ระบบตรวจจับข้อมูลแปลกปลอมบนเครือข่าย

Packet Detector

โดย

นายทิฆัมพร เกรียงวัฒนพงษ์

นายณพงศ์ นิ่มสังข์

นายณรงค์ ประสานศิลป์ชัย

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2547

ระบบตรวจจับข้อมูลแปลกปลอมบนเครือข่าย

Packet Detector

โดย

นายฑิฆัมพร เกรียงวัฒนพงษ์ 44010129

นายณพงศ์ นิ่มสังข์ 44010131

นายณรงค์ ประสานศิลป์ชัย 44010133

อาจารย์ที่ปรึกษา

ผศ. อัครพล ตรีรัตน์

อ. ธเนศ พัฒนธาดาพงษ์

ผศ. นภัทร สระเอี่ยม

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2547

ปริญญานิพนธ์ปีการศึกษา 2547

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง **ระบบตรวจจับข้อมูลแปลกปลอมบนเครือข่าย**

Packet Detector

ผู้จัดทำ

1. นายฑิฆัมพร เกรียงวัฒนพงษ์ 44010129

2. นายณพงศ์ นิ่มสังข์ 44010131

3. นายณรงค์ ประสานศิลป์ชัย 44010133

อาจารย์ที่ปรึกษา

(ผศ. อัครพล ตรีรัตน์)

อาจารย์ที่ปรึกษา

(อ. ธเนศ พัฒนธาดาพงษ์)

อาจารย์ที่ปรึกษา

(ผศ. นภัทร สระเอี่ยม)

ระบบตรวจจับข้อมูลแปลกปลอมบนเครือข่าย

Packet Detector

โดย นายฑิฆัมพร เกรียงวัฒนพงษ์ 44010129
นายณพงศ์ นิ่มสังข์ 44010131
นายณรงค์ ประสานศิลป์ชัย 44010133

อาจารย์ที่ปรึกษา ผศ. อัครพล ตรีรัตน์
อ. ธเนศ พัฒนธาดาพงษ์
ผศ. นภัทร สระเอี่ยม

บทคัดย่อ

ปริญญานิพนธ์นี้ นำเสนอรูปแบบของระบบป้องกันเครือข่ายคอมพิวเตอร์อย่างง่ายและทำให้เป็นระบบที่ใช้งานได้จริง ระบบจะเลือกทิ้งแพ็คเก็ตตามที่ได้กำหนดรูปแบบไว้ ระบบนี้จะกำหนดชุดข้อมูลของแหล่งที่มาและที่อยู่ปลายทางที่ถูกต้องตามทิศทางของทราฟฟิกที่ไหลภายในเครือข่าย ซึ่งเมื่อพบว่าตรงกับข้อมูลการบุกรุกที่เก็บไว้ก็จะแจ้งเตือนให้ผู้ใช้รับทราบเพื่อการควบคุม

Abstract

In this project, we propose the simple form of computer network security algorithm and then implement into such a practical system. The system should selectively discards packets based on configurable criteria. For each direction of traffic on the network , this system should be configured with a set of legal source and destination address that if any packets match with data then system must be alert the user for good system control.

สารบัญ

สารบัญรูปภาพ

หน้า

หน้า

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ความเป็นมาของปริญญานิพนธ์

ในปัจจุบันระบบการรักษาความปลอดภัยคอมพิวเตอร์มีความสำคัญมากขึ้น เนื่องจาการพัฒนาอินเตอร์เน็ตและระบบเครือข่ายไปอย่างรวดเร็ว ทำให้มีผู้ใช้มากขึ้นซึ่งย่อมมีผู้ใช้แบบปกติและผู้ใช้ที่มีลักษณะที่ผิดปกติ เช่น การโจรกรรมข้อมูลในระบบ การทำลายข้อมูลที่มีความสำคัญต่อองค์กร ฯลฯ ได้มีความตระหนักในเรื่องของความปลอดภัยและความเป็นส่วนตัวมานาน ดังจะเห็นได้จากความพยายามในการสร้างระบบความปลอดภัยสำหรับงานต่างๆ ขึ้นมา หนึ่งในนั้น คือระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์ในระบบปฏิบัติการลีนุกซ์ ซึ่งเป็นระบบที่ช่วยเพิ่มความปลอดภัยให้กับคอมพิวเตอร์มากขึ้น

เมื่อคำนึงถึงเรื่องความปลอดภัยของคอมพิวเตอร์มักเป็นการยากในการมองภาพที่ชัดเจนว่า อะไรที่จะบ่งบอกได้ว่าการใช้งานคอมพิวเตอร์มีความปลอดภัย เนื่องจากความปลอดภัยของคอมพิวเตอร์เป็นสิ่งที่จับต้องไม่ได้และยากต่อการวัด แต่อย่างไรก็ตามเราสามารถเปรียบเทียบความปลอดภัยของคอมพิวเตอร์กับการรักษาความปลอดภัยสถานที่ ในการรักษาความปลอดภัย (รปภ.) สถานที่นั้นนอกจากการ จัดบริเวณที่ต้องรักษาความปลอดภัย ให้มีรั้วรอบขอบชิด มีกุญแจที่ใช้ล็อกประตูหรือทางเข้าออก สิ่งหนึ่งที่จะขาดไม่ได้คือการจัดให้มีบุคคลหรืออุปกรณ์ที่คอยตรวจสอบ การละเมิดต่ออุปกรณ์หรือเครื่องกีดขวางที่จัดตั้งเพื่อความปลอดภัย ทั้งนี้เนื่องจากอาจมีผู้ไม่หวังดีพยายามบุกรุกโดยทำลายอุปกรณ์หรือเครื่องกีดขวางดังกล่าว ดังนั้นเราจึงต้องอาศัยระบบที่ใช้ตรวจสอบเมื่อมีการทำลายหรือล่วงล้ำต่ออุปกรณ์หรือเครื่องกีดขวางที่ได้ติดตั้งไว้อีกชั้นหนึ่ง ตัวอย่างอุปกรณ์ที่ใช้ตรวจสอบเช่น ระบบสัญญาณเตือนขโมยที่ใช้ควบคู่กับรั้วที่แข็งแรง ระบบเครือข่ายคอมพิวเตอร์ก็เช่นเดียวกัน บุคคลทั่วไปมักคิดว่าการติดตั้ง ไฟร์วอลล์ (Firewall) ตามลำพังก็สามารถทำให้เครือข่ายคอมพิวเตอร์มีความปลอดภัย แต่อย่างไรก็ตาม การติดตั้งไฟร์วอลล์ ให้กับระบบเครือข่ายคอมพิวเตอร์ก็เปรียบเสมือน การสร้างรั้วหรือกำแพงเพื่อตรวจสอบบุคคลที่จะเข้ามาในสถานที่ที่จะรักษาความปลอดภัย แต่หากมีบุคคลไม่หวังดีสามารถปีนรั้วเข้ามาได้ การรักษาความปลอดภัยโดยใช้รั้วก็หมดความหมาย ดังนั้นในการเพิ่มความปลอดภัยอีกประการหนึ่งคือการใช้ระบบตรวจจับการบุกรุกซึ่งมีคุณลักษณะที่กล่าวมาในตอนต้น

ในปริญญานิพนธ์ฉบับนี้ เป็นการออกแบบและสร้างอุปกรณ์ตรวจจับข้อมูลแปลกปลอมบนระบบเครือข่าย (Packet Detector) ซึ่งเป็นระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ โดยระบบตรวจจับข้อมูลแปลกปลอมบนระบบเครือข่ายนี้เป็นการป้องกันความไม่ถูกต้องความไม่เหมาะสมหรือการที่ผิดปกติ ซึ่งอ้างอิงกับ ระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์ (Intrusion Detection System – IDS) เป็นหลัก โดยระบบตรวจจับผู้บุกรุกเป็นแบบปฏิบัติการบนการไหลข้อมูลในเครือข่าย (Network - based Intrusion Detection System) ซึ่งใช้วิธีเกี่ยวกับการตรวจจับการใช้งานโดยการตรวจสอบกับข้อกำหนดการใช้งาน และ การตรวจสอบจากสถิติการใช้งานของผู้ใช้และนำข้อมูลมาวิเคราะห์หาความเป็นไปได้ในการบุกรุก (Signature Intrusion Detection)

1.2 วัตถุประสงค์ของปริญญานิพนธ์

1. เพื่อสร้างระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์อย่างง่ายและใช้งานได้จริงโดยใช้วิธีตรวจจับแบบการตรวจสอบกับข้อกำหนดการใช้งานบนระบบปฏิบัติการลีนุกซ์
2. เพื่อศึกษาวิธีการในการตรวจจับการบุกรุก
3. เพื่อศึกษาและเขียนแอพพลิเคชั่นบนระบบปฏิบัติการลีนุกซ์
4. เพื่อศึกษาและเขียนโปรแกรมภาษา HTML สำหรับการแสดงผล

1.3 เป้าหมายของการพัฒนาของปริญญานิพนธ์

เพื่อสร้างระบบการตวรจจับผู้บุกรุกบนเครือข่ายคอมพิวเตอร์อย่างง่าย โดยอาศัยหลักการและข้อมูลพื้นฐานของระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ ให้มีความปลอดภัย โดยการเก็บข้อมูลเพื่อนำไปเปรียบเทียบกับข้อมูลรูปแบบการบุกรุกที่กำหนดขึ้น และสะดวกในการตรวจสอบผลของการตรวจจับการบุกรุกผ่านทางเว็บเพจ เพื่อให้ผู้ใช้สามารถตรวจสอบผลการตรวจจับการบุกรุก จากที่ใดก็ได้ที่มีเครือข่ายอินเทอร์เน็ตเชื่อมต่ออยู่

1.4 ขอบเขตของปริญญานิพนธ์

ในโครงงานนี้ได้สร้างระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์ สำหรับระบบปฏิบัติการลีนุกซ์ Redhat 9.0 และมีการตรวจจับการบุกรุกเป็นการตรวจสอบการใช้งานทรัพยากรระบบที่ผิดปกติซึ่งเป็นพฤติกรรมของการบุกรุกที่อาศัยทฤษฎี การตรวจสอบเพื่อเปรียบเทียบข้อมูลที่เกี่ยวกับการโจมตีชนิดต่าง ๆ พร้อมทั้งช่องโหว่ของระบบ ในการตรวจจับการให้ใช้ช่องโหว่ต่างๆ เมื่อความพยายามในการเข้าใช้นั้นถูกจับได้ ระบบตรวจจับผู้บุกรุกจะนำแพ็คเก็ตนั้นไปเก็บไว้ในไฟล์ฐานข้อมูล เพื่อนำไปเปรียบเทียบไฟล์ฐานข้อมูลการบุกรุกรูปแบบต่าง ๆ และพบว่าตรงกับไฟล์ฐานข้อมูลการบุกรุกแบบหนึ่ง ระบบก็จะทำการแจ้งเตือน โดยการแสดงผลผ่านทาง เว็บเพจ โดยโปรแกรมที่ใช้เขียนเป็นโปรแกรมภาษาซี (C Language) และ ภาษาเอชทีเอ็มแอล (HTML Language) เพราะฉะนั้นจะเห็นได้ว่า ความสมบูรณ์ และประสิทธิภาพของระบบตรวจจับผู้บุกรุกชนิดนี้จะขึ้นอยู่กับรูปแบบของการตรวจจับและความทันสมัยของข้อมูลเกี่ยวกับการโจมตีต่าง ๆ

1.5 วิธีดำเนินงานของปริญญานิพนธ์

1. ศึกษาทฤษฎีความรู้พื้นฐานเกี่ยวกับระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์
2. ศึกษาวิธีการการโจมตีประเภทต่างๆ และโปรโตคอลการสื่อสารในระบบอินเทอร์เน็ต
3. ศึกษาความรู้พื้นฐานเกี่ยวกับระบบปฏิบัติการลีนุกซ์และการใช้ภาษาซีบนระบบปฏิบัติการลีนุกซ์
4. ออกแบบระบบตรวจจับผู้บุกรุกและเขียนโปรแกรม
5. ออกแบบรูปแบบการแสดงผลข้อมูลการตรวจจับของระบบและเขียนโปรแกรม
6. ทดสอบการใช้งานและปรับปรุงโปรแกรมระบบที่เขียนขึ้น

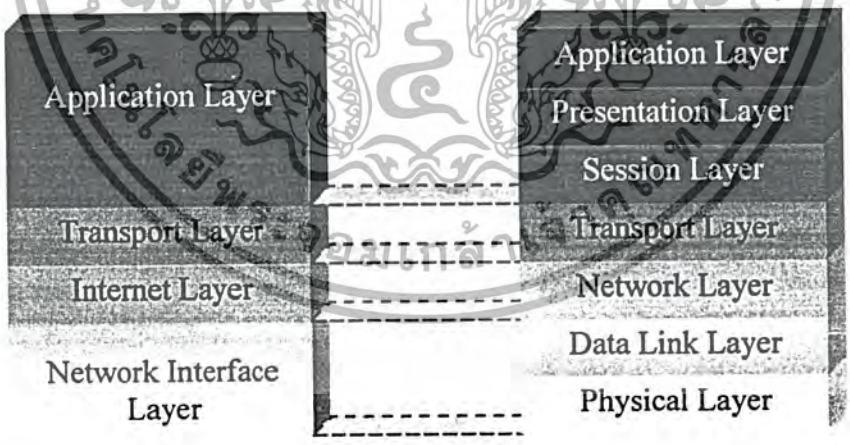
บทที่ 2
ทฤษฎีและหลักการ

2.1 ทีซีพีไอพีโพรโตคอล (TCP/IP Protocol)

โพรโตคอล (Protocol) คือ กฎ ขั้นตอน และรูปแบบข้อมูลที่ใช้ในการสื่อสารระหว่างเครื่องคอมพิวเตอร์ สองเครื่องใด ๆ ขึ้นไปที่เชื่อมต่อกันเป็นเครือข่าย อุปกรณ์ต่าง ๆ ที่อยู่บนเครือข่ายอินเทอร์เน็ตที่ติดต่อกันนั้น จะต้องมีการใช้ข้อตกลงในการสื่อสารข้อมูลร่วมกันเพื่อควบคุมการส่งและรับข้อมูล โดยทีซีพี (TCP - Transmission Control Protocol) และไอพี (IP - Internet Protocol) เป็น 2 โพรโตคอลที่สำคัญของเครือข่ายอินเทอร์เน็ต และเป็นหัวใจสำคัญของข้อตกลงในการสื่อสารข้อมูลที่เป็นที่รู้จักกันดีในชื่อว่า ทีซีพี/ไอพีโพรโตคอล (TCP/IP protocols)

ทีซีพี/ไอพีโพรโตคอล พัฒนาขึ้นในปี 1970 ในโครงการของ DARPA โดยมีวัตถุประสงค์ในการสร้างรูปแบบการสื่อสารที่สามารถค้นหาเส้นทางที่จะส่งข้อมูลได้โดยอัตโนมัติ เพื่อให้เกิดระบบการสื่อสารที่มีประสิทธิภาพสูงในทางทหาร ทีซีพีไอพีโพรโตคอล มีแนวคิดพื้นฐานแตกต่างจากโอเอสไอโมเดล (OSI Model) คือไม่ได้มีพื้นฐานของการสื่อสารแบบการสนทนา ทีซีพี/ไอพีโพรโตคอล เป็นภาพแสดงถึงโลกของระบบเครือข่ายสากล (Internetworking) ที่ทำการเคลื่อนย้ายและกำหนดเส้นทางให้กับข้อมูลระหว่างเครือข่ายและระหว่างเครื่องคอมพิวเตอร์ต่างๆ เมื่อเปรียบเทียบความสัมพันธ์ระหว่างทั้ง 2 โมเดล จะพบว่ามีบางเลเยอร์ที่มีการกำหนดคุณสมบัติที่เทียบได้ใกล้เคียงกัน แต่บางเลเยอร์ก็ไม่สามารถเทียบหาความสัมพันธ์กันได้เลย

2.1.1 ลำดับชั้นของทีซีพี/ไอพีโพรโตคอล (TCP/IP STACK)



รูปที่ 2.1 แสดงการเปรียบเทียบเลเยอร์ของโอเอสไอกับเลเยอร์ของทีซีพี/ไอพี

ในแต่ละระดับชั้นของทีซีพี/ไอพีมีการทำงานที่แตกต่างกัน ตั้งแต่การติดต่อกับแอพพลิเคชั่นจนกระทั่งแปลงเป็นสัญญาณส่งไปตามสายสัญญาณ ซึ่งการทำงานในแต่ละระดับชั้นของทีซีพี/ไอพี มีดังตารางที่ 2.1

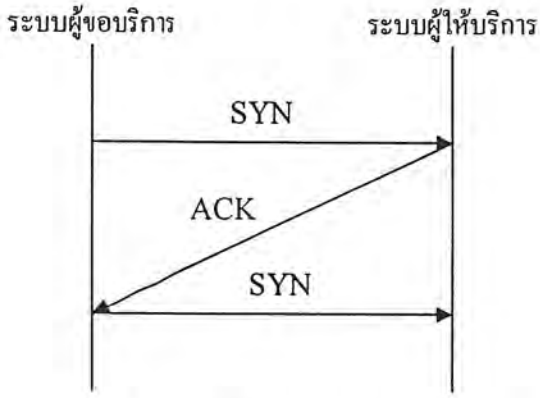
ชื่อระดับชั้น	หน้าที่
1. ชั้นแอพพลิเคชั่น (Application Layer)	ชั้นนี้รองรับการทำงานของแอพพลิเคชั่นต่างๆ ที่ทำงานเป็นโพรเซสอยู่ในเครื่องต้นทางและปลายทาง โดยจัดการเชื่อมต่อระหว่างโพรเซส หรือแอพพลิเคชั่นที่อยู่ต่างเครื่องกัน โดยการทำงานของแอพพลิเคชั่นต่างๆมีการติดต่อกันตามแต่ละโพรโตคอลเฉพาะแล้วแต่แอพพลิเคชั่นที่ใช้งาน ซึ่งจะขอบริการจากชั้นทรานสปอร์ตอีกทีหนึ่ง
2. ชั้นทรานสปอร์ต (Transport Layer)	มีการสร้างการเชื่อมต่อกันระหว่างแอพพลิเคชั่นแบบ 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)	ชั้นนี้มีหน้านี้ส่งผ่านข้อมูลระหว่างเครือข่าย โดยมีโพรโตคอลที่ทำงานเป็นคลไกสำคัญในการส่งผ่านข้อมูลไปยังเครือข่ายใดๆ 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)	ทำหน้าที่ในการแปลงข้อมูลให้อยู่ในรูปที่เหมาะสมกับเครือข่ายแต่ละแบบ ซึ่งแตกต่างกันออกไป และแปลงเป็นสัญญาณไฟฟ้าส่งไปยังเครือข่าย

ตารางที่ 2.1 การทำงานของแต่ละระดับชั้นของทีซีพี/ไอพี

ในชุดโพรโตคอลทีซีพี/ไอพีนี้ มีโพรโตคอลหลักที่ขอกล่าวถึง 5 โพรโตคอล ได้แก่ โพรโตคอลทีซีพี ,โพรโตคอลยูดีพี ซึ่งทำงานในชั้นทรานสปอร์ต และโพรโตคอลไอพี ซึ่งทำงานในชั้นอินเทอร์เน็ต โดยมีรายละเอียดดังต่อไปนี้

2.1.2 ทีซีพี (TCP)

โพรโตคอลทีซีพี (TCP - Transmission Control Protocol) นั้นมีการทำงานที่สำคัญอย่างหนึ่ง คือ การทำ "3-way Handshake" ซึ่งเป็นกระบวนการเริ่มต้นในการสร้างการเชื่อมต่อในชั้นทรานสปอร์ต กล่าวคือ ในการติดต่อกันระหว่างระบบในเครือข่ายต้องมีการสร้างการเชื่อมต่อไปยังระบบที่ให้บริการก่อน โดยผู้ขอบริการส่งสัญญาณ SYN เพื่อขอบริการ จากนั้นผู้ให้บริการจะส่งสัญญาณ ACK เพื่อตอบรับการเชื่อมต่อที่ร้องขอมา จึงสามารถรับส่งข้อมูลกันได้ ดังรูปที่ 2.2

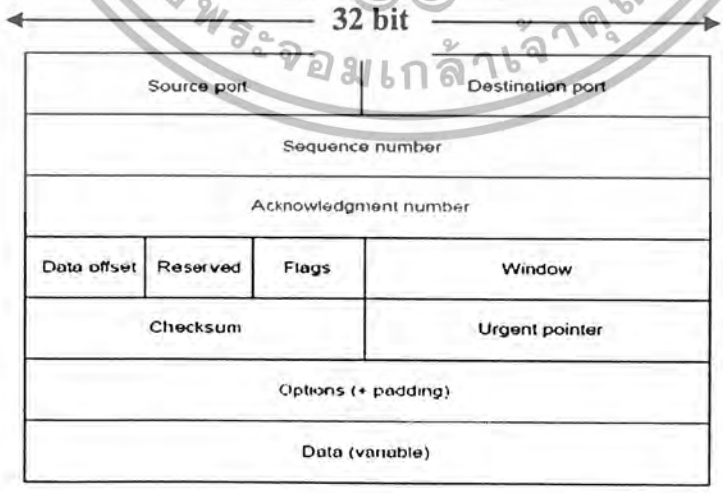


รูปที่ 2.2 แสดงการทำ 3-way Handshake

การเชื่อมต่อแบบ 3-way handshake นี้ เป็นการตรวจสอบความพร้อมของทั้งฝ่ายส่งและฝ่ายรับ และการกำหนดค่าเริ่มต้นของพารามิเตอร์ต่างๆ ของทั้งสองฝ่ายให้ตรงกัน หลังจากกระบวนการทำ 3-way handshake สิ้นสุด ทั้งสองฝ่ายจึงสามารถรับและส่งข้อมูลซึ่งกันและกันได้

ดังนั้นโพรโตคอลทีซีพีจึงเป็นโพรโตคอลที่มีการรับส่งข้อมูลแบบคอนเน็คชั่นโอเรียนเท็ด (Connection Oriented) ทำให้การทำงานของทีซีพีมีความน่าเชื่อถือมากขึ้น หน้าที่การทำงานของทีซีพีในการรับส่งข้อมูลมีหน้าที่หลัก 6 ข้อคือ

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



รูปที่ 2.3 แสดงชั้นของโพรโตคอลทีซีพี

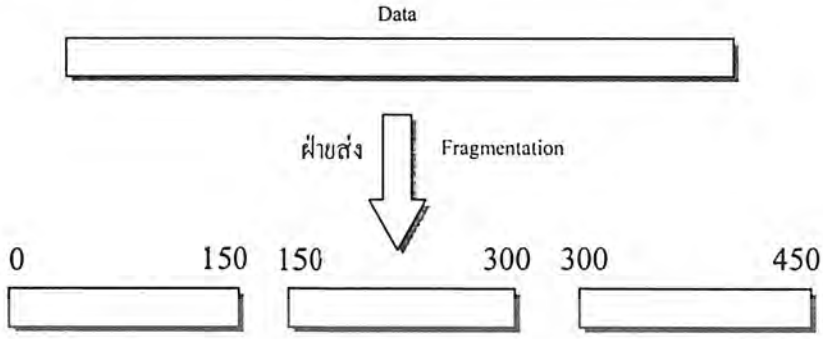
1. Source port(16 bit) เป็นหมายเลขพอร์ตของผู้ส่ง
2. Destination port(16 bit) เป็นหมายเลขพอร์ตของผู้รับ
3. Sequence number(32 bit) เป็นฟิลด์ที่ระบุหมายเลขลำดับอ้างอิงในการสื่อสารข้อมูลแต่ละครั้งเพื่อใช้ในการแยกแยะว่าเป็นข้อมูลชุดใดและนำมาจัดลำดับได้ถูกต้อง
4. Acknowledgment number(32 bit) เป็นหมายเลขลำดับแพ็กเก็ตถัดไปที่ทางฝั่งรับคาดหวัง ซึ่งเป็นการบอกเป็นนัยว่าแพ็กเก็ตที่มีหมายเลขลำดับก่อนหน้านี้ได้รับหมดแล้วนั่นเอง
5. Data offset(4 bit) เป็นตัวเลขที่บอกขนาดของข้อมูลส่วนทีซีพี header ซึ่งมีหน่วยเป็น 32 บิต
6. Reserved(6 bit) ถูกกำหนดเป็น 0 ตลอด ซึ่งข้อมูลส่วนนี้ไม่มีความหมายอะไร แต่เป็นการสงวนไว้ใช้งานสำหรับอนาคต ซึ่งอาจมีการเปลี่ยนแปลงของแพ็กเก็ต
7. Flags(6 bit) เป็นข้อมูลที่บอกถึง ทีซีพี segment สำหรับควบคุมการรับส่งข้อมูล ได้แก่
   - URG : Urgent Pointer Field Significant - แสดง Urgent Pointer
   - ACK : Acknowledgement Field Significant – แสดงการ Acknowledgement
   - PSH : Push Function
   - RST : Reset The Connection - แสดงเมื่อรีเซ็ตการเชื่อมต่อ
   - SYN : Synchronize Sequence Number - หมายเลขแพ็กเก็ตที่ส่งแบบซิงโครนัส
   - FIN : No more data from sender - แสดงว่าไม่มีข้อมูลที่ส่งจากผู้ส่งแล้ว
8. Window(16 bit) เป็นตัวเลขที่บอกปลายทางให้ทราบขนาดของวินโดว์ในการรับส่งข้อมูล
9. Checksum(16 bit) เป็นข้อมูลที่ใช้ในการตรวจสอบความผิดพลาดของข้อมูลในส่วนหัว
10. Urgent pointer(16 bit) ระบุ sequence number ของทีซีพี segment ล่าสุดที่อยู่ในโหมด urgent
11. Padding (variable) เป็นข้อมูลที่เพิ่มเข้าไปเพื่อให้ข้อมูลส่วนหัวมีจำนวนบิตที่หารด้วย 32 ลงตัว

2.1.3 ไอพี (IP)

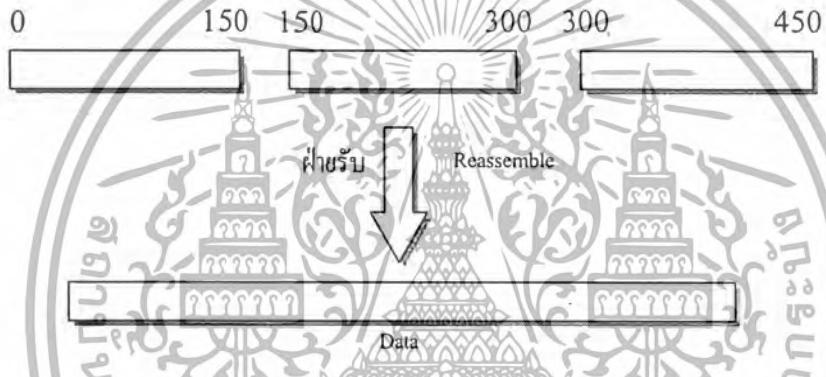
โพรโตคอลไอพี (IP – Internet Protocol) เป็นโพรโตคอลที่จัดการเกี่ยวกับแอดเดรสของแต่ละแพ็กเก็ต เพื่อให้ส่งแพ็กเก็ตต่างๆ ไปยังเป้าหมายได้ถูกต้อง การทำงานของไอพีเป็นเพียงการส่งข้อมูลไปยังเครื่องเป้าหมายเท่านั้น ไม่มีการส่งสัญญาณขอบริการ หรือสัญญาณให้บริการระหว่างกันเหมือนทีซีพี เรียกว่าการเชื่อมต่อแบบคอนเน็กชั่นเลส ซึ่งระบบทั้งสองตั้งสมมติฐานว่าการเชื่อมต่อระหว่างกันไม่มีความผิดพลาดเกิดขึ้นแน่

เนื่องจากมาตรฐานในเครือข่ายมีหลากหลาย ขนาดของแพ็กเก็ตในแต่ละมาตรฐานจึงมีความแตกต่างกันออกไป ทำให้การส่งข้อมูลระหว่างอุปกรณ์ในเครือข่ายนั้นอาจมีการแบ่งข้อมูลออกเป็นแพ็กเก็ตย่อยๆ ในระหว่างการส่ง เรียกว่า การทำแฟร็กเมนเตชั่น (Fragmentation) เช่น แพ็กเก็ตของ FDDI มีขนาด 4,500 ไบต์ หากเครื่องปลายขอยู่ในเครือข่ายอีเทอร์เน็ต ซึ่งมีขนาดของแพ็กเก็ตสูงสุดเพียง 1,500 ไบต์ ดังนั้นการส่งแพ็กเก็ตไปยังเครื่องปลายทางจึงต้องมีการแบ่งเป็นแพ็กเก็ตย่อย และเมื่อแพ็กเก็ตย่อยมาถึง

เครื่องเป้าหมายก็จะมารวมกันเป็นแพ็กเก็ตเดิมที่มีขนาด 4,500 ไบต์อีกครั้ง เรียกการรวมกันนี้ว่า การรีแอสเซมเบิ้ล (Reassemble) ซึ่งทำให้ได้ข้อมูลเหมือนที่ส่งมาจากเครื่องต้นทาง



รูปที่ 2.4 แสดงการทำแฟร็กเมนเตชั่น



รูปที่ 2.5 แสดงการรีแอสเซมเบิ้ล

<u>ส่วนประกอบของแพ็กเก็ตไอพี</u>

1. version : เป็นค่าตัวเลข 4 บิต บอกเวอร์ชันของมาตรฐานไอพีที่ใช้ โดยปกติมีค่าเป็น 4 ซึ่งหมายถึง IPv4
2. Internet Header Length (IHL) : เป็นตัวบอกความยาวเฮดเดอร์ของไอพี
   Type of Service : เป็นส่วนที่บอกการทำงานของแพ็กเก็ตที่ส่งว่าทำหน้าที่อะไร มีทั้งหมด 8 บิต
3. Total Length : มีขนาด 16 บิต บอกถึงความยาวในดาต้าแกรมของไอพี
4. Identification field : เป็นตัวเลข 16 บิต เป็นค่าประจำตัวของไอพีนั้น โดยโฮสต์ที่ส่งเป็นผู้กำหนด และเพิ่มค่าขึ้นหนึ่งเมื่อมีการส่งดาต้าแกรมของไอพีใหม่ ซึ่งใช้ในการประกอบกลับ
5. Flag : เป็นตัวเลข 3 bit บอกลักษณะของแพ็กเก็ตว่ามีการแฟร็กเมนต์หรือไม่
   Bit 0 : สงวนไว้ ปกติเป็น 0
   Bit 1 : 0 = บอกว่าแพ็กเก็ตมีการแตกแพ็กเก็ตย่อย
   1 = บอกว่าแพ็กเก็ตไม่มีการแตกแพ็กเก็ตย่อย

Bit 2 : 0 = บอกว่าแพ็กเก็ตนั้นเป็นแพ็กเก็ตสุดท้ายที่ได้จากการแตกแพ็กเก็ตย่อย

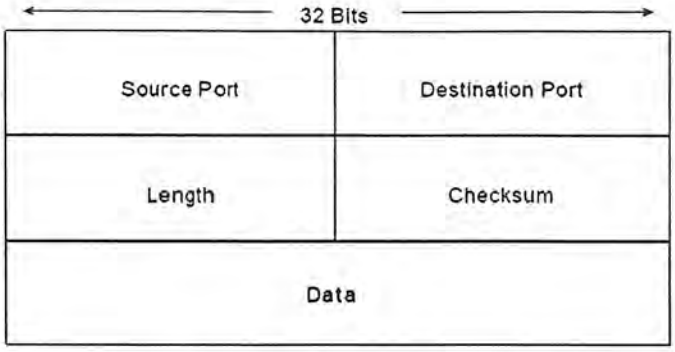
1 = บอกว่าแพ็กเก็ตนั้นยังไม่ใช่แพ็กเก็ตสุดท้ายที่ได้จากการแตกแพ็กเก็ตย่อย

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

รูปที่ 2.6 แสดงชั้นของโพรโตคอลไอพี

2.1.4 ยูดีพี (UDP)

