ระบบตรวจสอบช่องโหว่ของเครือข่ายคอมพิวเตอร์ผ่านเว็บเบราว์เซอร์

A WEB-BASED NETWORK VULNERABILITY SCANNER SYSTEM

นิธิ พรรณวดี

NITHI PHANAWADEE

นิพิฐ สง่ามั่งคั่ง

NIPITH SA-NGARMANGKANG

บดินทร์ วางอภัย

BORDIN WANGAPAI

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2553

A WEB-BASED NETWORK VULNERABILITY SCANNER SYSTEM

NITHI PHANAWADEE

NIPITH SA-NGARMANGKANG

BORDIN WANGAPAI

THIS THESIS IS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

BACHELOR OF ENGINEERING IN INFORMATION ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

หัวข้อปริญญานิพนธ์ ระบบตรวจสอบช่องโหว่ของเครือข่ายคอมพิวเตอร์ผ่านเว็บเบราว์เซอร์

รายชื่อนักศึกษา	นายนิธิ พรรณวดี	รหัสนักศึกษา 50010822
	นายนิพิฐ สง่ามั่งคั่ง	รหัสนักศึกษา 50010826
	นายบดินทร์ วางอภัย	รหัสนักศึกษา 50010847
ปริญญา	วิศวกรรมศาสตรบัณฑิต	
สาขาวิชา	วิศวกรรมสารสนเทศ	
พ.ศ.	2553	
อาจารย์ที่ปรึกษาปริญญานิพนธ์	ผศ.ดร.สุธีรา พันธุ์ธีรานุรักษ์	

ปริญญานิพนธ์ฉบับนี้ ได้รับการอนุมัติให้เป็นส่วนหนึ่งของการศึกษา ตามหลักสูตรวิศวกรรมศาสตร์บัณฑิต คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

.....

(ผศ.ดร.สุธีรา พันธุ์ธีรานุรักษ์)

อาจารย์ผู้ควบคุมปริญญานิพนธ์

หัวข้อปริญญานิพนธ์ ระบบตรวจสอบช่องโหว่ของเครือข่ายคอมพิวเตอร์ผ่านเว็บเบราว์เซอร์
(A Web-based Network Vulnerability Scanner System)

รายชื่อนักศึกษา นายนิธิ พรรณวดี รหัสนักศึกษา 50010822
นายนิพิฐ สง่ามั่งคั่ง รหัสนักศึกษา 50010826
นายบดินทร์ วางอภัย รหัสนักศึกษา 50010847

ปริญญา วิศวกรรมศาสตรบัณฑิต

สาขาวิชา วิศวกรรมสารสนเทศ

พ.ศ. 2553

อาจารย์ที่ปรึกษาปริญญานิพนธ์ ผศ.ดร.สุธีรา พันธุ์ธีรานุรักษ์

บทคัดย่อ

การตรวจสอบช่องโหว่ของเครื่องคอมพิวเตอร์นั้นสามารถทำได้โดยผู้ที่มีความรู้เกี่ยวกับระบบเครือข่ายเท่านั้นเนื่องจากเครื่องมือที่มีอยู่ในปัจจุบันนี้ต้องมีการนำมาติดตั้งที่เครื่องคอมพิวเตอร์ที่ต้องการจะตรวจสอบ และในบางครั้งการตรวจสอบผู้ตรวจสอบต้องทำการเขียนโปรแกรมเพื่อเรียกใช้งานคำสั่งต่าง ๆ เอง จึงทำให้การตรวจสอบช่องโหว่ทำได้ค่อนข้างลำบาก ดังนั้นโครงงานระบบตรวจสอบช่องโหว่บนเครือข่ายคอมพิวเตอร์ผ่านเว็บเบราว์เซอร์นี้จึงมีแนวคิดที่จะสร้างระบบดังกล่าวเพื่อให้ผู้ใช้งานสามารถเรียกใช้งานระบบได้อย่างง่าย โดยสามารถเรียกใช้งานได้เพียงแค่มีเครื่องคอมพิวเตอร์ที่ทำการเชื่อมต่อกับอินเตอร์เน็ตอยู่เท่านั้นก็สามารถใช้งานได้ โดยโครงงานนี้ได้พัฒนาทั้งระบบในส่วนผู้ใช้งานทั่วไปและผู้ดูแลระบบ ในการใช้งานนั้นผู้ใช้งานในองค์กรนั้น ๆ สามารถตรวจสอบข้อมูลเบื้องต้น และตรวจสอบข้อมูลช่องโหว่ของเครื่องคอมพิวเตอร์ในระบบเครือข่ายนั้นได้ หลักจากผู้ใช้งานตรวจสอบพบช่องโหว่ที่เกิดขึ้นแล้ว ระบบจะนำเสนอรายละเอียดของช่องโหว่ สาเหตุที่สามารถทำให้เกิดช่องโหว่ดังกล่าว พร้อมทั้งนำเสนอแนวทางของวิธีการแก้ไขช่องโหว่ที่เกิดขึ้นได้ อีกทั้งระบบนี้สามารถจัดเก็บข้อมูลประวัติของการตรวจสอบช่องโหว่ของเครื่องคอมพิวเตอร์ที่ได้เคยทำการตรวจสอบแล้วไว้ เพื่อผู้ใช้งานในองค์กรเดียวกัน สามารถดูประวัติดังกล่าวได้ ในส่วนผู้ดูแลระบบนั้นมีฟังก์ชันการทำงานเสริมขึ้นมาคือ การเพิ่มเติม แก้ไข ลบข้อมูลผู้ใช้งานระบบ และข้อมูลช่องโหว่ต่าง ๆ ที่มีการเปลี่ยนแปลงเพิ่มเติมตลอดเวลาได้

Thesis Title	A Web-based Network Vulnerability Scanner System	
Student	Mr. Nithi Phanawadee	Student ID. 50010822
	Mr. Nipith Sa-ngarmangkang	Student ID. 50010826
	Mr. Bordin Wangapai	Student ID. 50010847
Degree	Bachelor of Engineering	
Program	Information Engineering	
Year	2010	
Thesis Advisor	Asst. Prof. Dr. Sutheera Puntheeranurak	

ABSTRACT

Today, if users who would like to check vulnerability of your computer must have knowledge about network. Because many tools that are available now need to install the application on inspected computer and sometimes the user must use a command line to check the vulnerability. Therefore, a web-based network vulnerability scanner system is built so that users can access the system easily who just have a computer is connected to the internet. This project can support the end users of organizations and administrators. The user can check the computer information that you would like to know and check your computer's vulnerabilities on the network. After the user detects a vulnerability that occurs, the system will provide details of the vulnerability, cause of vulnerability and propose guidelines on how to fix vulnerabilities that occur. In addition, the system can store historical data of the validation of computer vulnerabilities that have already been checked then the user in the same organization can view that history. In the administration part, there are more functionality such as add modify and delete the user information and vulnerability because additional vulnerability information have changed throughout time.

กิตติกรรมประกาศ

โครงงานนี้ได้ดำเนินการจนสำเร็จลุล่วงไปได้ด้วยดี เนื่องจากได้รับคำแนะนำ สั่งสอนในการทำงานโครงงานนี้ และให้ความช่วยเหลือในด้านต่าง ๆ เป็นอย่างดีตลอดระยะเวลาในการทำงาน ซึ่งคณะผู้จัดทำต้องขอกราบขอบพระคุณ ผศ.ดร.สุธีรา พันธุ์ธีรานุรักษ์ อาจารย์ที่ปรึกษาโครงงานที่คอยเอาใจใส่ ให้คำแนะนำ จัดหาอุปกรณ์เพื่อการทำโครงงานนี้ และช่วยตรวจสอบแก้ไขข้อบกพร่องต่าง ๆ มาโดยตลอด

ขอกราบขอบพระคุณคณาจารย์วิศวกรรมศาสตร์ ภาควิชาสารสนเทศทุกท่าน ที่มีส่วนช่วยในการขัดเกลา และสั่งสอนเพื่อให้โครงงานชิ้นนี้สำเร็จลุล่วงไปได้อย่างสมบูรณ์

ขอขอบคุณพี่ ๆ เพื่อน ๆ และน้อง ๆ ทุกคนที่คอยช่วยเหลือและให้กำลังใจใยการทำงานกันและกันตลอดมาโดยตลอดทำให้ผ่านพ้นอุปสรรคต่าง ๆ ไปได้ด้วยดี

ท้ายที่สุดนี้ คณะผู้จัดทำต้องขอกราบขอบพระคุณ บิดา มารดา และทุก ๆ คนในครอบครัวของคณะผู้จัดทำ ที่ให้การเลี้ยงดู อบรมสั่งสอน และให้กำลังใจเมื่อคณะผู้จัดทำพบอุปสรรค จนทำให้มีทุกวันนี้ และขอบคุณทุก ๆ ท่านที่มีส่วนร่วมในความสำเร็จของโครงงานชิ้นนี้ ที่ไม่สามารถกล่าวไว้ ณ ที่นี้ได้หมด คุณประโยชน์อันใดที่เกิดจากโครงงานนี้เป็นผลจากความกรุณาของทุกท่านที่กล่าวมาข้างต้น คณะผู้จัดทำซาบซึ้งเป็นอย่างยิ่ง จึงใคร่ขอขอบพระคุณไว้ ณ ที่นี่ด้วย

คณะผู้จัดทำ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันความเสี่ยงของระบบเครือข่ายคอมพิวเตอร์มีเพิ่มมากขึ้นทุกวัน เนื่องจากระบบที่ใช้อยู่ล้วนแต่มีช่องโหว่ด้วยกันทั้งสิ้น ช่องโหว่เหล่านี้เกิดขึ้นทุกวัน โดยเฉลี่ยแต่ละเดือนจะมีมากกว่า 10 ช่องโหว่ขึ้นไป ซึ่งการที่จะให้บุคคลากรในองค์กรจัดการกับปัญหาเรื่องระบบความปลอดภัยนั้นไม่ใช่เรื่องง่าย มีความจำเป็นต้องมีผู้ดูแลระบบที่มีความรู้ทางด้านเทคนิคเป็นอย่างดี เพื่อให้การรักษาความปลอดภัยของระบบเป็นไปอย่างมีประสิทธิภาพมากที่สุด

ช่องโหว่ของระบบคอมพิวเตอร์และเครือข่ายมักจะเกิดจากการที่มีช่องทางการเชื่อมต่อที่ไม่จำเป็นเปิดใช้งานอยู่ หรืออาจเป็นที่ตัวโปรแกรมประยุกต์เองที่มีช่องโหว่หรือมีความผิดพลาดทำให้เกิดช่องทางที่สามารถนำมาใช้ในการโจมตีระบบได้ ในการวิเคราะห์จำเป็นต้องตรวจสอบช่องทางการเชื่อมต่อเหล่านี้ก่อนว่าทำงานอะไรบ้าง แล้วจึงตรวจสอบว่าโปรแกรมประยุกต์มีช่องโหว่ในตัวมันเองหรือไม่ ซึ่งมีความยุ่งยากในขั้นตอนและวิธีการตรวจสอบ การมีเครื่องมือในการตรวจสอบและวิเคราะห์ช่องโหว่นั้นจะช่วยแบ่งเบาภาระของผู้ดูแลระบบได้มากขึ้น

เนื่องจากความยุ่งยากในการตรวจสอบและความจำเป็นที่ต้องการใช้ผู้ดูแลระบบที่มีความสามารถและประสบการณ์ค่อนข้างสูง จึงได้พัฒนาเครื่องมือสำหรับตรวจสอบและวิเคราะห์ช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ และสามารถเสนอแนวทางในการปรับปรุงระบบให้มีความปลอดภัยที่สูงขึ้นต่อไปได้

1.2 จุดประสงค์

1.2.1 เพื่อพัฒนาโปรแกรมประยุกต์สำหรับตรวจสอบและวิเคราะห์ช่องโหว่หรือภัยต่าง ๆ ของระบบเครือข่ายคอมพิวเตอร์

1.2.2 เพื่อฝึกการพัฒนาโปรแกรมประยุกต์เพื่อให้บริการทางเครือข่ายคอมพิวเตอร์

1.3 ขอบเขตของโครงงาน

1.3.1 โปรแกรมสามารถแสดงผล แก้ไขปรับเปลี่ยน และการตั้งค่าอื่น ๆ ผ่านทางเว็บเบราว์เซอร์

1.3.2 โปรแกรมสามารถบอกรายละเอียดของเครือข่าย โฮสต์ และโปรแกรมประยุกต์ได้

1.3.3 โปรแกรมสามารถตรวจสอบและวิเคราะห์ช่องโหว่หรือภัยต่าง ๆ ที่อาจเกิดขึ้นกับระบบได้ทั้งในระดับเครือข่าย โฮสต์ ตลอดจนโปรแกรมประยุกต์ได้

1.3.4 โปรแกรมสามารถให้คำแนะนำในการปรับปรุงระบบให้มีความปลอดภัยมากขึ้น

1.3.5 โปรแกรมสามารถให้คำแนะนำในการรับมือกับเหตุการณ์ที่อาจเกิดขึ้นจากช่องโหว่นั้น ๆ ได้

1.4 ผลที่คาดว่าจะได้รับ

1.4.1 สามารถนำไปใช้ในการตรวจสอบและวิเคราะห์ช่องโหว่หรือภัยต่าง ๆ ของระบบเครือข่ายคอมพิวเตอร์ได้

1.4.2 ช่วยให้ทราบช่องโหว่ของระบบ เพื่อจะได้ทำการแก้ไขล่วงหน้าก่อนที่จะถูกโจมตี

1.4.3 สามารถแบ่งเบาภาระของผู้ดูแลระบบในการค้นหาช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ได้

1.4.4 มีความรู้ความเข้าใจเกี่ยวกับการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

1.4.5 มีความรู้ความเข้าใจเกี่ยวกับการพัฒนาโปรแกรมประยุกต์ให้ทำงานผ่านระบบเครือข่ายคอมพิวเตอร์

1.5 อุปกรณ์ที่ต้องใช้

1.5.1 ลินุกซ์อูบุนตูรุ่น 8.04 (Ubuntu version 8.04) เป็นระบบปฏิบัติการสำหรับเว็บเซิร์ฟเวอร์

1.5.2 อาปาเช่รุ่น 2 (Apache version 2) เป็นซอฟต์แวร์สำหรับเว็บเซิร์ฟเวอร์

1.5.3 พีเอชพีรุ่น 5 (PHP version 5) เป็นภาษาที่ใช้ในการพัฒนาเว็บโปรแกรมประยุกต์

1.5.4 มายเอสคิวแอลรุ่น 5 (MySQL version 5.0) เป็นฐานข้อมูลของโปรแกรม

1.5.5 โปรแกรมเอ็นแมปรุ่น 4 (Nmap version 4) เป็นโปรแกรมที่ทำงานอยู่เบื้องหลังในการสแกนพอร์ต

1.5.6 โปรแกรมเนสซัสรุ่น 3.2 (Nessus version 3.2) เป็นโปรแกรมที่ทำงานอยู่เบื้องหลังในการสแกนช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์

1.5.7 ภาษาเอ็นเอเอสแอล (NASL) ในการพัฒนาสคริปต์สำหรับการตรวจสอบช่องโหว่ร่วมกับโปรแกรมเนสซัส

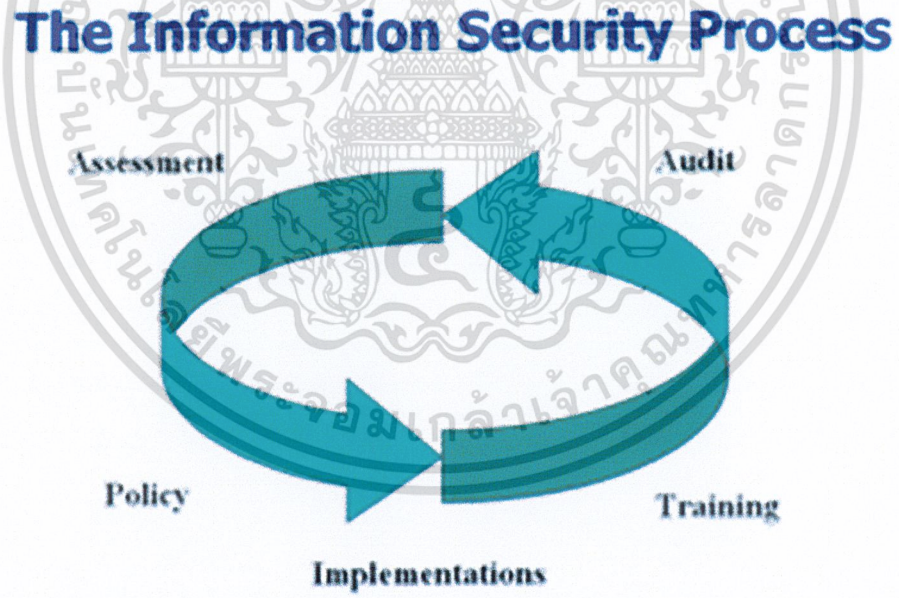
1.5.8 โอเพนเอสเอสเอช (OpenSSH) เป็นโปรแกรมในการล็อกอินเข้าสู่เชลล์ (Shell) ของลีนุกซ์อูบุนตู

บทที่ 2
ทฤษฎีพื้นฐานที่ใช้

2.1 กระบวนการรักษาความปลอดภัยข้อมูล

การป้องกันระบบความปลอดภัยข้อมูล ควรมีหลักในการจัดการอย่างเป็นระบบ โดยปกติแล้วกระบวนการรักษาความปลอดภัยข้อมูลประกอบด้วย 5 ขั้นตอนหลัก ดังแสดงความสัมพันธ์ของกระบวนการต่าง ๆ ได้ดังรูปที่ 2.1

- การประเมินความเสี่ยง (Risk Assessment)
- การกำหนดนโยบาย (Policy)
- การติดตั้งระบบป้องกัน (Implementation)
- การฝึกอบรม (Training)
- การตรวจสอบ (Audit)



รูปที่ 2.1 กระบวนการรักษาความปลอดภัยข้อมูล

แต่ละขั้นตอนนั้นมีความสำคัญต่อกระบวนการรักษาความปลอดภัยของข้อมูลขององค์กร อย่างไรก็ตามเพื่อให้กระบวนการนี้ได้ผล และมีประสิทธิภาพในการป้องกันเหตุการณ์ต่าง ๆ องค์กรจะต้องทำทุกขั้นตอนควบคู่กันไป

2.1.1 การบริหารความเสี่ยง (Risk Management)

การบริหารความเสี่ยง หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลงหรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ โดยการบริการความเสี่ยงนั้นจำเป็นต้องเข้าใจถึงความหมายของคำต่อไปนี้ คือ

1) ความเสี่ยง (Risk)

ความเสี่ยง คือ การวัดความสามารถ ที่จะดำเนินการให้วัตถุประสงค์ของงานประสพความสำเร็จ ภายใต้การตัดสินใจ งบประมาณ กำหนดเวลา และข้อจำกัดด้านเทคนิคที่เผชิญอยู่ อย่างเช่น การจัดทำโครงการเป็นชุดของกิจกรรม ที่จะดำเนินการเรื่องใดเรื่องหนึ่งในอนาคต โดยใช้ทรัพยากรที่มีอยู่อย่างจำกัด มาดำเนินการให้ประสบความสำเร็จ ภายใต้กรอบเวลาอันจำกัด ซึ่งเป็นกำหนดการปฏิบัติการในอนาคต ความเสี่ยงจึงอาจเกิดขึ้นได้ตลอดเวลา อันเนื่องมาจากความไม่แน่นอน และความจำกัดของทรัพยากรโครงการ ผู้บริหารโครงการจึงต้องจัดการความเสี่ยงของโครงการ เพื่อให้ปัญหาของโครงการลดน้อยลง และสามารถดำเนินการให้ประสบความสำเร็จตามเป้าหมายที่ตั้งไว้อย่างมีประสิทธิผลและประสิทธิภาพ

2) ช่องโหว่ (Vulnerability)

ช่องโหว่ คือช่องทางที่อาจใช้สำหรับการโจมตีได้ จุดอ่อนหรือช่องโหว่อาจมีในระบบคอมพิวเตอร์และเครือข่าย ซึ่งเป็นช่องทางให้ผู้ไม่ประสงค์ดีสามารถเจาะเข้าระบบหรือเครือข่ายได้ จุดอ่อนนั้นมีหลายระดับขึ้นอยู่กับความยากง่าย และระดับความชำนาญทางด้านเทคนิคที่สามารถใช้ประโยชน์จากมันได้

3) ภัยคุกคาม (Threat)

ภัยคุกคาม คือสิ่งที่อาจจะเกิดขึ้นและมีอันตรายต่อทรัพย์สินขององค์กร ภัยคุกคามนั้นปรกอบด้วย 3 ส่วน คือ เป้าหมาย (Target) ผู้โจมตี (Agent) และเหตุการณ์ (Event)

2.1.2 การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยงและจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

- โอกาสที่จะเกิด หมายถึง ความถี่หรือโอกาสที่จะเกิดความเสี่ยง
- ผลกระทบ หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง
- ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น ๕ ระดับ คือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก

ขั้นตอนที่สำคัญของการประเมินความเสี่ยง คือ

1. กำหนดขอบเขต
2. เก็บรวบรวมข้อมูล
3. วิเคราะห์นโยบายและระเบียบปฏิบัติ
4. วิเคราะห์ภัยคุกคาม (Threat Analysis)
5. วิเคราะห์จุดอ่อนหรือช่องโหว่ (Vulnerability Analysis)
6. ประเมินความเสี่ยง

2.1.3 การวิเคราะห์ช่องโหว่ (Vulnerability Analysis)

จุดประสงค์ของการวิเคราะห์ช่องโหว่นั้นก็เพื่อเป็นการทดสอบสถานภาพขององค์กรในปัจจุบันว่าล่อแหลมต่อการถูกโจมตี หรือถูกทำลายมากน้อยแค่ไหน หรือเป็นการทดสอบการรักษาความลับ ความคงสภาพ และความพร้อมใช้งานของข้อมูลที่สำคัญขององค์กร

ช่องโหว่หรือจุดอ่อนที่ค้นพบนั้นสามารถจัดระดับความเสี่ยงต่อองค์กรทั้งหลายจากภายในและภายนอก ช่องโหว่ที่มีระดับความเสี่ยงต่ำ หมายถึง ช่องโหว่ที่มีระดับความรุนแรงต่ำและความเปิดเผย (Exposure) ช่องโหว่ที่มีระดับความเสี่ยงสูง หมายถึง ช่องโหว่ที่อาจก่อให้เกิดความเสียหายต่อระบบสูง หรือมีระดับความรุนแรงสูง และง่ายต่อการโจมตี

2.2 เครือข่ายคอมพิวเตอร์ (Computer Network)

การเชื่อมต่อเครือข่ายคอมพิวเตอร์เป็นที่นิยมแพร่หลาย และมีโปรแกรมประยุกต์จำนวนมาก เช่น อีเมล เว็บ และโปรแกรมประเภทส่งข้อความด่วนทันที (Instant Messaging) ที่ทำงานบนระบบเครือข่าย โปรแกรมประยุกต์เหล่านี้จะต้องพึ่งพาโปรโตคอลของระบบเครือข่ายเฉพาะทาง ซึ่งแต่ละโปรโตคอลจะใช้วิธีการในการส่งผ่านข้อมูลพื้นฐานเหมือนกัน

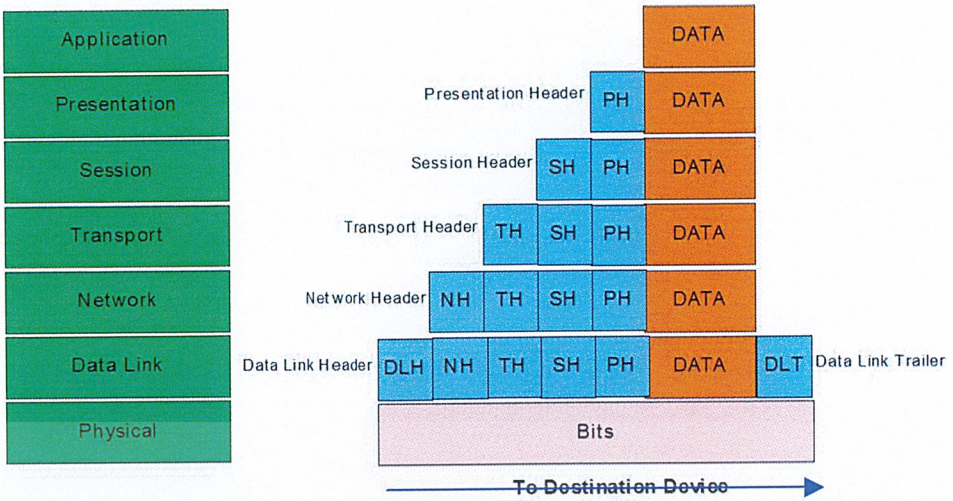
2.2.1 โครงสร้างเครือข่ายแบบโอเอสไอ (OSI Model)

โครงสร้างเครือข่ายแบบโอเอสไอ (OSI Model หรือ OSI Reference Model) เป็นมาตรฐานการอธิบายการติดต่อสื่อสารและโปรโตคอลของระบบคอมพิวเตอร์ที่ถูกพัฒนาขึ้นโดยองค์กรที่ชื่อว่า International Organization for Standardization (ISO) ซึ่งได้ถูกแบ่งย่อยออกเป็น 7 ลำดับชั้น เพื่อให้ง่ายต่อความเข้าใจว่าแต่ละลำดับชั้นมีความสำคัญอย่างไร และสัมพันธ์กันอย่างไร ซึ่งโดยปกติแล้วแต่ละลำดับชั้นจะมีความสัมพันธ์โดยตรงกับชั้นที่อยู่ติดกับชั้นนั้น ๆ

- **ชั้นฟิสิคอล (Physical Layer)** เป็นชั้นที่ต่ำที่สุด ที่เกี่ยวข้องกับการเชื่อมต่อทางกายภาพระหว่างจุดสองจุด มีหน้าที่หลักในการสื่อสารแบบบิตดิบ (raw bit streams) คือรับผิดชอบในการกระตุ้น ดูแลรักษา และยกเลิกการติดต่อการสื่อสารแบบบิตสตรีม

- **ชั้นดาต้าลิงค์ (Data link Layer)** เกี่ยวข้องกับการถ่ายโอนข้อมูลระหว่างจุดสองจุด ทำหน้าที่สูงกว่าชั้นฟิสิคอล เช่น การตรวจสอบข้อผิดพลาดและควบคุมลำดับการส่งข้อมูล
- **ชั้นเน็ตเวิร์ก (Network Layer)** จะจัดการการติดต่อสื่อสารข้ามเครือข่าย ซึ่งจะเป็นการทำงานติดต่อข้ามเครือข่ายแทนชั้นอื่น ๆ ที่อยู่ข้างบน
- **ชั้นทรานสปอร์ต (Transport Layer)** ทำหน้าที่ดูแลจัดการเรื่องของความผิดพลาดที่เกิดขึ้นจากการสื่อสาร ซึ่งการตรวจสอบความผิดพลาดนั้นจะพิจารณาจากข้อมูลส่วนที่เรียกว่า ส่วนตรวจสอบ (Checksum) และอาจมีการแก้ไขข้อผิดพลาดนั้นๆ โดยพิจารณาจากฝั่งต้นทางกับฝั่งปลายทาง (End-to-end) โดยหลัก ๆ แล้วชั้นนี้จะอาศัยการพิจารณาจากพอร์ตของเครื่องต้นทางและปลายทาง
- **ชั้นเซสชัน (Session Layer)** เป็นชั้นที่ควบคุมการสื่อสารจากต้นทางไปยังปลายทางและคอยควบคุมช่องทางการสื่อสารในกรณีที่มีหลาย ๆ โปรเซสต้องการรับส่งข้อมูลพร้อม ๆ กันบนเครื่องเดียวกัน ทำงานคล้ายกับเป็นหน้าต่างคอยสลับเปิดให้ข้อมูลเข้าออกตามหมายเลขพอร์ตที่กำหนด และยังให้อินเตอร์เฟซสำหรับชั้นแอพพลิเคชันด้านบนในการควบคุมขั้นตอนการทำงานของโปรโตคอลในชั้นทรานสปอร์ตและชั้นเน็ตเวิร์ก และทำหน้าที่ควบคุมจังหวะในการรับส่งข้อมูลของทั้ง 2 ด้าน ให้มีความสอดคล้องกัน (Synchronization) และกำหนดวิธีที่ใช้รับส่งข้อมูล
- **ชั้นพรีเซนเตชัน (Presentation Layer)** รับผิดชอบเรื่องรูปแบบของการแสดงผลเพื่อโปรแกรมต่าง ๆ ที่ใช้งานระบบเครือข่ายทำให้ทราบว่าข้อมูลที่ได้เป็นประเภทใด เช่น รูปภาพ, เอกสาร, ไฟล์วีดีโอ
- **ชั้นแอพพลิเคชัน (Application Layer)** จะครอบคลุมบริการที่เกี่ยวข้องกับการรักษาความปลอดภัย การเข้ารหัส การเชื่อมต่อระหว่างโปรแกรมประยุกต์ และเป็นชั้นที่โปรแกรมประยุกต์ใช้งานโดยตรง โดยโปรโตคอลที่อยู่บนชั้นนี้จะถูกออกแบบให้เหมาะสำหรับประเภทของโปรแกรมประยุกต์เฉพาะทาง

เมื่อข้อมูลได้รับการส่งผ่านโดยใช้โปรโตคอลเหล่านี้ ข้อมูลจะถูกส่งไปในลักษณะที่เรียกว่า แพกเกต (Packet) แต่ละแพกเกตจะเก็บข้อมูลของแต่ละชั้น เริ่มจากชั้นแอพพลิเคชันข้อมูลจะถูกเก็บอยู่ในแพกเกตของชั้นพรีเซนเตชันและแพกเกตของชั้นพรีเซนเตชันจะถูกห่อหุ้มอยู่ภายในแพกเกตของชั้นเซสชันและเป็นชั้น ๆ ต่อกันลงมาเรื่อย ๆ ซึ่งจะเรียกกระบวนการนี้ว่าการห่อหุ้ม (Encapsulation) แต่ละชั้นที่ถูกห่อหุ้มด้วยชั้นที่สูงกว่า จะประกอบด้วยส่วนเฮดเดอร์และส่วนเมสเสจ เฮดเดอร์จะเก็บข้อมูลที่จำเป็นต่อการสื่อสารของโปรโตคอลในชั้นนั้น ๆ ในขณะที่ส่วนเมสเสจจะเก็บข้อมูลของโปรโตคอลในชั้นที่สูงกว่าหนึ่งชั้น ดังแสดงในรูปที่ 2.2



รูปที่ 2.2 กระบวนห่อหุ้มแพกเกต

กระบวนการห่อหุ้มแพกเกตล้วนประกอบกันขึ้นมาเป็นภาษาที่ซับซ้อนที่เครื่องในอินเทอร์เน็ต และเครือข่ายประเภทอื่น ใช้เพื่อสื่อสารกับเครื่องอื่น โปรโตคอลเหล่านี้ได้รับการเขียนโปรแกรมบรรจุไว้ในเราท์เตอร์ ไฟร์วอลล์ และระบบปฏิบัติการเครือข่าย โปรแกรมที่ใช้ในเครือข่าย เช่น เว็บเบราเซอร์ หรืออีเมลไคลเอนต์ จำเป็นต้องไปติดต่อกับระบบปฏิบัติการที่ดูแลเรื่องการสื่อสารด้วยโปรโตคอลบนเครือข่ายก่อน เนื่องจากระบบปฏิบัติการมีหน้าที่นี้โดยตรง ดังนั้นการเขียนโปรแกรมผ่านเครือข่ายจึงจำเป็นต้องเรียนรู้วิธีการเรียกใช้บริการจากระบบปฏิบัติการให้ได้

2.2.2 ซ็อกเก็ต (Socket)

ซ็อกเก็ต เป็นวิธีการมาตรฐานในการเรียกใช้บริการของระบบปฏิบัติการ เพื่อการติดต่อสื่อสารผ่านระบบเครือข่าย ซ็อกเก็ตหนึ่งสามารถถูกมองว่าเป็นจุดเริ่มต้นหรือจุดสิ้นสุดของการเชื่อมต่อ คล้าย ๆ กับซ็อกเก็ตที่เป็นฮาร์ดแวร์อยู่บนตู้ควบคุมของโอเปอเรเตอร์ แต่ซ็อกเก็ตในที่นี้เป็นเพียงนามธรรมที่โปรแกรมเมอร์เรียกชื่อ ซึ่งคอยดูแลเรื่องรายละเอียดกระบวนการภายในที่ระบบปฏิบัติการกระทำอยู่ รวมถึงเรื่องการปฏิบัติตามกลไกของเครือข่ายโปรโตคอลซ็อกเก็ตสามารถถูกใช้เพื่อส่งหรือรับข้อมูลผ่านเครือข่ายได้ ข้อมูลนี้จะถูกเริ่มต้นส่งผ่านตั้งแต่ชั้นเซสชันซึ่งอยู่เหนือชั้นทรานสปอร์ตและชั้นเน็ตเวิร์กขึ้นไป ซึ่งชั้นเน็ตเวิร์คจะได้รับการจัดการโดยระบบปฏิบัติการด้วย ในการหาเส้นทางแพกเกตซ็อกเก็ตมีหลายประเภท ประเภทที่เป็นพื้นฐานที่สุด ได้แก่ สตรีมซ็อกเก็ต และดาต้าแกรมซ็อกเก็ต

1) สตรีมซ็อกเก็ต (Stream Socket)

สตรีมซ็อกเก็ต ได้ให้กลไกการสื่อสารแบบสองทิศทางที่เชื่อถือได้ คล้ายกับการสนทนากับใครสักคนทางโทรศัพท์ โดยด้านหนึ่งจะต้องเริ่มต้นสร้างการติดต่อไปยังอีกด้านหนึ่ง และหลังจากนั้นเมื่อการเชื่อมต่อถูกสร้างขึ้นมา อีกด้านหนึ่งก็จะสามารถสื่อสารกับต้นทางได้ นอกจากนั้นยังมีการยืนยันการสนทนาด้วยว่าสิ่งที่พูดไปนั้นถึงผู้รับปลายทาง สตรีมซ็อกเก็ตได้ใช้โปรโตคอล ทีซีพี (TCP) ซึ่งอยู่ในชั้นที่ 4 ของแบบจำลองเครือข่ายแบบโอเอสไอในระบบเครือข่ายคอมพิวเตอร์ ข้อมูลโดยปกติจะถูกส่งไปในลักษณะที่เรียกว่า แพกเกตโปรโตคอลทีซีพีได้รับการออกแบบมาเพื่อให้แพกเกตข้อมูลได้เดินทางไปถึงปลายทางได้อย่างไม่มีความผิดพลาดและมีลำดับการส่งที่ชัดเจน เว็บเซิร์ฟเวอร์ อีเมลเซิร์ฟเวอร์ และไคลเอนต์ โปรแกรมที่ใช้ติดต่อทั้งหมดล้วนใช้ทีซีพีและสตรีมซ็อกเก็ตเพื่อการสื่อสาร

2) ดาต้าแกรมซ็อกเก็ต (Datagram Socket)

