ระบบตรวจจับผู้บุกรุก

Intrusion Detection System (IDS)

โดย

นาย อมร วรรณพิณ

นาย อังคาร ชูมงคล

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2547

Intrusion Detection System (IDS)

By

Mr. Amorn Wannapin

Mr. Aungkarn Choomongkol

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENT FOR THE DEGREE OF

BACHELOR IN DEPARTMENT OF INFORMATION ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2004

หัวข้อปริญญานิพนธ์	ระบบบตรวจสอบผู้บุกรุก
ชื่อนักศึกษา	นายอมร วรรณพิณ รหัสนักศึกษา 44010592
	นายอังคาร ชูมงคล รหัสนักศึกษา 44010603
อาจารย์ที่ปรึกษา	อาจารย์ภุชงค์ หงษ์สุวรรณ
ระดับการศึกษา	ปริญญาตรี วิศวกรรมศาสตร์บัณฑิต
	สาขาวิศวกรรมสารสนเทศ
ภาควิชา	วิศวกรรมสารสนเทศ
ปีการศึกษา	2547

ปริญญานิพนธ์ฉบับนี้ได้รับความเห็นชอบจากอาจารย์ที่ปรึกษาเป็นที่เรียบร้อยแล้ว

.....

(อาจารย์ ภุชงค์ หงษ์สุวรรณ)

อาจารย์ผู้ควบคุมวิทยานิพนธ์

หัวข้อปริญญานิพนธ์	ระบบบตรวจสอบผู้บุกรุก
ชื่อนักศึกษา	นายอมร วรรณพิณ รหัสนักศึกษา 44010589
	นายอังคาร ชูมงคล รหัสนักศึกษา 44010603
อาจารย์ที่ปรึกษา	อาจารย์ภุชงค์ หงษ์สุวรรณ
ระดับการศึกษา	ปริญญาตรี วิศวกรรมศาสตร์บัณฑิต
	สาขาวิศวกรรมสารสนเทศ
ภาควิชา	วิศวกรรมสารสนเทศ
ปีการศึกษา	2547

บทคัดย่อ

วิทยานิพนธ์ ฉบับนี้ ศึกษาและพัฒนาระบบตรวจสอบผู้บุกรุกเครือข่าย(Intrusion Detection System) ซึ่งใช้ในการตรวจจับและแจ้งเตือน การบุกรุกต่างๆ ได้หลายรูปแบบ โดยในโครงงานนี้ คณะผู้จัดทำได้ศึกษาถึงการโจมตีต่างๆ 5 ประเภท ได้แก่ การสแกนพอร์ต การพยายามล็อกอิน (Brute force) การโจมตีจากม้าโทรจัน การโจมตีจากการแพร่กระจายของเวิร์ม และการโจมตีจากข้อบกพร่องของแอปพลิเคชั่น

Thesis Title	INTRUSION DETECTION SYSTEM
Student	Mr. Amorn Wannapin ID. 44010589
	Mr. Aungkarn Choomongkol ID. 44010603
Advisor	Mr. Puchong Hongsuwan
Graduate Level	Bachelor Degree of Information Engineering
Department	Information Engineering
Academic Year	2004

Abstract

In this project, we develop the Intrusion Detection System (IDS). IDS uses for detect the network intrusions and alert. In this project we detect 5 kinds of malicious attack, Port scanning , Brute force ,Trojan , Worm , and Application vulnerability

กิตติกรรมประกาศ

ในการทำปริญญานิพนธ์ฉบับนี้ไม่อาจสำเร็จไปได้เลย หากไม่ได้รับความช่วยเหลือจาก อาจารย์ภุ ชงค์ หงษ์สุวรรณ และอาจารย์ทุกๆท่านที่ได้ให้ความรู้ และประสบการต่างๆ ขอขอบคุณ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังแห่งนี้ ที่ได้ให้ใช้สถานที่ ในการศึกษาหาความรู้ ขอบคุณเพื่อนๆทุกคนที่ให้ความช่วยเหลือในทุกๆด้าน และสุดท้ายนี้ขอขอบคุณ บิดา มารดา ที่เป็นครูคนแรกและคอยให้กำลังใจตลอดมา จนสามารถทำปริญญานิพนธ์ฉบับนี้ให้สำเร็จลงได้ด้วยดี

คณะผู้จัดทำ

สารบัญ

สารบัญรูปภาพ

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ความเป็นมาของปริญญานิพนธ์

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

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

ในปริญญานิพนธ์ฉบับนี้ เป็นการออกแบบและสร้างอุปกรณ์ตรวจจับข้อมูลแปลกปลอมบนระบบเครือข่าย ซึ่งเป็นระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ โดยระบบตรวจจับข้อมูลแปลกปลอมบนระบบเครือข่ายนี้เป็นการป้องกัน ความไม่ถูกต้อง ความไม่เหมาะสมหรือการทำงานที่ผิดปรกติ ซึ่งอ้างอิงกับ ระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์ (Intrusion Detection System – IDS) เป็นหลัก โดยระบบตรวจจับผู้บุกรุกเป็นแบบปฏิบัติการบนการไหลข้อมูลใน

เครือข่าย เรียกว่า Network-based Intrusion Detection System ซึ่งใช้วิธีเกี่ยวกับการตรวจจับการใช้งานโดยการตรวจสอบกับข้อกำหนดการใช้งาน และ การตรวจสอบจากสถิติการใช้งานของผู้ใช้ และนำข้อมูลมาวิเคราะห์หาความเป็นไปได้ในการบุกรุก ที่เรียกว่า Signature Intrusion Detection

1.2 วัตถุประสงค์ของปริญญานิพนธ์

1. เพื่อสร้างระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์บนระบบปฏิบัติการลีนุกซ์
2. เพื่อศึกษาการทำงานของระบบปฏิบัติการลีนุกซ์
3. เพื่อศึกษาการใช้วิธีตรวจจับแบบการตรวจสอบกับข้อกำหนดการใช้งาน และตรวจสอบจากสถิติการใช้งานของระบบ (Signature Intrusion Detection)
4. เพื่อศึกษาและเขียนแอพพลิเคชั่นบนระบบปฏิบัติการลีนุกซ์

1.3 เป้าหมายของการพัฒนาของปริญญานิพนธ์

เพื่อพัฒนาระบบการรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ ให้มีความปลอดภัย โดยการเก็บข้อมูลเพื่อนำไปเปรียบเทียบกับข้อมูลรูปแบบการบุกรุกที่กำหนดขึ้น และสะดวกในการตรวจสอบผลของการตรวจจับการบุกรุก

1.4 ขอบเขตของปริญญานิพนธ์

ระบบที่พัฒนามีความสามารถในการตรวจจับผู้บุกรุกได้หลายลักษณะดังนี้

1.การสแกนพอร์ต(Port Scanning)

- 1.1 ฟิน สแกน(Fin Scan)
- 1.2 ซิน สแกน(Syn Scan)
- 1.3 ยูดีพี สแกน(UDP Scan)
- 1.4 นัลล์ สแกน(Null Scan)
- 1.5 คริสมาสต์ สแกน(Xmas Scan)
- 1.6 แอค สแกน(Ack Scan)
- 1.7 การสแกนแบบแฟรกเมนต์(Tiny Fragment Scan)

2.เวิร์ม(Worm)

- 2.1 เวิร์ม แซสเซอร์(Sasser Worm)
- 2.2 เวิร์ม นาชิ(Nachi Worm)
- 2.3 เวิร์ม เอสคิวแอล สแลมเมอร์(Sql Slammer Worm)

3.โทรจัน(Trojan)

3.1 การโจมตีพอร์ต โทรจัน

3.2 โทรจัน โดลี(Doly Trojan)

3.3โทรจัน อินเฟคเตอร์ (Infector Trojan)

3.4 โทรจัน ซับเซเวน(Sub7 Trojan)

4.การโจมตีช่องโหว่ของแอปพลิเคชัน (Application Vulnerability Attack)

4.1 การโจมตีช่องโหว่ของออราเคิล 9ไอ (Oracle 9i Vulnerability)

5.การโจมตีแบบ บรูทฟอร์ซ (Brute Force Attack)

5.1 บรูทฟอร์ซ เทลเน็ท(Telnet Brute Force)

5.2 บรูทฟอร์ซ เอสคิวแอล เซิร์ฟเวอร์(SQL Server Brute Force)

1.5 วิธีดำเนินงานของปริญญานิพนธ์

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

บทที่ 2
ทฤษฎีและหลักการ

2.1 ระบบตรวจจับผู้บุกรุกเครือข่าย (Intrusion Detection System – IDS)

แฮกเกอร์ (Hacker) โดยทั่วไปเราอาจเข้าใจว่าเป็นบุคคลหรือกลุ่มคนที่กระทำการประสงค์ร้ายกับเครื่องหรือระบบ เช่น แอบลอบเข้ามาในระบบแล้วทำให้ระบบเสียหาย

ในความเป็นจริงแล้วคำว่าแฮกเกอร์นั้น หมายถึง บุคคลหรือกลุ่มคนที่สนใจ หรือกระทำการเกี่ยวกับคอมพิวเตอร์ ที่นอกเหนือจากการใช้งานทั่วไปแต่เป็นในทางที่ดี เช่น กลุ่มที่พัฒนาโค๊ดต้นฉบับของเคอร์เนล หรือพัฒนาซอฟต์แวร์ขึ้นมาเองเพื่อนำมาใช้กับระบบปฏิบัติการที่ต้องการได้ หรือคอยพัฒนาซอฟต์แวร์ที่มาเพิ่มความปลอดภัยจากผู้ไม่ประสงค์ดีต่างๆ เป็นต้น ซึ่งไม่ได้ส่งผลร้ายกับใครหรือระบบใดๆ

ส่วนแคร็กเกอร์ (Cracker) นั้นจะเป็นบุคคลหรือกลุ่มคนที่กระทำการใดๆ โดยมีจุดประสงค์ไม่ดี ซึ่งถือว่าเป็นการผิดกฎหมายก็ว่าได้ เช่น ลักลอบเข้าเปลี่ยนแปลงแก้ไขเว็บไซต์ ทำลายข้อมูล ขโมยรหัสผ่าน ไม่ว่าจะเป็นรหัสผ่านเข้าระบบหรือรหัสผ่านของบัตรเครดิต การสร้างไวรัสคอมพิวเตอร์ เป็นต้น ซึ่งผลที่เกิดจากการกระทำดังกล่าวส่งผลให้เกิดความเสียหายกับบุคคลหรือองค์กร

ข้อมูลที่เรามองเห็นได้ขณะเราเล่นอินเทอร์เน็ตโดยผ่านแอพพลิเคชั่น(Application) เช่น เว็บเพจ (Webpage) ทางหน้าจอคอมพิวเตอร์ เป็นข้อมูลที่รับส่งกันตามปกติถูกต้องตามโพรโตคอลทุกประการ เพราะหากมีส่วนหนึ่งของข้อมูลนั้นเกิดผิดพลาด ไม่เป็นไปตามโพรโตคอลไม่ว่าจะเป็นที่ชั้นใด ข้อมูลนั้นก็จะถูกกำจัดทิ้งไป หรือข้อมูลบางอย่างที่ถึงแม้ว่าจะเป็นข้อมูลที่ถูกต้องตามปกติ แต่เป็นกลไกการรับส่งกันเองของโพรโตคอลเลเยอร์ล่างเพื่อให้การสื่อสารสมบูรณ์ ก็จะไม่ถูกส่งขึ้นมาให้ผู้ใช้ได้รับรู้ ซึ่งการทำงานลักษณะดังกล่าวในมุมมองของผู้ใช้งานแล้วน่าจะถูกต้องเพราะข้อมูลไม่เกี่ยวข้องก็ไม่น่าจะต้องส่งมาให้ผู้ใช้ได้พบเห็นแต่อย่างไร

ดังนั้นสิ่งที่ควรทำความเข้าใจเบื้องต้นก็คือ กิจกรรมต่างๆ บนเน็ตเวิร์คที่ผู้ใช้เห็นและรับรู้นั้นเป็นเพียงส่วนที่ถูกกำหนดในแอพพลิเคชั่นว่าให้นำมาแสดงต่อผู้ใช้เท่านั้น สิ่งอื่นๆ ที่ผู้ใช้ไม่ได้เห็น มิได้หมายความว่าไม่มีกิจกรรมใดเกิดขึ้น ยังมีอะไรที่เกิดขึ้นอีกมากมายที่เกิดขึ้นบนเน็ตเวิร์คหรือแม้กระทั่งบนเครื่องคอมพิวเตอร์ของเราเองโดยที่เราไม่รู้ตัวถึงแม้จะนั่งอยู่หน้าเครื่องตลอดเวลาก็ตาม อีกประการหนึ่งคือการสื่อสารของคอมพิวเตอร์นั้นมีระบบรักษาความปลอดภัยต่ำมาก โดยเฉพาะในระดับเน็ตเวิร์ค เลเยอร์ หากใช้งานตามค่าปกติโดยไม่ได้รับการปรับแต่งเป็นพิเศษแล้วแทบจะไม่สามารถป้องกันตัวเองได้จากการติดต่อจากผู้อื่นเลย คือใครอยากจะส่งข้อมูลมาหาเราก็สามารถทำได้ทันทีโดยที่เราหลีกเลี่ยงไม่ได้ สิ่งที่เราทำได้ก็คือเพียงแค่เลือกว่าจะนำข้อมูล

นั้นไปใช้งานหรือไม่ หากไม่ใช่สิ่งที่ต้องการก็กำจัดทิ้งไป หากว่าใช่สิ่งที่ต้องการก็นำมาใช้งาน แต่อย่างน้อยที่สุดก็ต้องรับเข้ามาก่อนเสมอ แทนที่จะสามารถรับเลือกเฉพาะข้อมูลที่ต้องการเท่านั้น ซึ่งแค่จุดอ่อนนี้เพียงจุดเดียวก็สามารถนำไปใช้ในการโจมตีเพื่อให้ปิดบริการเครื่องคอมพิวเตอร์ทั่วไปได้ทันที

หากเปรียบเทียบระบบหรือคอมพิวเตอร์ของเราเสมือนบ้าน ก็จะเป็นบ้านที่ไม่มีประตู ทุกคนสามารถเข้าออกได้อย่างเสรี ระบบปฏิบัติการและแอพพลิเคชั่นในเครื่องของเราเป็นเจ้าของบ้าน และข้อมูลที่สื่อสารกันไปมาบนเน็ตเวิร์คก็จะเป็นเหมือนคนเดินถนนทั่วไป เมื่อบ้านไม่มีประตูใครที่อยู่ข้างนอกอยากเข้ามาในบ้านก็เดินเข้ามาได้ตามปกติ เจ้าของบ้านนั้นมีหน้าที่เดินมาสอบถามทุกคนที่เข้ามาเพื่อให้ทราบว่าเป็นคนที่ต้องการติดต่อด้วยหรือไม่ หากไม่ใช่คนที่ติดต่อด้วยก็บอกให้เขากลับออกไป หากใช่ก็จะเชิญเข้ามาสนทนาด้วย เช่นหากแอพพลิเคชั่นของเรามีเฉพาะเมล์เซิร์ฟเวอร์(Mail Server) เจ้าของบ้านก็จะยินดีต้อนรับเฉพาะบุรุษไปรษณีย์เท่านั้น หากใครที่ไม่ใช่ก็จะไม่สนทนาด้วย ไม่ว่าจะเป็นคนดีหรือไม่ดี หรือเป็นผู้ทำหน้าที่อื่นที่อาจจะเข้ามาผิดบ้านก็ตาม อย่างไรก็ตามเจ้าของบ้านหลังนี้ไม่สามารถห้ามไม่ให้คนอื่นเดินเข้ามาได้หรือแม้กระทั่งไล่คนที่ไม่ต้องการออกไปก็ทำไม่ได้ ไม่ว่าใครจะเข้ามาในบ้านเจ้าของบ้านก็ต้องคอยออกมาสอบถามทุกครั้งไป ถึงแม้ว่าจะเป็นคนเดิมๆ ที่พยายามจะเข้ามาซ้ำแล้วซ้ำอีกตลอดทั้งวัน

โดยส่วนใหญ่แอพพลิเคชั่นที่ให้บริการถูกออกแบบมาเพื่อให้บริการดีที่สุด โดยไม่ได้ระวังอะไร เปรียบเสมือนคนที่มองโลกในแง่ดี ใครเข้ามาที่บ้านก็พยายามบริการอย่างดีที่สุด ดังนั้นหากใครจะ กลั่นแกล้งเจ้าของบ้านก็ทำได้ไม่ยากเย็น เช่นส่งคนเข้าไปในบ้านทีเดียวพร้อมกันหลายๆคนจนเจ้าของบ้านไม่มีเวลาไปทำงานอื่น (เทียบได้กับ ปิง ฟลัด (Ping Flood)), ส่งคนเข้ามาในบ้านแต่พอเจ้าของบ้านถามอะไร ก็ไม่ยอมตอบปล่อยให้เจ้าของบ้านรอเก้อ (ซิน ฟลัด (SYN Flood),ส่งคนหลายๆแบบมาหาเจ้าของบ้านเพื่อสืบว่าเจ้าของบ้านยินดีต้อนรับคนประเภทไหน (การสแกน พอร์ต (Port Scanning)) เป็นต้น เมื่อแอพพลิเคชั่นไม่ได้ถูกออกแบบมาให้ระมัดระวังเรื่องความปลอดภัย หากถูกก่อกวนมากๆ จนไม่สามารถรับมือได้ก็จะหยุดทำงานได้ในที่สุด

หากเปรียบระบบเป็นเสมือนบ้านแล้ว ระบบตรวจจับผู้บุกรุก จะเป็นเสมือนยามรักษาการณ์ทำหน้าที่เป็นผู้ช่วยเจ้าของบ้านเนื่องจากเจ้าของบ้านจะชำนาญเฉพาะเรื่องการบริการเท่านั้น กล่าวคือ ระบบตรวจจับผู้บุกรุก จะช่วยเสริมจุดด้อยส่วนนี้ให้แข็งแรงมากยิ่งขึ้น โดยทำตัวเป็นยามที่ชำนาญในการ วิเคราะห์คนผ่านเข้าออก โดยดูจากลักษณะของคนเหล่านั้น และรู้จักพฤติกรรมของคนอันธพาลหรือพวกก่อกวนเป็นอย่างดี หากใครมีพฤติกรรมน่าสงสัยก็จะรีบรายงานให้เจ้าของบ้านรู้ทันทีเมื่อได้รับรายงานแล้วจะดำเนินการอย่างไรต่อไปนั้นก็จะพิจารณาอีกที แต่อย่างน้อยที่สุดก็จะเป็นการป้องกันภัยล่วงหน้าสามารถรับรู้ถึงการพยายามบุกรุกหรือก่อกวนในทันทีที่เหตุการณ์เกิดขึ้น นับว่าระบบตรวจจับผู้บุกรุก เป็นเครื่องมือที่สำคัญอย่างยิ่งที่จะรับมือกับการบุกรุกเข้ามาของผู้ไม่หวังดี

ระบบตรวจจับผู้บุกรุก (IDS - Intrusion Detection System) เป็นระบบจัดการความปลอดภัยสำหรับคอมพิวเตอร์ และเครือข่ายที่พยายามตรวจหา และเตือนภัยเมื่อมีความพยายามในการบุกรุกเข้ามาในระบบ หรือ เครือข่าย เป็นอีกเครื่องมือหนึ่งที่ใช้กันอย่างมาก และมีความสำคัญอย่างยิ่งในปัจจุบัน ถึงแม้ว่าเครือข่ายอาจมีการการป้องกันการบุกรุกอยู่แล้ว โดยใช้ไฟร์วอลล์ (Fire wall) อย่างไรก็ตามไฟร์วอลล์ก็ยังไม่ใช่เครื่องมือที่จะป้องกันการบุกรุกได้โดยอัตโนมัติ จะต้องอาศัยผู้ที่บริหารที่กำหนดกฎให้เหมาะสมกับการใช้งาน และแม้จะมีกฎที่ดีแล้ว แต่ก็อาจไม่สามรถป้องกันการบุกรุกได้ การบริหารไฟร์วอลล์ที่ดีก็ควรจะมีการตรวจสอบย้อนหลัง และทดสอบการเจาะระบบเพื่อเป็นการทดสอบระบบอีกครั้ง ซึ่งตรงจุดนี้ ระบบตรวจจับผู้บุกรุกจะช่วยได้มาก เพื่อตรวจสอบแพ็กเก็ตต่างๆที่ผ่านเข้ามา ถ้าตรวจพบการบุกรุก ผู้บริหารก็สามารถนำข้อมูลที่ได้ไปปรับปรุงกฎให้รัดกุมยิ่งขึ้น

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

2.1.1 รูปแบบของระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์

มี วิธีหลักๆ ในการป้องกันผู้บุกรุก 2 วิธี คือ

1. วิธีตรวจสอบการใช้งานระบบที่ผิดปรกติ (Anomaly Intrusion Detection)

วิธีตรวจสอบการใช้งานทรัพยากรระบบที่ผิดปรกติตั้งอยู่บนสมมุติฐานว่าการกระทำใดๆที่เป็นการบุกรุกจะต้องมีการใช้งานระบบอย่างผิดปรกติ โดยมีการกระบวนการเก็บประวัติพฤติกรรมการใช้งานของผู้ใช้ และสังเกตการทำงานเกิดขึ้นของผู้ใช้ว่าเมื่อเข้ามาในระบบได้กระทำสิ่งใดบ้างแล้วรายงานเก็บประวัติซึ่งสามารถใช้เป็นข้อมูลตรวจสอบในการนำมาเปรียบเทียบว่าพฤติกรรมในปัจจุบันมีการใช้งานระบบที่ผิดปรกติกว่าประวัติพฤติกรรมของผู้ใช้เดิมมากน้อยเพียงใด หากมีการใช้ในปริมาณมากผิดปรกติจึงถือว่าเกิดการบุกรุก

ข้อเสียของการตรวจจับโดยวิธีตรวจสอบใช้งานระบบที่ผิดปรกติ คือ

- อาจมีพฤติกรรมการใช้งานทรัพยากรระบบของผู้ใช้ที่ผิดปรกติเกิดขึ้นแต่ไม่ได้เป็นการบุกรุกระบบ ทำให้ระบุสถานะผิดพลาด
- ตรวจไม่พบการบุกรุกระบบเนื่องจากการบุกรุกนั้นไม่ได้ใช้ทรัพยากรระบบอย่างผิดปรกติ
- หากผู้บุกรุกค่อยๆ เปลี่ยนพฤติกรรมการใช้งานไปทีละเล็กละน้อย ระบบจะไม่สามารถตรวจจับความผิดปรกติได้

2. วิธีการตรวจสอบกับข้อกำหนดการใช้งาน (Signature Intrusion Detection)

การตรวจสอบกับข้อกำหนดการใช้งาน (Signature Intrusion Detection) ประกอบด้วยการเก็บบันทึกและการระบุรูปแบบการบุกรุกซึ่งอาจบุกรุกจากจุดอ่อนของระบบหรือละเมิดกฎรักษาความปลอดภัย โดยมีตรวจจับคอยดูแลกิจกรรมต่างๆ ที่กระทำในปัจจุบันว่าพฤติกรรมการบุกรุกที่เคยเกิดขึ้นหรือได้รับราบงานว่าเป็นการบุกรุกหรือไม่ ในบางระบบมีการใช้กฎ (Rule-based expert system) โดยตั้งกฎขึ้นจากพฤติกรรมที่น่าสงสัย เช่น การ ล็อกอิน(login) ล้มเหลวเกินกว่า 3 ครั้งต่อเนื่องกัน ในเวลา 5 นาที ถือว่าพยายามบุกรุก และข้อมูลที่ใช้ตรวจสอบจะถูกนำมาเปรียบเทียบกับกฎ (Rules) ที่มีอยู่สังเกตว่ามีการนำข้อมูลทางเวลาเข้ามาพิจารณาด้วย การตรวจจับการบุกรุกโดยวิธีนี้สามารถมีการแก้ไขกฎหรือเพิ่มกฎได้ ในระบบทีเป็นปัญญาประดิษฐ์ (Artificial Intelligence) ระบบอาจทำการแก้ไขกฎหรือเพิ่มกฎได้ด้วยตนเอง