ยูดีพี (UDP - User Datagram Protocol) เป็นโพรโตคอลที่อยู่ใน เลเยอร์เดียวกันกับทีซีพีนั่นคือ ทรานสปอร์ตเลเยอร์ ส่งข้อมูลครั้งละ 1 ชุด เรียกว่า ยูดีพีดาต้าแกรม (UDP datagram) เน้นความเร็วในการส่งโดยไม่มีกลไกการตรวจสอบความสำเร็จในการรับส่งข้อมูล จึงเป็นการรับส่งข้อมูลแบบคอนเน็คชั่นเลส เมื่อมีความผิดพลาดที่เกิดขึ้นระหว่างการส่งข้อมูล จะไม่มีการแจ้งกลับผู้ส่ง เพื่อให้ส่งข้อมูลซ้ำ แต่จะยกเลิกข้อมูลนั้นทิ้ง นอกจากนี้ ยูดีพียังไม่ให้บริการ Flow control และไม่มีการรับประกันในเรื่องของเวลาในการส่งและไม่รับประกันเรื่องแบนด์วิดธ์



รูปที่ 2.7 แสดงชั้นของโพรโตคอลยูดีพี

Source Port(16 บิต) เป็นหมายเลขไอพีต้นทางของผู้ส่ง

Destination Port(16 บิต) เป็นหมายเลขไอพี ปลายทางที่รับดาต้าแกรม

Length(16 บิต) ระบุความยาวทั้งหมดของดาต้าแกรม

Checksum(16 บิต) ตรวจสอบความถูกต้องของข้อมูลในดาต้าแกรม

2.1.5 โพรโตคอลเออาร์พี (ARP)

โพรโตคอลเออาร์พี (ARP - Address Resolution Protocol) เป็นโพรโตคอลที่ออกแบบมา เพื่อใช้ในเครือข่ายที่สนับสนุนการบอร์ดคาสต์ถูกเรียกใช้งานโดยโพรโตคอลไอพี เพื่อช่วยแปลงหมายเลขไอพีไปเป็นหมายเลขฮาร์ดแวร์ปลายทาง เช่น เว็บเซิร์ฟเวอร์เครื่องหนึ่งเชื่อมต่ออยู่ในเครือข่ายอินเทอร์เน็ต และในการเชื่อมต่อนี้ต้องอาศัยการ์ดแลน(LAN card) ติดตั้งอยู่ ที่แลนการ์ดนี้จะมีหมายเลขเฉพาะประจำฮาร์ดแวร์ที่ไม่ซ้ำกับใคร เพื่อใช้อ้างอิงการส่งข้อมูลในเครือข่าย แต่เมื่อมาใช้งานใน โพรโตคอลทีซีพี/ไอพี ก็ต้องมีการกำหนดหมายเลขแอดเดรสไอพี ประจำตัวเพื่อใช้อ้างอิงกัน และโพรโตคอลเออาร์พี จะทำหน้าที่แปลงค่าหมายเลขไอพีให้เป็นหมายเลขฮาร์ดแวร์จริงในระดับการทำงานที่ชั้นอินเทอร์เน็ตนี้ ซึ่งกลไกการแปลงนี้เรียกว่า แอดเดรสรีโซลูชัน (address resolution)

Header	ARP/RARP datagram	FCS

hardware		protocol
HLEN	PLEN	operation
Sender HA (octets 0-3)		
Sender HA (octets 4-5)		Sender IA (octets 0-1)
Sender IA (octets 2-3)		Target HA (octets 0-1)
Target HA (octets 2-5)		
Target IA (octets 0-3)		

รูปที่ 2.8 เออาร์พีดาต้าแกรม

ส่วนประกอบของเออาร์พีดาต้าแกรม

1. Hardware 16 บิต : กำหนดชนิดของฮาร์ดแวร์เครือข่ายที่เออาร์พีทำงานอยู่ ค่าใช้งานมีตัวอย่างดังต่อไปนี้

1 อีเทอร์เน็ต

4 โทเค็นริง

5 เคออส(chaos)

6 เครือข่าย IEEE 802

7 อาร์คเน็ต

12 โลคัลทอล์ค

2. protocol 16 บิต : ชนิดของโพรโตคอลที่ร้องขอใช้เออาร์พี

3. HLEN 8 บิต : ขนาดของฮาร์ดแวร์แอดเดรสเป็นจำนวนไบต์ ค่าปกติที่ใช้งาน คือ 6 ซึ่งเท่ากับขนาด 6 ไบต์ของอีเทอร์เน็ตฮาร์ดแวร์แอดเดรส

4. PLEN 8 บิต : ขนาดของแอดเดรสระดับเน็ตเวิร์กเป็นจำนวนไบต์ ค่าปกติที่ใช้ คือ 4 ซึ่งเท่ากับขนาด 4 ไบต์ของไอพีแอดเดรส

5. Operation 16 บิต : กำหนดรูปแบบการใช้ดาทาแกรม ค่าในฟิลด์นี้ใช้กำหนดการทำงานของทั้งเออาร์พีและอาร์เออาร์พี ซึ่งมี 4 ค่า คือ

ARP request (ค่าเท่ากับ 1)

ARP reply (ค่าเท่ากับ 2)

RARP request (ค่าเท่ากับ 3)

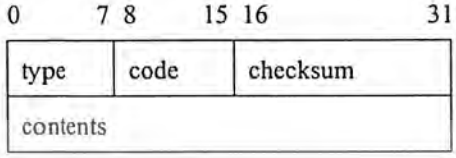
RARP reply (ค่าเท่ากับ 4)

6. Address : ฟิลด์แอดเดรสเรียงลำดับจากฮาร์ดแวร์และเน็ตเวิร์กแอดเดรสของสถานีที่ร้องขอตามด้วยฮาร์ดแวร์และเน็ตเวิร์กแอดเดรสของสถานีที่ตอบรับ

2.1.6 โพรโตคอล ไอซีเอ็มพี (ICMP)

โพรโตคอลไอซีเอ็มพี (ICMP : Internet Control Message Protocol) มีหน้าที่หลักของอยู่คือ การแจ้งหรือแสดงข้อความจากระบบ เพื่อบอกให้ผู้ใช้ทราบว่าเกิดอะไรขึ้นในการส่งผ่านข้อมูลนั้น ซึ่งปัญหาส่วนมากที่พบ คือส่งไปไม่ได้ หรือปลายทางรับข้อมูลไม่ได้ เป็นต้น นอกจากนี้โพรโตคอลไอซีเอ็มพียังถูกเรียกใช้งานจากเครื่องเซิร์ฟเวอร์ และเราเตอร์ อีกด้วย เพื่อแลกเปลี่ยนข้อมูลที่ใช้ควบคุม ส่วนรูปแบบการทำงานของโพรโตคอลไอซีเอ็มพีนั้นจะทำงานควบคู่กับโพรโตคอลไอพีในระดับเดียวกัน และข้อความต่างๆที่แจ้งให้ทราบจะถูกผนึกอยู่ภายในข้อมูลของไอพีอีกทีหนึ่ง ข้อความที่โพรโตคอลไอซีเอ็มพีส่งนั้น แบ่งออกได้ 2 แบบ คือ ไอซีเอ็มพีเออร์เรอร์เมสเซจ (ICMP error message) หรือข้อความแจ้งข้อผิดพลาด และ ไอซีเอ็มพีคิวรี่ (ICMP query) หรือข้อความเรียกขอข้อมูลเพิ่ม ตัวอย่างกลไกการทำงานของโพรโตคอลไอซีเอ็มพี เช่น เมื่อมีการส่งผ่านข้อมูลจากผู้ใช้ไปยังปลายทางที่ไม่ถูกต้อง หรือขณะนั้นเครื่องปลายทางเกิดปัญหาจนไม่สามารถรับข้อมูลได้ที่เราเตอร์จะส่งข้อความแจ้งเป็น ไอซีเอ็มพี

เมสเซจ (ICMP message) ที่ชื่อ เดสซิเนชั่นอันริชเชเบิ้ล (destination unreachable) ให้กับผู้ส่งข้อมูล นอกจากนี้ตัว ข้อมูลที่แจ้งข้อความก็จะมีส่วนของข้อมูลไอพีดาทาแกรมที่เกิดปัญหาด้วย ดังนั้นเมื่อผู้ส่งข้อมูลได้รับข้อความแจ้งแล้วก็จะได้ทราบว่าจุดที่เกิดปัญหานั้นอยู่ที่ใด ดังนั้นโพรโตคอลไอซีเอ็มพี จึงกลายมาเป็นเครื่องมืออย่างหนึ่งในการช่วยทดสอบเครือข่าย ยกตัวอย่างเช่น คำสั่งปิงที่เรามักใช้ทดสอบว่าเครื่องเซิร์ฟเวอร์ที่ให้บริการหรืออุปกรณ์ที่ต่ออยู่ในเครือข่าย อินเทอร์เน็ตนั้นยังทำงานเป็นปกติหรือไม่ แล้วคำสั่งปิงมีการเรียกใช้งานโพรโตคอล ไอซีเอ็มพี แจ้งเป็นข้อความให้ทราบอีกต่อหนึ่ง



รูปที่ 2.9 ฟอร์แมตของ ไอซีเอ็มพี

1. Type ขนาด 8 บิต : กำหนดค่าความผิดพลาดและการรายงานสถานะ การใช้งานในปัจจุบันมีทั้งหมด 15 ประเภท
2. code ขนาด 8 บิต : รหัสความผิดพลาดย่อย
3. Checksum ขนาด 16 บิต : ค่าผลรวมตรวจสอบแบบ 1's complement สำหรับใช้ตรวจสอบความผิดพลาด โดยคำนวณผลรวมของ type,code และ contents
4. Contents ขนาดไม่คงที่ : ฟิลด์นี้ใช้บรรจุข้อมูลข่าวสารเพิ่มเติมเพื่อแจ้งกลับซึ่งจะขึ้นอยู่กับค่า typeและ code

ICMP Type	Code	Description
0	0	Echo reply (to ping)
3	0	Destination network unreachable
3	1	Destination host unreachable
9	2	Destination protocol unreachable
3	3	Destination port unreachable
3	6	Destination network unknown
3	7	Destination host unknown
4	0	Source quench (congestion control)
8	0	Echo request
9	0	Router advertisement
10	0	Router discovery
11	0	TTL expired
12	0	IP header bad

ตารางที่ 2.2 แสดงตัวอย่างความหมายของชนิด (type) และรหัส (code) ของไอซีเอ็มพี (ICMP)

2.1.7 พอร์ต (Port)

พอร์ต (Prot) คือข้อมูลหมายเลขระดับชั้นทีซีพี ขนาด 16 บิตที่อ้างอิงถึง แอพพลิเคชั่นเลเยอร์ ในการสื่อสารเพื่อให้ส่งข้อมูลไปยัง แอพพลิเคชั่นเลเยอร์ ที่ถูกต้อง ไม่ใช่พอร์ตให้ที่โมเดม (modem) หรือ พริ้นเตอร์ (printer) เสียบหลังเครื่องคอมพิวเตอร์ แต่พอร์ต ในที่นี้ก็คือหมายเลขที่ใช้อ้างอิงเปรียบเทียบให้รู้กันเท่านั้นว่าจะใช้บริการอะไร ซึ่งแต่ละอย่างต่างกันที่ตัวเลขที่บอกมา ดังนั้น ในเซิร์ฟเวอร์หนึ่งๆ จึงสามารถเปิดให้บริการได้หลายๆ อย่าง โดยการสื่อสารมาที่ชื่อเซิร์ฟเวอร์ที่กำหนดไว้ชื่อเดียว แต่เวลาติดต่อเข้ามาจะต้องบอกด้วยว่าเข้ามาพอร์ตไหน ซึ่งเป็นกฎที่รู้กัน เช่น ต้องบอกด้วยว่าเชื่อมต่อไปยังเซิร์ฟเวอร์ไปที่พอร์ต หมายเลข 21 (FTP server) ถ้าเซิร์ฟเวอร์นั้นเปิดให้บริการที่พอร์ต 21 ก็จะใช้บริการได้ แต่ถ้าไม่ได้เปิดให้ใช้ ก็เกิดการสื่อสารไม่ได้นั่นเอง พอร์ตที่ใช้กันโดย มากจะมีมาตรฐานกำกับในตัววิธีการสื่อสารในโพรโตคอล ตัวนั้น ๆ ที่ให้บริการ ซึ่งมีกำหนดมาตรฐานเอาไว้เป็นเลขเดียวกัน

PORT	COMMON PROTOCOL	SERVICE	PORT	COMMON PROTOCOL	SERVICE
7	TCP	echo	80	TCP	http
9	TCP	discard	110	TCP	pop3
13	TCP	daytime	111	TCP	sunrpc
19	TCP	chargen	119	TCP	mtp
20	TCP	ftp-control	123	UDP	ntp
21	TCP	ftp-data	137	UDP	netbios-ns
23	TCP	telnet	138	UDP	netbios-dgm
25	TCP	smtp	139	TCP	netbios-ssn
37	UDP	time	143	TCP	imap
43	TCP	whois	161	UDP	snmp
53	TCP/UDP	dns	162	UDP	snmp-trap
67	UDP	bootps	179	TCP	bgp
PORT	COMMON PROTOCOL	SERVICE	PORT	COMMON PROTOCOL	SERVICE
68	UDP	bootpc	443	TCP	https (http/ssl)
69	UDP	tftp	520	UDP	rip
70	TCP	gcpher	1080	TCP	socks
79	TCP	Finger	33434	UDP	traceroute

ตารางที่ 2.3 แสดงตัวอย่างหมายเลขพอร์ตของบริการต่าง ๆ

2.2 ระบบตรวจจับผู้บุกรุกเครือข่าย (Intrusion Detection System – IDS)

ระบบตรวจจับผู้บุกรุก (IDS - Intrusion Detection System) เป็นระบบจัดการความปลอดภัยสำหรับคอมพิวเตอร์ และเครือข่ายที่พยายามตรวจหา และเตือนภัยเมื่อมีความพยายามในการบุกรุกเข้ามาในระบบ หรือ เครือข่าย เป็นอีกเครื่องมือหนึ่งที่ใช้กันอย่างมาก และมีความสำคัญอย่างยิ่งในปัจจุบัน ถึงแม้ว่าเครือข่ายอาจมรการการป้องกันการบุกรุกอยู่แล้ว โดยใช้ไฟร์วอลล์ (Fire wall) อย่างไรก็ตาม ไฟร์วอลล์ก็ยังไม่ใช่เครื่องมือที่จะป้องกันการบุกรุกได้โดยอัตโนมัติ จะต้องอาศัยผู้ที่บริหารที่กำหนดกฎให้เหมาะสมกับการใช้งาน และแม้จะมีกฎที่ดีแล้ว แต่ก็อาจไม่สามรถป้องกันการบุกรุกได้ การบริหารไฟร์วอลล์ที่ดีก็ควรจะมีการตรวจสอบข้อนหลัง และทดสอบการเจาะระบบเพื่อเป็นการทดสอบระบบอีกครั้ง ซึ่งตรงจุดนี้ ระบบตรวจจับผู้บุกรุกจะช่วยได้มาก เพื่อตรวจสอบแพ็กเก็ตต่างๆที่ผ่านเข้ามา ถ้าตรวจพบการบุกรุก ผู้บริหารก็สามารถนำข้อมูลที่ได้ไปปรับปรุงกฎให้รัดกุมยิ่งขึ้น

ดังนั้น ระบบตรวจจับการบุกรุก (Intrusion Detection System – IDS) ก็คือระบบที่ประกอบด้วยฮาร์ดแวร์และซอฟต์แวร์สำหรับทำหน้าที่ตรวจจับการบุกรุก (Intrusion Detection) ซึ่งเปรียบเสมือนยามคอยตรวจตราความเป็นไปและพฤติกรรมของข้อมูล ที่ผ่านมาในเน็ตเวิร์คว่ามีความน่าสงสัยหรือมีสิ่งผิดปกติหรือไม่ นั่นเอง

2.2.1 รูปแบบของระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์

มี วิธีหลักๆ ในการป้องกันผู้บุกรุก 2 วิธี คือ

1. วิธีตรวจสอบการใช้งานระบบที่ผิดปกติ (Anomaly Intrusion Detection)

วิธีตรวจสอบการใช้งานทรัพยากรระบบที่ผิดปกติตั้งอยู่บนสมมุติฐานว่าการกระทำใดๆ ที่เป็นการบุกรุกจะต้องมีการใช้งานระบบอย่างผิดปกติ โดยมีการกระบวนการเก็บประวัติพฤติกรรมการใช้งานของผู้ใช้ และสังเกตการทำงานเกิดขึ้นของผู้ใช้ว่าเมื่อเข้ามาในระบบได้กระทำสิ่งใดบ้างแล้วรายงานเก็บประวัติซึ่งสามารถใช้เป็นข้อมูลตรวจสอบในการนำมาเปรียบเทียบว่าพฤติกรรม ในปัจจุบันมีการใช้งานระบบที่ผิดปกติกว่าประวัติพฤติกรรมของผู้ใช้เดิมมากน้อยเพียงใด หากมีการใช้ในปริมาณมากผิดปกติจึงถือว่าเกิดการบุกรุก

ข้อเสียของการตรวจจับโดยวิธีตรวจสอบใช้งานระบบที่ผิดปกติ คือ

- อาจมีพฤติกรรมการใช้งานทรัพยากรระบบของผู้ใช้ที่ผิดปกติเกิดขึ้นแต่ไม่ได้เป็นการบุกรุกระบบ ทำให้ระบุสถานะผิดพลาด
- ตรวจไม่พบการบุกรุกระบบเนื่องจากการบุกรุกนั้นไม่ได้ใช้ทรัพยากรระบบอย่างผิดกติ
- หากผู้บุกรุกค่อยๆ เปลี่ยนพฤติกรรมการใช้งานไปทีละเล็กละน้อย ระบบจะไม่สามารถตรวจจับความผิดปกติได้

2. วิธีการตรวจสอบกับข้อกำหนดการใช้งาน (Signature Intrusion Detection)

การตรวจสอบกับข้อกำหนดการใช้งาน (Signature Intrusion Detection) ประกอบด้วยการเก็บบันทึกและการระบุรูปแบบการบุกรุกซึ่งอาจบุกรุกจากจุดอ่อนของระบบ หรือละเมิดกฎรักษาความปลอดภัย โดยมีตรวจจับคอยดูแลกิจกรรมต่างๆ ที่กระทำในปัจจุบันว่าพฤติกรรมการบุกรุกที่เคยเกิดขึ้นหรือได้รับรายงานว่าเป็นการบุกรุกหรือไม่ ในบางระบบมีการใช้กฎ (Rule-based expert system) โดยตั้ง

กฎขึ้นจากพฤติกรรมที่น่าสงสัย เช่น การ login ล้มเหลวเกินกว่า 3 ครั้งต่อเนื่องกัน ในเวลา 5 นาที ถือว่าพยายามบุกรุก และข้อมูลที่ใช้ตรวจสอบจะถูกนำมาเปรียบเทียบกับกฎ (Rules) ที่มีอยู่สังเกตว่ามีการนำข้อมูลทางเวลาเข้ามาพิจารณาด้วย การตรวจจับการบุกรุกโดยวิธีนี้สามารถมีการแก้ไขกฎหรือเพิ่มกฎได้ในระบบที่เป็นปัญญาประดิษฐ์ (Artificial Intelligence) ระบบอาจทำการแก้ไขกฎหรือเพิ่มกฎได้ด้วยตนเอง

ข้อเสียของวิธีการตรวจสอบกับข้อกำหนดการใช้งาน และตรวจสอบจากสถิติการใช้งานของระบบ (Signature Intrusion Detection) คือ

1. ประสิทธิภาพของระบบตรวจจับชนิดนี้ ขึ้นอยู่กับความยากในการรวบรวมข้อมูลเกี่ยวกับรูปแบบการโจมตี และการปรับปรุงข้อมูลเกี่ยวกับช่องโหว่ต่างๆ ให้ทันสมัยอยู่เสมอ เนื่องจากข้อมูลต่างๆ นั้นขึ้นอยู่กับระบบปฏิบัติการ, เวอร์ชั่น และ แอพพลิเคชั่น นอกจากชั้นการตรวจจับการโจมตีจากภายในนั้นทำได้ยากเนื่องจาก การโจมตีจากภายในเกี่ยวกับการละเมิดสิทธิของผู้ใช้งาน (user) ซึ่งไม่ได้เกี่ยวข้องกับช่องโหว่แต่อย่างใด

2. มีข้อจำกัดในเรื่องจำนวนของรูปแบบในการบุกรุก ซึ่งหากเป็นการบุกรุกที่ระบบไม่รู้จักมาก่อนจะทำให้ไม่สามารถตรวจจับการบุกรุกได้

2.2.2 ประเภทของระบบการตรวจจับผู้บุกรุก

ระบบตรวจจับผู้บุกรุก แบ่งเป็น 2 ประเภท คือ

1. ระบบตรวจจับผู้บุกรุกในโฮสต์ (Host-based Intrusion Detection System)

ระบบตรวจจับผู้บุกรุกในโฮสต์ (Host-based Intrusion Detection System) เป็นซอฟต์แวร์ที่ประมวลผลบนโฮสต์ โดยปกติแล้วระบบตรวจจับผู้บุกรุกประเภทนี้จะวิเคราะห์ล็อก (Log) เพื่อค้นหาข้อมูลเกี่ยวกับการบุกรุก ในระบบยูนิกซ์นั้นล็อกที่ระบบตรวจจับผู้บุกรุกจะตรวจสอบ ส่วนในวินโดวส์นั้นระบบตรวจจับผู้บุกรุกก็จะตรวจสอบอีเวนต์ล็อกต่างๆ เช่น ระบบ, แอพพลิเคชั่นและความปลอดภัย (Security) เป็นต้น โดยปกติระบบตรวจจับผู้บุกรุกจะอ่านเหตุการณ์ใหม่ที่เกิดขึ้นในล็อกและเปรียบเทียบกับกฎที่ตั้งไว้ก่อนหน้า ถ้าตรงก็จะแจ้งเตือนทันที ดังนั้นการที่ ระบบตรวจจับผู้บุกรุกจะตรวจจับการบุกรุกได้ระบบจะต้องบันทึกเหตุการณ์ต่างๆที่สำคัญที่เกิดขึ้นในระบบล็อกไฟล์ ถ้าไม่เช่นนั้น IDS ก็ไม่มีข้อมูลที่จะใช้วิเคราะห์ว่ามีการบุกรุกหรือไม่

นอกจากการตรวจสอบล็อกไฟล์แล้ว ระบบตรวจจับผู้บุกรุกบางชนิดสามารถตรวจสอบการเรียกใช้ฟังก์ชันของระบบปฏิบัติการ (System Call) ซึ่งถ้าเหตุการณ์คล้ายหรือตรงกับการบุกรุกระบบตรวจจับผู้บุกรุกก็จะแจ้งเตือน นอกจากนี้ ระบบตรวจจับผู้บุกรุก ยังสามารถตรวจสอบการแก้ไขไฟล์ในระบบได้ด้วย ซึ่งอาจทำได้โดยการตรวจสอบวันที่ที่แก้ไขครั้งสุดท้ายและขนาดของไฟล์ เป็นต้น วิธีที่แน่นอนกว่าคือ วิธีเช็คซัม (Check Sum) ของไฟล์แล้วเก็บไว้เพื่อเปรียบเทียบเมื่อมีการตรวจสอบความคงสภาพของไฟล์ในระบบ โดยเมื่อการคำนวณเช็คซัมใหม่แล้วค่าที่ได้ไม่ตรงกับค่าเดิมก็แสดงว่าไฟล์ได้ถูกแก้ไข

ข้อได้เปรียบของระบบตรวจจับผู้บุกรุกในโฮสต์ เช่น

- ระบบตรวจจับผู้บุกรุกในโฮสต์สามารถตรวจพบทุกการบุกรุกกับโฮสต์นั้นๆ ได้เสมอถ้าระบบสามารถบันทึกเหตุการณ์ดังกล่าวในล็อกได้ หรือการบุกรุกมีการเรียกใช้ซิสเท็มคอล

- ระบบตรวจจับผู้บุกรุกในโฮสต์สามารถบอกได้ว่าการบุกรุกนั้นสำเร็จหรือไม่ โดยการวิเคราะห์ข้อความในล็อกหรือจากหลักฐานอื่นๆ เช่น มีการแก้ไขไฟล์ที่สำคัญของระบบ เป็นต้น

- ระบบตรวจจับผู้บุกรุกในโฮสต์สามารถบ่งชี้ได้ว่า มีการเข้าใช้ระบบอย่างผิดปกติโดยผู้ใช้ของระบบเอง

ข้อเสียเปรียบของระบบตรวจจับผู้บุกรุกในโฮสต์คือ

- โพรเซสของระบบตรวจจับผู้บุกรุกอาจถูกโจมตีจนอาจไม่สามารถแจ้งเตือนได้

- ระบบตรวจจับผู้บุกรุกในโฮสต์จะแจ้งเตือน ก็เมื่อ เหตุการณ์ที่เกิดขึ้นนั้นตรงกับที่กำหนดไว้ก่อนหน้า ถ้าผู้บุกรุกมีเทคนิคใหม่ ๆ ระบบตรวจจับผู้บุกรุกอาจไม่แจ้งเตือนการบุกรุกก็ได้

- การทำงานของระบบตรวจจับผู้บุกรุกในโฮสต์ อาจมีผลกระทบต่อประสิทธิภาพของโฮสต์เอง เนื่องจากต้องตรวจสอบล็อกไฟล์และซิสเต็มคอลล์

2. ระบบตรวจจับผู้บุกรุกเครือข่าย (Network Intrusion Detection System)

ระบบตรวจจับผู้บุกรุกเครือข่าย (Network Intrusion Detection System หรือ NIDS) เป็นแขนงหนึ่งของระบบตรวจจับผู้บุกรุก (Intrusion Detection System หรือ IDS) โดยเน้นไปทางการตรวจจับทางเครือข่ายคอมพิวเตอร์เป็นหลักซึ่งก็หมายความว่าการตรวจสอบนั้นจะครอบคลุมทั้งเครือข่าย

โดยทั่วไปแล้วระบบตรวจจับผู้บุกรุกเครือข่ายนี้จะถูกติดตั้งบนเครื่องเดียว แต่ตรวจสอบและวิเคราะห์แพ็กเก็ตทั้งระบบเครือข่าย โดยจะต้องทำการติดตั้งระบบที่ใช้ฮับในการเชื่อมต่อ เพื่อที่จะสามารถรับข้อมูลทั้งหมดในช่องทางการสื่อสารได้ ถ้าเราติดตั้งระบบนี้บนสวิตช์ เราจะรับข้อมูลได้เฉพาะของเครื่องเราเท่านั้น ซึ่งก็จะทำไม่ให้ประสิทธิภาพ

2.2.3 หลักการทำงานพื้นฐานของระบบตรวจจับผู้บุกรุกแบบทางเครือข่าย

ระบบตรวจจับผู้บุกรุกเครือข่าย ทำงานโดยการนำแหล่งข้อมูลมาจากเครือข่าย และนำข้อมูลแพ็กเก็ตเหล่านั้นมาวิเคราะห์และเมื่อตรวจพบลักษณะที่ตรงกับข้อมูลที่จัดว่าเป็นการบุกรุกอยู่ก็จัดการตามที่ตั้งไว้ต่อไปซึ่งอาจจะเป็นการเก็บข้อมูลลงล็อกไฟล์ (log file) หรือการแสดงข้อความเตือนผู้ดูแลระบบ ซึ่งในส่วนของการที่ได้ข้อมูลมานั้น จะใช้หลักการของเครื่องมือ แพ็กเก็ตสนิฟเฟอร์ (Packet Sniffer) เป็นการดักจับแพ็กเก็ตที่ผ่านมาในเครือข่ายที่อยู่ในแชร์โดเมน (share domain) เดียวกัน

การที่แพ็กเก็ตสนิฟเฟอร์สามารถดักอ่านข้อมูลที่อยู่บนเน็ตเวิร์คได้นั้นมีสาเหตุที่สำคัญ คือ ด้วยลักษณะของโพรโตคอลอีเทอร์เน็ตที่ใช้หลักการกระจายของข้อมูล ไปยังทุกโฮสต์ที่อยู่ในเน็ตเวิร์ค และอาศัยโฮสต์แต่ละตัวทำหน้าที่จำแนกการสื่อสารของตนเอง นั่นหมายความว่าข้อมูลทุกแพ็กเก็ตที่ใช้สื่อสารกันนั้นได้ถูกส่งไปยังโฮสต์ทุกตัว ซึ่งจะได้รับพร้อมกันและเหมือนกัน เพียงแต่การที่สื่อสารกันได้อย่างถูกต้อง นั้นโฮสต์แต่ละตัวจะต้องมีกระบวนการที่สามารถรู้ได้ว่าข้อมูลแพ็กเก็ตใดเป็นของตัวเอง

และข้อมูลแพ็กเก็ตใดไม่ใช่ของตนเอง ทุกๆ แพ็กเก็ตที่กระจายลงบนเน็ตเวิร์คนั้นจะมีหมายเลขระบุชัดเจน คือ MAC Address หรือเรียกอีกอย่างหนึ่งว่า อีเทอร์เน็ตแอดเดรส (Ethernet Address) ซึ่งเป็นสิ่งที่บอกว่าแพ็กเก็ตมาจากฮาร์ดแวร์ใดในเน็ตเวิร์ค ทำให้สามารถระบุได้ว่าแพ็กเก็ตนั้นส่งมาจากโฮสต์ใด และต้องการส่งให้โฮสต์ใด

แมคแอดเดรส (MAC Address) จะเป็นหมายเลขเฉพาะตามฮาร์ดแวร์ทุกชนิดที่ใช้การสื่อสารโดยโพรโตคอลอีเทอร์เน็ต และในทางทฤษฎีแล้วฮาร์ดแวร์ทุกชนิดจะไม่มี แมคแอดเดรสที่ซ้ำกัน โดยทั่วไป แมคแอดเดรส จะถูกกำหนดตายตัวอยู่ในรอมของฮาร์ดแวร์และไม่สามารถเปลี่ยนแปลงได้ โดนซอฟแวร์ แต่เนื่องจาก การใช้งานของฮาร์ดแวร์นั้นต้องควบคู่ไปกับไดร์เวอร์ของฮาร์ดแวร์นั้นๆ ซึ่งโดยปกติแล้ว ไดร์เวอร์จะถูกกำหนดให้ปฏิบัติตามโพรโตคอลคือ

- ให้รับข้อมูลที่มี แมคแอดเดรส เป็นของตนเองเท่านั้น (ห้ามอ่านข้อมูลผู้อื่น)
- ให้ส่งข้อมูลโดยใช้ แมคแอดเดรส ของตนเองเท่านั้น (ห้ามปลอมเป็นผู้อื่น)

แต่ยังมีโหมดการทำงานที่อนุญาตฮาร์ดแวร์รับข้อมูลของผู้อื่นเข้ามาได้โดยไม่มีการปิดกั้นเรียกว่า โพรมิสคูอัสโหมด (Promiscuous Mode) เป็นโหมดที่ทำให้ ฮาร์ดแวร์อ่านข้อมูลดิบทั้งหมดบนเน็ตเวิร์ค เข้ามาในเครื่องคอมพิวเตอร์ของตนเอง ได้โดยไม่สนในว่าจะเป็นของใคร ส่งให้ใคร และเป็นการละเมิดข้อบังคับของโพรโตคอลหรือไม่

และเนื่องจาก ระบบตรวจจับผู้บุกรุกทางเครือข่ายทำงานโดยอาศัยหลักการนี้ ดังนั้นจึงทำให้เกิดข้อจำกัดในการใช้งาน คือ จะไม่สามารถตรวจจับนอกแชร์โดเมนของตัวเองได้ ดังนั้นถ้าเครือข่ายเป็นเครือข่ายที่ใช้สวิตช์ ระบบตรวจจับผู้บุกรุกจะไม่สามารถทำงานได้

2.2.4 การโจมตี

การโจมตีเครือข่ายหรือระบบนั้นควรให้ความสำคัญสูงสุด เมื่อระบบตรวจจับผู้บุกรุกรายงานเหตุการณ์นี้ ผู้ดูแลระบบตอบสนองกับเหตุการณ์นี้ทันทีเพื่อป้องกันการสูญเสียมากกว่านี้ บางครั้งระบบตรวจจับผู้บุกรุกอาจแยกแยะระหว่างการโจมตีจริงๆ กับการสแกนหาจุดอ่อน เนื่องจากเหตุการณ์ทั้งสองนั้นระบบตรวจจับผู้บุกรุก จะตรวจพบซิกเนเจอร์ของการโจมตีเหมือนกัน ผู้ดูแลระบบอาจต้องวิเคราะห์ข้อมูลเพิ่มเติม การสแกนหาจุดอ่อนนั้น ระบบตรวจจับผู้บุกรุกจะรายงานการโจมตีหลายๆรูปแบบในช่วงเวลาสั้นๆ กับระบบใดระบบหนึ่ง ส่วนการโจมตีจริงนั้นอาจมีการรายงานการโจมตีแค่รูปแบบเดียวกับระบบใดระบบหนึ่ง ซึ่งผู้จัดทำได้ทำการศึกษาการโจมตีลักษณะต่าง ๆ ดังนี้