การสื่อสารผ่านทางดาต้าแกรมซ็อกเก็ตนั้นจะคล้ายกับการส่งจดหมายไปยังผู้รับแทนการโทรศัพท์ การเชื่อมต่อนั้นจะเป็นแบบทิศทางเดียวและไม่น่าเชื่อถือ เช่น การส่งจดหมายไปหลายฉบับนั้นไม่สามารถแน่ใจได้ทีเดียวว่ามันจะถูกส่งไปถึงในลักษณะเรียงลำดับตามต้องการ หรือจดหมายนั้นจะถึงปลายทางทุกฉบับหรือไม่ ดาต้าแกรมซ็อกเก็ตได้ใช้โปรโตคอลยูดีพี (UDP) แทนการใช้ทีซีพี ซึ่งเป็นโปรโตคอลที่ง่ายๆ ไม่ซับซ้อน เพราะยูดีพีไม่มีการสร้างการเชื่อมต่อที่เป็นรูปธรรมนัก เพียงแค่ให้บริการพื้นฐานในการส่งข้อมูลจากจุดหนึ่งไปยังอีกจุดหนึ่งนั้นเอง การใช้ดาต้าแกรมซ็อกเก็ตนี้จะทำให้เกิดโอเวอร์เฮดเพียงเล็กน้อยเท่านั้น

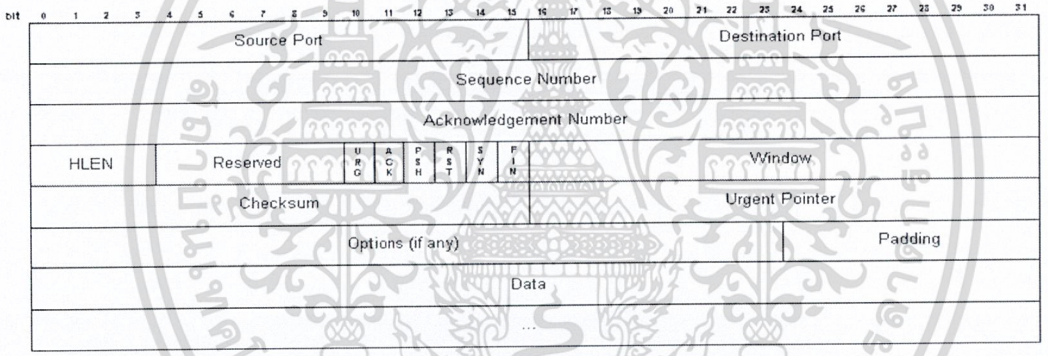
2.2.3 ทรานมิชชันคอนโทรลโปรโตคอล (Transmission Control Protocol)

ตารางที่ 2.1 ตารางแสดงแฟล็กแต่ละชนิดของทีซีพี

TCP flag	Meaning	Purpose
URG Urgent	Identifies	ข้อมูลที่สำคัญ
ACK	Acknowledgment	แสดงว่าได้รับแพกเกตแล้ว มักถูกเซตสำหรับการเชื่อมต่อส่วนใหญ่
PSH	Push	บอกให้ผู้รับ push ข้อมูลต่อทันที แทนที่จะเก็บลงไปในฮัมเมอร์
RST	Reset	เริ่มการเชื่อมต่อใหม่
SYN	Synchronize	ซิงโครไนซ์หมายเลขลำดับ ที่จุดเริ่มต้นของการเชื่อมต่อ
FIN	Finish	ปิดการเชื่อมต่ออย่างเรียบร้อยเมื่อทั้งสองฝั่งต้องการจบการสนทนา

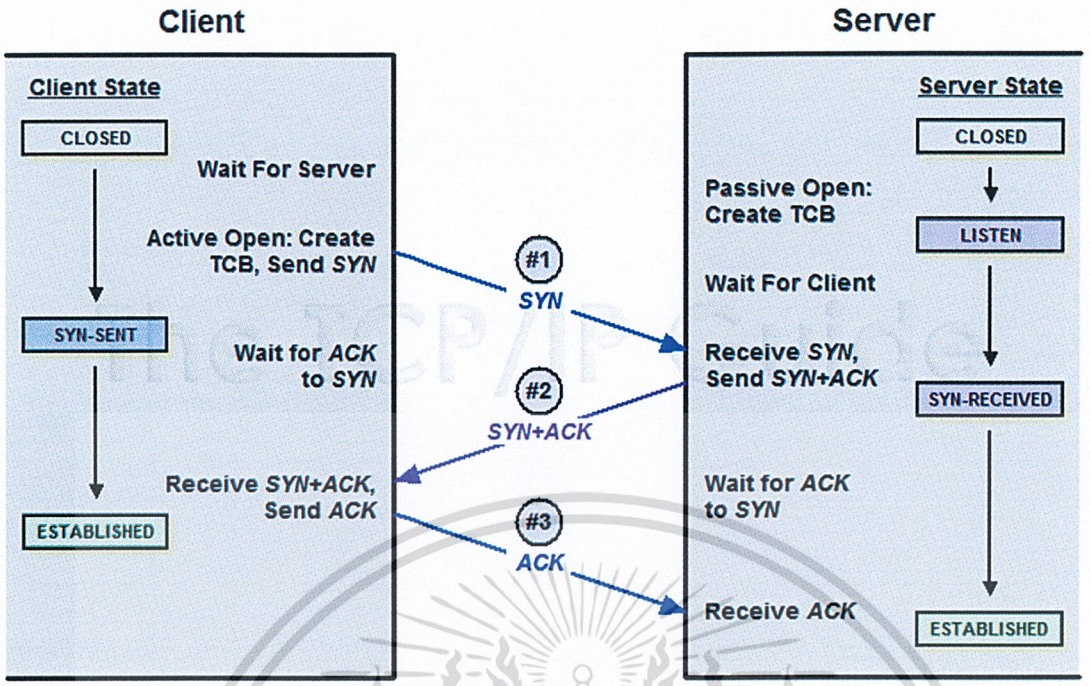
ทีซีพีเป็นโปรโตคอลที่อยู่ในชั้นทรานสปอร์ตชั้นและเป็นโปรโตคอลที่นิยมใช้มากที่สุดบนอินเทอร์เน็ต บริการที่ใช้ทีซีพี เช่น เทลเน็ต (telnet), เอชทีทีพี (HTTP), เอสเอ็มทีพี (SMTP) และ เอฟทีพี (FTP) ซึ่งเหตุผลที่โปรโตคอลทีซีพีได้รับความนิยมเนื่องจากโปรโตคอลทีซีพีได้รับการออกแบบให้มีการส่งข้อมูลได้โดยที่ชั้นบนไม่จำเป็นต้องรับรู้รายละเอียดที่น่าเชื่อถือ และทำงานแบบสองทิศทางระหว่างสองไอพีแอดเดรส ความน่าเชื่อถือนั้นเกิดจากโปรโตคอลทีซีพีจะรับประกันให้ว่าแพกเกตสามารถส่งไปยังผู้รับปลายทางได้แน่นอน ในลักษณะที่มีการเรียงลำดับชัดเจน หากมีบางแพกเกตไปไม่ถึง ผู้รับจะแจ้งให้ผู้ส่งทำการส่งใหม่ซ้ำจนกระทั่งได้รับแพกเกตที่หายไป ฟังก์ชันการทำงานข้างต้นเกิดขึ้นได้โดยอาศัยเซตของบิตแฟล็ก ที่เรียกว่าทีซีพีแฟล็ก (TCP Flag) แสดงได้ในตารางที่ 2.1

แฟล็กเหล่านี้ได้รับการเก็บไว้ในส่วนเฮดเดอร์ของโปรโตคอลทีซีพีพร้อมกับหมายเลขพอร์ตต้นทางและปลายทาง เฮดเดอร์ของโปรโตคอลทีซีพีได้รับการอธิบายไว้ในเอกสาร RFC หมายเลข 739 ดังแสดงในรูปที่ 2.3



รูปที่ 2.3 เฮดเดอร์ของโปรโตคอลทีซีพี

หมายเลขลำดับ (Sequence Number) และหมายเลขแสดงการตอบรับ (Acknowledgment Number) ได้ถูกใช้เพื่อเก็บรักษาสถานะของการรับส่งข้อมูลนี้ แฟล็ก SYN และ ACK ถูกใช้พร้อมกันเพื่อเปิดการเชื่อมต่อในลักษณะกระบวนการแฮนด์เช็ก (handshake) 3 ขั้น ดังแสดงในรูปที่ 2.4 เมื่อไคลเอนต์ต้องการเปิดการเชื่อมต่อไปยังเซิร์ฟเวอร์ ไคลเอนต์จะส่งแพกเกตเปล่า ๆ ที่แฟล็ก SYN ถูก ON ขึ้นมา และแฟล็ก ACK เป็น OFF เซิร์ฟเวอร์จะตอบสนองด้วยแพกเกตที่แฟล็ก SYN และ ACK ทั้งคู่ถูก ON ขึ้นมา และเพื่อให้การเชื่อมต่อนี้สมบูรณ์ ไคลเอนต์จะส่งแพกเกตเปล่าที่มีการกำหนดแฟล็ก ACK เป็น ON และแฟล็ก SYN เป็น OFF หลังจากนั้น ทุก ๆ แพกเกตในการเชื่อมต่อจะมีแฟล็ก ACK เป็น ON และแฟล็ก SYN เป็น OFF เสมอ เฉพาะสองแพกเกตแรกในการเชื่อมต่อเท่านั้นที่มีแฟล็ก SYN เป็น ON เนื่องจากสองแพกเกตนี้จำเป็นต้องทำหน้าที่ซิงโครไนซ์หมายเลขลำดับ



รูปที่ 2.4 กระบวนการกระบวนการแฮนด์เช็ก 3 ขั้นของโปรโตคอลทีซีพี

หมายเลขลำดับจะทำให้โปรโตคอลทีซีพี สามารถจัดแพกเกตที่ไม่เรียงลำดับ ให้อยู่ในลำดับแถวที่ถูกต้องได้ และเพื่อช่วยในการค้นหาว่ามีแพกเกตไหนหายไปบ้าง และเพื่อป้องกันไม่ให้แพกเกตเกิดการสับสนปนเข้าไปในการเชื่อมต่ออื่น

เมื่อเริ่มต้นสร้างการเชื่อมต่อ แต่ละด้านจะสร้างหมายเลขลำดับเริ่มต้น หมายเลขนี้จะถูกส่งแลกเปลี่ยนกันกับคู่สนทนาฝั่งตรงข้ามในสองแพกเกตแรกที่มีการเซตแฟล็ก SYN ไว้ จากนั้นในแต่ละครั้งที่แพกเกตถูกส่งไป หมายเลขลำดับจะได้รับการเพิ่มขึ้นเท่ากับจำนวนไบต์ที่พบในส่วนข้อมูลของแพกเกต หมายเลขนี้ถูกใส่ไว้ในเฮดเดอร์ของโปรโตคอลทีซีพี นอกจากนั้น แต่ละเฮดเดอร์ของโปรโตคอลจะมีหมายเลขลำดับ ซึ่งเท่ากับหมายเลขลำดับบวกด้วยหนึ่ง

โปรโตคอลทีซีพีนั้นเหมาะสมสำหรับโปรแกรมประยุกต์ที่ต้องการความน่าเชื่อถือและการสื่อสารสองทิศทาง แต่อย่างไรก็ตาม มันก็มีส่วนโอเวอร์เฮดเกิดขึ้นในการสื่อสารด้วย

2.2.4 ยูสเซอร์ดาต้าแกรมโปรโตคอล (User Datagram Protocol)

โปรโตคอลยูดีพีนั้นมีโอเวอร์เฮดน้อยกว่าโปรโตคอลทีซีพี แต่ฟังก์ชันความสามารถน้อยกว่าโปรโตคอลทีซีพี ซึ่งทำให้โปรโตคอลยูดีพีมีพฤติกรรมคล้ายกับไอพี ในแง่ที่โปรโตคอลยูดีพีเองก็ทำงานแบบไม่มีการสร้างการเชื่อมต่อ (Connectionless) และไม่น่าเชื่อถือ ซึ่งต้องอาศัยระดับแอปพลิเคชันที่ไม่ต้องการการตรวจสอบและความน่าเชื่อถือใด ๆ แต่ต้องการความรวดเร็วเป็นหลัก ก็มักจะเลือกใช้โปรโตคอลยูดีพี เฮดเดอร์ของโปรโตคอลยูดีพีประกอบด้วยเฉพาะหมายเลข

พอร์ตต้นทาง หมายเลขพอร์ตปลายทาง ความยาว และส่วนตัวสอบเท่านั้น ซึ่งรวมกันเพียง 16 ไบต์

2.2.5 พอร์ต (Port)

สำหรับแอปพลิเคชันในชั้นสูง ๆ ที่ใช้โปรโตคอลทีซีพี โปรโตคอลยูดีพี จะมีหมายเลขพอร์ต ซึ่งจะเป็นเลข 16 บิต เริ่มตั้งแต่ 0 ถึง 65535 หมายเลขพอร์ตใช้สำหรับตัดสินว่าเซอร์วิสใดที่ต้องการเรียกใช้ ในทางทฤษฎีแล้ว หมายเลขพอร์ตแต่ละหมายเลขถูกเลือกสำหรับเซอร์วิสใด ๆ ขึ้นอยู่กับระบบปฏิบัติการที่ใช้ ไม่จำเป็นต้องเหมือนกัน แต่ได้มีกำหนดขึ้นให้ใช้ค่อนข้างเป็นมาตรฐานเพื่อให้มีการติดต่อการส่งข้อมูลที่ดีขึ้น ทางไอเอเน็นเอ (Internet Assigned Numbers Authority : IANA) เป็นหน่วยงานกลางในการประสานการเลือกใช้พอร์ตว่า พอร์ตหมายเลขใดควรเหมาะสำหรับเซอร์วิสใด และได้กำหนดในอาร์เอฟซีหมายเลข 1700 (RFC 1700) ตัวอย่างเช่น เลือกใช้โปรโตคอลทีซีพี พอร์ตหมายเลข 23 กับเซอร์วิสเทลเน็ต และเลือกใช้โปรโตคอลยูดีพี พอร์ตหมายเลข 69 สำหรับเซอร์วิสทีเอฟที (Trivial File transfer Protocol : TFTP)

หมายเลขพอร์ตถูกจัดแบ่งออกเป็น 2 ประเภท ตามที่ได้กำหนดในอาร์เอฟซีหมายเลข 1700 คือพอร์ตที่นิยมใช้กันอย่างแพร่หลาย และพอร์ตลงทะเบียน

- พอร์ตที่นิยมใช้กันอย่างแพร่หลาย จะเป็นพอร์ตที่ระบบส่วนใหญ่และค่อนข้างมาตรฐาน ทำให้เครื่องที่อยู่ไกลออกไป สามารถรู้ได้ว่าจะติดต่อกับทางพอร์ตหมายเลขอะไรสำหรับเซอร์วิสเฉพาะนั้น ๆ กำหนดให้ใช้โดยผู้ใช้ที่มีสิทธิพิเศษ (Privileged User) โดยพอร์ตเหล่านี้ ใช้สำหรับการติดต่อระหว่างเครื่องที่มีระบบเวลาที่ยาวนาน วัตถุประสงค์เพื่อให้เซอร์วิสแก่ผู้ใช้แปลกหน้า จึงจำเป็นต้องกำหนดพอร์ตติดต่อสำหรับเซอร์วิสนั้น ๆ
- พอร์ตลงทะเบียน (Registered Ports) จะเป็นพอร์ตหมายเลข 1024 ขึ้นไป ซึ่งไอเอเน็นเอไม่ได้กำหนดไว้

ในการใช้การติดต่อด้วยโปรโตคอลสามารถกระทำได้ 2 วิธี คือ การเชื่อมต่อแบบพาสซีฟ (Passive Connection) คือ การติดต่อที่กระบวนการของโปรแกรมประยุกต์สั่งให้โปรโตคอลทีซีพีรอหมายเลขพอร์ตสำหรับการร้องขอการติดต่อจากโฮสต์ เมื่อโปรโตคอลทีซีพีได้รับการร้องขอแล้วจึงทำการเลือกหมายเลขพอร์ตให้ และแบบแอ็คทีฟทีซีพี (Active TCP) ก็จะให้กระบวนการของโปรแกรมประยุกต์เป็นฝ่ายเลือกหมายเลขพอร์ตให้เลย

2.2.6 ไอพีแอดเดรส (IP Address)

เป็นหมายเลขที่ใช้ในระบบเครือข่ายที่ใช้โปรโตคอลอินเทอร์เน็ต คล้ายกับหมายเลขโทรศัพท์ ที่เครื่องคอมพิวเตอร์ เครื่องเราท์เตอร์ เครื่องแฟกซ์ จะมีหมายเลขเฉพาะตัวโดยใช้เลขฐานสอง จำนวน 32 บิต โดยการเขียนจะเขียนเป็นชุด 4 ชุด โดยแต่ละชุดจะใช้เลขฐานสอง

จำนวน 8 บิต ซึ่งโดยทั่วไปแล้ว ผู้คนส่วนใหญ่จะคุ้นเคยกับระบบเลขฐานสิบ จึงมักแสดงผลโดยการใช้เลขฐานสิบ จำนวน 4 ชุด ซึ่งแสดงถึงหมายเลขเฉพาะของเครื่องนั้น สำหรับการส่งข้อมูลภายในเครือข่ายแลน แวน หรืออินเทอร์เน็ต โดยหมายเลขไอพีมีไว้เพื่อให้ผู้ส่งรู้ว่าเครื่องของผู้รับคือใคร และผู้รับสามารถรู้ได้ว่าผู้ส่งคือใคร

ตัวอย่างของหมายเลขไอพี ได้แก่ 161.246.34.31 ซึ่งเมื่อแปลงกลับมาในรูปแบบที่อ่านได้จะเรียกว่า โดเมนแอดเดรส ผ่านทางระบบโดเมน (Domain Name System) ซึ่งหมายเลขนั้นหมายถึง www.ite.kmitl.ac.th

ระบบตัวเลขไอพีที่ใช้ในปัจจุบันเป็นระบบ ไอพีเวอร์ชันที่ 4 (IPv4) ซึ่งจะเป็นระบบ 32 บิตหรือสามารถระบุเลขไอพีได้ตั้ง 0.0.0.0 ถึง 255.255.255.255 ตัวเลขบางตัวเป็นไอพีสงวนไว้สำหรับหน้าที่เฉพาะเช่น 127.0.0.0 จะเป็นการระบุถึงตัวอุปกรณ์เองไม่ว่าอุปกรณ์นั้นจะมีไอพีสื่อสารจริง ๆ เป็นเท่าไร อย่างไรก็ตามจากระบบตัวเลขที่จำกัดนี้สามารถเพิ่มขยายด้วยเทคนิคของไอพีส่วนตัว (Private IP) กับการแปลงไอพี (Network Address Translation : NAT)

2.3 เนสซัส (Nessus)

เนสซัสเป็นสแกนเนอร์ที่ได้รับความนิยมมากตัวหนึ่งในปัจจุบัน โครงการเนสซัสถือกำเนิดขึ้นในปี 1998 ซึ่งในตอนนั้นยังไม่มีซอฟต์แวร์ที่สามารถสแกนช่องโหว่ของระบบที่เปิดเผยซอร์สโค้ด Renaud Deraison จึงได้ตัดสินใจที่จะเริ่มโครงการ ซึ่งต่อมาได้เป็นที่รู้จักกันในชื่อโครงการเนสซัส (Nessus)

เนสซัสเป็นโปรแกรมสแกนช่องโหว่ที่มีประสิทธิภาพ และยังเป็นซอฟต์แวร์ที่เปิดเผยซอร์สโค้ด ทำให้สามารถใช้บริการได้โดยไม่เสียค่าใช้จ่าย อีกทั้งยังอนุญาตให้ผู้ใช้งานที่มีความเชี่ยวชาญ สามารถพัฒนาการตรวจสอบช่องโหว่ของระบบคอมพิวเตอร์โดยไม่จำเป็นที่จะต้องเป็นส่วนหนึ่งของทีมพัฒนาโครงการ ความสามารถเดียวกันนี้ส่งผลให้เกิดการอัพเดทข้อมูลของช่องโหว่ที่รวดเร็ว ทำให้เนสซัสเป็นโปรแกรมที่มีข้อมูลของช่องโหว่ที่ทันสมัยอยู่เสมอ

2.3.1 ส่วนประกอบพื้นฐาน

สถาปัตยกรรมเนสซัสนั้นถูกออกแบบมาให้มีความรวดเร็ว และใช้ทรัพยากรของเครื่องน้อยที่สุด สามารถทำงานได้หลาย ๆ งานในช่วงเวลาเดียวกัน ส่วนประกอบพื้นฐานของเนสซัสประกอบด้วย

- ระบบไคลเอนต์และเซิร์ฟเวอร์ (Nessus Client and Server)
- ปลั๊กอิน (Nessus Plugins)
- ฐานความรู้ (Nessus Knowledge Base)

1) ระบบไคลเอนต์และเซิร์ฟเวอร์ (Nessus Client and Server)

โครงการเนสซัสได้ถูกออกแบบมาในระบบไคลเอนต์เซิร์ฟเวอร์โมเดล ทำให้สามารถสแกนหาช่องโหว่ได้หลาย ๆ ช่องโหว่ในเวลาเดียวกันอย่างมีประสิทธิภาพ

เนสซัสไคลเอนต์สามารถที่จะเชื่อมต่อกับ เนสซัสเซิร์ฟเวอร์ได้ในหลาย ๆ ทาง ทั้งแบบเข้ารหัสและแบบยืนยันตัวตน ถ้าเนสซัสเซิร์ฟเวอร์ที่ต้องการจะเชื่อมต่อนั้นรอการเชื่อมต่ออยู่ที่ 127.0.0.1 ก็จะสามารถเลือกการเชื่อมต่อแบบไม่ต้องเข้ารหัสได้ แต่การใช้การเชื่อมต่อที่มีการเข้ารหัสจะทำให้เกิดความมั่นใจมากขึ้นในสแกนช่องโหว่ เพราะการเชื่อมต่อแบบเข้ารหัสนั้นจะสามารถป้องกันผู้โจมตีที่ทำการดักจับข้อมูลที่กำลังทำการสแกนได้

2) ปลั๊กอิน (Plug-in)

เนสซัสมีปลั๊กอินเฉพาะตัว ที่สามารถสแกนช่องโหว่ของระบบคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ ปลั๊กอินของเนสซัสจะใช้ภาษาเอ็นเอเอสแอล (Nessus Attack Scripting Language : NASL) ซึ่งเป็นภาษาที่เนสซัสออกแบบขึ้นมาเอง อนุญาตให้นักวิเคราะห์ระบบความปลอดภัยสามารถสร้างปลั๊กอินของตนสำหรับการตรวจสอบช่องโหว่ อีกทั้งยังอนุญาตให้สร้างการตรวจสอบช่องโหว่สำหรับโปรโตคอลและบริการต่าง ๆ ซึ่งแตกต่างกันในแต่ละเครือข่ายด้วย

3) ฐานความรู้ (Knowledge Base)

ฐานความรู้ เป็นสิ่งที่ทำให้ปลั๊กอินในปัจจุบันสามารถรับข้อมูลที่เกิดจากปลั๊กอินก่อนหน้านี้ได้ ซึ่งอาจจะเป็นความปลอดภัยที่ต้องการตรวจสอบสำหรับเว็บเซิร์ฟเวอร์ ถ้าปลั๊กอินหนึ่งได้ค้นพบช่องโหว่ก็จะส่งผลการทดสอบให้ปลั๊กอินที่กำลังทำการรันอยู่ด้วย ปลั๊กอินมีความสามารถในการตั้งค่าตัวแปรในฐานความรู้ของเนสซัสสำหรับเครื่องนั้น ๆ เช่น สคริปต์ภาษาเอ็นเอเอสแอล ที่ทำการรันพบว่ามีอาปาเช่รันอยู่บนเครื่อง ปลั๊กอินจะทำการตั้งค่าฐานความรู้เป็นตัวแปรที่มีค่าตามแบนเนอร์อาปาเช่ที่แสดงออกมาโดยตามหลังค่าของตัวแปร “www/banner/80”

ฐานความรู้ข้างต้นเปิดโอกาสให้ปลั๊กอินอื่นๆ สามารถอ่านค่าจากตัวแปร “www/banner/80” ภายหลังจากนี้ หากปลั๊กอินต่อไปได้พบสตริงในแบนเนอร์ ที่มีคำว่า “opessl/0.9.7a” ในค่าที่ถูกรีเทิร์นกลับมา ปลั๊กอินจะรายงานกลับมาว่าเครื่องนี้มีช่องโหว่โดยมีโอเพนเอสเอสแอลที่ยังไม่ได้อัพเดท ซึ่งเมื่อเป็นเช่นนี้แล้ว ทุกปลั๊กอินที่ใช้ข้อมูลนี้ก็จะได้รับทราบข้อมูลดังกล่าวด้วย จากความสามารถข้างต้นทำให้เนสซัสมีความรวดเร็วและมีประสิทธิภาพมากขึ้นหากมีการเพิ่มปลั๊กอินในอนาคตซึ่งมีความสามารถในการค้นหาฐานความรู้เพื่อรับทราบข้อมูลแทนที่จะไปสแกนหาจากเครือข่าย

2.3.2 องค์ประกอบที่ส่งผลต่อประสิทธิภาพของเนสซัส

1) การเลือกปลั๊กอินเนสซัส

การเลือกปลั๊กอินเนสซัสเป็นองค์ประกอบสำคัญต่อความแม่นยำของการสแกนช่องโหว่

การเลือกปลั๊กอินนั้นต้องทำความเข้าใจเกี่ยวกับผลกระทบของการเลือกปลั๊กอินในแต่ละแบบ ถ้าปลั๊กอินเนสซัสไม่สามารถใช้งานได้ เนสซัสจะไม่สามารถตรวจสอบช่องโหว่ได้

2) การอ้างถึงของปลั๊กอิน

โดยปกติถ้าสคริปต์มีการอ้างถึง สคริปต์นั้นจะไม่สามารถใช้งานได้จนกว่าสคริปต์ที่มีการอ้างถึงที่กำหนดจะทำการใช้งานสำเร็จแล้ว ดังนั้นโครงสร้างของกลุ่มปลั๊กอินจะทำให้ส่งผลกระทบโดยตรงต่อผลการสแกน

2.4 เว็บโปรแกรมมิ่ง (Web Programming)

2.4.1 เว็บเซอร์วิส (Web Service)

เว็บเซอร์วิส คือ เว็บแอพพลิเคชัน (Web Application) ยุคใหม่ ที่ประกอบด้วยส่วนย่อยๆ มีความสมบูรณ์ในตัวเอง สามารถติดตั้ง ค้นหา เริ่มทำงานได้ผ่านเว็บ เว็บเซอร์วิสสามารถทำอะไรก็ได้ตั้งแต่งานง่าย ๆ เช่น ดึงข้อมูล จนถึงกระบวนการทางธุรกิจที่ซับซ้อน เมื่อเว็บเซอร์วิสตัวใดตัวหนึ่งเริ่มทำงาน เว็บเซอร์วิสตัวอื่นก็สามารถรับรู้และเริ่มทำงานได้อีกด้วย เหตุผลที่เป็นเว็บเซอร์วิสเพราะเราซอฟต์แวร์สื่อกลาง (Middleware) อื่น ๆ มากมาย แม้ซอฟต์แวร์สื่อกลางเหล่านี้จะสามารถรองรับได้ แต่ไม่มีตัวใดตัวหนึ่งที่เด่นจริง แต่เว็บเซอร์วิสมีจุดเด่นในเรื่องของการให้บริการข้อมูลที่สะดวก ใช้งานง่าย จึงกลายเป็นตัวประสานซอฟต์แวร์สื่อกลางต่าง ๆ เข้าด้วยกัน เว็บเซอร์วิสทำหน้าที่เป็นตัวกลางให้ซอร์ฟแวร์สื่อกลางเหล่านี้สามารถคุยกันได้ และมีประสิทธิภาพกว่าวิธีการเดิม ๆ มาก หากมองจากกรณีของเอ็นเทียร์แอปพลิเคชัน (N-Tier Application) จะพบว่า เว็บเซอร์วิสคือกลไกในการเข้าถึงบริการที่แต่ละซอฟต์แวร์สื่อกลางให้บริการ การเข้าถึงจะลิสเทนเนอร์ (Listener) และส่วนประกอบที่ระบุถึงบริการต่าง ๆ ที่รองรับการทำงาน โดยการทำงานจริง ๆ นั้นก็ใช้วิธีการปกติของซอฟต์แวร์สื่อกลางนั้น ๆ

พื้นฐานของเว็บเซอร์วิส ก็คือเอกซ์เอ็มแอลกับเอชทีทีพี ซึ่งจะพบว่า เอชทีทีพีก็เป็นที่รู้จักกันดี และไปได้ทั่วทุกแห่งที่มีอินเทอร์เน็ต ส่วนเอกซ์เอ็มแอล คือภาษาสากลที่สามารถปรับแต่งได้ตามใจชอบ เพื่อให้เกิดกิจกรรมระว่างไคลเอนต์และบริการ หรือระหว่างส่วนประกอบต่างๆ เบื้องหลังเว็บเซิร์ฟเวอร์ก็คือ ข้อความเอกซ์เอ็มแอลจะถูกแปลงให้การขอบริการจากซอฟต์แวร์สื่อกลาง และผลที่ได้ก็จะแปลงกลับมาในรูปเอกซ์เอ็มแอล ยกตัวอย่างให้เห็นง่าย ๆ ถ้าต้องการให้เครื่องพีซีอ่านค่าจากพอร์ตอนุกรมแล้วส่งไปประมวลผลบนเครื่องยูนิกซ์ แล้วส่งผลกลับมาแสดงบนจอพีซี ถ้าเป็นเมื่อก่อนก็คงต้องแปลงข้อมูลที่ได้ให้อยู่ในรูปของแอสกี้ (ASCII) แล้วส่งไปยังยูนิกซ์ พร้อมคำสั่งว่าให้ทำอะไร ในฝั่งยูนิกซ์ก็ต้องมาแยกว่าอันไหนคือคำสั่ง อันไหนคือข้อมูล เมื่อประมวลผลแล้ว จะส่งกลับมาในรูปแบบไหน แล้วถ้าหากจะส่งไปหาเครื่องที่เป็นแมคแอดเดรส (MAC Address) จะต้องเขียนโปรแกรมเพิ่มในส่วนไหนบ้าง จะพบว่าเราต้องพัฒนากัน

เป็นคู่ ๆ ไป และต้องนิยามในแต่ละฝั่งให้ชัดเจน แต่หากเป็นเว็บเซอร์วิส จะพบว่า เราสามารถแปลงข้อมูลให้อยู่ในรูปเอกซ์เอ็มแอล โดยต้องการรู้แค่มาตรฐานเอกซ์เอ็มแอลก็พอ แล้วต่างคนต่างก็เขียนเซอร์วิสของตัวเอง ไม่ต้องกังวลเรื่องของการเชื่อมโยงอีกต่อไป และโปรโตคอลที่ส่งก็คือเอชทีทีพีนั่นเอง ถ้าสามารถเชื่อมโยงกับเอชทีทีพี หรือเว็บได้ ก็ใช้บริการทุกอย่างได้ แต่การเข้าถึงและการสั่งงานนั้นยังเป็นเพียงโครงสร้างพื้นฐาน แต่ในความเป็นจริงยังมีอะไรมากกว่านั้น เช่น การค้นหา การทำธุรกรรม ความปลอดภัย การพิสูจน์ตัวตน และอื่น ๆ อันเป็นบริการที่ทำให้เป็นบริการพื้นฐานจริงๆ ระบบเพิ่มเติมที่ต้องมีและต้องรักษาความสะดวกและใช้งานง่ายไว้ด้วย พื้นฐานของ เว็บเซอร์วิสเต็มรูปแบบคือเอกซ์เอ็มแอล + เอชทีทีพี + เอชทีทีพี + เอสโอเอพี + ดับเบิ้ลยูเอสดีเอล + ยูดีดีไอ (XML + HTTP + SOAP + WSDL + UDDI) หรือในระดับสูงกว่านั้น ต่อไปนี้คือรายละเอียดคร่าว ๆ ของแต่ละส่วน แต่ควรตระหนักว่าแต่ละส่วนอาจจะยังเป็นเทคโนโลยีที่กำลังอยู่ระหว่างพัฒนา

2.4.2 อาปาเช่เว็บเซิร์ฟเวอร์ (Apache Web Server)

เป็นโปรแกรมที่ใช้รองรับการให้บริการที่เรียกว่า เวิลด์ไวด์เว็บ (World Wide Web : WWW) ซึ่งผู้ใช้งานอินเทอร์เน็ตโดยทั่วไปรู้จักคุ้นเคยกันเป็นอย่างดี ทั้งยังเป็นบริการหนึ่งที่มีผู้ใช้งานสูงสุดบนชั้นเน็ตเวิร์กอีกด้วย ผู้ใช้ทั่วไปนิยมใช้บริการเวิลด์ไวด์เว็บนี้เพื่อค้นหา หรือเลือกดูข้อมูลที่สนใจ และดึงเอาข้อมูลที่ต้องการมาใช้งาน ส่วนองค์กรต่าง ๆ นิยมใช้เพื่อการประชาสัมพันธ์ข้อมูล หรือใช้เป็นช่องทางการติดต่อสื่อสารกับผู้ใช้งานอีกทางหนึ่ง ให้ประโยชน์ในการส่งผ่านข้อมูลทั่วไป หรือใช้ในการทำธุรกรรมพาณิชย์อิเล็กทรอนิกส์ ทั้งนี้เนื่องมาจากการติดตั้งเว็บเซิร์ฟเวอร์ขึ้นมาเพื่อใช้งานนั้นสามารถทำได้โดยไม่ยุ่งยาก และเสียค่าใช้จ่ายไม่มากนัก

อาปาเช่เป็นซอฟต์แวร์ที่อยู่ในลักษณะของ โอเพ่นซอร์ส (open source) ที่เปิดให้บุคคลทั่วไปสามารถเข้ามาร่วมพัฒนาส่วนต่าง ๆ ของอาปาเช่ได้ ซึ่งทำให้เกิดเป็น โมดูลที่เกิดประโยชน์มากมาย เช่น mod_perl, mod_python หรือ mod_php ซึ่งเป็นโมดูลที่ทำให้อาปาเช่สามารถใช้ประโยชน์ และทำงานร่วมกับภาษาอื่นได้ แทนที่จะเป็นเพียงเซิร์ฟเวอร์ที่ให้บริการเพียงแค่ เอชทีเอ็มแอลอย่างเดียว นอกจากนี้อาปาเช่เองยังมีความสามารถอื่นๆ ด้วย เช่น การยืนยันตัวบุคคลจะเรียกใช้โมดูล mod_auth, mod_access, mod_digest หรือเพิ่มความปลอดภัยในการสื่อสารผ่านโปรโตคอลเอชทีทีพีเอสด้วยโมดูล mod_ssl นอกจากนี้ ก็ยังมีโมดูลอื่นๆ ที่ได้รับความนิยมใช้ เช่น mod_vhost ทำให้สามารถสร้างโฮสต์ท์เสมือน www.sample.com, wiki.sample.com, mail.sample.com หรือ www.ilovewiki.org ภายในเครื่องเดียวกันได้ หรือ mod_rewrite เป็นเครื่องมือที่จะช่วยให้ยูอาร์แอลของเว็บนั้นอ่านง่ายขึ้น

2.4.3 เซิร์ฟเวอร์-ไซด์ สคริปต์ (Server Side Script)