ข้อเสียของวิธีการตรวจสอบกับข้อกำหนดการใช้งาน และตรวจสอบจากสถิติการใช้งานของระบบ (Signature Intrusion Detection) คือ

1. ประสิทธิภาพของระบบตรวจจับชนิดนี้ ขึ้นอยู่กับความยากในการรวบรวมข้อมูลเกี่ยวกับรูปแบบการโจมตี และการปรับปรุงข้อมูลเกี่ยวกับช่องโหว่ต่างๆ ให้ทันสมัยอยู่เสมอ เนื่องจากข้อมูลต่างๆ นั้นขึ้นอยู่กับระบบปฏิบัติการ, เวอร์ชั่น, แพลทฟอร์ม(platform) และแอพพลิเคชั่น นอกจากชั้นการตรวจจับการโจมตีจากภายในนั้นทำได้ยากเนื่องจาก การโจมตีจากภายในเกี่ยวกับการละเมิดสิทธิของผู้ใช้งาน (user) ซึ่งไม่ได้เกี่ยวข้องกับช่องโหว่แต่อย่างใด

2. มีข้อจำกัดในเรื่องจำนวนของรูปแบบในการบุกรุก ซึ่งหากเป็นการบุกรุกที่ระบบไม่รู้จักมาก่อนจะทำให้ไม่สามารถตรวจจับการบุกรุกได้

2.1.2 ประเภทของระบบการตรวจจับผู้บุกรุก

ระบบตรวจจับผู้บุกรุก แบ่งเป็น 2 ประเภท คือ

1. ระบบตรวจจับผู้บุกรุกในโฮสต์ (Host-based Intrusion Detection System)

ระบบตรวจจับผู้บุกรุกในโฮสต์ (Host-based Intrusion Detection System) เป็นซอฟแวร์ที่ประมวลผลบนโฮสต์ โดยปกติแล้วระบบตรวจจับผู้บุกรุกประเภทนี้จะวิเคราะห์ล็อก (Log) เพื่อค้นหาข้อมูลเกี่ยวกับการบุกรุก ในระบบยูนิกซ์นั้นล็อกที่ ระบบตรวจจับผู้บุกรุก จะตรวจสอบ เช่น ซิสล็อก(Syslog),ลาสล็อก(Lastlog) และ Wtmp เป็นต้น ส่วนในวินโดวส์นั้นระบบตรวจจับผู้บุกรุกก็จะตรวจสอบอีเวนต์ล็อกต่างๆ เช่น ซิสเต็ม(System), แอพพลิเคชั่น และซีเคียวริตี(Security) เป็นต้น โดยปกติระบบตรวจจับผู้บุกรุกจะอ่านเหตุการณ์ใหม่ที่เกิดขึ้นในล็อกและเปรียบเทียบกับกฎที่ตั้งไว้ก่อนหน้า ถ้าตรงก็จะแจ้งเตือนทันที ดังนั้นการที่ ระบบตรวจจับผู้บุกรุกจะตรวจจับการบุกรุกได้ระบบจะต้องบันทึกเหตุการณ์ต่างๆที่สำคัญที่เกิดขึ้นในระบบล็อกไฟล์ ถ้าไม่เช่นนั้น ไอดีเอส (IDS) ก็ไม่มีข้อมูลที่จะใช้วิเคราะห์ว่ามีการบุกรุกหรือไม่

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

ข้อได้เปรียบของระบบตรวจจับผู้บุกรุกในโฮสต์ เช่น

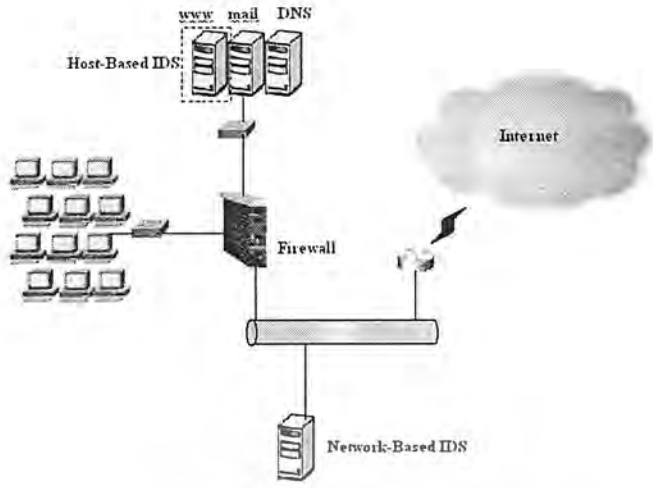
- ระบบตรวจจับผู้บุกรุกในโฮสต์สามารถตรวจพบทุกการบุกรุกกับโฮสต์นั้นๆ ได้เสมอถ้าระบบสามารถบันทึกเหตุการณ์ดังกล่าวในล็อกได้ หรือการบุกรุกมีการเรียกใช้ซิสเท็มคอล
- ระบบตรวจจับผู้บุกรุกในโฮสต์สามารถบอกได้ว่าการบุกรุกนั้นสำเร็จหรือไม่ โดยการวิเคราะห์ข้อความในล็อกหรือจากหลักฐานอื่นๆ เช่น มีการแก้ไขไฟล์ที่สำคัญของระบบ เป็นต้น
- ระบบตรวจจับผู้บุกรุกในโฮสต์สามารถบ่งชี้ได้ว่า มีการเข้าใช้ระบบอย่างผิดปกติโดยผู้ใช้ของระบบเอง

ข้อสียเปรียบของระบบตรวจจับผู้บุกรุกในโฮสต์คือ

- โพรเซสของระบบตรวจจับผู้บุกรุกอาจถูกโจมตีจนอาจไม่สามารถแจ้งเตือนได้
- ระบบตรวจจับผู้บุกรุกในโฮสต์จะแจ้งเตือน ก็เมื่อ เหตุการณ์ที่เกิดขึ้นนั้นตรงกับที่กำหนดไว้ก่อนหน้า ถ้าผู้บุกรุกมีเทคนิคใหม่ ๆ ระบบตรวจจับผู้บุกรุกอาจไม่แจ้งเตือนการบุกรุกก็ได้
- การทำงานของระบบตรวจจับผู้บุกรุกในโฮสต์ อาจมีผลกระทบต่อประสิทธิภาพของโฮสต์เองเนื่องจากต้องตรวจสอบล็อกไฟล์และซิสเต็มคอลล์

2. ระบบตรวจจับผู้บุกรุกเครือข่าย (Network Intrusion Detection System)

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



รูปที่ 2.1 แสดงระบบตรวจจับผู้บุกรุกแบบต่าง ๆ

โดยระบบนี้จะทำการตรวจสอบแพ็กเก็ตต่างๆ บนเครือข่ายเพื่อดูว่ามีข้อมูลที่ผิดปกติ หรือว่ามีพฤติกรรมที่น่าสงสัยหรือไม่ ซึ่งก็คือการพยายามค้นหาผู้บุกรุก (Hacker) ที่กำลังพยายามเข้ามาในระบบ หรือ ปิดการให้บริการของระบบ (a denial of service attack) โดยการนำแพ็กเก็ตต่างๆ ที่เข้ามาสู่ระบบ แล้วนำมาวิเคราะห์เปรียบเทียบกับกฎต่างๆ ที่ระบุไว้ว่าเป็นการโจมตีหรือการบุกรุก หรือถึงนโยบายขององค์กรก็นำมาพิจารณาด้วย เพื่อตรวจสอบว่ามีสิ่งผิดปกติขึ้นกับระบบหรือไม่ ตัวอย่างที่เกิดขึ้นคือ การส่งแพ็กเก็ตที่เป็นการร้องขอการเชื่อมต่อ (TCP connection request (SYN)) สู่พอร์ต (port) ต่างๆ บนเครื่องเป้าหมาย หรือส่งแพ็กเก็ตจำนวนมากจนเครื่องเป้าหมายรับไม่ไหว ทำให้ระบบต้องหยุดตัวลง โดยทั่วไปแล้วระบบตรวจจับผู้บุกรุกเครือข่ายนี้จะถูกติดตั้งบนเครื่องเดียว แต่ตรวจสอบและวิเคราะห์แพ็กเก็ตทั้งระบบเครือข่าย โดยจะต้องทำการติดตั้งระบบที่ใช้ฮับ (Hub) ในการเชื่อมต่อ เพื่อที่จะสามารถรับข้อมูลทั้งหมดในช่องทางการสื่อสารได้ ถ้าเราติดตั้งระบบนี้บนสวิตซ์ เราจะรับข้อมูลได้เฉพาะของเครื่องเราเท่านั้น ซึ่งก็จะทำไม่ให้ประสิทธิภาพ

ระบบที่จะศึกษาและทำขึ้นมาในที่นี้คือ ระบบตรวจจับผู้บุกรุกเครือข่าย (Network Intrusion Detection System)

2.1.3 หลักการทำงานพื้นฐานของระบบตรวจจับผู้บุกรุกแบบทางเครือข่าย

ระบบตรวจจับผู้บุกรุกเครือข่าย ทำงานโดยการใช้แหล่งข้อมูลจากเครือข่าย เป็นการดักจับแพ็กเก็ตที่ผ่านมาในเครือข่ายที่อยู่ในแชร์โดเมน (share domain) เดียวกัน และนำข้อมูลแพ็กเก็ตมาวิเคราะห์และเมื่อตรวจพบลักษณะที่ตรงกับข้อมูลที่จัดว่าเป็นการบุกรุกอยู่ก็จัดการตามที่ตั้งไว้ต่อไปซึ่งอาจจะเป็นการเก็บข้อมูลลงล็อกไฟล์ (log file) หรือการแสดงข้อความเตือนผู้ดูแลระบบ ซึ่งในส่วนของการที่ได้ข้อมูลมานั้น จะใช้หลักการของเครื่องมือที่ชื่อว่า แพ็กเก็ตแคปเจอร์ (Packet Capture)

คำว่า แพกเก็ต แคปเจอร์(Packet Captor) เป็นโปรแกรมวิเคราะห์เน็ตเวิร์ก โดยอาศัยการดักจับข้อมูลภายในเน็ตเวิร์กทั้งหมดมาวิเคราะห์การใช้งานระบบเน็ตเวิร์ก โหมดการทำงานที่อนุญาตฮาร์ดแวร์รับข้อมูลของผู้อื่นเข้ามาได้โดยไม่มีการปิดกั้นเรียกว่า โพรมิสเชียสโหมด (Promiscuous Mode) เป็นโหมดที่ทำให้ ฮาร์ดแวร์อ่านข้อมูลดิบทั้งหมดบนเน็ตเวิร์คเข้ามาในเครื่องคอมพิวเตอร์ของตนเอง ได้โดยไม่สนในว่าจะเป็นของใคร ส่งให้ใคร และเป็นการละเมิดข้อบังคับของโพรโตคอลหรือไม่

2.1.4 ประโยชน์ของระบบตรวจจับผู้บุกรุกที่เป็นแบบทางเครือข่าย

ระบบตรวจจับผู้บุกรุกทางเครือข่ายมีหลายจุด ซึ่งระบบตรวจจับผู้บุกรุกที่เป็นแบบโฮสต์เบสไม่สามารถทำได้โดยลำพัง ได้แก่การที่สามารถดักจับแพ็กเก็ตแบบเรียลไทม์ และวิเคราะห์มันได้ ในหัวข้อต่อไปนี้จะเป็นจุดแข็งที่แสดงให้ถึงความจำเป็นของการมีระบบตรวจจับผู้บุกรุกเป็นส่วนหนึ่งระบบรักษาความปลอดภัย

1. ค่าของการดูแลจัดการ ระบบรักษาความปลอดภัยทางเครือข่าย ให้การนำมาใช้กับระบบที่ต้องการเป็นไปได้ง่าย โดยสามารถติดตั้งเป็นจุดๆ ไปได้ และใช้ได้กับเครื่องเป้าหมายที่กว้างซอฟต์แวร์ที่ติดตั้งไม่จำเป็นต้องติดในทุกเครื่องเหมือนกับแบบระบบตรวจจับผู้บุกรุกในโฮสต์ การที่จุดติดตั้งการตรวจจับมีจำนวนน้อย ทำให้ค่าการดูแลและจัดการเป็นไปอย่างมีประสิทธิภาพมากขึ้น

2. การวิเคราะห์แพ็กเก็ต ระบบตรวจจับผู้บุกรุกทางเครือข่าย จะตรวจสอบในส่วนหัวของแพ็กเก็ตเพื่อหาสัญญาณของการบุกรุก หรือการกระทำที่เป็นที่น่าสงสัย ซึ่งการโจมตีเพื่อปิดบริการในปัจจุบันหลายตัวจะถูกตรวจสอบพบได้โดยการดูที่ส่วนหัวของมัน เมื่อแพ็กเก็ตผ่านมาในเครือข่าย ตัวอย่างเช่น การโจมตีแบบ แลนด์(Land) จะเป็นแพ็กเก็ตที่ถูกปลอมขึ้นมาให้มี ไอพีแอดเดรส ต้นทางและปลายทางเหมือนกัน ซึ่งการโจมตีประเภทนี้จะถูกตรวจพบได้โดยง่าย เมื่อใช้ระบบตรวจจับผู้บุกรุกทางเครือข่ายทำงานแบบเรียลไทม์ ทั้งนี้การโจมตีที่ใช้แพ็กเก็ตแฟร็กเมนต์ เช่น เทียร์ดรอป(Teardrop) ก็สามารถถูกตรวจพบได้ในชั้นการวิเคราะห์แพ็กเก็ตเช่นกัน ซึ่งระบบตรวจจับผู้บุกรุกในโฮสต์ จะไม่สามารถตรวจพบการโจมตีประเภทเหล่านี้ได้ และนอกจากการตรวจสอบที่ส่วนหัวของแพ็กเก็ตแล้ว ระบบตรวจสอบผู้บุกรุกทางเครือข่ายยังสามารถตรวจสอบในส่วนเนื้อข้อมูลในแพ็กเก็ต เพื่อที่จะหาคำสั่งเฉพาะหรือรูปแบบโครงสร้างบางชนิดที่ใช้ในการโจมตี ซึ่งคำสั่งเหล่านี้จะเป็นตัวชี้บอกถึงว่าเป็นการโจมตี ไม่ว่าการโจมตีนั้นจะสำเร็จหรือไม่ก็ตาม ตัวอย่างเช่น ผู้บุกรุกทำการลองตรวจสอบการมีของโปรแกรม แบ็ค ออริฟิส(Back Orifice) ในระบบที่ไม่ถูกบุกรุกโดย แบ็ค ออริฟิส ซึ่งการกระทำนี้จะไม่มีผลกระทบต่อระบบนี้ แต่เราจะสามารถรู้ได้ถึงความพยายามที่จะบุกรุก ซึ่งถ้าเป็นระบบตรวจจับผู้บุกรุกในโฮสต์ จะไม่สามารถตรวจสอบแบบข้อมูลในแพ็กเก็ตได้

3. การลบร่องรอย ระบบตรวจจับผู้บุกรุกคอมพิวเตอร์เครือข่ายใช้การตรวจจับแบบเรียลไทม์ (Real Time) และเมื่อตรวจจับได้แล้ว ผู้บุกรุกจะไม่สามารถลบหลักฐานนี้ทิ้งได้ สิ่งที่ตรวจจับได้ไม่ใช่เพียงแค่การโจมตีเท่านั้น แต่ยังมีข้อมูลอื่นที่อาจนำต่อไปได้ถึงผู้บุกรุกด้วย ปัญหาหนึ่งของระบบตรวจจับผู้บุกรุกทางคอมพิวเตอร์แบบโฮสต์เบสที่มักจะพบคือ ผู้บุกรุกเข้าใจและมีความรู้ในเรื่องล็อกไฟล์เป็นอย่างดี และมันก็มักจะเป็นที่แรกที่ผู้บุกรุกจะไปลบรอยของตัวเอง และเอาออก หรือทำลายข้อมูลส่วนนั้น

4. การตรวจจับและตอบสนองแบบเรียลไทม์ ระบบตรวจจับผู้บุกรุกทางเครือข่ายตรวจจับความผิดปกติ หรือการบุกรุกที่เกิดขึ้นอย่างต่อทันเหตุการณ์และรายงานในทันที ตัวอย่างเช่น ถ้าตรวจสอบพบว่าการโจมตีเพื่อให้ปิดบริการเกิดขึ้นโดยเกิดบนโพรโตคอล ทีซีพีอาจจะมีการสั่งให้ระบบส่ง ทีซีพี รีเซต(TCP Reset) ในทันทีเพื่อหยุดยั้งการโจมตีไว้ก่อนที่จะทำให้เกิดความเสียหายแก่ระบบมากขึ้น ในอีกหลาย ๆ สถานการณ์ ด้วยระบบตรวจจับผู้บุกรุกในโฮสต์ การรับทราบถึงเหตุการณ์ที่เกิดขึ้นในภายหลังและบางทีอาจไม่มีกี่เดือนถึงเลยเนื่องมาจากที่ระบบได้เสียไปก่อนแล้ว ในการที่มีการเตือนแบบเรียลไทม์นั้นจะทำให้สามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที หรือถ้าไม่ต้องการก็สามารถรวบรวมข้อมูลไว้เพื่อวิเคราะห์ต่อในภายหลังได้

5. การตรวจจับเจตนาที่มุ่งร้าย ระบบจะมีประโยชน์มากในการตรวจจับถึงเจตนาของการ กระทำ ถ้านำระบบตรวจจับผู้บุกรุกทางเครือข่ายไปไว้ก่อนไฟร์วอลล์เราจะสามารถรู้ได้ถึงความพยายามในการที่จะโจมตีของผู้บุกรุกได้ แม้ว่าแพ็กเก็ตที่ต้องการโจมตีนั้นจะถูกปฏิเสธโดยไฟร์วอลล์ก็ตาม ถ้าเป็นระบบตรวจจับผู้บุกรุกในโฮสต์ จะไม่มีโอกาสตรวจพบความพยายามที่จะโจมตีที่จะปฏิเสธออกไปแล้วนี้เลย เนื่องจากมันไม่ได้ถูกกระทำจริงบนโฮสต์ แต่มันก็ถือว่าเป็นสิ่งจำเป็นที่ต้องรู้ถึงความถี่และชนิดของการโจมตีที่กระทำบนเครือข่ายของเรา

6. การทำให้สมบูรณ์ยิ่งขึ้น และ การช่วยตรวจสอบ ระบบตรวจสอบผู้บุกรุกจะเป็นองค์ประกอบที่ทำให้ส่วนอื่นๆ ที่ใช้ในมาตรการรักษาความปลอดภัยอยู่แล้ว สมบูรณ์ยิ่งขึ้น ตัวอย่างเช่น ในการเข้ารหัสข้อมูล แม้ว่าระบบตรวจสอบผู้บุกรุกบนเครือข่ายจะไม่สามารถอ่านข้อมูลที่เข้ารหัสได้ แต่มันจะสามารถตรวจสอบได้ว่า ข้อมูลในเครือข่ายอันไหนที่ไม่ได้ถูกเข้ารหัสไว้ ส่วนในกรณีของไฟร์วอลล์ ระบบตรวจสอบผู้บุกรุกบนเครือข่ายจะช่วยในการตรวจสอบว่ามันได้ทำหน้าที่ในการป้องกันแพ็กเก็ตที่ควรจะปฏิเสธได้ถูกต้อง ครบถ้วนหรือยัง

7. การไม่ขึ้นอยู่กับระบบปฏิบัติการใด ๆ ระบบตรวจสอบผู้บุกรุกบนเครือข่าย ไม่ขึ้นอยู่กับ ระบบปฏิบัติการของโฮสต์ที่ต้องการตรวจสอบความผิดปกติ เหมือนกับวิธีของระบบตรวจจับผู้บุกรุกในโฮสต์ ซึ่งข้อมูลในล็อกของระบบตรวจจับผู้บุกรุกในโฮสต์ จะได้มาได้ต้องขึ้นกับการทำงานของระบบปฏิบัติงานที่ถูกต้องการ ไม่ขึ้นอยู่กับระบบปฏิบัติการใดๆ ระบบตรวจสอบผู้บุกรุกบนเครือข่ายไม่ขึ้นอยู่กับระบบปฏิบัติการของโฮสต์ ที่ต้องการตรวจสอบความ

ผิดปกติ เหมือนกับวิธีของระบบตรวจจับผู้บุกรุกในโฮสต์ ซึ่งข้อมูลในล็อกของระบบตรวจจับผู้บุกรุกในโฮสต์ จะได้มาได้ต้องขึ้นกับการทำงานของระบบปฏิบัติงานที่ถูกต้อง

2.1.5 ข้อดีและข้อเสียของระบบตรวจจับผู้บุกรุก

ข้อดีของระบบตรวจจับผู้บุกรุก

1. การตอบสนองทันทีทันใด

จริงๆ แล้วการวิเคราะห์การบุกรุกนั้น หากเป็นผู้เชี่ยวชาญที่ความรู้ ความเข้าใจด้านเน็ตเวิร์คและโพรโตคอลเป็นอย่างดี ก็จะวิเคราะห์ได้โดยอาศัยเครื่องมือเพียงเล็กน้อยเท่านั้น คือ ใช้เครื่องมือทำการจัดเก็บบันทึกข้อมูลทั้งหมดที่มีการสื่อสารกันบนเน็ตเวิร์คแล้วนำข้อมูลที่ได้เหล่านั้นมาวิเคราะห์โดยพฤติกรรมและความสัมพันธ์ ก็จะสามารถหาสิ่งผิดปรกติที่เกิดขึ้นได้ แต่การวิเคราะห์ในลักษณะดังกล่าวจะกระทำได้ก็ต่อเมื่อได้เกิดเหตุการณ์ไปแล้วเนื่องจากการวิเคราะห์จะเป็นไปในลักษณะการวิเคราะห์ข้อมูลย้อนหลัง มาสามารถที่จะกระทำได้ในทันที ซึ่งระบบตรวจจับผู้บุกรุก จะช่วยแก้ไขข้อบกพร่องในส่วนนี้ เพราะ ระบบตรวจจับผู้บุกรุก สามารถตรวจจับได้ทันทีที่มีความผิดปรกติเกิดขึ้น และช่วยให้ทำการแก้ไขได้ทันท่วงที การทำงานพื้นฐานของระบบตรวจจับผู้บุกรุก จะเหมือนกบการที่ทำโดยคน เพียงแต่ ระบบตรวจจับผู้บุกรุก นั้นทำงานโดยอัตโนมัติและการทำงานอยู่ตลอดเวลาไม่มีหยุด จึงสามารถตอบสนองต่อสิ่งที่ผิดปรกติได้รวดเร็วกว่า ซึ่งถ้าให้คนมานั่งตรวจจับก็ไม่สามารถทำได้ตลอดเวลา

2. การมีฐานความรู้ของการวิเคราะห์

จากที่กล่าวมาข้างต้น การที่จะตรวจจับสิ่งผิดปรกติและแยกแยะกิจกรรมเหล่านั้นออกจากการสื่อสารข้อมูลตามปรกติได้นั้นจะต้องอาศัยความชำนาญ และเข้าใจในรูปแบบของการสื่อสารข้อมูลและการบุกรุกเป็นอย่างดี นั่นคือทักษะที่จำเป็นของนักวิเคราะห์การบุกรุก (Intrusion Analysis) ซึ่งผู้เชี่ยวชาญในระดับที่จะทำงานเช่นนี้ได้มีไม่มากนัก ประกอบกับเทคนิคและกลวิธีในการบุกรุกหรือก่อกวนนั้นได้พัฒนาขึ้นทุกวัน วิธีการตรวจจับและวิเคราะห์จำเป็นต้องพัฒนาตามให้สอดคล้องกันจึงจะตรวจจับได้อย่างมรประสิทธิผล ซึ่งในส่วนนี้ผู้เชี่ยวชาญเองก็อาจจะทำได้ไม่ดีเท่า