2.2.4.1 การส่งแพ็กเก็ตจำนวนมาก (Amount of Packets Sending)

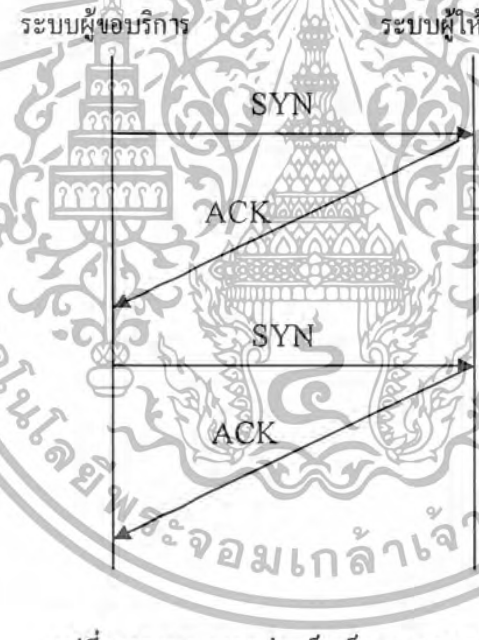
การโจมตีแบบนี้เป็นการส่งแพ็กเก็ตปริมาณมากเข้าไปยังระบบเป้าหมาย อาจทำให้ระบบเป้าหมายไม่สามารถให้บริการบางอย่าง หรือไม่สามารถทำงานต่อไปได้ ซึ่งแพ็กเก็ตที่ส่งออกไปนี้สามารถแบ่งออกได้เป็น

(1) แพ็กเก็ตข้อมูล (Data Packets)

การโจมตีวิธีนี้ทำได้โดยการส่งแพ็กเก็ตข้อมูลปริมาณมาก เมื่อข้อมูลเข้ามาสู่เครื่องเป้าหมายก็เก็บไว้ในบัฟเฟอร์ก่อนนำมาประมวลผลอีกครั้ง ดังนั้นหากส่งแพ็กเก็ตเข้ามาเป็นปริมาณมาก อาจทำให้บัฟเฟอร์ของเครื่องเป้าหมายไม่เพียงพอที่จะสามารถรองรับแพ็กเก็ตเหล่านั้นได้ทั้งหมด ซึ่งอาจทำให้เครื่องเป้าหมายให้บริการได้ช้าลง หรือต้องหยุดการให้บริการไปเลย

(2) แพ็กเก็ตสำหรับการควบคุม (Control Packets)

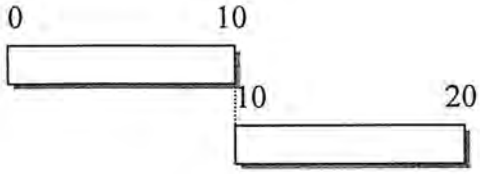
ตัวอย่างของการโจมตีแบบนี้ ได้แก่ การทำ SYN Flooding ปกติการเชื่อมต่อแบบ 3-way handshake เป็นไปตามลักษณะที่ได้อธิบายในหัวข้อ 2.3 แต่ในการโจมตีลักษณะนี้ใช้วิธีทำให้การทำ 3-way handshake ไม่สมบูรณ์ กล่าวคือ เครื่องที่ขอบริการส่งสัญญาณ SYN ไป แต่เมื่อได้รับสัญญาณ ACK จากเครื่องที่ให้บริการแล้ว ไม่ส่งสัญญาณ SYN ตอบกลับไป ทำให้เครื่องที่ให้บริการต้องเปิดการเชื่อมต่อรอการตอบกลับ ดังรูปที่ 2.10 ซึ่งการเปิดการเชื่อมต่อรอเอาไว้นี้ต้องใช้ทรัพยากรของระบบส่วนหนึ่ง และหากมีการส่งสัญญาณในลักษณะนี้มากๆ และทรัพยากรของระบบมีไม่เพียงพอ อาจทำให้ระบบไม่สามารถให้บริการอย่างอื่น หรือให้บริการกับผู้ร้องขอรายอื่นได้



รูปที่ 2.10 แสดงการส่งแพ็กเก็ตแบบ SYN Flood

2.2.4.2 ความผิดปกติของแฟร็กเมนต์ (Abnormal Fragmentation)

การโจมตีวิธีนี้อาศัยหลักการแฟร็กเมนเตชันและรีแอสเซมเบิ้ลที่กล่าวไว้ข้างต้น โดยทำให้แพ็กเก็ตนั้นต้องมีการรีแอสเซมเบิ้ล (กำหนดค่า MF flag = 0) ซึ่งปกติการรีแอสเซมเบิ้ลแพ็กเก็ตทั้งหมดต้องสามารถเชื่อมต่อกันได้สนิท ดังรูปที่ 2.11 แต่แพ็กเก็ตที่ผู้บุกรุกส่งไปมีการแก้ไขข้อมูลในบางฟิลด์ ทำให้เกิดความผิดปกติในกระบวนการรีแอสเซมเบิ้ล ซึ่งการโจมตีในลักษณะนี้ แบ่งได้ดังต่อไปนี้



รูปที่ 2.11 แสดงการรีแอสเซมบลีแบบปกติ

(1) การส่งแพ็กเก็ตที่มีลำดับผิดปกติ (Abnormal Sequences of Packets Sending)

ปกติการส่งแพ็กเก็ตมักเรียงตามลำดับกันไป หากไม่เรียงลำดับก็ต้องรอจนกว่าแพ็กเก็ตก่อนหน้านี้มาถึง เพื่อเรียงลำดับแพ็กเก็ตที่เครื่องรับ แต่การโจมตีแบบนี้กลับส่งเฉพาะแพ็กเก็ตสุดท้ายเพื่อให้ระบบเป้าหมายรอแพ็กเก็ตก่อนหน้า และส่งไปเป็นปริมาณมากๆ เพื่อให้ระบบเป้าหมายไม่สามารถให้บริการอย่างอื่นได้

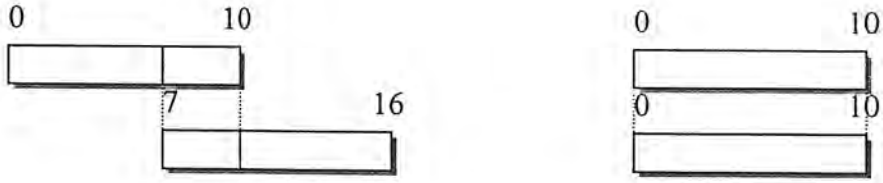
รูปที่ 2.12 แสดงแพ็กเก็ตสุดท้ายที่ต้องรอแพ็กเก็ตก่อนหน้า

โดยปกติแล้วการโจมตีในรูปแบบนี้ผู้โจมตีจะแก้ไขข้อมูลในฟิลด์แสดงลำดับของแพ็กเก็ต (Fragment Offset) ของแพ็กเก็ตไอพี ซึ่งเป็นส่วนที่แสดงลำดับของข้อมูลหลังจากกระบวนการแฟร็กเมนต์เตชันโดยแก้ให้ส่งแพ็กเก็ตสุดท้ายหรือแพ็กเก็ตหลังๆ เพียงแพ็กเก็ตเดียวเลย ทำให้ระบบเป้าหมายต้องรอแพ็กเก็ตก่อนหน้านี้

(2) การส่งแพ็กเก็ตที่มีขนาดเหลื่อมกัน (Overlapped Packets' Size Sending)

ปกติแพ็กเก็ตที่ส่งมาต้องนำมาต่อกันที่ระบบเป้าหมายได้พอดี แต่การโจมตีแบบนี้เป็นการส่งแพ็กเก็ตที่มีขนาดเหลื่อมกัน หรือซ้อนทับกัน ทำให้ข้อมูลเมื่อมาต่อกันแล้วเกิดความผิดพลาดหรือไม่สามารถเชื่อมต่อกันได้ โดยปกติแล้วการโจมตีแบบนี้ ผู้บุกรุกสามารถแก้ไขข้อมูลได้ 2 แห่งใหญ่ๆ ได้แก่

- การแก้ไขข้อมูลที่ฟิลด์แสดงลำดับของแพ็กเก็ต (Fragment Offset) ของแพ็กเก็ตไอพีหลังจากกระบวนการรีแอสเซมเบิ้ล ซึ่งทำให้ลำดับในการส่งมีความผิดพลาด และอาจเกิดการเหลื่อมล้ำของแพ็กเก็ต กระบวนการรีแอสเซมเบิ้ลอาจเกิดปัญหาได้
- การแก้ไขฟิลด์แสดงความยาวของ (Total Length) ของแพ็กเก็ตไอพี หลังจากกระบวนการรีแอสเซมเบิ้ล ขนาดของแพ็กเก็ตที่มาต่อไม่พอดีกัน ทำให้ไม่สามารถรวมแพ็กเก็ตได้ หรือหากรวมได้ ข้อมูลที่ได้ก็ไม่ถูกต้อง



รูปที่ 2.13 แสดงการรีแอสเซมบลีแบบแพ็กเก็ตมีขนาดเหลื่อมกัน

(3) การส่งแพ็กเก็ตแบบวนลูป (Loop)

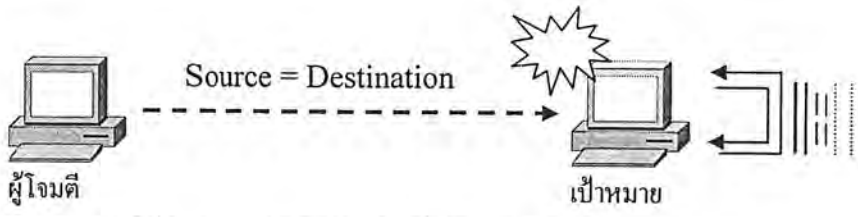
คือ การส่งโดยกำหนดค่าแอดเดรสต้นทาง (Source Address) และแอดเดรสปลายทาง (Destination Address) ให้เหมือนกันทำให้เกิดการรับส่งวนไปวนมาอยู่ที่เครื่องเป้าหมายเอง

ตัวอย่างของการโจมตีแบบนี้ได้แก่ LAND ซึ่งเป็นโปรแกรมโจมตีที่มีลักษณะดังนี้ คือ

- หมายหมายแอดเดรสต้นทาง และแอดเดรสปลายทางเป็นค่าเดียวกัน คือ เป็นแอดเดรสของเครื่องเป้าหมาย
- หมายเลขพอร์ตต้นทางเท่ากับหมายเลขพอร์ตปลายทาง
- SYN Flag ถูกตั้งเสมือนขอเริ่มต้นการเชื่อมต่อ

โดยปกติเมื่อมีการส่งสัญญาณ SYN มาก็ต้องมีการตอบกลับไปด้วยสัญญาณ SYN ACK ดังนั้นในที่นี้การตอบกลับจะตอบไปที่เครื่องเดิม ซึ่งในกรณีนี้ไม่มีกำหนดอยู่ในโพรโตคอลว่าควรทำอย่างไร โฮสต์จึงพยายามตอบสนองตามข้อกำหนดเท่าที่มีอยู่โดยการตอบกลับไปที่ไอพีแอดเดรส และพอร์ตต้นทางที่ถูกบุกรุกมา นั่นหมายถึงการตอบกลับเข้ามายังตัวเอง ซึ่งจะทำให้มีการตอบกลับไปมาของทีซีพีวนรอบอยู่ในตัวเองด้วยความเร็วสูง ทำให้คอมพิวเตอร์ต้องใช้ทรัพยากรที่มีอยู่ทั้งหมดเพื่อคอยจัดการกับทีซีพีที่ตอบกลับไปกลับมาจนไม่สามารถทำงานอื่นได้อีก ทำให้ต้องรีเซตเครื่องใหม่เพื่อหยุดการวนรอบของมัน

แพ็กเก็ตประเภทนี้เกิดจากการปลอมไอพีแอดเดรส ซึ่งถ้ามีการจัดการป้องกันการปลอมที่ดีพอก็สามารถป้องกันได้ แต่การป้องกันการปลอมนั้นสามารถบังคับใช้ได้ผลกับการปลอมข้าม เน็ตเวิร์กเท่านั้น ถ้าเป็นการปลอมในแชร์โดเมน(share domain)เดียวกันจะไม่สามารถทำได้ ซึ่งในปัจจุบันมีการปรับปรุง ทีซีพีสแต็กให้รัดกุมขึ้นจนการโจมตีแบบนี้ไม่เป็นผลกับคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการที่ได้รับการแก้ไขแล้ว



รูปที่ 2.14 รูปแสดงการโจมตีด้วย Land Attack

2.2.4.3 การสแกนพอร์ต (Port Scan)

จากความสำคัญของพอร์ตที่ทีซีพีใช้หมายเลขพอร์ต เพื่อระบุว่าข้อมูลที่ส่งเข้ามานั้นเป็นของแอพพลิเคชั่นใด และแอพพลิเคชั่นต่างๆ ก็จะเลือกใช้พอร์ตหมายเลขต่างๆ กัน เช่น FTP ใช้พอร์ตหมายเลข 21, SMTP ใช้พอร์ตหมายเลข 25 เป็นต้น เมื่อแอพพลิเคชั่นเลือกพอร์ตใดมาใช้งานแล้วก็มีหน้าที่คอยดูว่ามีการติดต่อมาที่พอร์ตของตนหรือไม่ หากมีก็ทำการตอบรับกลับไป ด้วยความสำคัญของพอร์ตนี้เอง พอร์ตจึงเป็นเป้าหมายของผู้บุกรุก เพื่อที่จะรู้ได้ว่ามีแอพพลิเคชั่นใดบ้างที่ทำงานอยู่บนโฮสต์ โดยปกติ ทั่วไปแล้วแอพพลิเคชั่นแต่ละชนิดที่เปิดให้บริการอยู่จะใช้หมายเลขพอร์ตที่ตายตัวและรู้จักกันโดยทั่วไป ดังนั้นเมื่อทำการสแกนแล้วก็จะนำผลมาเปรียบเทียบกับมาตรฐาน

การสแกนพอร์ต เป็นการสำรวจแต่ละโฮสต์ โดยมีขอบเขตเฉพาะโฮสต์เพียงตัวเดียว เป็นการส่งสัญญาณไปสอบถามยังทุกๆพอร์ตที่มีอยู่บนโฮสต์ ทั้ง ทีซีพี และ ยูดีพี เพื่อตรวจสอบว่ามีการเปิดให้บริการอะไรบ้างบนโฮสต์นั้น ซึ่งนั้นหมายถึงว่ามีแอพพลิเคชั่นประเภทใดอยู่บ้าง เทคนิคต่างๆ ที่นำมาใช้เพื่อการสแกนพอร์ตนั้นล้วนเป็นการดัดแปลงข้อกำหนดในโพรโตคอลมาใช้งานทั้งสิ้น อาจจะมีบางส่วนที่ใช้ช่องว่างที่ไม่มีกำหนดไว้ในโพรโตคอลเพื่อทำให้ได้ผลลัพธ์มาในที่สุด ดังจะอธิบายแต่ละวิธีต่อจากนี้

TCP SYN Scan

วิธีนี้ผู้สแกนจะทำการส่ง SYN แพ็กเก็ต (เซตค่าแฟล็ก SYN ไว้เป็น 1) เพื่อทำการติดต่อโดยตรงกับเป้าหมายโดยไม่ผ่านระบบปฏิบัติการ และรอผลการตอบรับของเป้าหมายกลับมา ซึ่งหากเป้าหมายทำงานอยู่ก็จะตอบกลับมาด้วย SYN ACK (เป็นแพ็กเก็ตที่ เซตค่าแฟล็ก SYN และ ACK ไว้เป็น1) หรือหากไม่มีแอพพลิเคชั่นทำงานอยู่จะตอบกลับมาด้วย RST การสแกนแบบนี้หากตรวจสอบบนโฮสต์เป้าหมายจะพบว่ามีการขอเชื่อมต่อเข้ามา แต่ไม่สามารถเปิดการติดต่อได้สำเร็จ เทคนิคนี้บางครั้งถูกเรียกว่า half-open scanning คือไม่สามารถทำ 3-way handshake ได้ จึงไม่มีการเชื่อมต่อใดๆเกิดขึ้นระหว่างเครื่องผู้สแกน กับเครื่องที่ถูกสแกน

FIN Scan

เป็นการส่ง FIN แพ็กเก็ตไปยังเป้าหมาย โดยที่เครื่องเป้าหมายก็จะยังตอบแพ็กเก็ตนั้นกลับไป แม้จะไม่มีการสื่อสารใดๆมาก่อนก็ตาม ซึ่งโดยปกติแล้วแพ็กเก็ตที่เซตค่า FIN เป็น 1 จะเป็นแพ็กเก็ตที่ใช้ในการตอบกลับ และการตอบกลับของเครื่องเป้าหมายสำหรับพอร์ตที่เปิดไว้ และพอร์ตที่ไม่ได้เปิดให้บริการก็ไม่เหมือนกัน หากเป็นพอร์ตที่เปิดอยู่ก็จะตอบด้วย FIN ACK กลับไป และหากเป็นพอร์ตที่ไม่ได้เปิดก็จะตอบด้วย RST ACK

SYN/FIN Scan

วิธีนี้จะใช้ ทีซีพี Flag ทั้ง SYN และ FIN พร้อมกัน ซึ่งปกติเป็นแฟล็กที่ไม่มีกำหนดไว้ในโพรโตคอล และจะไม่พบแฟล็กเช่นนี้ในการสื่อสารตามปกติเป็นอันขาด เพราะโดยปกติแล้ว SYN Flag จะใช้เมื่อเริ่มการติดต่อ ส่วน FIN จะใช้เมื่อต้องการยุติการติดต่อ การตอบรับของโฮสต์แต่ละประเภทในกรณีที่ทำงานอยู่นั้นอาจจะแตกต่างกันไป เช่นเป็น SYN ACK หรือ FIN ACK อย่างใดอย่างหนึ่ง ส่วนการตอบรับในกรณีที่พอร์ตปิดจะตอบเหมือนกันคือ RST

Null Scan

วิธีนี้จะไม่ใช้แฟล็กใดๆในการสแกนเลย โดยส่งแพ็กเก็ตที่ไม่มีแฟล็กใดที่ถูกเซตไว้เลยไปยังเป้าหมาย เป็นการเซตแฟล็กทุกค่าให้เป็น 0 หมด ซึ่งแพ็กเก็ตลักษณะนี้จะไม่มีอยู่ในโพรโตคอล โดยทั่วไปการตอบสนองแพ็กเก็ตที่ไม่ได้อยู่ในโพรโตคอล จะมีการตอบรับที่ต่างกันออกไปตามแต่ประเภทของระบบปฏิบัติการ ดังนั้นนอกจากการใช้แพ็กเก็ตเหล่านี้เพื่อการสแกนพอร์ตแล้วยังสามารถนำแพ็กเก็ตเหล่านี้ไปใช้ในการตรวจสอบระบบปฏิบัติการของเป้าหมายได้อีกด้วย โดยการส่งแพ็กเก็ตที่มีแฟล็กซึ่งไม่อยู่ในข้อกำหนด การส่งแพ็กเก็ตลักษณะนี้ หากพอร์ตของเครื่องเป้าหมายปิดอยู่ การตอบรับจะเป็นการส่ง RST กลับไป

Xmas Scan

จะเป็นการส่งแพ็กเก็ตทีซีพีที่เซตแฟล็ก FIN, Push, URGENT ไปยังพอร์ตเป้าหมายที่เครื่องปลายทาง ซึ่งมักไม่เป็นที่สนใจในการตรวจสอบเท่ากับ SYN-ACK-RST เครื่องปลายทางจะส่งแพ็กเก็ตทีซีพี RST ของพอร์ตที่ปิดอยู่กลับมาให้

UDP Scan

จะส่งแพ็กเก็ตของโพรโตคอลยูดีพี ไปยังพอร์ตเป้าหมาย แต่เนื่องจากยูดีพีมีการจัดการที่แตกต่างจากทีซีพีโดยโพรโตคอลยูดีพี เป็นโพรโตคอลลักษณะคอนเน็กชันเลส(connectionless) ดังนั้นผลลัพธ์ของการสแกนเมื่อพอร์ตเปิดอยู่นั้นจะไม่สามารถคาดการณ์ได้ ขึ้นอยู่กับแต่ละแอพพลิเคชั่น และไม่มีมาตรฐานที่เหมือนกันแต่อย่างใด ดังนั้นการสแกนยูดีพี จึงต้องดูผลลัพธ์จาก ICMP เป็นหลัก หากพอร์ตไม่เปิดให้บริการ จะมี ICMP Message ว่า UDP Port Unreachable กลับมา และหากพอร์ตเปิดให้บริการ อาจมีการตอบรับหรือไม่ และอย่างไร จะขึ้นอยู่กับการทำงานของแอพพลิเคชั่นที่เปิดพอร์ตนั้น แต่ที่แน่ๆคือจะไม่มี ICMP Message กลับมาอีก

2.2.4.4 การตรวจสอบระบบปฏิบัติการ (Finger Print)

เป็นเครื่องมือที่ใช้สำหรับการตรวจสอบว่าเครื่องเป้าหมายใช้ระบบปฏิบัติการใดเนื่องจากจุดอ่อนของระบบปฏิบัติการแต่ละตัวมีไม่เหมือนกันหากผู้โจมตีทราบว่าระบบปฏิบัติการของเครื่องเป้าหมายเป็นระบบปฏิบัติการใดย่อมส่งผลให้สามารถเลือกใช้เครื่องมือในโจมตีที่ตรงกับระบบปฏิบัติการนั้นได้ ทำให้ผลจากการโจมตีเกิดได้มากกว่าการใช้เครื่องมือที่ทำงานได้ไม่ตรงกับระบบปฏิบัติการ

การตรวจสอบระบบปฏิบัติการมีเทคนิคที่ใช้หลายวิธี ตั้งแต่วิธีที่ไม่ต้องใช้เครื่องมือใดๆ เพียงแค่มีโปรแกรมเท็ลเน็ต ตัวอย่างเช่นการตรวจสอบจากแบนเนอร์ (Banner) เนื่องจากแบนเนอร์จะเป็นข้อความที่ใช้แสดงการตอบรับเมื่อทำการเชื่อมต่อสำเร็จเพื่อบอกให้ไคลเอนต์ทราบว่าเครื่องเซิร์ฟเวอร์ใช้ระบบปฏิบัติการใดอยู่ ดังนั้นในแบนเนอร์จึงมีการแสดงชื่อระบบปฏิบัติการด้วย ทำให้สามารถตรวจสอบได้ว่าเครื่องดังกล่าวใช้ระบบปฏิบัติการใด นอกจากนี้การสแกนพอร์ตยังสามารถตรวจสอบคร่าวๆ เช่นกันว่าเป้าหมายใช้ระบบปฏิบัติการตระกูลใด เช่นเครื่องที่เปิดบริการพอร์ต 139 (NetBios) โดยมากจะเป็นระบบปฏิบัติการตระกูลไมโครซอฟท์วินโดว์ เป็นต้น

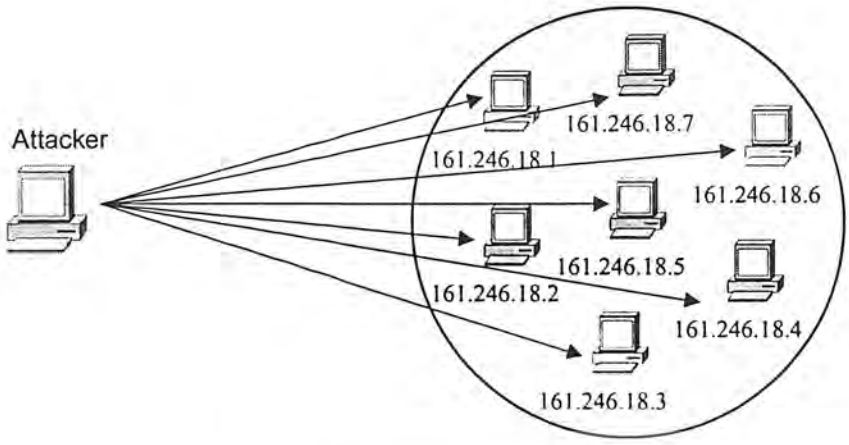
เทคนิคที่ได้กล่าวมาเป็นเทคนิคขั้นพื้นฐาน ไม่จำเป็นต้องใช้เครื่องมือพิเศษ แต่ก็มีข้อจำกัด เนื่องจากข้อมูลในแบนเนอร์หรือบริการต่างๆ สามารถถูกควบคุมได้จากผู้ดูแลระบบ ส่งผลให้บ้างครั้ง ข้อมูลที่ได้จากการสำรวจอาจผิดพลาด ทำให้เกิดวิธีการตรวจสอบระบบปฏิบัติการที่เรียกกว่า ทีซีพี สแต็กฟิงเกอร์ปรินซ์ (TCP Stack Fingerprint) โดยเป็นวิธีที่ใช้หลักความเป็นจริงที่ว่าชั้นทีซีพีสแต็กของระบบปฏิบัติการแต่ละระบบ จะมีการสร้างแพ็กเก็ตในชั้นทีซีพีที่แตกต่างกันในส่วนของรายละเอียดปลีกย่อย หรือมีการตอบสนองแตกต่างกันในกรณีที่ได้รับแพ็กเก็ตที่ผิดปกติ หากนำความแตกต่างของแพ็กเก็ตมาเปรียบเทียบกับข้อมูลในฐานข้อมูล จะทำให้สามารถตรวจสอบได้ว่าระบบปฏิบัติการนั้นเป็นระบบใด การทำงานของโปรแกรมตรวจสอบระบบปฏิบัติการที่ใช้หลักการของทีซีพีสแต็กฟิงเกอร์ปรินซ์ คือโปรแกรมจะสร้างข้อมูลในชั้นทีซีพีที่มีแฟล็กผิดปกติแล้วส่งไปยังเครื่องเป้าหมาย เมื่อเป้าหมายได้รับข้อมูลดังกล่าวจะไม่สามารถตอบสนองด้วยรูปแบบที่กำหนดได้ เนื่องจากชั้นทีซีพีสแต็กของระบบไม่ได้ออกแบบมาสำหรับกรณีที่ได้รับแพ็กเก็ตดังกล่าว เครื่องเป้าหมายจะตอบสนองต่อแพ็กเก็ตดังกล่าวแตกต่างกันตามการโปรแกรมในชั้นทีซีพีสแต็กของแต่ละระบบปฏิบัติการ จากความแตกต่างดังกล่าวนี้เองทำให้สามารถตรวจสอบระบบปฏิบัติการว่าเป็นระบบปฏิบัติการใด

2.2.4.5 ไอพีสแกน (IP Scan)

การสำรวจวิธีนี้เป็นพื้นฐานเบื้องต้นปกติไม่ว่าจะเป็นผู้บริหารเครือข่ายระบบเองหรือผู้ โดยจะเริ่มการพิจารณาจากแพ็กเก็ตที่ปรากฏขึ้นในเน็ตเวิร์กเพียงอย่างเดียวนั้น ยากที่จะแยกแยะได้ว่าเป็นการกระทำที่มุ่งร้ายหรือไม่ แต่อย่างน้อยที่สุดก็เป็นสัญญาณเตือนเบื้องต้นในการทำการตรวจสอบต่อไปว่าผู้กระทำมีจุดมุ่งหมายอย่างไร วิธีการสำรวจนี้ใช้การส่งไอซีเอ็มพีเอคโครีเควสต์ (ICMP Echo Request) ไปยังโฮสต์ทุกตัวในเน็ตเวิร์ก เพื่อสำรวจดูว่าในเน็ตเวิร์กเป้าหมายนั้นมีโฮสต์ใดที่เปิดใช้งานอยู่บ้าง เมื่อโฮสต์ใดก็ตามได้รับ ไอซีเอ็มพีเอคโครีเควสต์ (ICMP Echo Request) เข้ามาก็จะต้องตอบกลับไปด้วยไอซีเอ็มพีเอคโครีพลาย (ICMP Echo Reply) การตอบกลับมานี่เองจะเป็นสิ่งยืนยันได้ว่าโฮสต์นั้นเปิดใช้งานอยู่ การจะสังเกตว่า ไอซีเอ็มพีเอคโครีเควสต์ (ICMP Echo Request) แพ็กเก็ตนั้นต้องสงสัยว่าจะเป็นการสำรวจเน็ตเวิร์กหรือไม่ มิอาจพิจารณาได้จากแพ็กเก็ตเดียว จำเป็นต้องพิจารณาจากรูปแบบและความต่อเนื่องของหลายแพ็กเก็ต โดยจุดที่จะสามารถระบุได้ว่ามีความเป็นไปได้สูงคือ

1. แพ็กเก็ตนั้นมาจากที่เดียวกันและส่งไปยังโฮสต์ปลายทางหลายๆโฮสต์ ซึ่งถ้าไอพีแอดเดรสมาจากภายนอกเน็ตเวิร์ก ก็มีความเป็นไปได้สูงที่จะเป็นการสแกนที่มุ่งร้าย เพราะบุคคลภายนอกไม่ควรสำรวจเน็ตเวิร์กผู้อื่นโดยไม่มีหน้าที่ และโดยพลการ

2. ช่วงเวลาระหว่างแพ็กเก็ตมีค่าน้อยมาก ปัจจัยในส่วนของเวลาระหว่างแพ็กเก็ตนั้นจะบอกได้ว่าแพ็กเก็ตเหล่านั้นถูกส่งมาจากคำสั่งปิงปกติหรือถูกส่งมาจากเครื่องมือที่ใช้สำหรับสแกนโดยเฉพาะ หากระยะเวลาระหว่างแพ็กเก็ตนั้นมีค่าน้อยกว่า 0.5 วินาที ให้สันนิษฐานได้ว่าเป็นแพ็กเก็ตที่มาจาก เครื่องมือแน่นอน



รูปที่ 2.15 แสดงการไอพีสแกนของผู้บุกรุก

2.2.4.6 ไอพีสปูฟิง (IP Spoofing)

ไอพีสปูฟิง (IP Spoofing) หมายถึง การที่ผู้บุกรุกอยู่นอกเครือข่ายแล้วแกล้งทำเป็นว่าคอมพิวเตอร์ที่เชื่อถือได้ (Trusted) โดยอาจจะใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่าย หรืออาจจะใช้ไอพีแอดเดรสข้างนอกเครือข่ายเชื่อว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ หรืออนุญาตให้เข้าใช้ทรัพยากรในเครือข่ายได้ โดยปกติแล้วการโจมตีแบบไอพีสปูฟิงเป็นการเปลี่ยนแปลง หรือเพิ่มข้อมูลเข้าไปแบบแพ็กเก็ตที่รับส่งระหว่างไคลเอนต์และเซิร์ฟเวอร์ หรือคอมพิวเตอร์สื่อสารกันในเครือข่าย การที่จะทำแบบนี้ได้ผู้บุกรุกจะต้องปรับเราท์ติ้ง เทเบิ้ลของเราท์ติ้งเพื่อให้ส่งต่อแพ็กเก็ตไปที่เครื่องของผู้บุกรุก หรืออีกวิธีหนึ่งคือการที่ผู้บุกรุกสามารถแก้ไขให้แอพพลิเคชั่น ส่งข้อมูลที่เป็นประโยชน์ต่อการเข้าถึงแอพพลเคชั่นนั้นผ่านทางอีเมล์ หลังจากนั้นผู้บุกรุกก็สามารถเข้าใช้แอพพลิเคชั่นได้โดยใช้ข้อมูลดังกล่าว

อย่างไรก็ตาม ถ้าผู้บุกรุกสามารถปรับเปลี่ยนเราท์ติ้งเทเบิ้ลเพื่อให้ส่งข้อมูลไปยังเครื่องปลอมได้ผู้บุกรุกสามารถรับส่งข้อมูลกับแอพพลิเคชั่นนั้นเปรียบเสมือนเป็นหนึ่งในผู้ใช้ทั่วๆไปได้ ไอพีสปูฟิงไม่จำเป็นจะต้องเป็นคอมพิวเตอร์ที่อยู่นอกเครือข่ายเท่านั้น แต่อาจจะเป็นผู้ใช้ที่อยู่ข้างในที่ไม่มีสิทธิก็ได้ ซึ่งอย่างที่เป็นที่ทราบกันดีว่า การโจมตีเครือข่ายนั้น 90% จะเป็นการโจมตีจากภายในเครือข่ายเอง

