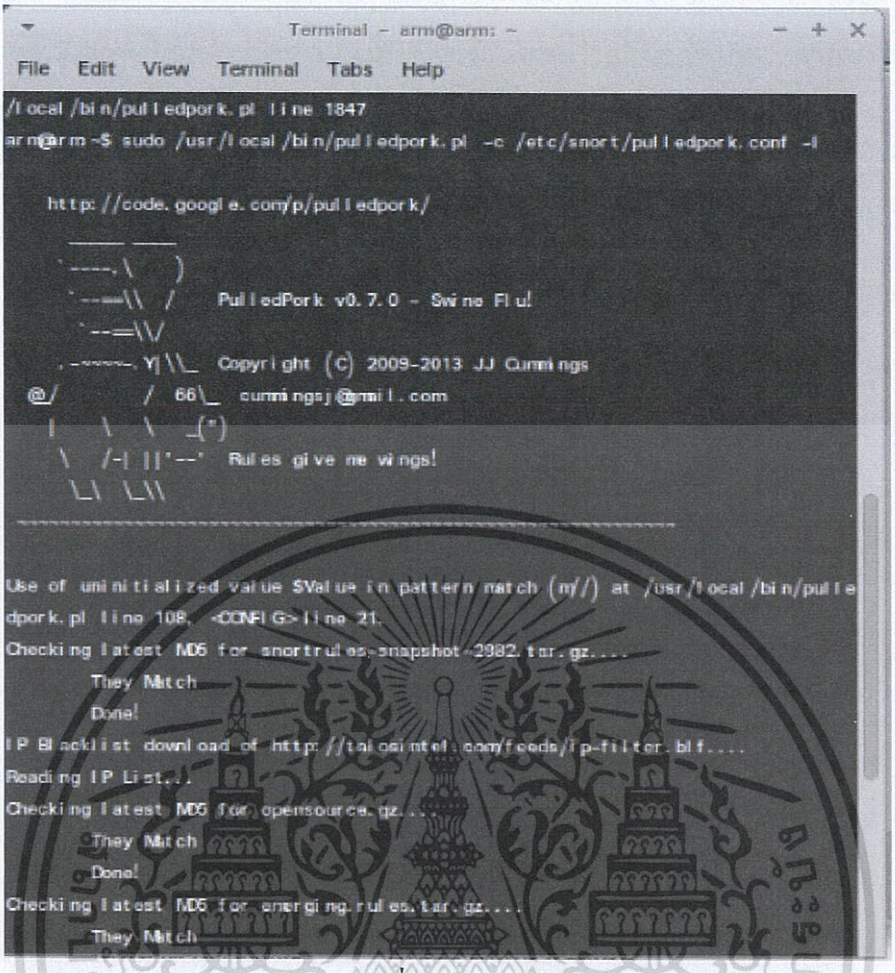
```
sudo wget https://github.com/shirkdog/pulledpork/archive/master.zip
sudo unzip master.zip
cd pulledpork-master/etc
cp  pulledpork.conf /etc/snort/
```

26) รันโปรแกรม Pulled Pork

โปรแกรม 4.26 คำสั่งรันโปรแกรม Pulled Pork

```
sudo /usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf -l
```

หากสำเร็จจะได้ผลดังรูป 4.9



รูป 4.6 ผลการรันคำสั่งของโปรแกรม Pulled Pork

หลังจากที่รันคำสั่ง จากโปรแกรม 4.26 จะมีไฟล์ snort.rules และ snort_dynamicrules เพิ่มขึ้นมา รวมถึงกฎทั้งหมดจะถูกรวมไว้ที่ 2 ไฟล์นี้ ซึ่งเป็น rulesets จากเว็บไซต์ Snort.org และกฎทั้งหมดนี้จะสามารถใช้งานได้ก็ต่อเมื่อไปตั้งค่าที่ไฟล์ snort.conf โดยเพิ่มคำสั่งจากโปรแกรม 4.27 ลงไปที่บรรทัด 548 ของไฟล์ snort.conf

โปรแกรม 4.27 คำสั่งตั้งค่าในไฟล์ snort.conf

```
include $RULE_PATH/snort.rules
```