ระบบตรวจจับผู้บุกรุก สามารถช่วยแบ่งเบาภาระของนักวิเคราะห์ลงได้มาก โดยหากรู้รูปแบบพฤติกรรมแน่ชัดว่าเป็นการมุ่งร้ายก็ให้จัดเก็บข้อมูลรูปแบบเหล่านี้ในระบบตรวจจับผู้บุกรุกเสีย เมื่อมีกิจกรรมดังกล่าวเกิดขึ้นในเน็ตเวิร์คระบบตรวจจับผู้บุกรุก ก็สามารถตรวจพบได้ทันที และเมื่อค้นพบรูปแบบใหม่ก็จัดเก็บลงในระบบตรวจจับผู้บุกรุก อีก ทำให้ระบบตรวจจับผู้บุกรุกเสมือนมีฐานความรู้ในการวิเคราะห์การบุกรุกได้ดีในระดับหนึ่ง และขีดความสามารถก็จะเพิ่มขึ้นเรื่อยๆ ตามปริมาณของรูปแบบที่เก็บอยู่ในฐานความรู้นั่นเอง หากมีการบำรุงรักษาฐานความรู้ในตัวระบบตรวจจับผู้บุกรุก ได้ดีและนำ ระบบตรวจจับผู้บุกรุก ไปใช้ในจุดที่เหมาะสมแล้ว การบุกรุกที่ไม่ใช่เทคนิคใหม่ล่าสุดจริงๆ ก็แทบจะไม่สามารถเล็ดรอดสายตา ระบบตรวจจับผู้บุกรุก ไปได้ ถึง

ขั้นนี้แล้วแม้ว่าจะเป็น ระบบตรวจจับผู้บุกรุก ธรรมดาๆ ก็มีความสามารถมากกว่าผู้บริหารระบบทั่วไปเสียอีก

สำหรับนักวิเคราะห์แล้วเมื่อมีระบบตรวจจับผู้บุกรุก จะทำให้ไม่ต้องห่วงหน้าพะวงหลัง เพราะการบุกรุกที่สามารถตรวจจับได้ง่ายๆ ก็สามารถตรวจพบได้โดยระบบตรวจจับผู้บุกรุก อย่างน้อยระบบตรวจจับผู้บุกรุก ก็ช่วยกลั่นกรองข้อมูลเบื้องต้นได้ในระดับหนึ่งและแบ่งเบาภาระได้พอสมควร

3. การช่วยตรวจสอบข้อบกพร่องของระบบป้องกันอื่นๆ

เน็ตเวิร์คของผู้ใช้อาจมีการป้องกันการบุกรุกอยู่แล้วโดยใช้ไฟร์วอลล์ อย่างไรก็ตามไฟร์วอลล์มิใช่เครื่องมือที่จะป้องกันการบุกรุกได้โดยอัตโนมัติ จะต้องอาศัยผู้ที่บริหารระบบกำหนดกฎให้เหมาะสมกับการใช้งาน อีกประการหนึ่ง ถึงแม้จะมีการตั้งกฎที่เหมาะสมแล้วก็ตาม แต่กฎเหล่านั้นอาจไม่สามารถป้องกันการบุกรุกได้ การบริหารไฟร์วอลล์ที่ดีก็ควรจะมีการตรวจสอบย้อนหลัง (Audit) และการทดสอบการเจาะระบบ (Penetration Test) เพื่อเป็นการตรวจทานระบบอีกครั้งหนึ่ง

ระบบตรวจจับผู้บุกรุก สามารถช่วยได้มาก โดยติดตั้งระบบตรวจจับผู้บุกรุก ไว้หลังไฟร์วอลล์ และทำการทดสอบเจาะระบบด้วยวิธีต่างๆ เพื่อดูว่ามีเทคนิคใดที่สามารถเจาะผ่านไฟร์วอลล์ได้บ้าง และหากมีแพ็กเกจใดผ่านเข้าไปได้ ระบบตรวจจับผู้บุกรุก ก็จะตรวจพบ ทำให้ผู้บริหารระบบสามารถปรับปรุงกฎให้รัดกุมมาก

ข้อเสียของระบบตรวจจับผู้บุกรุก

ถึงแม้ระบบตรวจจับผู้บุกรุก จะมีประโยชน์ค่อนข้างมาก ในการช่วยรักษาความปลอดภัยและการเตือนภัยล่วงหน้า แต่ก็มีข้อเสียอยู่หลายประการซึ่งผู้ที่จะนำไปใช้จะต้องตระหนักไว้

1. การละเมิดความเป็นส่วนบุคคล

เนื่องจาก ระบบตรวจจับผู้บุกรุก มีพื้นฐานจากการนำข้อมูลทั้งหมดที่สื่อสารกันมาทำการวิเคราะห์ ซึ่งข้อมูลเหล่านั้นจะต้องครอบคลุมถึงข้อมูลทั่วไปที่มีการสื่อสารกันตามปรกติ และการมีทราบว่ามีความผิดปรกติหรือไม่นั้นก็จะต้องอ่านข้อมูลทั้งหมดด้วย ดังนั้นไม่ว่าจะมีกิจกรรมใดๆ ที่เกิดขึ้นในเน็ตเวิร์คไม่ว่าจะเป็นการท่องเว็บ , การดาวน์โหลด(Down Load) ข้อมูล , การแช็ท (Chat) คุยกัน , ไอซีคิว(ICQ) , จดหมายอิเล็กทรอนิกส์(e-mail) และกิจกรรมอื่นๆ ที่สื่อสารข้อมูลผ่านเน็ตเวิร์ค ก็จะสามารถถูกเปิดอ่านได้จาก ระบบตรวจจับผู้บุกรุก นั่นหมายความว่าระบบตรวจจับผู้บุกรุก สามารถนำไปใช้ในทางที่ผิดเพื่อละเมิดสิทธิส่วนบุคคลได้ การทำงานของ ระบบตรวจจับผู้บุกรุก เปรียบเสมือนการที่ตำรวจต้องการตรวจสอบและดักจับผู้ไม่หวังดีที่คอยโทรศัพท์ก่อกวนชาวบ้านในหมู่บ้าน และเพื่อการนี้ตำรวจจึงต้องทำการดักฟังโทรศัพท์ของทุกคนที่อยู่ในหมู่บ้านนั้น ซึ่งอาจมีเพียงหนึ่งในพันที่เป็นผู้ร้าย แต่ตำรวจที่ทำหน้าที่ดักฟังก็จะรู้ความลับของคนทุกคน บางทีการที่มีคนดักฟังความลับของทุกคนอาจเป็นอันตรายกว่าการโดนผู้ร้ายก่อกวนก็เป็นได้

ดังนั้นการนำระบบตรวจจับผู้บุกรุก มาติดตั้งในเน็ตเวิร์คจะต้องได้รับการอนุมัติจากหน่วยงานอย่างถูกต้องแล้วเท่านั้น และผู้ทำหน้าที่ในด้านนี้จะต้องเป็นผู้ที่ได้รับความไว้วางใจและมีความรับผิดชอบสูงในอันที่จะไปละเมิดสิทธิส่วนบุคคลของคนอื่น และหากเห็นข้อมูลใดๆ ก็จะต้องไม่เปิดเผยข้อมูลเหล่านั้นแก่บุคคลอื่น โดยทั่วไปแล้วการติดตั้งอุปกรณ์ที่สามารถอ่านข้อมูลของผู้อื่นบนเน็ตเวิร์คได้นั้นจะเป็นข้อห้ามอันดับต้นๆ ในนโยบายรักษาความปลอดภัยเลยทีเดียว สิ่งทีเป็นข้อสังเกต คือ การกระทำในลักษณะนี้ยากต่อการป้องกันในทางเทคนิค ดังนั้นหน่วยงานโดยทั่วจึงต้องกำหนดเป็นข้อห้ามในนโยบายความปลอดภัย และมีบทลงโทษสำหรับผู้ที่ละเมิดในขั้นรุนแรง

2. การตอบโต้อัตโนมัติ

ระบบตรวจจับผู้บุกรุกที่มีจำหน่ายอยู่ในท้องตลาดจะมีส่วนหนึ่งที่ให้ผู้ใช้สามารถกำหนดการดำเนินการอย่างหนึ่งอย่างใดเมื่อตรวจพบการบุกรุกเกิดขึ้น เช่น ส่งจดหมายเตือนผู้ดูแลระบบ เรียกวิทยุติดตามตัว ส่งคำสั่งไปยังไฟร์วอลล์เพื่อจำกัดการเข้าออกของข้อมูล และสิ่งที่สำคัญที่สุดซึ่งอาจจะส่งผลเสียหายใหญ่หลวงต่อเจ้าของได้ก็คือ การโจมตีกลับไปยังต้นกำเนิดของการบุกรุก (Counter attack) โดยที่ ระบบตรวจจับผู้บุกรุก เองก็จะรู้จักวิธีการโจมตีแบบต่างๆ ดีอยู่แล้ว จึงมิใช่เรื่องยากเย็นแต่อย่างใดที่จะทำการโจมตีผู้อื่น ผู้ผลิตจึงมักเพิ่มเติมส่วนนี้ให้แก่ระบบตรวจจับผู้บุกรุก เสมือนหนึ่งการติดอาวุธ ไว้ให้ต่อกรกับผู้บุกรุก

ผู้ดูแลระบบบางส่วนอาจรู้สึกสะใจและคิดว่าเหมาะสมแล้ว กับการโจมตีกลับไปยังผู้บุกรุกเหล่านั้นให้หลาบจำจะได้ไม่พยายามมาข้องแวะอีก เป็นนโยบายรักษาความปลอดภัยแบบตาต่อตาฟันต่อฟัน และเชื่อว่าหากกำหนดให้การโจมตีกลับเป็นไปอย่างอัตโนมัติแล้วน่าจะทำให้ปลอดภัยมากขึ้น ในค่ำคืนที่เงียบสงบใครจะไปรู้ว่า ระบบตรวจจับผู้บุกรุก อาจจะกำลังต่อกรอยู่กับผู้บุกรุก ที่กำลังแอบเข้ามาในระบบอย่างสุดกำลัง และสู้ยิบตาเพื่อรักษามิให้ผู้บุกรุกทำการบุกรุกเข้ามาในเน็ตเวิร์คได้ ในโลกแห่งความเป็นจริงแล้วการตัดสินใจว่าผู้ใดเป็นผู้บุกรุก อย่างชัดเจนนั้นมิได้ทำได้โดยง่ายและในเวลาอันรวดเร็ว การที่กำหนดให้ ระบบตรวจจับผู้บุกรุก ทำการตอบโต้กลับไปในทันทีโดยมีข้อมูลเพียงผิวเผินนั้น นอกจากจะไม่ช่วยให้เน็ตเวิร์คของเราปลอดภัยแล้ว ยังทำให้เรากลายไปเป็นผู้บุกรุก ที่คอยโจมตีผู้อื่นเสียเอง ยกตัวอย่างความเสียหายเช่น

- การวิเคราะห์ผิดพลาดเข้าใจว่ากิจกรรมที่เกิดขึ้นเป็นการบุกรุกและระบบตรวจจับผู้บุกรุก จะดำเนินการโจมตีกลับในทันที กรณีผู้บริสุทธิ์ก็จะถูกโจมตีจาก ระบบตรวจจับผู้บุกรุก ของเราโดยที่ไม่รู้เรื่องใดๆ
- การวิเคราะห์ถูกต้องแต่แอดเดรสของต้นทางเป็นแอดเดรสปลอม กรณีหากระบบตรวจจับผู้บุกรุก ไม่มีกลไกในการตรวจสอบแอดเดรสที่มีประสิทธิภาพ อาจไม่สามารถแยกแยะได้ว่าต้นทางของการโจมตีแท้จริงนั้นเป็นที่ไหน และทำการโจมตีกลับไปก็อาจจะมิใช่ตัวการที่แท้จริง และเหตุการณ์จะเลวร้ายยิ่งขึ้นหากแอดเดรสที่

ปลอมมานั้นเป็นหน่วยงานของความมั่นคงหรือหน่วยงานทางทหาร และเมื่อนั้นผู้ดูแลระบบอาจจะตระหนักได้ว่าระบบตรวจจับผู้บุกรุก ตัวเดียวอาจจะทำให้เขาต้องเข้าไปนอนในคุกหลายคืน เทคนิคการปลอมแอดเดรสลักษณะนี้อาจเป็นการยืมมือ ระบบตรวจจับผู้บุกรุก ของเราไปโจมตีผู้อื่นอีกทอดหนึ่งได้เป็นอย่างดี

- การวิเคราะห์แอดเดรสที่ถูกต้อง และการโจมตีกลับไปก็ตรงไปยังผู้บุกรุก อย่างถูกต้องตามที่ ต้องการ แต่ผลที่ได้ก็อาจจะทำให้ผู้บุกรุก หยุดความพยายามไปชั่วขณะเท่านั้น อีกไม่นานก็หาวิธีกลับมาใหม่ และไม่เกิดผลใดๆ เลยนอกจากจะเป็นการยั่วยุให้มีความรุนแรงมากขึ้นเท่านั้น

สิ่งสำคัญที่ผู้ทำหน้าที่ด้านความปลอดภัยและผู้บริหารระบบ ควรจะตระหนักไว้คือ ท่านไม่มีสิทธิ์พิเศษที่จะไปตอบโต้ผู้บุกรุกโดยการโจมตีกลับไม่ว่าในกรณีใด สิ่งที่ท่านจะทำได้ดีที่สุด คือ ทำระบบให้แข็งแรงมั่นคงและปลอดภัยที่สุดเท่านั้น นั่นคือ ปิดประตูบ้านให้แน่น ตรวจตราอย่างรัดกุมและใช้งานเท่าที่จำเป็น ส่วนผู้ที่กระทำผิดเหล่านั้นควรจะปล่อยให้เป็นไปตามกฎหมายและกระบวนการยุติธรรมจะดีที่สุด เพราะการตอบโต้การกระทำที่ผิดกฎหมายด้วยวิธีที่ผิดกฎหมายจะทำให้เรากลายเป็นจำเลยไปด้วยในที่สุด

3. การเตือนภัยที่ผิดพลาด

ข้อนี้อาจไม่ใช่ข้อเสียที่สำคัญของการใช้ระบบตรวจจับผู้บุกรุก หากผู้ใช้มีความรู้ในการใช้งานที่ดีพอและเข้าใจหลักการวิเคราะห์การบุกรุกของระบบตรวจจับผู้บุกรุก ได้ดี อย่างที่ได้กล่าวแล้วข้างต้น ก็คือ อาจจะมีกิจกรรมปรกติหลายอย่างที่มีลักษณะใกล้เคียงหรือบางครั้งเหมือนกับการพยายามบุกรุก ซึ่งแน่นอนว่าหาก ระบบตรวจจับผู้บุกรุก ได้ถูกกำหนดให้ตรวจจับกิจกรรมประเภทดังกล่าวแล้วก็จะมีการเตือนในทันทีที่ตรวจพบและเป็นหน้าที่ของนักวิเคราะห์ที่จะทำการสืบค้นข้อมูลด้านอื่นๆ มาประกอบการวินิจฉัยอีกครั้งหนึ่งว่าพฤติกรรมดังกล่าวที่ตรวจพบนั้นเป็นการบุกรุกหรือไม่อย่างไรระบบตรวจจับผู้บุกรุก ที่ถูกกำหนดให้มีความไวเป็นพิเศษมักจะสามารถตรวจจับพฤติกรรมที่ก้ำกึ่งนั้นได้มากเป็นพิเศษ ตัวอย่างเช่น ระบบตรวจจับผู้บุกรุก ได้ถูกกำหนดไว้ว่า เมื่อได้รับ ปิง แพ็คเก็ต(Ping Packet) จากแอดเดรสเดิมติดต่อกัน 10 แพ็กเกจภายใน 30 วินาที ให้เตือนว่าเป็นการพยายามโจมตีโดยเทคนิค ปิง ฟลัด เป็นต้น หากเน็ตเวิร์คเป็นเน็ตเวิร์คที่ใช้งานโดยวิศวกรระบบ และมีการทดสอบ ปิง (Ping) บ่อยๆ ก็อาจจะทำให้ระบบตรวจจับผู้บุกรุก เตือนอยู่แทบตลอดเวลา โดยไม่ได้มีการบุกรุกที่แท้จริง

การเตือนโดยมิได้มีการบุกรุกจริงนั้น อาจจะดูเหมือนว่าไม่มีการส่งผลเสียหายประการใดและน่าจะเกิดประโยชน์เสียด้วยซ้ำ เพราะจะทำให้ผู้ดูแลระบบมีความตื่นตัวตลอดเวลา แต่ในความเป็นจริงแล้วธรรมชาติของมนุษย์มีแนวโน้มจะละเลยต่อสิ่งเหล่านี้ หากเตือนแล้วไม่มีการบุกรุกจริงบ่อยครั้งเข้าความน่าเชื่อถือของระบบตรวจจับผู้บุกรุก ก็จะลดลงตามลำดับ และเมื่อมีความพยายามบุกรุกจริงก็จะไม่ได้ให้ความสนใจเท่าที่ควรและไม่ได้หาทางป้องกันอย่างเหมาะสม นั่นคือระบบ

ตรวจจับผู้บุกรุก จะกลายเป็นเด็กเลี้ยงแกะที่เวลาหมาป่าเข้ามาจริงก็ไม่มีผู้ได้รับฟัง ดูเผินๆ อาจจะเหมือนว่ายังดีกว่าการไม่มี ระบบตรวจจับผู้บุกรุกแต่การไม่มีระบบตรวจจับผู้บุกรุกอยู่ในระบบโดยไม่ได้นำมาปรับแต่งอย่างเหมาะสม และเชื่อมั่นว่าระบบตรวจจับผู้บุกรุก สามารถจะคอยระแวดระวังและเก็บหลักฐานต่างๆ ไว้ให้นั้นจะทำให้ผู้บริหารระบบนิ่งนอนใจและคลายความเคร่งครัดในการปฏิบัติงานลง อาจจะถึงขั้นหย่อนยานกว่าการป้องกันในระดับปรกติที่ไม่มีระบบตรวจจับผู้บุกรุกได้ นอกจากนี้การปล่อยให้ระบบตรวจจับผู้บุกรุก มีการเตือนอย่างไม่เหมาะสมจะทำให้เกิดข้อมูลในลักษณะที่เป็นการบุกรุกจริงและการเตือนผิดพลาดผสมกันอยู่อาจจะทำให้การเตือนที่เป็นของจริงถูกกลบไปและยากต่อการสังเกต อย่าลืมว่าผู้บุกรุก ที่มีความสามารถที่จะทิ้งร่องรอยเหล่านี้ถูกนำไปผสมปนเปกับการตรวจจับอื่นๆ อีกนับพัน ย่อมมีโอกาสสูงที่จะถูกมองเลยไปโดยไม่มีผู้ใดให้ความสนใจ

2.1.6 การแจ้งเตือนภัยของระบบตรวจจับผู้บุกรุก

ระบบตรวจจับผู้บุกรุกจะรายงานเฉพาะสิ่งที่กำหนดให้รายงานเท่านั้น มีอยู่สองสิ่งที่ผู้ดูแลระบบจะต้องคอนฟิกให้กับระบบตรวจจับผู้บุกรุกสิ่งแรกคือ ซิกเนเจอร์ของการบุกรุก สิ่งที่สองคือสิ่งที่ผู้ดูแลให้ความสำคัญหรือเหตุการณ์ที่คาดว่าจะเป็นผลไปสู่การบุกรุกในภายหน้า ซึ่งเหตุการณ์ต่างๆเหล่านี้อาจเป็นทราฟิกที่ไม่ปกติหรืออาจเป็นบางข้อความในล็อก การคอนฟิกซิกเนเจอร์ให้กับระบบตรวจจับผู้บุกรุกของแต่ละองค์กรนั้นอาจจะไม่เหมือนกัน ซึ่งจะขึ้นอยู่กับองค์กรนั้นว่าจะให้ความสนใจกับการบุกรุกประเภทใดเมื่อระบบตรวจจับผู้บุกรุกได้ถูกปรับแต่งอย่างถูกต้องแล้ว เหตุการณ์ที่ระบบตรวจจับผู้บุกรุกจะรายงานให้ทราบนั้นสามารถแบ่งออกได้เป็น 3 ประเภท คือ

- การสำรวจเครือข่าย
- การโจมตี
- เหตุการณ์ที่น่าสงสัยหรือผิดปกติ

1. การสำรวจเครือข่าย

เหตุการณ์ที่เป็นการสำรวจเครือข่ายเป็นความพยายามของผู้บุกรุกที่จะรวบรวมข้อมูลเกี่ยวกับระบบเครือข่ายก่อนที่จะโจมตีจริงๆ เช่น

- การสแกน ไอพี(IP Scans) : การสแกน ไอพี เป็นความพยายามของผู้บุกรุกที่ทราบเกี่ยวกับโฮสต์ต่างๆที่อยู่ในเครือข่ายซึ่งระบบที่สแกนนั้น อาจใช้การปิง ช่วงของหมายเลขไอพีของเครือข่ายนั้น
- การสแกน พอร์ต(Port Scans) : หลังจากที่ผู้บุกรุกนั้นได้ข้อมูลเกี่ยวกับว่าเครือข่ายมีโฮสต์ใดอยู่บ้าง ข้อมูลต่อมาที่ผู้บุกรุกต้องการคือ บริการใดบ้างที่แต่ละโฮสต์ให้บริการอยู่ ซึ่งหมายเลขพอร์ตนั้นจะเป็นสิ่งที่บ่งบอกว่ามีแอพพลิเคชันใดอยู่บ้างที่ให้บริการอยู่
- การสแกนโทรจัน(Trojan Scans) : การสแกนโทรจันนั้นเป็นความพยายามของผู้บุกรุกที่จะตรวจเช็คว่ามีพอร์ตของโทรจันใดบ้างที่เปิดอยู่

- การสแกนหาจุดอ่อนของระบบ(Vulnerability Scans) : การสแกนหาจุดอ่อนของระบบเป็นความพยายามที่จะใช้การโจมตีหลายๆแบบกับระบบใดระบบหนึ่งเพื่อตรวจเช็คดูว่าระบบนี้มีจุดอ่อนอย่างไร

2. การโจมตี

การโจมตีเครือข่ายหรือระบบนั้นควรให้ความสำคัญสูงสุด เมื่อระบบตรวจจับผู้บุกรุกรายงานเหตุการณ์นี้ ผู้ดูแลระบบตอบสนองกับเหตุการณ์นี้ทันทีเพื่อป้องกันการสูญเสียมากกว่านี้ บางครั้งระบบตรวจจับผู้บุกรุกอาจแยกแยะระหว่าง การโจมตีจริงๆกับการสแกน หาจุดอ่อน เนื่องจากเหตุการณ์ทั้งสองนั้นระบบตรวจจับผู้บุกรุกจะตรวจพบซิกเนเจอร์ของการโจมตีเหมือนกัน ผู้ดูแลระบบอาจต้องวิเคราะห์ข้อมูลเพิ่มเติม การสแกนหาจุดอ่อนนั้น ระบบตรวจจับผู้บุกรุกจะรายงานการโจมตีหลายๆรูปแบบในช่วงเวลาสั้นๆ กับระบบใดระบบหนึ่ง ส่วนการโจมตีจริงนั้นอาจมีการรายงานการโจมตีแค่รูปแบบเดียวกับระบบใดระบบหนึ่ง