เป็นสคริปต์ที่ทำงานที่ฝั่งเซิร์ฟเวอร์ ถูกประมวลผลโดยโปรแกรมเว็บเซิร์ฟเวอร์ เพื่อแปลงเป็นเอกสารในรูปแบบเอชทีทีพี แล้วส่งผลลัพธ์ที่ได้ไปให้เว็บเบราว์เซอร์ที่ฝั่งไคลเอนต์อีก

ทีหนึ่ง จุดเด่นคือ ไม่ต้องคำนึงว่าฝั่งผู้ใช้จะใช้งานเบราว์เซอร์ชนิดใด เพราะการประมวลผลเกิดขึ้นที่ฝั่งเซิร์ฟเวอร์เอง แต่ต้องคำนึงถึงโปรแกรมเว็บเซิร์ฟเวอร์ว่า สามารถรองรับการทำงานได้หรือไม่ จึงควรเลือกเซิร์ฟเวอร์ที่ใช้โปรแกรมเว็บเซิร์ฟเวอร์ที่รองรับการทำงานได้ด้วย เช่น หากต้องการใช้งานเอเอสพี ก็ต้องเลือกเซิร์ฟเวอร์ที่เป็นระบบปฏิบัติการวินโดว์เอ็นที, วินโดว์ 2000, วินโดว์ 2003 แต่ถ้าหากต้องการใช้งาพีเอชพีหรือซีจีไอ (CGI) ก็ต้องเลือกเซิร์ฟเวอร์ที่เป็นยูนิกซ์หรือลีนุกซ์เป็นต้น ข้อเสียเซิร์ฟเวอร์ไซด์สคริปต์ คือ ถ้าหากมีการส่งข้อมูลมาให้เซิร์ฟเวอร์ประมวลผลมาก ๆ จะเป็นภาระให้เซิร์ฟเวอร์ในการประมวลผล และเป็นการสร้างความหนาแน่นให้เส้นทางจราจรในระบบเครือข่ายมากขึ้น ทำให้การทำงานช้าลง

2.4.4 ไคลเอนต์-ไซด์ สคริปต์ (Client Side Script)

เป็นสคริปต์ที่ทำงานที่ฝั่งไคลเอนต์ ถูกประมวลผลด้วยโปรแกรมเว็บเบราว์เซอร์ของผู้ใช้และแสดงผลเป็นเว็บเพจออกมาให้ผู้ใช้ดู มีจุดเด่นตรงที่สามารถโต้ตอบกับผู้ใช้ได้อย่างรวดเร็ว และเนื่องจากสคริปต์ชนิดนี้ทำงานที่ฝั่งผู้ใช้เอง จึงไม่มีข้อจำกัดในการเลือกใช้เซิร์ฟเวอร์ ซึ่งก็หมายความว่า เว็บเซิร์ฟเวอร์จะเป็นระบบปฏิบัติการใด ๆ ก็ได้ แต่มีข้อเสียตรงที่ต้องคำนึงถึงว่าทางเบราว์เซอร์ของผู้ใช้สนับสนุนและสามารถใช้งานสคริปต์ที่เราเขียนได้หรือไม่

2.4.5 พีเอชพี (Hypertext Preprocessor : PHP)

เป็นภาษาคอมพิวเตอร์ในลักษณะเซิร์ฟเวอร์-ไซด์ สคริปต์ โดยลิขสิทธิ์อยู่ในลักษณะโอเพนซอร์ส ภาษาพีเอชพีใช้สำหรับจัดทำเว็บไซต์ และแสดงผลออกมาในรูปแบบเอชทีเอ็มแอล โดยมีรากฐานโครงสร้างคำสั่งมาจากภาษา ภาษาซี ภาษาจาวา และภาษาเพิร์ล ภาษาพีเอชพีนั้นง่ายต่อการเรียนรู้ ซึ่งเป้าหมายหลักของภาษานี้ คือให้นักพัฒนาเว็บไซต์สามารถเขียน เว็บเพจ ที่มีความตอบโต้ได้อย่างรวดเร็ว

2.4.6 จาวาสคริปต์ (JavaScript)

จาวาสคริปต์ เป็นภาษาในรูปแบบของภาษาโปรแกรมแบบโปรโตไทป์ (Prototype)โดยมีโครงสร้างของภาษาและไวยกรณ์อยู่บนพื้นฐานของภาษาซี

ปัจจุบันมีการใช้จาวาสคริปต์ที่ฝังอยู่ในเว็บเบราว์เซอร์ในหลายรูปแบบ เช่น ใช้เพื่อสร้างเนื้อหาที่เปลี่ยนแปลงเสมอภายในเว็บเพจ ใช้เพื่อตรวจสอบความถูกต้องของข้อมูลที่ผู้ใช้กรอกก่อนนำเข้าระบบ, ใช้เพื่อเข้าถึงข้อมูลที่อยู่ภายใต้โครงสร้างรูปแบบวัตถุเอกสาร (Document Object Model : DOM) เป็นต้น

นอกจากนี้จาวาสคริปต์ยังถูกฝังอยู่ในแอปพลิเคชันต่าง ๆ นอกเหนือจากเว็บเบราว์เซอร์ได้อีกด้วย เช่น widget ของ Yahoo! เป็นต้น โดยรวมแล้วจาวาสคริปต์ถูกใช้เพื่อให้นักพัฒนาโปรแกรม สามารถเขียนสคริปต์เพื่อสร้างคุณสมบัติพิเศษต่าง ๆ เพิ่มเติมจากที่มีอยู่บนโปรแกรมประยุกต์ดั้งเดิม

โปรแกรมใด ๆ ที่สนับสนุนจาวาสคริปต์จะมีตัวขับเคลื่อนจาวาสคริปต์ (JavaScript Engine) ของตัวเอง เพื่อเรียกใช้งานโครงสร้างเชิงวัตถุของโปรแกรมหรือโปรแกรมประยุกต์นั้น ๆ

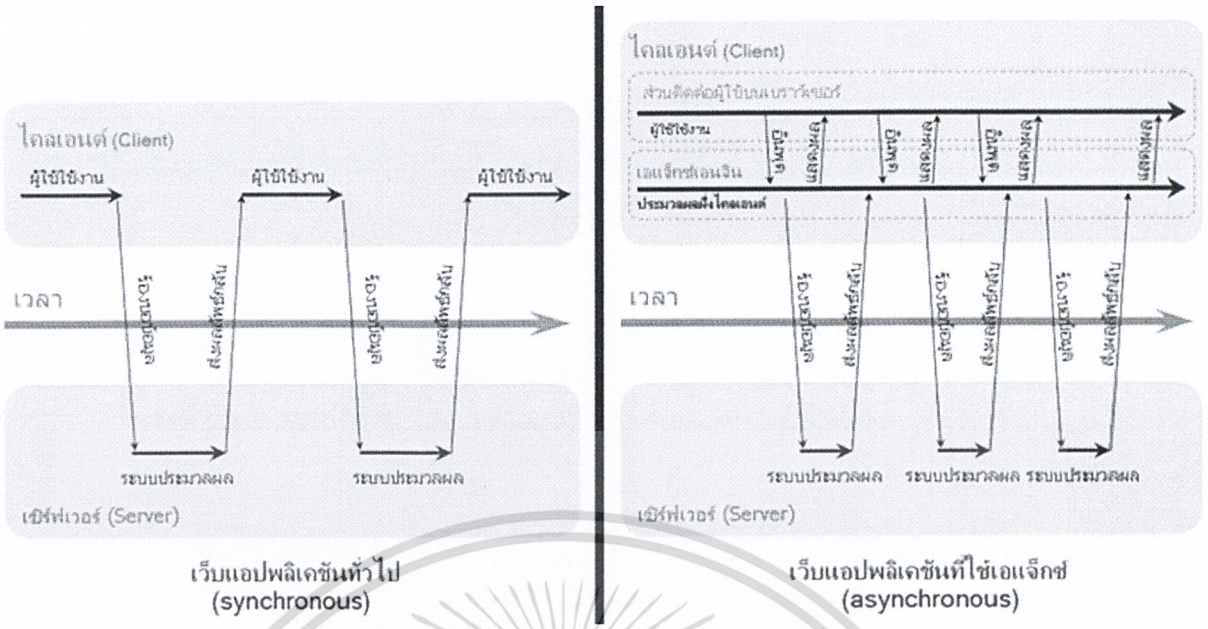
2.4.7 เอแจ็กซ์ (Asynchronous JavaScript And XML : AJAX)

เป็นกลุ่มของเทคนิคในการพัฒนาเว็บแอปพลิเคชันเพื่อให้ความสามารถโต้ตอบกับผู้ใช้ได้ดีขึ้น โดยการรับส่งข้อมูลในฉากหลัง ทำให้ทั้งหน้าไม่ต้องโหลดใหม่ทุกครั้งที่มีการเปลี่ยนแปลง ซึ่งช่วยทำให้เพิ่มการตอบสนอง ความรวดเร็ว และการใช้งานโดยรวม เอแจ็กซ์นั้นไม่ใช่เทคโนโลยีใหม่ แต่เป็นเทคนิคที่ได้ใช้เทคโนโลยีหลายอย่างที่มีอยู่แล้วรวมกันดังต่อไปนี้

- เอกซ์เอชทีเอ็มแอล (XHTML) หรือเอชทีเอ็มแอล และซีเอสเอส (CSS) ใช้ในการแสดงผลลัพธ์และรูปแบบข้อมูล
- อีซีเอ็มเอสคริปต์ (ECMAScript) เช่นจาวาสคริปต์ ในการเข้าถึงโครงสร้างรูปแบบวัตถุเอกสาร เพื่อใช้ในการแสดงข้อมูลที่มีการเปลี่ยนแปลงหรือโต้ตอบกับผู้ใช้
- เอกซ์เอ็มแอลเอชทีทีพีรีเควส (XMLHttpRequest) ใช้ในการแลกเปลี่ยนข้อมูลอะซิง-โครนัสกับเว็บเซิร์ฟเวอร์
- เอกซ์เอ็มแอล (XML) ใช้เป็นรูปแบบข้อมูลในการแลกเปลี่ยน ซึ่งรูปแบบอื่นก็สามารถใช้ได้เช่นกันไม่ว่าจะเป็น เอชทีเอ็มแอล, เจเอสโอเอ็น (JSON), อีบีเอ็มแอล (EBML), หรือเพลนเท็กซ์

วิธีการทำงานของเว็บแอปพลิเคชันแบบดั้งเดิมนั้น โดยปกติแล้วเมื่อผู้ใช้ทำการร้องขอข้อมูลจากเซิร์ฟเวอร์ ตัวเว็บเบราว์เซอร์จะทำการส่งข้อมูลการร้องขอโดยใช้โพรโทคอลเอชทีทีพีเพื่อติดต่อกับเว็บเซิร์ฟเวอร์ และที่เว็บเซิร์ฟเวอร์จะทำการประมวลผลจากการร้องขอที่ได้รับ และส่งผลลัพธ์เป็นหน้าเว็บเพจกลับไปให้ผู้ใช้ วิธีการข้างต้นเป็นวิธีการแบบการร้องขอและการตอบรับ ซึ่งผู้ใช้จะต้องรอระหว่างที่เซิร์ฟเวอร์ประมวลผลอยู่ ซึ่งเป็นหลักการทำงานแบบ ซิงโครนัส แต่การทำงานของเว็บแอปพลิเคชันที่ใช้เทคนิคเอแจ็กซ์จะเป็นการทำงานแบบอะ-ซิงโครนัส หรือการติดต่อสื่อสารแบบไม่ต่อเนื่อง โดยเซิร์ฟเวอร์จะทำการส่งผลลัพธ์เป็นเว็บเพจให้ผู้ใช้ทันทีโดยไม่ต้องรอให้ประมวลผลเสร็จก่อน หลังจากนั้นเว็บเพจที่ผู้ใช้ได้รับจะทำการดึงข้อมูลในส่วนต่างๆทีหลัง หรือจะดึงข้อมูลก็ต่อเมื่อผู้ใช้ต้องการเท่านั้น

เทคนิคเอแจ็กซ์นั้นสามารถสร้างเอชทีเอ็มแอล ได้ในเครื่องผู้ใช้ ทำให้ขนาดข้อมูลนั้นเล็กลงในครั้งต่อ ๆไป เพราะสามารถส่งเพียงข้อมูล และคำสั่งจาวาสคริปต์ลงมาเฉพาะส่วนที่มีการเปลี่ยนแปลง แทนที่จะต้องส่งข้อมูลใหม่หมดมาทั้งหน้า ซึ่งทั้งนี้ขึ้นอยู่กับการออกแบบของเว็บแอปพลิเคชันนั้น ๆ และเนื่องจากการใช้เทคนิคเอแจ็กซ์นั้นทำให้การเปลี่ยนแปลงต่าง ๆ เช่น การแก้ไข เพิ่มเติม ลบทิ้งรายการข้อมูล หรือการดึงข้อมูลที่ต้องการจะค้นหานั้น สามารถทำได้ในฉากหลัง ทำให้ผู้ใช้รู้สึกการตอบสนองนั้น คล้ายคลึงกับโปรแกรมคอมพิวเตอร์ มากกว่าเว็บปกติที่ต้องรอโหลดใหม่ทั้งหน้าสำหรับการเปลี่ยนแปลงต่าง ๆ



รูปที่ 2.5 เปรียบเทียบระหว่างเว็บแอปพลิเคชันแบบดั้งเดิมกับแบบที่ใช้เอแจ็กซ์

2.4.8 เอชทีเอ็มแอล (HTML)

เป็นภาษามาร์กอัพ (Markup Language) หลักในปัจจุบันที่ใช้ในการสร้างเว็บเพจ หรือข้อมูลอื่นที่เรียกดูผ่านทางเว็บเบราว์เซอร์ ซึ่งตัวโค้ดจะแสดงโครงสร้างของข้อมูล ในการแสดงหัวข้อ ลิงก์ ย่อหน้า รายการ รวมถึงการสร้างแบบฟอร์ม เชื่อมโยงภาพหรือวิดีโอด้วย โครงสร้างของโค้ดเอชทีเอ็มแอลจะอยู่ในลักษณะภายในวงเล็บสามเหลี่ยม

2.4.9 มายเอสคิวแอล (MySQL)

มายเอสคิวแอล คือ โปรแกรมระบบจัดการฐานข้อมูล มีหน้าที่เก็บข้อมูลอย่างเป็นระบบ รองรับคำสั่งเอสคิวแอล (Structured Query Language : SQL) เป็นเครื่องมือสำหรับเก็บข้อมูล ที่ต้องใช้ร่วมกับเครื่องมือหรือโปรแกรมอื่นอย่างบูรณาการ เพื่อให้ได้ระบบงานที่รองรับความต้องการของผู้ใช้ เช่น ทำงานร่วมกับเว็บเซิร์ฟเวอร์ เพื่อให้บริการแก่ภาษาสคริปต์ที่ทำงานฝั่งเครื่องให้บริการ เช่น ภาษาพีเอชพี, ภาษาเอเอสพี หรือภาษาเจเอสพี (JSP) เป็นต้น หรือทำงานร่วมกับโปรแกรมประยุกต์ (Application Program) เช่น ภาษาวิชวลเบสิก (Visual Basic) ภาษาจาวา หรือภาษาซี เป็นต้น

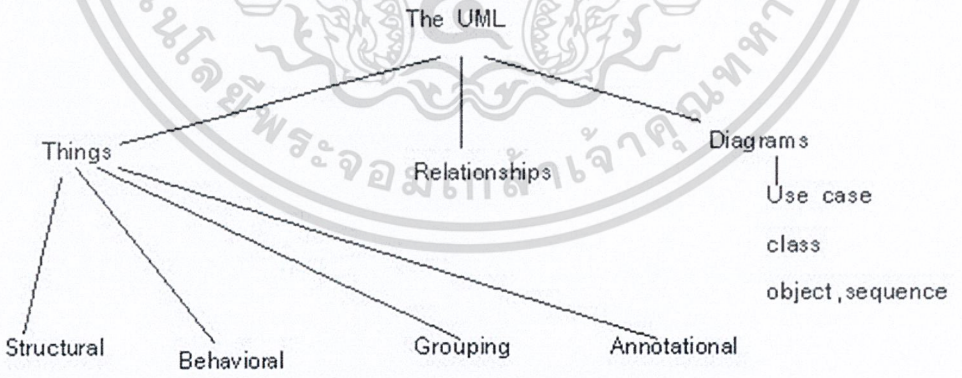
มายเอสคิวแอล เป็นระบบฐานข้อมูลแบบโอเพนซอร์ส สำหรับจัดการระบบฐานข้อมูล (Database System) ผ่านเอสคิวแอล โปรแกรมนี้ถูกพัฒนาโดย บริษัท MySQL AB ในประเทศสวีเดน มีทั้งแบบใช้ฟรี และเชิงธุรกิจ

2.5 ยูเอ็มแอล (Unified Modeling Language : UML)

ยูเอ็มแอลเป็นโมเดลมาตรฐานที่ใช้ในวิธีการออกแบบการพัฒนาเชิงวัตถุ (Object-oriented Design Methodology) เป็นเครื่องมือที่ได้รับการยอมรับเพิ่มขึ้นตลอดเวลา เริ่มประยุกต์ใช้กับระบบงานมากขึ้น เพราะเป็นเครื่องมือที่มีความหลากหลายในการแสดงแบบซอฟต์แวร์ ซึ่งสัญลักษณ์ที่ใช้แสดงนั้นจะได้มาจากการรวมเอาวิธีการในการออกแบบและวิเคราะห์แบบเชิงวัตถุทั้ง 3 แบบ คือ

- **แนวคิดแบบบูช (Booch Method)** เป็นวิธีการที่มีชื่อเสียงมาก เพราะมีไดอะแกรมจำนวนมากสำหรับใช้งาน แต่มีข้อเสียคือมีมากเกินความจำเป็น และยุ่งยากมากในการวาดไดอะแกรม ด้วยมือ แนวความคิดแบบบูชเมธอด จะทำการวิเคราะห์ทั้งแบบไมโคร และไมโครดีเวลลอปเม้นท์ (Micro Development) และอยู่บนพื้นฐานของการพัฒนาระบบงานแบบกรรมวิธีวนรอบเพิ่มพูน (Iteration and Incremental Processs)
- **โมเดลแบบโอเอ็มที (Object-Modeling Technique : OMT)** ประกอบด้วยโมเดลจำนวนมาก ครอบคลุมถึงออปเจคโมเดล (Object Model), ไดนามิกโมเดล (Dynamic Model), ฟังก์ชันนอลโมเดล (Functional Model), ยูสเคสโมเดล (Use-case Model)
- **วิธีแบบยูสเคส (Use case methodology)** เป็นรูปแบบวิธีการทำงานที่เน้นความต้องการด้วย มีพื้นฐานการทำงานอยู่บนยูสเคสโมเดลซึ่งยูสเคสโมเดลนี้ จะถูกใช้ตลอดทุกระยะในการพัฒนาระบบงาน

2.5.1 องค์ประกอบของยูเอ็มแอล



รูปที่ 2.6 องค์ประกอบของยูเอ็มแอล

จากรูปที่ 2.6 แสดงให้เห็นถึง องค์ประกอบต่าง ๆ ของยูเอ็มแอล โดยมีรายละเอียดดังต่อไปนี้

2.5.1.1 สัญลักษณ์ทั่วไป (Things)

คือสัญลักษณ์พื้นฐานที่ถูกใช้งานในการสร้างไดอะแกรมยูเอ็มแอลต่าง ๆ โดย แบ่งเป็นหมวดย่อย ๆ ดังนี้

- หมวดโครงสร้าง (Structural) ได้แก่ ยูสเคส (Use-case), คลาส (Class), อินเตอร์เฟส (Interface), คอมโพเนนต์ (Component), คอลลาบอเรชัน (Collaboration) และโหนด (Node)
- หมวดพฤติกรรม (Behavioral) คือส่วนที่เป็นไดนามิกของยูเอ็มแอล ได้แก่ การปฏิสัมพันธ์ (Interaction), สเตทแมชชีน (State machine)
- หมวดจัดกลุ่ม (Grouping) เพื่อใช้ในการรวบรวมองค์ประกอบต่าง ๆ ในโมเดลให้เหมาะสม ได้แก่ แพ็กเกจ (Package)
- หมวดคำอธิบายประกอบ (Annotational)

2.5.1.2 ความสัมพันธ์ (Relationships)

- ความสัมพันธ์แบบพึ่งพา (Dependency Relationship)
- ความสัมพันธ์แบบเจเนอรัลไลเซชัน (Generalization Relationship) หรือความสัมพันธ์แบบไม่เจาะจง ได้แก่ ความสัมพันธ์แบบสืบทอดคุณสมบัติ (Inheritance)

2.5.1.3 ไดอะแกรมต่าง ๆ (Diagrams)

ประกอบด้วย 9 ไดอะแกรม โดยในแต่ละไดอะแกรมจะเปรียบเสมือนมุมมองในด้านต่างๆ ของระบบที่กำลังพัฒนา ซึ่งจะช่วยในการวิเคราะห์ออกแบบเป็นไปได้อย่างมีประสิทธิภาพและง่ายดายมากยิ่งขึ้น ในที่นี้จะนำเสนอเพียง 4 ไดอะแกรม โดยมีรายละเอียดดังนี้

1) ยูสเคสไดอะแกรม (Use Case Diagram)

เป็นไดอะแกรมที่ช่วยให้ผู้พัฒนาทราบถึงความสามารถของระบบว่าต้องทำอะไรได้บ้าง ทราบถึงผู้ใช้งานในแต่ละส่วนของระบบและเกิดความง่ายในการสื่อสารระหว่างผู้พัฒนากับผู้ใช้ระบบ ส่วนประกอบสำคัญยูสเคสได้แก่

- ยูสเคส คือความสามารถหรือฟังก์ชันของระบบซอฟต์แวร์ที่จะพัฒนา โดยการเขียนยูสเคสจะใช้วงรีและคำอธิบายฟังก์ชันการทำงานอยู่ในวงรีนั้น ดังแสดงในรูปที่ 2.7

รูปที่ 2.7 แสดงตัวอย่างยูสเคส

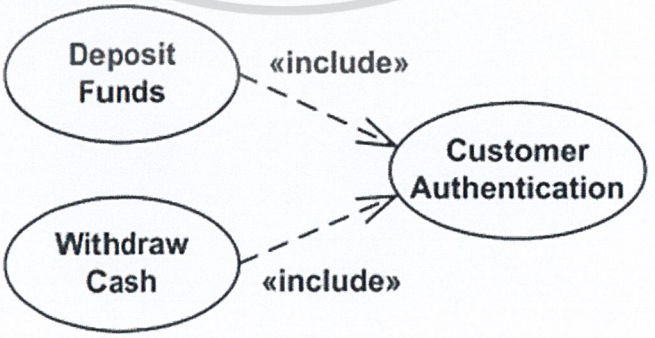
- แอ็กเตอร์ (Actor) คือ ผู้ที่กระทำกับระบบ หรือผู้ที่เกี่ยวข้อง โดยจะเป็นคนหรือไม่ก็ได้ ซึ่งเป็นผู้แลกเปลี่ยนข้อมูลข่าวสารกับระบบที่จะทำการพัฒนา โดยเราจะใช้สัญลักษณ์รูปคนแทนสัญลักษณ์ของแอ็กเตอร์นั้น ดังแสดงในรูปที่ 2.8

รูปที่ 2.8 แสดงตัวอย่างแอ็กเตอร์

- เส้นแสดงความสัมพันธ์ (Relationship) คือ เส้นเพื่อแสดงความสัมพันธ์ระหว่างแอ็กเตอร์กับแอ็กเตอร์ หรือยูสเคสกับยูสเคส
  - ความสัมพันธ์แบบขยาย (Extend Relationship) ใช้เพื่อบอกว่ายูสเคสหนึ่ง ถูกช่วยเหลือโดยการทำงานยูสเคสอื่น โดยจะใช้ <<extend>> เป็นเครื่องหมายอ้างอิง ดังแสดงในรูปที่ 2.9

รูปที่ 2.9 แสดงความสัมพันธ์แบบขยาย

  - ความสัมพันธ์แบบรวม (Include Relationship) ใช้เพื่อบอกว่ายูสเคสหนึ่งถูกอาศัยการทำงานของยูสเคสอื่นๆ โดยจะใช้ <<include>> เป็นเครื่องหมายอ้างอิง ดังแสดงในรูปที่ 2.10



รูปที่ 2.10 แสดงความสัมพันธ์แบบรวม

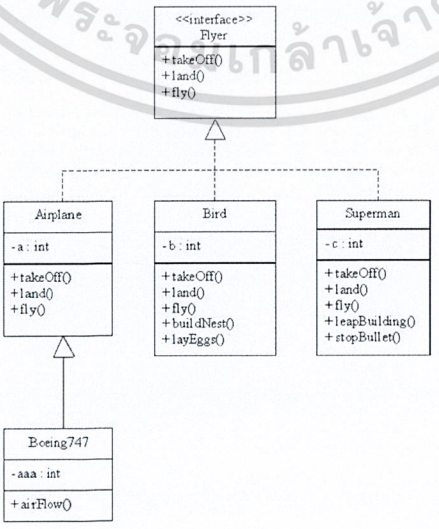
2) คลาสไดอะแกรม (Class Diagram)

จะแสดงรายละเอียดของคลาสและความสัมพันธ์ระหว่างคลาสในมุมมองแบบลอจิคอล (logical view) องค์ประกอบของคลาสไดอะแกรม ได้แก่

- คลาส, โครงสร้างของคลาส และพฤติกรรมของคลาส
- ตัวบ่งชี้ความหลากหลาย (Multiplicity) และเนวิเกชัน (Navigation)
- ชื่อของหน้าที่ (Role)
- ความสัมพันธ์เชิงโครงสร้าง (Association), ความสัมพันธ์แบบรวม (Aggregation), ความสัมพันธ์แบบพึ่งพา (Dependency), และการสืบทอดคุณสมบัติ (Inheritance)

คลาสไดอะแกรมประกอบด้วยสัญลักษณ์ของคลาสและเส้นแสดงความสัมพันธ์ ในส่วนของสัญลักษณ์คลาสจะถูกวาดเป็นรูปสี่เหลี่ยมซึ่งประกอบด้วย 3 ส่วนดังรูปนั่นคือ ชื่อคลาส อยู่ในส่วนบนสุด แอตทริบิวต์อยู่ตรงส่วนกลาง และโอเปอเรชันในส่วนล่างสุด ส่วนของเส้นแสดงความสัมพันธ์สามารถแบ่งเป็น 3 รูปแบบใหญ่ ๆ คือ

1. ความสัมพันธ์แบบพึ่งพา (Dependency) เป็นความสัมพันธ์เกิดขึ้นเมื่อการเปลี่ยนแปลงที่เกิดขึ้นกับคลาสที่ถูกพึ่งพิงจะส่งผลต่อคลาสที่พึ่งพิงคลาสดังกล่าว
2. ความสัมพันธ์แบบทั่วไป เป็นความสัมพันธ์ระหว่างซูเปอร์คลาสและซับคลาสนั่นเอง
3. ความสัมพันธ์เชิงโครงสร้าง เป็นความสัมพันธ์อีกชนิดหนึ่งระหว่างคลาส ซึ่งแบ่งได้ดังนี้
   3.1 ความสัมพันธ์เชิงโครงสร้างปกติ (Normal Association) มักใช้ในโมเดลระบบที่ซับซ้อน
   3.2 ความสัมพันธ์แบบรวม เป็นความสัมพันธ์ระหว่างคลาสหรือออบเจ็กต์ในแง่ของการรวมกัน



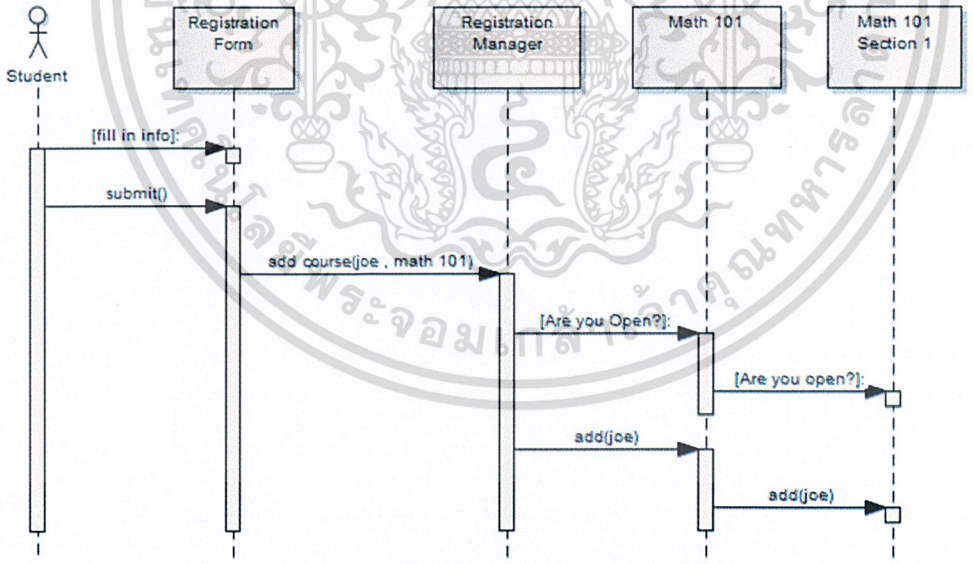
รูปที่ 2.11 แสดงตัวอย่างการเขียนคลาสไดอะแกรม

จากรูปที่ 2.11 เป็นตัวอย่างการเขียนคลาสไดอะแกรม โดยจะแบ่งออกเป็น 5 คลาส คือ คลาส Flyer, คลาส Airplane, คลาส Bird, คลาส Superman และคลาส Boeing747 ซึ่งจะมีแอตทริบิวและเมธอดกำหนดอยู่ที่คลาส และจะเห็นว่าคลาส Boeing747 จะเป็นคลาสที่สืบทอดคุณสมบัติมาจากคลาส Airplane ส่วนคลาส Airplane, Bird, Superman ก็จะเป็นคลาสที่สืบทอดคุณสมบัติมาจากคลาส Flyer ด้วย

3) ซีเควนซ์ไดอะแกรม (Sequence Diagram)

จะเป็นไดอะแกรมที่ใช้แสดงถึงคลาสที่มีส่วนร่วมในแต่ละยูสเคสและข้อความที่ส่งผ่านระหว่างคลาสบนเวลาต่าง ๆ ซีเควนซ์ไดอะแกรมจะเป็นโมเดลแบบไดนามิกที่จะแสดงลำดับของข้อความที่ถูกส่งผ่านระหว่างคลาสออกมาอย่างชัดเจน

ซีเควนซ์ไดอะแกรมประกอบด้วยแกนสมมติ 2 แกนคือ แกนนอน และแกนตั้ง โดยแกนนอนจะแสดงขั้นตอนการทำงาน หรือการส่งข้อความระหว่างวัตถุ ส่วนแกนตั้งเป็นแกนเวลา ทั้ง 2 แกนต้องสัมพันธ์กัน สัญลักษณ์ประกอบด้วย ส่วนที่บอกชื่อของออบเจ็กต์ว่าเป็นออบเจ็กต์อะไร โดยเรียงจากซ้ายไปขวาตามลำดับการทำงานของระบบคือ ออบเจ็กต์ทางซ้ายจะทำงานก่อนออบเจ็กต์ที่อยู่ขวามือ โดยจะมีข้อความเป็นการติดต่อที่ส่งจากออบเจ็กต์หนึ่งไปยังออบเจ็กต์หนึ่งหรืออาจส่งกลับมาหาตัวเองก็ได้



รูปที่ 2.12 แสดงตัวอย่างการเขียนซีเควนซ์ไดอะแกรม

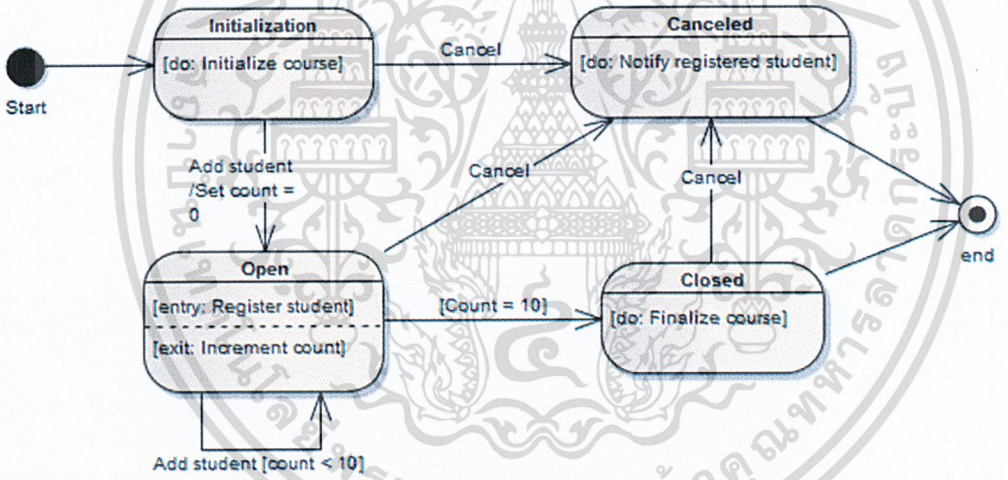
จากรูปที่ 2.12 เป็นตัวอย่างการเขียนซีเควนซ์ไดอะแกรมในการลงทะเบียนเรียนในวิชาคณิตศาสตร์ โดยการทำงานจะเริ่มจากนักเรียนทำการลงทะเบียนรายวิชาไปยังระบบ ระบบลงทะเบียนก็จะตรวจสอบไปยังรายวิชาคณิตศาสตร์ว่าเปิดให้ลงทะเบียนรายวิชาหรือไม่ หลังจาก

นั้นรายวิชาคณิตศาสตร์ก็จะตรวจสอบไปยังกลุ่มที่ 1 ว่าเปิดให้ลงทะเบียนรายวิชาหรือไม่ ถ้าเปิดให้ลงทะเบียน ระบบก็จะลงทะเบียนรายวิชาคณิตศาสตร์ให้กับนักเรียนคนนี้

4) สเตทไดอะแกรม (State Diagram)

จะเป็นโมเดลแบบไดนามิกที่แสดงสถานะ ต่าง ๆ ที่คลาสหนึ่งคลาสจะเป็นได้ในระหว่างช่วงชีวิตในการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น โดยทั่วไปแล้ว สเตทไดอะแกรมจะไม่ถูกใช้กับคลาสทั้งหมด แต่จะใช้อธิบายเฉพาะคลาสที่มีความซับซ้อนสูง ๆ เท่านั้น เพื่อที่จะช่วยให้การออกแบบอัลกอริทึมง่ายขึ้น