27) หลังจากทำการตั้งค่าไฟล์ snort.conf จำเป็นต้องดาวน์โหลดกฎและการตั้งค่าใหม่โดยการรันไฟล์ snort.conf อีกครั้ง

โปรแกรม 4.28 คำสั่งรันไฟล์ snort.conf

```
sudo snort -T -c /etc/snort/snort.conf
```

28) จากนั้นรันคำสั่งจากโปรแกรม 4.29

โปรแกรม 4.29 คำสั่งเข้าใช้ schedule ของเครื่องเซิร์ฟเวอร์

```
sudo crontab -e
```

จากนั้นโปรแกรมจะให้เลือก editor และเพิ่มคำสั่งจากโปรแกรม 4.30 ลงในบรรทัดสุดท้าย

โปรแกรม 4.30 คำสั่งกำหนดค่า schedule ให้กับเครื่องเซิร์ฟเวอร์

```
01 04 * * * /usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf -l
```

29) ติดตั้งโปรแกรม BASE และโปรแกรมที่เกี่ยวข้อง

โปรแกรม 4.31 คำสั่งติดตั้งโปรแกรม BASE และโปรแกรมที่เกี่ยวข้อง

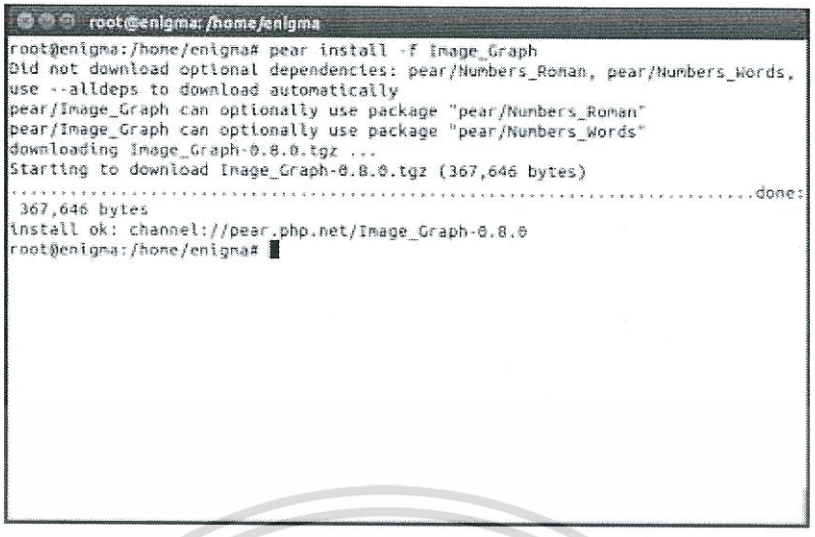
```
sudo apt-get install -y apache2 libapache2-mod-php5 php5 php5-mysql php5-common php5-gd
php5-cli php-pear
```

30) ติดตั้ง Image Graph

โปรแกรม 4.32 คำสั่งติดตั้ง Image Graph

```
sudo pear install -f Image_Graph
```

จะได้ผลดังรูป 4.10



รูป 4.7 การติดตั้งโปรแกรม Image Graph

31) ก่อนจะติดตั้ง BASE ต้องติดตั้งโปรแกรม ADOB ก่อน

โปรแกรม 4.33 คำสั่งติดตั้งโปรแกรม ADOB

```
cd ~/snort_src
wget https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-520-for-php5/adodb-5.20.4.tar.gz/download
tar -xvzf adodb520.tgz
sudo mv adodb5 /var/adodb
```

32) ติดตั้งโปรแกรม BASE

โปรแกรม 4.34 คำสั่งติดตั้งโปรแกรม BASE

```
cd ~/snort_src
wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz
tar -zxvf base-1.4.5.tar.gz
```