3. เหตุการณ์ที่น่าสงสัยหรือผิดปกติ

เหตุการณ์อื่นๆที่ผิดปกติและไม่ได้จัดอยู่ในประเภทต่างๆที่กล่าวมาข้างต้นถือเป็นเหตุการณ์ที่น่าสงสัยว่าอาจมีการโจมตีเครือข่ายเกิดขึ้น ซึ่งผู้ดูแลระบบต้องวิเคราะห์และสืบหาสาเหตุของเหตุการณ์ที่ว่านี้ต่อ ตัวอย่างเช่น บางโฮสต์อาจส่งแพ็กเก็ตที่มีข้อมูลส่วนหัวผิดไปจากที่กำหนดในมาตรฐาน ซึ่งเหตุการณ์นี้อาจเกิดขึ้นเนื่องจากการโจมตีแบบใหม่ หรือเน็ตเวิร์คการ์ดเครื่องส่งอาจเสีย หรือข้อมูลอาจเกิดผิดพลาดระหว่างการส่งผ่านสายสัญญาณ ระบบตรวจจับผู้บุกรุกจะไม่มีข้อมูลเพียงพอที่จะบอกได้ว่าเหตุการณ์นี้เกิดขึ้นเพราะอะไร แต่จะแจ้งเตือนให้ผู้ดูแลระบบทราบเพื่อค้นหาสาเหตุที่แท้จริงต่อไป

พอร์ตเป็นช่องทางการสื่อสารของ ทีซีพี/ไอพี กับแอพพลิเคชั่น ไม่มีพอร์ตก็ไม่มีช่องทางในการสื่อสารกับผู้อื่น หน้าที่สำคัญของพอร์ตว่าคือการแยกข้อมูลของแต่ละแอพพลิเคชั่นออกจากกันมิให้ผสมปนเป ในการทำงานจริงนั้นข้อมูลที่เข้ามาและออกจากโฮสต์จะมีจำนวนมากและใช้งานเครื่องคอมพิวเตอร์พร้อม ๆ กันโดยหลายวัตถุประสงค์

เนื่องจาก ทีซีพี/ไอพี เป็นโปรโตคอลที่ทำงานในเลเยอร์ที่ค่อนข้างสูง ดังนั้นพอร์ตของ ทีซีพี/ไอพี จึงเป็นลักษณะลอจิคัล คือไม่ได้อาศัยองค์ประกอบทางกายภาพใด ๆ เป็นเพียงข้อมูลขนาด 16 บิตซึ่งอยู่ในไบต์ที่ 0-4 ของ ทีซีพีเฮดเดอร์ และ ยูดีพีเฮดเดอร์ เท่านั้น ต่างจากพอร์ตทั่วไปซึ่งเป็นพอร์ตอีเธอร์เน็ต (Ethernet Port) ซึ่งพอร์ตประเภทนี้จะต้องอาศัยองค์ประกอบทางกายภาพ การเพิ่มหรือลดจะต้องมีการเพิ่มหรือลดลงจริง ๆ จึงจะกระทำได้ และแน่นอนว่าหากเป็นพอร์ตที่ต้องอาศัยองค์ประกอบทางกายภาพจริง ๆ แล้วก็ย่อมจะมีขีดจำกัดทางกายภาพด้วยเช่นเดียวกัน ตัวอย่างเช่น เครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้งานกันอยู่ในปัจจุบันจะมีพอร์ตอนุกรมมาให้ 2 พอร์ต หากใช้เม้าส์แบบอนุกรมก็จะเสียบไป 1 พอร์ต และหากต้องการใช้โมเด็มก็จะเสียไปอีก 1 พอร์ต ดราวนี้

หากต้องการต่ออุปกรณ์อื่น ๆ เพิ่มเติมที่จะต้องใช้พอร์ตอนุกรมเหมือนกันเช่น พลอตเตอร์ ก็จะทำไม่ได้เว้นแต่จะซื้อการ์ดสำหรับเพิ่มพอร์ตอนุกรมมาเพิ่มเติม

การมีพอร์ตก็คือการมีช่องทางในการสื่อสารกับผู้อื่นได้ ดังนั้นถึงแม้ว่าอุปกรณ์ของเราจะมีความสามารถที่ดีอย่างไรก็จะไม่สามารถนำมาใช้งานได้หากไม่มีพอร์ตที่จะใช้ต่อเชื่อมกับอุปกรณ์อื่น หากเราไม่มีพอร์ตที่จะเชื่อมไปยังอุปกรณ์ที่เป็นประเภทเอาท์พุต เช่น เครื่องพิมพ์ พลอตเตอร์ เราก็จะไม่สามารถพิมพ์ผลงานออกมาได้ ในทางกลับกันหากเราไม่มีพอร์ตที่จะเชื่อมต่อกับอุปกรณ์ประเภทอินพุตเราก็จะไม่สามารถรับข้อมูลเข้ามาได้เช่นเดียวกัน และการที่ไม่มีช่องทางในการรับข้อมูลเข้ามาที่เครื่องของเรานับว่าเป็นสิ่งที่ดีในแง่ของความปลอดภัยเพราะตราบใดที่คนอื่นไม่สามารถเข้ามาวุ่นวายกับเครื่องของเราได้มากเท่าไรเครื่องของเราก็จะปลอดภัยมากขึ้นเท่านั้น

2.2 รูปแบบการโจมตี

2.2.1 การสแกนพอร์ต

พอร์ตเป็นช่องทางการสื่อสารของ ทีซีพี/ไอพี กับแอพพลิเคชั่น ไม่มีพอร์ตก็ไม่มีช่องทางในการสื่อสารกับผู้อื่น หน้าที่สำคัญของพอร์ตว่าคือการแยกข้อมูลของแต่ละแอพพลิเคชั่นออกจากกันมีให้ผสมปนเป ในการทำงานจริงนั้นข้อมูลที่เข้ามาและออกจากโฮสต์จะมีจำนวนมากและใช้งานเครื่องคอมพิวเตอร์พร้อม ๆ กันโดยหลายวัตถุประสงค์

เนื่องจาก ทีซีพี/ไอพี เป็นโปรโตคอลที่ทำงานในเลเยอร์ที่ค่อนข้างสูง ดังนั้นพอร์ตของ ทีซีพี/ไอพี จึงเป็นลักษณะลอจิคัล คือไม่ได้อาศัยองค์ประกอบทางกายภาพใด ๆ เป็นเพียงข้อมูลขนาด 16 บิตซึ่งอยู่ในไบต์ที่ 0-4 ของ ทีซีพีเฮดเดอร์ และ ยูดีพีเฮดเดอร์ เท่านั้น ต่างจากพอร์ตทั่วไปซึ่งเป็นพอร์ตอีเธอร์เน็ต (Ethernet Port) ซึ่งพอร์ตประเภทนี้จะต้องอาศัยองค์ประกอบทางกายภาพ การเพิ่มหรือลดจะต้องมีการเพิ่มหรือลดลงจริง ๆ จึงจะกระทำได้ และแน่นอนว่าหากเป็นพอร์ตที่ต้องอาศัยองค์ประกอบทางกายภาพจริง ๆ แล้วก็ย่อมจะมีขีดจำกัดทางกายภาพด้วยเช่นเดียวกัน ตัวอย่างเช่น เครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้งานกันอยู่ในปัจจุบันจะมีพอร์ตอนุกรมมาให้ 2 พอร์ต หากใช้เม้าส์แบบอนุกรมก็จะเสียบไป 1 พอร์ต และหากต้องการใช้โมเด็มก็จะเสียไปอีก 1 พอร์ต ดราวนี้หากต้องการต่ออุปกรณ์อื่น ๆ เพิ่มเติมที่จะต้องใช้พอร์ตอนุกรมเหมือนกันเช่น พลอตเตอร์ ก็จะทำไม่ได้เว้นแต่จะซื้อการ์ดสำหรับเพิ่มพอร์ตอนุกรมมาเพิ่มเติม

การมีพอร์ตก็คือการมีช่องทางในการสื่อสารกับผู้อื่นได้ ดังนั้นถึงแม้ว่าอุปกรณ์ของเราจะมีความสามารถที่ดีอย่างไรก็จะไม่สามารถนำมาใช้งานได้หากไม่มีพอร์ตที่จะใช้ต่อเชื่อมกับอุปกรณ์อื่น หากเราไม่มีพอร์ตที่จะเชื่อมไปยังอุปกรณ์ที่เป็นประเภทเอาท์พุต เช่น เครื่องพิมพ์ พลอตเตอร์ เราก็จะไม่สามารถพิมพ์ผลงานออกมาได้ ในทางกลับกันหากเราไม่มีพอร์ตที่จะเชื่อมต่อกับอุปกรณ์ประเภทอินพุตเราก็จะไม่สามารถรับข้อมูลเข้ามาได้เช่นเดียวกัน และการที่ไม่มีช่องทางในการรับข้อมูลเข้ามาที่เครื่องของเรานับว่าเป็นสิ่งที่ดีในแง่ของความปลอดภัยเพราะตราบใดที่คนอื่นไม่สามารถเข้ามาวุ่นวายกับเครื่องของเราได้มากเท่าไรเครื่องของเราก็จะปลอดภัยมากขึ้นเท่านั้น

พอร์ตของ ทีซีพี/ไอพี

พอร์ตของ ทีซีพี/ไอพี (หมายถึงทั้ง พอร์ต ทีซีพี และ พอร์ต ยูดีพี) จะทำหน้าที่คล้ายคลึงกับตัวอย่างที่ยกมาข้างต้นแต่เป็นไปสำหรับหรับแอพพลิเคชั่นที่ใช้ ทีซีพี/ไอพี เท่านั้นจึงจะสามารถสื่อสารผ่านพอร์ตกันได้เข้าใจ พอร์ตของ ทีซีพี และ ยูดีพี จะมีได้ทั้งสิ้นอย่างละ 65534 พอร์ต ดังนั้นหากเครื่องของเราใช้โปรโตคอลนี้ก็จะมีช่องทางสื่อสารกับผู้อื่นได้ถึง 131,068 พอร์ต ถ้าหากพอร์ตเหล่านี้มองเห็นได้ด้วยตาเปล่าเราจะต้องทึ่งที่เครื่องคอมพิวเตอร์เล็กนิดเดียวสามารถมีช่องทางการสื่อสารได้มากมายมหาศาลขนาดนี้

โดยทั่วไปพอร์ตจะมีอยู่ 2 สถานะคือเปิดและปิด พอร์ตเปิดหมายถึงการมีแอพพลิเคชั่นใด ๆ ใช้งานพอร์ตนั้นและเปิดรับการสื่อสารที่พอร์ตดังกล่าว หากมีการพยายามติดต่อมายังพอร์ตที่เปิดไว้ก็จะมีการตอบรับและดำเนินการสื่อสารกันต่อไป พอร์ตที่ปิดหมายถึงการไม่มีแอพพลิเคชั่นใดใช้งานพอร์ตนั้นและคอยที่จะตอบรับการสื่อสาร ดังนั้นหากมีความพยายามติดต่อมายังพอร์ตที่ปิดอยู่ก็จะถูกปฏิเสธทันทีตามที่กำหนดไว้ในโปรโตคอล ไม่ว่าจะเป็น ทีซีพี หรือ ยูดีพี การที่จะเริ่มการสื่อสารใด ๆ นั้นจะต้องมีฝ่ายใดฝ่ายหนึ่งเปิดพอร์ตรอไว้ก่อนเรียกว่าเป็นเซิร์ฟเวอร์ (server) และพอร์ตที่เปิดก็จะเรียกว่าเซิร์ฟเวอร์พอร์ต (server port) และอีกฝ่ายหนึ่งจะต้องส่งสัญญาณมาขอติดต่อด้วยเรียกว่าไคลเอนต์ (client) พร้อมทั้งเปิดพอร์ตของตนเองไว้เพื่อรอรับการติดต่อกลับจากเซิร์ฟเวอร์เรียกว่าไคลเอนต์พอร์ต (client port) หากไม่มีการเปิดเซิร์ฟเวอร์พอร์ตรอไว้ การสื่อสารใด ๆ ของ ทีซีพี/ไอพี ก็จะไม่สามารถเริ่มต้นได้ ถ้าจะเปรียบเทียบกลับไปยังตัวอย่างข้างต้นหากเราทำการซื้อหาพลอตเตอร์มาเรียบร้อยเพื่อจะใช้งานแต่ไม่มีพอร์ตอนุกรมที่เครื่องคอมพิวเตอร์ เราก็จะต้องไปซื้อฮาร์ดแวร์มาเพื่อเพิ่มพอร์ตของเราเสียก่อนจึงจะเริ่มต้นใช้งานได้

การเปิดพอร์ต

โดยตัวพอร์ตเองแล้วไม่สามารถเปิดปิดได้เองตามชอบใจ จะเห็นว่าเวลาใช้งานอุปกรณ์ที่เป็น ทีซีพี/ไอพี นั้นเราจะสามารถกำหนดได้เพียงส่วนที่อยู่ในระดับ ไอพี คือ หมายเลข ไอพี(IP Address),ซับเน็ต มาสก์(Subnet Mask) และเกทเวย์(Gateway) เท่านั้น จะไม่สามารถกำหนดได้ว่าจะเปิดพอร์ตใดบ้าง การที่พอร์ตใดจะเปิดให้บริการเป็นเซิร์ฟเวอร์พอร์ตนั้นจะต้องมีแอพพลิเคชั่นทำงานอยู่บนพอร์ตนั้นเสมอ หมายถึงจะต้องมีโปรแกรมที่รับหน้าที่โต้ตอบและจัดการการสื่อสารที่มายังพอร์ตนั้น จึงอาจจะเปรียบได้ว่าพอร์ตก็คือแอพพลิเคชั่น การที่มีพอร์ตเปิดอยู่ก็หมายถึงการมีแอพพลิเคชั่นทำงานอยู่นั่นเอง

ทีซีพี/ไอพี จะมีแอพพลิเคชั่นมาตรฐานที่ใช้งานมาตั้งแต่ยุคต้นของ ทีซีพี/ไอพี แอพพลิเคชั่นเหล่านี้ได้ทำการจับจองพอร์ตหมายเลขต่าง ๆ ไว้กันแต่เนิ่น ๆ เช่น เอฟทีพี(FTP), เอสเอ็มทีพี(SMTP) ,เอชทีทีพี(HTTP) ,พ็อพ(POP) ,เทลเน็ท(TELNET) และเพื่อให้เป็นมาตรฐานสำหรับไคลเอนต์จะได้ติดต่อถูกพอร์ต แอพพลิเคชั่นเหล่านี้ก็จะทำการยึดพอร์ตหมายเลขเหล่านั้น

เป็นการถาวร และเป็นที่รู้กันว่าหากระบุหมายเลขพอร์ตเหล่านั้นก็จะหมายถึงแอพพลิเคชั่นนั้นนั่นเองเช่น หากพูดถึงพอร์ต 80 ก็จะหมายถึงเว็บเซิร์ฟเวอร์ เป็นต้น

อย่างไรก็ตามความสัมพันธ์ระหว่างพอร์ตและแอพพลิเคชั่นเป็นความสัมพันธ์กันอย่างหลวม ๆ คือเป็นไปตามความสมัครใจมิได้มีการบังคับว่าพอร์ตอะไรต้องใช้กับแอพพลิเคชั่นอะไรเป็นการเฉพาะเจาะจง หรือหากแอพพลิเคชั่นไม่ใช้พอร์ตนั้นแล้วจะทำงานไม่ได้ จริง ๆ แล้วโดยส่วนใหญ่แอพพลิเคชั่นสามารถปรับเปลี่ยนให้เลือกใช้พอร์ตใด ๆ ให้เป็นเซิร์ฟเวอร์พอร์ตก็ได้ เช่น หากเราไม่ต้องการใช้พอร์ต 80 ก็อาจจะเปลี่ยนให้ไปเซิร์ฟเวอร์พอร์ตของเว็บเซิร์ฟเวอร์ไปทำงานที่พอร์ต 800 ก็ได้ แต่นั่นหมายถึงจะต้องไปเปลี่ยนที่เว็บเบราท์เซอร์บนทุกเครื่องให้มาเรียกใช้เว็บเซิร์ฟเวอร์ที่พอร์ต 800 ด้วยจึงจะใช้งานได้ โดยทั่วไปเพื่อไม่ให้เกิดความสับสนและตัดภาระที่จะต้องคอยปรับเปลี่ยนพอร์ตที่ไคลเอนต์ การเปิดให้บริการแอพพลิเคชั่นมาตรฐานจึงมักใช้พอร์ตตามมาตรฐานไปด้วย

ในขณะใดขณะหนึ่งอุปกรณ์ ทีซีพี/ไอพี จะสามารถใช้พอร์ตใดพอร์ตหนึ่งเป็นเซิร์ฟเวอร์พอร์ตสำหรับแอพพลิเคชั่นได้เพียงแอพพลิเคชั่นเดียวเท่านั้น เช่น หากใช้พอร์ต 800 เป็นเว็บเซิร์ฟเวอร์แล้ว ก็จะไม่สามารถใช้พอร์ต 800 เพื่อเป็นเซิร์ฟเวอร์ เอฟทีพี ได้จนกว่าจะหยุดการทำงานของเว็บเซิร์ฟเวอร์เสียก่อน เป็นต้น

หลังจาก ทีซีพี/ไอพี ได้รับความนิยมก็มีผู้พัฒนาแอพพลิเคชั่นต่าง ๆ ที่ทำงานอยู่บน TCP/IP ออกมาอย่างมากมาย และเลือกใช้พอร์ตที่เหลืออยู่มาเป็นเซิร์ฟเวอร์พอร์ตต่าง ๆ ซึ่งจะเป็นที่รู้กันเฉพาะผู้ใช้แอพพลิเคชั่นนั้น ๆ และมิได้เป็นมาตรฐานอีกต่อไป โดยส่วนใหญ่แต่ละแอพพลิเคชั่นจะมีการระบุไว้ในข้อมูลทางเทคนิคว่าจะใช้พอร์ตใดเป็นดีฟอลต์ คุณอาจจะเคยได้ยินคำถามจากผู้ใช้ว่าแอพพลิเคชั่นคุยกันที่พอร์ตไหน นั่นหมายถึงแอพพลิเคชั่นใช้พอร์ตใดเป็นเซิร์ฟเวอร์พอร์ตนั่นเอง

นอกจากแอพพลิเคชั่นเปิดพอร์ตเพื่อใช้งานแล้ว ระบบปฏิบัติการที่อาศัย ทีซีพี/ไอพี ก็จะต้องเปิดพอร์ตเพื่อใช้ในกิจการของระบบปฏิบัติการด้วยเช่นกัน โดยที่ผู้ใช้ไม่รู้ตัว เพราะเป็นการใช้งานภายในของระบบปฏิบัติการและผู้ผลิตคิดว่าผู้ใช้ไม่จำเป็นต้องรู้ หลายครั้งที่ระบบปฏิบัติการมีความหละหลวมจึงทำให้ผู้ใช้ถูกบุกรุกจากพอร์ตเหล่านั้นด้วย ซึ่งเมื่อเริ่มใช้แอพพลิเคชั่นมากโปรแกรมขึ้นเครื่องคอมพิวเตอร์ของเราก็จะเริ่มเปิดพอร์ตมากขึ้น ซึ่งเป็นการเปิดช่องทางให้ผู้อื่นติดต่อเข้ามาได้มากขึ้นตามไปด้วย จากนั้นความเสี่ยงก็เริ่มมากขึ้นนับแต่นั้นเป็นต้นมา

ในตารางที่ 2.1 จะแสดงให้เห็นพอร์ตมาตรฐานของ ทีซีพี สำหรับแอพพลิเคชั่นที่ใช้งานกันอยู่ในปัจจุบัน และตารางที่ 2.2 สำหรับพอร์ตมาตรฐานของ ยูดีพี

Port Number	Services

Port Number	Services
1	Tcpmux
7	Echo
13	Time
17	Qotd(Quote of the day)
19	Chargen
21	Ftp
22	Ssh(Secure Shell)
23	Telnet
43	Whois
53	DNS(Domain Name Server)
70	Gopher
79	Finger
80	Http
87	Link
95	Supdup
109-110	POP
111	Portmap
135	Epmap
139	NetBIOS
143	IMAP
144	News Windows Sys
443	HttpS(Secure Web Server)
512	Remote Exec
513	Remote Login
514	Remote Shell
515	Priter
540	UUCP
749-751	Kerberos
1080	Socks
5632	PC Anywhere

ตารางที่ 2.1 พอร์ตมาตรฐานของ ทีซีพี สำหรับแอพพลิเคชั่นที่ใช้งานกันอยู่ในปัจจุบัน

Port Number	Services
7	Echo
13	Time
17	Qotd(Quote of the day)
19	Chargen
53	DNS
67-68	BootP
69	TFTP
88	Kerberos
111	Portmap
137-138	NetBIOS
161-162	SNMP
177	X11 logins
513	Who
514	Syslog
517	Talk
518	Ntalk
2049	NFS
5631	PC Anywhere

ตารางที่ 2.2 พอร์ตมาตรฐานของ ยูดีพี สำหรับแอพพลิเคชั่นที่ใช้งานกันอยู่ในปัจจุบัน

การปิดพอร์ต

การปิดพอร์ตก็คือการไม่ยอมรับการติดต่อมายังพอร์ตนั้น ๆ เช่นเดียวกันกับการเปิดพอร์ต เราไม่สามารถปิดพอร์ตนั้นโดยตรงได้ด้วยโฮสต์ทั่วไป (สามารถทำได้บน ไฟร์วอลล์(Firewall), เราเตอร์ หรืออุปกรณ์ สวิตช์ เลเยอร์ 3(Layer 3 Switch) แต่ความสามารถจะมากน้อยแตกต่างกัน) เพราะพอร์ตจะเปิดได้ก็ต่อเมื่อมีแอพพลิเคชั่นทำงานอยู่ ดังนั้นหากจะปิดพอร์ตก็จะต้องทำการหยุดการทำงานของแอพพลิเคชั่นก่อนแล้วพอร์ตก็จะถูกปิดไปเอง

สำหรับในมุมมองด้านความปลอดภัยแล้วการปิดพอร์ตเป็นการป้องกันตัวเองขั้นพื้นฐานอย่างน้อยที่สุดก็จะเป็นการลดความเสี่ยงของการที่จะถูกบุกรุก ยิ่งเปิดพอร์ตน้อยเท่าไหร่ก็จะยิ่งปลอดภัยเท่านั้น เปรียบเสมือนบ้านของเราที่บังเอิญมีหน้าต่างมากถึง 131,068 บาน แต่หากเราปิดประตูลงกลอนให้แน่นหนาทุกบานขโมยย่อมจะเข้ามาได้ยาก เลือกเปิดหน้าต่างเฉพาะที่จำเป็นจะได้จัดเวรยามเฝ้าดูได้ หากเปิดหน้าต่างทิ้งไว้มาก ทั้งที่ตั้งใจและไม่ตั้งใจก็ย่อมจะทำให้การรักษาความปลอดภัยเป็นไปได้ยากขึ้นเท่านั้น

หากพิจารณากันผิวเผินและการปิดพอร์ตไม่น่าจะเป็นเรื่องยาก ส่วนใหญ่ที่มีปัญหาเกิดขึ้นก็เนื่องมาจากพอร์ตไม่ได้ปิดนั่นเอง มีสาเหตุหลายประการที่ทำให้พอร์ตต่าง ๆ ถูกเปิดทิ้งไว้ ดังนี้