2.2.4.7 การบุกรุกประเภทอื่น ๆ

การโจมตีประเภทอื่นนอกจากที่ได้กล่าวมาแล้วข้างต้น ส่วนใหญ่เกิดจากการใช้จุดอ่อนหรือข้อผิดพลาดของแอพพลิเคชั่นที่เครื่องเป้าหมายใช้อยู่ในการโจมตีเครื่องเป้าหมายเอง ไม่ว่าจะเป็นจุดอ่อนของระบบปฏิบัติการ หรือข้อผิดพลาดของซอฟต์แวร์ก็ตาม

ในกรณีเช่นนี้เจ้าของเครื่องสามารถแก้ไขได้เอง โดยการนำโปรแกรมแพ็ทช์ (Patch) หรือเซอร์วิสแพ็ค (Service Pack) ต่างๆ มาลงเพื่อแก้ข้อผิดพลาดเหล่านี้ หรือหลีกเลี่ยงไปใช้โปรแกรมอื่นที่ไม่เกิดปัญหา ซึ่งการโจมตีในลักษณะนี้ไม่อยู่ในขอบเขตที่ศึกษา

บทที่ 3
การออกแบบและการสร้าง

3.1 ขอบเขตของระบบต้นแบบการตรวจจับผู้บุกรุกทางเครือข่ายคอมพิวเตอร์ที่สร้างขึ้น

แพ็กเก็ตดีเทคเตอร์ (Packet Detector) ที่สร้างขึ้น มุ่งเน้นการศึกษาซึ่งอ้างอิงกับ ระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์ (Intrusion Detection System – IDS) เป็นหลัก โดยระบบตรวจจับผู้บุกรุกเป็นแบบปฏิบัติการบนการไหลข้อมูลในเครือข่าย ซึ่งใช้วิธีเกี่ยวกับการตรวจจับการใช้งานโดยการตรวจสอบกับข้อกำหนดการใช้งาน และการตรวจสอบจากสถิติการใช้งานของผู้ใช้และนำข้อมูลมาวิเคราะห์หาความเป็นไปได้ในการบุกรุก โดยที่การบุกรุกเป็นแบบที่ทำการศึกษา ตามทฤษฎีและหลักการในบทที่สองส่วนรูปแบบการบุกรุกอื่นที่นอกเหนือจากกรณีที่ศึกษา จะไม่ถูกนำมาพิจารณาเพื่อการออกแบบและการสร้าง

3.2 ขั้นตอนการออกแบบและการสร้าง

เมื่อทำการศึกษารูปแบบการสื่อสารเครือข่ายคอมพิวเตอร์และพิจารณาถึงข้อบกพร่อง ที่ทำให้สามารถทำการโจมตีเครือข่ายคอมพิวเตอร์ได้ รวมถึงการศึกษาในส่วนรูปแบบของระบบการตรวจสอบเครือข่ายคอมพิวเตอร์ ทำให้เราต้องการรูปแบบระบบตรวจจับข้อมูลแปลกปลอมบนเครือข่าย (Packet Detector) ซึ่งอ้างอิงการรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์แบบระบบตรวจจับผู้บุกรุก โดยใช้วิธีการตรวจสอบกับข้อกำหนดการใช้งานและตรวจสอบจากสถิติการใช้งานของระบบมี โดยมีขั้นตอนการออกแบบเพื่อต้องการให้ระบบมีความสามารถในการทำงานดังต่อไปนี้

(1) ติดตั้งโปรแกรมได้ โดยผ่านคำสั่ง make , make install
(2) ถอนการติดตั้งโปรแกรมได้ โดยผ่านคำสั่ง make uninstall , make clean
(3) เก็บข้อมูลของแพ็กเก็ต และสามารถแสดงข้อมูลของแพ็กเก็ตผ่านหน้าจอ
(4) เก็บข้อมูลของแพ็กเก็ตเพื่อวิเคราะห์การบุกรุกตามเวลาจริง และแสดงผลผ่านหน้าจอ
(5) แสดงส่วนช่วยเหลือผู้ใช้โปรแกรม
(6) วิเคราะห์แพ็กเก็ตที่เกิดความผิดปกติแบบมีปริมาณมาก (Amount of Packets Sending)
(7) วิเคราะห์แพ็กเก็ตที่เกิดความผิดปกติแบบมีการทำแฟร็กเมนเตชั่นที่ผิดปกติ (Fragmentation)
(8) วิเคราะห์แพ็กเก็ตที่เกิดความผิดปกติแบบมีการส่งแพ็กเก็ตแบบวนลูป (Land)
(9) วิเคราะห์แพ็กเก็ตสแกนพอร์ต (Scan port)ชนิดต่างๆได้ เช่น FIN, NULL, XMAS
(10) วิเคราะห์แพ็กเก็ตไอพีสแกน (IP Scan)
(11) วิเคราะห์แพ็กเก็ตที่ตรวจสอบระบบปฏิบัติการ (Finger print)
(12) แสดงข้อมูลการโจมตีผ่านเว็บเพจ
(13) แสดงผลเก็บลงล็อกไฟล์และสามารถเปลี่ยนไดเร็กทอรีที่เก็บล็อกไฟล์

ดังนั้นขั้นตอนการสร้างต่าง ๆ จะทำตามขั้นตอนการออกแบบ ซึ่งผู้จัดทำจะขออธิบายในส่วนขั้นตอนตั้งแต่ขั้นที่ (3) จนถึงขั้นตอนที่ (12) ซึ่งเป็นส่วนที่เป็นเนื้อหาหลักที่ทำการศึกษา

ขั้นตอนการทำงานของระบบโดยรวมซึ่งแสดงให้ดูเป็นตัวอย่างอยู่ 2 ฟังก์ชั่น คือ

1. ฟังก์ชั่นที่ใช้สำหรับการดูลักษณะแพ็กเก็ตที่เข้ามาในเครือข่าย โดยเมื่อต้องการใช้ฟังก์ชั่นนี้ให้ทำการพิมพ์คำสั่ง packet_detector –v ดังรูปที่ 3.1
2. ฟังก์ชั่นที่ใช้สำหรับการตรวจสอบการบุกรุก โดยเมื่อต้องการใช้ฟังก์ชั่นนี้ให้ทำการพิมพ์คำสั่ง packet_detector –R ดังรูปที่ 3.1

รูปที่ 3.1 โฟลว์ชาร์ทระบบทั้งหมดของแพ็คเก็ตดีเทคเตอร์ในการทำงานแบบแสดงผลข้อมูลออกทาง

รูปที่ 3.2โฟลว์ชาร์ทแสดงระบบทั้งหมดของแพ็คเก็ตดีเทคเตอร์ในการทำงานแบบการวิเคราะห์การบุกรุก

จากรูปที่ 3.1 และ 3.2 จะพิจารณาได้ว่ามีขั้นตอนการทำงานที่เหมือนกันซึ่งสามารถแยกขั้นตอนการทำงานออกได้ดังหัวข้อต่อไปนี้

3.2.1 ส่วนรับคำสั่งและกำหนดค่าเริ่มต้น

รูปที่ 3.3 โฟลว์ชาร์ทแสดงการเซ็ตค่าเริ่มต้น

จากรูปที่ 3.3 เมื่อเริ่มโปรแกรม สิ่งแรกที่จะต้องออกแบบคือ รูปแบบการทำงาน เนื่องจากแพ็กเก็ตดีเทคเตอร์ นอกจากต้องการตรวจจับการบุกรุกทางเครือข่ายแล้ว ยังต้องการให้ระบบสามารถทำการมอนิเตอร์ (Monitor) แพ็กเก็ต โดยไม่ต้องตรวจสอบการบุกรุกเพื่อตรวจสอบประสิทธิภาพของระบบเครือข่าย รวมถึงสามารถที่จะบอกรายละเอียดของแต่ละแพ็กเก็ต ที่ส่งผ่านสายอีเทอร์เน็ตถึงข้อมูลภายในแพ็กเก็ตนั้น และทำการตีความ ออกมา โดยสามารถที่จะเลือกรูปแบบการรายงานผลได้ ดังนั้นโฟลว์ชาร์ทนี้จะแสดงถึงลำดับในการรับคำสั่ง ซึ่งเมื่อรับคำสั่งเสร็จแล้วจะจบการทำงานเลยโดยที่ไม่มีการวนกลับมาเซ็ตค่าเริ่มต้นอีก

3.2.2 ส่วนดักจับแพ็กเก็ตหรือแพ็กเก็ตสนิฟเฟอร์

ในส่วนการทำงานนี้เป็นการทำงานในลักษณะแพ็กเก็ตสนิฟเฟอร์ ซึ่งในการเขียนโปรแกรมภาษาซีจะทำการเพิ่มไลบารี่ที่ชื่อว่า pcap.h ซึ่งเป็นไฟล์เฮดเดอร์ เพื่อที่จะนำไปสู่ฟังก์ชั่นในการติดต่อการ์ดแลน โดยกำหนดให้การ์ดแลนอยู่ในโหมดโพรมิสคูอัส ซึ่งการใช้งานจะเป็นลำดับขั้น การทำงานในลักษณะแพ็กเก็ตสนิฟเฟอร์แสดงไว้เป็นโฟลว์ชาร์ทการกำหนดค่าให้กับฟังก์ชั่นดังรูปที่ 3.4

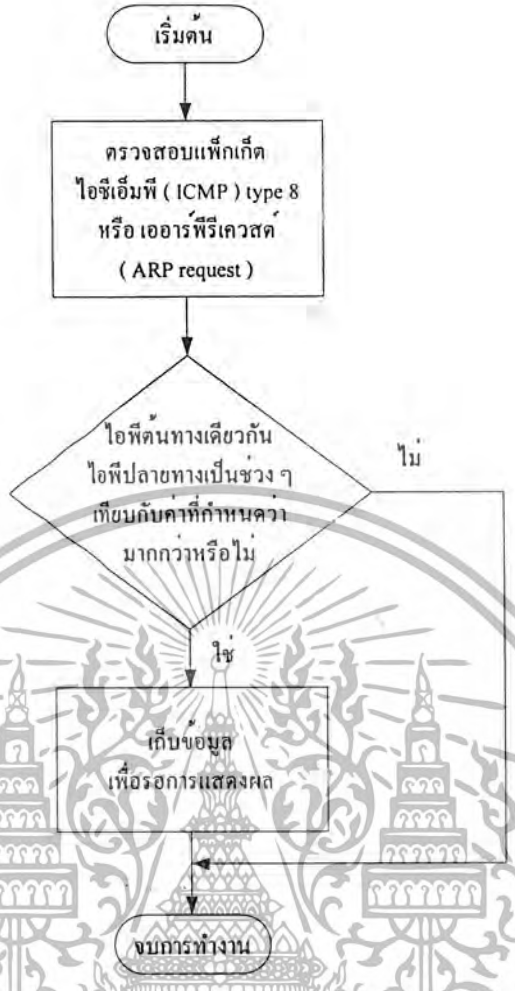
รูปที่ 3.4 โฟลว์ชาร์ทแสดงการดักจับแพ็กเก็ต

3.2.3 ส่วนวิเคราะห์แพ็กเก็ต

การวิเคราะห์แพ็กเก็ต จะทำการวิเคราะห์แพ็กเก็ต จนทราบข้อมูลเบื้องต้น เช่น เป็นโพรโตคอลอะไร ขนาดแพ็กเก็ตเท่าไร เข้ามาเมื่อวัน , เดือน , ปี , เวลา เท่าไร จากใคร ถึงใคร เมื่อวิเคราะห์ข้อมูลเบื้องต้นเสร็จแล้ว ขั้นตอนต่อไปของการวิเคราะห์แพ็กเก็ตคือ ตรวจสอบกับรูปแบบข้อมูลของระบบ ว่าตรงกับรูปแบบการบุกรุกที่ผู้ใช้ได้กำหนดไว้หรือไม่ รวมถึงการตรวจสอบว่าข้อมูลในบัฟเฟอร์ต่าง ๆ ที่ใช้ในการประมวลผลโปรแกรมว่าสามารถลบออกไปได้หรือไม่ด้วย

3.2.3.1 ไอพีสแกน (IP Scan)

การตรวจจับไอพีสแกนสามารถทำได้โดยการตรวจสอบดูแพ็กเก็ตไอซีเอ็มพีเอคโครีเควสต์ชนิด 8 (ICMP Echo Request type 8) ที่เข้ามายังระบบ หากมีแพ็กเก็ตลักษณะนี้จำนวนมากและมีปลายทางแตกต่างกัน จะสามารถสรุปได้ว่าในเครือข่ายกำลังถูกสำรวจโดยไอพีสแกน



รูปที่ 3.5 โฟลว์ชาร์ทแสดงการตรวจสอบการโจมตีแบบไอพีสแกน (IP Scan)

จากบทที่สอง อีกวิธีหนึ่งที่สรุปได้ว่าเป็นการบุกรุกแบบไอพีสแกนคือการส่งแพ็กเก็ตชนิด เออาร์พีรีเควสต์ (ARP request) โดยวิธีการตรวจการบุกรุกแบบนี้ทำได้โดยตรวจสอบแพ็กเก็ต เออาร์พีรีเควสต์ หากมีแพ็กเก็ตนี้จำนวนมากและมีลักษณะส่งจาก ไอพีแอดเดรสต้นทางเดียวกัน และไอพีแอดเดรสปลายทางเป็นช่วง ๆ โดยมีการส่งแพ็กเก็ตจำนวนมากสรุปได้ว่าเป็นการบุกรุกแบบไอพีสแกน

จากรูปที่ 3.5 การเปรียบเทียบกับค่าที่กำหนดนั้น ทำไปเพื่อป้องกันโปรแกรมไม่ให้เข้าใจผิดว่าการตรวจจับที่เกิดขึ้นนั้นไม่รวมการปิงที่เป็นการสำรวจเครือข่ายเบื้องต้นของผู้ใช้งานทั่วไป เช่น คำสั่ง ping 161.246.18.51 จะเป็นการสำรวจเครือข่ายว่า สามารถส่งแพ็กเก็ตข้อมูลไปถึงผู้รับปลายทางหรือไม่ ซึ่งโดยทั่วไปจะมีค่า จำนวนแพ็กเก็ตต่อวินาทีประมาณ 1 แพ็กเก็ต ต่อวินาที แต่ในปริญญานิพนธ์ฉบับนี้ได้ทำการกำหนดค่าที่ใช้ในการเปรียบเทียบ ไว้ 5 แพ็กเก็ต ต่อวินาที

เช่นเดียวกันกับเออาร์พีรีเควสต์ การเปรียบเทียบกับค่าที่กำหนดทำไปเพื่อป้องกันโปรแกรมไม่ให้เข้าใจผิดว่า การตรวจจับที่เกิดขึ้นนั้นไม่รวมการตรวจไอพีที่เกิดจากการปิงอีกเช่นกัน เพราะในขั้นตอนการปิงนั้น แท้ที่จริงแล้วในตอนเริ่มต้น เครื่องต้นทางจะต้องทำการสร้างตารางเออาร์พี (ARP Table) เพื่อสร้างเส้นทางการเชื่อมต่อ แต่ในปริญญานิพนธ์ฉบับนี้ ได้ทำการกำหนดค่าที่ใช้ในการเปรียบเทียบ ไว้ 5 แพ็กเก็ต ต่อวินาที อีกเช่นกัน

3.2.3.2 การสแกนพอร์ต (Port Scan)

การตรวจสอบการสแกนพอร์ตทำได้โดย การตรวจดูแพ็กเก็ตที่มีแฟล็กของ ทีซีพีหรือยูดีพี เฮดเดอร์ หลังจากนั้นจะดูหมายเลขพอร์ตปลายทางเป็นลักษณะแบบกระจาย คือแพ็กเก็ตมีการส่งไปยังเครื่องๆ เดียวแต่มีการส่งไปยังพอร์ตต่างๆ กัน เป็นจำนวนมากหรือไม่ หากตรงกับรูปแบบที่กำหนดจะสรุปได้ว่าเป็นการบุกรุกแบบสแกนพอร์ต

รูปที่ 3.6 โฟลว์ชาร์ทแสดงการตรวจสอบการสแกนพอร์ต (Scan Port)

จากรูปที่ 3.6 การเปรียบเทียบกับค่าที่กำหนดนั้น ทำไปเพื่อป้องกันโปรแกรมไม่ให้เข้าใจผิด โดยแพ็กเก็ตที่จะทำให้เข้าใจผิดได้ก็คือการติดต่อสื่อสาร 3-way handshake ซึ่งตอนเริ่มต้นของกระบวนการนี้จะส่ง ทีซีพีแพ็กเก็ตที่มี ทีซีพีแฟล็กเป็น SYN โดยเมื่อส่งไปครั้งแรกแล้วไม่มีการติดต่อกลับ เครื่องต้นทางก็จะส่งแพ็กเก็ตดังกล่าวไปเป็นจำนวนแพ็กเก็ตหนึ่ง ซึ่งหากไม่มีการกำหนดค่าไว้ จะทำให้ระบบสับสนได้และอาจแจ้งเตือนผิด ซึ่งในปริญญานิพนธ์ฉบับนี้ ได้กำหนดค่าสำหรับพิจารณาการบุกรุกแบบนี้ไว้ที่ 30 แพ็กเก็ตต่อวินาที

3.2.3.3 การตรวจสอบระบบปฏิบัติการ (Finger Print)

การตรวจจับการตรวจสอบปฏิบัติการ สามารถตรวจสอบได้จากการพิจารณาแฟล็กที่ถูกส่งไปในชั้นทีซีพีของทุกๆ พอร์ตว่าเป็นแพ็กเก็ตแบบผิดปกติหรือไม่ กล่าวคือในแต่ละแพ็กเก็ตของทีซีพีโพรโตคอลนั้นจะมีรูปแบบแฟล็กตายตัวอยู่ ตามสถานะปัจจุบันของแพ็กเก็ตทีซีพี

รูปที่ 3.7 โฟลว์ชาร์ทแสดงการตรวจสอบการบุกรุกแบบการตรวจสอบระบบปฏิบัติการ (Finger Print)

หากต้องการเริ่มต้นการเชื่อมต่อโพรโตคอลทีซีพี จะต้องกำหนดให้แฟล็ก ACK เป็น 1 ส่วนแฟล็กอื่นต้องเป็น 0 หรือหากต้องการยกเลิกการเชื่อมต่อโพรโตคอลทีซีพี จะต้องกำหนดให้แฟล็ก FIN เป็น 1 ส่วนแฟล็กอื่นเป็น 0 เป็นต้น

วิธีการตรวจจับที่ใช้ในโปรแกรมนั้นได้ทำการตรวจจับโดยตรวจสอบทีซีพีแฟล็กว่าไม่ได้มีใช้งานอยู่จริงหรือไม่ ถ้าเป็นจริงจะระบุว่าเป็นการบุกรุกโดยการตรวจสอบเพื่อระบุระบบปฏิบัติการ เนื่องจากการตรวจจับวิธีนี้เป็นกรณีมาตรฐาน ที่โปรแกรมที่ทำการระบุระบบปฏิบัติการทุกโปรแกรมจะนำมาตรวจสอบ และเป็นแฟล็กที่ไม่สามารถเกิดได้จริงเมื่อมีการใช้งานโพรโตคอลทีซีพี ดังรูปที่ 3.7

3.2.3.4 การส่งแพ็กเก็ตปริมาณมาก (Amount of Packets Sending)

การตรวจจับการโจมตีประเภทนี้ เราต้องวิเคราะห์แพ็กเก็ตที่เข้าในเน็ตเวิร์ค โดยดูที่แอดเดรสปลายทางเป็นหลัก คือเมื่อมีแพ็กเก็ตเข้ามาเราก็จะทำการนำค่าของแอดเดรสปลายทางมาดูว่ามีข้อมูลเก็บอยู่หรือยัง ถ้ายังเราก็จะสร้างข้อมูลของมันขึ้นมา ส่วนถ้าเกิดว่ามีข้อมูลอยู่แล้วเราก็จะทำการเพิ่มค่าของตัวนับ ซึ่งหมายถึงจำนวนแพ็กเก็ตที่เข้ามาในเครื่อง ในการเพิ่มค่าตัวนับนั้นต้องทำการตรวจสอบค่าของช่วงเวลาระหว่างแพ็กเก็ตก่อนว่ามีค่าอยู่ในช่วงที่กำหนดหรือไม่ เพื่อความไม่ผิดพลาดในการวิเคราะห์ ถ้าเกิดว่าเกินช่วงเวลาเราก็จะทำการลบข้อมูลนั้นทิ้ง หลังจากที่ทำการเพิ่มค่าของตัวนับแล้ว ก็นำข้อมูลที่เก็บไว้เหล่านั้นมาเปรียบเทียบกับค่ามาตรฐานของเน็ตเวิร์คนี้ติดตั้งอยู่ หากค่าที่นับได้มากกว่าค่าที่ยอมรับได้ ก็ให้แจ้งเตือนแก่ผู้ดูแลระบบ ซึ่งการทำงานดังกล่าวมานี้ เป็นไปดังรูปที่ 3.8

รูปที่ 3.8 โฟลว์ชาร์ทแสดงการตรวจสอบการส่งแพ็กเก็ตปริมาณมาก (Amount of Packets Sending)

การวิเคราะห์แบบนี้อยู่ที่การหาค่าที่ระบบยอมรับได้ เพราะขึ้นอยู่กับปัจจัยหลายประการ เช่น อัตราเร็วของเครือข่าย อัตราเร็วของหน่วยประมวลผลเครื่อง ปริมาณหน่วยความจำในเครื่องเป็นต้น การหาค่าที่ระบบยอมรับได้นี้ สามารถทำได้โดยการเปิดการการเชื่อมต่อกับระบบที่วิเคราะห์ จากนั้นหา

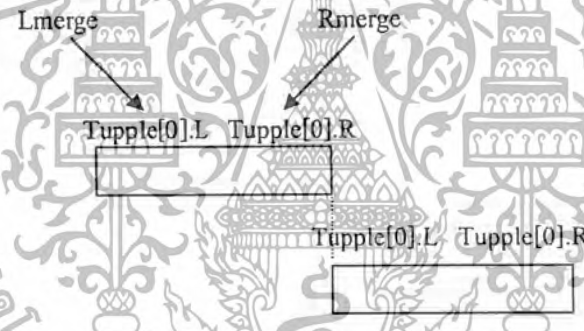
จำนวนแพ็กเก็ตที่เข้ามาในระบบในลักษณะการใช้งานปกติของแต่ละช่วงเวลา จากนั้นนำค่าสูงสุดที่ได้มาเป็นค่าที่ระบบยอมรับได้ โดยระบบที่วิเคราะห์มีค่าที่ยอมรับได้ประมาณ 20,000-30,000 แพ็กเก็ตต่อนาที

3.2.3.5 ความผิดปกติของแฟร็กเมนต์ (Fragmentation)

การตรวจสอบความผิดปกติของแฟร็กเมนต์มีขั้นตอนค่อนข้างซับซ้อน ซึ่งอธิบายตามประเภทของความผิดปกติ การส่งแพ็กเก็ตที่มีลำดับผิดปกติ และแพ็กเก็ตที่มีขนาดเลื่อมล้ำกัน การวิเคราะห์ความผิดปกติของแพ็กเก็ตในลักษณะนี้ ต้องวิเคราะห์หลังกระบวนการรีแอสเซมเบิ้ล ดังนั้นจึงนำบัฟเฟอร์เข้ามาช่วยในการเก็บข้อมูล เพื่อนำมาวิเคราะห์ ดังนี้

- Fragment Buffer

  คือ บัฟเฟอร์ที่เก็บข้อมูลในการวิเคราะห์ ซึ่งเก็บข้อมูลของแพ็กเก็ตไอพี และข้อมูลที่จำเป็นอื่นๆ ไว้ได้แก่ หมายเลขแพ็กเก็ต (ID), จำนวนแพ็กเก็ตที่มีหมายเลขแพ็กเก็ตเดียวกัน, แอดเดรสปลายทาง, ขอบซ้ายและขอบขวาของแพ็กเก็ต (Lmerge และ Rmerge) ซึ่งชี้โดยตัวแปร tupple ดังรูปที่ 3.9 จำนวน tupple และเฟล็กแสดงค่าของแพ็กเก็ต



รูปที่ 3.9 แสดงการเก็บข้อมูลใน fragment buffer ของตัวแปร tupple

- Overlap Buffer

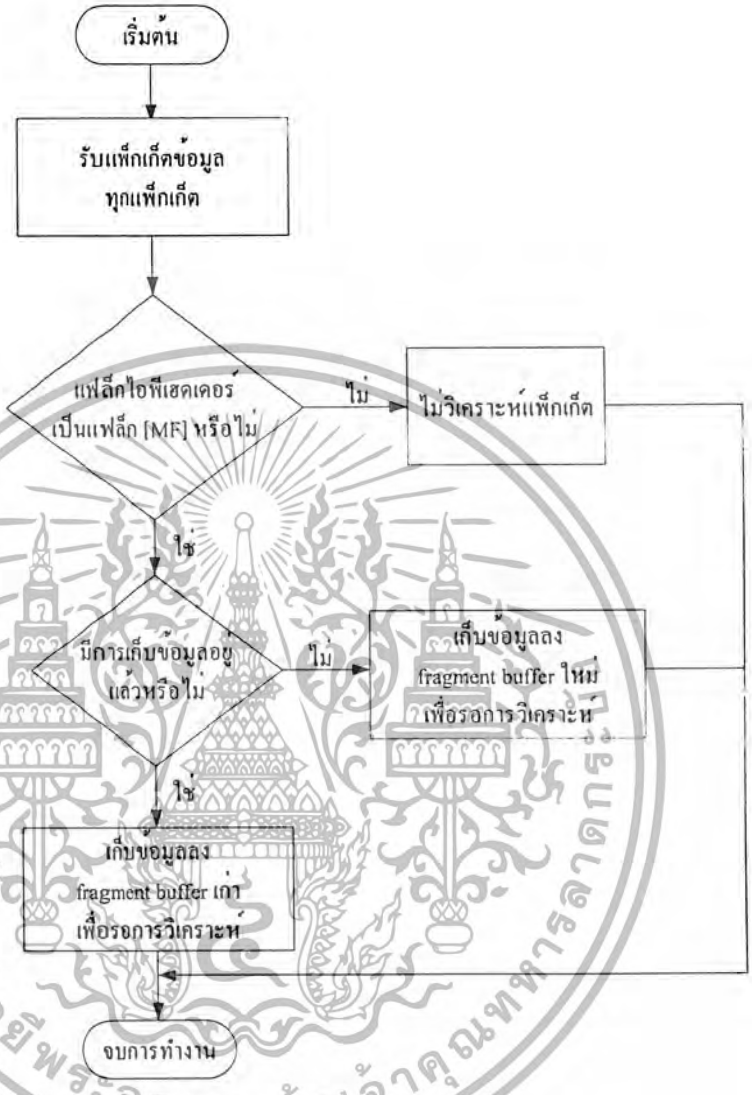
  คือ บัฟเฟอร์ที่เก็บข้อมูล เมื่อตรวจพบว่าเกิดการเหลื่อมล้ำของแพ็กเก็ต

- Gap Frame Buffer

  คือ บัฟเฟอร์ที่เก็บข้อมูล เมื่อตรวจพบว่าเกิดการประกอบเฟรมไม่ได้ในลักษณะมีช่องว่างระหว่างแพ็กเก็ต

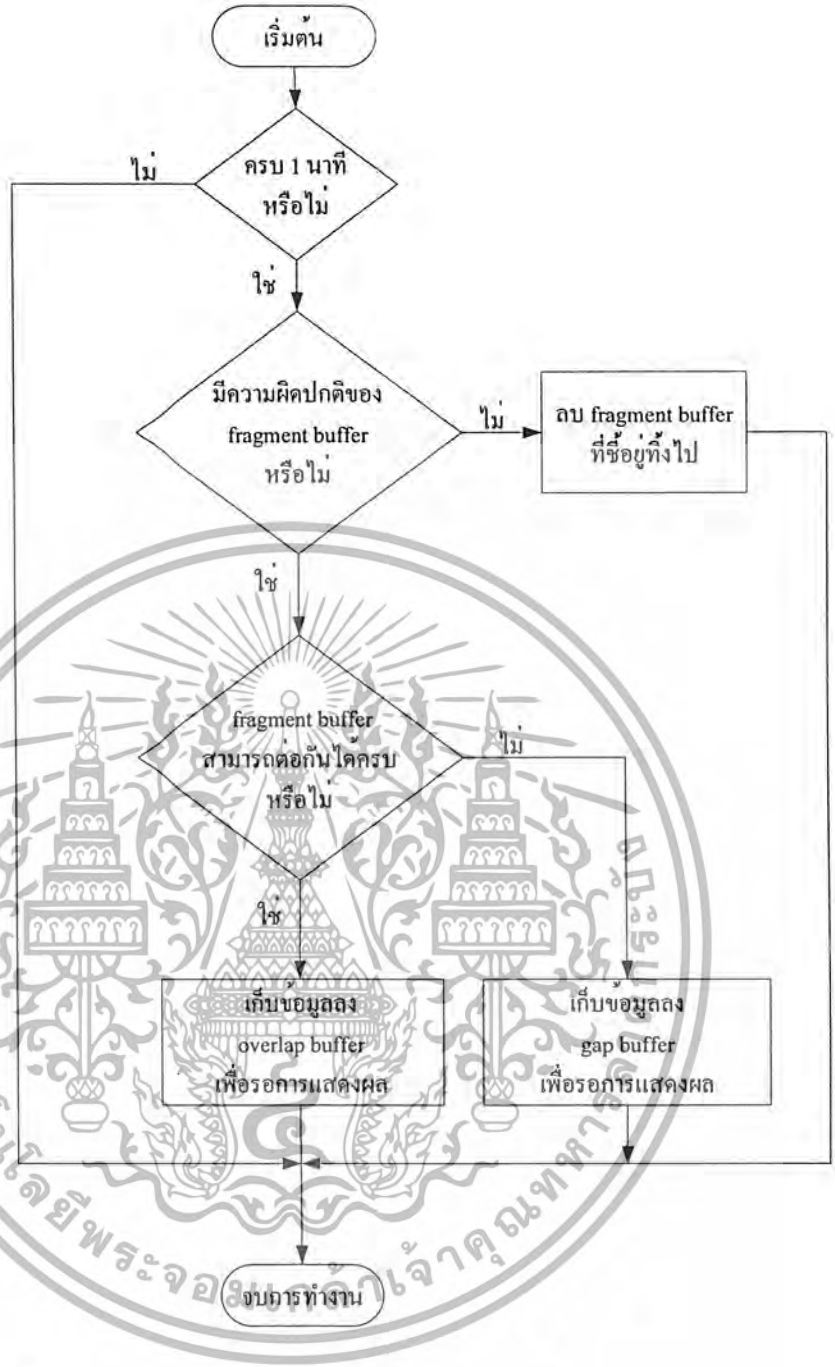
ข้อมูลที่เก็บไว้ของ Overlap Buffer และ Gap Frame Buffer มีโครงสร้างการเก็บข้อมูลที่มีส่วนประกอบเหมือนกัน ในการวิเคราะห์ใช้บัฟเฟอร์ทั้งสามนี้ร่วมกัน โดยเก็บข้อมูลแพ็กเก็ตที่เข้ามาทั้งหมดลงใน Fragment Buffer และหากแพ็กเก็ตที่ส่งมาสามารถรวมกันได้ก็รวมกันเป็นแพ็กเก็ตเดียวที่ต่อเนื่องกัน โดยดูจากขอบซ้ายและขอบขวา เช่น จากรูปที่ 3.9 หาก Tupple[0].R = Tupple[1].L แสดงว่าแพ็กเก็ตทั้งสองนี้สามารถเชื่อมต่อกันได้ ให้รวมเป็นแพ็กเก็ตเดียวกัน โดยแพ็กเก็ตใหม่มี Lmerge = Tupple[0].L และ Rmerge = Tupple[1].R แต่หากรวมกันแล้วเกิดความผิดปกติ ให้แจ้งมายัง Overlap Buffer และ Gap

Frame Buffer แล้ว แต่ชนิดความผิดปกติที่เกิดขึ้น กระบวนการวิเคราะห์แสดงไว้ดังรูปที่ 3.10 และ รูปที่ 3.11