33) ก็อปปี้และให้สิทธิ์แก่โฟลเดอร์นั้นๆ

โปรแกรม 4.35 คำสั่งก็อปปี้และให้สิทธิ์แก่โฟลเดอร์นั้นๆ

```
sudo mv base-1.4.5 /var/www/html/base/
cd /var/www/html/base
sudo cp base_conf.php.dist base_conf.php
sudo chown -R www-data:www-data /var/www/html/base
sudo chmod o-r /var/www/html/base/base_conf.php
```

```
sudo gedit /var/www/html/base/base_conf.php
และตั้งค่าดังนี้
$BASE_urlpath = '/base';            # line 50
$DBlib_path = '/var/adodb/';        #line 80
$alert_dbname = 'snort';            # line 102
$alert_host = 'localhost';
$alert_port = '';
$alert_user = 'snort';
$alert_password = 'MYSQLSNORTPASSWORD';    # line 106
```

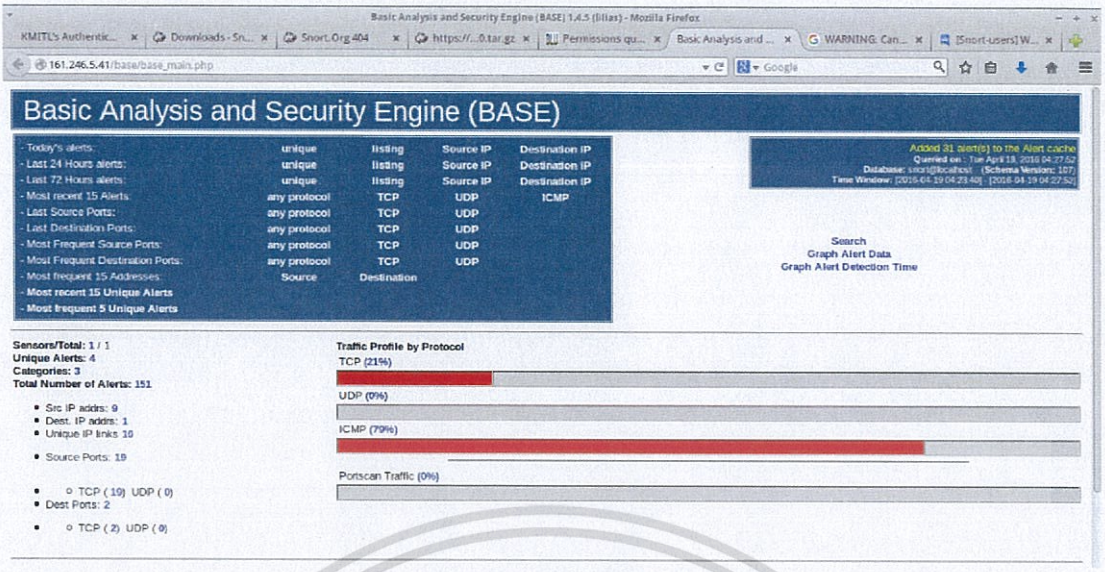
34) Restart Apache

โปรแกรม 4.36 คำสั่ง Restart Apache

```
sudo service apache2 restart
```

35) เข้าไปที่ http://ServerIP/base/index.php แล้วจะแสดงหน้าเว็บไซต์ดังรูป 4.11

(ServerIP คือ หมายเลข IP ของเครื่องเซิร์ฟเวอร์)



รูป 4.8 การทดสอบโปรแกรม BASE

4.3.2 ทดสอบสร้างกฎของโปรแกรม Snort ในไฟล์ /etc/snort/rules/local.rules

4.3.2.1 ทดสอบสร้างกฎของการโจมตีด้วย DDoS

โปรแกรม 4.38 คำสั่งการสร้างกฎของการโจมตีด้วย DDoS

```
alert tcp any any -> $HOME_NET 80 (flags: S; msg:"DDoS Attack"; flow: stateless;
threshold: type both, track by_dst, count 70, seconds 10; sid:10001; rev:1;)
```

4.3.2.2 ทดสอบสร้างกฎของการโจมตีด้วย SSH Brute Force Attack

โปรแกรม 4.39 คำสั่งการสร้างกฎของการโจมตีด้วย SSH Brute Force Attack

```
alert tcp any any -> $HOME_NET 22 (msg:"Potential SSH Brute Force Attack";
flow:to_server; flags;S; threshold:type threshold, track by_src, count 7, seconds 60;
classtype:attempted-dos; sid2001219;rev:4; resp:rst_all;)
```