พอร์ตที่เปิดไว้โดยไม่ตั้งใจ

ดังที่กล่าวไว้ข้างต้นว่าการเปิดพอร์ตเป็นการเปิดแบบลอจิคัลและมองไม่เห็น ดังนั้นหากไม่ทำการตรวจสอบโฮสต์ของเราให้ดีก็จะไม่ทราบว่ามีพอร์ตใดเปิดอยู่ — จะพบได้ค่อนข้างมากในอินเตอร์เน็ตที่เว็บเซิร์ฟเวอร์ซึ่งควรจะมีหน้าที่ให้บริการสำหรับ เอชทีทีพี บนพอร์ต 80 เพียงอย่างเดียวแต่กลับมีพอร์ตอื่น ๆ เปิดร่วมอยู่ด้วยเป็นจำนวนมาก จากประสบการณ์ที่ผ่านมากพบว่าเหตุที่มักจะมีแอพพลิเคชั่นอื่น ๆ มาเปิดพอร์ตบนโฮสต์ของเราโดยที่เราไม่เคยติดตั้งเข้าไปด้วยเลยก็เนื่องมาจากการแถมมากับระบบปฏิบัติการนั่นเอง ระบบปฏิบัติการระยะหลังเกือบทุกค่ายมักเอาใจผู้ใช้โดยการทั้งแจกทั้งแถมแอพพลิเคชั่นที่คาดว่าลูกค้าจะใช้เมื่อติดตั้งระบบปฏิบัติการ หากไม่ทำการตรวจสอบอย่างละเอียด โดยทำเพียงแค่ตกลงตามค่าดีฟอลต์ที่ให้มา ระบบปฏิบัติการก็จะชวนสมัครพรรคพวกแอพพลิเคชั่นต่าง ๆ มาเปิดพอร์ตบนเครื่องของเราอย่างสนุกสนาน จึงพบเห็นได้ไม่ยากที่ติดตั้งเว็บเซิร์ฟเวอร์แล้วจะได้แถม เอฟทีพี(FTP), เอสเอ็มทีพี(SMTP) ,เอชทีทีพี(HTTP) , พ็อพ(POP) ,เทลเน็ท(TELNET) และอื่น ๆ มาครบชุด กว่าจะรู้ว่าพอร์ตเหล่านี้เปิดทิ้งไว้ก็ตอนที่เซิร์ฟเวอร์ถูกเจาะพรุนเสียแล้ว

อย่างไรก็ตามข้อผิดพลาดเช่นนี้แก้ไขไม่ยากนัก เพียงตรวจสอบว่ามีแอพพลิเคชั่นใดบ้างที่ทำงานอยู่โดยที่เราไม่ต้องการจากนั้นก็หยุดการทำงานของแอพพลิเคชั่นนั้นเสียพอร์ตก็จะถูกปิดไปเอง จุดสำคัญอยู่ที่ให้รู้จักดูแลแอพพลิเคชั่นบนเครื่องเราและเริ่มตระหนักว่าการเปิดพอร์ตใด ๆ เป็นสิ่งที่ต้องกระทำไปด้วยความระมัดระวังที่สุด

พอร์ตของระบบปฏิบัติการ

พอร์ตประเภทนี้จะต่างกับประเภทแรกที่เป็นพอร์ตของแถมซึ่งจะปิดทิ้งเสียก็ได้ แต่พอร์ตเหล่านี้อาจจำเป็นสำหรับระบบปฏิบัติการนั้น ๆ หากไม่เปิดพอร์ตเหล่านี้ระบบปฏิบัติการก็จะไม่สามารถทำงานได้อย่างสมบูรณ์ ตัวอย่างเช่น ในวินโดว์ เอ็นที (Microsoft Windows NT) จะต้องใช้

พอร์ตหมายเลข 135-139 ของ ทีซีพี ในการทำงาน พอร์ตประเภทนี้จะไม่สามารถปิดลงได้เนื่องจากแอพพลิเคชั่นที่ใช้งานพอร์ตนั้นเป็นส่วนหนึ่งของระบบปฏิบัติการเสียเอง

พอร์ตประเภทนี้นอกจากจะปิดไม่ได้แล้วยังเป็นสัญญาณอย่างดีในการบอกกล่าวต่อผู้อื่น (รวมทั้งผู้ไม่ประสงค์ดีด้วย) ว่าโฮสต์ของเราที่กำลังให้บริการอยู่นั้นเป็นระบบปฏิบัติการอะไร หากกำลังคิดจะบุกรุกเข้ามาก็ควรจะเลือกเครื่องมือให้ถูกต้องจะได้ไม่เสียเวลามาก

พอร์ตที่เปิดแบบสุ่ม

ถึงแม้ว่าเซิร์ฟเวอร์พอร์ตโดยส่วนใหญ่จะต้องมีหมายเลขพอร์ตที่แน่นอนเพื่อให้สามารถรอรับการติดต่อจากไคลเอนต์ได้ตลอดเวลา แต่จะมีแอพพลิเคชั่นบางประเภทที่มีการใช้งานพอร์ตมากกว่า 1 พอร์ต โดยมีหมายเลขพอร์ตที่คงที่อยู่ที่เป็นหลักไว้ 1 พอร์ต และอาจจะใช้พอร์ตอื่นซึ่งเป็นแบบสุ่มในการทำงานประกอบกัน หรือบางกรณีก็อาจจะสลับกันเป็นเซิร์ฟเวอร์และไคลเอนต์ (ในมุมมองของ ทีซีพี/ไอพี) ชั่วคราวและเมื่อการทำงานเสร็จสิ้นก็จะปิดพอร์ตไปเอง เช่น เอฟทีพี, ไคลเอนต์ ของ ออราเคิล(Oracle Client) เป็นต้น โดยทั่วไปพอร์ตที่เปิดเป็นการชั่วคราวนี้จะมีการตกลงกันระหว่างไคล์เอนต์และเซิร์ฟเวอร์ เพื่อทำงานนัดแนะหมายเลขพอร์ตที่เปิดขึ้นใหม่แล้วทั้งคู่ก็จะเปลี่ยนไปสื่อสารกันที่พอร์ตนั้น ๆ

การเปิดพอร์ตประเภทนี้จะสร้างปัญหาให้แก่ผู้ดูแลระบบคือ

- พอร์ตที่เปิดไว้เป็นการชั่วคราวควรจะปิดเมื่อการใช้งานเสร็จสิ้นลง แต่หากแอพพลิเคชั่นทำงานผิดพลาดหรือหยุดทำงานลงกลางคัน (Abnormal termination) พอร์ตก็อาจจะถูกเปิดค้างทิ้งไว้
- การไม่มีหมายเลขพอร์ตที่แน่นอนจะทำให้ควบคุมและตรวจสอบได้ยาก หากพอร์ตที่ใช้บังเอิญไปตรงกับพอร์ตที่อันตรายซึ่งใช้โดยโปรแกรมประกอบโทรจัน เมื่อมีโปรแกรมโทรจันทำงานอยู่จริงก็จะทำให้ไม่ได้รับความสนใจเพราะจะคิดว่าเป็นพอร์ตของแอพพลิเคชั่นปกติ
- หากมีการนำไฟร์วอลล์มาใช้งาน และจะต้องกำหนดกฎสำหรับไฟร์วอลล์แล้วจะทำได้ยาก เพราะกฎของไฟร์วอลล์จะตั้งอยู่บนพื้นฐานของการใช้พอร์ตเป็นหลัก หากมีพอร์ตไม่แน่นอนก็จะทำให้ไม่สามารถกำหนดกฎได้อย่างรัดกุม

สิ่งที่ต้องระมัดระวังเสมอในการพยายามปิดพอร์ตที่คิดว่าไม่จำเป็นก็คือ ถ้าเกิดพอร์ตนั้นจำเป็นต้องใช้และมีความเกี่ยวพันกับแอพพลิเคชั่น การปิดพอร์ตอาจจะส่งผลกระทบทำให้แอพพลิเคชั่นทำงานไม่ได้หรือทำงานได้ไม่สมบูรณ์ ถึงแม้ว่าบางพอร์ตอาจจะมีความเสี่ยงต่อความปลอดภัยแต่หากจำเป็นต้องเปิดไว้เพื่อให้ระบบยังคงให้บริการได้ก็จำเป็นต้องยอมรับความเสี่ยงเหล่านั้น อย่าลืมว่าวัตถุประสงค์หลักของระบบใด ๆ ก็คือการให้บริการ สิ่งที่จะต้องทำคือเพิ่ม

ความสามารถในการให้บริการได้อย่างปลอดภัย การทำให้ปลอดภัยมากขึ้นแต่ระบบให้บริการไม่ได้ย่อมไม่ก่อให้เกิดประโยชน์อันใด

เมื่อพอร์ตเป็นสิ่งสำคัญการสแกนพอร์ตก็ถือเป็นขั้นตอนที่สำคัญด้วยเช่นเดียวกัน สิ่งที่ทำให้การสแกนพอร์ตเป็นการกระทำที่ถือได้ว่ามุ่งร้ายระบบคือ ผลลัพธ์ของการสแกนพอร์ตจะทำให้แฮกเกอร์สามารถล่วงรู้ได้ว่ามีแอพพลิเคชันใดบ้างที่ทำวานอยู่บนโฮสต์ โดยปกติทั่วไปแล้วแอพพลิเคชั่นแต่ละชนิดที่เปิดให้บริการอยู่ก็สามารถนำข้อมูลที่ได้มาเทียบกับบริการมารตรฐาน ก็จะทราบได้ว่ามีแอพพลิเคชั่นใดที่เปิดให้บริการอยู่ และข้อมูลเหล่านี้ก็จะเป็นประโยชน์ต่อการเลือกเทคนิคการโจมตีต่อไป

2.2.2โทรจัน

ม้าโทรจัน (Trojan Horse)

โปรแกรมประเภทโทรจันเป็นโปรแกรมที่แอบแฝงมาในคราบของโปรแกรมปกติธรรมดาที่ใช้งานอยู่ทั่วไป แต่เบื้องหลังนอกจากจะทำหน้าที่โปรแกรมนั้นควรทำแล้วโปรแกรมประเภทนี้ยังทำหน้าที่อื่นแอบแฝงโดยที่เราไม่รู้ตัว ซึ่งแน่นอนว่าสิ่งเหล่านั้นย่อมเป็นสิ่งที่เราไม่พึงประสงค์จะให้ทำเป็นแน่ เช่น ดักจับรหัสผ่าน, เก็บข้อมูลการกดแป้นพิมพ์ เป็นต้น รวมไปถึงที่เกี่ยวข้องกับพอร์ตคือ เมื่อถึงเวลาที่กำหนดไว้โทรจันเหล่านี้ก็จะอาศัยพอร์ตใดพอร์ตหนึ่งในการแอบส่งข้อมูลออกไปยังจุดหมายปลายทางที่ใดที่หนึ่งในอินเตอร์เน็ต

แบ็คออริฟิช (Back Orifice) หรือแบ็คดอร์ (Backdoor)

โปรแกรมประเภทนี้มีหน้าที่ชัดเจนคือ เมื่อมันทำงานอยู่บนเครื่องใดแล้วมันจะแอบเปิดพอร์ตให้ไคลเอนต์จากภายนอกสามารถเข้ามาควบคุมเครื่องได้ในระดับต่าง ๆ หรือบางครั้งอาจสามารถเข้ามาใช้เสมือนผู้มีสิทธิ์ในระบบสูงสุด โดยไม่ต้องผ่านการตรวจสอบรหัสผ่านและการรักษาความปลอดภัยของระบบปฏิบัติการตามปกติ เปรียบเสมือนเราปิดหน้าต่างประตูไว้เรียบร้อยทุกบานแต่มีคนรับใช้ที่เป็นพวกเดียวกับขโมยทำงานอยู่ในบ้าน และแอบถอดกลอนประตูทิ้งไว้ทำให้ขโมยพวกเดียวกันแอบเข้ามาในบ้านตอนกลางคืน

โปรแกรมทั้ง 2 ประเภทนี้มีอันตรายสูงมากสำหรับทุก ๆ ระบบ เพราะเป็นการโจมตีจากภายในออกมาหาภายนอก กล่าวคือโดยปกติแล้วผู้ดูแลระบบจะทำให้การป้องกันการโจมตีหรือการบุกรุกจากภายนอกที่พยายามเข้ามาภายใน แต่สำหรับการโจมตีโดยอาศัยโทรจันหรือแบ็คออริฟิชเป็นเครื่องมือนั้น จะอาศัยความบกพร่องของการดูแลเครื่องภายในที่อาจไม่ระแวดระวังในการนำโปรแกรมต่าง ๆ มาติดตั้งในเครื่อง เมื่อโปรแกรมเหล่านี้สามารถแฝงตัวเข้ามาทำงานบนโฮสต์แล้ว

มันจะทำการเปิดพอร์ตเชื้อเชิญให้ผู้บุกรุกทั้งหลาย หลบหลีกระบบรักษาความปลอดภัยเข้ามาภายในได้เป็นอย่างดี และเป็นช่องทางในการบุกรุกไปยังที่อื่นต่อไป

โปรแกรมเหล่านี้อาจจะถูกเขียนโดยผู้ที่ฝักใฝ่ในการบุกรุกเครือข่ายที่มีอยู่ทั่วไป เมื่อทดลองใช้แล้วได้ผลดีก็นำออกมาเผยแพร่ให้ผู้อื่นนำไปใช้งาน คนอื่นที่สนใจเมื่อพบก็นำไปใช้ในการบุกรุกต่อปัจจุบันมีโปรแกรมประเภทนี้จำนวนมากเผยแพร่อยู่บนอินเตอร์เน็ต ทำให้ความเสี่ยงต่อการถูกบุกรุกจากวิธีนี้ยิ่งทวีความรุนแรงมากยิ่งขึ้น

อย่างไรก็ตามโปรแกรมประเภทเหล่านี้อาจตบตาไม่ให้ผู้ใช้รู้ตัวได้แต่ไม่สามารถหลบหลีกการตรวจจับได้ หากผู้ดูแลเน็ตเวิร์กมีความเข้าใจและมีความตั้งใจในการที่จะตรวจสอบการใช้เน็ตเวิร์กมากเพียงพอ ถึงแม้โปรแกรมประเภทนี้จะเขียนไว้ลึกลับซับซ้อนอย่างไรก็คงต้องอาศัยการรับส่งข้อมูลผ่าน ทีซีพี/ไอพี อยู่ดี และแน่นอนว่าจะต้องปฏิบัติตามโปรโตคอล เช่นเดียวกับแอพพลิเคชั่นทั่ว ๆ ไป สิ่งที่จะเป็นจุดสังเกตและตรวจจับได้เมื่อมีโปรแกรมประเภทนี้ทำงานก็คือพอร์ตที่มันใช้นั่นเอง

แอพพลิเคชั่นใด ๆ ที่ใช้งานอยู่บน ทีซีพี/ไอพี จะต้องใช้พอร์ตเป็นของตนเองไม่เว้นแม้แต่โทรจันและแบ็คออริฟิช โปรแกรมประเภทนี้ส่วนใหญ่จะใช้พอร์ตที่มีหมายเลขแน่นอนในการสื่อสารข้อมูลระหว่างตัวเองกับไคลเอนต์ เช่น เน็ตบัส(Netbus) พอร์ต12345,ซับเซเวน (Subseven) พอร์ต(1999) ซึ่งเมื่อมีการตรวจสอบพบว่าโปรแกรมเหล่านี้ใช้พอร์ตหมายเลขใด หมายเลขพอร์ตเหล่านั้นก็จะถูกเผยแพร่เพื่อให้ผู้ดูแลระบบระมัดระวังการสื่อสารที่จะเกิดขึ้นบนพอร์ตเหล่านี้เป็นพิเศษ และถือเป็นพอร์ตต้องห้ามที่ไม่ควรใช้งาน ตัวอย่างหมายเลขพอร์ตและโปรแกรมโทรจันที่ใช้งานพอร์ตเหล่านี้แสดงไว้ที่ภาคผนวก

แต่ก็มีบางพอร์ทใช้พอร์ทร่วมกับแอพพลิเคชั่นปกติ เพื่อให้เป็นการยากที่จะตรวจจับ เช่น พอร์ต21 ซึ่งโดยปกติเป็นบริการของเอฟทีพี แต่ก็มีโทรจันร่วมใช้ด้วยเช่น แบล็คคอนสตรัคชัน, เบลดรันเนอร์ ,โดลีโทรจัน,วินแครช ฯลฯ หรือโทรจันบางประเภทที่สามารถสุ่มเปิดพอร์ทขึ้นมาในแต่ละครั้งที่มันรัน เช่นในเวอร์ชันหลังๆของโทรจัน ซับเซเวน โดยในการตรวจจับก็จะยากขึ้นโดยต้องลงไปดูในส่วนของลักษณะพิเศษของมัน(Signature) ว่ามีลักษณะอย่างไร ในขณะที่โทรจันประเภทอื่นที่ใช้พอร์ทประจำจะสามารถตรวจจับได้อย่างง่ายๆจากพอร์ทที่มันใช้

2.2.3เวิร์ม

เวิร์มเป็นโปรแกรมคอมพิวเตอร์ เช่นเดียวกับโปรแกรมไวรัส แต่แพร่กระจายผ่านเครือข่ายไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ที่ต่ออยู่บนเครือข่ายด้วยกัน ลักษณะการแพร่กระจายคล้ายตัวหนอนที่เจาะไชไปยังเครื่องคอมพิวเตอร์ต่าง ๆ แพร่พันธุ์ด้วยการคัดลอก

ตัวเองออกเป็นหลาย ๆ โปรแกรม และส่งต่อผ่านเครือข่ายออกไป มีผลทำให้เครื่องทำงานผิดปกติ หรือใช้งานไม่ได้ ไปจนถึงทำให้ทราฟฟิค(Traffic) ในเครือข่ายท่วมจนใช้การไม่ได้

2.2.4 การโจมตีแบบ บรูซฟอร์ซ(Brute force Attack)

การโจมตีแบบบรูซฟอร์ซ คือการพยายามล็อกอินเข้าไปในระบบโดยใช้ วิธีเดา พาสเวิร์ด หรือลองสุ่ม ล็อกอินเข้าไปหลายๆครั้งจนกว่าจะล็อกอินเข้าไปได้ โดยอาจจะมีตัวช่วยคือคำในดิคชันนารี หรือคำศัพท์ต่างๆที่น่าจะเป็นพาสเวิร์ด

2.2.5 ความบกพร่องของแอพพลิเคชั่น

นอกจากการอาศัยโปรแกรมประเภทม้าโทรจันหรือแบ็คออริฟิชซึ่งออกแบบมาเพื่อต้อนรับแฮกเกอร์โดยเฉพาะแล้ว แอพพลิเคชั่นทั่วๆ ไปก็เป็นช่องทางที่สามารถใช้เพื่อเป็นทางผ่านได้เช่นกัน การที่แฮกเกอร์สามารถเจาะเข้าสู่ระบบได้นั้นก็โดยอาศัยความบกพร่องของแอพพลิเคชั่น การที่แอพพลิเคชั่นถูกเขียนขึ้นมาอย่างไม่รัดกุมเพียงพอและเปิดโอกาสให้ผู้ที่รู้ช่องทางเหล่านี้ใช้ประโยชน์จากมันในการเล็ดรอดเข้ามาในระบบ โดยเฉพาะแอพพลิเคชั่นที่เป็นเวอร์ชั่นแรก ๆ มักจะแฝงมาด้วยช่องว่างเหล่านี้เสมอ แฮกเกอร์โดยส่วนใหญ่จะมีข้อมูลนี้อยู่แล้ว (หรือหากไม่มีก็สามารถเข้าไปค้นหาในเว็บไซต์ที่เป็นแหล่งชุมนุมของแฮกเกอร์ซึ่งจะมีข้อมูลเหล่านี้รออยู่แล้ว) นอกจากข้อมูลว่าแอพพลิเคชั่นใดมีรูรั่วแล้ว วิธีที่จะอาศัยรูรั่วเหล่านั้นเข้ามาในระบบก็เป็นที่เผยแพร่กันทั่วไป บางประเภทอาจจะใช้เทคนิคเพียงเล็กน้อย บางประเภทอาจจะต้องอาศัยเทคนิคที่ซับซ้อนประกอบกับลำดับที่ถูกต้องจึงจะสามารถเข้าไปได้ อย่างไรก็ตามถึงแม้ว่าจะยากเย็นเพียงใดก็จะมีผู้นำขั้นตอนเหล่านั้นมาเขียนเป็นโปรแกรมอัตโนมัติเพื่อทำหน้าที่เจาะระบบออกมาให้ผู้สนใจได้นำไปใช้

บทที่ 3
การออกแบบและการสร้าง

3.1 ขอบเขตของระบบตรวจจับผู้บุกรุกทางเครือข่ายคอมพิวเตอร์ที่สร้างขึ้น

ระบบตรวจจับผู้บุกรุกเครือข่ายคอมพิวเตอร์ (Intrusion Detection System – IDS) ที่สร้างขึ้น เป็นแบบปฏิบัติการบนการไหลข้อมูลในเครือข่าย ซึ่งใช้วิธีเกี่ยวกับการตรวจจับการใช้งานโดยจับทุกๆแพคเกจที่ส่งออกและเข้ามาสู่ระบบ และนำข้อมูลของแพคเกจที่ได้มาทำการวิเคราะห์และตรวจสอบความเป็นไปได้ในการบุกรุก โดยที่การบุกรุกเป็นแบบที่ทำการศึกษา ตามทฤษฎีและหลักการในบทที่สองส่วนรูปแบบการบุกรุกอื่นที่นอกเหนือจากกรณีที่ศึกษา จะไม่ถูกนำมาพิจาราณาเพื่อการออกแบบและการสร้าง

3.2 ขั้นตอนการออกแบบและการสร้าง

เมื่อทำการศึกษารูปแบบการสื่อสารเครือข่ายคอมพิวเตอร์และพิจาราณาถึงช้อบกพร่อง ที่ทำให้สามารถทำการโจมตีเครือข่ายคอมพิวเตอร์ได้ รวมถึงการศึกษาในส่วนรูปแบบของระบบการตรวจสอบเครือข่ายคอมพิวเตอร์ ทำให้เราต้องการรูปแบบโปรแกรมตรวจจับข้อมูลแปลกปลอมบนเครือข่าย ที่มีความสามารถต่างๆดังต่อไปนี้

1) โปรแกรมสามารถจับและแสดงรายละเอียดของแพคเกจทุกแพคเกจที่ผ่านระบบเครือข่ายที่โปรแกรมทำงานอยู่ได้
2) สามารถบันทึกข้อมูลแพคเกจที่ดักจับมาลงในไฟล์ได้
3) สามารถวิเคราะห์และแสดงผลการตรวจจับรูปแบบการโจมตีจากบทที่ 2 ได้

ดังนั้นขั้นตอนการสร้างต่าง ๆ จะทำตามขั้นตอนการออกแบบ และจากขั้นตอนที่ 1 ถึงขั้นตอนที่ 3 ทำให้ผู้ออกแบบได้กำหนดโหมด(mode)การใช้งานออกมาเป็น 3 โหมดดังต่อไปนี้

1) โหมดการทำงานแบบดูข้อมูลแบบเวลาจริงโดยไม่มีการเก็บข้อมูล (-v)
2) โหมดการทำงานแบบเก็บข้อมูลไว้ในไฟล์ (-l)
3) โหมดการตรวจจับผู้บุกรุก (-R) ในโหมดนี้จะทำการเก็บข้อมูลลงไฟล์ไปด้วยในตัว

จากการออกแบบทั้งหมด ทำให้ได้โปรแกรมซึ่งมีหน้าที่หลักๆซึ่งสามารถแบ่งออกมาได้ดังนี้

3.2.1 ส่วนรับคำสั่งและกำหนดค่าเริ่มต้น

รูปที่ 3.1 โฟล์วชาร์ทแสดงการเซ็ตค่าเริ่มต้น

จากรูปที่ 3.1 เมื่อเริ่มโปรแกรม สิ่งแรกที่จะต้องออกแบบคือ รูปแบบการทำงาน เนื่องจากโปรแกรม นอกจากต้องการตรวจจับการบุกรุกทางเครือข่ายแล้ว ยังต้องการให้ระบบสามารถทำการมอนิเตอร์ (Monitor) แพ็คเก็ตโดยไม่ต้องตรวจสอบการบุกรุกเพื่อตรวจสอบประสิทธิภาพของระบบเครือข่าย รวมถึงสามารถที่จะบอกรายละเอียดของแต่ละแพ็คเก็ต ที่ส่งผ่านสายอีเธอร์เน็ตถึงข้อมูลภายในแพ็คเก็ตนั้น และทำการตีความ ออกมา โดยสามารถที่จะเลือกรูปแบบการรายงานผลได้ ดังนั้นโฟลว์ชาร์ทนี้จะแสดงถึงลำดับในการรับคำสั่ง ซึ่งเมื่อรับคำสั่งเสร็จแล้วจะจบการทำงานเลยโดยที่ไม่มีการวนกลับมาเซ็ตค่าเริ่มต้นอีก