รูปที่ 3.10 โฟลว์ชาร์ทแสดงการเก็บข้อมูลลง Fragment Buffer

แต่หากไม่มีความผิดปกติขึ้น เมื่อครบ 1 นาที โปรแกรมตรวจสอบจาก fragment Buffer ว่าหากมีแพ็กเก็ตใดยังไม่ได้ประกอบไม่ครบ ก็ให้เก็บไว้ใน Overlap Buffer หรือ Gap Frame Buffer เช่นเดียวกัน และเมื่อ ครบ 1 นาที ข้อมูลใน Overlap Buffer และ Gap Buffer นี้ จะออกมาที่หน้าจอ เพื่อแจ้งให้ผู้ดูแลระบบทราบ หรือเก็บไว้ในล็อกไฟล์ เพื่อบันทึกความผิดปกติที่เกิดขึ้นไว้ แต่หากไม่มีความผิดปกติใดๆ เกิดขึ้นเลย และแพ็กเก็ตเหล่านั้นสามารถประกอบเป็นเฟรมได้ อย่างถูกต้อง ให้ลบเฟรมเหล่านั้นออกจากบัฟเฟอร์ทันที เพื่อไม่ให้สิ้นเปลืองเนื้อที่ในการจัดเก็บ



รูปที่ 3.11 โฟลว์ชาร์ทแสดงการตรวจสอบความผิดปกติในการทำแฟร็กเมนเตชั่น (Fragmentation)

3.2.3.6 การส่งแพ็กเก็ตแบบวนลูป (Loop)

สามารถทำได้โดยการเปรียบเทียบค่าแอดแดรสต้นทาง และแอดเดรสปลายทางของแพ็กเก็ตหากไอพี เป็นค่าเดียวกันแสดงว่ามีความผิดปกติเกิดขึ้น เพราะทำให้เกิดการส่งในลักษณะวนลูป ซึ่งขั้นตอนการตรวจสอบเป็นไปตามรูปที่ 3.12

รูปที่ 3.12 แสดงการตรวจสอบแพ็กเก็ตที่ส่งแบบวนลูป (Loop)

3.2.4 ส่วนรายงานผลต่อผู้ใช้

รูปที่ 3.13 โฟลว์ชาร์ทแสดงการแสดงการรายงานผล

บทที่ 4

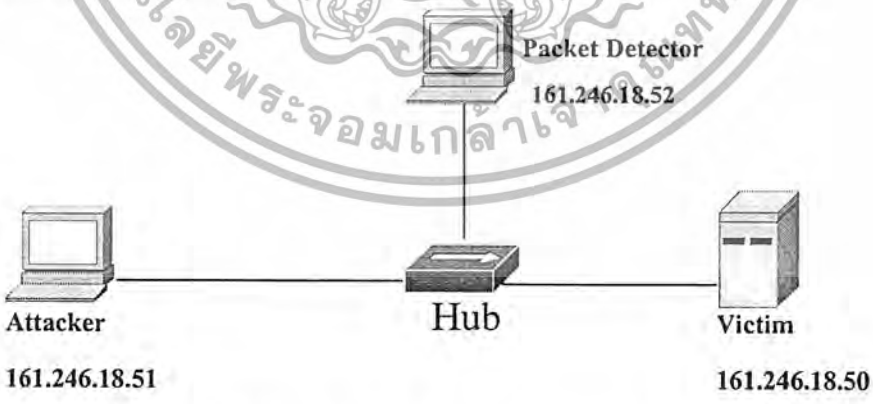
การทดลองและผลการทดลอง

4.1 อุปกรณ์การติดตั้งก่อนการทดสอบ

ขั้นตอนการทดสอบแพ็กเก็ตดีเทคเตอร์ (Packet Detector) ได้ทำการทดสอบโดยมีรายละเอียดของคอมพิวเตอร์ที่เกี่ยวข้องที่ใช้ทดสอบดังนี้

1. เครื่องที่ติดตั้งโปรแกรม (Packet Detector)
   - การ์ดแลนความเร็ว 100 Mb
   - IP address 161.246.18.52
   - ระบบปฏิบัติการลีนุกซ์เรดแฮท 9.0 เคอร์เนลเวอร์ชั่น 2.4.20-8
2. เครื่องที่ใช้ทำการโจมตี (Attacker)
   - การ์ดแลนความเร็ว 100 Mb
   - IP address 161.246.18.51
   - ระบบปฏิบัติการลีนุกซ์เรดแฮท 9.0 เคอร์เนลเวอร์ชั่น 2.4.20-8
3. เครื่องที่ใช้เป็นเหยื่อทดสอบ (Victim)
   - การ์ดแลนความเร็ว 100 Mb
   - IP address 161.246.18.50
   - ระบบปฏิบัติการลีนุกซ์เรดแฮท 9.0 เคอร์เนลเวอร์ชั่น 2.4.20-8
4. ฮับ

ระบบเครือข่ายที่ใช้ทดสอบในบทนี้ เป็นระบบที่ทำงานบนการ์ดแลนและอุปกรณ์ที่มีความเร็วทั้งระบบ 100 เมกกะบิต มีลักษณะดังรูปที่ 4.1



รูปที่ 4.1 แสดงโครงสร้างเครือข่ายในการทดสอบ

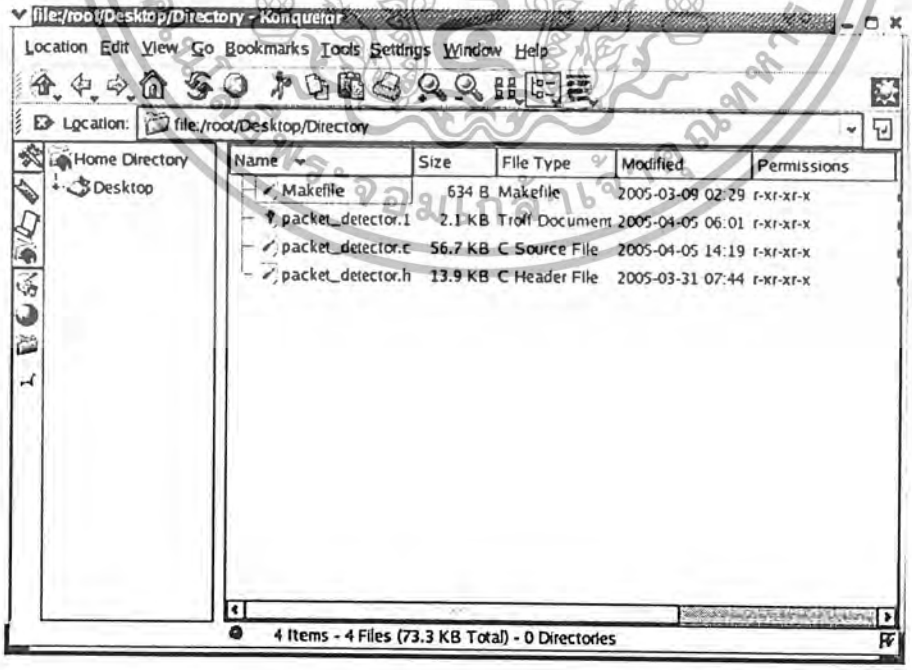
ก่อนติดตั้งระบบตรวจจับผู้บุกรุกทางเครือข่ายคอมพิวเตอร์ ผู้ติดตั้งต้องคำนึงถึงปัจจัยดังต่อไปนี้ เพื่อไม่ให้เกิดปัญหาในการติดตั้งดังนี้

1. ระบบนี้สร้างขึ้นบนระบบปฏิบัติการลีนุกซ์ Redhat 9.0 ดังนั้นจึงควรติดตั้งระบบบนระบบปฏิบัติการที่มีลักษณะใกล้เคียง หรือมีลักษณะเดียวกับระบบปฏิบัติการดังกล่าว ที่มีคอมไฟล์เลอร์ภาษาซีอยู่ด้วย
2. เครื่องที่ใช้ควรมีหน่วยความจำอย่างน้อย 400 KB (สำหรับโปรแกรมขณะทำงาน)
3. เครื่องที่ติดตั้งระบบต้องอยู่ในบรอดคาสโดเมน (Broadcast domain) เดียวกับเครื่องที่ต้องการตรวจจับ ซึ่งหมายถึงการที่สามารถรับข้อมูลแพ็กเก็ตที่ทั้งเครือข่ายนั้น ๆ ได้รับ หรือตรวจจับภายในเครื่องเดียวกัน
4. ต้องใช้สิทธิ์รูท (root) ของระบบในการใช้งานระบบ

การติดตั้งระบบตรวจจับผู้บุกรุกทางเครือข่ายคอมพิวเตอร์นั้น สามารถทำได้โดยใช้ขั้นตอนต่อไปนี้

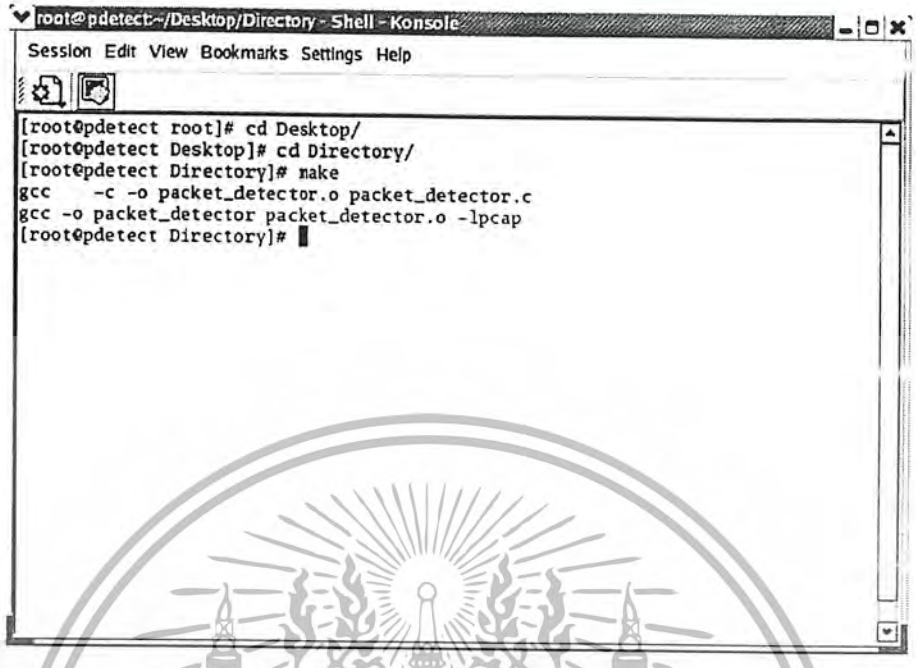
1. สร้างไดเร็กทอรีเพื่อเก็บไฟล์ที่ใช้ในการติดตั้ง โดยใช้คำสั่ง mkdir <ชื่อไดเร็กทอรี> แล้วนำไฟล์ต่างๆ ที่ใช้ในการติดตั้งไปไว้ในไดเร็กทอรีที่เตรียมไว้ ดังรูปที่ 4.2 ซึ่งได้แก่ ไฟล์ดังต่อไปนี้

- packet_detector.c
- packet_detector.h
- Makefile
- packet_detector.1



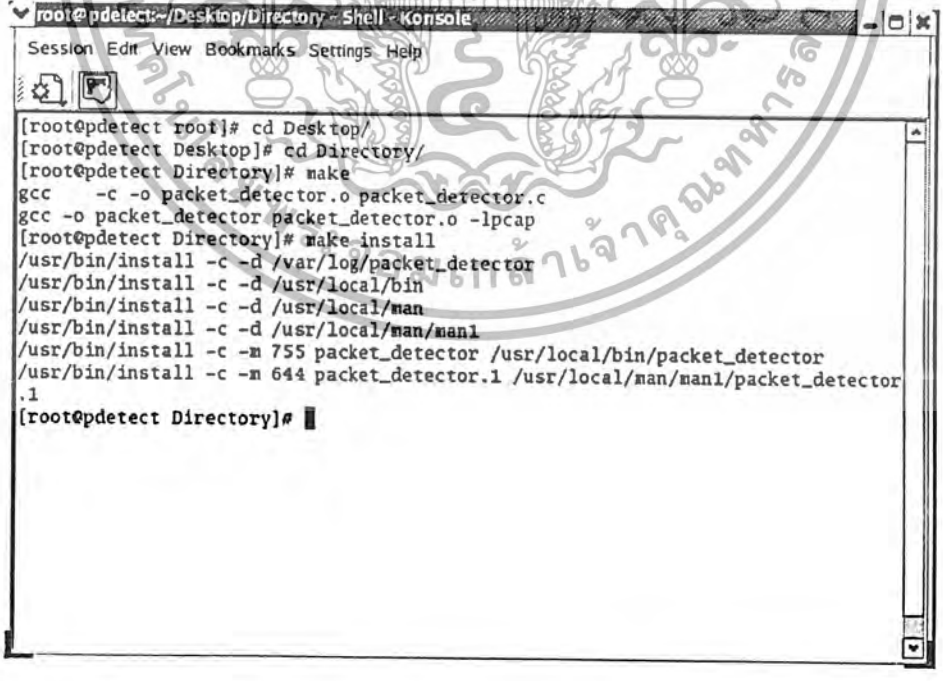
รูปที่ 4.2 แสดงไฟล์ที่ใช้ในการติดตั้ง

2. เรียกคำสั่ง make เพื่อคอมไฟล์โปรแกรมทั้งหมด ในไดเร็กทอรีที่เก็บไฟล์สำหรับการติดตั้ง ดังรูปที่ 4.3

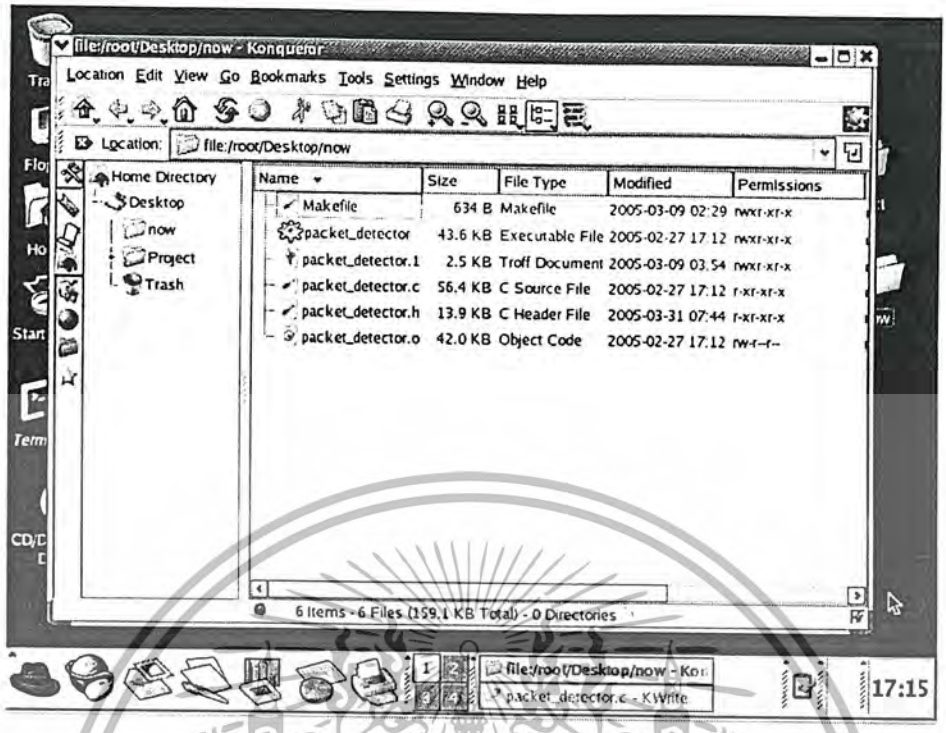


รูปที่ 4.3 แสดงการเรียกคำสั่ง make

3. จากนั้นเรียกคำสั่ง make install เพื่อสร้างที่เก็บ file ต่างๆ และ copy files ไปไว้ในไดเร็กทอรีที่กำหนด ดังรูปที่ 4.4



รูปที่ 4.4 แสดงการเรียกคำสั่ง make install



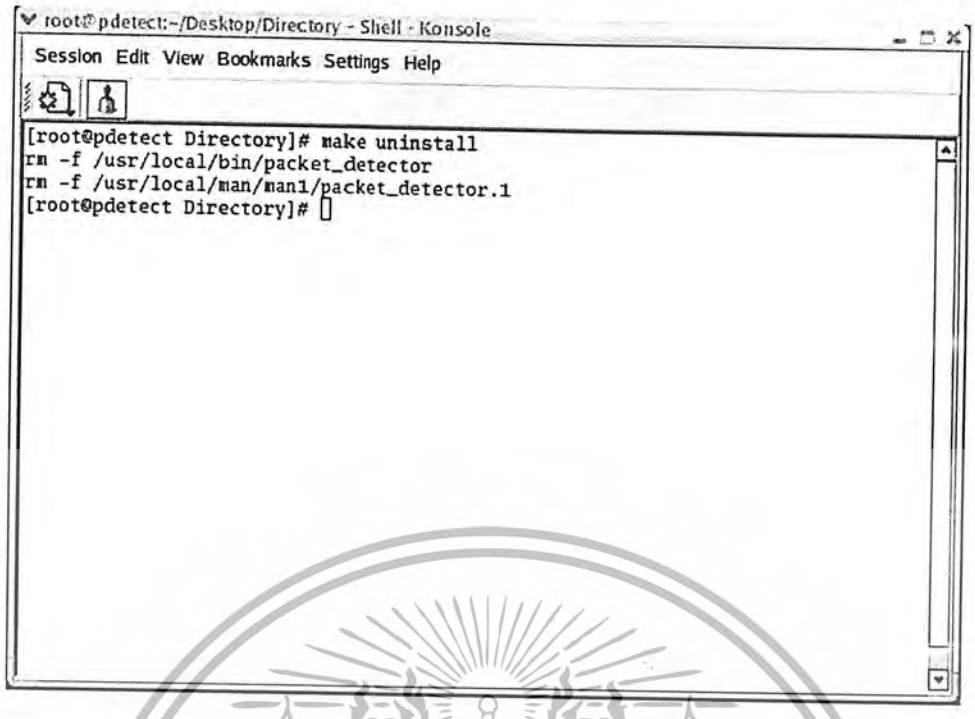
รูปที่ 4.5 แสดงไฟล์ทั้งหมดที่เกี่ยวข้องกับโปรแกรม

จากรูปที่ 4.5 เห็นได้ว่ามีการสร้างไดเร็กทอรีที่จำเป็นต่อการใช้งาน จากนั้นโปรแกรมจะนำไฟล์ต่างๆ ที่ต้องการใช้ไปไว้ในไดเร็กทอรีที่ใช้งานดังต่อไปนี้

- /usr/local/bin นำไฟล์ packet ซึ่งเป็นไฟล์ที่เรียกใช้งานระบบไปเก็บไว้
- /usr/local/man/man1 นำไฟล์ packet.1 ซึ่งเป็นแมนเพจไปเก็บไว้

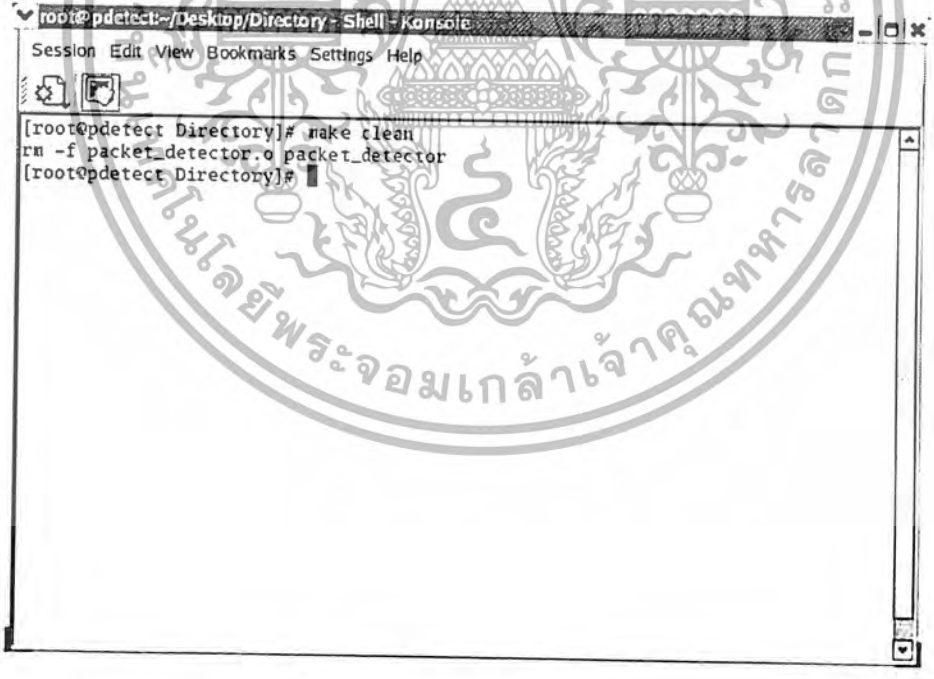
เมื่อติดตั้งระบบแล้ว แต่ไม่ต้องการใช้งานระบบอีก ผู้ใช้สามารถถอดระบบออกจากเครื่องได้ โดยมีขั้นตอนดังต่อไปนี้

(1) เรียกคำสั่ง make uninstall เพื่อลบไฟล์ต่างๆ ที่ไม่จำเป็นต้องใช้ในไดเร็กทอรีที่เก็บไฟล์เหล่านั้น ดังรูปที่ 4.6



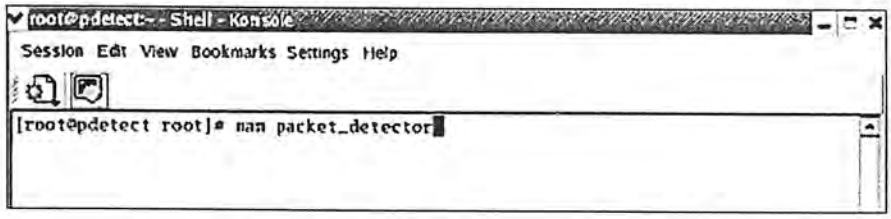
รูปที่ 4.6 แสดงการเรียกคำสั่ง make uninstall

(2) จากนั้นเรียกคำสั่ง make clean เพื่อลบ object files ทั้งหมดออก ดังรูปที่ 4.7

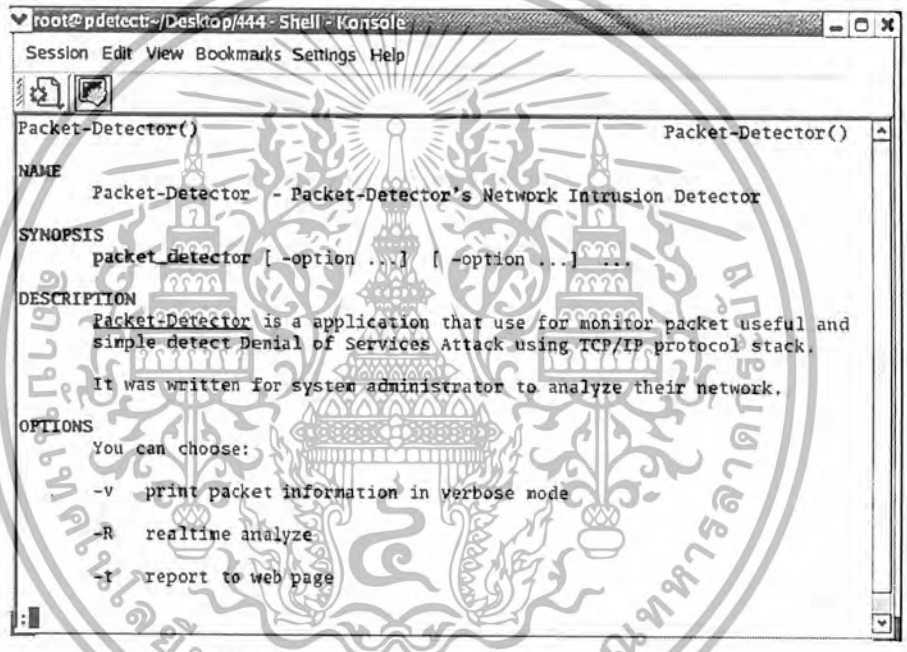


รูปที่ 4.7 แสดงการเรียกคำสั่ง make clean

หากเกิดปัญหาในการใช้งานผู้ใช้สามารเรียกขอความช่วยเหลือจากระบบได้ โดยการเรียกแมนเพจขึ้นมาดู โดยใช้คำสั่ง man packet_detector ซึ่งนำเสนอออปชั่นต่างๆ ที่ให้เลือกใช้งาน และข้อมูลต่างๆ เกี่ยวกับระบบ ดังรูปที่ 4.8



รูปที่ 4.8 การพิมพ์คำสั่ง man page



รูปที่ 4.9 แสดงผลหน้าจอหน้าต่าง man page

การเรียกใช้งานระบบ สามารถเรียกใช้ได้บนคอมมานไลน์ที่หน้าจอเทอร์มินอลของระบบปฏิบัติการลีนุกซ์ โดยเรียกใช้คำสั่ง packet_detector - <option> โดยมีคำสั่งให้เลือกใช้ที่เกี่ยวข้องกับการออกแบบและการสร้างดังนี้

- v	พิมพ์ข้อมูลของแพ็กเก็ตที่เก็บได้ออกหน้าจอ
- R	ตรวจสอบการโจมตีแบบตามเวลาจริง
- t	แสดงผลออกทางเว็บเพจ

4.2 เครื่องมือที่ใช้ทดสอบการโจมตี

เนื่องจากในปัจจุบันได้มีผู้พัฒนาเครื่องมือที่ใช้ในการโจมตี เพื่อให้ปฏิเสธการให้บริการกันอย่างมากมาย ส่วนใหญ่สามารถดาวน์โหลดได้ฟรีจากอินเทอร์เน็ต ความแตกต่างกันของเครื่องมือแต่ละตัวคือรูปแบบการโจมตีและระดับความรุนแรงในการโจมตี

การทดสอบการทำงานในบทนี้ได้เลือกเครื่องมือที่ได้รับความนิยมใช้กันอย่างแพร่หลาย และมีระดับความรุนแรงสูงมาใช้ทำการทดสอบ โดยมีรายชื่อเครื่องมือที่เลือกใช้พารามิเตอร์ที่สั่งให้เครื่องมือดังกล่าวทำงาน ดังนี้

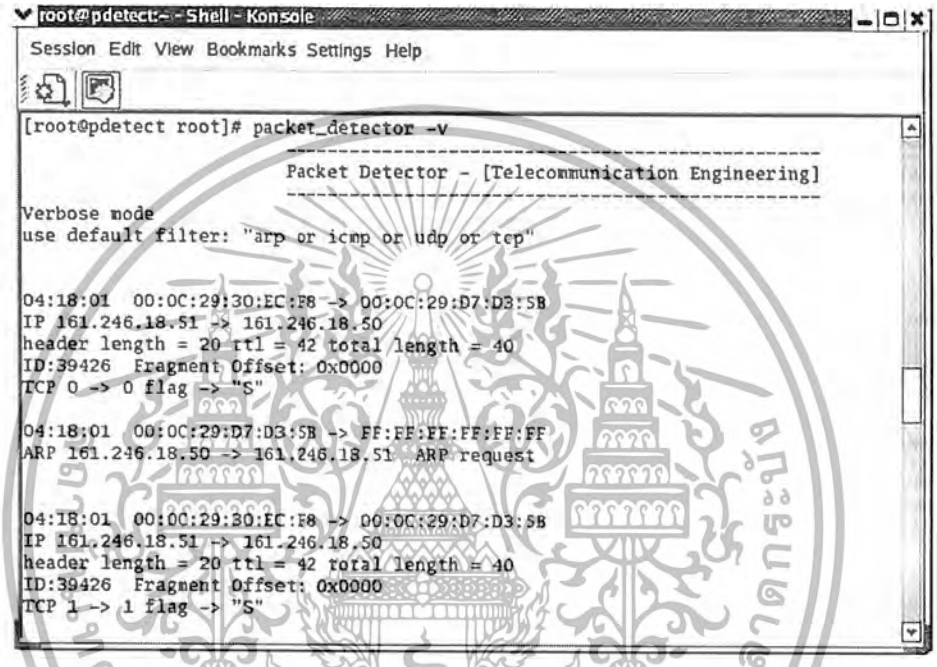
ประเภทของการโจมตี	เครื่องมือที่ใช้และพารามิเตอร์ที่ระบุ
ปิงสวีป	nmap -sP 161.246.18.0/24
สแกนพอร์ต	nmap -sT –sU 161.246.18.50
ตรวจสอบระบบปฏิบัติการ	nmap –O 161.246.18.50
แพ็กเก็ตจำนวนมาก	./synflood 161.246.18.51 161.246.18.50 8000 50000
แพ็กเก็ตแบบวนลูป	./scanspoof 161.246.18.50 161.246.18.50 500
แฟร็กเมนต์ที่เหลื่อมล้ำกัน	./teardrop 161.246.18.51 161.246.18.50 –n 60000
แฟร็กเมนต์ที่เกิดช่องว่าง	./jolt 161.246.18.50 161.246.18.51 10000
โจมตีแบบผสม	./scanspoof 161.246.18.50 161.246.18.50 65000

ตารางที่ 4.1 แสดงชื่อโปรแกรมบางส่วนที่ใช้ทดสอบการบุกรุกแบบต่างๆ

4.3 การทดลองส่วนการแสดงผลข้อมูลออกทางหน้าจอ

ในขั้นตอนนี้เป็นการเก็บข้อมูลของแพ็กเก็ตที่เข้าสู่ระบบ โดยผู้ใช้อาจเลือกให้ระบบเก็บข้อมูลดังกล่าวลงล็อกไฟล์ หรือแสดงข้อมูลของแพ็กเก็ตเหล่านั้นบนหน้าจอก็ได้

กรณีต้องการดูแพ็กเก็ตโดยไม่ต้องการเก็บข้อมูลเหล่านั้นไว้ ผู้ใช้สามารถเลือกใช้ออปชั่น packet_detector –v ตามโฟลว์ชาร์ทรูปที่ 3.1 ซึ่งเมื่อสั่งคำสั่งดังกล่าว ระบบจะแสดงข้อมูลของแพ็กเก็ตที่เข้าสู่ระบบผ่านหน้าจอเทอร์มินอล โดยแสดงข้อมูลของเฮดเดอร์ของแพ็กเก็ตทั้งของทีซีพี/ไอพี และอีเทอร์เน็ตบางส่วน รวมทั้งวันและเวลาที่แพ็กเก็ตเหล่านั้นเข้ามาด้วย ดังรูปที่ 4.10