4.3.3 ทดสอบการดักจับการโจมตีของโปรแกรม Snort

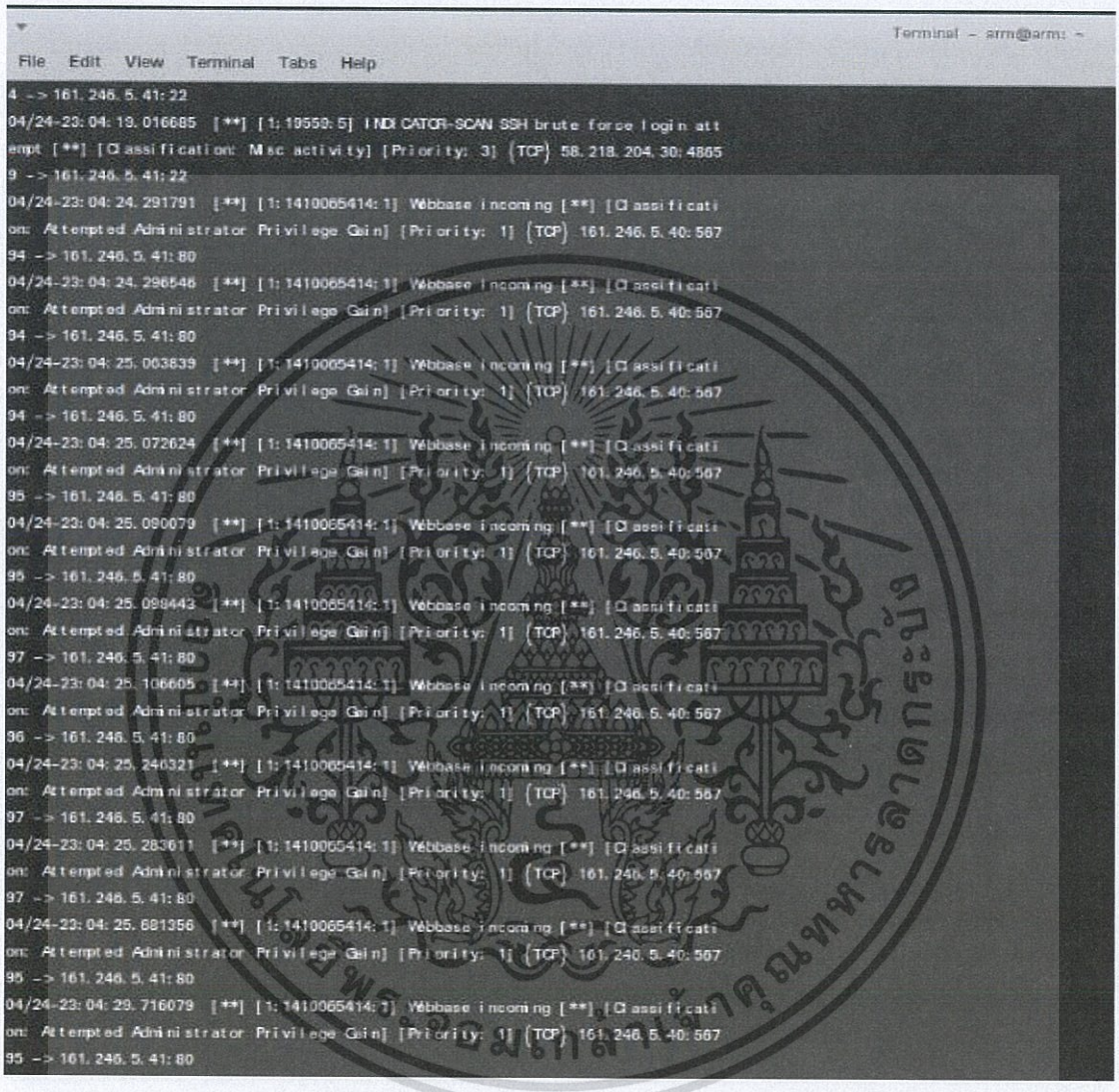
4.3.3.1 ทดสอบการโจมตีโดยการส่ง TCP Packet

โดยใช้คำสั่งดังโปรแกรม 4.40

โปรแกรม 4.40 คำสั่งในการส่ง TCP Packet จำนวนมาก

```
# hping3 -S -p 80 --flood --rand-source <target ip>
```