3.2.2 ส่วนดักจับแพ็กเก็ต

ในส่วนการทำงานนี้เป็นการทำงานในลักษณะดักจับแพ็กเก็ต ซึ่งในการเขียนโปรแกรมภาษาซีจะทำการเพิ่มไลบารี่ที่ชื่อว่า pcap.h ซึ่งเป็นไฟล์เฮดเดอร์ เพื่อที่จะนำไปสู่ฟังก์ชั่นในการติดต่อการ์ดแลน โดยกำหนดให้การ์ดแลนอยู่ในโหมดโพรมิสคูอัส ซึ่งการใช้งานจะเป็นลำดับขั้นการทำงานในลักษณะแพ็กเก็ตสนิฟเฟอร์แสดงไว้เป็นโฟลว์ชาร์ทการกำหนดค่าให้กับฟังก์ชั่นดังรูปที่ 3.2

รูปที่ 3.2 โฟล์วชาร์ทแสดงการดักจับแพ็กเก็ต

3.2.3 ส่วนวิเคราะห์แพ็กเก็ต

การวิเคราะห์แพ็กเก็ต จะทำการวิเคราะห์แพ็กเก็ต จนทราบข้อมูลเบื้องต้น เช่น เป็นโปรโตคอลอะไร ขนาดแพ็กเก็ตไหร่ เข้ามาเมื่อวัน , เดือน , ปี , เวลา เท่าไหร่ จากใคร ถึงใคร เมื่อวิเคราะห์ข้อมูลเบื้องต้นเสร็จแล้ว ขั้นตอนต่อไปของการวิเคราะห์แพ็กเก็ตคือ ตรวจสอบกับรูปแบบข้อมูลของระบบ ว่าตรงกับรูปแบบการบุกรุกที่ผู้ใช้ได้กำหนดไว้หรือไม่ รวมถึงการตรวจสอบว่าข้อมูลในบัฟเฟอร์ต่าง ๆ ที่ใช้ในการประมวลผลโปรแกรมว่าสามารถลบออกไปได้หรือไม่ด้วย

3.2.3.1 การแสกนพอร์ตแบบต่างๆ

- การสแกนพอร์ตโดยวิธี ซิน สแกน(SYN Scan)

การสแกนพอร์ตแบบ ซิน สแกน หากพิจารณาดู จากแพ็กเก็ตที่ส่งไปยัง เซิร์ฟเวอร์ โดยผิวเผินจะใกล้เคียงกับวิธี คอนเน็ค รีเควส แต่สิ่งที่แตกต่างกันคือ วิธีนี้ผู้สแกนจะทำการส่ง ซิน แพคเก็ต (SYN Package) มาเพื่อทำการติดต่อเองโดยตรงกับเป้าหมายโดยไม่ผ่านระบบปฏิบัติการ และรอการตอบรับของผลเป้าหมายกลับมา ซึ่งจะมีอยู่ 2 แบบคือ หากมีแอ็พพลิเคชั่นทำงานอยู่ ก็จะตอบกลับมาด้วย ซิน แอค หรือหากไม่มีแอพลิเคชั่นทำงานอยู่ก็จะตอบกลับมาด้วย รีเซ็ต(RST)

เมื่อมีการตอบรับด้วย ซิน แอค จากเป้าหมายกลับมา ระบบปฏิบัติการของโฮสต์ของผู้สแกนก็จะทำการตอบรับไปอีกครั้งด้วย รีเซ็ต เนื่องจากระบบปฏิบัติการไม่ได้เป็นผู้ส่งแพ็กเก็ตไปทำการติดต่อ

การสแกนแบบนี้หากตรวจสอบบนโฮสต์เป้าหมายนั้นจะพบว่า มีความพยายามขอเชื่อมต่อเข้ามา แต่ไม่สามารถเปิดการติดต่อได้สำเร็จเลย เพราะทุกครั้งจะไม่สามารถทำ ทรีเวย์ แฮนด์เชค(3 ways-handshake) ได้สำเร็จ จึงไม่มีการเชื่อมต่อใด ๆ เกิดขึ้นระหว่าง Server.com กับ Client.com ได้ ซึ่งจะส่งผลดีให้ฝ่ายแฮ็กเกอร์คือ สำหรับระบบที่มีการบันทึก ล็อก ประวัติการเชื่อมต่อผ่าน ทีซีพี ไว้จะไม่สามารถ บันทึกพฤติกรรมการสแกนวิธีนี้ได้เพราะการเชื่อมต่อไม่สำเร็จ ดังนั้นผู้ที่เป็นเจ้าของ Server.com ก็จะไม่ทราบว่าเครื่องตนเองถูกสแกนไปแล้ว

วิธี ซิน สแกน นี้สามารถทำการสแกนเป้าหมายได้อย่างรวดเร็ว เพราะเพียงแค่ส่ง ซิน แพ็กเก็ตออกไปยังโฮสต์และพอร์ตที่ต้องการอย่างต่อเนื่องตลอดเวลา เท่าที่แบนด์วิดธ์(Band width) จะเอื้ออำนวย ถ้ามีแบนด์วิดธ์มากก็จะสแกนได้เร็วมาก ซึ่งสำหรับการสแกนพอร์ตนั้นความเร็วในการสแกนเป็นสิ่งสำคัญ เพราะการสแกนพอร์ตไม่สามารถใช้เทคนิคของการบรอดคาสต์ (Broadcast) มาช่วยได้จะต้องกระทำไปบนพื้นฐานของการสแกนหนึ่งครั้ง ต่อหนึ่งพอร์ต ต่อหนึ่งโฮสต์เสมอ ในขณะที่ ทีซีพี มีพอร์ต 65535 พอร์ต หากจะทำการสแกนให้หมดทุกพอร์ตอาจต้องใช้เวลานานมาก ๆ ดังนั้นวิธีที่สามารถส่ง ซิน แพ็กเก็ต ได้อย่างรวดเร็วจะช่วยการทำงานในส่วนนี้ได้มาก

- การสแกนพอร์ตโดยวิธี ฟิน สแกน(FIN Scan)

เมื่อ ซิน สแกน นั้น สามารถทำได้โดยง่าย ก็ย่อมสามารถถูกตรวจจับได้โดยง่ายเช่นกัน แต่อีกวิธีหนึ่งคือ ฟิน สแกน นั้นเป็นการสแกนที่สังเกตุได้ค่อนข้างยาก โดยเฉพาะหากลำดับพอร์ตของการสแกนเป็นแบบสุ่มและเว้นระยะพอสมควรซึ่งจะทำให้แพ็กเก็ตที่ใช้สแกน สามารถเล็ดลอดเข้ามาได้โดยไร้ร่องรอย เพราะโดยปกติที่วไปหากเราทำการวิเคราะห์แพ็กเก็ตที่อยู่บนเน็ตเวิร์กนั้น แฟลก ของ ทีซีพี คือ ซิน(SYN) และ ฟิน(FIN) จะเป็นสิ่งที่ระบุทิศทางของแพ็กเก็ต ซิน คือ แพ็กเก็ตที่ส่งเข้ามาขอติดต่อด้วย ส่วน ฟิน เป็นแพ็กเก็ตที่ตอบกลับ หากสังเกตเฉพาะพอร์ตของแพ็กเก็ตที่เข้ามาเป็นราย แพ็กเก็ตนั้นเพียงอย่างเดียวโดยไม่พิจารณาปัจจัยอื่น ก็จะทำให้ผลวิเคราะห์ผิดพลาดได้

โดยส่วนใหญ่เราอาจเข้าใจว่าการติดต่อกับเซิร์ฟเวอร์พอร์ตจะต้องให้ ซิน แฟลกเท่านั้นซึ่งก็เป็นความเข้าใจที่ผิดหากการติดต่อนั้นเป็นไปเพื่อจะขอใช้บริการจากแอพพลิเคชั่นนั้นจริง ๆ เพราะการสื่อสารใด ๆ โดยใช้โปรโตคอล ทีซีพี จะต้องเริ่มต้นด้วย ซิน แพ็กเก็ตเสมอ แต่หากไม่ต้องการจะใช้บริการจากเซิร์ฟเวอร์นั้น แต่หวังผลเพียงหยั่งดูว่าเซิร์ฟเวอร์พอร์ตนั้น ๆเปิดให้บริการหรือไม่ก็อาจใช้แพ็กเก็ตแบบอื่น ๆ ได้

การกระตุ้นและการตอบสนองของ ทีซีพี นั้น จะเห็นว่าโปรโตคอล ทีซีพี มิได้ตอบเฉพาะ ซิน เท่านั้น แฟลก อื่น ๆ ที่ส่งมาก็จะได้รับการตอบสนองเช่นเดียวกัน จุดบกพร่องสำคัญที่ทำให้การพยายามหยั่งตรวจสอบพอร์ตอื่นนั้นบังเกิดผลก็เนื่องมากจาก ทีซีพี เป็นโปรโตคอลที่กำหนดจังหวะการสื่อสารกันตามลำดับโดยมี แฟลก เป็นตัวบอกสถานะการสื่อสารของแพ็กเก็ตนั้น ๆ โดยคาดหวังว่าทุกคนจะปฏิบัติตามที่โปรโตคอลกำหนดไว้อย่างเคร่งครัด ประกอบกับในการสื่อสารข้อมูลจริงนั้นจะมีแพ็กเก็ตที่มี แฟลก ซิน , ฟิน, พุช(PUSH) ของแต่ละเซสชั่น(Session)วิ่งกันอลหม่าน ทำให้มีการอาศัยช่วงเหล่านี้ส่งแพ็กเก็ตที่ไม่เป็นไปตามลำดับที่กำหนดไว้ในโปรโตคอลแฝงเข้าไปด้วย และการทำ ฟิน สแกน ก็เช่นกัน

โดยปกติ ฟิน แพ็กเก็ตจะเป็นแพ็กเก็ตจบของทีซีพี ที่จะส่งเมื่อยุติการติดต่อ นั่นหมายถึงจะต้องมีการสื่อสารกันมาก่อนแล้วแต่ ฟิน สแกนจะเป็นการส่ง ฟิน แพ็กเก็ตไปยังเป้าหมายโดยไม่มีการสื่อสารใด ๆ มาก่อน เรียกว่า เป็นการจบโดยไม่มีปีมีขลุ่ย และไม่เคยติดต่อกัน แน่นอนว่าการได้รับ ฟิน ที่ไม่มีปีมีขลุ่ยเข้ามานั้น โฮสต์ที่ได้รับจะต้องทราบอย่างแน่นอนว่าไม่เคยได้รับการติดต่อจาก ไอพี แอดเดรส และพอร์ตต้นทางนั้นมาก่อนเลย แต่อย่างไรก็ตามโฮสต์ก็ยังคงตอบ ฟิน แพ็กเก็ตนั้นกลับไปอยู่ดี และที่สำคัญที่สุดคือโดยปกติการตอบ ฟิน แพ็กเก็ตกลับไปของพอร์ตที่เปิดไว้ และพอร์ตที่ไม่ได้เปิดให้บริการก็ไม่เหมือนกัน หากเป็นพอร์ตที่ไม่ได้เปิดอยู่โฮสต์ก็จะตอบด้วยรีเซ็ตแฟลก และหากเป็นพอร์ตที่เปิดให้บริการอยู่ ก็จะตอบด้วย ฟิน แอค กลับไป เมื่อนำการตอบรับจากโฮสต์ มาพิจารณาก็จะทราบได้ทันทีว่า พอร์ตนั้นเปิดให้บริการอยู่หรือไม่โดยไม่ต้องส่ง ซิน ไปแม้แต่แพ็กเก็ตเดียว

- การสแกนพอร์ตโดยวิธีคริสต์มาสสแกน(Xmas Scan)

โดยปกติจะไม่ใช้ทีซีพี แฟลกทั้งสามตัวซึ่งจะเป็นที่สังเกตุได้ง่าย คือ ซิน หรือ แอค หรือ รีเซ็ท ในการสแกน ทั้งนี้เพื่อหลบเลี่ยงการถูกตรวจจับได้มากที่สุด แต่จะใช้ ฟิน พุช เออร์เจ้น ซึ่งไม่ค่อยเป็นที่สนใจเท่าใดนักในการสแกนเพื่อให้เป้าหมายตอบกลับมาอย่างใดอย่างหนึ่ง

-การสแกนพอร์ตโดยวิธีนัลล์สแกน (Null Scan)

วิธีนี้จะไม่ใช้แฟลกใดๆในการสแกนเลย โดยส่งแพ็กเก็ตที่ไม่มีแฟล็กใดถูกเซ็ทไว้เลยไปยังเป้าหมาย โดยทั่วไปแล้วแพ็กเก็ตประเภทนี้ จะไม่อยู่ในข้อกำหนดของโปรโตคอลจึงไม่มีผู้สนใจ นอกจากนี้ยังทำให้โปรโตคอลในเลเยอร์สูงขึ้นไปไม่ทราบว่ามีการส่งแพ็กเก็ตเข้ามาด้วย

โดยทั่วไปการตอยสนองแพ็กเก็ตที่ไม่ได้กำหนดในโปรโตคอล จะมีการตอบรับที่แตกต่างกันไปตามแต่ ประเภทของระบบปฏิบัติการ ดังนั้นนอกจากการใช้แพ็กเก็ตเหล่านี้เพื่อการสแกนพอร์ตแล้ว ยังสามารถนำแพ็กเก็ตเหล่านี้ ไปใช้ในการตรวจสอบระบบปฏิบัติการของเป้าหมายได้อีกด้วย โดยการส่งแพกเก็ตที่มีแฟลก ซึ่งไม่อยู่ในข้อกำหนดของโปรโตคอลเข้าไปหลายๆแบบ และตรวจสอบการตอบกลับมา โดยทั่วไปแล้วระบบปฏิบัติการแต่ละแบบจะมีการตอบสนองที่ไม่เหมือนกัน เมื่อนำข้อมูลที่ตอบกลับมาไปเทียบกับตารางมาตรฐานของแต่ละระบบก็จะทราบได้ทันที

จากการสแกนโดย ทีซีพีแฟลกแปลกประหลาดทั้งแบบคริสต์มาส สแกนและนัลล์ สแกน จะเห็นว่าการตอบรับการสแกนทั้งสองแบบจะเหมือนกันคือ หากพอร์ตเปิดอยู่ก็จะไม่ตอบแพ็กเก็ตใดๆกลับมา(ซึ่งค่อนข้างแปลกสำหรับโปรโตคอลทีซีพี เพราะปกติทีซีพีมักจะตอบเสมอ) และหากพอร์ตปิดอยู่ก็จะตอบกลับด้วยรีเซ็ทแฟลก เพื่อให้รู้ว่าพอร์ตปิดอยู่

อย่างไรก็ตามเนื่องจากแฟลกต่างๆที่ใช้ในการสแกน ทั้งสองประเภทนั้นมิได้มีกำหนดอยู่ในโปรโตคอล โดยเฉพาะเมื่อใช้กับพอร์ตที่เปิดอยู่นั้นการตอบรับที่ถูกต้องตามโปรโตคอลที่ระบุตาม อาร์เอฟซี 793 ก็คือไม่ควรตอบใดๆกลับไป(ใน อาร์เอฟซี 793 มิได้กล่าวถึงแฟลกประเภทนี้ แต่จะระบุเฉพาะแฟลกที่ต้องตอบรับกลับไป ดังนั้นแฟลกที่เข้ามาไม่ใช่แฟลกดังกล่าวก็ไม่ต้องตอบรับ)แต่การอิมพลีเมนต์โปรโตคอล ทีซีพี/ไอพี ของระบบปฏิบัติการต่างๆนั้นจะทำงานแตกต่างกันออกไป การตอบรับสำหรับพอร์ตที่เปิดอยู่จึงแตกต่างกันออกไปด้วย ดังนั้นการสแกนทั้งสองวิธีหากนำไปใช้ในระบบปฏิบัติการแต่ละประเภทอาจได้ผลลัพธ์ที่แตกต่างกันออกไปได้

- การสแกนพอร์ตโดยการแฟร็กเมนต์ (Tiny Fragmented Packets)

ด้วยคุณสมบัติของไอพี ที่สามารถแบ่งย่อยข้อมูลให้เหมาะสมกับขนาดของการส่งแต่ละครั้งได้จึงทำให้บางครั้งการส่งข้อมูลหนึ่งครั้งไปยังปลายทางอาจถูกแบ่งย่อยไปเป็นหลายๆแพ็กเก็ตไปยังปลายทางและไอพีที่ปลายทางก็จะทำการรวมแพ็กเก็ตย่อยเหล่านั้นกลับมาเป็นข้อมูลเดิมอีกครั้ง ดังนั้นในมุมมองของเลเยอร์ที่สูงกว่า ไอพี ก็ไม่จำเป็นจะต้องรู้ว่าข้อมูลถูกแบ่งย่อยออกไปหรือไม่อย่างไร เพราะไอพีจะเป็นตัวจัดการให้ทั้งหมดทั้งตอนแบ่งย่อยและตอนรวมกลับมาใหม่ โดยทั่วไปแล้วไอพีจะทำการแบ่งย่อยข้อมูลเมื่อขนาดของข้อมูลใหญ่เกินกว่าที่จะบรรจุลงในดาต้าแกรมเดียวเท่านั้นได้ แต่สำหรับแฮกเกอร์ทั้งหลายกลับมองเห็นคุณสมบัติข้อนี้และนำมาใช้ให้เป็นประโยชน์ เพื่อการสแกนอย่างแยบยล

ด้วยการสแกนที่กล่าวมาข้างต้น จะเห็นได้ว่าการใช้เทคนิคของแฟลกในระดับทีซีพี เพื่อกระตุ้นเป้าหมายโดยการปรับเปลี่ยน ทีซีพี แฟลกให้เป็นค่าต่างๆส่งเข้าไปยังพอร์ทที่ตนเองอยากรู้สถานะเป็นการหยั่งดู แต่ถึงจะมีการปรับเปลี่ยนทีซีพี แฟลกอย่างไรแพ็กเก็ตเหล่านี้ก็เป็นที่สังเกตุง่ายอยู่ดี จึงมีผู้คิดค้นวิธีสแกนที่สามารถอำพรางตนเองจากการตรวจจับโดยอาศัยการแฟร็กเมนต์ในระดับไอพี เทคนิคของวิธีนี้คือการแบ่งทีซีพีเฮดเดอร์ ออกมาด้วยวิธีการแฟร็กเมนต์ให้กลายเป็นไอ

พีแพ็กเก็ตเล็กๆ แล้วส่งแฟร็กเมนต์นั้นไปยังเป้าหมายเพื่อให้แฟรกเมนต์ถูกนำกลับไปรวมกันเป็นทีซีพีเฮดเดอร์สมบูรณ์ที่ปลายทาง

ปกติ ทีซีพีเฮดเดอร์ จะมีขนาด 20 ไบต์(ถ้ามีออปชั่นด้วยก็จะมากกว่า 20 ไบต์) แทนที่จะส่งทีซีพีเฮดเดอร์ไปยังเป้าหมายในครั้งเดียวซึ่งอาจถูฏตรวจพบได้ง่าย ดังนั้นก่อนการส่งผู้สแกนจะทำการแบ่งทีซีพีเฮดเดอร์ออกเป็น 2 ส่วนโดยส่ง 16 ไบต์แรกไปก่อน จากนั้นจึงส่งอีกสี่ไบต์หลัง การสแกนหนึ่งครั้งจะใช้ สอง แพ็กเก็ต สำหรับที่เป้าหมายปลายทางนั้น ไอพีก็จะรับ 2 แพ็กเก็ตนี้แล้วรวบรวมทั้ง 2 แพ็กเก็ต ส่งต่อไปยัง ทีซีพี และทีซีพี ก็จะตอบกลับมาเสมือนตอบรับการสแกนตามปกติ

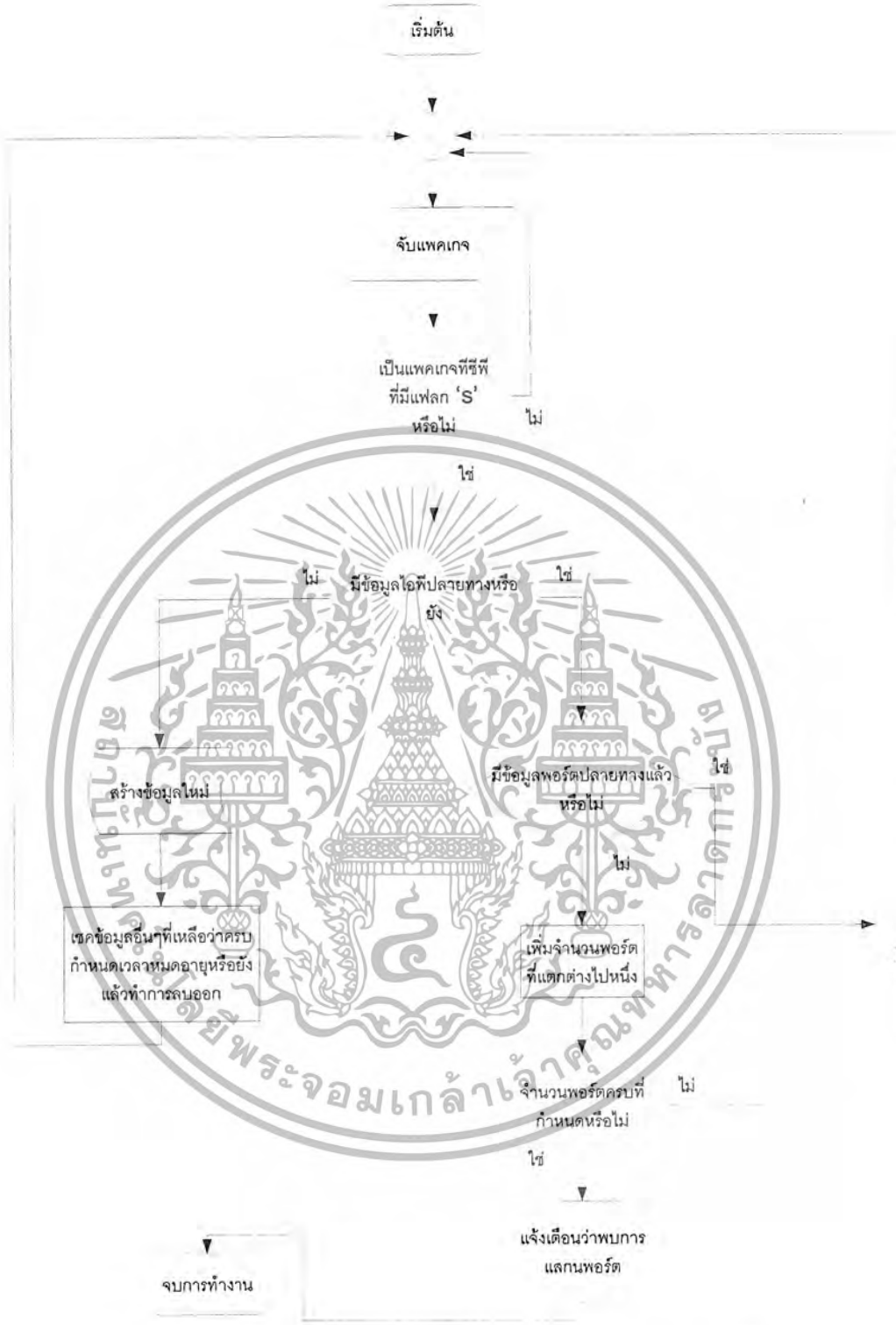
-การสแกนพอร์ท ยูดีพี (UDP Scan)