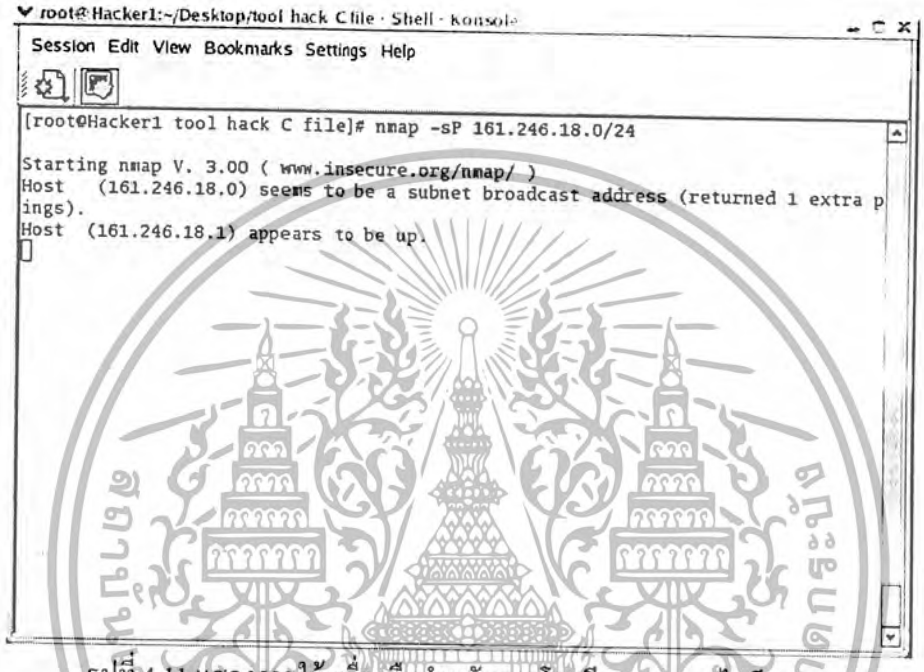


รูปที่ 4.10 แสดงการแสดงผลข้อมูลแพ็กเก็ตผ่านหน้าจอเทอร์มินอล

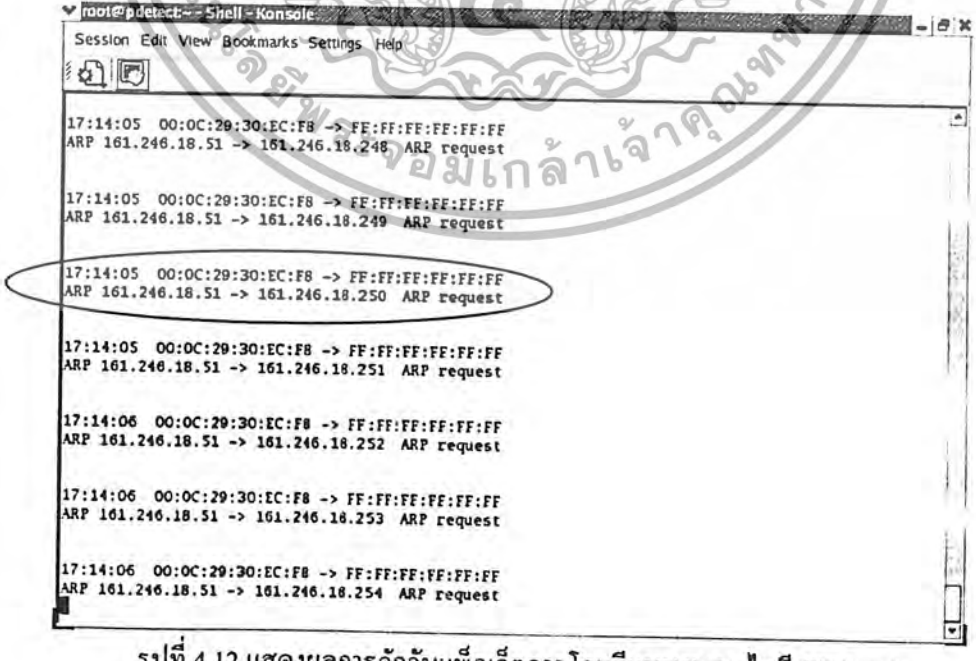
ในลักษณะการทำงานแบบนี้จะไม่มีการตรวจสอบการบุกรุก แต่จะเป็นเพียงการแสดงผลข้อมูลที่วิ่งผ่านเครือข่าย การดูข้อมูลของแพ็กเก็ตในลักษณะนี้มีข้อดีที่ไม่ต้องเปลืองเนื้อที่ในการเก็บข้อมูล แต่เป็นเพียงการเรียกดูข้อมูลอย่างเดียว ไม่ได้มีการเก็บข้อมูลของแพ็กเก็ตที่เข้ามาในระบบไว้เลย

4.3.1 การทดลองการโจมตีแบบสแกนไอพี (IP Scan)

ทำการทดลองการโจมตีจากเครื่องที่ใช้ทำการโจมตีโดยมีหมายเลขไอพี 161.246.18.51 โดยใช้การโจมตีแบบ สแกนไอพี ซึ่งใช้โปรแกรมการโจมตีดังตารางที่ 4.1 โดยโจมตีไปยังเครื่องที่ใช้เป็นเหยื่อทดสอบหมายเลขไอพี 161.246.18.50 โดยใช้เครื่องที่ติดตั้งโปรแกรมแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 ผลที่ได้จากเครื่องที่ใช้โจมตีที่มีหมายเลขไอพี 161.246.18.51 คือ หมายเลขไอพีที่เครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายที่ทำการสแกนนั้นกำลังเปิดใช้งานอยู่ ดังรูปที่ 4.11



รูปที่ 4.11 แสดงการใช้เครื่องมือสำหรับการโจมตีแบบสแกนไอพี (IP Scan)



รูปที่ 4.12 แสดงผลการดักจับแพ็กเก็ตการโจมตีแบบสแกนไอพี (IP Scan)

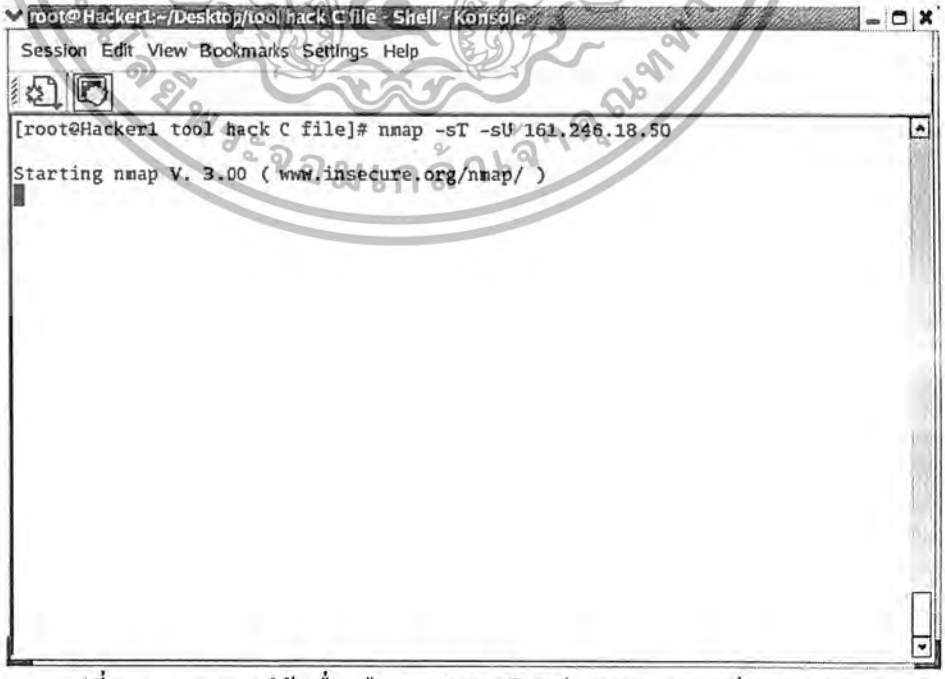
จากการทดลอง ผลที่ได้จากการดักจับแพ็กเก็ตจากเครื่องที่ทำการติดตั้งแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 แสดงดังรูปที่ 4.12 ซึ่งผลที่ออกมาทางหน้าจอแสดงผลนั้น จะอธิบายหนึ่งแพ็กเก็ตเป็นตัวอย่างมีความหมายเรียงลำดับ ดังนี้คือ

1. เวลาที่ดักจับแพ็กเก็ต คือ เวลาที่ 17 นาฬิกา 14 นาที 6 วินาที
2. มีค่า แมคแอดเดรส เครื่องต้นทางเป็น 00:0C:29:30:EC:F8
3. มีค่า แมคแอดเดรส เครื่องปลายทางเป็น FF:FF:FF:FF:FF:FF
4. ชนิดโพรโตคอลเป็นแบบ ARP
5. มีหมายเลขไอพีต้นทางเป็น 161.246.18.51
6. มีหมายเลขไอพีปลายทางเป็น 161.246.18.250
7. ชนิดของโพรโตคอล ARP เป็นแบบ ARP request

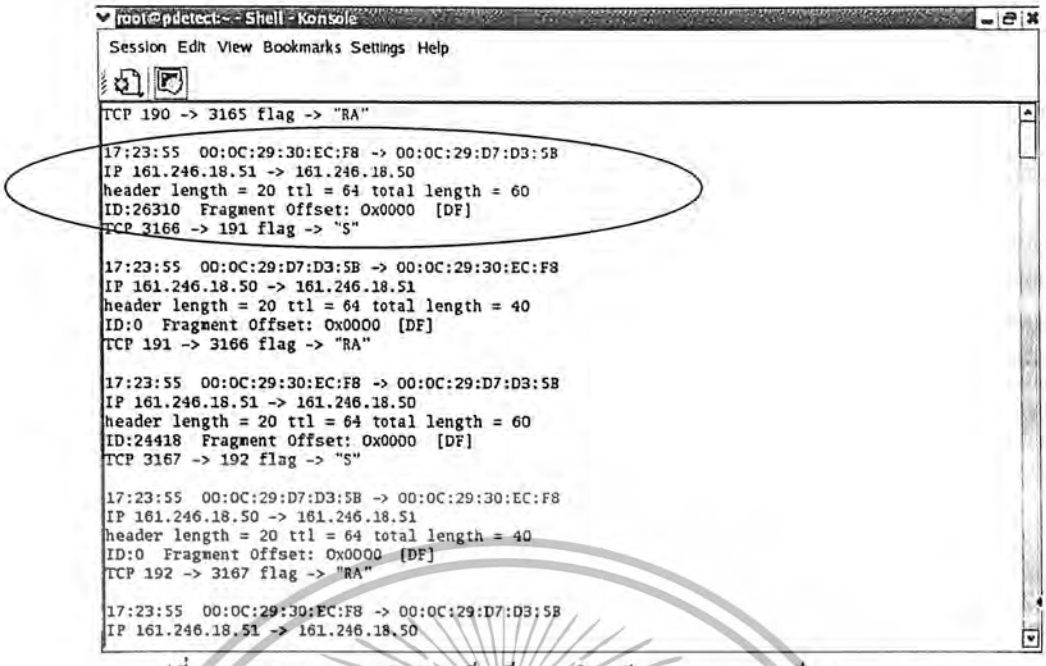
เมื่อดูจากผลการดักจับแพ็กเก็ตโดยรวม จะสังเกตเห็นว่าเป็นแพ็กเก็ตที่เป็นเออาร์พีรีเควสต์โดยมีหมายเลขไอพีเพิ่มขึ้นเรื่อย ๆ ทำให้ผู้ใช้งานสามารถคาดเดาได้ว่าได้เกิดการบุกรุกแบบ สแกนไอพี ในเครือข่าย 161.246.18.0 นี้แล้ว

4.3.2 การทดลองการโจมตีแบบสแกนพอร์ต (Scan Port)

ทำการทดลองการโจมตีจากเครื่องที่ใช้ทำการโจมตีโดยมีหมายเลขไอพี 161.246.18.51 โดยใช้การโจมตีแบบ สแกนพอร์ท ซึ่งใช้โปรแกรมการโจมตีดังตารางที่ 4.1 ซึ่งได้แสดงวิธีใช้ดังรูปที่ 4.13 โดยโจมตีไปยังเครื่องที่ใช้เป็นเหยื่อทดสอบหมายเลขไอพี 161.246.18.50 โดยใช้เครื่องที่ติดตั้งโปรแกรมแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 ผลที่ได้จากเครื่องที่ใช้โจมตีที่มีหมายเลขไอพี 161.246.18.51 คือจะได้หมายเลขพอร์ตปลายทางที่เครื่องคอมพิวเตอร์ที่อยู่ในหมายเลขไอพีปลายทาง ที่ทำการสแกนนั้นกำลังเปิดใช้งานอยู่



รูปที่ 4.13 แสดงการใช้เครื่องมือสำหรับการโจมตีแบบสแกนพอร์ต (Scan Port)



รูปที่ 4.14 แสดงผลการดักจับแพ็กเก็ตการโจมตีแบบสแกนพอร์ต (Scan Port)

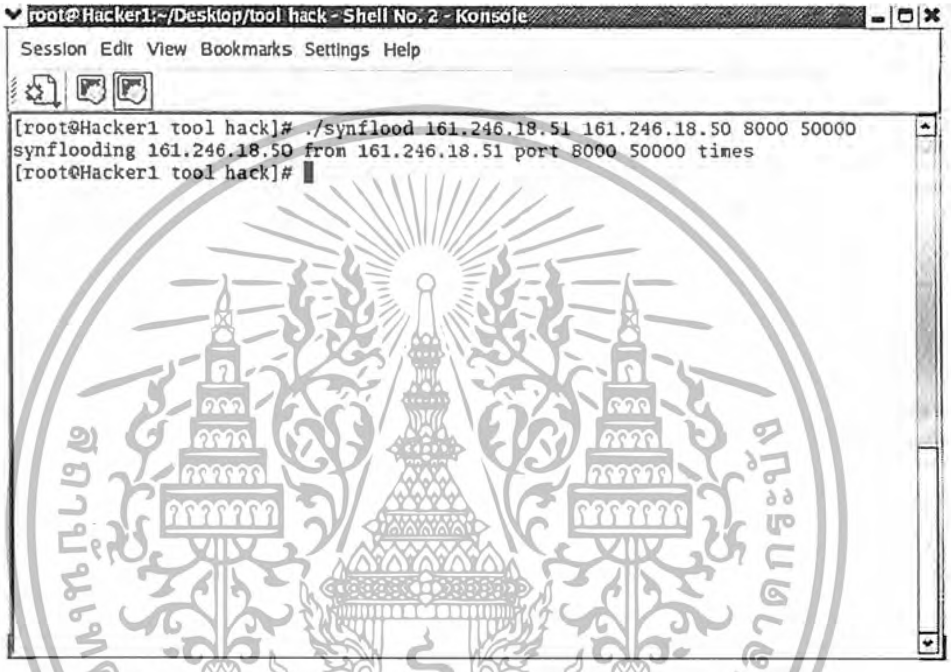
จากการทดลอง ผลที่ได้จากการดักจับแพ็กเก็ตจากเครื่องที่ทำการติดตั้งแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 แสดงดังรูปที่ 4.14 ซึ่งผลที่ออกมาทางหน้าจอแสดงผลนั้น จะอธิบายหนึ่งแพ็กเก็ตเป็นตัวอย่างมีความหมายเรียงลำดับ ดังนี้คือ

1. เวลาที่ดักจับแพ็กเก็ต คือ เวลาที่ 17 นาฬิกา 23 นาที 55 วินาที
2. มีค่า แมคแอดเดรส เครื่องต้นทางเป็น 00:0C:29:30:EC:F8
3. มีค่า แมคแอดเดรส เครื่องปลายทางเป็น 00:0C29:D7:D3:5B
4. มีหมายเลข ไอพีต้นทางเป็น 161.246.18.51
5. มีหมายเลข ไอพีปลายทางเป็น 161.246.18.50
6. มีความยาวเฮดเดอร์ไอพีเท่ากับ 20 ไบต์ ซึ่งแปลว่าไม่มีส่วนของ ไอพีออปชั่น
7. มีค่า ttl เท่ากับ 64
8. มีความยาวของแพ็กเก็ตทั้งหมดเท่ากับ 60 ไบต์
9. มีหมายเลขไอดีเท่ากับ 26310
10. มีแฟร็กเมนท์ออฟเซ็ทเป็นแฟล็ก [DF] ซึ่งหมายความว่าไม่มีการ fragment แพ็กเก็ต
11. ชนิดโพรโตคอลเป็นแบบ TCP
12. มีพอร์ทต้นทางเป็น 3166 และพอร์ตปลายทางเป็น 191
13. มีแฟล็กทีซีพีเป็นแฟล็ก SYN ซึ่งหมายถึงแฟล็ก SYN นั่นเอง

เมื่อดูจากผลการดักจับแพ็กเก็ตโดยรวม ซึ่งแสดงข้อมูลต่าง ๆ ออกมา จะสังเกตได้ว่ามีหมายเลขไอพีต้นทางเป็น 161.246.18.51 ส่งแพ็กเก็ตที่มีลักษณะพอร์ทปลายทางเป็นลำดับ และมีแฟล็กทีซีพีเป็น SYN ทำให้ผู้ใช้งานสามารถคาดเดาได้ว่าได้เกิดการบุกรุกแบบ สแกนพอร์ท ในเครือข่าย 161.246.18.0 นี้แล้ว

4.3.3 การทดลองการโจมตีแบบการส่งแพ็กเก็ตปริมาณมาก (Amount of Packets Sending)

ทำการทดลองการโจมตีจากเครื่องที่ใช้ทำการโจมตีโดยมีหมายเลขไอพี 161.246.18.51 โดยใช้การโจมตีแบบ การส่งแพ็กเก็ตเป็นปริมาณมาก ซึ่งใช้โปรแกรมการโจมตีดังตารางที่ 4.1 ซึ่งได้แสดงวิธีใช้ดังรูปที่ 4.15 โดยโจมตีไปยังเครื่องที่ใช้เป็นเหยื่อทดสอบหมายเลขไอพี 161.246.18.50 โดยใช้เครื่องที่ติดตั้งโปรแกรมแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 ผลที่ได้จากเครื่องที่ใช้โจมตีที่มีหมายเลขไอพี 161.246.18.51 คือเครื่องดังกล่าวจะทำการส่งแพ็กเก็ตที่มีทีซีพีแฟล็ก SYN ไปยังเครื่องเป้าหมาย โดยส่งไปที่พอร์ต 8,000 ด้วยจำนวน 50,000 แพ็กเก็ต



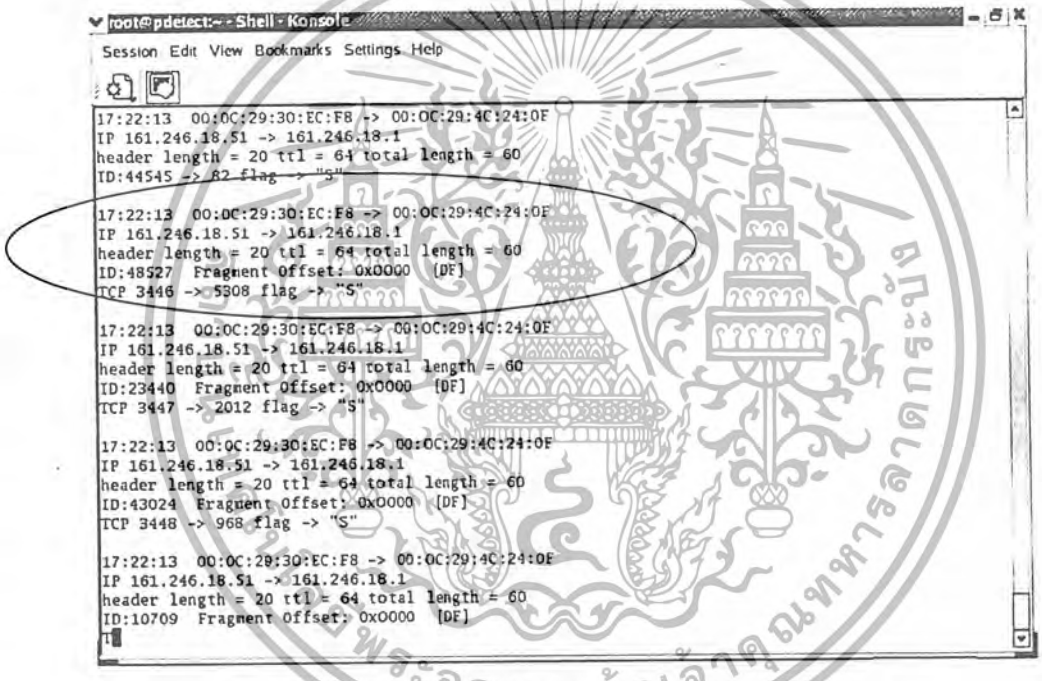
รูปที่ 4.15 แสดงการใช้เครื่องมือสำหรับการโจมตีแบบการส่งแพ็กเก็ต ปริมาณมาก (Amount of Packets Sending)

จากการทดลอง ผลที่ได้จากการดักจับแพ็กเก็ตจากเครื่องที่ทำการติดตั้งแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 แสดงดังรูปที่ 4.16 ซึ่งผลที่ออกมาทางหน้าจอแสดงผลนั้น จะอธิบายหนึ่งแพ็กเก็ตเป็นตัวอย่างมีความหมายเรียงลำดับ ดังนี้คือ

1. เวลาที่ดักจับแพ็กเก็ต คือ เวลาที่ 17 นาฬิกา 22 นาที 13 วินาที
2. มีค่า แมคแอดเดรส เครื่องต้นทางเป็น 00:0C:29:30:EC:F8
3. มีค่า แมคแอดเดรส เครื่องปลายทางเป็น 00:0C29:4C:24:0F
4. มีหมายเลขไอพีต้นทางเป็น 161.246.18.51
5. มีหมายเลขไอพีปลายทางเป็น 161.246.18.1
6. มีความยาวเฮดเดอร์ไอพีเท่ากับ 20 ไบต์ ซึ่งแปลว่าไม่มีส่วนของ ไอพีออปชั่น

7. มีค่า ttl เท่ากับ 64
8. มีความยาวของแพ็กเก็ตทั้งหมดเท่ากับ 60 ไบต์
9. มีหมายเลขไอดีเท่ากับ 48527
10. มีแฟร็กเมนท์ออฟเซ็ทเป็นแฟล็ก [DF] ซึ่งหมายความว่าไม่มีการแฟร็กเมนต์ แพ็กเก็ต
11. ชนิดโพรโตคอลเป็นแบบ ทีซีพี
12. มีพอร์ทต้นทางเป็น 3446 และพอร์ตปลายทางเป็น 5308
13. มีแฟล็กทีซีพีเป็นแฟล็ก SYN ซึ่งหมายถึงแฟล็ก SYN นั่นเอง

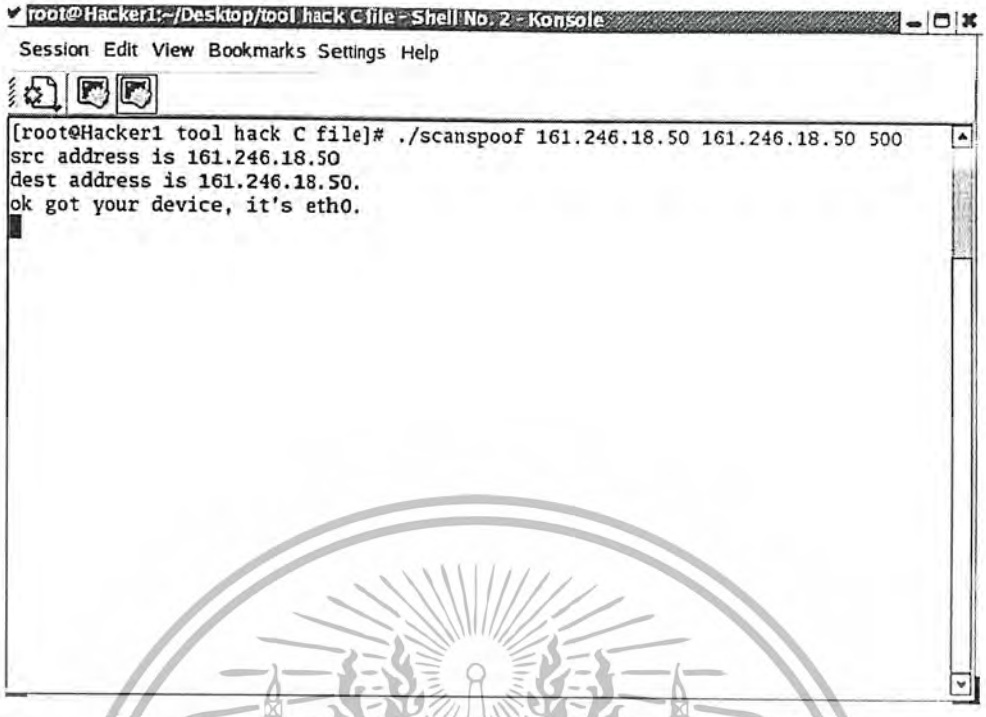
เมื่อดูจากผลการดักจับแพ็กเก็ตโดยรวม ซึ่งแสดงข้อมูลต่าง ๆ ออกมา จะสังเกตได้ว่ามีหมายเลขไอพีต้นทางเป็น 161.246.18.51 ผู้ใช้งานต้องทำการสำรวจเครือข่ายว่า เครือข่ายนั้น ๆ มีจำนวนแพ็กเก็ตมากเกินไปหรือไม่ ถ้าส่งแพ็กเก็ตปริมาณมาก ในเครือข่าย 161.246.18.0 นี้แล้ว



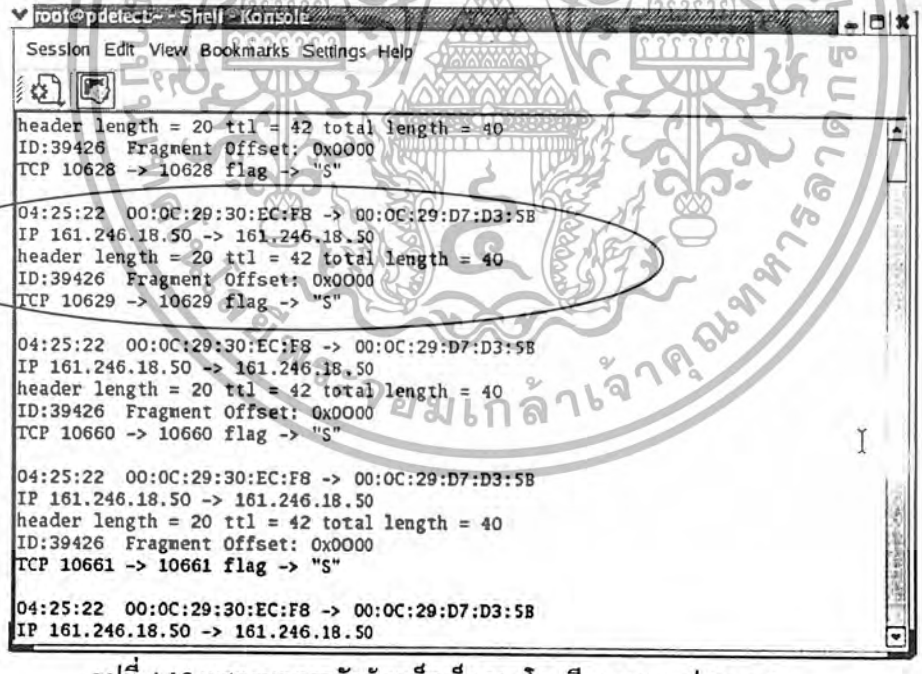
รูปที่ 4.16 แสดงผลการดักจับแพ็กเก็ตการโจมตีแบบการส่งแพ็กเก็ตปริมาณมาก (Amount of Packets Sending)

4.3.4 การทดลองการโจมตีแบบวนลูป (Loop)

ทำการทดลองการโจมตีจากเครื่องที่ใช้ทำการโจมตีโดยมีหมายเลขไอพี 161.246.18.51 โดยใช้การโจมตีแบบ การส่งแพ็กเก็ตแบบวนลูป ซึ่งใช้โปรแกรมการโจมตีดังตารางที่ 4.1 ซึ่งได้แสดงวิธีใช้ดังรูปที่ 4.17 โดยโจมตีไปยังเครื่องที่ใช้เป็นเหยื่อทดสอบหมายเลขไอพี 161.246.18.50 โดยใช้เครื่องที่ติดตั้งโปรแกรมแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 ผลที่ได้จากเครื่องที่ใช้โจมตีที่มีหมายเลขไอพี 161.246.18.51 คือเครื่องดังกล่าวจะทำการส่งแพ็กเก็ตที่มีหมายเลขไอพี 161.246.18.50 ซึ่งเป็นการใช้เทคนิค ไอพีสปูฟิ่ง โดยส่งไปยังเครื่องเป้าหมายหมายเลขไอพี 161.246.18.50 ด้วยจำนวน 500 แพ็กเก็ต



รูปที่ 4.17 แสดงการใช้เครื่องมือสำหรับการโจมตีแบบวนลูป (Loop)



รูปที่ 4.18 แสดงผลการดักจับแพ็กเก็ตการโจมตีแบบวนลูป (Loop)

จากการทดลอง ผลที่ได้จากการดักจับแพ็กเก็ตจากเครื่องที่ทำการติดตั้งแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 แสดงดังรูปที่ 4.18 ซึ่งผลที่ออกมาทางหน้าจอแสดงผลนั้น จะอธิบายหนึ่งแพ็กเก็ตเป็นตัวอย่างมีความหมายเรียงลำดับ ดังนี้คือ

1. เวลาที่ดักจับแพ็กเก็ต คือ เวลาที่ 17 นาฬิกา 22 นาที 13 วินาที
2. มีค่า แมคแอดเดรส เครื่องต้นทางเป็น 00:0C:29:30:EC:F8
3. มีค่า แมคแอดเดรส เครื่องปลายทางเป็น 00:0C29:D7:D3:5B
4. มีหมายเลขไอพีต้นทางเป็น 161.246.18.50 ซึ่งเป็นหมายเลขไอพีเดียวกันกับปลายทาง
5. มีหมายเลขไอพีปลายทางเป็น 161.246.18.50
6. มีความยาวเฮดเดอร์ไอพีเท่ากับ 20 ไบต์ ซึ่งแปลว่าไม่มีส่วนของ ไอพีออปชั่น
7. มีค่า ttl เท่ากับ 64
8. มีความยาวของแพ็กเก็ตทั้งหมดเท่ากับ 60 ไบต์
9. มีหมายเลขไอดีเท่ากับ 39426 ซึ่งเมื่อสังเกตแพ็ตเก็ตอื่นก็จะมีหมายเลขไอดีเดียวกัน
10. มีแฟร็กเมนท์ออฟเซ็ตไม่ระบุ
11. ชนิดโพรโตคอลเป็นแบบ ทีซีพี
12. มีพอร์ทต้นทางเป็น 10629 และพอร์ตปลายทางเป็น 10629
13. มีแฟล็กทีซีพีเป็นแฟล็ก S ซึ่งหมายถึงแฟล็ก SYN นั่นเอง

เมื่อดูจากผลการดักจับแพ็กเก็ตโดยรวม ซึ่งแสดงข้อมูลต่าง ๆ ออกมา จะสังเกตได้ว่ามีหมายเลขไอพีต้นทางเป็น 161.246.18.51 ส่งแพ็กเก็ตที่มีลักษณะ มีแฟล็กทีซีพีเป็น SYN อย่างต่อเนื่องและส่งมาหลายแพ็กเก็ตทำให้ผู้ใช้งานสามารถคาดเดาได้ว่าได้เกิดการบุกรุกแบบ ส่งแพ็กเก็ตปริมาณมาก ในเครือข่าย 161.246.18.0 นี้แล้ว

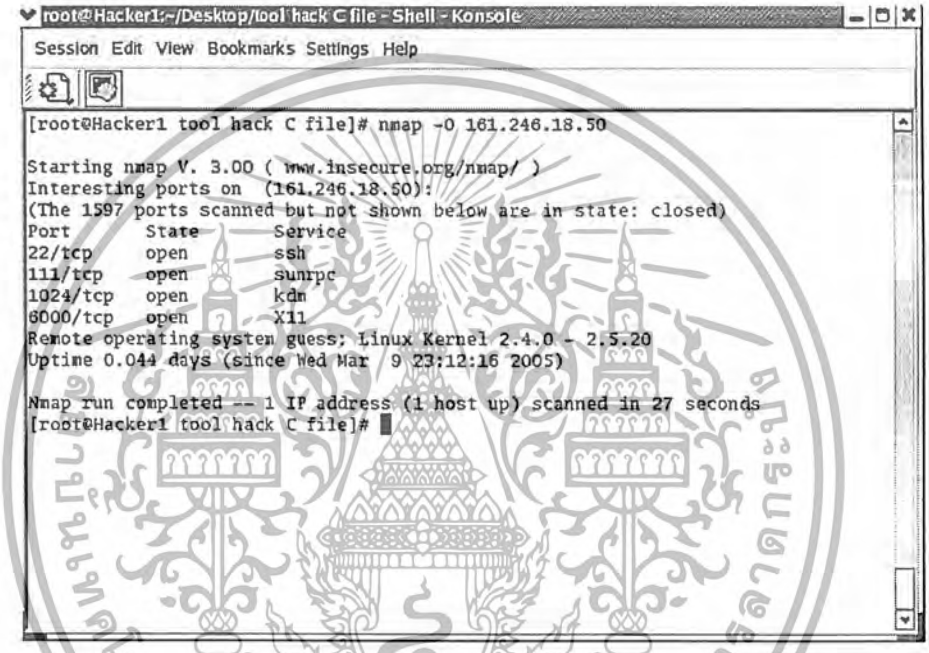
4.3.5 การทดลองการโจมตีแบบการตรวจสอบระบบปฏิบัติการ (Finger Print)