และผลที่ได้จากการตรวจจับการโจมตีจากโปรแกรม barnyard2 เป็นดังรูป 4.13

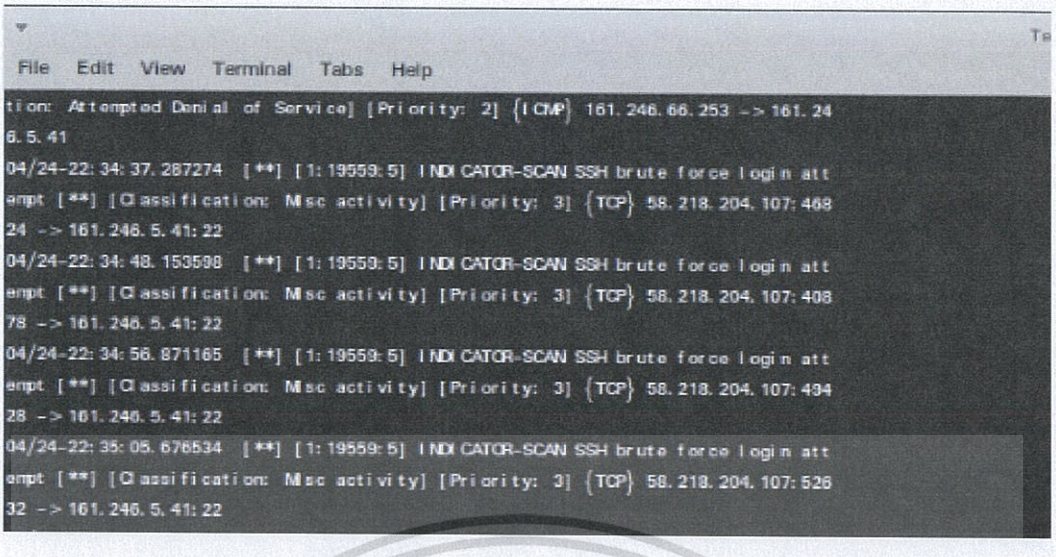


รูป 4.9 การแจ้งเตือนเมื่อมีการโจมตีโดยส่ง TCP Packet จำนวนมาก

4.3.3.2 ทดสอบการโจมตีโดย SSH Brute Force Attack

โดยใช้การล็อกอินเข้าเครื่องปลายทางหลายๆครั้ง หรือใช้การสคริปคำสั่งให้ทำการ SSH เข้าไปยังเครื่องเป้าหมายโดยใส่ Password ที่ไม่ถูกต้องลงไป

และผลที่ได้จากการตรวจจับการโจมตีจากโปรแกรม barnyard2 เป็นดังรูป 4.14



รูป 4.10 การแจ้งเตือนเมื่อมีการโจมตีด้วย SSH Brute Force Attack

4.4 ทดสอบติดตั้งโปรแกรมที่ใช้สำหรับการตรวจสอบสถานะของเครื่องที่ต้องการ (Zabbix) บนระบบปฏิบัติการ Ubuntu

บ่อยครั้งที่เครื่องเซิร์ฟเวอร์ต่างๆ ที่ให้บริการในภาควิชาวิศวกรรมคอมพิวเตอร์นั้นไม่สามารถให้บริการได้ และผู้ดูแลจะทราบก็ต่อเมื่อมีผู้ใช้งานแจ้งเข้ามาว่าบริการนั้นใช้งานไม่ได้ในขณะนั้น เช่น เว็บไซต์ของภาควิชาฯ เป็นต้น

ดังนั้นหากมีโปรแกรมที่คอยตรวจสถานะของเครื่องเซิร์ฟเวอร์อยู่ตลอดเวลา ผู้ดูแลระบบก็จะสามารถทราบได้ว่าขณะนั้นเครื่องเซิร์ฟเวอร์ยังสามารถให้บริการได้อยู่หรือไม่ หากไม่สามารถให้บริการได้ผู้ดูแลก็จะทราบได้ทันที และทำการแก้ไขต่อไป