ยูดีพี มีการจัดการพอร์ตที่แตกต่างจากทีซีพี คือไม่มีกลไกที่แน่นอนในการควบคุมการรับส่งข้อมูล เช่นเดียวกับทรีเวย์ แฮนด์เชค ของทีซีพีดังนั้นผลลัพธ์ของการสแกนเมื่อพอร์ตเปิดใช้งานอยู่นั้นจะไม่สามารถคาดการณ์ได้ ขึ้นอยู่กับแต่ละแอพพลิเคชั่นและไม่มีมาตรฐานที่เหมือนกัน แต่อย่างไร ดังนั้นการสแกนพอร์ตยูดีพี จึงต้องดูผลลัพธ์จากไอซีเอ็มพีเป็นหลัก หากมีไอซีเอ็มพีตอบกลับมาแสดงว่าพอร์ตนั้นไม่เปิด หากไม่มี ไอซีเอ็มพี ตอบกลับมาแสดงว่าพอร์ตนั้นเปิดใช้งานอยู่ วิธีการเบื้องต้นของการสแกนคือพยายามติดต่อไปยังพอร์ตยูดีพีเป้าหมายเพื่อคอยดูการตอบรับมาดังนี้

- พอร์ตไม่เปิดให้บริการ จะมีข้อความไอซีเอ็มพีว่า UDP Port Unreachable
- พอร์ตเปิดให้บริการ อาจจะมีการตอบรับหรือไม่ และอย่างไร จะขึ้นอยู่กับการทำงานของแอพพลิเคชั่นที่เปิดพอร์ตนั้น แต่ที่แน่ๆคือจะไม่มี ข้อความไอซีเอ็มพีกลับมา

การสแกนพอร์ตของยูดีพีในลักษณะนี้ ก็เปรียบเสมือน ซินสแกน ของทีซีพี เพราะเป็นการส่งแพ็กเก็ตไปทดสอบการตอบรับของพอร์ตยูดีพี พอร์ตนั้นๆ โดยการพยายามจะติดต่อกับแอพพลิเคชั่นที่ทำงานอยู่บนพอร์ตนั้นตามปกติแล้วให้โฮสต์นั้นตอบรับกลับมาอย่างใดอย่างหนึ่ง เพียงแต่ยูดีพี ไม่มีแฟล็ก จึงไม่สามารถใช้เทคนิคอื่นมาหลบหลีกหรืออำพรางตนเองได้ ต้องใช้การส่งแพ็กเก็ตเหมือนกันเข้าไปทุกครั้ง

หลักการตรวจการแสกนพอร์ตทุกชนิดจะมีลักษณะเหมือนกัน คือ พยายามตรวจสอบว่า ถ้าในช่วงเวลาสั้นๆช่วงหนึ่ง หากมีแพคเกจจำนวนหนึ่งที่มีไอพีปลายทางเหมือนกันแต่มีพอร์ตปลายทางแตกต่างเป็นจำนวนที่กำหนดไว้ แสดงว่าเกิดการแสกนพอร์ตขึ้น



รูปที่ 3.3 โฟล์วชาร์ทแสดงการตรวจจับการแสกนพอร์ตแบบวิธีซินแสกน

ดังตัวอย่างในรูปที่ 3.2 เป็นโฟล์วชาร์ทแสดงการตรวจจับแบบวิธีซินแสกน ซึ่งการตรวจจับก็จะแตกต่างกันไปเฉพาะตรงส่วนการเช็คแฟลกหรือโปรโตคอลของแพคเกจดังที่จะแสดงดังต่อไปนี้

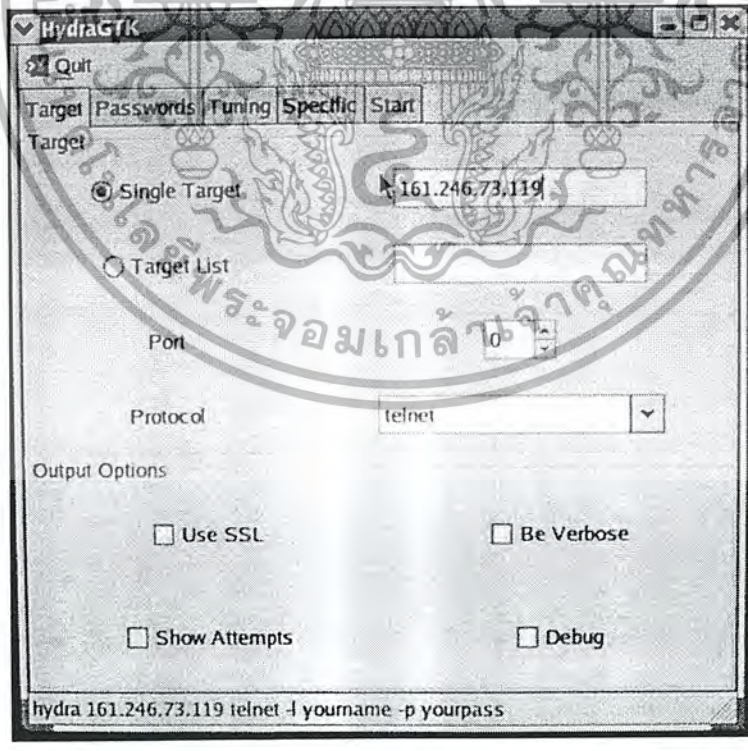
ซินแสกน : ตรวจจับเฉพาะแพคเกจทีซีพีที่มีแฟลกเป็น 'S'

- ฟินแสกน : ตรวจจับเฉพาะแพคเกจทีซีพีที่มีแฟลกเป็น 'F'
- นูลแสกน (null) : ตรวจจับเฉพาะแพคเกจทีซีพีที่มีแฟลกเป็น ' '
- คริสต์มาสแสกน (Xmas) : ตรวจจับเฉพาะแพคเกจทีซีพีที่มีแฟลกเป็น 'FPU'
- แอคแสกน (Ack) : ตรวจจับเฉพาะแพคเกจทีซีพีที่มีแฟลกเป็น 'A'
- ยูดีพีแสกน : ตรวจจับเฉพาะแพคเกจยูดีพี

3.2.3.2 บรูทฟอร์ซแอทแทค (Brute force)

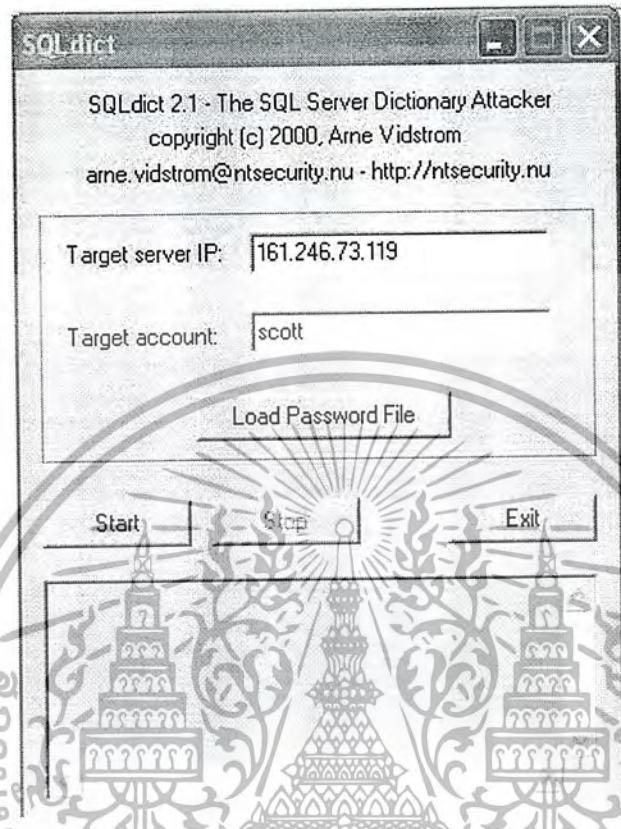
หลักการตรวจจับต้องทำการตรวจสอบหาว่า ในช่วงเวลาสั้นๆช่วงหนึ่ง ได้มีแพคเกจที่แจ้งการล็อกอินผิดพลาด โดยมาจากไอพีต้นทางเดียวกันมากเกินปรกติ แสดงว่าเกิดการโจมตีด้วยวิธีนี้ขึ้น

- โจมตีระบบเทลเน็ทด้วยบรูซฟอร์ซ โดยจะพยายามล็อกอินเข้าไปที่พอร์ตเทลเน็ท(พอร์ต 23) หลายๆครั้งมากๆ โดยทำการสุ่มยูสเซอร์เนมและพาสเวอร์ด



รูปที่ 3.4 แสดงโปรแกรมที่ใช้ในการบรูซฟอร์ซ เทลเน็ท

-โจมตี เอสคิวแอลเซิร์ฟเวอร์ด้วยบรูซฟอร์ซ โดยพยายามล็อกอินไปที่พอร์ต 1433 โดยการสุ่มยูสเซอร์เนม และพาสเวอร์ด



รูปที่ 3.5แสดงโปรแกรมที่ใช้ในการทำบรูซฟอร์ซ เอสคิวแอล

รูปที่ 3.6 โฟล์วชาร์ทแสดงการตรวจจับการบุกรุกแบบบรูทฟอร์ซ

3.2.3.3 การติดต่อไปที่พอร์ตแบ็คดอร์ (Backdoor Port)

หลักการตรวจจับคือ ตรวจสอบพอร์ตปลายทางว่าเป็นพอร์ตที่อยู่ในลิสต์พอร์ตโทรจันหรือไม่ และดูการตอบกลับจากพอร์ตว่ามีการหรือไม่ ถ้าตอบกลับจะแจ้งแบบระดับอันตราย แต่ถ้าไม่มีการตรวจจับจะทำการแจ้งเตือนแบบปรกติ

รูปที่ 3.7 โฟล์วชาร์ทแสดงการตรวจจับการบุกรุกแบบแบ็คดอร์พอร์ต

3.2.3.4 การโจมตีแบบโดลีโทรจัน

ชื่อ:DolyTrojan

ชนิด:ม้าโทรจัน

ชื่ออื่นที่รู้จัก:Backdoor.AZ,Backdoor.Doly

ระดับความรุนแรง :ปานกลาง

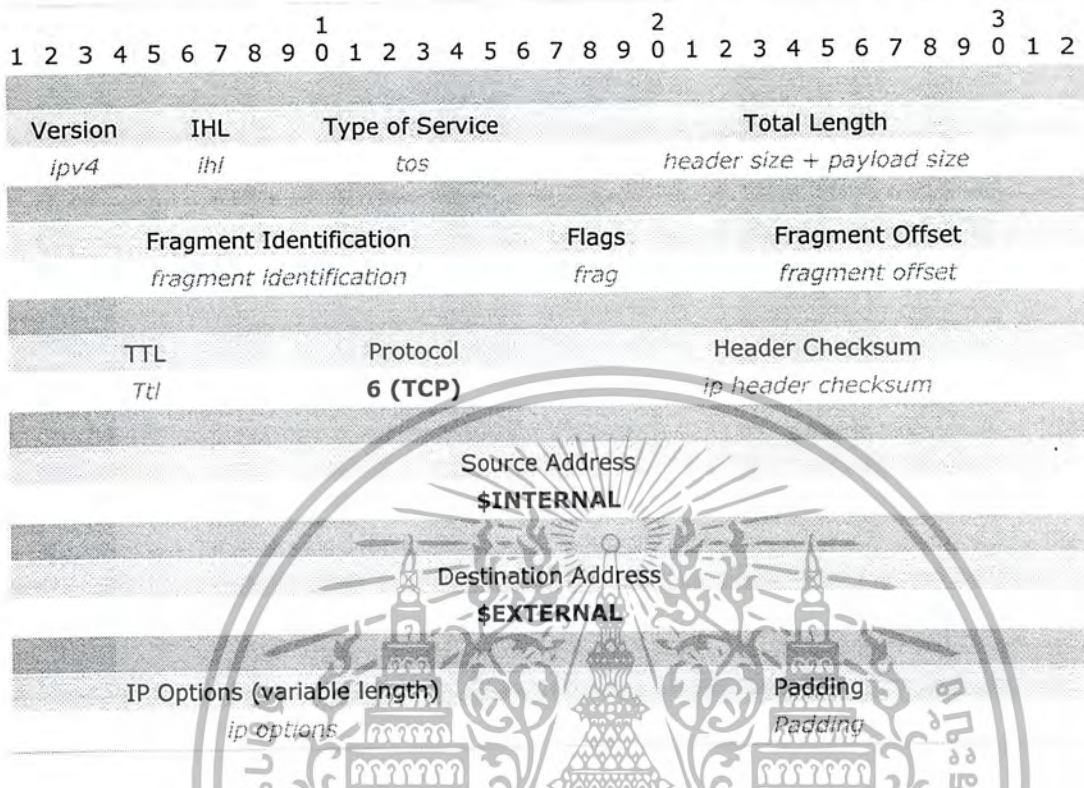
ลักษณะทั่วไป

โดลี โทรจัน ถูกเขียนในประเทศอิสราเอล โดยใช้ภาษาวิชวลเบสิค โดลีมีความสามารถในการขโมยข้อมูล ควบคุมเครื่องเป้าหมายได้ในหลายๆทาง รวมถึงความสามารถในการขโมยข้อมูลพาสเวิร์ด จนถึงทำให้เครื่องเป้าหมายใช้การไม่ได้ ในเวอร์ชันหลังๆ โดยเครื่องเป้าหมายที่ถูกโจมตีเป็นเครื่องในตระกูลวินโดวส์ต่างๆตั้งแต่วินโดวส์ 95 วินโดวส์98 วินโดวส์เอ็นที วินโดวส์2000 จนมาถึงวินโดวส์เอ็กซ์พี แต่ในระบบปฏิบัติการอื่นจะไม่ติดโทรจันชนิดนี้ เมื่อไฟล์ของโดลีถูกเอ็กซีคิวต์ มันก็จะแพร่พันธุ์โดยใช้ชื่อแบบสุ่ม โดยมีนามสกุลเป็น อีเอ็กซ์อี หรือ ดีแอลแอล นอกจากนี้เมื่อไฟล์ของโดลีถูกส่งผ่านเมล์มันยังสามารถมาในรูปของไฟล์นามสกุล เจพีจี หรือ บีเอ็มพี ได้อีกด้วย

ไฟล์ที่พบ

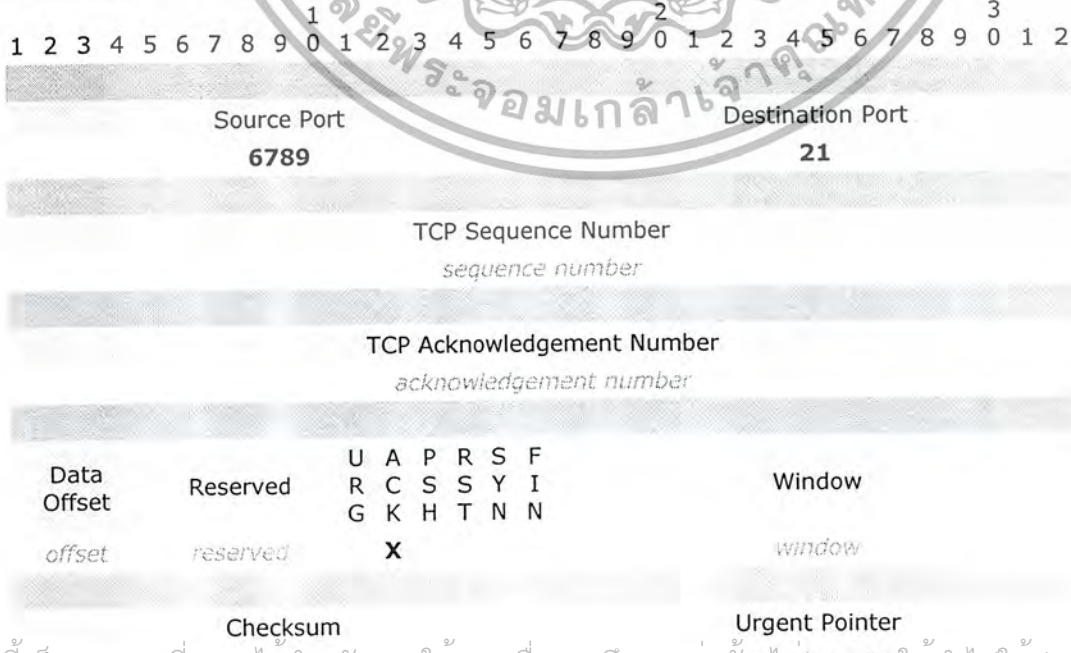
Doly1.1.zip - Doly1.2.zip - 3,977,753 bytes Doly135.zip - 5,942,944 bytes Doly15.zip - 4,348,735 bytes Doly16.zip - 2,627,852 bytes Doly_Trojan_v17.zip - 842,982 bytes Doly17_Server.zip - 172,912 bytes Doly2.0.zip - Send_to_victim.zip - 2,386,049 bytes Send_to_victim2.zip - 2,392,257 bytes Send_to_victim3.zip - 2,361,750 bytes Doly_Client[SE].zip - 844,595 bytes Doly_Server[SE].zip - 186,105 bytes Dolytrojan.exe - 251,904 bytes Doly.exe - Doly1.2.exe - 2,004,818 bytes Doly135.exe - 2,813071 bytes Doly15.exe - 1,990,448 bytes Doly16.exe - 1,463,805 bytes Setup.exe - 2,049,807 bytes Ssetup.exe - 1,271,877 bytes Ssetup.exe - 2,454,690 bytes Ssetup.exe - 3,226,540 bytes Ddoly121.zip - 406 bytes Dhacker.exe - 45,056 bytes Download.exe - 2,429,558 bytes Interactive.exe - 2,398,769 bytes Setup.exe - 436,227 bytes Setup.exe - 2,423,695 bytes Ndc.exe - 204,800 bytes Nds.exe - 106,496 bytes Mdm.exe - Tesk.exe - 169,472 bytes Tesk.sys - Mstesk.exe - Kernal32.exe - Iecookie.exe - Sys.exe - Sys.lon - Send_to_victim.zip - 2,386,029 bytes Send_to_victim2.zip - 2,392,257 bytes Send_to_victim3.zip - 2,361,750 bytes Vbrun60.exe - [1 Mb]

IP HEADER



ภาพที่3.8แสดงไอพีเฮดเดอร์ของ โทรจันโคลี

TCP Packet Header



ภาพที่ 3.9 แสดงทีซีพีเฮดเดอร์ของโทรจันโดลี

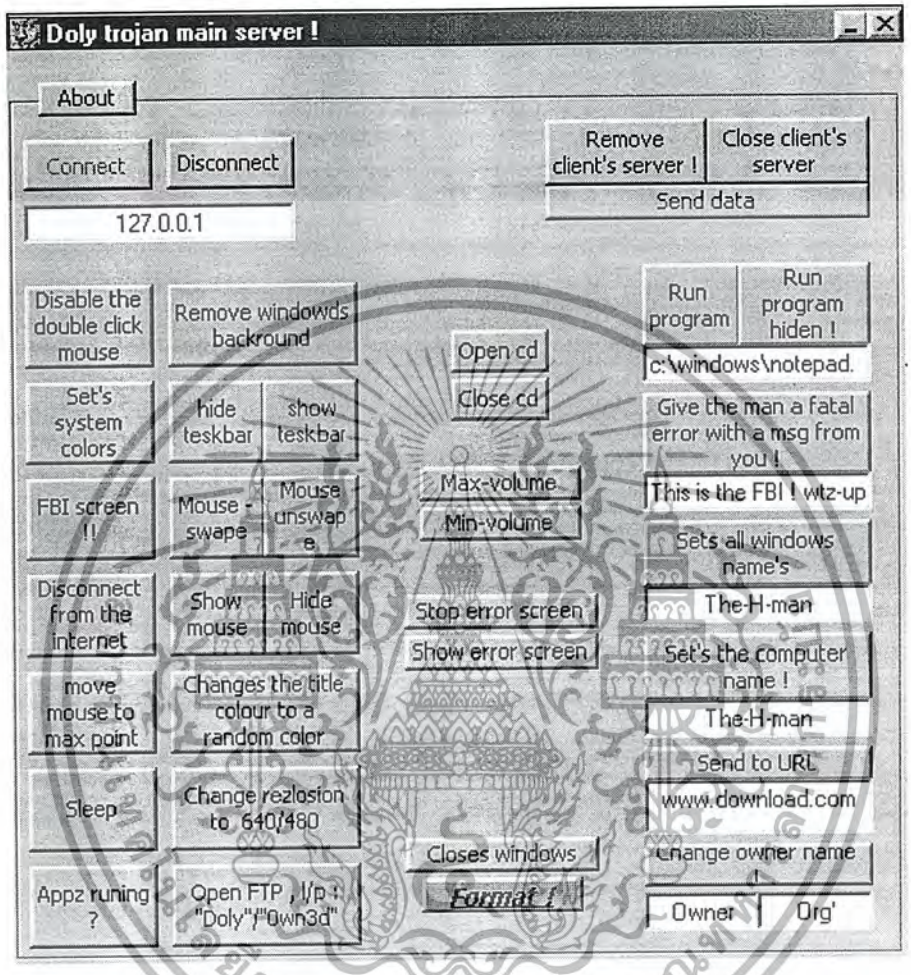
โดลีจะใช้พอร์ท 21 ซึ่งซ้ำกับพอร์ทมาตรฐาน คือพอร์ทเอฟทีพี ใช้ในการเชื่อมต่อเพื่อให้ยากต่อการตรวจจับแต่ข้อมูลที่ส่งจะมีลักษณะพิเศษ(Signature)ดังรูป ทำให้สามารถนำมาใช้ตรวจสอบได้

```
Trojan active - Doly
08/25-23:15:21.681048 192.168.30.15:6789 -> 192.168.30.12:1076
TCP TTL:128 TOS:0x0 ID:23043  DF
*****PA* Seq: 0x3184EC   Ack: 0xE93C   Win: 0x2232
57 74 7A 75 70 20 55 73 65 72 30 31 20 2D 20 59  Wtzup User01 - Y·
6F 75 72 20 43 6F 6E 6E 65 63 74 65 64 20 74 6F  our Connected to
20 3A 20 63 6C 6F 61 6B                          : cloak
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
Trojan active - Doly
08/25-23:16:04.505667 192.168.30.15:6789 -> 192.168.30.12:1080
TCP TTL:128 TOS:0x0 ID:27139  DF
*****PA* Seq: 0x322CD5   Ack: 0xE94C   Win: 0x2232
57 74 7A 75 70 20 55 73 65 72 30 32 20 2D 20 59  Wtzup User02 - Y
6F 75 72 20 43 6F 6E 6E 65 63 74 65 64 20 74 6F  our Connected to
20 3A 20 63 6C 6F 61 6B                          : cloak
```

คุณสมบัติ

- เอ็นเนเบิล/ดิสเอเบิลเมาส์
- ตั้งค่าสีของระบบ
- สั่งให้หน้าจอเป็นข้อความ เอฟบีไอ
- ตัดการเชื่อมต่อจากอินเตอร์เน็ท
- ย้ายเมาส์ไปที่จุดสูงสุด
- เปลี่ยนโมดของวินโดวส์เป็นสลีปโหมด
- ลบภาพพื้นหลังของวินโดวส์
- ซ่อนหรือแสดงทาสก์บาร์
- เปลี่ยนปุ่มของเมาส์
- ซ่อน/แสดงเมาส์
- เปลี่ยนความละเอียดของจอเป็น640*480
- เปิดเซิร์ฟเวอร์เอฟทีพี
- เปิด/ปิด ซีดีรอม
- รันโปรแกรมต่างๆ
- ส่งข้อความชนิดร้ายแรงมา(fatal error message)