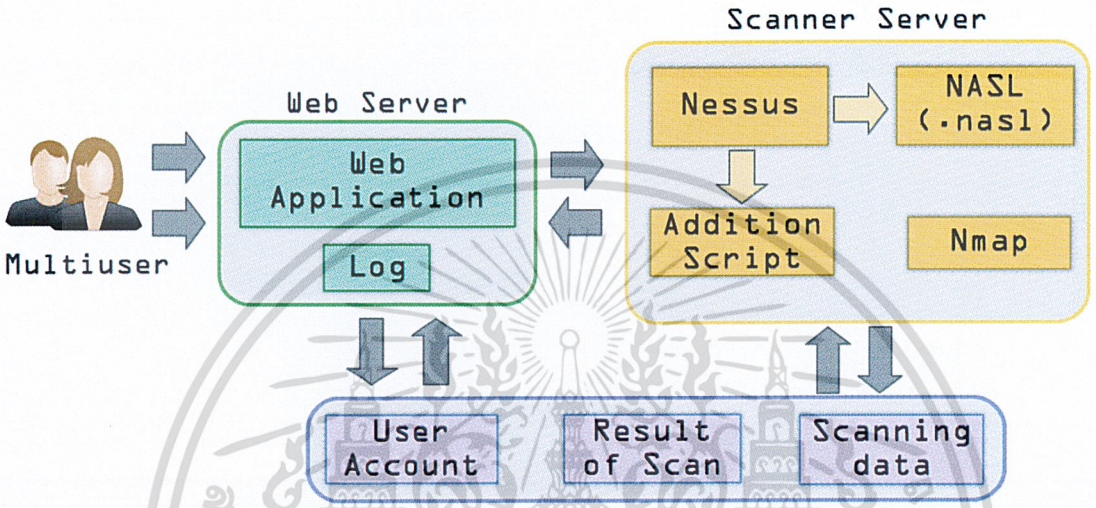
สเตทไดอะแกรมจะแสดงจุดเริ่มต้นและจุดสิ้นสุดสถานะ โดยจุดเริ่มต้นสถานะจะมีสัญลักษณ์เป็นรูปวงกลมทึบ และจุดสิ้นสุดสถานะจะเป็นรูปวงกลมโปร่งล้อมรอบวงกลมทึบข้างใน ในแต่ละสถานะของไดอะแกรมจะถูกแสดงเป็นรูปสี่เหลี่ยมหัวมน และเชื่อมกันด้วยเส้นลูกศรชี้จากสถานะหนึ่งไปยังอีกสถานะหนึ่ง สามารถเขียนคำอธิบายเหตุการณ์ที่ทำให้เปลี่ยนสถานะตรงเส้นลูกศรได้ บางสเตทไดอะแกรมจะมีสถานะวนเวียน



รูปที่ 2.13 แสดงตัวอย่างการเขียนสเตทไดอะแกรม

บทที่ 3
การออกแบบระบบ

3.1 ภาพรวมของระบบ



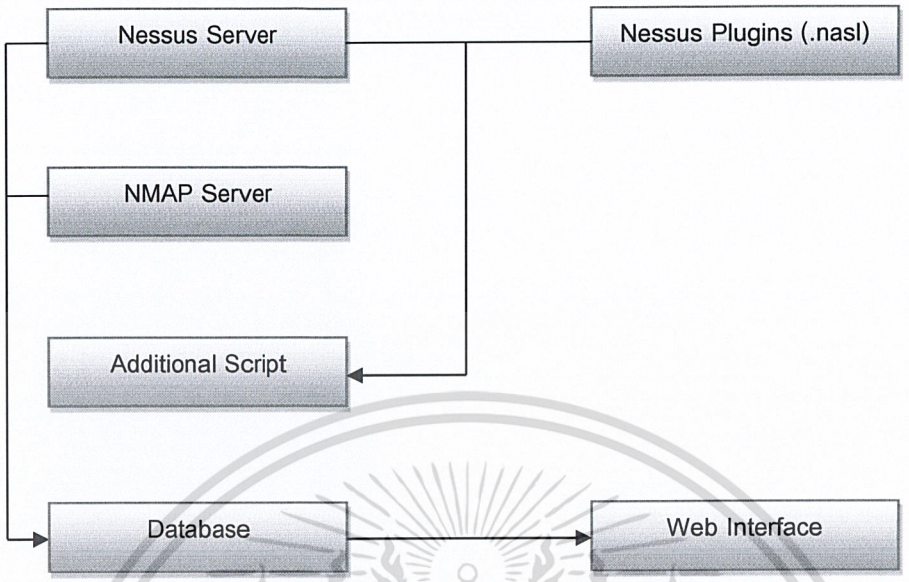
รูปที่ 3.1 ภาพรวมของระบบ

ระบบถูกพัฒนาขึ้นเพื่อให้บริการในการตรวจสอบช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ โดยที่ผู้ใช้งานสามารถใช้งานผ่านเว็บเบราว์เซอร์ โดยการระบุไอพีแอดเดรสหรือชื่อเครื่องคอมพิวเตอร์ที่ต้องการตรวจสอบ แล้วรอผลการตรวจสอบจากระบบว่าคอมพิวเตอร์เครื่องนั้นมีช่องโหว่อะไรบ้าง และมีวิธีการแก้ไขปัญหานั้นอย่างไร

ภาพรวมของระบบแสดงดังรูปที่ 3.1 ผู้ใช้สามารถเข้าใช้งานระบบผ่านเว็บเบราว์เซอร์ ทำให้ง่ายและสะดวกในการใช้งาน อีกทั้งยังสามารถใช้ได้กับทุกเครื่อง โดยไม่จำเป็นต้องติดตั้งโปรแกรม การติดต่อระหว่างผู้ใช้และระบบนั้นจะติดต่อกันผ่านทางโปรโตคอลเอสเอสแอล (Secure Sockets Layer : SSL) ซึ่งทำให้มีความปลอดภัยในการส่งข้อมูลมากยิ่งขึ้น

การทำงานของระบบจะเริ่มจากที่ผู้ใช้ส่งคำสั่งการสแกนไปที่สแกนเนอร์เซิร์ฟเวอร์ ซึ่งมีโปรแกรมเอ็นแมปและเนสซัสเป็นโปรแกรมที่ทำงานอยู่เบื้องหลัง (Back-end) โดยทั้งสองโปรแกรมจะทำหน้าที่แตกต่างกันออกไป เอ็นแมปจะเป็นโปรแกรมที่ทำหน้าที่เป็นพอร์ตสแกนเนอร์ ส่วนเนสซัสจะเป็นสแกนเนอร์ที่ตรวจสอบช่องโหว่ของระบบ ซึ่งผลที่ได้จากการสแกนนั้นจะส่งกลับไปยังผู้ใช้ และถูกบันทึกลงในฐานข้อมูลเพื่อเป็นประวัติการสแกนของผู้ใช้งานนั้น ๆ ด้วย

3.2 สแกนเนอร์เซิร์ฟเวอร์



รูปที่ 3.2 โครงสร้างของสแกนเนอร์เซิร์ฟเวอร์

สแกนเนอร์เซิร์ฟเวอร์นั้นมีหลักการทำงานอย่างคร่าว ๆ ดังรูปที่ 3.2 คือจะมีเอ็นแมปเซิร์ฟเวอร์และเนสซัสเซิร์ฟเวอร์ทำหน้าที่ในการสแกนค่าพารามิเตอร์ต่าง ๆ จากคำสั่งของผู้ใช้จากเว็บเบราว์เซอร์ แล้วทำงานตามคำสั่งจากพารามิเตอร์นั้น ๆ เมื่อทำการสแกนเป้าหมายเรียบร้อยก็จะทำการบันทึกผลการสแกนลงฐานข้อมูลและนำไปแสดงผลบนหน้าเว็บ ซึ่งสามารถเรียกดูผลการสแกนนี้ภายหลังได้ ซึ่งสแกนเนอร์เซิร์ฟเวอร์จะแบ่งการทำงานออกเป็น 2 ส่วน ดังนี้

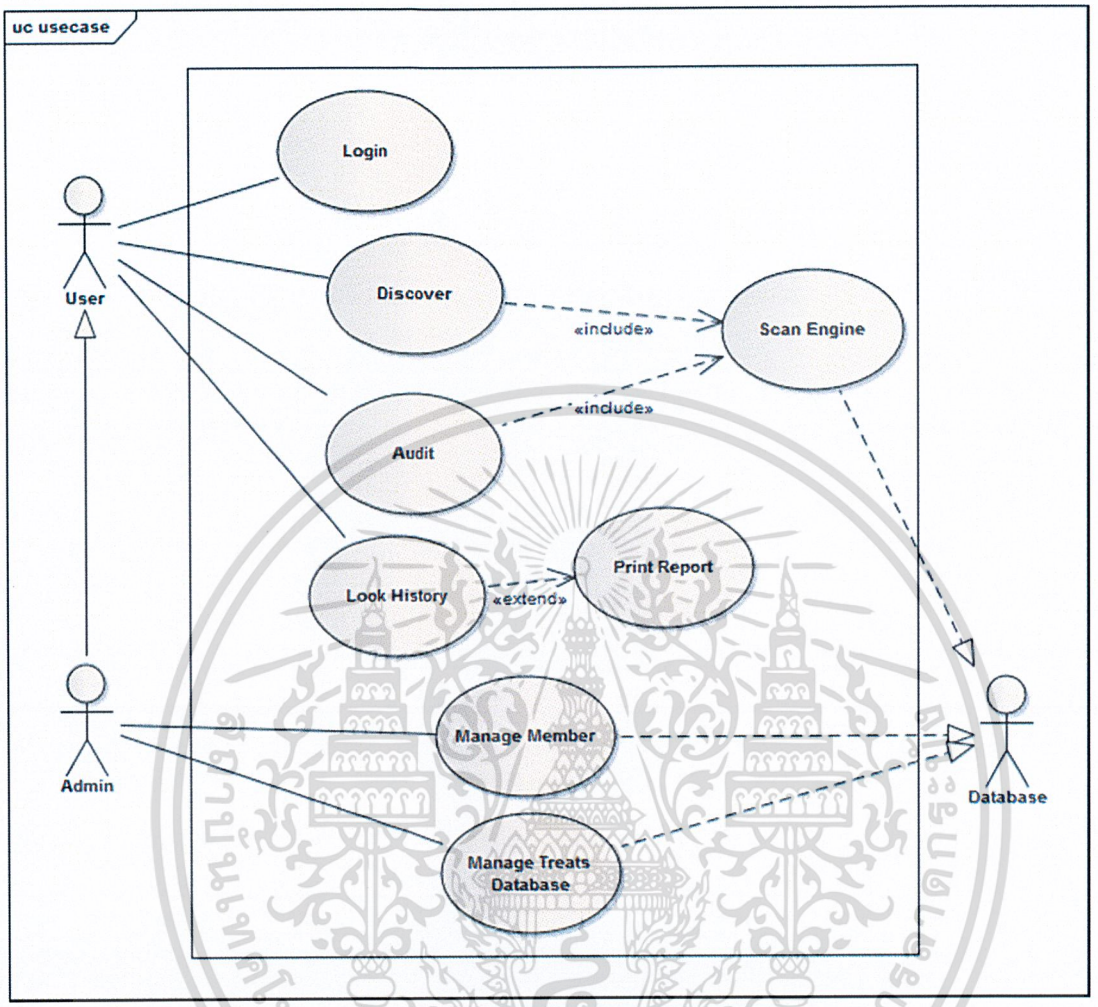
3.2.1 เอ็นแมปเซิร์ฟเวอร์

เป็นโปรแกรมที่จะทำงานในส่วนของการตรวจสอบข้อมูลเบื้องต้นของเป้าหมาย ซึ่งจะเป็นการเน้นไปที่การสแกนพอร์ตของเครื่องเป้าหมายเป็นหลัก โดยผลที่จากตัวเอ็นแมปเซิร์ฟเวอร์นี้จะระบบสถานของเครื่อง พอร์ตที่เปิดมีบริการอะไรบ้างและเครื่องเป้าหมายเป็นระบบปฏิบัติการใด

3.2.2 เนสซัสเซิร์ฟเวอร์

เนสซัสเซิร์ฟเวอร์จะมีหน้าที่หลักในการตรวจสอบช่องโหว่ของเป้าหมายนั้น ๆ โดยจะทำการเรียกเนสซัสปลั๊กอินในการตรวจสอบช่องโหว่ของเป้าหมาย โดยจะเป็นเครื่องมือหลักในการค้นหาช่องโหว่จากร่องรอยต่าง ๆ หรือจากการทดสอบต่าง ๆ ตามมาตรฐาน โดยผลที่ได้จะบอกรายละเอียดได้ครอบคลุมในส่วนเอ็นแมปเซิร์ฟเวอร์ทั้งหมด และจะเพิ่มในส่วนของช่องโหว่ที่ตรวจพบหรือคำแนะนำด้านความปลอดภัยต่าง ๆ พร้อมทั้งแนวทางในการปฏิบัติหรือแก้ไขต่าง ๆ เพื่อให้เกิดความปลอดภัยกับระบบหรือเครื่องเป้าหมาย

3.3 ยูสเคสไดอะแกรม (Use Case Diagram)



รูปที่ 3.3 ยูสเคสไดอะแกรมของระบบ

จากรูปที่ 3.3 จะสังเกตเห็นว่ามีผู้กระทำต่อระบบอยู่ 3 คน คือ ผู้ใช้งาน (User), ผู้ดูแลระบบ (Admin) และ ฐานข้อมูล (Database) โดยที่ผู้ดูแลระบบมีความสามารถแบบผู้ใช้งานได้ทุกอย่าง แต่มีบางเหตุการณ์ที่ผู้ดูแลระบบทำได้ แต่ผู้ใช้งานไม่สามารถทำได้ในระบบ ส่วนฐานข้อมูลเป็นผู้กระบบต่อระบบที่ถูกกระทำเพียงอย่างเดียวมีหน้าที่เก็บข้อมูลลงในฐานข้อมูล

ตารางที่ 3.1 เหตุการณ์ที่มีในระบบ (Event Table)

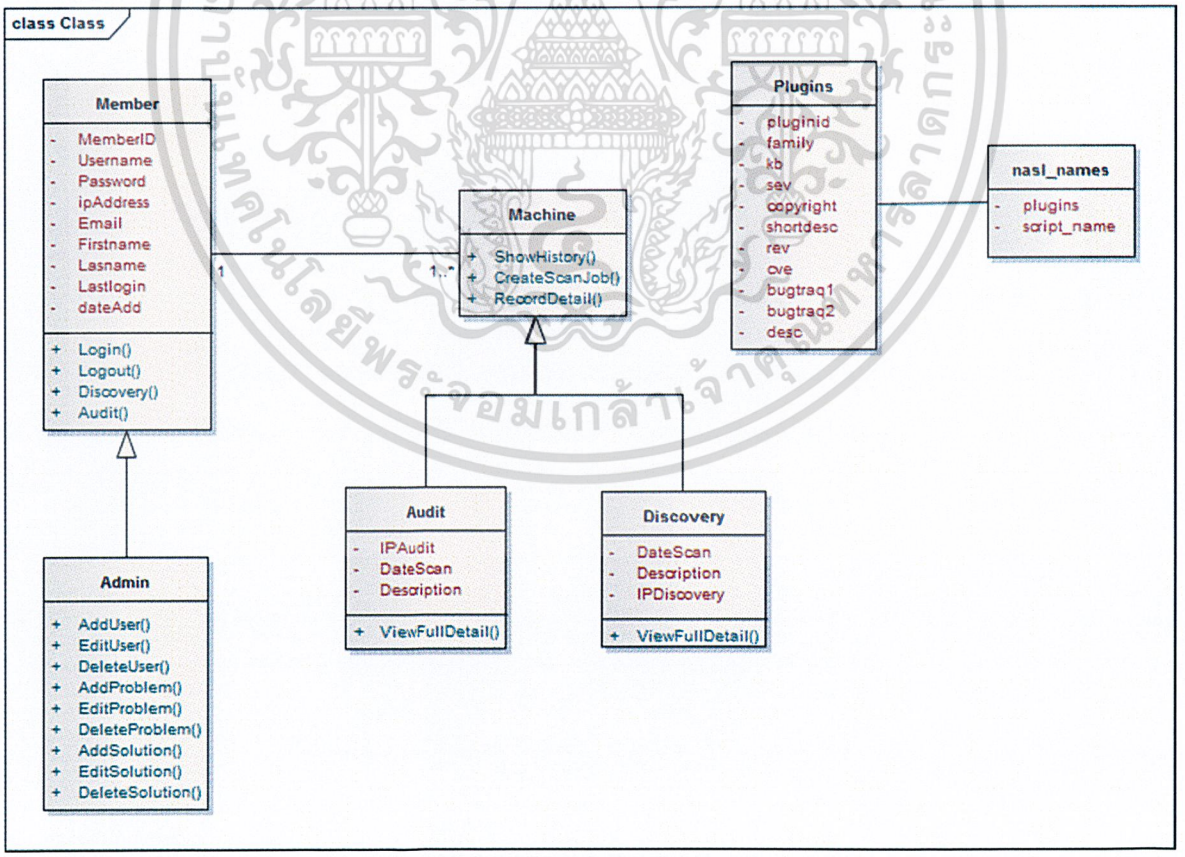
Event	Description	Actor	Abused
Login	การเข้าสู่ระบบ	User/Admin	None
Discover	การสแกนค้นหาเป้าหมาย	User/Admin	None

ตารางที่ 3.1 เหตุการณ์ที่มีในระบบ (ต่อ)

Event	Description	Actor	Abused
Audit	การสแกนและตรวจสอบเพื่อหาช่องโหว่ของเครื่องเป้าหมาย	User/Admin	Database
History	การเลือกเป้าหมายที่เคยตรวจสอบ	User/Admin	Database
Manage Member	การจัดการฐานข้อมูลของผู้ใช้ระบบ	Admin	Database
Manage Threat Database	การจัดการข้อมูลของช่องโหว่และวิธีแก้ไขปัญหา	Admin	Database

จากยูสเคสไดอะแกรม และตารางเหตุการณ์จะสังเกตว่า Discover และ Audit นั้น คือการสแกน จึงจำเป็นต้องใช้ สแกนเอนจิน (Scan Engine) ทำการเพิ่มเข้าไปด้วยแต่ทั้ง 2 แบบจะสแกนในรูปแบบที่ต่างกัน

3.4 คลาสไดอะแกรม (Class Diagram)



รูปที่ 3.4 คลาสไดอะแกรมของระบบ

ตารางที่ 3.2 ข้อมูลของคลาส Member

Field	Key		Data Type	Description
	PK	FK		
MemberID	✓		int	รหัสของผู้ใช้
Username			varchar(20)	ชื่อผู้ใช้
Password			varchar(20)	รหัสผ่านเพื่อเข้าใช้
ipAddress			int	ไอพีแอดเดรสของผู้ใช้
Email			varchar(30)	อีเมลของผู้ใช้
Firstname			varchar(100)	ชื่อจริงผู้ใช้
Lastname			varchar(100)	นามสกุลผู้ใช้
LastLogin			timestamp	เวลาที่ใช้ครั้งล่าสุด
Dateadd			timestamp	เวลาที่ผู้ใช้ถูกนำเข้าสู่ระบบ
flag			int(11)	ระบุว่าเป็นผู้ดูแลระบบ

ตารางที่ 3.3 เมธอดของคลาส Member

Method	Description
Login()	การทำงานเพื่อเข้าสู่ระบบ
Logout()	การทำงานเพื่อออกจากระบบ
Discover()	การทำงานเพื่อค้นหา Machine
Audit()	การทำงานเพื่อต้องการรับทราบข้อมูลของ Machine

จากรูปที่ 3.4 คลาส User และ คลาส Admin เป็นคลาสที่สืบทอดจากคลาส Member มีแอตทริบิวท์ (Attribute) และ เมธอด (Method) เหมือน คลาส Member ซึ่งในคลาส User มีเมธอดเหมือนกับคลาส Member ทั้งหมด แต่คลาส Admin มีเมตธอตเพิ่มดังนี้

ตารางที่ 3.4 เมธอดของคลาส Admin ที่เพิ่มมา

Method	Description
AddMemberDB()	การทำงานเพื่อเพิ่ม ผู้ใช้
EditMemberDB()	เมื่อต้องการแก้ไขข้อมูลผู้ใช้
DeleteMemberDB()	เมื่อต้องการนำผู้ใช้ออกจากระบบ

ตารางที่ 3.4 เมธอดของคลาส Admin ที่เพิ่มมา (ต่อ)

Method	Description
AddProblem()	เพิ่มข้อมูลช่องโหว่ใหม่
EditProblem()	แก้ไขข้อมูลช่องโหว่เดิมที่มี
DeleteProblem()	ลบช่องโหว่ออกจากฐานข้อมูล
AddSolution()	เพิ่มวิธีแก้ปัญหาของช่องโหว่
EditSolution()	แก้ไขวิธีแก้ปัญหาของช่องโหว่
DeleteSolution()	ลบวิธีแก้ปัญหาของช่องโหว่

ตารางที่ 3.5 เมธอดของคลาส Machine

Method	Description
ShowHistory()	แสดงประวัติการแสกนของเครื่อง
RecordDetail()	บันทึกข้อมูลที่ของเครื่อง
CreateScanJob()	สร้างการสแกนครั้งใหม่ของเครื่อง

ตารางที่ 3.6 ข้อมูลของคลาส Audit

Field	Key		Data Type	Description
	PK	FK		
Memberid	✓	✓	int	ไอพีของผู้ตรวจสอบ
Dateaudit			timestamp	เวลาที่ตรวจสอบ
IPAudit			time	ไอพีของเครื่องที่ตรวจสอบ
description			text	รายละเอียดของเครื่องที่ตรวจสอบ

ตารางที่ 3.7 เมตธอตของคลาส Audit

Method	Description
viewfulldetail()	ดูรายละเอียด

ตารางที่ 3.8 ข้อมูลของคลาส Discovery

Field	Key		Data Type	Description
	PK	FK		
Memberid	✓	✓	int	ไอพีของผู้ตรวจสอบ

ตารางที่ 3.8 ข้อมูลของคลาส Discovery (ต่อ)

Field	Key		Data Type	Description
	PK	FK		
Datescan			timestamp	เวลาที่ตรวจสอบ
description			text	รายละเอียดของเครื่องที่ตรวจสอบ

ตารางที่ 3.9 เมตธอตของคลาส Discovery

Method	Description
viewfulldetail()	ดูรายละเอียด

ตารางที่ 3.10 ข้อมูลของคลาส nasl_name

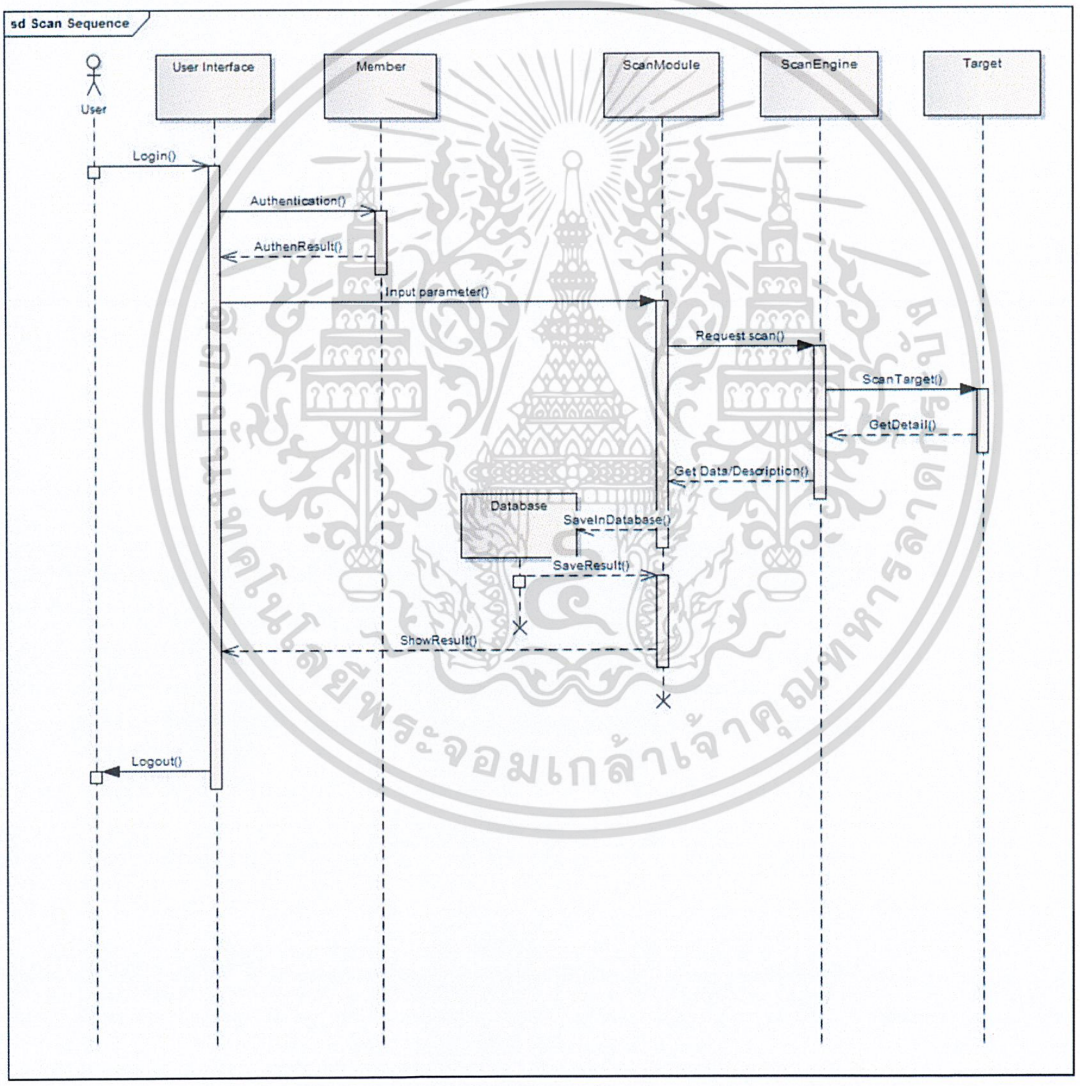
Field	Key		Data Type	Description
	PK	FK		
pluginid	✓		int	หมายเลขปลั๊กอิน
Script_name			varchar(64)	ชนิดของสคริปต์ที่ไปรันโปรแกรม

ตารางที่ 3.11 ข้อมูลของคลาส plugin

Field	Key		Data Type	Description
	PK	FK		
pluginid	✓	✓	varchar(20)	รหัสของปลั๊กอิน
family			varchar(128)	หมวดหมู่ของปลั๊กอิน
kb			varchar(128)	แหล่งอ้างอิงของปลั๊กอิน
sev			varchar(128)	ชนิดของการโจมตี
copyright			varchar(128)	เจ้าของลิขสิทธ์
shortdesc			varchar(128)	อธิบายเนื้อหาอย่างย่อย
rev			varchar(128)	การปรับปรุงรุ่นที่
cve			varchar(128)	รหัสอ้างอิงของ ซีวีอี
Bugtraq1			varchar(128)	รหัสอ้างอิงจากบัคแทรก
Bugtraq2			varchar(128)	รหัสอ้างอิงจากบัคแทรกที่สอง
desc			text	เนื้อหาของปลั๊กอิน

3.4 ซีเควนซ์ไดอะแกรม (Sequence Diagram)

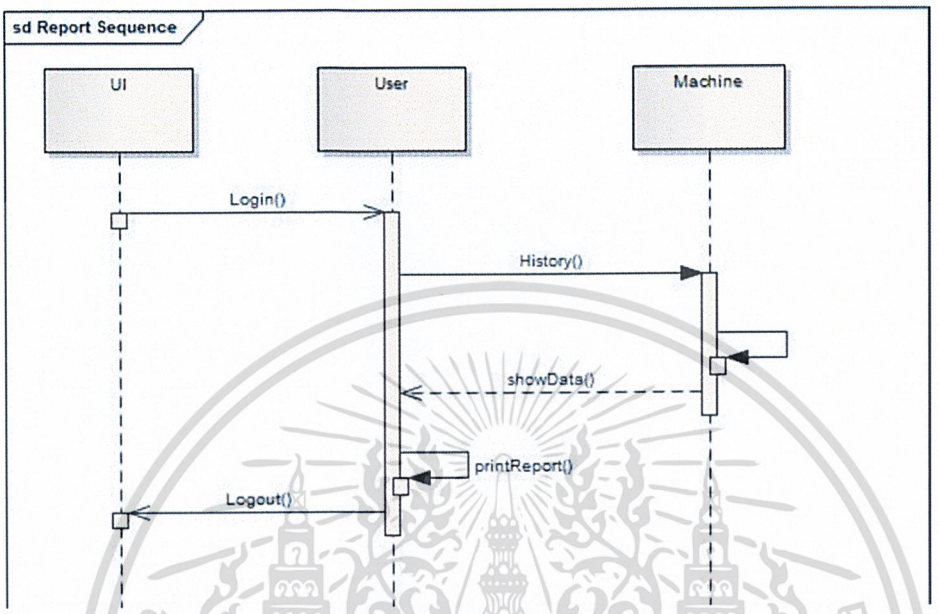
การทำงานของการสแกน เริ่มต้นที่ส่วนติดต่อกับผู้ใช้ จากการล๊อกอิน ไปสู่ในส่วน คลาส Member หลังจากนั้นก็เลือกทำการตรวจสอบว่ามี ผู้ใช้ชื่อนี้อยู่จริงหรือไม่ ถ้ามีจึงเข้าสู่ระบบ และถ้าต้องการตรวจสอบข้อมูลของเครื่อง จึงทำการกรอกค่าพารามิเตอร์ ไปสู่สแกนโมดูล หลังจากนั้น สแกนโมดูลจะเรียกใช้ตัวสแกนเอนจิน เพื่อตรวจสอบข้อมูลของเป้าหมายที่ได้เลือกไว้ หลังจากนั้น สแกนเอนจินรับรู้ข้อมูลของเป้าหมาย จะส่งกลับมาให้สแกนโมดูลเก็บข้อมูลลงฐานข้อมูล พร้อมกับแสดงข้อมูลของเป้าหมายที่ได้ทำการสแกนให้แก่ผู้ใช้งานดู เมื่อไม่ต้องการใช้ระบบจึงทำการออกจากระบบ ดังรูปที่ 3.5



รูปที่ 3.5 ซีเควนซ์ไดอะแกรมของการสแกน

การทำงานของการออกรายงาน เริ่มต้นที่ส่วนติดต่อกับผู้ใช้ จากการล๊อกอิน ไปสู่ในส่วนของคลาส User จากนั้นจะตรวจสอบไปยังคลาส Machine ว่าผู้ใช้คนนี้เคยทำการสแกนมาก่อน

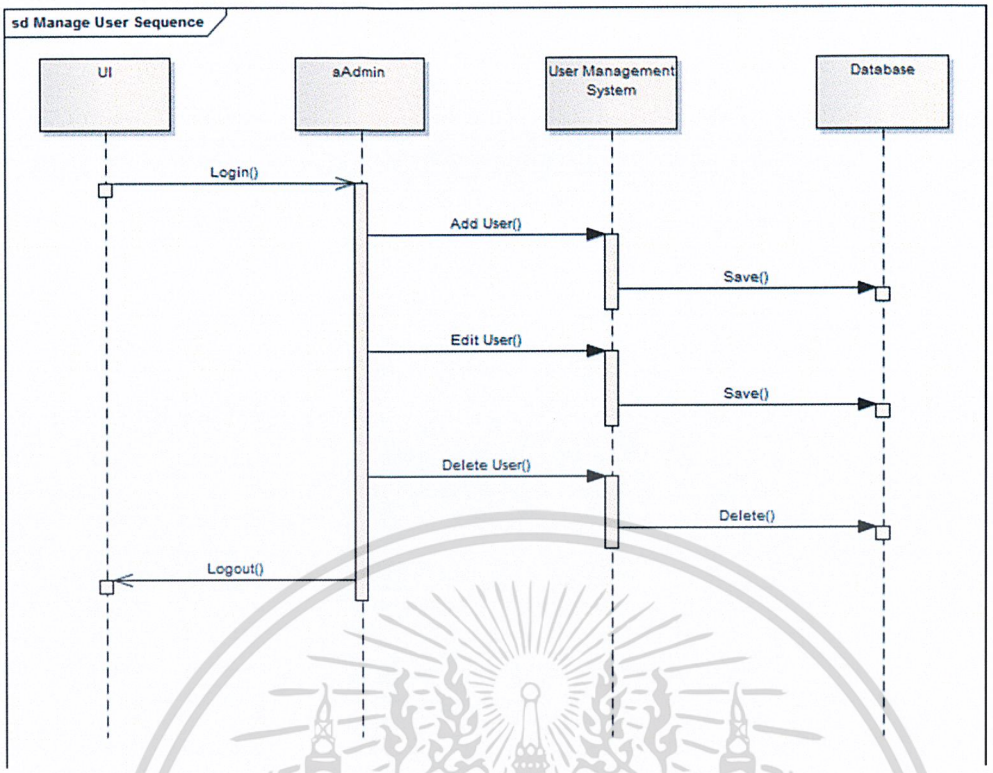
แล้วหรือไม่ ซึ่งถ้าเคยสแกนมาก่อนแล้วก็จะสามารถเรียกดูข้อมูลของการสแกนก่อนหน้าได้ โดยผู้ใช้สามารถพิมพ์รายงานการสแกนดังกล่าวออกมาในรูปแบบต่าง ๆ ได้ เมื่อไม่ต้องการใช้ระบบแล้วจึงทำการออกจากระบบ ดังแสดงในรูปที่ 3.6



รูปที่ 3.6 ซีเควนซ์ไดอะแกรมของการออกรายงาน

ในส่วนการจัดการผู้ใช้งาน ดังแสดงในรูปที่ 3.7 นั้นต้องเป็นผู้ใช้งานในระดับผู้ดูแลระบบเท่านั้น จึงจะสามารถจัดการกับผู้ใช้งานได้ โดยที่ผู้ดูแลระบบสามารถจัดการผู้ใช้งานได้ 3 แบบ คือ

1. AddUser() เมื่อผู้ดูแลระบบต้องการเพิ่มผู้ใช้งาน คลาส Admin จะทำการส่งรายละเอียดของการเพิ่มผู้ใช้งานไปยังโมดูล User Management System หลังจากนั้นจะทำการเพิ่มผู้ใช้งานลงบนฐานข้อมูล
2. EditUser() เมื่อผู้ดูแลระบบต้องการแก้ไขข้อมูลผู้ใช้งานที่มีอยู่ในระบบ คลาส Admin จะทำการส่งรายละเอียดของการแก้ไขผู้ใช้งานไปยังโมดูล User Management System หลังจากนั้นจะทำการแก้ไขข้อมูลของผู้ใช้งาน แล้วบันทึกไปยังฐานข้อมูล
3. DeleteUser() เมื่อผู้ดูแลระบบต้องการลบผู้ใช้งานที่มีอยู่ออกจากระบบ คลาส Admin จะทำการส่งรายละเอียดของการลบผู้ใช้งานไปยังโมดูล User Management System หลังจากนั้นจะทำการลบผู้ใช้นี้ออกจากฐานข้อมูล