4.4.1 ขั้นตอนการติดตั้งโปรแกรม Zabbix

1) ดาวน์โหลด และติดตั้งตัว Source Zabbix

โปรแกรม 4.41 คำสั่งดาวน์โหลด และติดตั้ง Source Zabbix

```
# wget http://repo.zabbix.com/zabbix/3.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.0-1+trusty_all.deb
# dpkg -i zabbix-release_3.0-1+trusty_all.deb
```

2) ติดตั้ง Zabbix Server

โปรแกรม 4.42 คำสั่งติดตั้ง Zabbix Server

```
# apt-get update
# apt-get install zabbix-server-mysql zabbix-frontend-php
```

3) ติดตั้ง Zabbix Agent (สำหรับเครื่องที่ต้องการตรวจสอบ)

โปรแกรม 4.43 คำสั่งติดตั้ง Zabbix Agent

```
# apt-get install zabbix-agent
```

4) สร้าง User และตารางสำหรับ MySQL

โปรแกรม 4.44 คำสั่งสร้าง User และตารางสำหรับ MySQL

```
# cd /usr/share/doc/zabbix-server-mysql
# mysql -uroot –p <password>
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> grant all privileges on zabbix.* to zabbix@localhost identified by '<password>';
mysql> quit;
# cd database/mysql
# zcat create.sql.gz | mysql -uroot zabbix
```

5) ตั้งค่า Database ให้กับโปรแกรม Zabbix ที่ไฟล์ zabbix_server.conf

โปรแกรม 4.45 ตั้งค่า Database ให้กับโปรแกรม Zabbix

```
# nano /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabbixpassword
```

6) รันโปรแกรม Zabbix

โปรแกรม 4.46 คำสั่งรันโปรแกรม Zabbix

```
# service zabbix-server start
```

7) ปรับ Time zone ของเว็บไซต์

โปรแกรม 4.47 คำสั่งปรับ Time zone ของเว็บไซต์ที่ไฟล์ zabbix.conf

```
# sudo nano /etc/apache2/conf-enabled/zabbix.conf.
php_value date.timezone Asia/Bangkok
# service apache2 restart
```

4.5 ทดลองติดตั้งโปรแกรมตรวจสอบการใช้งานในระบบเครือข่ายของภาควิชาวิศวกรรมคอมพิวเตอร์ (ntop) บนระบบปฏิบัติการ Ubuntu

โปรแกรม ntop เป็นเครื่องมือในการเก็บ traffic การใช้งานของ internet ของ User แต่ละคน ซึ่งสามารถนำมาใช้เป็นส่วนหนึ่งของเก็บ Log ได้เหมือนกัน

4.5.1 ขั้นตอนการติดตั้งโปรแกรม ntop

1) ติดตั้งโปรแกรม RRDTool และโปรแกรมที่เกี่ยวข้อง

โปรแกรม 4.48 คำสั่งติดตั้งโปรแกรม RRDTool และโปรแกรมที่เกี่ยวข้อง

```
# sudo apt-get install rrdtool
# sudo apt-get install libpcap-dev libxml2-dev pango-graphite libpng12-dev freetype2-demos
libart-2.0-dev glibc-doc libglib2.0-dev libpango1.0-dev libgdbm-dev
# ./configure
# make
# sudo make install
```

2) ดาวน์โหลดไฟล์ ntop เวอร์ชั่นล่าสุด

โปรแกรม 4.49 คำสั่งดาวน์โหลดไฟล์โปรแกรม ntop

```
# wget https://sourceforge.net/projects/ntop/files/ntop/Stable/ntop-5.0.1.tar.gz/download
# tar fvxz ntop-5.0.1.tar.gz
# sudo apt-get install python3.4-dev php5-geoip php5-dev libgeoip-dev
```

โปรแกรม 4.49 คำสั่งดาวน์โหลดไฟล์โปรแกรม ntop (ต่อ)

```
# cd ntop-5.0.1
# ./configure --with-rrd-home=/opt/rrdtool-1.5.5
# make
# sudo make install
# sudo make install-am
```

3) สร้าง User ชื่อ ntop และเปลี่ยน owner ให้เป็น ntop

โปรแกรม 4.50 คำสั่งสร้าง User ชื่อ ntop และเปลี่ยน owner ให้เป็น ntop

```
# useradd ntop
# sudo chown ntop:ntop /usr/local/share/ntop
```