ทำการทดสองการโจมตีจากเครื่องที่ใช้ทำการโจมตีโดยมีหมายเลขไอพี 161.246.18.51 โดยใช้การโจมตีแบบ การตรวจสอบระบบปฏิบัติการ ซึ่งใช้โปรแกรมการโจมตีดังตารางที่ 4.1 ซึ่งได้แสดงวิธีใช้ดังรูปที่ 4.19 โดยโจมตีไปยังเครื่องที่ใช้เป็นเหยื่อทดสอบหมายเลขไอพี 161.246.18.50 โดยใช้เครื่องที่ติดตั้งโปรแกรมแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 ผลที่ได้จากเครื่องที่ใช้โจมตีที่มีหมายเลขไอพี 161.246.18.51 คือเครื่องดังกล่าวจะทำการส่งแพ็กเก็ตที่มีทีซีพีแฟล็กหลายรูปแบบ เพื่อที่จะนำผลการตอบกลับจากเครื่องเป้าหมายไปวิเคราะห์ว่าเป็นระบบปฏิบัติการอะไร

จากการทดลอง ผลที่ได้จากการดักจับแพ็กเก็ตจากเครื่องที่ทำการติดตั้งแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 แสดงดังรูปที่ 4.20 ซึ่งผลที่ออกมาทางหน้าจอแสดงผลนั้น จะอธิบายหนึ่งแพ็กเก็ตเป็นตัวอย่างมีความหมายเรียงลำดับ ดังนี้คือ

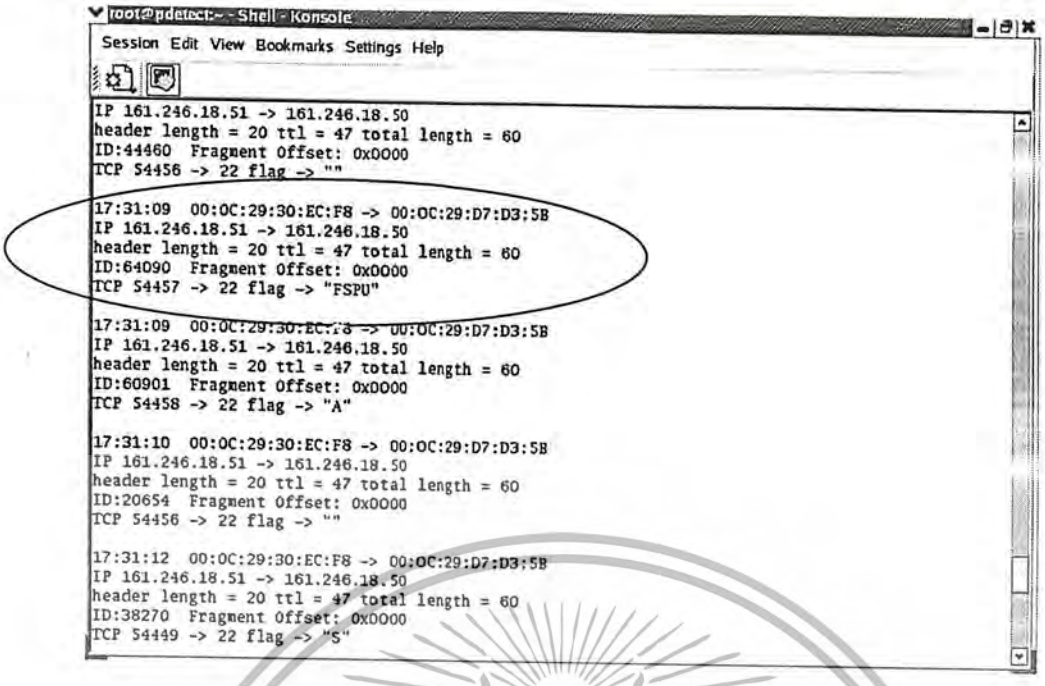
1. เวลาที่ดักจับแพ็กเก็ต คือ เวลาที่ 17 นาฬิกา 22 นาที 13 วินาที
2. มีค่า แมคแอดเดรส เครื่องต้นทางเป็น 00:0C:29:30:EC:F8
3. มีค่า แมคแอดเดรส เครื่องปลายทางเป็น 00:0C29:D7:D3:5B
4. มีหมายเลขไอพีต้นทางเป็น 161.246.18.51
5. มีหมายเลขไอพีปลายทางเป็น 161.246.18.50
6. มีความยาวเฮดเดอร์ไอพีเท่ากับ 20 ไบต์ ซึ่งแปลว่าไม่มีส่วนของ ไอพีออปชั่น

7. มีค่า ttl เท่ากับ 47
8. มีความยาวของแพ็กเก็ตทั้งหมดเท่ากับ 60 ไบต์
9. มีหมายเลขไอดีเท่ากับ 64090
10. มีแฟรีกเมนท์ออฟเซ็ตไม่ระบุ
11. ชนิดโพรโตคอลเป็นแบบ ทีซีพี
12. มีพอร์ทต้นทางเป็น 54457 และพอร์ตปลายทางเป็น 22
13. มีแฟล็กทีซีพีเป็นแฟล็ก FSPU ซึ่งหมายถึงแฟล็ก FIN , SYN , PSH , URG ซึ่งไปไปไม่ได้ที่จะเกิดแฟล็กแบบนี้ขึ้นจริง



รูปที่ 4.19 แสดงการใช้เครื่องมือสำหรับการโจมตีแบบการตรวจสอบระบบปฏิบัติการ (Finger Print)

เมื่อดูจากผลการดักจับแพ็กเก็ตโดยรวม ซึ่งแสดงข้อมูลต่าง ๆ ออกมา จะสังเกตได้ว่ามีหมายเลขไอพีต้นทางเป็น 161.246.18.51 ส่งแพ็กเก็ตที่มีลักษณะ มีแฟล็กทีซีพีที่ไม่มีโอกาสเกิดขึ้นจริงในการใช้งาน ทำให้ผู้ใช้งานสามารถคาดเดาได้ว่าเกิดการบุกรุกแบบ ตรวจสอบระบบปฏิบัติการ ในเครือข่าย 161.246.18.0 นี้แล้ว



รูปที่ 4.20 แสดงผลการดักจับแพ็กเก็ตการโจมตีแบบการตรวจสอบระบบปฏิบัติการ (Finger Print)

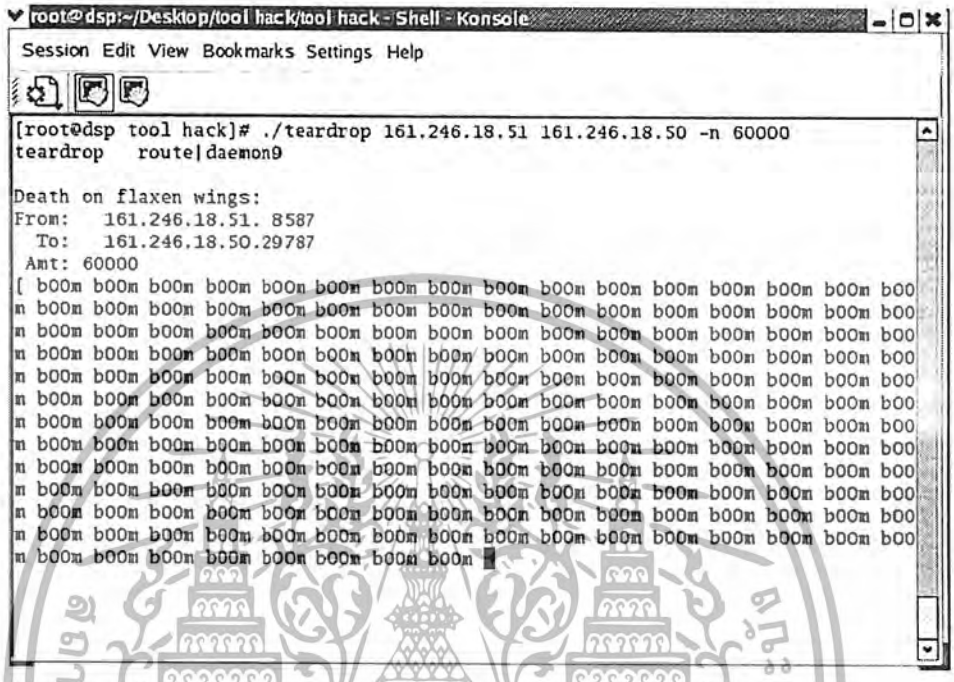
4.3.6 การทดลองการโจมตีแบบแฟรกเมนต์ที่ผิดปกติ (Abnormal Fragmentation)

ทำการทดลองการโจมตีจากเครื่องที่ใช้ทำการโจมตีโดยมีหมายเลขไอพี 161.246.18.51 โดยใช้การโจมตีแบบ การตรวจสอบระบบปฏิบัติการ ซึ่งใช้โปรแกรมการโจมตีดังตารางที่ 4.1 ซึ่งได้แสดงวิธีใช้ดังรูปที่ 4.21 โดยโจมตีไปยังเครื่องที่ใช้เป็นเหยื่อทดสอบหมายเลขไอพี 161.246.18.50 โดยใช้เครื่องที่ติดตั้งโปรแกรมแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 ผลที่ได้จากเครื่องที่ใช้โจมตีที่มีหมายเลขไอพี 161.246.18.51 คือการส่งแพ็กเก็ตที่มีการแฟรกเมนเตชั่นที่ผิดปกติ

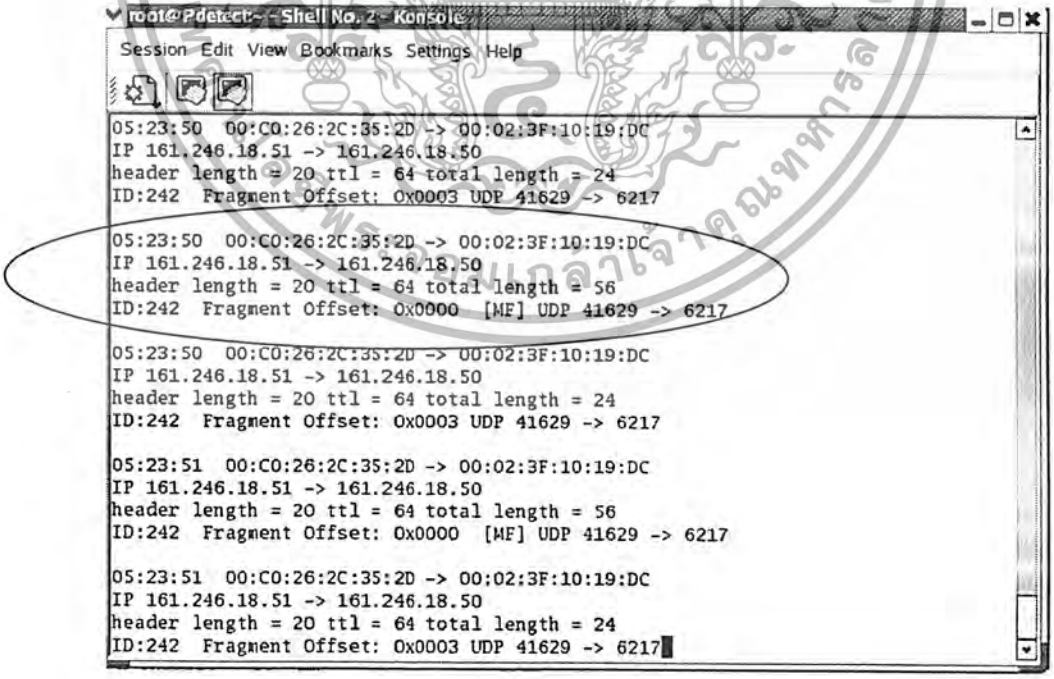
จากการทดลอง ผลที่ได้จากการดักจับแพ็กเก็ตจากเครื่องที่ทำการติดตั้งแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 แสดงดังรูปที่ 4.22 ซึ่งผลที่ออกมาทางหน้าจอแสดงผลนั้น จะอธิบายหนึ่งแพ็กเก็ตเป็นตัวอย่างมีความหมายเรียงลำดับ ดังนี้คือ

1. เวลาที่ดักจับแพ็กเก็ต คือ เวลาที่ 5 นาฬิกา 23 นาที 50 วินาที
2. มีค่า mac address เครื่องต้นทางเป็น 00:C0:26:2C:35:2D
3. มีค่า mac address เครื่องปลายทางเป็น 00:02:3F:10:19:DC
4. มีหมายเลขไอพีต้นทางเป็น 161.246.18.51
5. มีหมายเลขไอพีปลายทางเป็น 161.246.18.50
6. มีความยาวเฮดเดอร์ไอพีเท่ากับ 20 ไบต์ ซึ่งแปลว่าไม่มีส่วนของ ไอพีออฟชั่น
7. มีค่า ttl เท่ากับ 64
8. มีความยาวของแพ็กเก็ตทั้งหมดเท่ากับ 56 ไบต์
9. มีหมายเลขไอดีเท่ากับ 242 ซึ่งเมื่อสังเกตแพ็ตเก็ตอื่นก็จะมีหมายเลขไอดีเดียวกัน

10. มีแฟร็กเมนท์ออฟเซ็ตเป็นแบบ [MF] ซึ่งมีการทำแฟร็กเมนเตชั่น ปลายทางจะต้องทำการรอรับแพ็กเก็ตต่อไปเพื่อทำการรีแอสเซมบลี
11. ชนิดโพรโตคอลเป็นแบบ ยูดีพี
12. มีพอร์ทต้นทางเป็น 41629 และพอร์ตปลายทางเป็น 6217



รูปที่ 4.21 แสดงการใช้เครื่องมือสำหรับการโจมตีแบบแฟร็กเมนต์ผิดปกติ (Abnormal Fragmentation)



รูปที่ 4.22 แสดงผลการดักจับแพ็กเก็ตการโจมตีแบบแฟร็กเมนต์ที่ผิดปกติ (Abnormal Fragmentation)

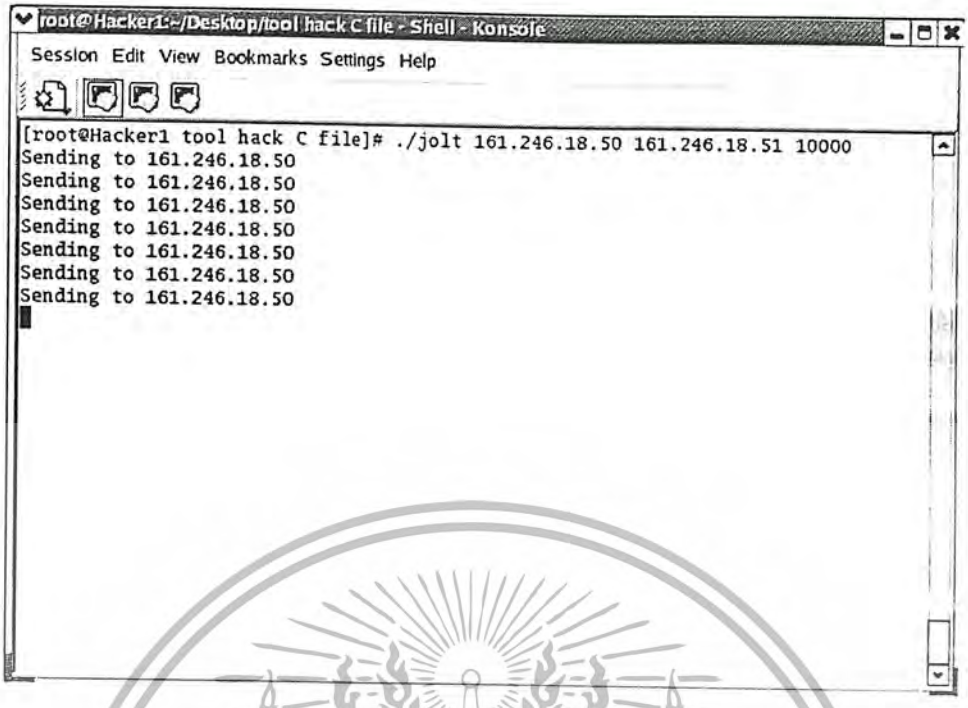
เมื่อดูจากผลการดักจับแพ็กเก็ตโดยรวม ซึ่งแสดงข้อมูลต่าง ๆ ออกมา จะสังเกตได้ว่ามีหมายเลขไอพีต้นทางเป็น 161.246.18.51 ส่งแพ็กเก็ตที่มีลักษณะหมายเลขไอดีของแพ็กเก็ตซ้ำ ๆ กันและมีการระบุว่าทำการแฟร็กเมนเตชั่นมา ทำให้ปลายทางต้องรอการรีแอสเซมบลีจึงจะนำข้อมูลไปใช้งาน จึงทำให้ผู้ใช้งานสามารถคาดเดาได้ว่าเกิดการบุกรุกแบบ แฟร็กเมนต์ที่ผิดปกติ ในเครือข่าย 161.246.18.0 นี้แล้ว

อีกตัวอย่างหนึ่งสำหรับการแฟร็กเมนเตชั่นที่ผิดปกติ โดยทำการทดลองการโจมตีจากเครื่องที่ใช้ทำการโจมตีโดยมีหมายเลขไอพี 161.246.18.51 ใช้โปรแกรมการโจมตีดังตารางที่ 4.1 ซึ่งได้แสดงวิธีใช้ดังรูปที่ 4.23 โดยโจมตีไปยังเครื่องที่ใช้เป็นเหยื่อทดสอบหมายเลขไอพี 161.246.18.50 โดยใช้เครื่องที่ติดตั้งโปรแกรมแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 ผลที่ได้จากเครื่องที่ใช้โจมตีที่มีหมายเลขไอพี 161.246.18.51 คือการส่งแพ็กเก็ตที่ลำดับของไอพีออฟเซต 13 บิต ที่มีลำดับผิดปกติ

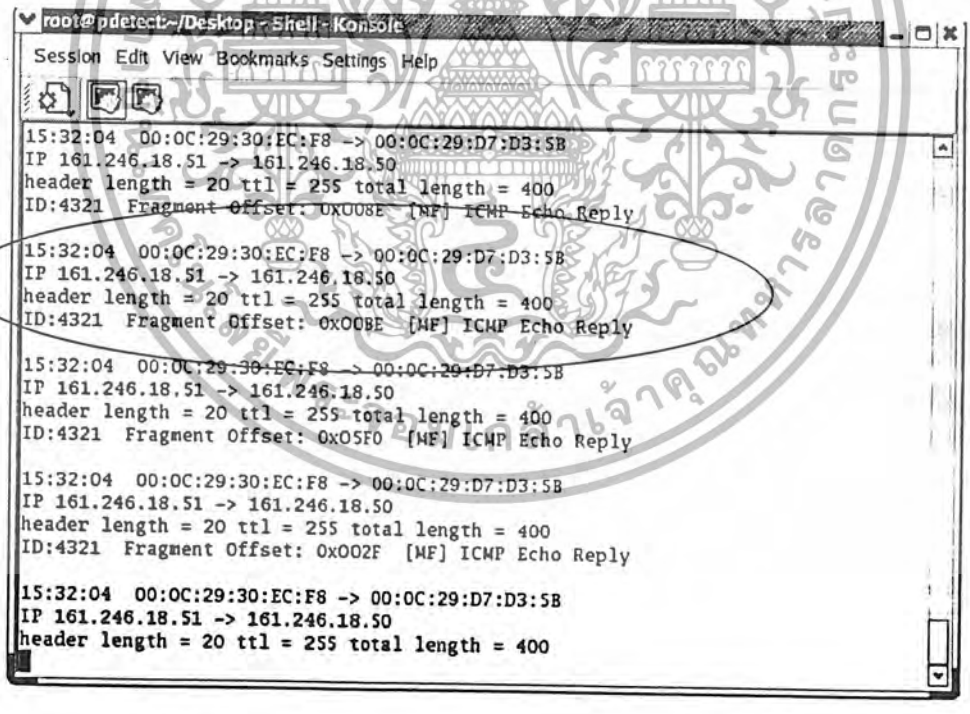
จากการทดลอง ผลที่ได้จากการดักจับแพ็กเก็ตจากเครื่องที่ทำการติดตั้งแพ็กเก็ตดีเทคเตอร์หมายเลขไอพี 161.246.18.52 แสดงดังรูปที่ 4.24 ซึ่งผลที่ออกมาทางหน้าจอแสดงผลนั้น จะอธิบายหนึ่งแพ็กเก็ตเป็นตัวอย่างมีความหมายเรียงลำดับ ดังนี้คือ

1. เวลาที่ดักจับแพ็กเก็ต คือ เวลาที่ 15 นาฬิกา 32 นาที 4 วินาที
2. มีค่า แมคแอดเดรส เครื่องต้นทางเป็น 00:0C:29:30:EC:F8
3. มีค่า แมคแอดเดรส เครื่องปลายทางเป็น 00:0C29:D7:D3:5B
4. มีหมายเลขไอพีต้นทางเป็น 161.246.18.51
5. มีหมายเลขไอพีปลายทางเป็น 161.246.18.50
6. มีความยาวเฮดเดอร์ไอพีเท่ากับ 20 ไบต์ ซึ่งแปลว่าไม่มีส่วนของ ไอพีออปชั่น
7. มีค่า ttl เท่ากับ 255
8. มีความยาวของแพ็กเก็ตทั้งหมดเท่ากับ 400 ไบต์
9. มีหมายเลขไอดีเท่ากับ 4321 ซึ่งเมื่อสังเกตแพ็ตเก็ตอื่นก็จะมีหมายเลขไอดีเดียวกัน
10. มีแฟร็กเมนต์ออฟเซ็ตเป็นแบบ [MF] ซึ่งมีการทำแฟร็กเมนเตชั่น ปลายทางจะต้องทำการรอรับแพ็กเก็ตต่อไปเพื่อทำการรีแอสเซมบลี
11. มีหมายเลขออฟเซ็ท เป็น 0x00BE ซึ่งเมื่อเทียบกับแพ็กเก็ตอื่นจะไม่เหมือนกัน
12. ชนิดโพรโตคอลเป็นแบบ ICMP Echo request

เมื่อดูจากผลการดักจับแพ็กเก็ตโดยรวม ซึ่งแสดงข้อมูลต่าง ๆ ออกมา จะสังเกตได้ว่ามีหมายเลขไอพีต้นทางเป็น 161.246.18.51 ส่งแพ็กเก็ตที่มีลักษณะ บอกว่ามีการทำแฟร็กเมนเตชั่นมา ทำให้ปลายทางต้องรอการรีแอสเซมบลีจึงจะนำข้อมูลไปใช้งาน ซึ่งหมายเลขออฟเซ็ทไม่เป็นลำดับหมายเลข ทำให้ผู้ใช้งานสามารถคาดเดาได้ว่าเกิดการบุกรุกแบบ แฟร็กเมนต์ที่ผิดปกติ ในเครือข่าย 161.246.18.0 นี้แล้วอีกเช่นกัน



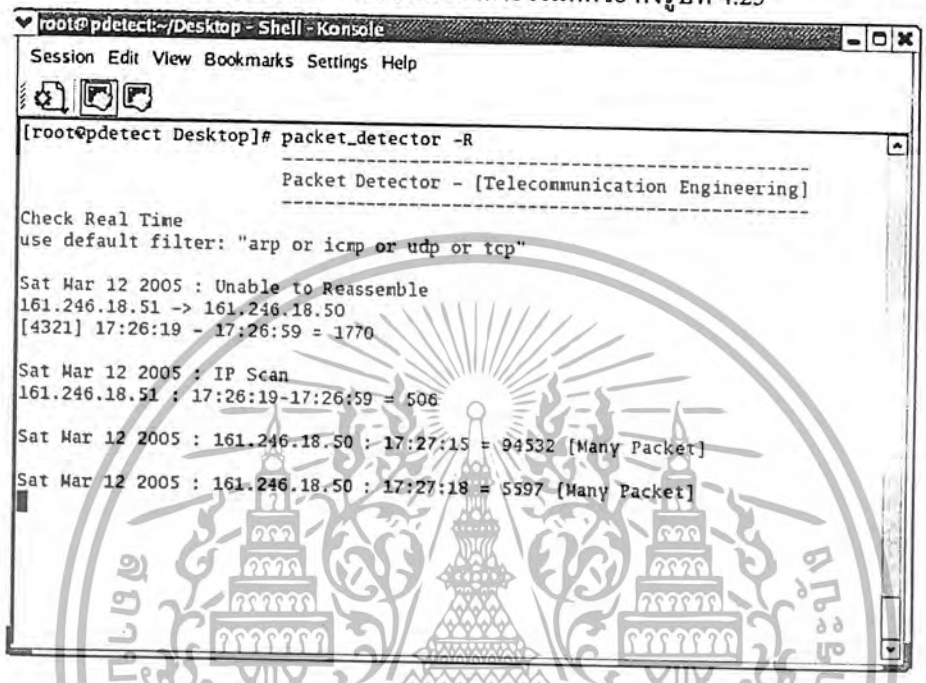
รูปที่ 4.23 แสดงการใช้เครื่องมือสำหรับการโจมตีแบบแฟร็กเมนต์ที่ผิดปกติ (Abnormal Fragmentation)



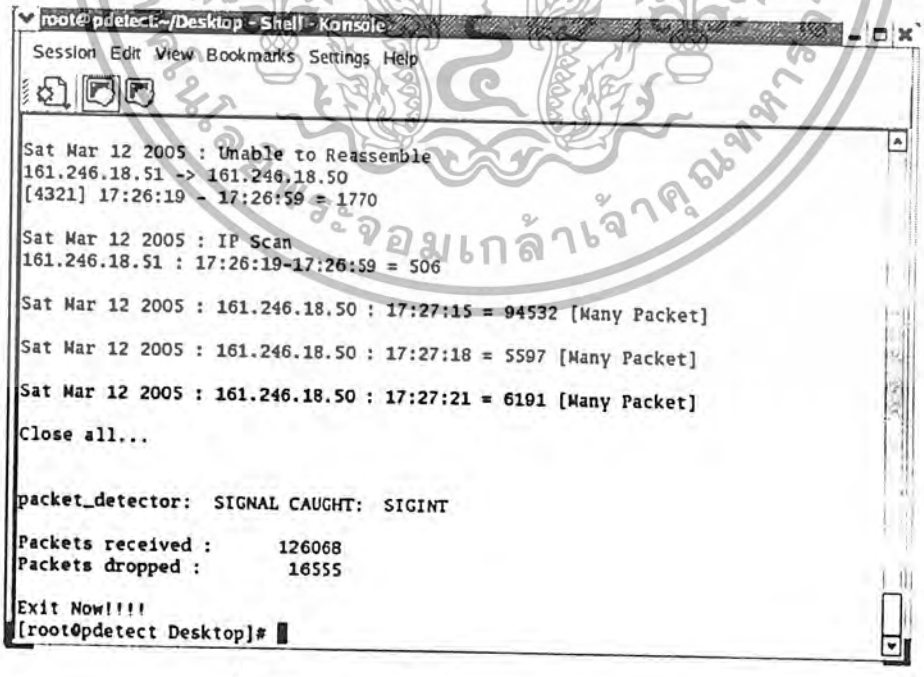
รูปที่ 4.24 แสดงผลการดักจับแพ็กเก็ตการโจมตีแบบแฟร็กเมนต์ที่ผิดปกติ(Abnormal Fragmentation)

4.4 การทดลองส่วนการวิเคราะห์การบุกรุก

ในผลการทดลองส่วนนี้เป็นการนำข้อมูลของแพ็กเก็ตที่เข้ามาขณะนั้น มาวิเคราะห์ในขณะนั้นเลย โดยเรียกใช้คำสั่ง packet_detector –R ตามโฟลว์ชาร์ทรูปที่ 3.2 ทำให้ได้ข้อมูลการโจมตีตามเวลาจริง ซึ่งแสดงผลออกมาผ่านหน้าจอเทอร์มินอล โดยจะแสดงผลทั้งเครื่องเป้าหมายที่ถูกโจมตี วันและช่วงเวลาที่ถูกโจมตี จำนวนแพ็กเก็ตที่โจมตีเข้ามา และชนิดของการโจมตีด้วย ดังรูปที่ 4.25



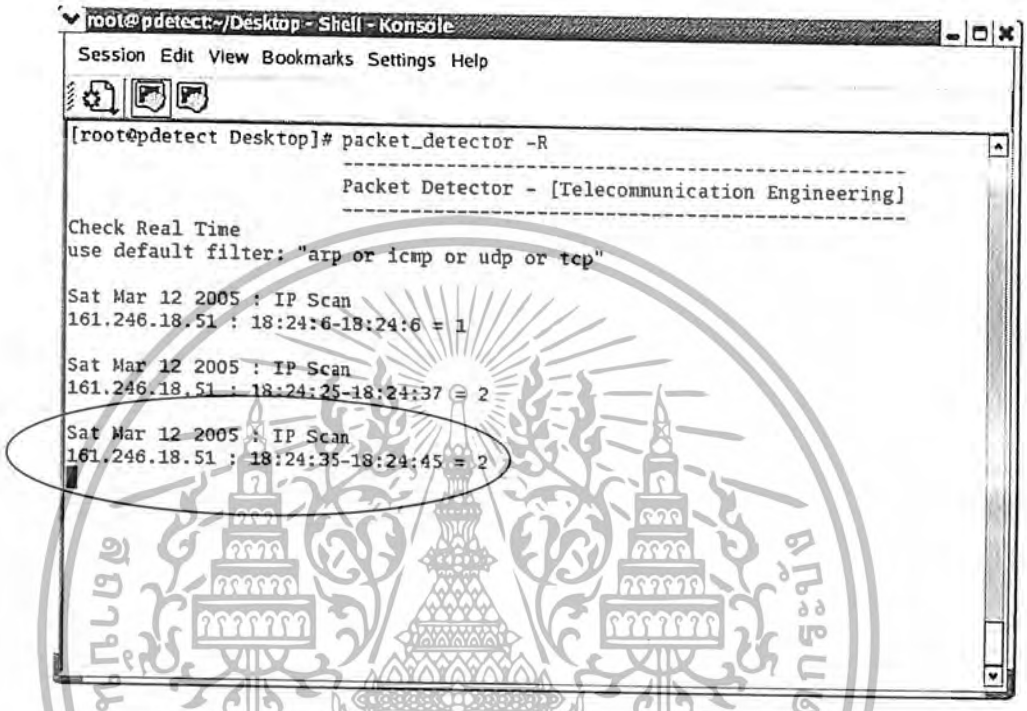
รูปที่ 4.25 การตรวจจับใน mode real time



รูปที่ 4.26 การออกจากโหมดการทำงาน real time

เมื่อผู้ใช้งานต้องการหยุดการทำงานของโปรแกรม ทำได้โดยการกดปุ่ม Ctrl + c เมื่อออกจากการทำงาน จะมีการสรุปผลการดักจับแพ็กเก็ต ว่าแพ็กเก็ตมีจำนวนทั้งหมดเท่าไหร่แล้วมีการละเลยการตรวจสอบกี่แพ็กเก็ตดังรูปที่ รูปที่ 4.26

4.4.1 การตรวจสอบการบุกรุกแบบสแกนไอพี (IP Scan)

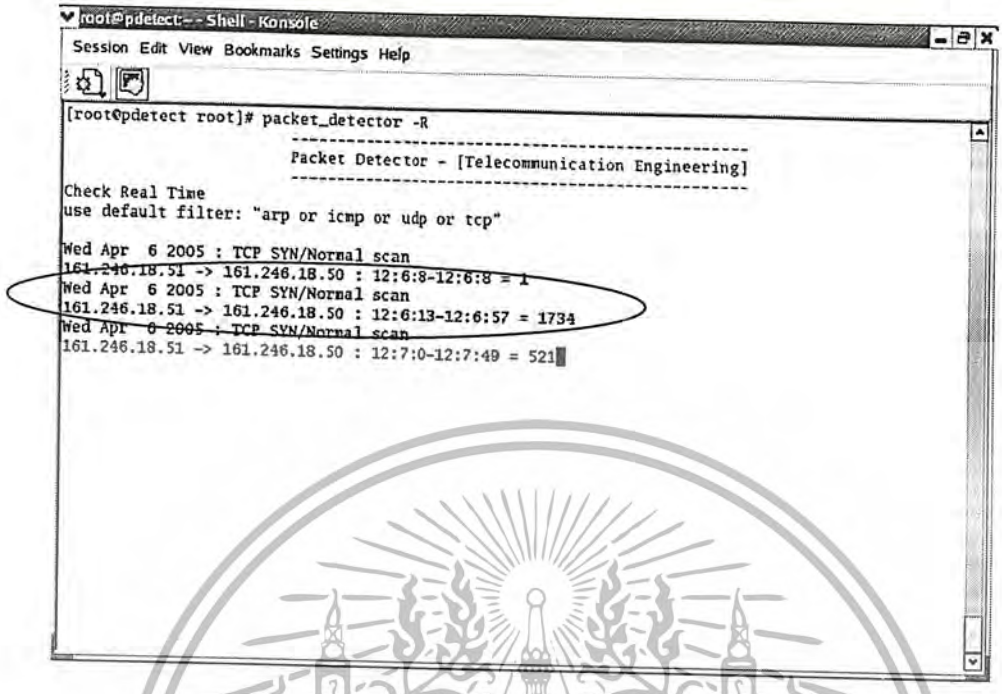


รูปที่ 4.27 แสดงการแจ้งเตือนเมื่อเจอการบุกรุกแบบสแกนไอพี (IP Scan)