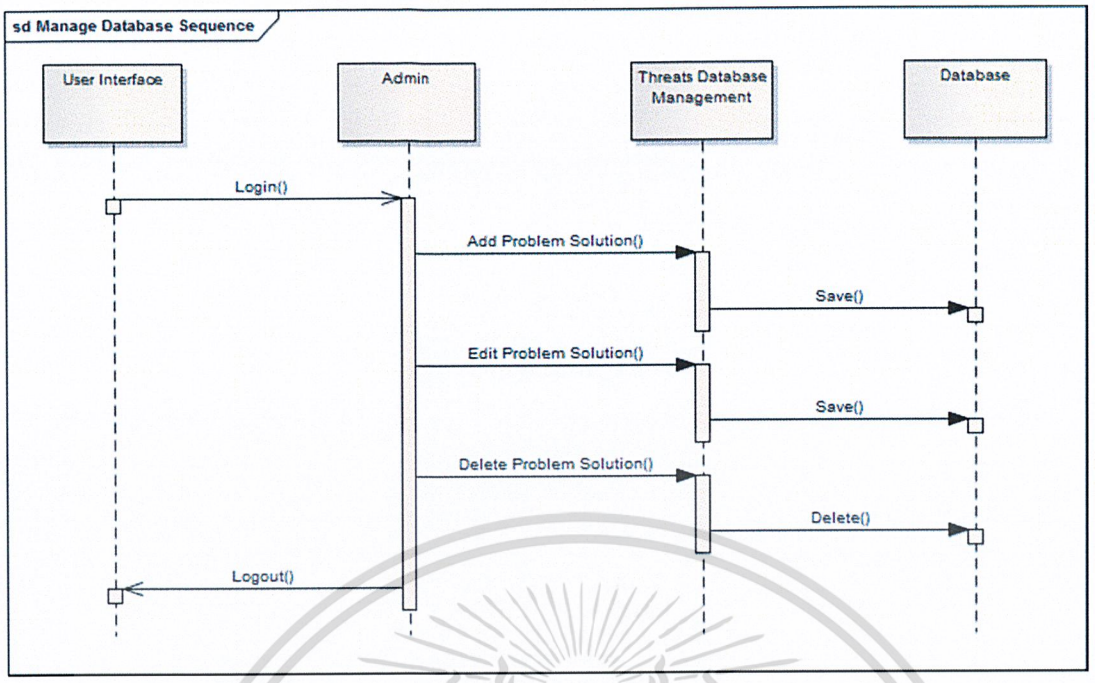


รูปที่ 3.7 ซีเควนซ์ไดอะแกรมของการจัดการผู้ใช้งาน

ในการจัดการฐานข้อมูลช่องโหว่ เริ่มต้นจากการล๊อกอินเป็นผู้ดูแลระบบ จากนั้นผู้ดูแลระบบจะสามารถจัดการฐานข้อมูลช่องโหว่ได้ โดยจะแบ่งออกเป็น 3 ส่วน คือ

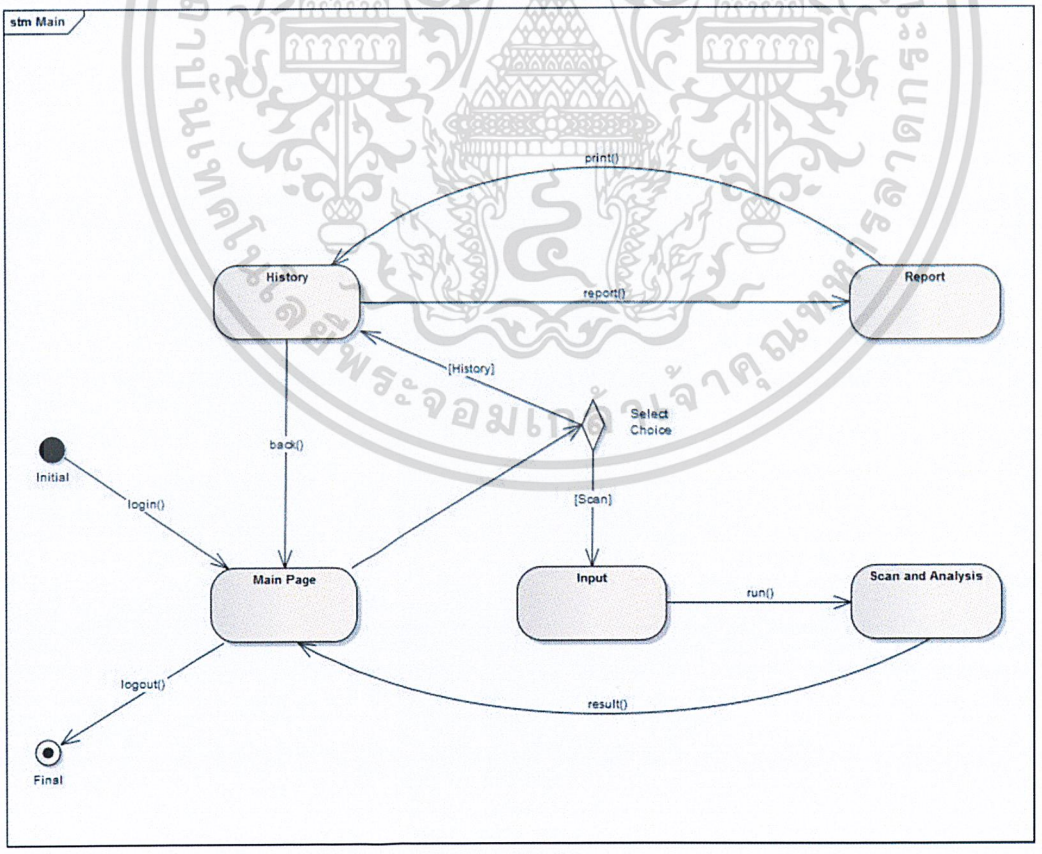
1. Add Problem Solution() เมื่อต้องการเพิ่มข้อมูลช่องโหว่เข้าสู่ระบบ คลาส Admin จะทำการส่งรายละเอียดของการเพิ่มข้อมูลช่องโหว่ ไปยังโมดูล Threats Database Management หลังจากนั้นจะส่งข้อมูลไปบันทึกลงบนฐานข้อมูล
2. Edit Problem Solution() เมื่อต้องการแก้ไขข้อมูลช่องโหว่ที่มีอยู่ในระบบ คลาส Admin จะทำการส่งรายละเอียดของการแก้ไขข้อมูลช่องโหว่ ไปยังโมดูล Threats Database Management หลังจากนั้นจะส่งข้อมูลการแก้ไขนี้ไปปรับปรุงที่ฐานข้อมูล
3. Delete Problem Solution() เมื่อต้องการลบข้อมูลช่องโหว่ออกจากระบบ คลาส Admin จะทำการส่งรายละเอียดของการลบข้อมูลช่องโหว่ไปยังโมดูล Threats Database Management หลังจากนั้นระบบจะทำการลบข้อมูลนี้ออกจากฐานข้อมูล

และเมื่อผู้ดูแลระบบจัดการกับฐานข้อมูลช่องโหว่เสร็จเรียบร้อยแล้ว ก็จะทำการออกจากระบบ ดังรูปที่ 3.8



รูปที่ 3.8 ซีเควนซ์ไดอะแกรมของการจัดการฐานข้อมูลช่องโหว่

3.5 สเตทไดอะแกรม (State Diagram)



รูปที่ 3.9 สเตทไดอะแกรมของระบบ

การทำงานเริ่มจาก ค่าเริ่มต้นแล้ว Login เข้าสู่ระบบ มาที่หน้าหลัก (Main page) ซึ่งสามารถแสดงรายละเอียดของขั้นตอนต่าง ๆ ได้ในตารางที่ 3.12

ตารางที่ 3.12 รายละเอียดของสเตทไดอะแกรม

State	Operation	Next State	Description
Main Page	Scan	Input	ต้องการสแกนเครื่องใหม่
	History	History	ต้องการเลือกเครื่องที่เคยสแกนแล้ว
	Logout	Final (End)	ออกจากระบบ
Input	run	Scan and Analysis	ทำการทำงานใส่ค่าพารามิเตอร์
History	report	Report	ต้องการออกรายงาน
Scan and Analysis	result	Main page	แสดงผลการสแกนแล้วกลับสู่หน้าหลัก
Report	Generator	History	สร้างรายงานออกมาแล้วกลับไปสู่หน้าแสดงผลเครื่อง

บทที่ 4

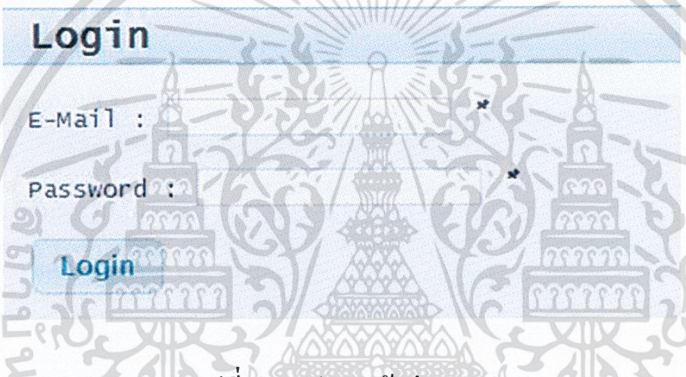
การทดลองและผลการทดลอง

4.1 การทำงานส่วนของผู้ใช้งาน

ผู้ใช้งานที่มีชื่อผู้ใช้และรหัสผ่านแล้ว สามารถที่จะเข้ามาใช้ในระบบการตรวจสอบช่องโหว่ได้ เข้ามาที่เครื่องที่ได้ติดตั้งระบบไว้ โดยผ่านทางเว็บเบราว์เซอร์ของผู้ใช้งาน

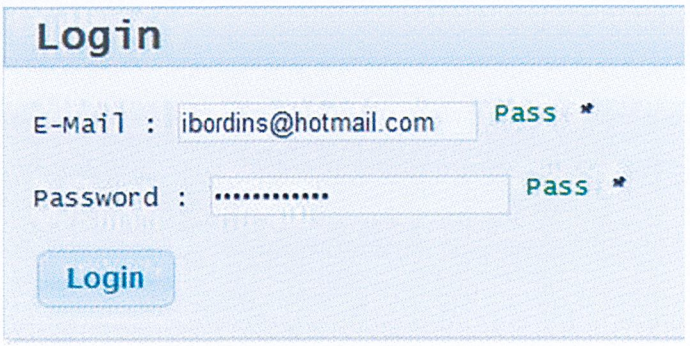
4.1.1 การเข้าสู่ระบบ (Login)

เมื่อผู้ใช้งานเข้ามาที่หน้าแรกของระบบผ่านเว็บเบราว์เซอร์แล้ว ผู้ใช้งานจะพบกับหน้าล๊อกอินที่ให้กรอกชื่อผู้ใช้และรหัสผ่าน ดังรูปที่ 4.1



รูปที่ 4.1 รูปการเข้าสู่ระบบ

หลังจากนั้นผู้ใช้ระบบกรอกชื่อผู้ใช้และรหัสผ่าน ตามที่ระบุไว้ในระบบว่าอีเมลและรหัสผ่าน ระบบจะตรวจสอบทันทีว่าที่อีเมลที่กรอกเป็นอีเมลที่ถูกต้องตามหลักการเขียนหรือไม่ และรหัสผ่านเกินแปดตัวอักษรตามที่ระบบกำหนดไว้หรือไม่ ซึ่งถ้าถูกต้องจะปรากฏตัวหนังสือผ่านสีเขียว ดังรูปที่ 4.2

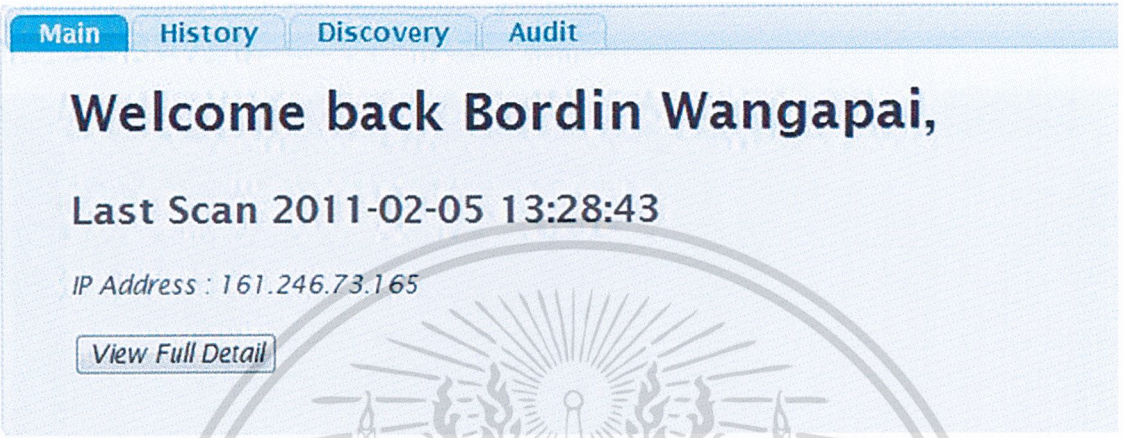


รูปที่ 4.2 รูปกรอกข้อมูลเพื่อเข้าสู่ระบบ

เมื่อผู้ใช้ทำการยืนยันการล๊อกอินด้วยการกดปุ่มล๊อกอินแล้ว ข้อมูลจะถูกส่งไปตรวจสอบกับฐานข้อมูลว่ามีข้อมูลของผู้ใช้อยู่ในระบบจริงหรือไม่ ถ้าพบข้อมูลในฐานข้อมูล ระบบก็จะอนุญาตให้ผู้ใช้สามารถผ่านเข้าไปที่หน้าเว็บหลักได้

4.1.2 การใช้งานระบบ

เมื่อผู้ใช้งานเข้าสู่ระบบแล้ว จะเข้าสู่หน้าหลักหน้าของระบบ ดังรูปที่ 4.3



รูปที่ 4.3 รูปหน้าหลักเข้าสู่ระบบ

ระบบจะแสดงชื่อผู้ใช้ รวมถึงข้อมูลของผู้ใช้ในครั้งล่าสุด โดยที่ผู้ใช้สามารถเรียกดูรายละเอียดครั้งล่าสุดที่ได้ทำการใช้งานระบบเพื่อตรวจสอบเครื่องล่าสุดได้ หลังจากนั้นผู้ใช้จะสังเกตเห็นมีเมนูให้เปลี่ยนหน้าด้านบนของหน้า

Main คือ หน้าหลักของระบบ

History คือ การดูรายละเอียดเครื่องที่ได้ทำการตรวจสอบแล้ว

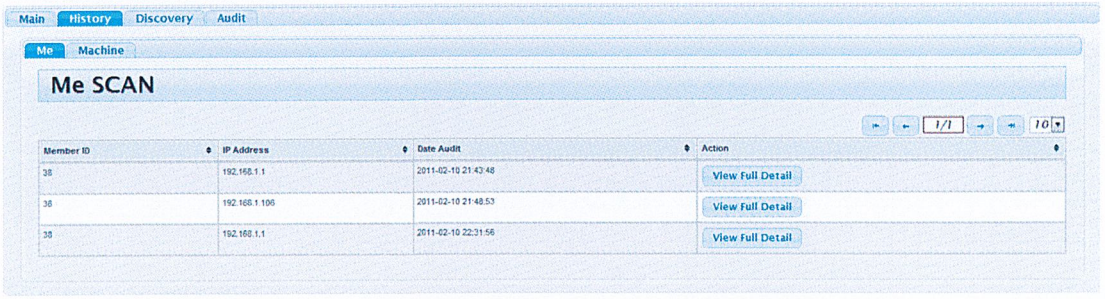
Discovery คือ การค้นหาข้อมูลของเครื่องที่ตรวจสอบเบื้องต้น

Audit คือ การตรวจสอบเครื่องว่ามีช่องโหว่ใดบ้างในเครื่องนั้น

ผู้ใช้สามารถกดปุ่ม View Full Detail เพื่อดูรายละเอียดของการตรวจสอบครั้งล่าสุดได้

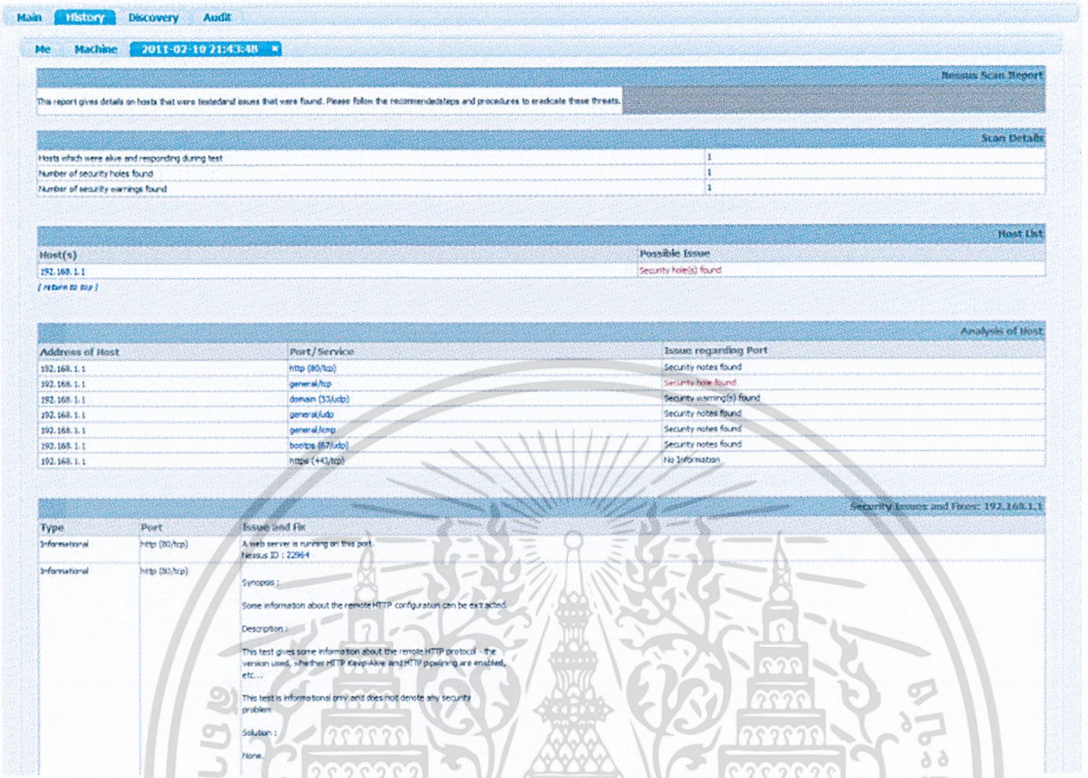
1) การดูรายละเอียดเครื่องที่ตรวจสอบแล้ว (History)

เมื่อเลือกเมนูด้านบนเพื่อดูรายละเอียดของเครื่องที่ได้ทำการตรวจสอบแล้ว จะปรากฏรายละเอียดของเครื่องที่ผู้ใช้งานคนนั้นได้ตรวจสอบไว้ก่อนหน้านี้ ดังรูปที่ 4.4



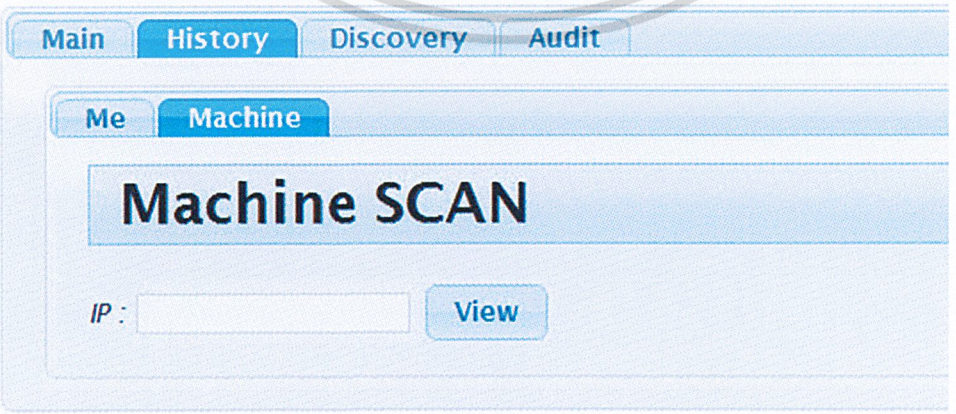
รูปที่ 4.4 รูปดูรายละเอียดเครื่องที่ตรวจสอบแล้วอ้างอิงจากผู้ใช้งาน

เมื่อผู้ใช้งานต้องการดูรายละเอียดของการตรวจสอบครั้งนั้นให้ ผู้ใช้งานกด ดูรายละเอียดทั้งหมด ของผู้ใช้งานจะได้ผล ดังรูปที่ 4.5



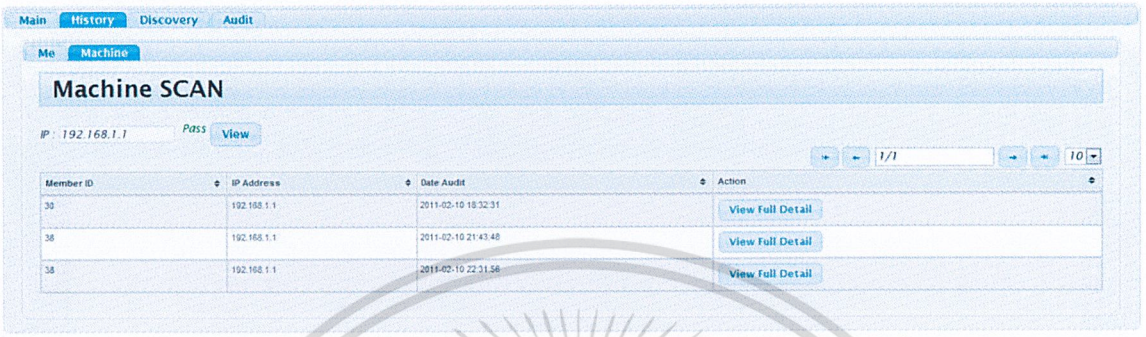
รูปที่ 4.5 การดูรายละเอียดทั้งหมดของเครื่องที่เคยตรวจสอบแล้ว

เมื่อผู้ใช้ต้องการทราบเครื่องที่เคยตรวจสอบโดยที่ผู้ใช้รู้ ไอพีของเครื่องแล้ว ให้ผู้ใช้เลือกเมนูรองลงมาเป็น Machine เมื่อผู้ใช้งานระบบเลือกเพื่อจะดูผ่านไอพีของเครื่องแล้ว จะปรากฏหน้าดังรูปที่ 4.6



รูปที่ 4.6 การดูรายละเอียดผ่านไอพีของเครื่อง

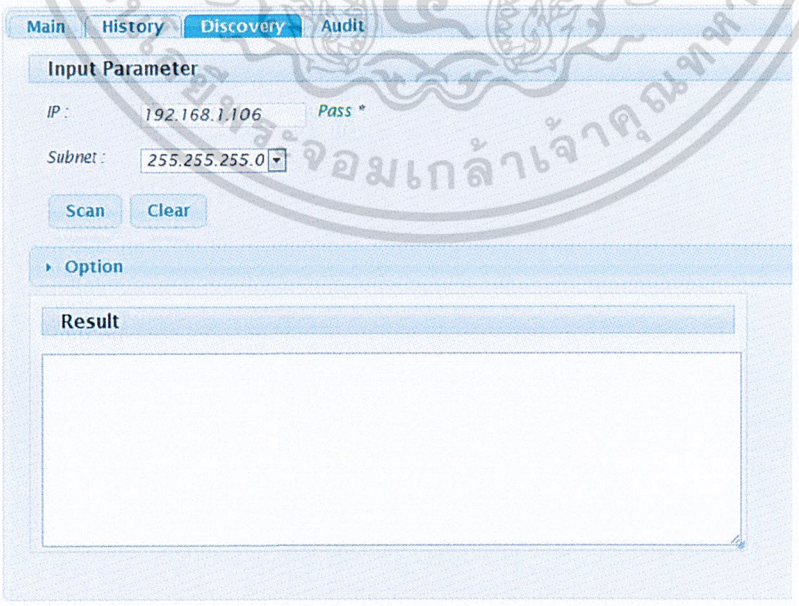
หลังจากนั้นผู้ใช้งานระบบ กรอกไอพีของเครื่องที่ต้องการดูรายละเอียด หลังจากผู้ใช้ได้กรอกไอพีของเครื่องเรียบร้อยแล้ว ผู้ใช้จึงกดปุ่มดูรายละเอียด เพื่อที่ต้องการแสดงเครื่องว่าถูกตรวจสอบไปทั้งหมดกี่ครั้งและ เพื่อดูรายละเอียดทั้งหมดได้ของเครื่องนั้นโดยที่ผู้ใช้คนนี้อาจไม่ใช่คนที่ตรวจสอบเองได้ ดังรูปที่ 4.7



รูปที่ 4.7 การดูรายละเอียดของเครื่องผ่านไอพีที่ได้กรอกแล้ว

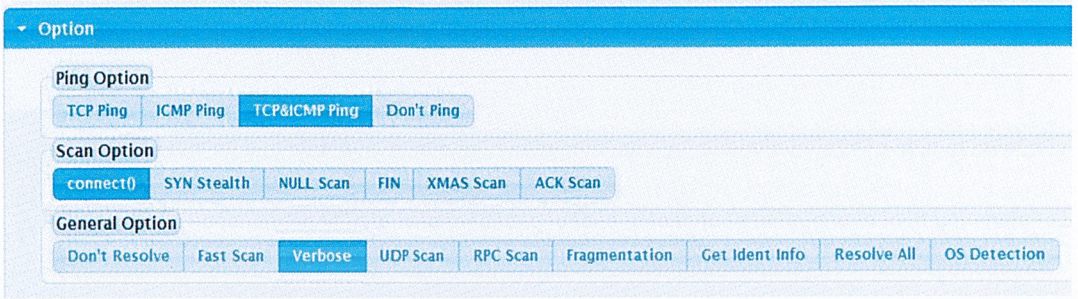
2) การสแกนข้อมูลของเป้าหมายเบื้องต้น (Discovery)

การสแกนข้อมูลเบื้องต้นของเป้าหมาย จะเป็นการสแกนที่เน้นไปที่การสแกนพอร์ตของเครื่องเป้าหมายเป็นหลัก โดยเมื่อเข้าสู่เมนู Discovery หลังจากนั้นให้กรอกไอพีของเครื่องที่ต้องการสแกน ระบบจะตรวจสอบว่าค่าพารามิเตอร์ที่รับมาเป็นไอพีแอดเดรสที่ถูกต้องหรือไม่ เมื่อตรวจสอบว่าเป็นไอพีแอดเดรสที่ถูกต้องจะปรากฏตัวหนังสือสีเขียว ดังรูปที่ 4.8



รูปที่ 4.8 การกรอกไอพีของการสแกนเป้าหมายเบื้องต้น

หลังจากนั้นสามารถเลือกตัวเลือกการค้นหาข้อมูลเบื้องต้นได้ดังรูปโดย เลือกไปที่ตัวเลือก จะปรากฏตัวเลือกการค้นหาข้อมูลและวิธีการค้นหาข้อมูล ดังรูปที่ 4.9



รูปที่ 4.9 การเลือกตัวเลือกในการสแกนเป้าหมายเบื้องต้น

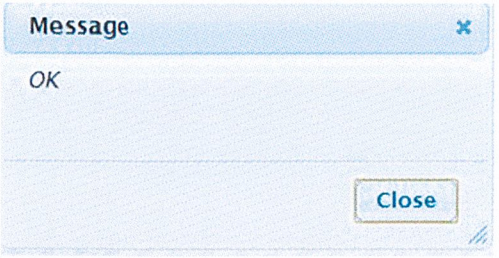
ในส่วนของตัวเลือก (Option) ของการสแกนนั้น จะแบ่งออกเป็น 3 หมวดใหญ่ คือ

- Ping Option เป็นการเลือกวิธีที่จะใช้ในการติดต่อกับเครื่องเป้าหมาย
- Scan Option เป็นการเลือกวิธีที่จะใช้ในการสแกนพอร์ตกับเครื่องเป้าหมาย
- General Option เป็นตัวเลือกเสริมในการสแกน

Ping Option และ Scan Option เลือกได้หนึ่งรูปแบบของแต่ละตัวเลือก ส่วน General Option นั้นสามารถเลือกได้มากกว่าหนึ่งรูปแบบ โดยตัวเลือกแต่ละแบบมีความหมายดังนี้

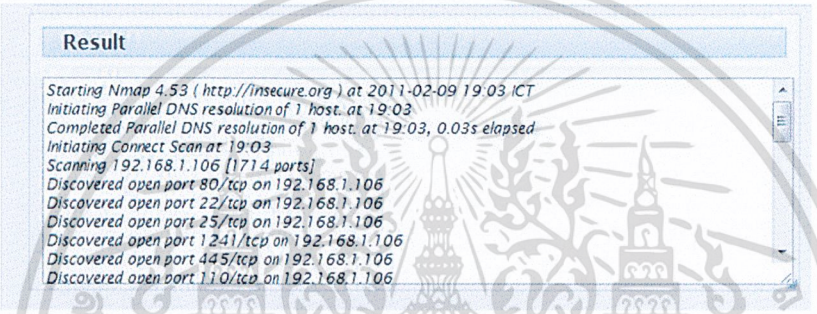
1. Don't Resolve : ไม่บอกรายละเอียดของพอร์ต
2. Fast Scan : เป็นการสแกนแบบรวดเร็ว ในกรณีที่ต้องการทราบแค่เครื่องนั้นได้ทำการใช้งานพอร์ตใดบ้างและเปิดการทำงานเซอร์วิสอะไรอยู่ในพอร์ตนั้น ๆ
3. Verbose : เป็นการสแกนโดยใช้หลาย ๆ เวอร์โบซิตี้ (Verbosity)
4. UDP Scan : เป็นการสแกนโดยการส่งแพกเกตยูดีพี
5. RPC Scan : เป็นการสแกนโดยการส่งแพกเกตอาร์พีซี (Remote Procedure Call: RPC)
6. Fragmentation : เป็นการสแกนแบบแบ่งเป็นส่วน ๆ ของพอร์ตนั้น
7. Get Ident Info : เป็นตัวเลือกในการสแกนเมื่อต้องการรายละเอียดที่ละเอียดขึ้น
8. Resolve All : เป็นตัวเลือกในการสแกนเมื่อต้องการรายละเอียดทั้งหมด
9. OS Detection : เป็นการสแกนเพื่อตรวจสอบว่าเครื่องเป้าหมายใช้ระบบปฏิบัติการใด

เมื่อผู้ใช้ยืนยันการสแกนด้วยการกด Scan คำสั่งของผู้ใช้จะถูกส่งไปยังโปรแกรมเอ็นแมป เอ็นแมปจะทำการสแกนจะส่งผลกลับมายังระบบ และบันทึกผลการสแกนในครั้งนี้ไปยังฐานข้อมูล เพื่อนำไปเป็นประวัติการสแกนของผู้ใช้ดังรูปที่ 4.10



รูปที่ 4.10 แสดงการค้นหาข้อมูลเบื้องต้นเสร็จเรียบร้อย

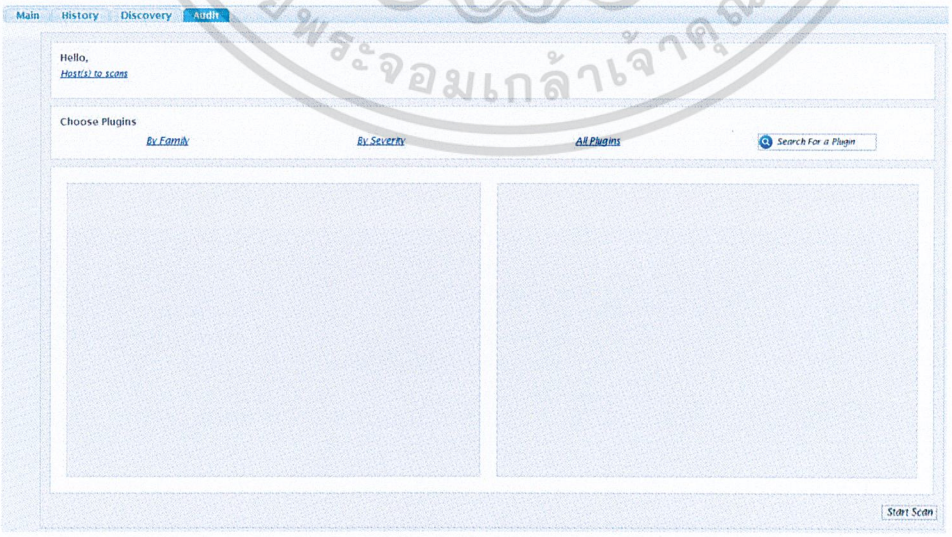
หลังจากที่ได้ทำการสแกนและบันทึกผลการสแกนลงในฐานข้อมูลแล้ว ผลลัพธ์ดังกล่าวจะแสดงผลให้ผู้ใช้ได้ทราบถึงรายละเอียดของการสแกน ดังรูปที่ 4.11 โดยผู้ใช้สามารถขยายกล่องผลลัพธ์นี้ได้โดยการคลิกเมาส์ลากที่มุมขวาล่างของกล่องผลลัพธ์



รูปที่ 4.11 แสดงผลลัพธ์หลังจากการค้นหาข้อมูลเบื้องต้น

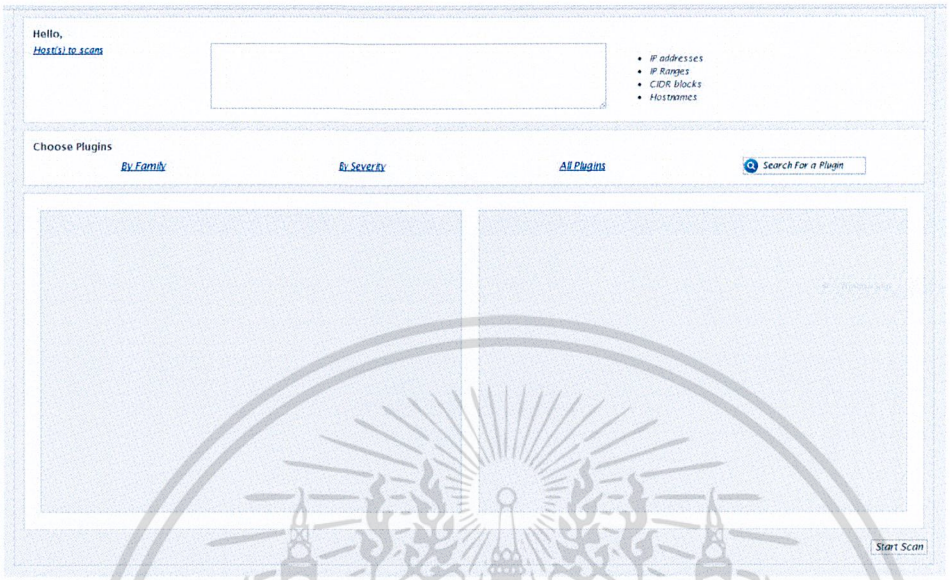
3) การตรวจสอบช่องโหว่ของเครื่องเป้าหมาย (Audit)

การตรวจสอบช่องโหว่ของเครื่องเป้าหมาย จะเป็นการตรวจสอบช่องโหว่ของเครื่องเป้าหมายอย่างละเอียด ว่าเครื่องเป้าหมายนั้นมีช่องโหว่อะไรบ้าง รวมทั้งยังสามารถแสดงวิธีการแก้ไขปัญหาของช่องโหว่นั้น ๆ ได้อีกด้วย เมื่อเข้าสู่เมนู Audit จะพบกับหน้าดังรูปที่ 4.12



รูปที่ 4.12 หน้าต่างเพื่อเตรียมการตรวจสอบช่องโหว่

หลังจากที่เข้ามาสู่หน้าต่างเพื่อตรวจสอบช่องโหว่แล้ว ผู้ใช้งานสามารถระบุเครื่องเป้าหมายที่ต้องการตรวจสอบช่องโหว่ได้โดยระบุไอพีแอดเดรสหรือชื่อโฮสต์ได้ โดยการเลือกที่ Hosts to Scans หลังจากนั้นจะขึ้นกล่องข้อความให้ป้อนค่า ดังรูปที่ 4.13