4) สร้าง password ของ ntop โดย user จะเป็น admin

โปรแกรม 4.51 คำสั่งสร้าง password ของ ntop

```
# sudo ldconfig
# sudo ntop -A
```

5) รัน port 3000 เพราะ ntop จะใช้ port 3000 ในการรัน และทำการรัน ntop

โปรแกรม 4.52 คำสั่งรัน port 3000 และรัน ntop

```
# sudo netstat -tanp|grep 3000
# sudo ntop –d -L
```

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุป

โครงงานระบบรักษาความปลอดภัยสำหรับเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์เป็นโครงงานที่ต้องการทำให้ระบบเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์มีความปลอดภัยมากยิ่งขึ้น อีกทั้งยังสามารถระบุถึงสาเหตุของปัญหาได้และเก็บเป็นบันทึกรายงานเอาไว้ เพื่อทำให้ผู้ดูแลระบบเครือข่ายวิเคราะห์และเลือกใช้วิธีในการแก้ไขปัญหานั้นๆได้ง่ายขึ้น ซึ่งเราสามารถสรุปผลได้จากการทดลองในบทที่ 4

5.1.1 การทดลองเปลี่ยนการตั้งค่าการเข้าถึงสวิตช์จากเทลเน็ตเป็นซีเคียวเชลล์

จากการทดลองนั้นทำให้สวิตช์ของภาควิชาวิศวกรรมคอมพิวเตอร์นั้นมีความปลอดภัยจากการดักจับข้อมูลมากยิ่งขึ้น เพราะด้วยโปรโทคอลของซีเคียวเชลล์นั้นมีการเข้ารหัสลับของข้อมูลไว้ทำให้ผู้ดักจับข้อมูลไม่สามารถอ่านข้อความได้ซึ่งในเทลเน็ตไม่มี

5.1.2 ทดลองการรวบรวมบันทึกกิจกรรมมาที่ส่วนกลาง

ทำให้เราสามารถระบุถึงคำสั่งในการรวบรวมบันทึกการทำงานต่างๆ มาที่ส่วนกลางได้ ทำให้ผู้ดูแลระบบมีความสะดวกสบายในการเปิดบันทึกการทำงานต่างๆ ที่อาจมีข้อผิดพลาดจากการทำงานของตัวอุปกรณ์ในระบบเครือข่าย

5.1.3 ทดลองติดตั้งและทดสอบโปรแกรมดักจับผู้บุกรุกที่เข้ามาโจมตีเว็บไซต์ของภาควิชาวิศวกรรมคอมพิวเตอร์ (Snort)

ผลจากการทดลองสามารถดักจับผู้บุกรุกได้ทั้งในรูปแบบการโจมตีด้วย DDoS Attack โดยการส่ง Packet TCP จำนวนมาก และการโจมตีด้วย SSH Brute Force Attack

5.1.4 ทดลองติดตั้งโปรแกรมที่ตรวจสอบสถานะของเครื่อง (Zabbix)

ผลจากการทดลองทำให้สามารถตรวจสอบข้อมูลการใช้งานของเครื่องได้ว่ามีการใช้งานของ CPU เป็นอย่างไร มีการใช้ Memory เป็นอย่างไร เพื่อตรวจสอบว่าเครื่องนั้นมีการใช้งานที่ผิดปกติหรือไม่

5.1.5 ทดลองติดตั้งโปรแกรมตรวจสอบการใช้งานอินเทอร์เน็ตในระบบเครือข่ายของภาควิชาวิศวกรรมคอมพิวเตอร์ (ntop)

ผลการติดตั้งนั้นเราสามารถที่จะตรวจสอบการใช้งานของระบบเครือข่ายภาควิชาฯ ได้ว่าในระบบเครือข่ายนั้นมีการใช้งานอินเทอร์เน็ตมากน้อยแค่ไหน มีเครื่องใดที่ใช้งานมากผิดปกติหรือไม่