จากรูปที่ 4.27 แสดงการแจ้งเตือนการบุกรุกแบบ ไอพีสแกน ซึ่งมีความหมายคือ

1. ชื่อวัน ชื่อเดือน เลขวัน และปี ค.ศ. คือ Sat Mar 12 2005
2. ชื่อการบุกรุก คือ ไอพีสแกน
3. หมายเลขไอพีต้นทาง 161.246.18.51
4. เวลาเริ่มต้น และ เวลาสิ้นสุดของแพ็กเก็ตที่ดักจับได้ในขณะนั้นเป็นชั่วโมง นาที วินาที คือ 18:24:35 – 18:24:45
5. จำนวนแพ็กเก็ตที่ดักจับขณะนั้น คือ 2 แพ็กเก็ต

4.4.2 การตรวจสอบการบุกรุกแบบสแกนพอร์ต (Scan port)

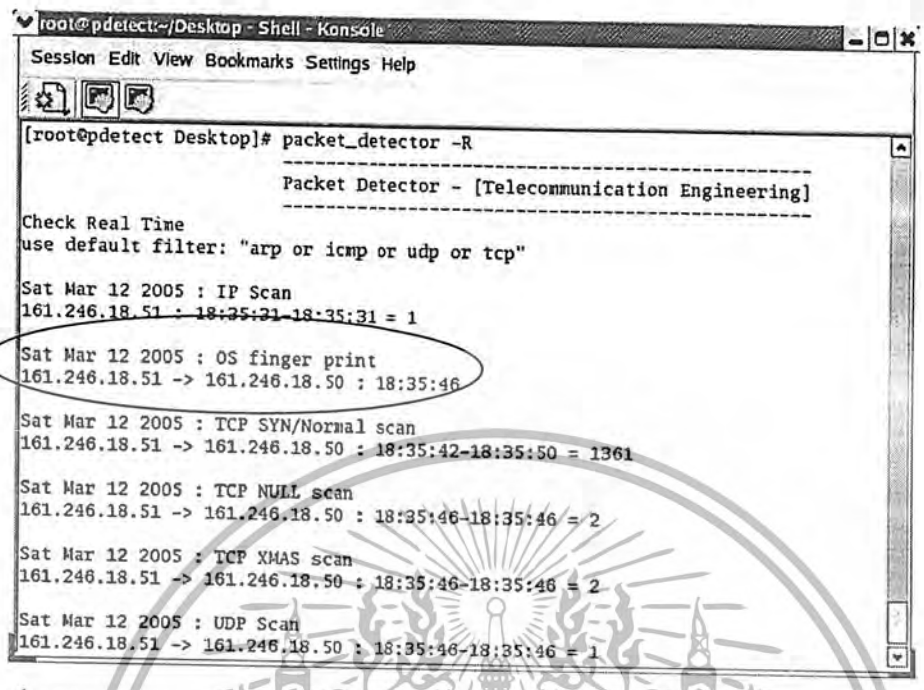


รูปที่ 4.28 แสดงการแจ้งเตือนเมื่อเจอการบุกรุกโดยการสแกนพอร์ต (Scan Port)

จากรูปที่ 4.28 แสดงการแจ้งเตือนการบุกรุกแบบ สแกนพอร์ต ซึ่งมีความหมายคือ

1. ชื่อวัน ชื่อเดือน เลขวัน และปี ค.ศ. คือ Wed Apr 6 2005
2. ชื่อการบุกรุก คือ TCP SYN/Normal scan
3. หมายเลขไอพีต้นทาง 161.246.18.51
4. หมายเลขไอพีปลายทาง 161.246.18.50
5. เวลาเริ่มต้น และ เวลาสิ้นสุดของแพ็กเก็ตที่ดักจับได้ในขณะนั้นเป็นชั่วโมง นาที วินาที คือ 12:6:13 – 12:6:57
6. จำนวนแพ็กเก็ตที่ดักจับขณะนั้น คือ 1734 แพ็กเก็ต

4.4.3 การตรวจสอบการบุรุกแบบตรวจสอบระบบปฏิบัติการ (Finger Print)

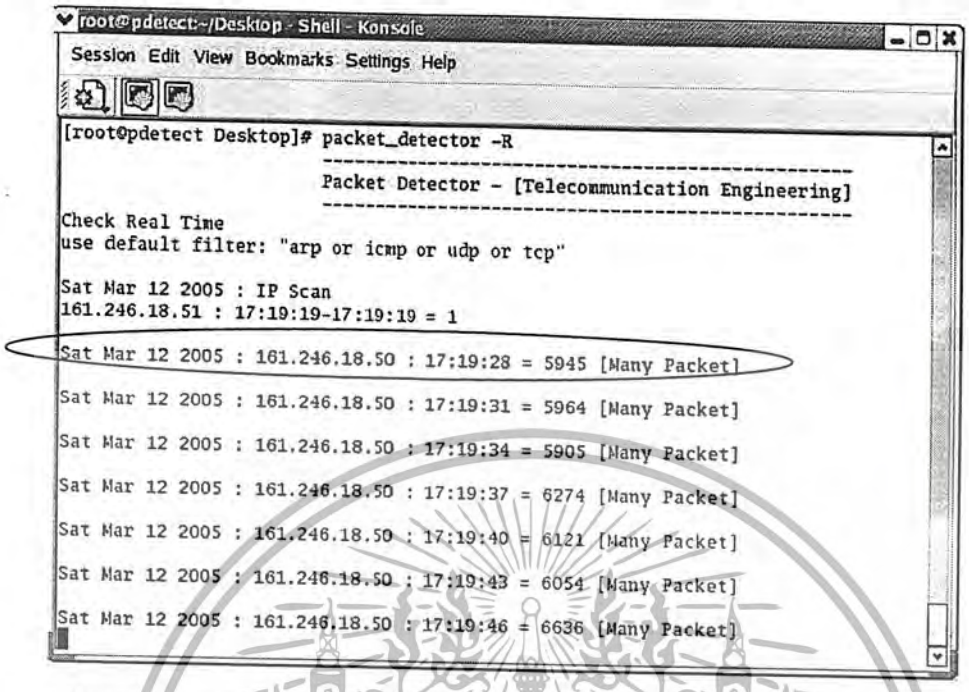


รูปที่ 4.29 แสดงการแจ้งเตือนเมื่อเจอการบุกรุกตรวจสอบระบบปฏิบัติการ (Finger Print)

จากรูปที่ 4.29 แสดงการแจ้งเตือนการบุกรุกแบบ ตรวจสอบระบบปฏิบัติการ ซึ่งมีความหมายคือ

1. ชื่อวัน ชื่อเดือน เลขวัน และปี ค.ศ. คือ Sat Mar 12 2005
2. ชื่อการบุกรุก คือ Finger Print
3. หมายเลขไอพีต้นทาง 161.246.18.51
4. หมายเลขไอพีปลายทาง 161.246.18.50
5. เวลาเริ่มต้น ของแพ็กเก็ตที่ดักจับได้ในขณะนั้นเป็นชั่วโมง นาที วินาที คือ 18:35:46

4.4.4 การตรวจสอบการบุกรุกแบบการส่งแพ็กเก็ตจำนวนมาก (Amount of Packets Sending)

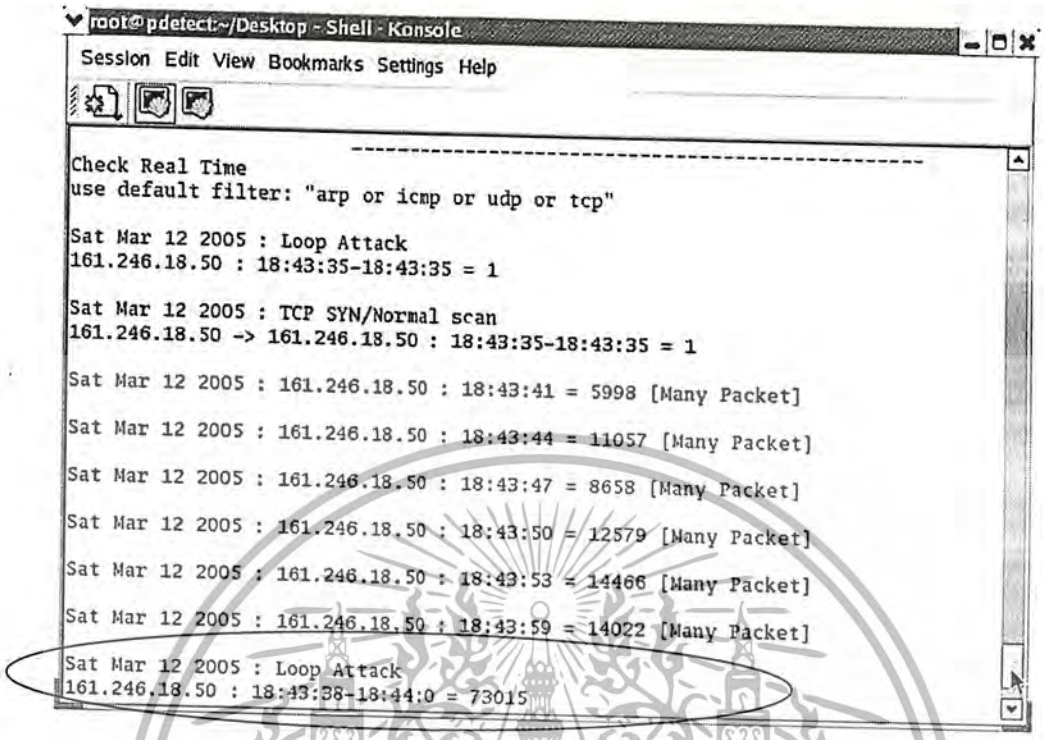


รูปที่ 4.30 แสดงการแจ้งเตือนมีการโจมตีแบบส่งแพ็กเก็ตจำนวนมาก(Amount of Packets Sending)

จากรูปที่ 4.30 แสดงการแจ้งเตือนการบุกรุกแบบ ส่งแพ็กเก็ตจำนวนมากซึ่งมีความหมายคือ

1. ชื่อวัน ชื่อเดือน เลขวัน และปี ค.ศ. คือ Sat Mar 12 2005
2. หมายเลขไอพีปลายทาง 161.246.18.50
3. เวลาเริ่มต้น ของแพ็กเก็ตที่ดักจับได้ในขณะนั้นเป็นชั่วโมง นาที วินาที คือ 17:19:28
4. จำนวนแพ็กเก็ตที่ดักจับขณะนั้น คือ 5945 แพ็กเก็ต
5. ชนิดการบุกรุก เป็นแบบ Amount of Packet

4.4.5 การตรวจสอบการบุกรุกแบบวนลูป (Loop)

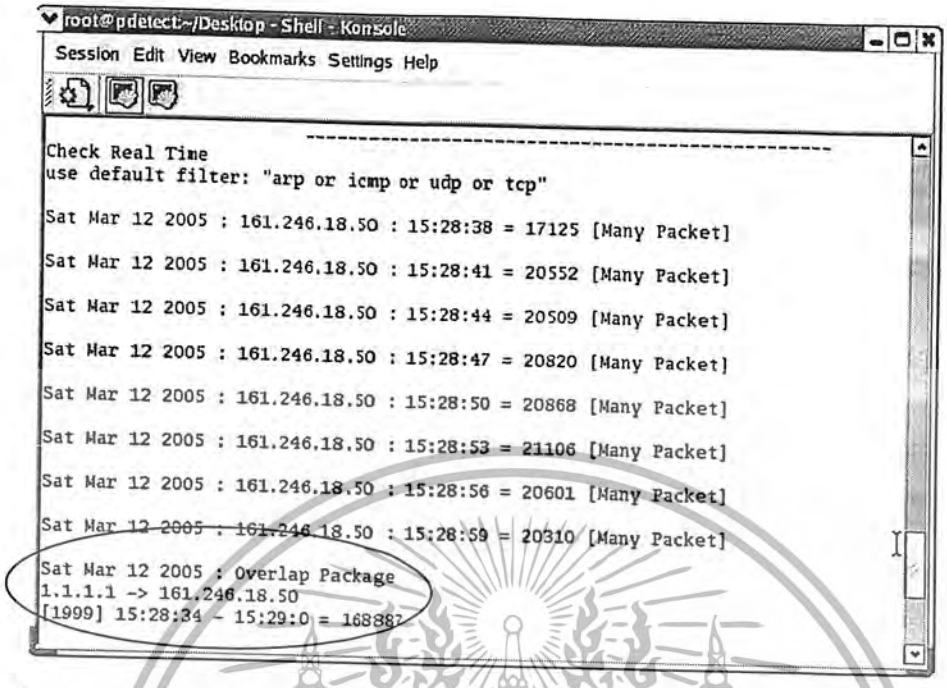


รูปที่ 4.31 แสดงการแจ้งเตือนมีการโจมตีแบบแบบวนลูป (Loop)

จากรูปที่ 4.31 แสดงการแจ้งเตือนการบุกรุกแบบ วนลูป ซึ่งมีความหมายคือ

1. ชื่อวัน ชื่อเดือน เลขวัน และปี ค.ศ. คือ Sat Mar 12 2005
2. ชนิดการบุกรุก เป็นแบบ Loop Attack
3. หมายเลขไอพีปลายทาง 161.246.18.50
4. เวลาเริ่มต้น และ เวลาสิ้นสุดของแพ็กเก็ตที่ดักจับได้ในขณะนั้นเป็นชั่วโมง นาที วินาที คือ 18:43:38 – 18:44:0
5. จำนวนแพ็กเก็ตที่ดักจับขณะนั้น คือ 73015 แพ็กเก็ต

4.4.6 การตรวจสอบการบุกรุกแบบแพ็กเก็ตเหลื่อมล้ำกัน (Overlap)

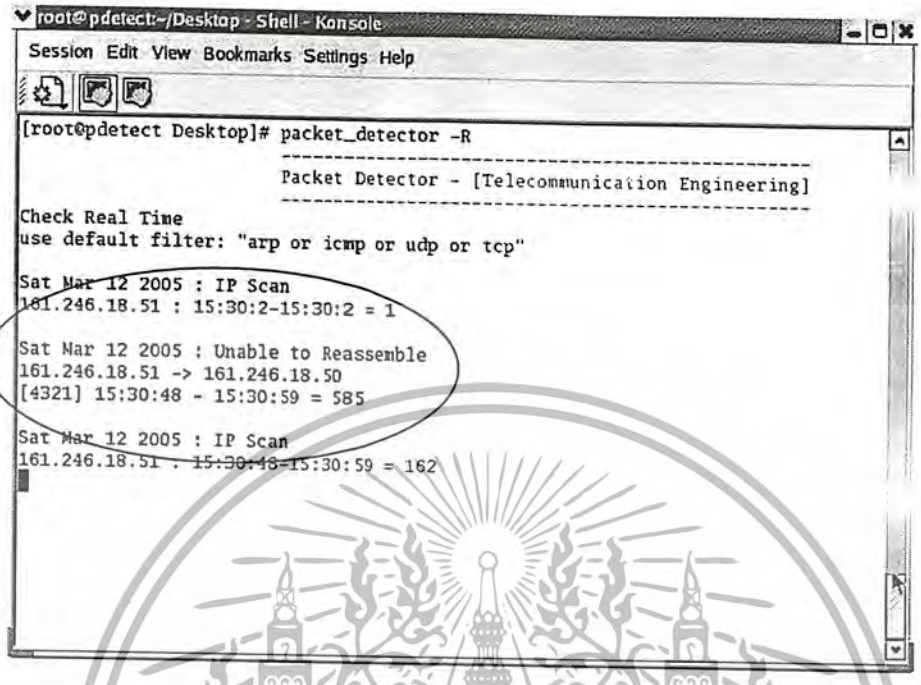


รูปที่ 4.32 แสดงการแจ้งเตือนมีการ โจมตีแบบแฟร็กเมนเตชั่นชนิดทับซ้อนกัน (Overlap Fragmentation)

จากรูปที่ 4.32 แสดงการแจ้งเตือนการบุกรุกแบบแฟร็กเมนเตชั่นชนิดทับซ้อนกัน ซึ่งมีความหมายคือ

1. ชื่อวัน ชื่อเดือน เลขวัน และปี ค.ศ. คือ Sat Mar 12 2005
2. ชื่อการบุกรุก คือ Overlap Packet
3. หมายเลขไอพีต้นทาง 1.1.1.1
4. หมายเลขไอพีปลายทาง 161.246.18.50
5. หมายเลขไอดีของแพ็กเก็ต คือ 1999
6. เวลาเริ่มต้น และ เวลาสิ้นสุดของแพ็กเก็ตที่ดักจับได้ในขณะนั้นเป็นชั่วโมง นาที วินาที คือ 15:28:34 – 15:29:0
7. จำนวนแพ็กเก็ตที่ดักจับขณะนั้น คือ 168887 แพ็กเก็ต

4.4.7 การตรวจสอบการบุกรุกแบบแพ็กเก็ตเกิดช่องว่าง (Gap)



รูปที่ 4.33 แสดงการแจ้งเตือนมีการโจมตีแบบแฟร็กเมนเตชั่นชนิดเกิดช่องว่าง (Gap Fragmentation)

จากรูปที่ 4.33 แสดงการแจ้งเตือนการบุกรุกแบบ แฟร็กเมนเตชั่นชนิดเกิดช่องว่าง ซึ่งมีความหมายคือ

1. ชื่อวัน ชื่อเดือน เลขวัน และปี ค.ศ. คือ Sat Mar 12 2005
2. ชื่อการบุกรุก คือ Unable to Reassemble
3. หมายเลขไอพีต้นทาง 161.246.18.51
4. หมายเลขไอพีปลายทาง 161.246.18.50
5. หมายเลขไอดีของแพ็กเก็ต คือ 4321
6. เวลาเริ่มต้น และ เวลาสิ้นสุดของแพ็กเก็ตที่ดักจับได้ในขณะนั้นเป็นชั่วโมง นาที วินาที คือ 15:30:48 – 15:30:59
7. จำนวนแพ็กเก็ตที่ดักจับขณะนั้น คือ 585 แพ็กเก็ต

4.5 การแสดงผลผ่านทางเว็บ

นอกจากการแสดงผลทางหน้าจอ และเก็บทางล็อกไฟล์ที่กำหนดแล้ว ระบบยังสามารถแสดงผลผ่านทางเว็บไซต์ได้ โดยจะแสดงผลของการวิเคราะห์ที่สรุปว่าเป็นการโจมตี เพื่อเป็นการแจ้งเตือนต่อผู้ดูแลระบบ

ในหน้าจอการแสดงผล จะแสดงข้อมูลดังนี้คือ

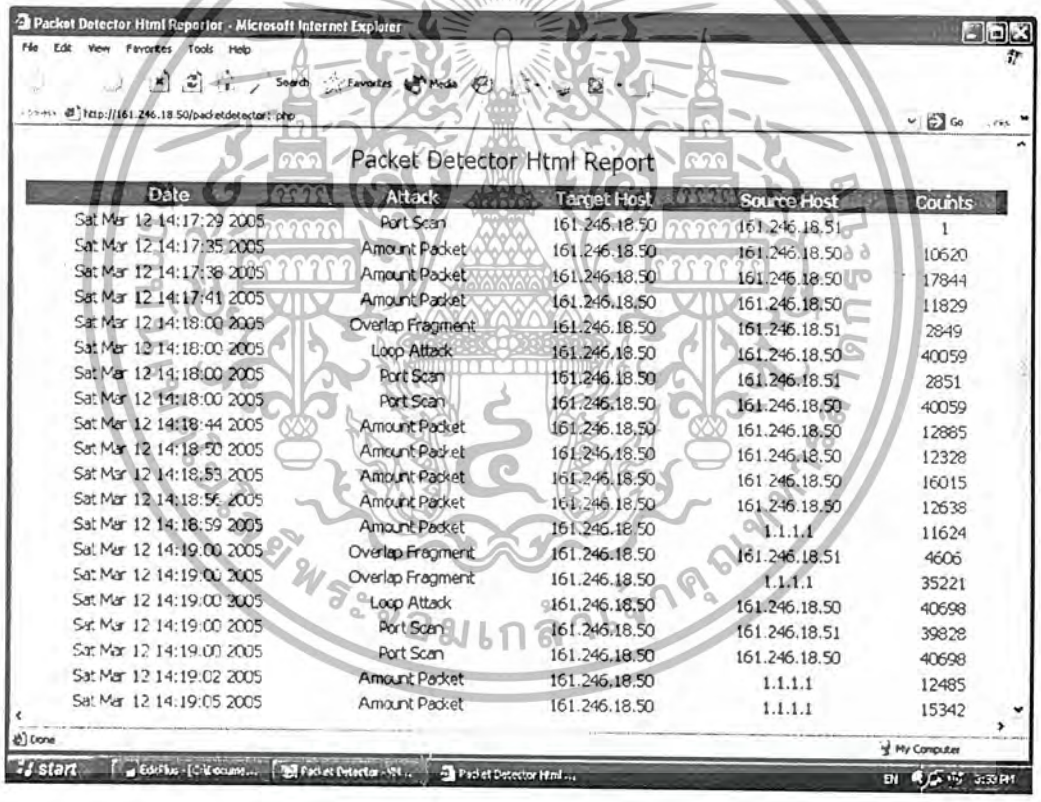
Date : วันที่ และ เวลาที่เกิดการโจมตี

Attack : ประเภทของการโจมตีที่เกิดขึ้น

Target Host : ไอพีของเครื่องคอมพิวเตอร์ที่เป็นเป้าหมายในการโจมตี

Source Host : ไอพีของเครื่องคอมพิวเตอร์ต้นทางที่ส่งแพ็กเก็ต

Count : จำนวนแพ็กเก็ตการโจมตี



Date	Attack	Target Host	Source Host	Counts
Sat Mar 12 14:17:29 2005	Port Scan	161.246.18.50	161.246.18.51	1
Sat Mar 12 14:17:35 2005	Amount Packet	161.246.18.50	161.246.18.50	10620
Sat Mar 12 14:17:38 2005	Amount Packet	161.246.18.50	161.246.18.50	17844
Sat Mar 12 14:17:41 2005	Amount Packet	161.246.18.50	161.246.18.50	11829
Sat Mar 12 14:18:00 2005	Overlap Fragment	161.246.18.50	161.246.18.51	2849
Sat Mar 12 14:18:00 2005	Loop Attack	161.246.18.50	161.246.18.50	40059
Sat Mar 12 14:18:00 2005	Port Scan	161.246.18.50	161.246.18.51	2851
Sat Mar 12 14:18:00 2005	Port Scan	161.246.18.50	161.246.18.50	40059
Sat Mar 12 14:18:44 2005	Amount Packet	161.246.18.50	161.246.18.50	12885
Sat Mar 12 14:18:50 2005	Amount Packet	161.246.18.50	161.246.18.50	12328
Sat Mar 12 14:18:53 2005	Amount Packet	161.246.18.50	161.246.18.50	16015
Sat Mar 12 14:18:56 2005	Amount Packet	161.246.18.50	161.246.18.50	12638
Sat Mar 12 14:18:59 2005	Amount Packet	161.246.18.50	1.1.1.1	11624
Sat Mar 12 14:19:00 2005	Overlap Fragment	161.246.18.50	161.246.18.51	4606
Sat Mar 12 14:19:00 2005	Overlap Fragment	161.246.18.50	1.1.1.1	35221
Sat Mar 12 14:19:00 2005	Loop Attack	161.246.18.50	161.246.18.50	40698
Sat Mar 12 14:19:00 2005	Port Scan	161.246.18.50	161.246.18.51	39828
Sat Mar 12 14:19:00 2005	Port Scan	161.246.18.50	161.246.18.50	40698
Sat Mar 12 14:19:02 2005	Amount Packet	161.246.18.50	1.1.1.1	12485
Sat Mar 12 14:19:05 2005	Amount Packet	161.246.18.50	1.1.1.1	15342

รูปที่ 4.34 เว็บแสดงผลการแจ้งเตือนเมื่อมีการโจมตีจากข้อมูลที่วิเคราะห์ได้

บทที่ 5
สรุปและวิจารณ์

5.1 คุณสมบัติของระบบ

ระบบตรวจจับข้อมูลแปลกปลอมบนเครือข่าย (Packet Detector) ที่สร้างขึ้น มีความสามารถในการทำงานดังต่อไปนี้

(1) ติดตั้งโปรแกรมได้ โดยผ่านคำสั่ง make , make install

(2) ถอนการติดตั้งโปรแกรมได้ โดยผ่านคำสั่ง make uninstall , make clean

(3) เก็บข้อมูลของแพ็กเก็ต และสามารถแสดงข้อมูลของแพ็กเก็ตผ่านหน้าจอ

(4) เก็บข้อมูลของแพ็กเก็ตเพื่อวิเคราะห์การบุกรุกตามเวลาจริง และแสดงผลผ่านหน้าจอ

(5) แสดงส่วนช่วยเหลือผู้ใช้โปรแกรม

(6) วิเคราะห์แพ็กเก็ตที่เกิดความผิดปกติแบบมีปริมาณมาก (Amount of Packets Sending)

(7) วิเคราะห์แพ็กเก็ตที่เกิดความผิดปกติแบบมีการทำแฟร็กเมนเตชั่นที่ผิดปกติ (Fragmentation)

(8) วิเคราะห์แพ็กเก็ตที่เกิดความผิดปกติแบบมีการส่งแพ็กเก็ตแบบวนลูป (Land)

(9) วิเคราะห์แพ็กเก็ตสแกนพอร์ต (Scan port)ชนิดต่างๆ ได้ เช่น FIN, NULL, XMAS

(10) วิเคราะห์แพ็กเก็ตไอพีสแกน (IP Scan)

(11) วิเคราะห์แพ็กเก็ตสแกนระบบปฏิบัติการ (Finger print)

(12) แสดงข้อมูลการโจมตีผ่านเว็บเพจ

(13) แสดงผลเก็บลงล็อกไฟล์และสามารถเปลี่ยนไดเร็กทอรีที่เก็บล็อกไฟล์

5.2 ข้อจำกัดของระบบ

(1) ระบบนี้สร้างขึ้นบนระบบปฏิบัติการลีนุกซ์ซึ่งอาจแตกต่างกัน หากนำไปใช้งานในระบบอื่น

(2) ผู้ที่มีสิทธิ์รูท (root) เท่านั้นที่จะสามารถใช้งานโปรแกรมนี้ได้

(3) ระบบนี้สามารถตรวจจับผู้บุกรุกทางเครือข่ายคอมพิวเตอร์ได้เฉพาะเครื่องปลายทางที่อยู่ในบรอดคาสต์โดเมน (Broadcast domain) เดียวกันเท่านั้นจำนวนเครื่องในบรอดคาสต์โดเมนนั้นๆ ไม่ควรเกิน 255 เครื่อง

(4) ผู้ใช้ต้องเลือกออปชั่นในการทำงานเองผ่านคอมมานไลน์

(5) ในกรณีที่เครือข่ายนั้นมีแพ็กเก็ตปริมาณมาก อาจทำให้บัฟเฟอร์ที่ใช้เก็บข้อมูลของแพ็กเก็ตก่อนนำมาวิเคราะห์เต็มได้ ดังนั้นควรคำนึงถึงข้อจำกัดในเรื่องเนื้อที่ในการจัดเก็บด้วย

5.3 ปัญหาและอุปสรรค

ในการออกแบบและสร้างระบบตรวจจับข้อมูลแปลกปลอมบนเครือข่าย (Packet Detector) นี้ มีปัญหาและอุปสรรคในการพัฒนาหลายประการ ได้แก่

(1) ความไม่สมบูรณ์ของไลบรารีในลีนุกซ์ เช่น บางฟังก์ชันระบุว่าสามารถทำงานอย่างหนึ่งได้ แต่เมื่อได้ลองใช้จริงแล้วทำไม่ได้

(2) เมื่อแพ็กเก็ตที่มีเข้ามาในขณะใดขณะหนึ่งมีเป็นจำนวนมาก อาจทำให้บางแพ็กเก็ตถูกละเลยการตรวจสอบได้

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จได้ด้วยดี เนื่องจากได้รับการแนะนำ สนับสนุน และให้คำปรึกษาเป็นอย่างดีจาก อาจารย์อัครพล ตรีรัตน์ , อาจารย์ธเนศ พัฒนธาดาพงษ์ และ อาจารย์นภัทร สระเอี่ยม ซึ่งเป็นที่ปรึกษาปริญญานิพนธ์ ทางคณะผู้จัดทำต้องขอขอบพระคุณเป็นอย่างสูง รวมทั้งอาจารย์ภาควิชาโทรคมนาคม คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่าน ที่ให้การอบรมสั่งสอนวิชาความรู้แก่คณะผู้จัดทำมาโดยตลอด

ขอขอบคุณ คุณธนสิน จิตแก้ว และทุก ๆ คน จากบริษัทโกลบอลเทคโนโลยี อินทิเกรทเทด จำกัด ที่ให้ความคิดริเริ่มของปริญญานิพนธ์ฉบับนี้

ขอขอบคุณผู้ดูแลระบบคอมพิวเตอร์ภาควิชาโทรคมนาคม และสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังที่อำนวยความสะดวกในการใช้งานเครือข่าย

สุดท้ายนี้ขอขอบพระคุณสำหรับบุคคลที่สำคัญที่สุดที่ทำให้คณะผู้จัดทำมีวันนี้ คือ บิดา มารดา ผู้เป็นที่เคารพรักยิ่งของคณะผู้จัดทำ ซึ่งท่านให้การอบรมสั่งสอน เลี้ยงดู และให้โอกาสในการศึกษาอย่างเต็มที่ และขอขอบคุณเพื่อนๆ ที่ให้ข้อคิดเป็น และเป็นกำลังใจให้เสมอมา

คณะผู้จัดทำ

บรรณานุกรม

[1] Carl Endorf, Eugene Schultz and Jim Mellander , "Intrusion Detection & Prevention" McGraw-Hill/Osborne, Emeryville, California .

[2] Rafeeq Ur Rehman , "Intrusion Detection Systems with Snort" Pearson Education , Inc. Publishing as Prentice Hall PTR Upper Saddle River, New Jersey .

[3] Neil Matthew, Rick Stones , "Beginning Linux Programming" Wrox Press Ltd, Chicago .

[4] Mike D. Schiffman ,"Building Open Source Network Security Tools" Wiley Publishing, Inc.

[5] Stephen Northcutt, Judy Novak ,"Network Intrusion Detection" Third Edition, New Riders

[6] H.M. Deitel,P.J. Deitel, "C How To Program" Third Edition, Prentice hall, Upper Saddle River, New Jersey 07458

[7] อรพิน ประวัติบริสุทธ์, "คู่มือเรียนภาษาซี", กรุงเทพฯ; โปรวิชั่น 2547.

[8] ประภาพร ช่างไม้, "คู่มือเขียนโปรแกรมภาษา C ฉบับผู้เริ่มต้น", นนทบุรี : อินโฟเพรส,2545

[9] จตุชัย แพงจันทร์, อนุโชต วุฒิพรพงษ์ , "เจาะระบบ Network ฉบับสมบูรณ์" บริษัท ไอดีซี อิโฟ ดิสทริบิวเตอร์ เซ็นเตอร์ จำกัด ,2546 .

[10] เรืองไกร รังสิพล , "เจาะระบบ TCP/IP จุดอ่อนของโปรโตคอลและวิธีป้องกัน" บริษัท โปรวิชั่น จำกัด,2544 .

[11] ประภาพร ช่างไม้, "Linux Redhat ฉบับผู้เริ่มต้น" บริษัท ไอดีซี อิโฟ ดิสทริบิวเตอร์ เซ็นเตอร์ จำกัด ,2547 .

[12] อภิชน ไวท์ยางกูร, อังสนา วงศ์รัตนวิจิตร , "ระบบตรวจจับผู้บุกรุกเครือข่ายบนยูนิกส์" ปริญญานิพนธ์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ปีการศึกษา 2544 .

เวปไซต์อ้างอิง

[1] http://www.snort.org

[2] http://www.securityfocus.com

[3] http://www.cert.org

[4] http://www.whitehats.com

[5] htto://www.packetstorm.com