รูปที่ 4.13 หน้าต่างกรอกไอพีในการตรวจสอบช่องโหว่

หลังจากนั้นกรอกไอพีของเครื่องที่ต้องการตรวจสอบแล้ว ผู้ใช้ยังสามารถเลือกปลั๊กอินในการตรวจสอบได้อีกด้วย โดยจะแบ่งออกเป็น 3 หมวดหมู่ ดังนี้

- By Family : แบ่งตามหมวดหมู่
- By Severity : แบ่งตามประเภทการโจมตี
- All Plugins : เลือกทุกปลั๊กอินในการตรวจสอบ

ปลั๊กอินตามหมวดหมู่ (By Family) จะแบ่งออกเป็น 43 หมวดหมู่ดังนี้

1. AIX Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอล (Local) ของระบบปฏิบัติการเอไอเอ็กซ์ (AIX - Advanced Interactive eXecutive)
2. Backdoors เป็นการตรวจสอบว่ามีการติดตั้งแบ็กดอร์อยู่ในระบบหรือไม่
3. CentOS Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการเซนร์โอเอส (CentOS - Community Enterprise Operating System)
4. CGI abuses เป็นการหาช่องโหว่ของซีจีไอ (CGI - Common Gateway Interface)
5. CGI abuses XSS เป็นการหาช่องโหว่ของซีจีไอ (CGI) ด้วยวิธี Cross-site Scripting (XSS)
6. CISCO เป็นการหาช่องโหว่ของอุปกรณ์ซิสโก้
7. Databases เป็นการหาช่องโหว่ของระบบจัดการฐานข้อมูล

8. Debian Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอล (Local) ของระบบปฏิบัติการดีเบียน (Debian)
9. Default Unix Accounts เป็นการหาช่องโหว่ทางบัญชีผู้ใช้เริ่มต้นของระบบยูนิกซ์
10. Denial of Service เป็นการหาช่องโหว่โดยทำการโจมตีเพื่อปิดการให้บริการ
11. Fedora Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอล (Local) ของระบบปฏิบัติการ Fedora
12. Finger abuses เป็นการหาช่องโหว่ของคำสั่งฟิงเกอร์ (Finger)
13. Firewalls เป็นการหาช่องโหว่ของไฟร์วอลล์
14. FreeBSD Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการ FreeBSD
15. FTP เป็นการหาช่องโหว่ของโปรโตคอลเอฟทีพี (FTP – File Transfer Protocol)
16. Gain a shell remotely เป็นการหาช่องโหว่จากการรีโมทเชลล์
17. Gain root remotely เป็นการหาช่องโหว่จากสิทธิ์ของรูทในการรีโมท
18. General เป็นปลั๊กอินทั่ว ๆ ไป
19. Gentoo Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการ Gentoo
20. HP-UX Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการ HP-UX
21. MacOS X Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการ MacOS X
22. Mandrake Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการ Mandrake
23. Misc. เป็นปลั๊กอินที่ไม่เข้าพวกใด ๆ
24. Netware เป็นการหาช่องโหว่ทางระบบเครือข่ายของเน็ตแวร์
25. NIS เป็นการหาช่องโหว่ทางระบบการตรวจจับการบุกรุกเกี่ยวกับพอร์ตที่อนุญาต
26. Peer-To-Peer File Sharing เป็นการหาช่องโหว่ที่เกิดจากโปรแกรมจำพวกเพียร์ทูเพียร์ (P2P - Peer To Peer)
27. Port scanners เป็นปลั๊กอินที่ใช้วิธีการสแกนพอร์ตเป็นหลัก
28. Red Hat Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการ RedHat
29. Remote file access เป็นการตรวจสอบช่องโหว่การเข้าถึงไฟล์จากระยะไกล
30. RPC เป็นการตรวจสอบช่องโหว่ของอาร์พีซี (RPC - Remote Procedure Call)

31. Service detection เป็นการตรวจจับเซอร์วิสที่เปิดให้บริการอยู่บนเครื่องเป้าหมาย
32. Settings เป็นการตรวจสอบการที่ตั้งค่าที่อาจะทำให้เกิดช่องโหว่
33. Slackware Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของ Slackware
34. SMTP problems เป็นการตรวจสอบช่องโหว่ที่เกิดจากโปรโตคอลเอสเอ็มทีพี (SMTP – Simple Mail Transfer Protocol)
35. SNMP เป็นการตรวจสอบช่องโหว่ของเอสเอ็มทีพี (SMTP – Simple Mail Transfer Protocol) รวมทั้งการตั้งค่าบัญชีผู้ใช้งาน
36. Solaris Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการ Solaris
37. SuSE Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการ SuSE
38. Ubuntu Local Security Checks เป็นการตรวจสอบความปลอดภัยแบบโลคอลของระบบปฏิบัติการ Ubuntu
39. Useless services เป็นการตรวจสอบการเปิดเซอร์วิสที่ไม่มีความจำเป็น
40. Web Servers เป็นการตรวจสอบช่องโหว่จากการตั้งค่าเว็บเซิร์ฟเวอร์
41. Windows เป็นการตรวจสอบช่องโหว่เฉพาะของวินโดว์ส
42. Windows : Microsoft Bulletins เป็นการตรวจสอบการลงซอฟต์แวร์แก้ไขข้อบกพร่อง (Patch) ของวินโดวส์
43. Windows : User management เป็นการตรวจสอบการตั้งค่าการจัดการชื่อผู้ใช้งานของวินโดวส์

ปลั๊กอินตามประเภทการโจมตี (By Severity) แบ่งออกเป็น 11 ประเภท ดังนี้

1. Attack เป็นปลั๊กอินที่มีการจำลองการโจมตีไปยังเครื่องเป้าหมาย
2. Denial เป็นปลั๊กอินที่มีการจำลองการทำเกิดการปฏิเสธการให้บริการ (DoS - Denial of Service) ไปยังเครื่องเป้าหมาย
3. Destructive Attack เป็นปลั๊กอินที่อาจสร้างความเสียหายกับเครื่องเป้าหมาย
4. End เป็นปลั๊กอินที่ทำให้เครื่องเป้าหมายหยุดการให้บริการ
5. Flood เป็นปลั๊กอินที่มีการส่งแพกเกตข้อมูลจำนวนมาก
6. Infos เป็นปลั๊กอินที่มีการเก็บข้อมูลจากเครื่องเป้าหมาย
7. Init เป็นปลั๊กอินที่มีการเก็บข้อมูลเพื่อเป็นประโยชน์ต่อปลั๊กอินถัดไป
8. Kill_host เป็นปลั๊กอินที่มีการทำให้เครื่องเป้าหมายหยุดการทำงาน
9. Mixed เป็นปลั๊กอินที่มีการผสมผสานการโจมตีแบบต่าง ๆ เข้าด้วยกัน

10. Scanner เป็นปลั๊กอินที่มีการเปลี่ยนการสแกนเป็นแบบต่าง ๆ

11. Setting เป็นปลั๊กอินที่มีการพยายามอ่านการตั้งค่าของบริการต่าง ๆ

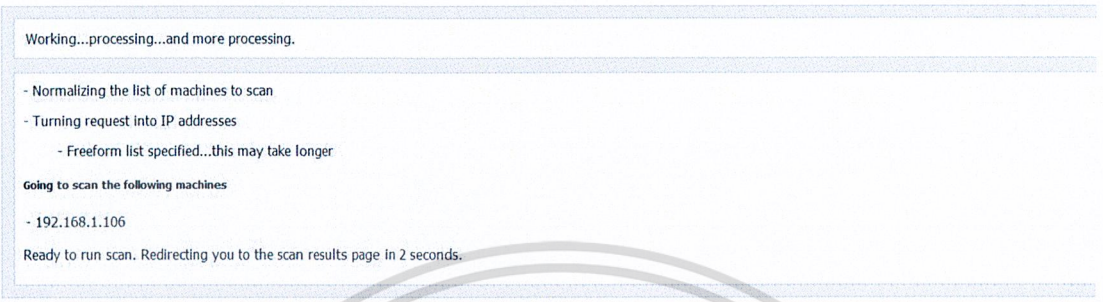
ปลั๊กอินทั้งหมด (All Plugins) เป็นการใช้ปลั๊กอินทั้งหมดที่มีอยู่ในระบบ ในการตรวจสอบช่องโหว่ของเครื่องเป้าหมาย ซึ่งในการเลือกใช้ทุกปลั๊กอินเช่นนี้ จะทำให้การตรวจสอบช่องโหว่ใช้เวลาเพิ่มขึ้น

เมื่อเลือกปลั๊กอินที่ต้องการตรวจสอบเครื่องเป้าหมายได้แล้ว ให้กดเลือกปลั๊กอิน ยกตัวอย่างเช่น เลือกปลั๊กอินเว็บเซิร์ฟเวอร์ดังรูปที่ 4.14 ถ้าผู้ใช้ต้องการตรวจสอบเป้าหมายด้วยปลั๊กอินหลาย ๆ ตัว สามารถเลือกเพิ่มเติมได้

รูปที่ 4.14 เลือกปลั๊กอินเว็บเซิร์ฟเวอร์ในการตรวจสอบช่องโหว่

รูปที่ 4.15 เลือกปลั๊กอินยูสเลสเซอร์วิสเป็นปลั๊กอินที่สอง

เมื่อผู้ใช้เลือกปลั๊กอินและต้องการที่จะตรวจสอบช่องโหว่ของเครื่องเป้าหมายแล้ว ให้กด Start Scan ที่มุมขวาของหน้าจอ คำสั่งการตรวจสอบช่องโหว่จะถูกส่งไปยังเนสซัสเซิร์ฟเวอร์ให้ทำการวิเคราะห์ช่องโหว่ของเป้าหมาย ซึ่งระหว่างการรอการตรวจสอบช่องโหว่จากเนสซัสเซิร์ฟเวอร์นั้น จะแสดงดังรูปที่ 4.16



รูปที่ 4.16 หน้าต่างรอการตรวจสอบช่องโหว่

คำสั่งการตรวจสอบช่องโหว่จากผู้ใช้ผ่านเว็บเบราว์เซอร์จะถูกส่งต่อไปยังเนสซัสเซิร์ฟเวอร์ เพื่อทำการตรวจสอบเป้าหมายว่าเครื่องเป้าหมายมีช่องโหว่อะไรบ้าง เมื่อเนสซัสเซิร์ฟเวอร์ค้นพบช่องโหว่ของเป้าหมายแล้ว ก็จะทำการรวบรวมข้อมูลช่องโหว่และวิธีแก้ไขทั้งหมดของเป้าหมายนั้น ๆ ส่งกลับมายังหน้าเว็บเบราว์เซอร์ให้แก่ผู้ใช้ รวมทั้งบันทึกข้อมูลเหล่านี้ลงฐานข้อมูลของระบบ เพื่อเป็นประวัติการตรวจสอบของผู้ใช้และเครื่องเป้าหมายนี้ต่อไป ดังรูปที่ 4.17 เน้นการการแสดงผลการตรวจสอบช่องโหว่ทั้งหมด

4) อธิบายผลที่ได้จากการตรวจสอบช่องโหว่

จากรูปที่ 4.17 สามารถอธิบายผลที่ได้จากการตรวจสอบช่องโหว่ของเป้าหมาย มีรายละเอียดดังนี้

1. รายงานการตรวจสอบของเนสซัส (Nessus Scan Report)
2. รายละเอียดการตรวจสอบ (Scan Detail)
   2.1. จำนวนโฮสที่ตรวจสอบ (Hosts which were alive and responding during test)
   2.2. จำนวนช่องโหว่ทั้งหมด (Number of security holes found)
   2.3. เตือนว่ามีโอกาสเป็นช่องโหว่จำนวนเท่าไหร่ (Number of security warnings found)
3. โฮสลิสต์ (Host List) บอกเครื่องที่ถูกตรวจสอบ และบอกว่าค้นพบอะไรบ้าง
4. รายการที่ตรวจพบว่าเปิดอยู่และมีการใช้งานแล้วมีการวิเคราะห์แล้วได้ผลว่า โฮสต์ไหนเปิดพอร์ตไหนและมีปัญหาหรือไม่มีอย่างไรบ้างของพอร์ตนั้น
5. อธิบายถึงรายละเอียดของและวิธีแก้ไขต่าง ๆ ชนิดของปัญหาและระดับของปัญหา ของปัญหาต่าง ๆ มากมาย (Security Issue and Fixes)

Nessus Scan Report

This report gives details on hosts that were testedand issues that were found. Please follow the recommendedsteps and procedures to eradicate these threats.

Scan Details

Hosts which were alive and responding during test	1
Number of security holes found	1
Number of security warnings found	1

Host List

Host(s)	Possible Issue
192.168.1.1	Security hole(s) found

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
192.168.1.1	http (80/tcp)	Security notes found
192.168.1.1	general/tcp	Security hole found
192.168.1.1	domain (53/udp)	Security warning(s) found
192.168.1.1	general/udp	Security notes found
192.168.1.1	general/icmp	Security notes found
192.168.1.1	bootps (67/udp)	Security notes found
192.168.1.1	https (443/tcp)	No Information

Security Issues and Fixes: 192.168.1.1

Type	Port	Issue and Fix
Informational	http (80/tcp)	A web server is running on this port. Nessus ID : 22964
Informational	http (80/tcp)	Synopsis : Some information about the remote HTTP configuration can be extracted. Description : This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem Solution : None. Risk factor : None Plugin output : Protocol version : HTTP/1.1 SSL : no Pipelining : no Keep-Alive : no Options allowed : (Not implemented) Headers : Server: Date: Thu, 10 Feb 2011 22:31:09 GMT WWW-Authenticate: Basic realm="Linksys WAG54G2" Content-Type: text/html Connection: close Nessus ID : 24260
Informational	http (80/tcp)	Synopsis : A web server is running on the remote host. Description : This plugin attempts to determine the type and the version of the remote web server. Risk factor : None Plugin output : The remote web server type is : Nessus ID : 10107
Vulnerability	general/tcp	Information about this scan : Nessus version : 3.2.1 Plugin feed version : 200805290058 Type of plugin feed : Release ERROR: Your plugin feed has not been updated since 2008/5/29 Performing a scan with an older plugin set will yeld out of date results and

รูปที่ 4.17 ผลที่ได้หลังจากการตรวจสอบช่องโหว่

บทที่ 5
บทวิจารณ์และสรุป

5.1 ผลที่ได้รับ

- มีระบบการตรวจสอบช่องโหว่ของเครือข่ายคอมพิวเตอร์ผ่านเว็บเบราว์เซอร์
- สามารถปรับปรุงสมรรถภาพเพื่อความปลอดภัยของข้อมูลโดยใช้ระบบนี้ได้
- สามารถใช้ระบบนี้ได้ถึงแม้ว่าจะไปเข้าระบบเครือข่ายที่ไหนก็ตาม
- คณะผู้จัดทำได้รับความรู้การทำเว็บโปรแกรมประยุกต์ และระบบรักษาความปลอดภัยทางคอมพิวเตอร์

5.2 ปัญหาที่พบ

- ผลการตรวจสอบช่องโหว่ของระบบอาจไม่ถูกต้องมากนัก ถ้าทำการตรวจสอบเป้าหมายที่อยู่ภายใต้ไฟร์วอลล์หรือแนต (Network Address Translation : NAT)
- หากมีการใช้งานระบบในจำนวนที่มากเกินไป อาจทำให้สแกนเนอร์เซิร์ฟเวอร์ไม่สามารถตอบสนองการร้องขอจากผู้ใช้ได้

5.3 แนวทางการแก้ไขปัญหา

- ใช้เทคนิคการหลีกเลี่ยงระบบตรวจจับการบุกรุก (IDS Evasion) ในการตรวจสอบช่องโหว่ของระบบ ซึ่งอาจทำให้สามารถตรวจสอบผ่านไฟร์วอลล์หรือแนตได้
- จำกัดจำนวนผู้ใช้งานสแกนเนอร์เซิร์ฟเวอร์ ไม่ให้มีการใช้งานมากจนเกินไป

5.4 แนวทางพัฒนาต่อ

- พัฒนาในการเขียนปลั๊กอินเพิ่มเติม รวมทั้งปรับปรุงปลั๊กอินที่มีอยู่เดิมให้มีประสิทธิภาพยิ่งขึ้น
- พัฒนาในการเก็บผลการตรวจสอบจากสแกนเนอร์เซิร์ฟเวอร์ให้ละเอียดยิ่งขึ้น
- พัฒนาในเรื่องของการรองรับจำนวนผู้ใช้งานระบบให้มากยิ่งขึ้น
- พัฒนาให้ออกรายงานได้หลายรูปแบบได้

บรรณานุกรม

[1] adobe developer connection.[ออนไลน์]. เข้าถึงได้จาก : http://www.adobe.com/devnet.html (วันที่ค้นข้อมูล : 15 ตุลาคม 2553).

[2] jquery.[ออนไลน์]. เข้าถึงได้จาก : http://jquery.com/ (วันที่ค้นข้อมูล : 15 ตุลาคม 2553).

[3] jquery-ui.[ออนไลน์]. เข้าถึงได้จาก : http://jquery-ui.com/ (วันที่ค้นข้อมูล : 15 ตุลาคม 2553).

[4] nmap security scanner.[ออนไลน์]. เข้าถึงได้จาก : http://nmap.org/ (วันที่ค้นข้อมูล : 15 ตุลาคม 2553).

[5] nessus.[ออนไลน์]. เข้าถึงได้จาก : http://www.nessus.org/ (วันที่ค้นข้อมูล : 18 ตุลาคม 2553).

[6] php manual. [ออนไลน์]. เข้าถึงได้จาก : http://php.net/manual/en/ (วันที่ค้นข้อมูล : 16 ตุลาคม 2553).

[7] w3schools.[ออนไลน์]. เข้าถึงได้จาก : http://www.w3schools.com/ (วันที่ค้นข้อมูล : 15 ตุลาคม 2553).

[8] wikipedia.[ออนไลน์]. เข้าถึงได้จาก : http://wikipedia.org/ (วันที่ค้นข้อมูล : 15 ตุลาคม 2553).

[9] ubuntu.[ออนไลน์]. เข้าถึงได้จาก : http://ubuntu.org/ (วันที่ค้นข้อมูล : 15 ตุลาคม 2553).

ภาคผนวก

ภาคผนวก ก.

คู่มือการติดตั้งอูบุนตูเซิร์ฟเวอร์รุ่น 8.04 (Ubuntu Server 8.04)

การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์

ดาวน์โหลดจาก : http://software.kmitl.ac.th/mirror/ubuntu_releases/8.04/

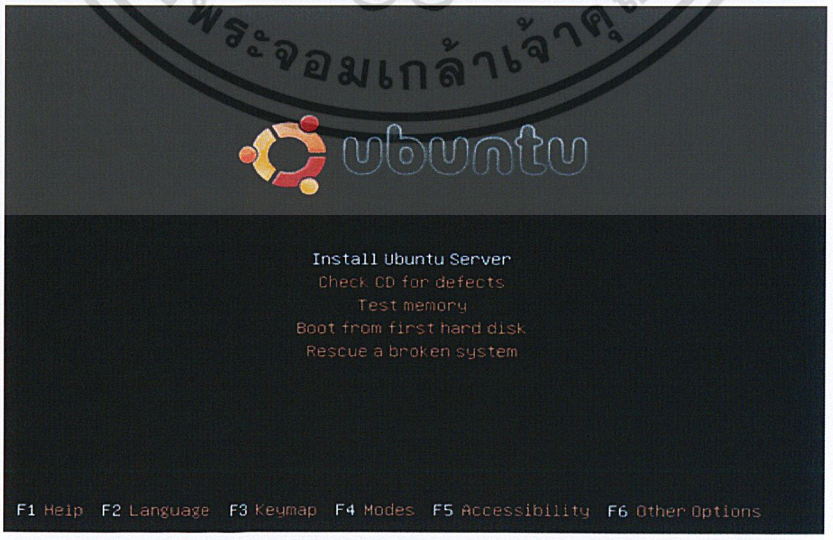
ชื่อไฟล์ : ubuntu-8.04.4-server-i386.iso รุ่น : LTS 8.04.4 แบบ : Intelx86

นำซีดีอิมเมจไฟล์ (CD Image File) ที่ดาวน์โหลดมาชื่อ ubuntu-8.04.4-server-i386.iso เขียนลงแผ่นซีดี (CD Disc) ก่อนนำมาติดตั้ง

1. ทำการติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ที่เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ โดยระบบจะให้เลือกภาษาที่จะใช้ในการติดตั้งดังรูปที่ ก.1 ในขั้นตอนนี้จะเลือกภาษาอังกฤษ

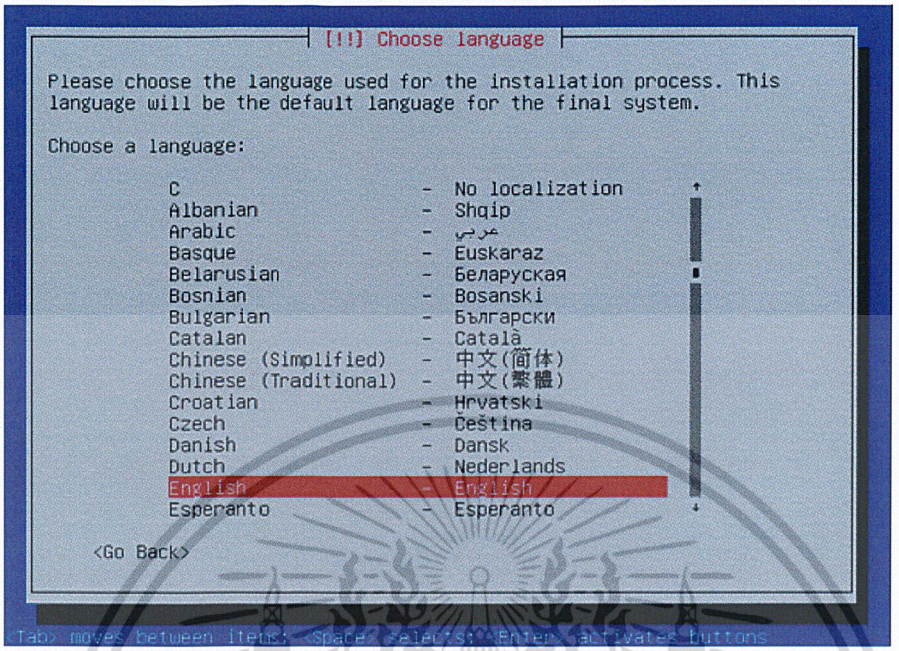
รูปที่ ก.1 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 1

2. หลังจากนั้นจะเข้าสู่หน้าหลักของการติดตั้ง ในขั้นตอนนี้จะเลือก Install Ubuntu Server ดังรูปที่ ก.2



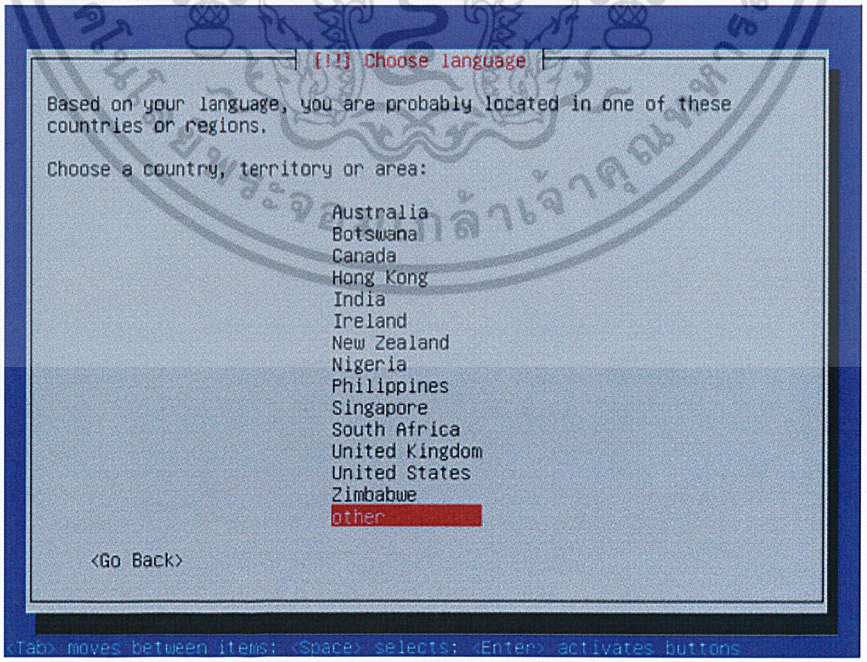
รูปที่ ก.2 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 2

3. ในขั้นตอนนี้ระบบจะให้เลือกภาษาที่ใช้ในการติดตั้งอูบุนตูเซิร์ฟเวอร์อีกครั้งดังรูปที่ ก.3



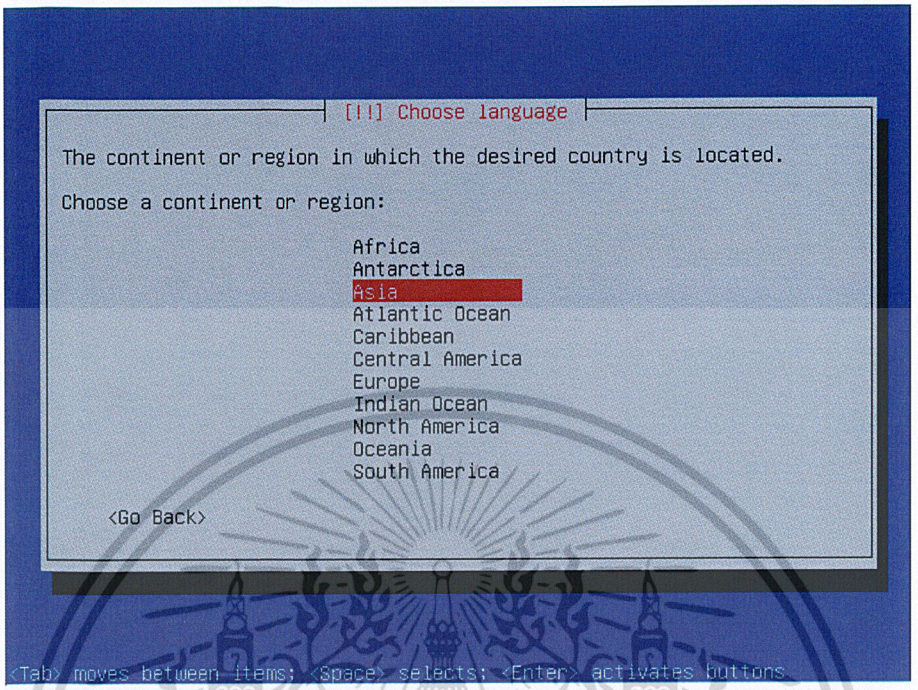
รูปที่ ก.3 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 3

4. เลือกที่อยู่ของเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ ในที่นี้คือประเทศไทย จะทำการเลือก other ตามรูปที่ ก.4



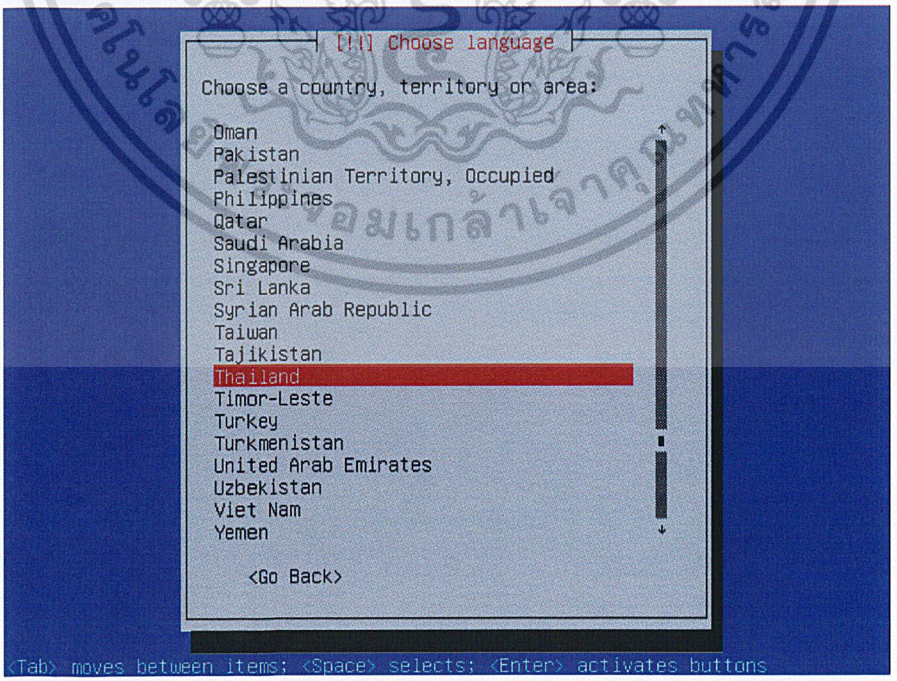
รูปที่ ก.4 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 4

5. เลือกภูมิภาคเอเชีย (Asia) ดังรูปที่ ก.5



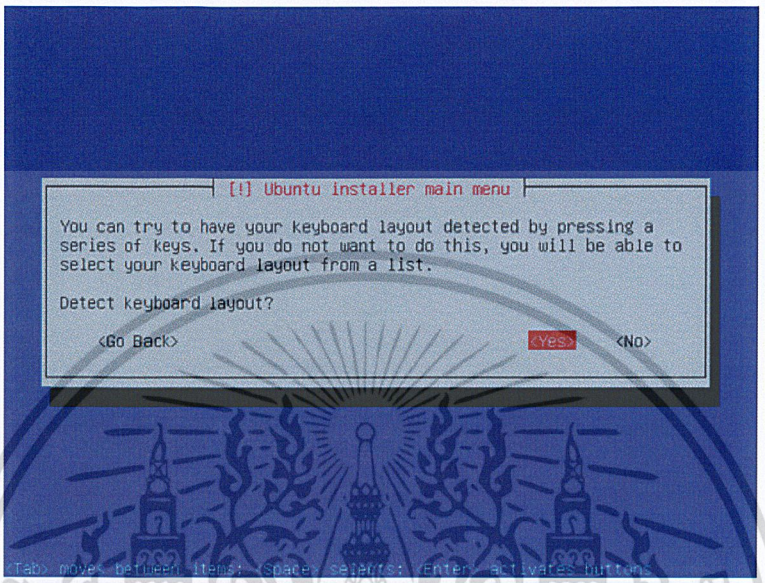
รูปที่ ก.5 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 5

6. เลือกประเทศไทย (Thailand) ดังรูปที่ ก.6



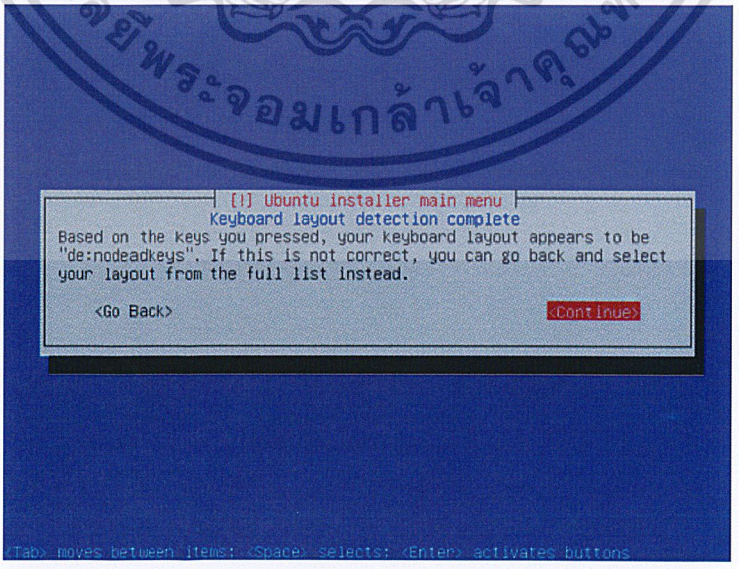
รูปที่ ก.6 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 6

7. ในขั้นตอนนี้ระบบจะถามผู้ติดตั้งว่าจะทำการตรวจสอบภาษาที่ใช้กับคีย์บอร์ดหรือไม่ ในที่นี้จะทำการตรวจสอบเพื่อที่จะทำให้สามารถพิมพ์ข้อความภาษาไทยได้อย่างถูกต้องดังรูปที่ ก.7



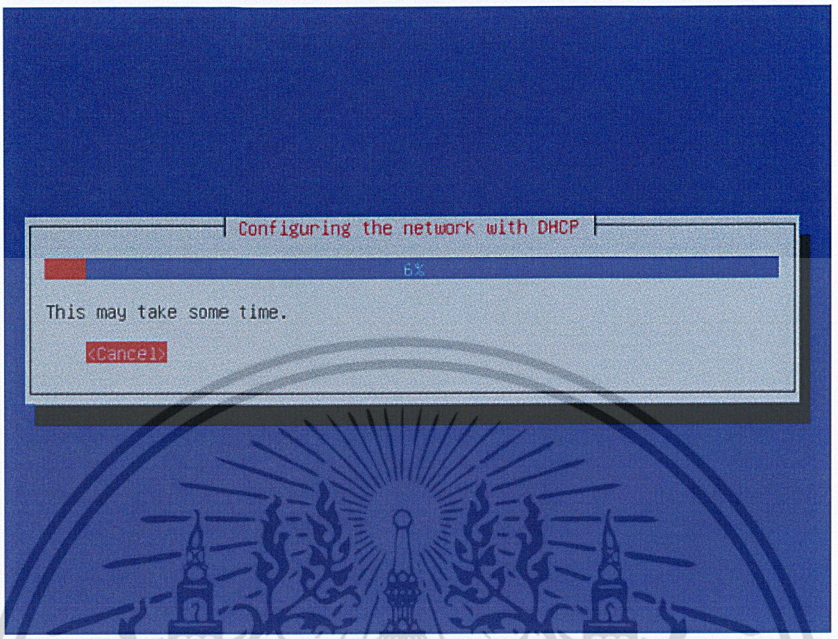
รูปที่ ก.7 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 7

8. ระบบจะแจ้งผู้ติดตั้งว่าได้ทำการตรวจพบคีย์บอร์ดที่เป็นภาษาไทยเรียบร้อยแล้ว ในขั้นตอนนี้ให้กด Continue ดังรูปที่ ก.8



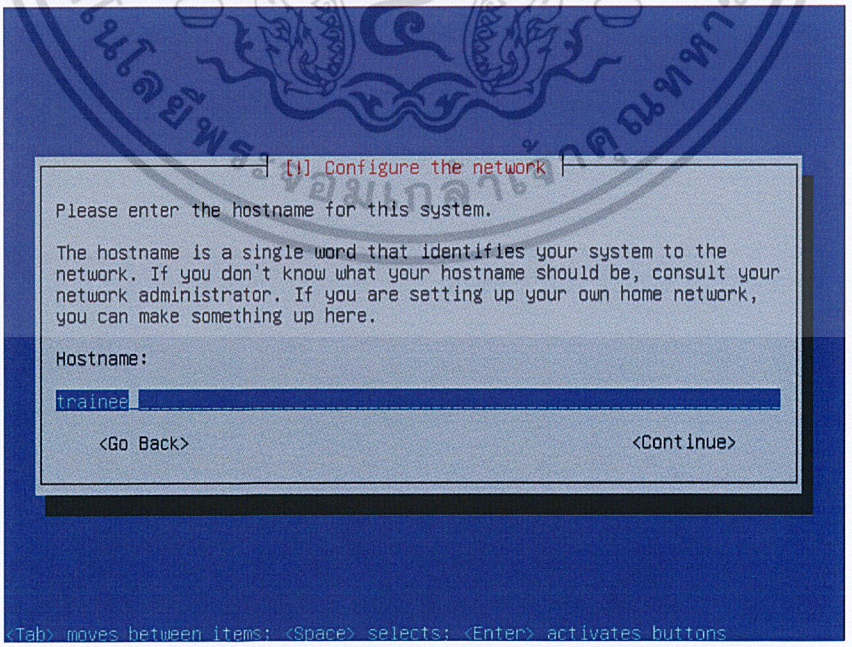
รูปที่ ก.8 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 8