5.2 ปัญหาและอุปสรรค์

1) การหาข้อมูลสินทรัพย์ของภาควิชาวิศวกรรมคอมพิวเตอร์ตามหาได้ยากและต้องออกทำการสำรวจหลายครั้ง
2) การทดลองในพื้นที่จริงอาจทำให้ระบบมีความเปลี่ยนแปลงได้
3) การติดตั้งโปรแกรมในบางครั้งอาจเกิดข้อผิดพลาดได้
4) การติดตั้งโปรแกรมบางตัวต้องการ Libraries ที่ช่วยในการรัน บางครั้งจึงอาจเกิดปัญหาที่หากโหลด Libraries ที่โปรแกรมต้องการมาไม่ครบ

5.3 แนวทางการแก้ไข

1) มอบหมายให้ผู้ดูแลแต่ละห้องช่วยทำการสำรวจ
2) ระมัดระวังสิ่งที่อาจจะทำให้เกิดการเปลี่ยนแปลงกับระบบ
3) หาแนวทางการแก้ปัญหานั้นๆ จากอาจารย์ที่ปรึกษา หรือค้นหาการแก้ปัญหาจากอินเทอร์เน็ต
4) หาก Libraries โหลดมาไม่ครบ ขณะที่รันโปรแกรมจะมีบอกว่ายังขนาด Libraries ตัวไหนบ้าง แล้วจึงโหลดเข้ามาเพิ่มภายหลัง

5.4 แนวทางการพัฒนาต่อ

1) พัฒนาให้การตรวจจับและบันทึกประวัติเมื่อไม่สามารถเข้าถึงเว็บไซต์ภาควิชาวิศวกรรมคอมพิวเตอร์มีความแม่นยำมากยิ่งขึ้นเพื่อลดจำนวนเอชที่อยู่ไอพี (IP Address) ที่ต้องสงสัยให้น้อยลง
2) ทำระบบจัดเก็บบันทึกกิจกรรมส่วนกลางเพื่อรวบรวมบันทึกกิจกรรมส่วนกลางไว้ที่เดียวสำหรับวิเคราะห์เมื่อระบบเกิดปัญหาขึ้น
3) ปรับการตั้งค่า Rules ของโปรแกรมดักจับการโจมตีจากผู้บุก Snort ให้มีความเหมาะสมกับภาควิชาวิศวกรรมคอมพิวเตอร์มากยิ่งขึ้น

บรรณานุกรม

จตุชัย แพงจันทร์. 2553. **Master in Security 2nd Edition.** พิมพ์ครั้งที่ 1. นนทบุรี : ไอดีซีฯ.

วิศัลย์ ประสงค์สุข. 2554. **เชื่อมต่ออย่างปลอดภัยด้วย SSH Tunnel.** [Online]. Available : https://www.thaicert.or.th/papers/technical/2011/pa2011te006.html.

Support. 2549. **รู้จักกับการโจมตีระบบเครือข่ายแบบ Distributed Denial of Service (DDoS) และวิธีการป้องกัน.** [Online]. Available : http://www.mvt.co.th/viewarticle.php?cid=3&nid=82&page=4

Jason Wilder. 2555. **Centralized Logging.** [Online]. Available : http://jasonwilder.com/blog/2012/01/03/centralized-logging

Wikipedia. 2557. **Secure channel.** [Online]. Available : https://en.wikipedia.org/wiki/Secure_channel

Cisco. **Configuring Secure Shell (SSH).** [Online]. Available : http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_01001.html

ดร.บรรจง หะรังษี. **ความรู้เบื้องต้นของการเข้ารหัสข้อมูล (Introduction to Cryptography).** [Online]. Available : http://www.tnetsecurity.com/content_attack/crypt_basicknowledge.php

CALYPTIX. 2015. **Top 7 Network Attack Types in 2015 So Far.** [Online]. Available : http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far

Robert Fekete. **Procedure – Configuring syslog-ng on client hosts.** [Online]. Available : https://www.balabit.com/sites/default/files/documents/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/configure-clients.html

Snort. **Snort Setup Guides.** [Online]. Available: https://www.snort.org/documents

Pulledpork. **File config pulledpork.conf.** [Online]. Available: https://github.com/shirkdog/pulledpork/blob/master/etc/pulledpork.conf