9. ระบบจะทำการตรวจสอบข้อมูลจากแผ่นซีดีการติดตั้ง รวมไปถึงการตั้งค่าไอพีแอดเดรส ซึ่งในขั้นตอนนี้จะเป็นการคอนฟิกไอพีแอดเดรสแบบดีเอชซีพี (DHCP) ดังรูปที่ ก.9



รูปที่ ก.9 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 9

10. ในขั้นตอนนี้จะเป็นการคอนฟิกชื่อโฮสเนมของเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ โดยการใส่ชื่อโฮสเนมแล้วกด Continue ในที่นี้ใส่ว่า ‘trainee’ ดังรูปที่ ก.10

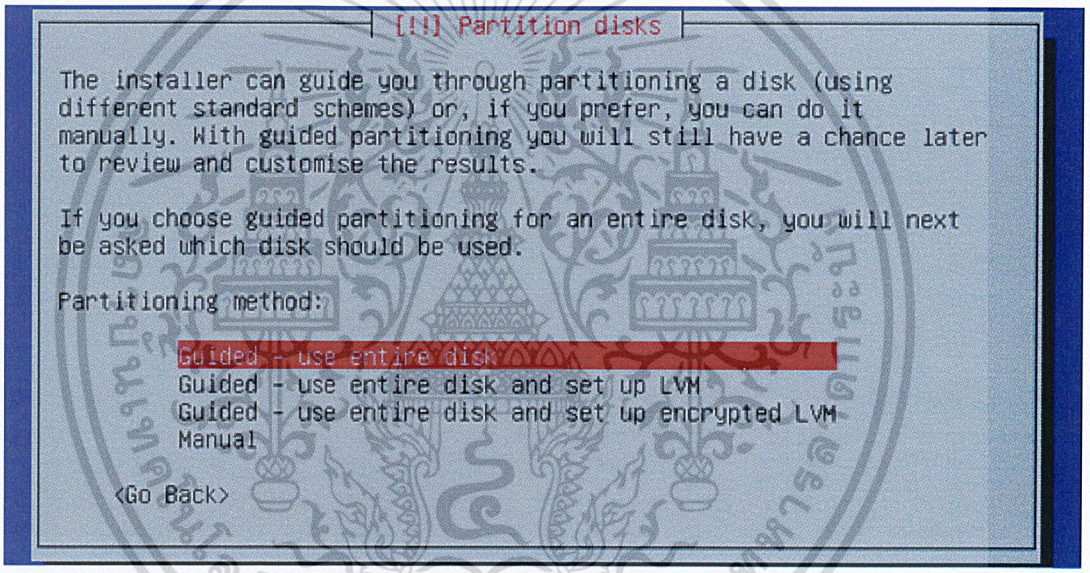


รูปที่ ก.10 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 10

11. ขั้นตอนต่อไปเป็นการจัดการกับฮาร์ดดิสก์ โดยจะเป็นการเลือกพาร์ทิชันที่จะใช้ลงอูบุนตู เซิร์ฟเวอร์โดยมี 4 ทางเลือกด้วยกันคือ

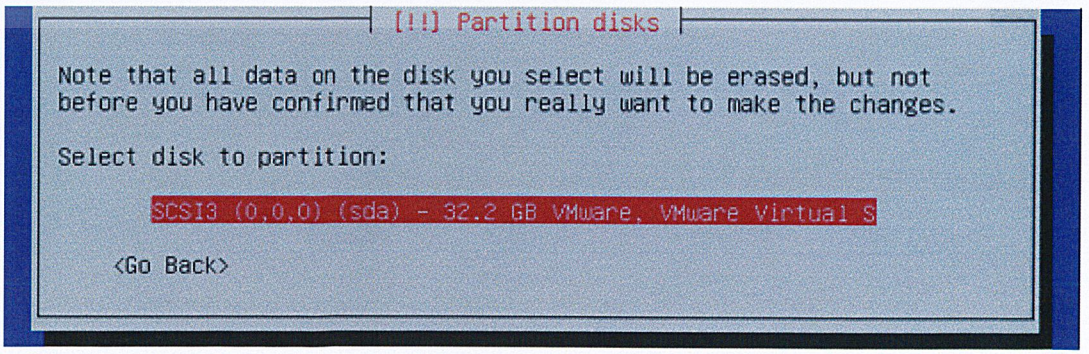
- Guided – use entire disk คือ ให้สร้างพาร์ทิชันให้อัตโนมัติ
- Guided – use entire disk and set up LVM คือ ให้สร้างพาร์ทิชันให้อัตโนมัติ และรวมพื้นที่จากหลายๆไดรฟ์ (Drive)
- Guied – use entire disk and set up encrypted LVM คือ ให้สร้างพาร์ทิชันให้อัตโนมัติ และรวมพื้นที่จากหลายๆไดรฟ์ (Drive) แบบเข้ารหัส
- Manual คือ สร้างพาร์ทิชันเอง

ในขั้นตอนนี้จะเลือก Guided – use entire disk ดังรูปที่ ก.11



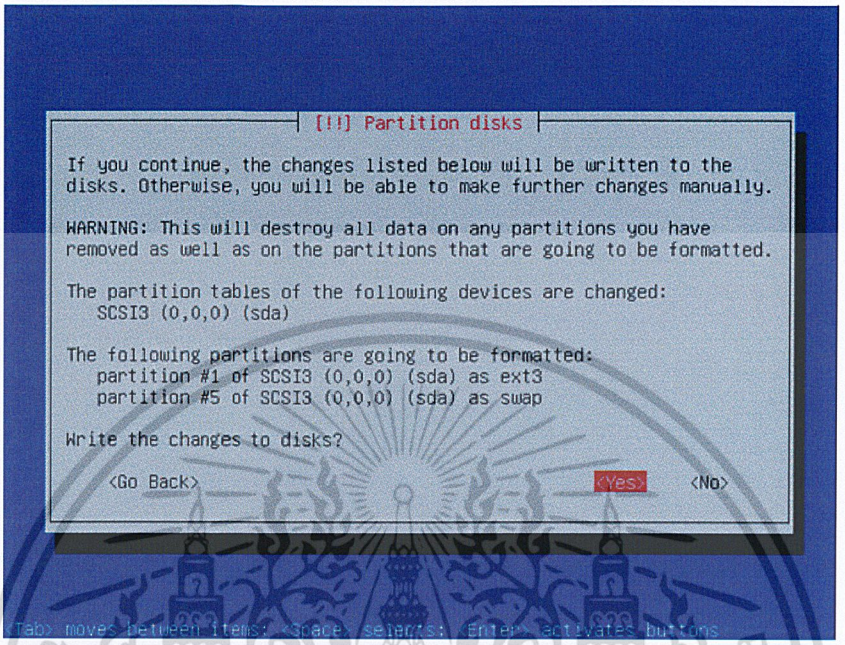
รูปที่ ก.11 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 11

12. เลือกพาร์ทิชันที่จะใช้ติดตั้งอูบุนตูเซิร์ฟเวอร์ ดังรูปที่ ก.12



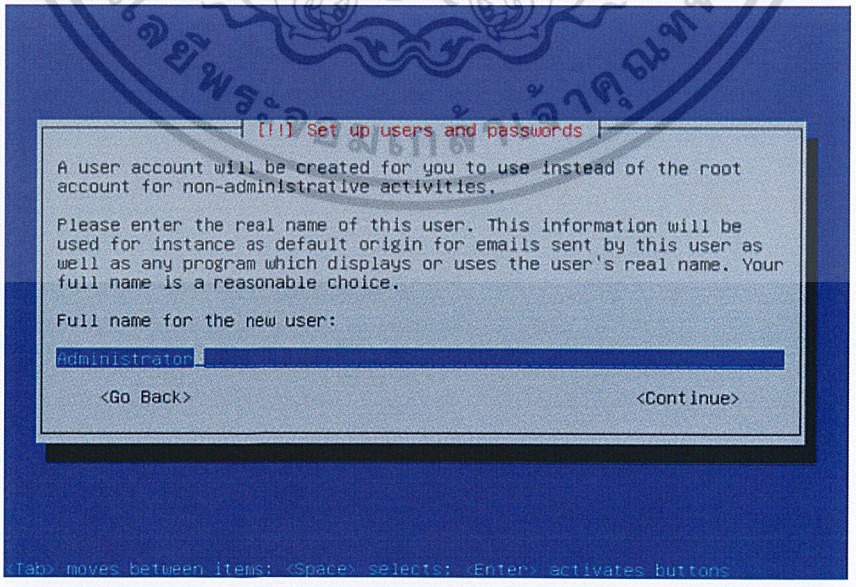
รูปที่ ก.12 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 12

13. ระบบจะแสดงรายละเอียดต่าง ๆ ของการติดตั้งลงในพาร์ทิชัน และให้ผู้ติดตั้งยืนยันการติดตั้ง ลงในฮาร์ดดิส ในขั้นตอนนี้จะเลือก Yes ดังรูปที่ ก.13



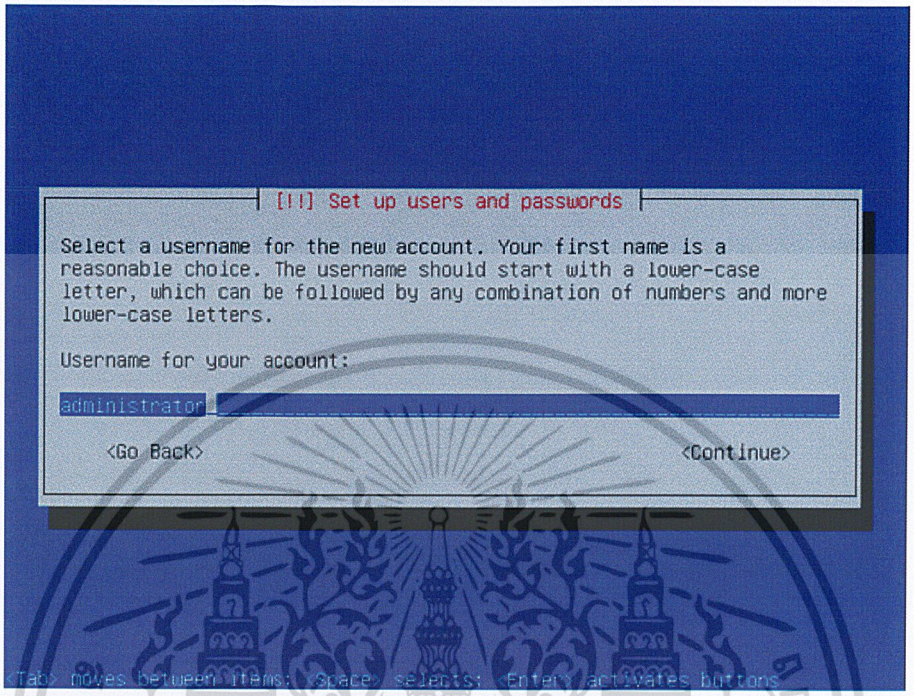
รูปที่ ก.13 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 13

14. ในขั้นตอนนี้จะเป็นการกำหนดชื่อจริงของผู้ดูแลระบบ โดยการพิมพ์ชื่อเต็มแล้วกด Continue ในที่นี้ใส่ว่า ‘Administrator’ ดังรูปที่ ก.14



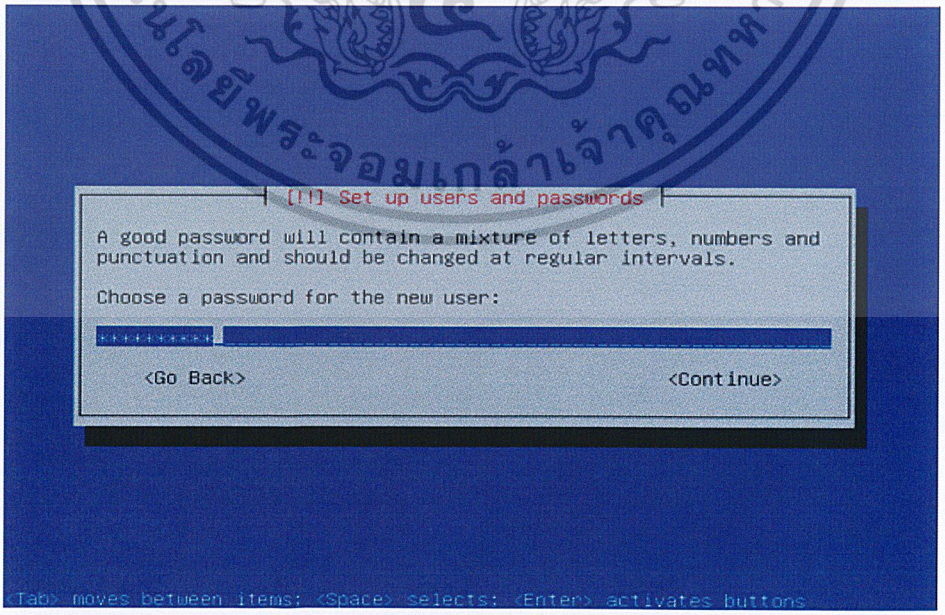
รูปที่ ก.14 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 14

15. ต่อไปเป็นการตั้งชื่อยูเซอร์เนมของผู้ดูแลระบบ ซึ่งจะใช้ในการล๊อกอินเข้าใช้งานอูบุนตู เซิร์ฟเวอร์ ในที่นี้ใส่ว่า ‘administrator’ ดังรูปที่ ก.15



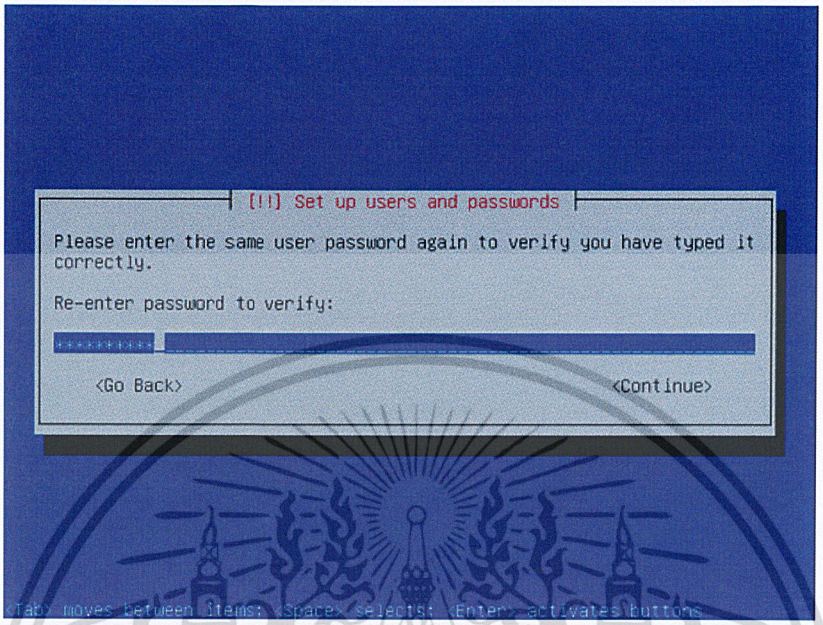
รูปที่ ก.15 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 15

16. กำหนดรหัสผ่านของยูเซอร์ผู้ดูแลระบบดังรูปที่ ก.16



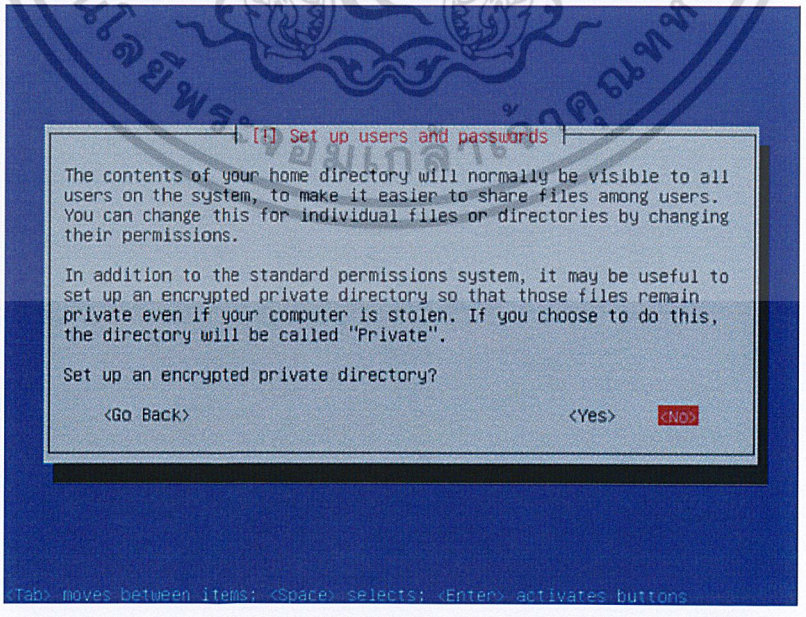
รูปที่ ก.16 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 16

17. ระบบจะให้ยืนยันรหัสผ่านอีกครั้ง เพื่อป้องกันการใส่รหัสในครั้งแรกไม่ถูกต้องดังรูปที่ ก.17



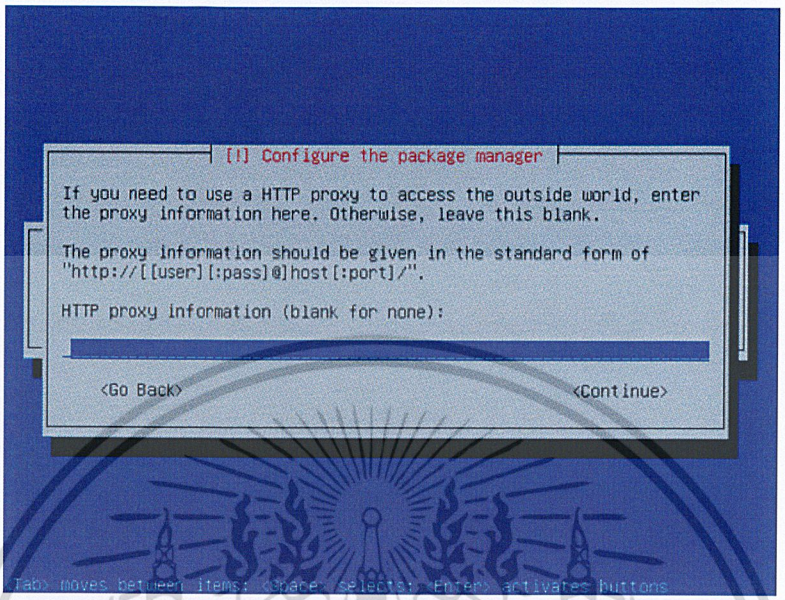
รูปที่ ก.17 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 17

18. ขั้นตอนต่อไปเป็นการกำหนดความปลอดภัยของโฟลเดอร์ส่วนตัวของยูเซอร์ว่าจะให้เข้ารหัสโฟลเดอร์ไว้หรือเปล่า ในขั้นตอนนี้จะเลือก No ดังรูปที่ ก.18



รูปที่ ก.18 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 18

19. ต่อไปจะเป็นการกำหนดการตั้งค่าพร็อกซี่ (Proxy) โดยในขั้นตอนนี้จะไม่ใส่ค่าใด ๆ เพราะระบบไม่จำเป็นต้องใช้พร็อกซี่ดังรูปที่ ก.19

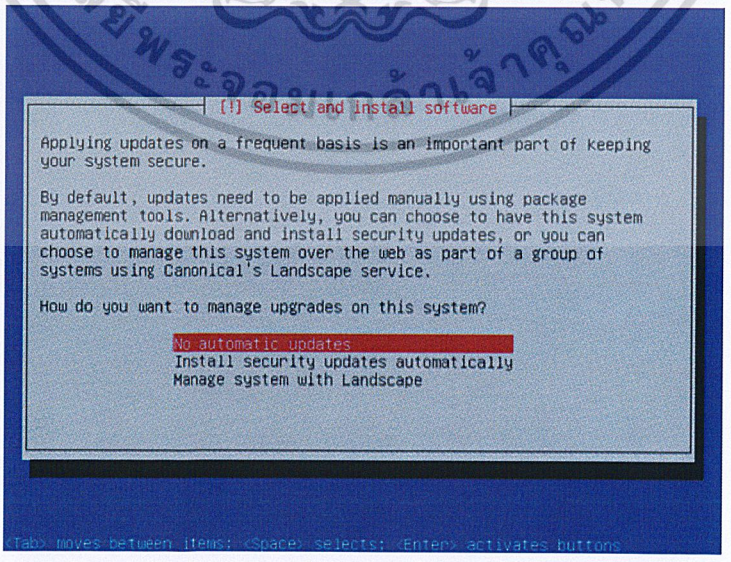


รูปที่ ก.19 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 19

20. ระบบจะถามผู้ติดตั้งว่าจะทำการอัพเดทระบบปฏิบัติการแบบใดดังนี้

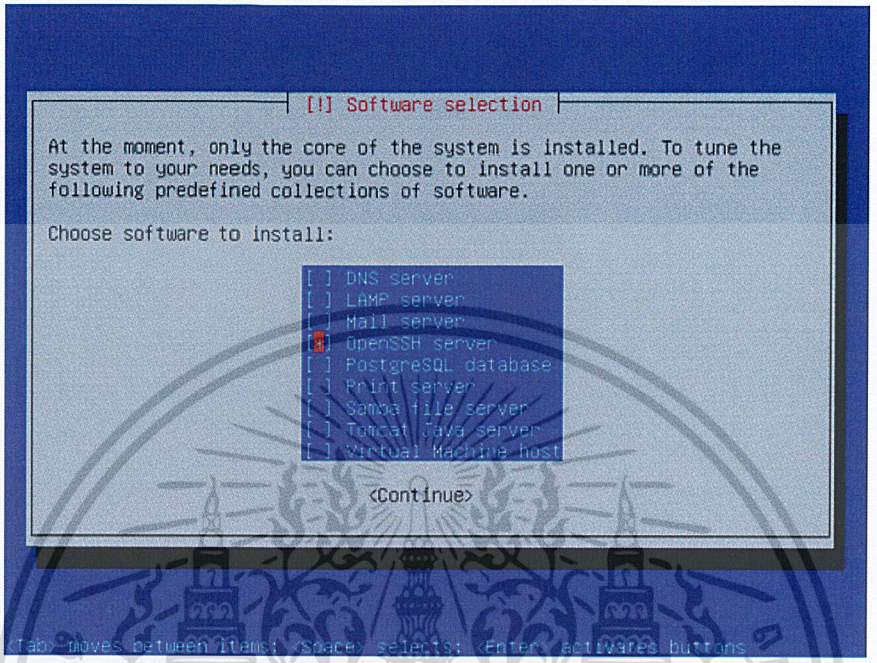
- No automatic update คือ ไม่ให้ติดตั้งอัพเดทใหม่อัตโนมัติ
- Install security update automatically คือ ให้ติดตั้งอัพเดทความปลอดภัยอัตโนมัติ
- Manage System with Landscape คือ เลือกเอง

ในขั้นตอนนี้จะเลือก No automatic updates ดังรูปที่ ก.20



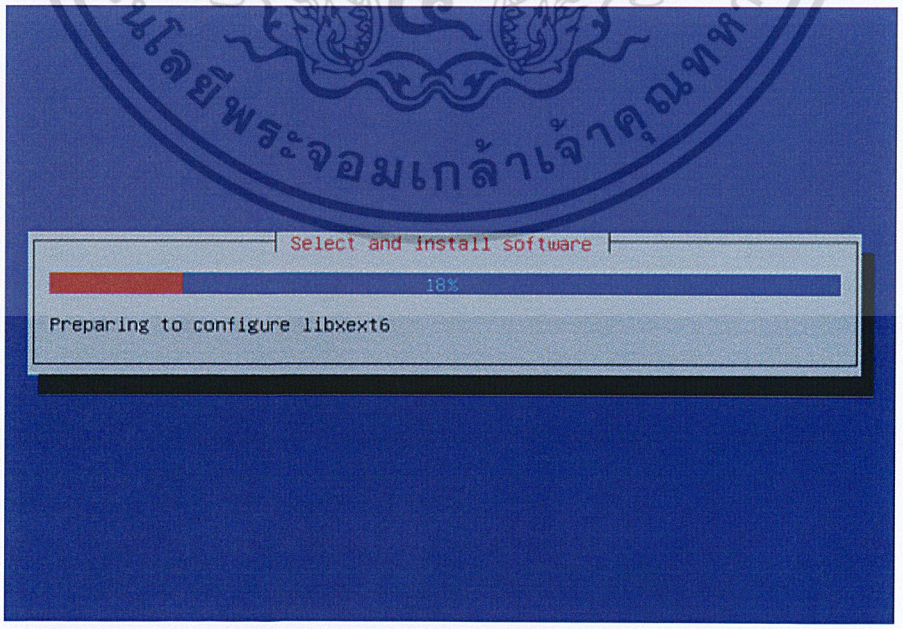
รูปที่ ก.20 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 20

21. ในขั้นตอนนี้จะเป็นการเลือกซอร์ฟแวร์ที่จะติดตั้งพร้อมกับระบบปฏิบัติการ ซึ่งในขั้นตอนนี้จะเลือกเอาเฉพาะโอเพนเอสเอสเอชเซิร์ฟเวอร์ (OpenSSH server) สำหรับการใช้งานโปรแกรมเอสเอสเอช ดังรูปที่ ก.21



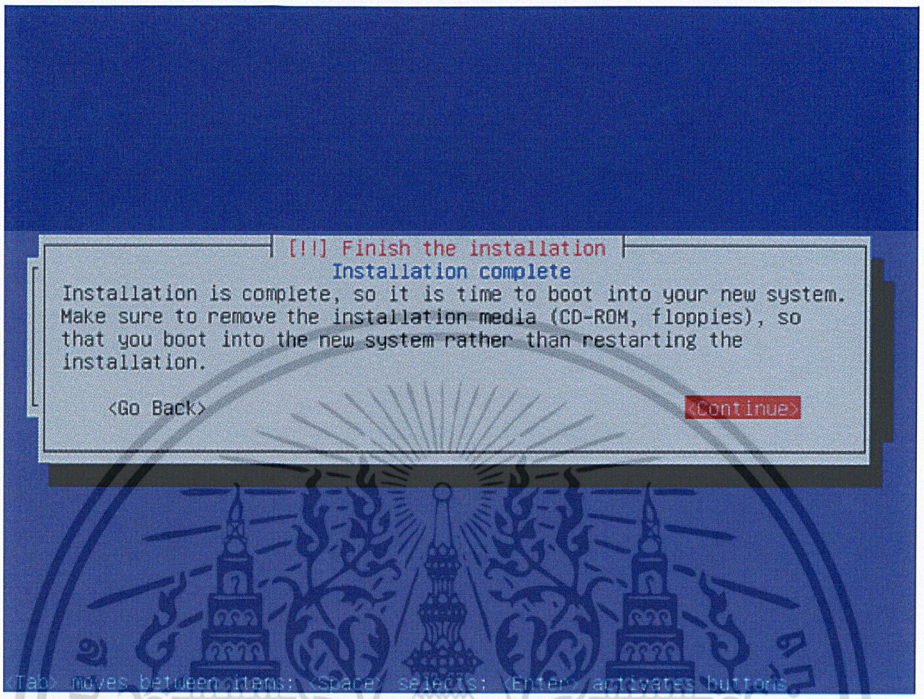
รูปที่ ก.21 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 21

22. ระบบจะทำการติดตั้งโปรแกรมตามที่ได้เลือกไว้ในขั้นตอนที่ผ่านมาดังรูปที่ ก.22



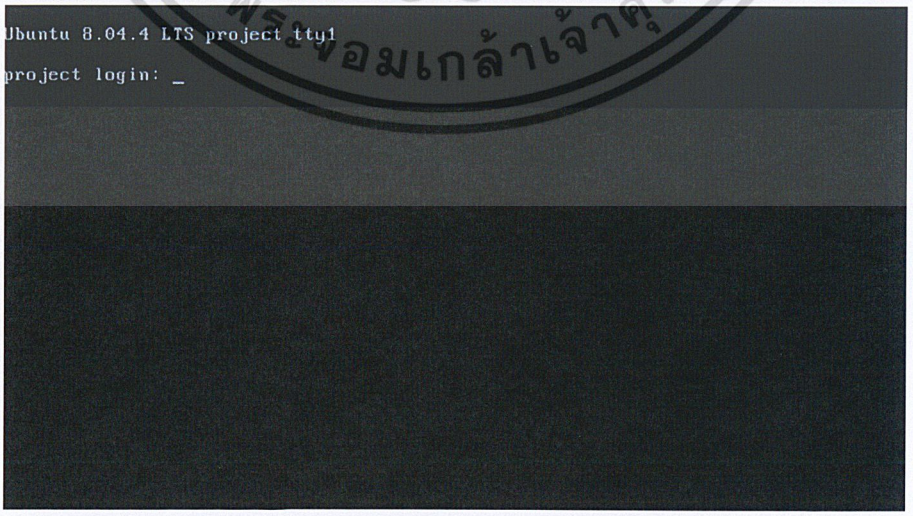
รูปที่ ก.22 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 22

23. ขั้นตอนสุดท้ายของการติดตั้งอูบุนตูเซิร์ฟเวอร์ ระบบจะแจ้งให้ผู้ติดตั้งทราบว่าระบบได้ทำการติดตั้งเสร็จสมบูรณ์แล้ว ให้กด Continue เพื่อรีสตาร์ทเครื่องดังรูปที่ ก.23



รูปที่ ก.23 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 23

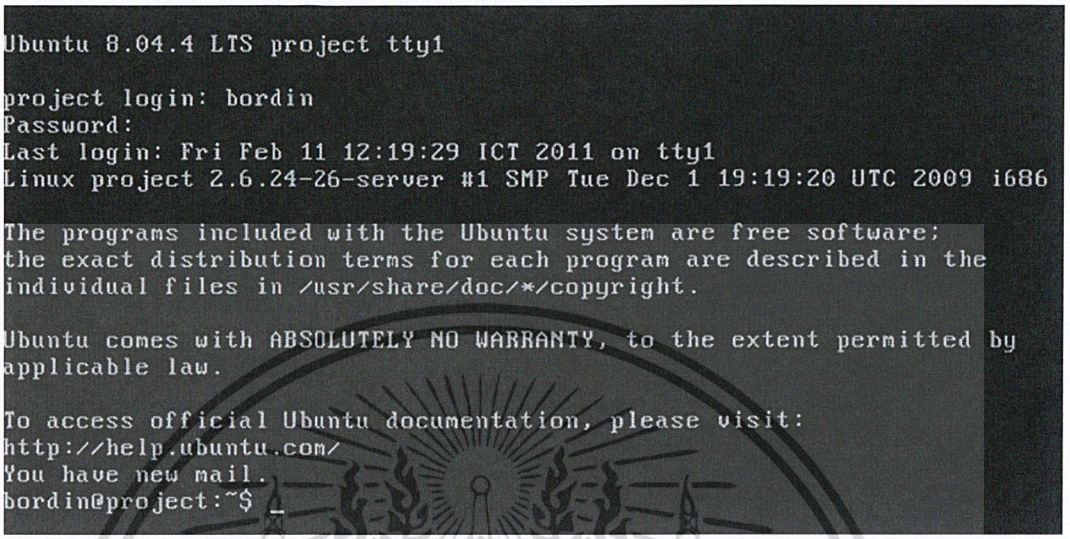
24. หลังจากรีสตาร์ทเครื่องแล้วจะพบกับหน้าจอล๊อกอินดังรูปที่ ก.24 แสดงว่าได้ทำการติดตั้งเสร็จสมบูรณ์แล้วดังรูปที่ ก.24



รูปที่ ก.24 การติดตั้งระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 24

การตั้งค่าเครือข่ายบนระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์

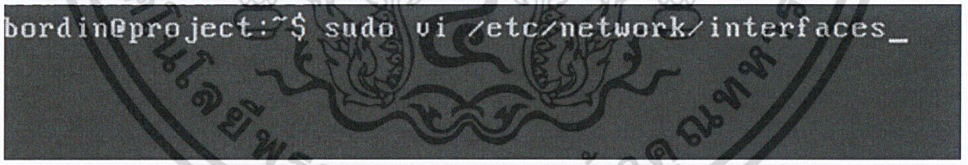
1. ล๊อกอินโดยการใส่ยูเซอร์เนมและรหัสผ่านที่กำหนดไว้ในขั้นตอนการติดตั้ง



รูปที่ ก.25 การตั้งค่าเครือข่ายบนระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 1

2. พิมพ์คำสั่งลงในคอมมานด์ไลน์ ดังรูป ก.26

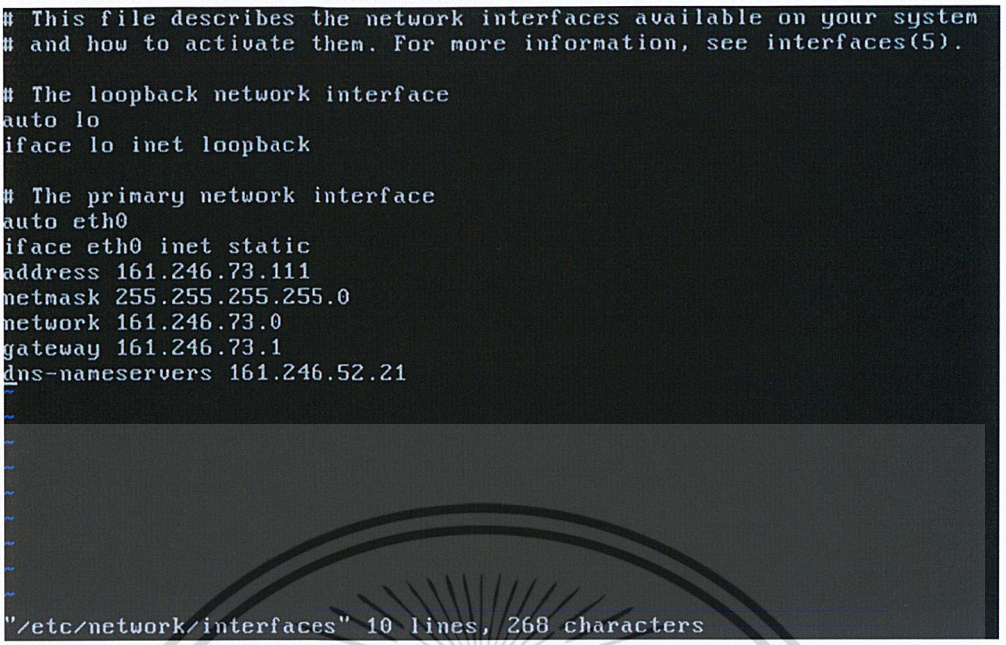
```
sudo vi /etc/network/interface
```



รูปที่ ก.26 การตั้งค่าเครือข่ายบนระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 2

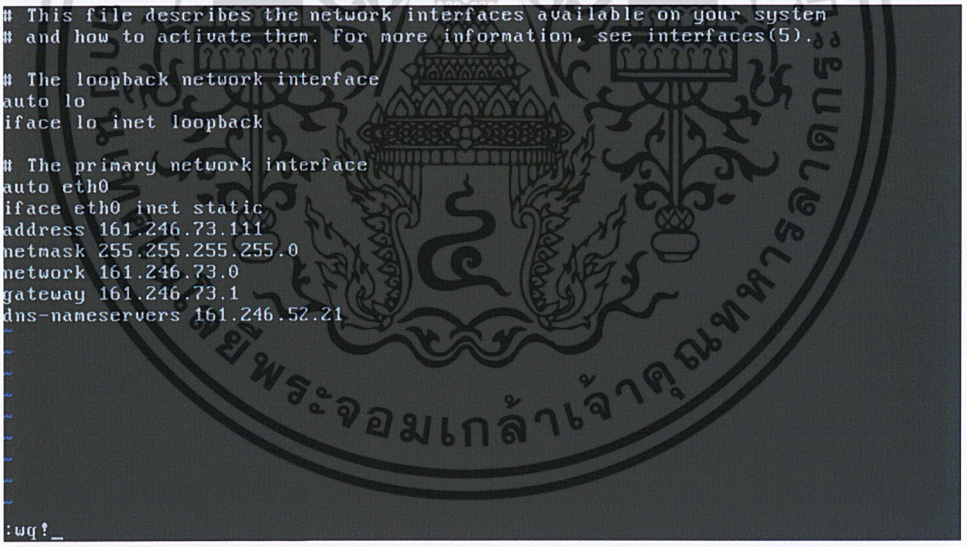
3. คอนฟิกไอพีแอดเดรสแบบสแตติก (Static IP Address) ดังรูป ก.27

```
auto eth 0
iface eth0 inet static
address [หมายเลขไอพีแอดเดรส]
netmask [หมายเลขซับเน็ตมาร์ก]
gateway [ไอพีแอดเดรสของเครื่องเกตเวย์]
dns-nameserver [ไอพีแอดเดรสของดีเอ็นเอสเซิร์ฟเวอร์]
```



รูปที่ ก.27 การตั้งค่าเครือข่ายบนระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 3

4. หลังจากนั้นให้กดปุ่ม ESC และปุ่ม : แล้วพิมพ์ wq! เพื่อเป็นการบันทึกการเปลี่ยนแปลง

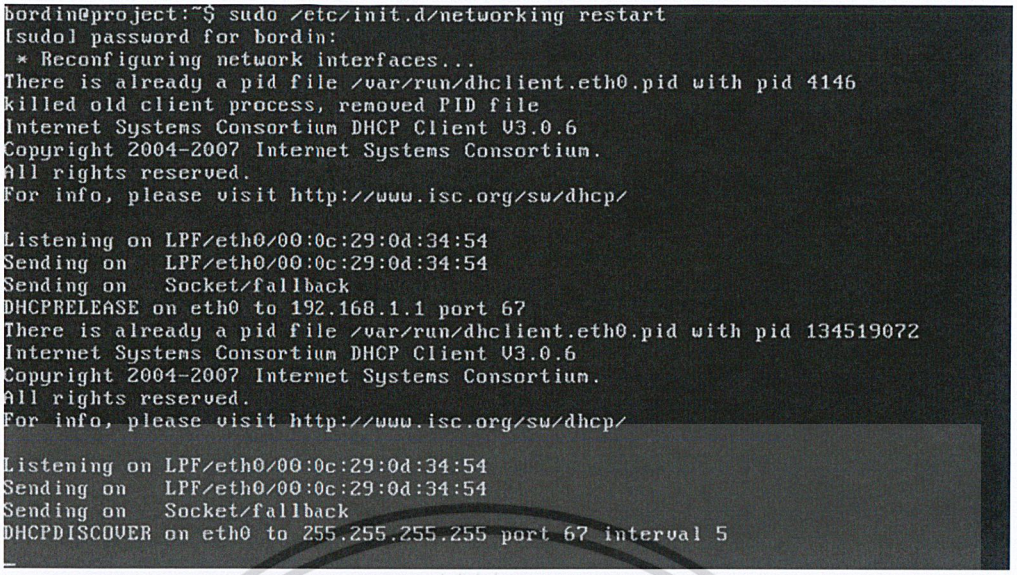


รูปที่ ก.28 การตั้งค่าเครือข่ายบนระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 4

5. ทำการรีสตาร์ทการ์ดเครือข่ายโดยใช้คำสั่ง

```
sudo /etc/init.d/networking restart
```

หลังจากนั้นจะแสดงผลดังรูป ก.29



รูปที่ ก.29 การตั้งค่าเครือข่ายบนระบบปฏิบัติการอูบุนตูเซิร์ฟเวอร์ขั้นตอนที่ 5

ภาคผนวก ข.

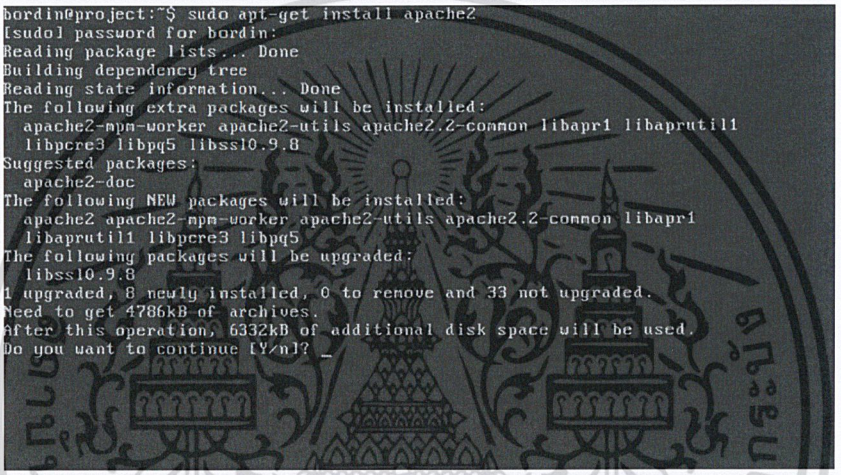
คู่มือการติดตั้งแลมพ์เซิร์ฟเวอร์ (LAMP : Linux, Apache, MySQL, PHP)

ขั้นตอนการติดตั้งอาปาเช่เว็บเซิร์ฟเวอร์

1. พิมพ์คำสั่งต่อไปนี้ลงบนเทอร์มินอล

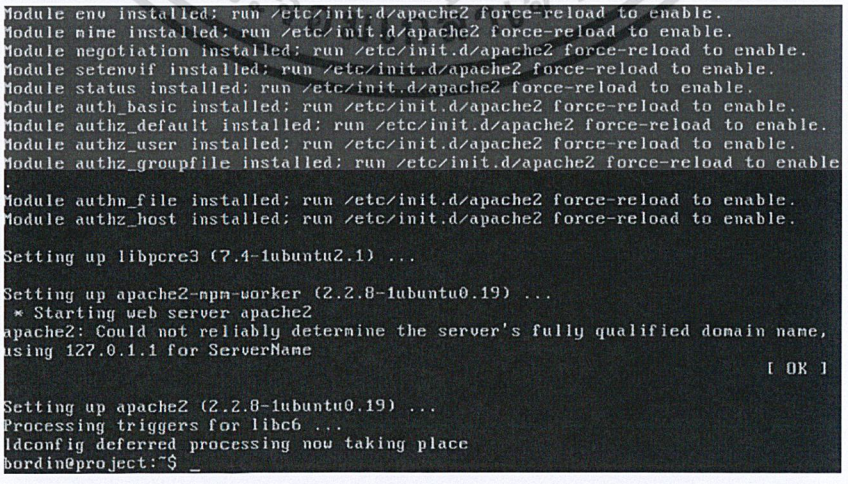
```
sudo apt-get install apache2
```

2. ระบบปฏิบัติการจะถามยูเซอร์เนมและรหัสผ่านก่อนที่จะทำการติดตั้งแพกเกตเพื่อยืนยันว่าเป็นผู้ดูแลระบบ
3. ระบบแสดงรายละเอียดของการติดตั้งให้ทราบ โดยที่ต้องกดปุ่ม Y เพื่อยืนยันการติดตั้ง ดังรูป ข.1



รูปที่ ข.1 การติดตั้งอาปาเช่เว็บเซิร์ฟเวอร์

4. ขั้นตอนนี้จะแสดงให้เห็นว่าระบบได้ทำการติดตั้งอาปาเช่เสร็จสมบูรณ์แล้ว ดังรูป ข.2



รูปที่ ข.2 ติดตั้งอาปาเช่เว็บเซิร์ฟเวอร์เสร็จสมบูรณ์แล้ว

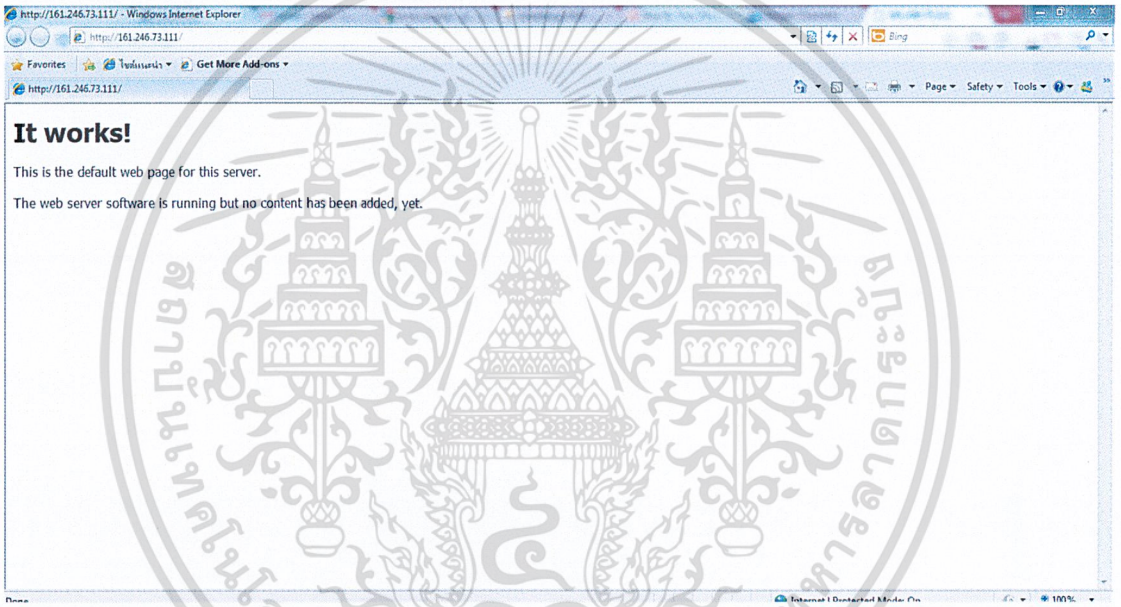
การทดสอบการติดตั้งอาปาเช่เว็บเซิร์ฟเวอร์

เพื่อให้แน่ใจว่าได้ทำการติดตั้งอาปาเช่เสร็จสมบูรณ์แล้ว เราควรทดสอบผลการติดตั้งว่าสามารถใช้งานอาปาเช่เว็บเซิร์ฟเวอร์ได้อย่างถูกต้องหรือไม่

1. เปิดเบราว์เซอร์ หลังจากนั้นใส่แอดเดรสต่อไปนี้ลงบนเบราว์เซอร์

```
http://161.246.73.111/
```

2. เมื่อเห็นหน้าเพจนี้แสดงว่าอาปาเช่เว็บเซิร์ฟเวอร์สามารถทำงานได้อย่างถูกต้อง



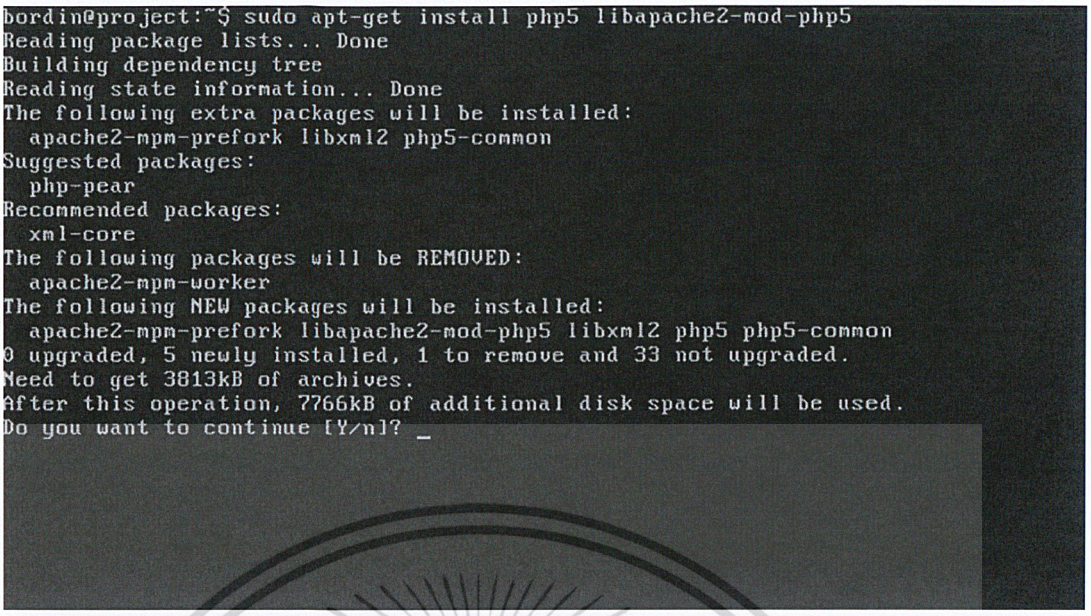
รูปที่ ข.3 ทดสอบการติดตั้งอาปาเช่เว็บเซิร์ฟเวอร์เสร็จสมบูรณ์แล้ว

ขั้นตอนการติดตั้งพีเอชพี

1. พิมพ์คำสั่งดังต่อไปนี้ลงบนเทอร์มินอล

```
sudo apt-get install php5 libapache2-mod-php5
```

2. ระบบปฏิบัติการจะถามยูเซอร์เนมและรหัสผ่านก่อนที่จะทำการติดตั้งแพกเกตเพื่อยืนยันว่าเป็นผู้ดูแลระบบ
3. ระบบแสดงรายละเอียดของการติดตั้งให้ทราบ โดยที่ต้องกดปุ่ม Y เพื่อยืนยันการติดตั้ง



รูปที่ ข.4 การติดตั้งพีเอชพี

4. เพื่อให้พีเอชพีและอาปาเช่ทำงานร่วมกันได้อย่างสมบูรณ์ จะทำการรีสตาร์ทอาปาเช่ ด้วยคำสั่งต่อไปนี้

```
sudo /etc/init.d/apache2 restart
```

การทดสอบการติดตั้งพีเอชพี

1. พิมพ์คำสั่งดังต่อไปนี้ลงบนเทอร์มินอล โดยจะเป็นการสร้างไฟล์ที่มีนามสกุล .php ขึ้นมาไฟล์หนึ่งเพื่อทดสอบผลการติดตั้ง

```
sudo vi /var/www/testphp.php
```

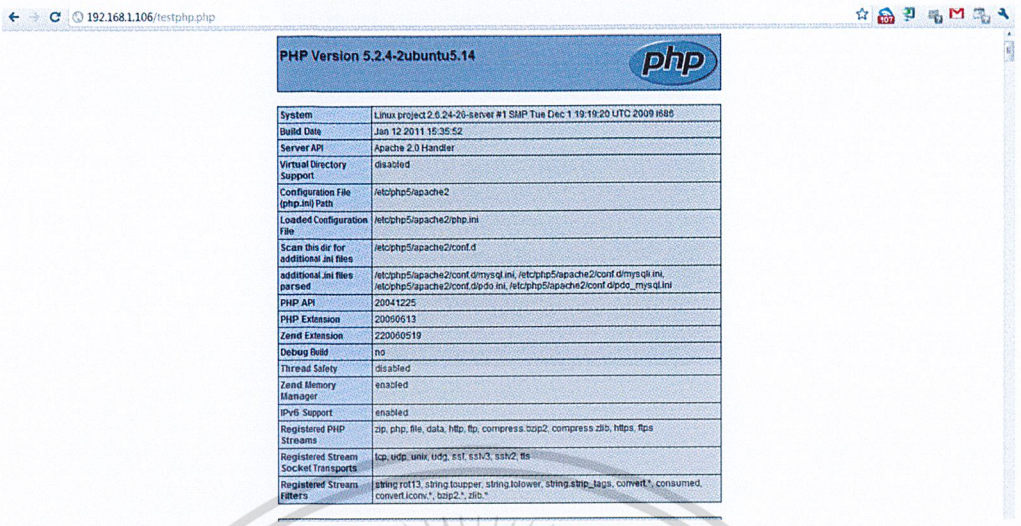
2. พิมพ์ข้อความต่อไปนี้ในไฟล์ testphp.php โดยตัวแปร phpinfo() คือตัวแปรที่ใช้ในการแสดงข้อมูลของพีเอชพี

```
<?php phpinfo(); ?>
```

3. หลังจากนั้นทำการบันทึกไฟล์ testphp.php
4. เปิดเบราว์เซอร์ แล้วพิมพ์แอดเดรสต่อไปนี้ลงบนเบราว์เซอร์

```
http://161.246.73.111/testphp.php
```

5. เมื่อเห็นหน้าเพจนี้แสดงว่าพีเอชพีสามารถทำงานได้อย่างถูกต้องตามรูปที่ ข.5



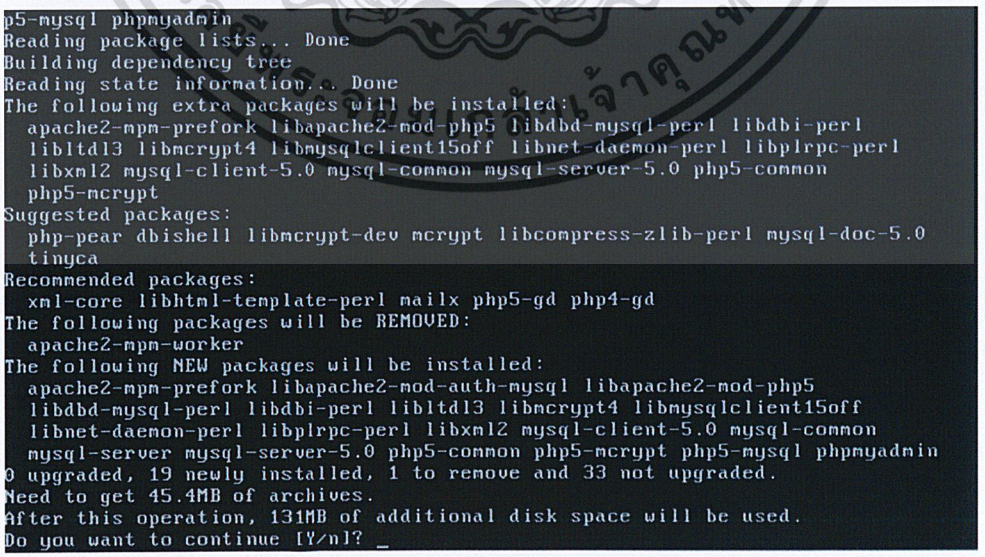
รูปที่ ข.5 พีเอชพีสามารถทำงานได้อย่างถูกต้อง

ขั้นตอนการติดตั้งมายเอสคิวแอล

1. พิมพ์คำสั่งดังต่อไปนี้ลงบนเทอร์มินอล

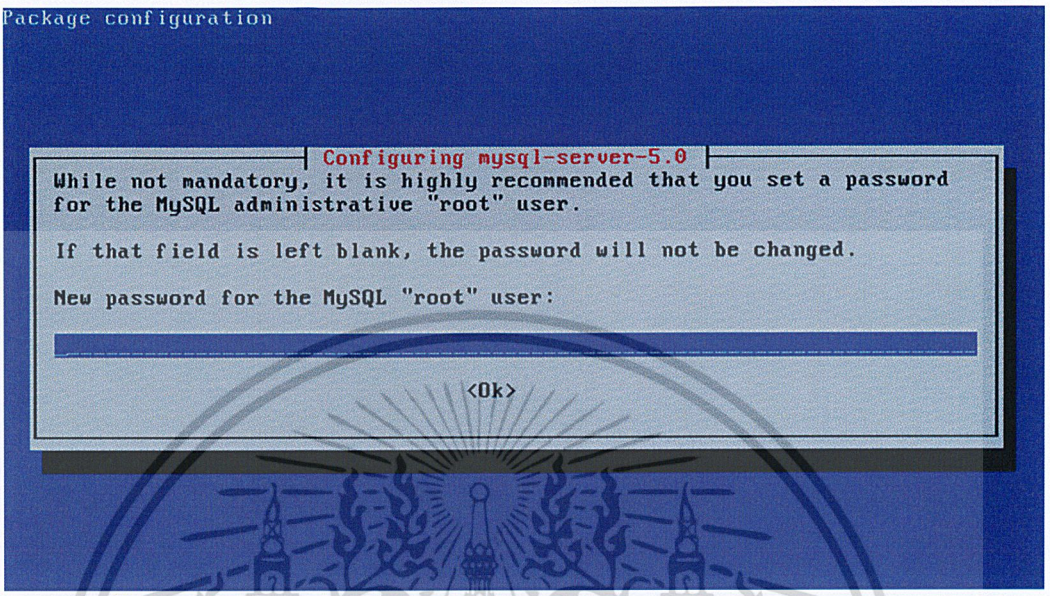
```
sudo apt-get install mysql-server libapache2-mod-auth-mysql php5-mysql phpmyadmin
```

2. ระบบแสดงรายละเอียดของการติดตั้งให้ทราบ โดยที่ต้องพิมพ์ Y เพื่อยืนยันการติดตั้ง ดังรูป ข.6



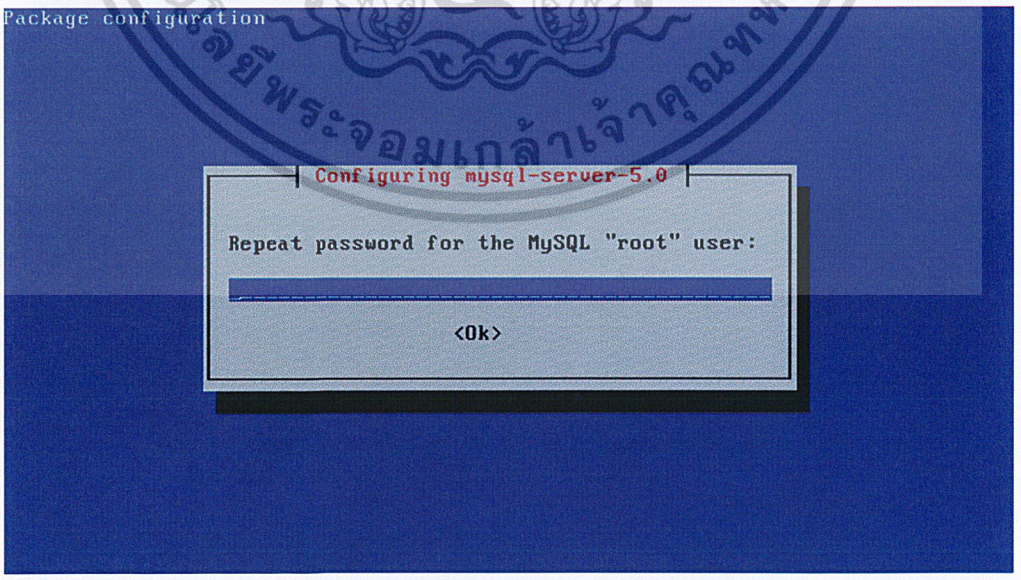
รูปที่ ข.6 การติดตั้งมายเอสคิวแอลขั้นตอนที่ 1 และขั้นตอนที่ 2

3. ขั้นตอนต่อไปเป็นการกำหนดยูเซอร์เนมและรหัสผ่านรูท (root) ของมายเอสคิวแอล โดยให้ใส่รหัสผ่านที่ช่องว่าง แล้วกด Ok ดังรูป ข.7



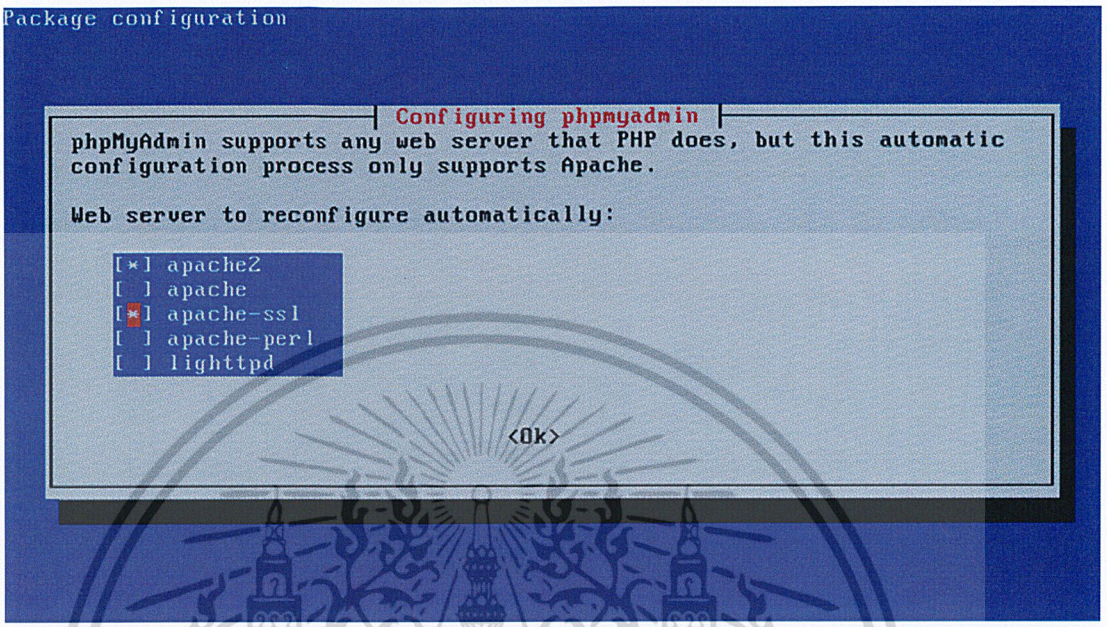
รูปที่ ข.7 การติดตั้งมายเอสคิวแอลขั้นตอนที่ 3

4. การติดตั้งจะให้ยืนยันรหัสผ่านอีกครั้ง เพื่อยืนยันความถูกต้องของรหัสผ่าน ให้ใส่รหัสผ่านเดียวกับขั้นตอนที่ 3 ดังรูป ข.8



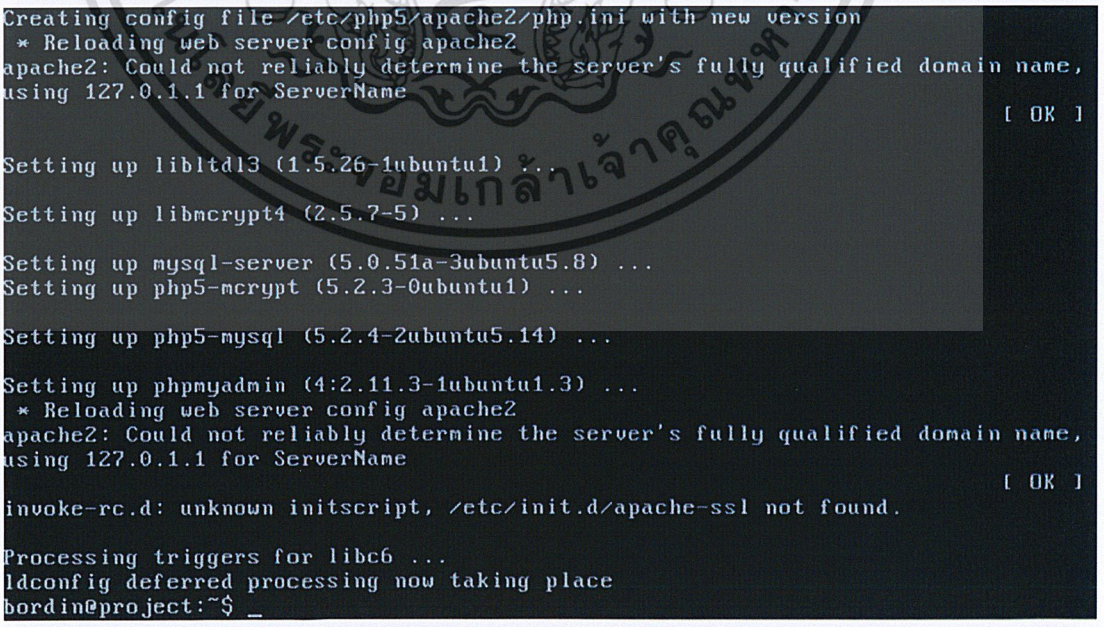
รูปที่ ข.8 การติดตั้งมายเอสคิวแอลขั้นตอนที่ 4

5. ในขั้นตอนนี้จะเป็นการตั้งค่าพีเอชพีมายแอดมิน โดยในขั้นตอนนี้ให้เลือก apache2 และ apche-ssl แล้วกด Ok ดังรูป ข.9



รูปที่ ข.9 การติดตั้งมายเอสคิวแอลขั้นตอนที่ 5

6. รอจนกว่าการติดตั้งจะเสร็จสมบูรณ์ดังรูป ข.10



รูปที่ ข.10 การติดตั้งมายเอสคิวแอลขั้นตอนที่ 6

ขั้นตอนการตั้งค่าพีเอชพีและมายเอสคิวแอล

1. เปิดไฟล์ php.ini ด้วยคำสั่งบนเทอร์มินอลดังนี้

```
sudo vi /etc/php5/apache2/php.ini
```

2. ค้นหาบรรทัดที่มีข้อความนี้

```
;extension=mysql.so
```

3. ให้ทำการแก้ไขโดยการเอาคอมเม้นท์ (;) ออก
4. หลังจากนั้นทำการบันทึกการเปลี่ยนแปลง แล้วรีสตาร์ทอาปาเช่อีกครั้งด้วยคำสั่งต่อไปนี้

```
sudo /etc/init.d/apache2 restart
```

ภาคผนวก ค.

คู่มือการติดตั้งเอ็นแมปสแกนเนอร์

การติดตั้งโปรแกรมเอ็นแมปสแกนเนอร์

1. ติดตั้งโปรแกรมเอ็นแมปสแกนเนอร์ด้วยคำสั่งต่อไปนี้

```
sudo apt-get install nmap
```

2. รอจนกว่าโปรแกรมจะติดตั้งเสร็จสมบูรณ์

```
bordin@project:~$ sudo apt-get install nmap
[sudo] password for bordin:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  nmap
0 upgraded, 1 newly installed, 0 to remove and 33 not upgraded.
Need to get 1013kB of archives.
After this operation, 3506kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com hardy/main nmap 4.53-3 [1013kB]
Fetched 1013kB in 8s (122kB/s)
Selecting previously deselected package nmap.
(Reading database ... 18859 files and directories currently installed.)
Unpacking nmap (from .../archives/nmap_4.53-3_i386.deb) ...
Setting up nmap (4.53-3) ...

bordin@project:~$ _
```

รูปที่ ค.1 การติดตั้งโปรแกรมเอ็นแมป

การตั้งค่าโปรแกรมเอนแมปสแกนเนอร์

ในการใช้งานโปรแกรมเอ็นแมปสแกนเนอร์นั้นจำเป็นที่จะต้องมีการใช้งานในระดับรูทถึงจะสามารถใช้งานได้ครอบคลุมทุกคำสั่ง โดยให้ทำการเปลี่ยนเพอร์มิชชัน (Permission) ของโปรแกรมเอ็นแมป ด้วยคำสั่งต่อไปนี้

```
sudo chmod +s /usr/bin/nmap
```

ภาคผนวก ง.

คู่มือการติดตั้งเนสซัสแกนเนอร์เซิร์ฟเวอร์

การติดตั้งเนสซัสสแกนเนอร์เซิร์ฟเวอร์

1. ดาวน์โหลดโปรแกรมได้ที่ http://www.nessus.org/download/ โดยเลือกรุ่นของเนสซัสให้ตรงกับระบบปฏิบัติการที่ใช้ด้วย
2. นำไฟล์ที่ได้ไปวางไว้ที่ไดเรกทอรี /home/wvs/
3. หลังจากนั้นทำการติดตั้งโปรแกรมโดยใช้คำสั่ง

```
wvs@iteproject:/# sudo chmod 777 /home/wvs/Nessus-3.2.1-ubuntu804_i386.deb
wvs@iteproject:/# sudo dpkg -i /home/wvs/Nessus-3.2.1-ubuntu804_i386.deb
```

4. หลังจากนั้นจะได้ผลออกมาดังรูปที่ ง.1

```
root@iteproject:/# dpkg -i /home/bordin/Nessus-3.2.1-ubuntu804_i386.deb
Selecting previously deselected package nessus.
(Reading database ... 21912 files and directories currently installed.)
Unpacking nessus (from .../Nessus-3.2.1-ubuntu804_i386.deb) ...
Setting up nessus (3.2.1) ...
nessusd (Nessus) 3.2.1. for Linux
(C) 1998 - 2008 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded

 - Please run /opt/nessus/sbin/nessus-adduser to add an admin user
 - Register your Nessus scanner at http://www.nessus.org/register/ to obtain
   all the newest plugins
 - You can start nessusd by typing /etc/init.d/nessusd start
```

รูปที่ ง.1 การติดตั้งเนสซัสเซิร์ฟเวอร์

การตั้งค่าเนสซัสสแกนเนอร์เซิร์ฟเวอร์

1. เข้าสู่ระบบด้วยสิทธิ์รูทของระบบ แล้วเพิ่มผู้ใช้งานเนสซัส โดยใช้คำสั่ง

```
root@iteproject:/# /opt/nessus/sbin/nessus-adduser
```

2. หลังจากใช้คำสั่งเพื่อเพิ่มผู้ใช้งานเนสซัสแล้ว จะแสดงได้ดังรูป ง.2 ซึ่งโปรแกรมจะให้ใส่ชื่อผู้ใช้, รหัสผ่าน หลังจากนั้นให้กดปุ่ม Y เพื่อยืนยันการตั้งค่า

```
Add a new nessusd user
----------------------



Login : wvs
Authentication (pass/cert) [pass] : pass
Login password :
Login password (again) :

User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that wvs has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)



Login          : wvs
Password       : ***********
DN             :
```

```
Rules         :



Is that ok ? (y/n) [y] y
user added.
root@iteproject:/#
```

รูปที่ ง.2 การตั้งค่าเนสซัสเซิร์ฟเวอร์

3. ลงทะเบียนผู้ใช้เนสซัสที่ http://www.nessus.org/register/ ซึ่งจะทำให้สามารถอัพเดทปลั๊กอินรุ่นล่าสุดของเนสซัสได้
4. หลังจากนั้นทำการลงทะเบียนเนสซัสเซิร์ฟเวอร์โดยใช้คำสั่ง

```
/opt/nessus/bin/nessus-fetch --register 46DA-8BCC-7A3D-B02E-8A2A
```

5. สตาร์ทเซอร์วิสของเนสซัสโดยใช้คำสั่ง

```
/etc/init.d/nessusd start
```