- เปลี่ยนชื่อของคอมพิวเตอร์
- ปิดเซิร์ฟเวอร์
- ลบเซิร์ฟเวอร์



ภาพที่ 3.10 แสดงตัวควบคุมเซิร์ฟเวอร์ของโทรจันโดลี

หลักการตรวจสอบคือ ดูที่พอร์ตปลายทางว่าเป็นพอร์ตเบอร์ 21 หรือไม่ และ หาว่าในข้อมูลแพคเกจมีข้อความที่แสดงถึงการโจมตีอยู่หรือไม่ ถ้าพบทั้งสองอย่างจะทำการแจ้งเตือน

รูปที่ 3.11 โฟล์วชาร์ทแสดงการตรวจจับการบุกรุกแบบโคลีโทรจัน

3.2.3.5 อินเฟคเตอร์โทรจัน (Infector Trojan)

ชื่อ : Infector Trojan

ชนิด:ม้าโทรจัน

ชื่ออื่นที่รู้จัก:,Backdoor.ciadoor,Backdoor:Win32/Ciadoor

ระดับความรุนแรง : ปานกลาง

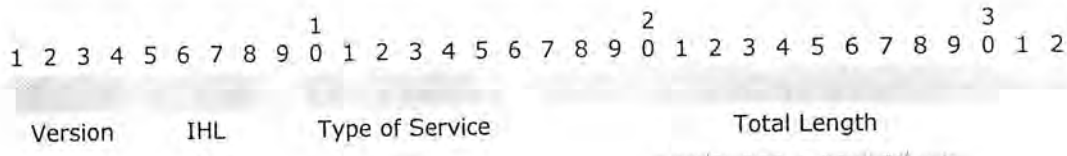
ลักษณะทั่วไป

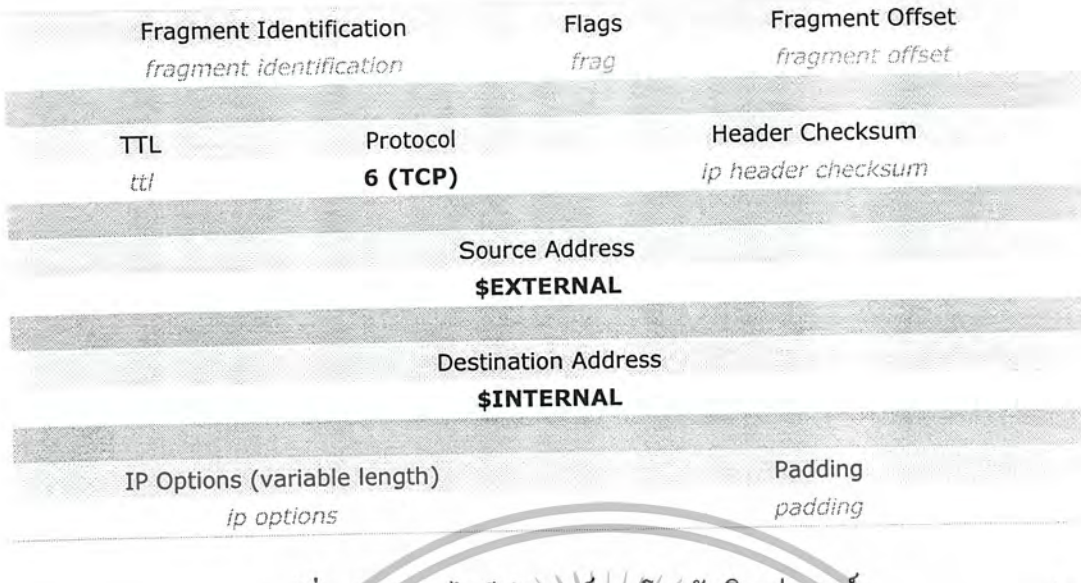
อินเฟคเตอร์ เป็นโทรจันชนิดที่ควบคุมจากระยะไกล(Remote Access Trojan) ซึ่งถูกพัฒนาโดยกลุ่มที่เรียกว่า "เอฟซี" จากประเทศอังกฤษ โดยในระยะแรกๆไม่มีคุณสมบัติอะไรมากมาย แต่ก็ค่อยๆพัฒนาอย่างช้าๆ จนมีชื่อเสียง และในปัจจุบัน ก็มักจะเป็นตัวเลือกแรกๆให้กับแฮกเกอร์มือใหม่ คุณสมบัติ และอินเตอร์เฟสของมันก็เหมาะสมกับผู้ใช้

ไฟล์ที่พบ

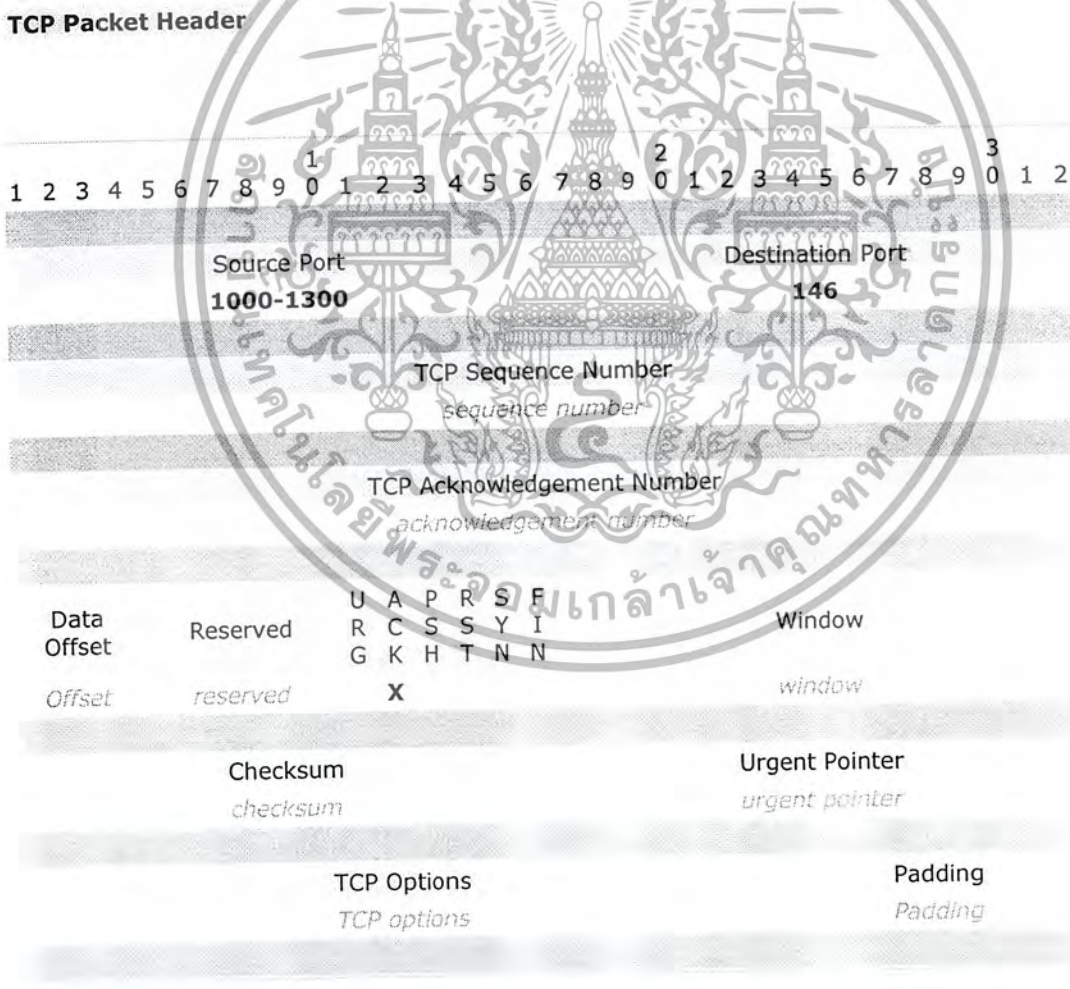
Fc.zip - 462,863 bytes Infector. zip - 95,103 bytes Infector. zip - 101,764 bytes Infector1.0.zip - 285,601 bytes Infector1.3.zip - 445,950 bytes Infector1.4.zip - 504,012 bytes Infector1.4.2.zip - 570,490 bytes Infector1.6.zip - 604,218 bytes Infector1.6a.zip - 661,515 bytes Infector1.6b.zip - 691,336 bytes Infector1.7c.zip - Infector_1.7_bonus.zip - Infector2.0.zip - 36,395 bytes Infector9.0.zip - 5,599 bytes Infector_v2.zip - 35,713 bytes Infector.exe - 18,929 bytes Infector.exe - 87,944 bytes Infector.exe - 184,832 bytes Infector.exe - 291,840 bytes File_id.exe - 3,632 bytes Client.exe - 174,080 bytes Client.exe - 178,176, bytes Client.exe - 294,912 bytes Client.exe - 333,824 bytes Server.exe - 120,320 bytes Server.exe - 293,888 bytes Server 1.6b_new.exe - 527,872 bytes Unpacked_server.exe - 299,008 bytes Unpacked_server.exe - 300,544 bytes Editsrv.exe - 114,688 bytes Editsrv.exe - 140,800 bytes Editsrv.exe - 233,984 bytes Editsrv.exe - 236,544 bytes Editserv.exe - 141,312 bytes Fc32.exe - 414,208 bytes Fc_1.6server_a.exe - 534,016 bytes Uhanfo.exe - 6,912 bytes Trojan.exe - D3x.drv - Setup.int bytes Msnapplication.exe - - 532,016 bytes

IP HEADER





รูปที่ 3.12 แสดงไอพีเฮดเดอร์ของโทรจันอินเฟคเตอร์



รูปที่ 3.13 แสดงทีซีพีเฮดเดอร์ของโทรจันอินเฟคเตอร์

เมื่อติดโทรจัน ชนิดนี้แล้วโทรจันจะติดต่อมาที่พอร์ต 146 โดยจะส่ง ข้อความขอล็อกอิน และ พาสเวิร์ดดังรูปข้างล่าง

```
Client to Server
Client authenticates itslef as being an Infector Client
Hex : 46 43 20 Ascii : FC
Server to Client
Server requests password.
Hex : 57 48 41 54 49 53 49 54 Ascii : WHATISIT
Data Transfered upon Completed Connection <1.6 :
Client to Server
Hex : 46 43 20 Ascii : FC
Server to Client
Hex : 57 48 41 54 49 53 49 54 Ascii : WHATISIT
Attempted Connection :
Source port: 1000<1300
Destination port: 146
Packet size: 62
Packet data:
0000: 44 45 53 54 00 00 20 53 52 43 00 00 08 00 45 00
0010: 00 30 34 1D 40 00 76 06 87 7C C2 6A F1 EF D4 18
0020: C0 BB 04 F8 00 92 00 B8 7B 4E 00 00 00 00 70 02
0030: 20 00 9B FB 00 00 02 04 02 18 01 01 04 02
```

คุณสมบัติ

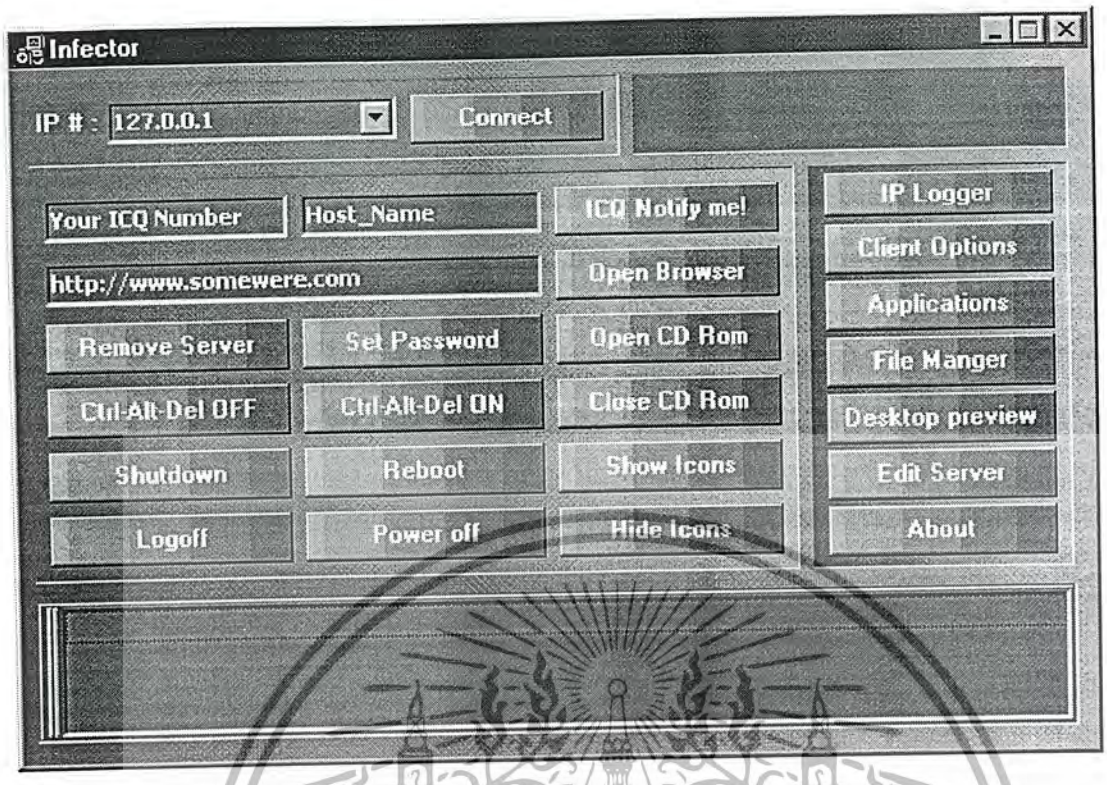
เกี่ยวกับเซิร์ฟเวอร์

–ปิดเซิร์ฟเวอร์,ลบเซิร์ฟเวอร์,เปลี่ยนพาสเวิร์ด

เกี่ยวกับระบบ

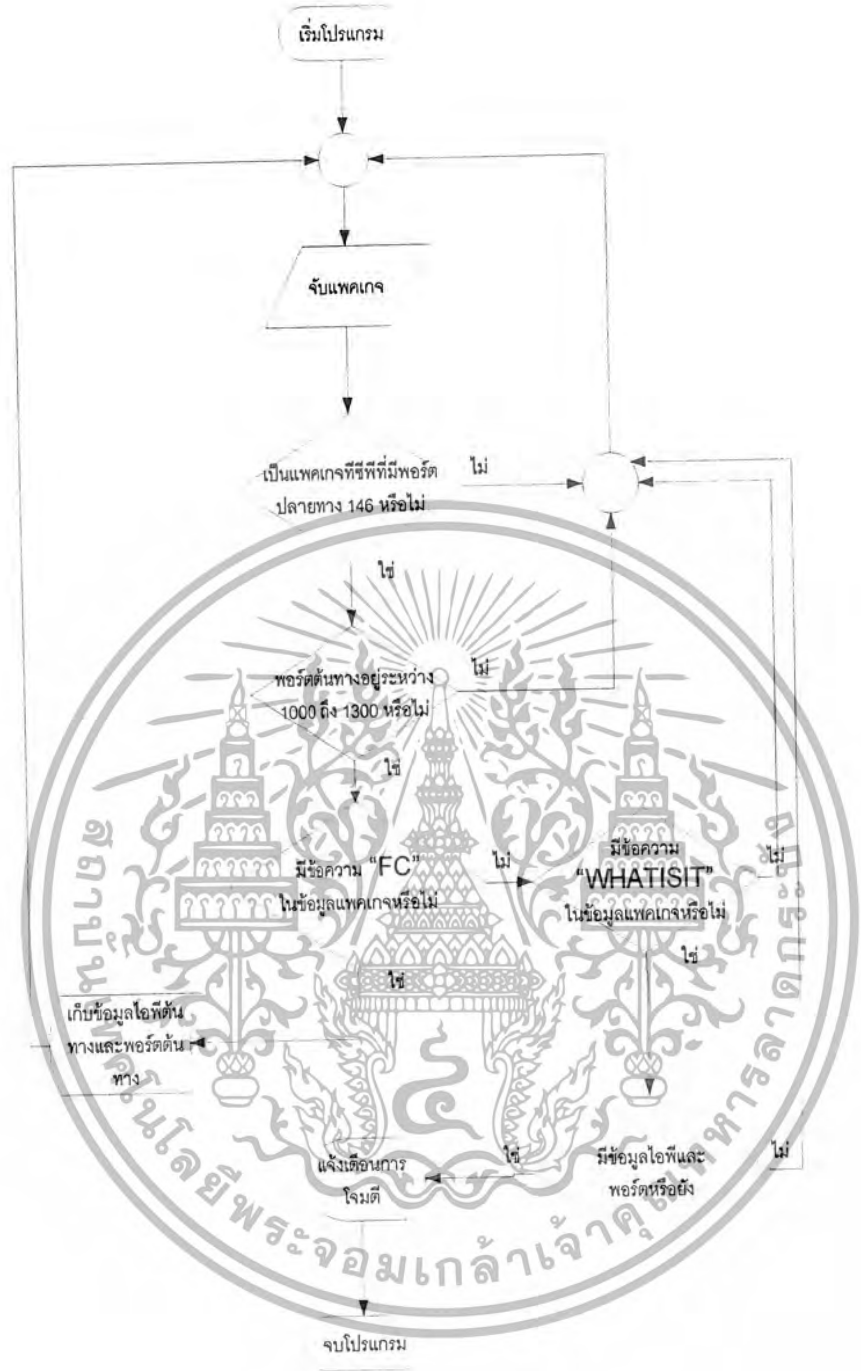
- รีสตาร์ตเครื่อง, ปิดเครื่อง, ล็อกออฟ ขโมยข้อมูล - ข้อมูลเกี่ยวกับเครื่อง, ยูสเซอร์เนม พาสเวิร์ด, ไทม์โซน, บุ๊คมาร์ก และ ไฟล์ที่ได้รับจาก ไอซีคิว, เวอร์ชั่นของวินโดว์, ความเร็วของ ซีพียู,ขโมยข้อมูลในมายด็อคคูเมนต์,ดูในมายเฟเวอร์ริต, คุกกี้,โปรแกรมไฟล์, คุณสมบัติทั่วไป

– เปิด/ปิดซีดีรอม, กด Ctrl+Alt+Del, ซ่อนเดสก์ทอปไอคอน, ซ่อนซิสเต็มคล็อก, ซ่อนซิสเต็มเทรย์, ซ่อนปุ่มสตาร์ท, ซ่อนทาสก์บาร์, ดิสเอเบิล/เอเนเบิลเมาส์, ดิสเอเบิล/เอเนเบิลเดสก์ทอป, ดิสเอเบิล/เอเนเบิลทาสก์บาร์, เปิด/ปิดมอนิเตอร์, เปิด/ปิดสกรอล็อค, เปิด/ปิดนัมล็อค, เปิด/ปิดแค็ปล็อค, เปิดบราวเซอร์, สแกนพอร์ต, ดิสเอเบิล/เอเนเบิลคีย์บอร์ด, สลับปุ่มเมาส์, เปิดหน้าต่างแช็ท, เปิดเอฟทีพีเซอร์เวอร์, พิมพ์ภาพที่สกรีน, เปลี่ยนค่าในรีจิสเตอร์, ควบคุมเมาส์, แสดงกล่องข้อความต่างๆ, เปลี่ยนสีของวินโดวส์



รูปที่ 3.14 แสดงตัวควบคุมเซิร์ฟเวอร์ของโทรจัน อินเฟคเตอร์

หลักการตรวจจับคือ ดูแพคเกจที่ซีพีที่พอร์ตปลายทางเป็นหมายเลข 146 และ ต้นทางอยู่ระหว่าง 1000-1300 จากนั้นตรวจข้อมูลในแพคเกจว่ามี "FC" อยู่หรือไม่ ถ้ามีก็จะทำการเก็บข้อมูลของโฮสต์และพอร์ตไว้ แต่ถ้าไม่มีก็จะทำการตรวจหาข้อความว่า "WHATISIT" ว่ามีอยู่หรือไม่ ถ้ามีแล้วจะทำการตรวจข้อมูลว่าโฮสต์และพอร์ตนี้ได้ทำการส่งข้อมูล "FC" แล้วหรือยัง ถ้าส่งแล้วก็จะทำการแจ้งเตือนการโจมตี



รูปที่ 3.15 โฟล์วชาร์ทแสดงการตรวจจับการบุกรุกแบบอินเฟคเตอร์โทรจัน

3.2.3.6 ซับเซเวนโทรจัน

ชื่อ:Subseven Trojan

ชนิด:ม้าโทรจัน

ชื่ออื่นที่รู้จัก : Backdoor.SubSeven, Backdoor-G, BackDoor-G2, BackDoor-G22, TSB Trojan,

Serbian Badman Trojan, Badman Trojan

ระดับความรุนแรง :ปานกลาง

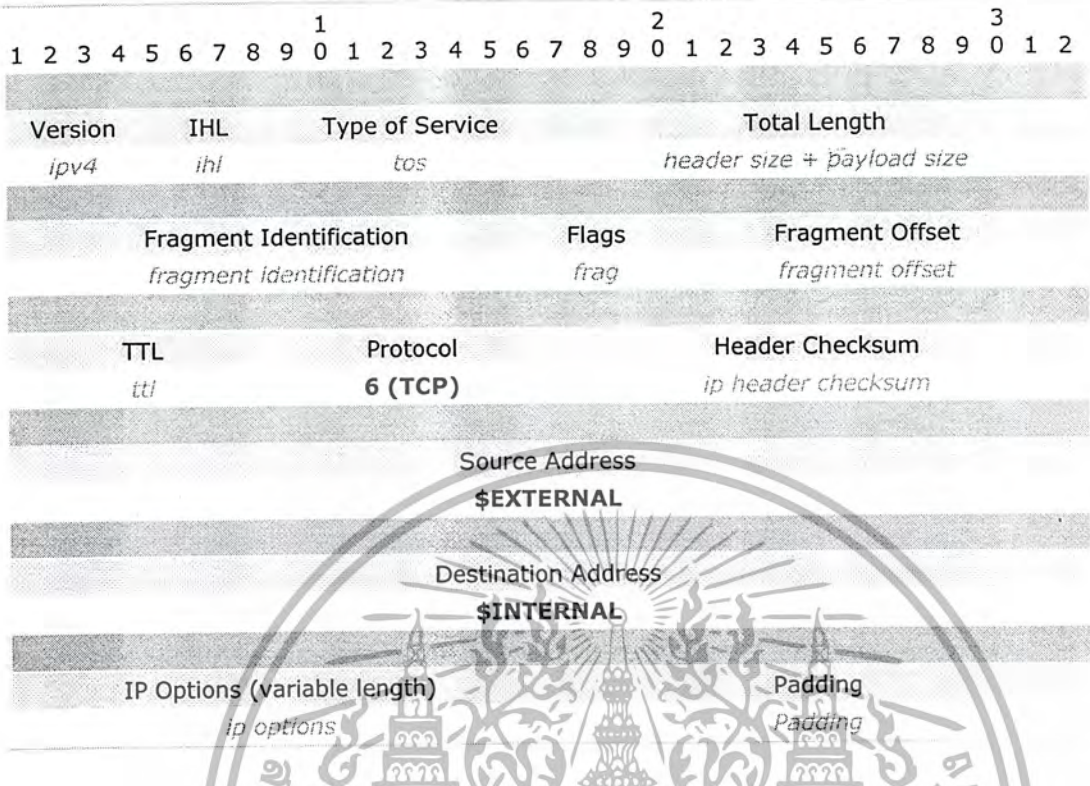
ลักษณะทั่วไป

ซับเซเวน แบ็คดอร์ พบครั้งแรกในเดือนพฟษภาคม 1999 เขียนโดยภาษาเดลไฟ ในเวอร์ชันแรกๆจะส่งไฟล์มาในรูปที่ไม่เป็นแพ็กเก็ต แต่ในเวอร์ชั่นหลังๆจะมาในรูปที่เป็นแพ็กเก็ตทำให้ยากต่อการตรวจสอบของโปรแกรมแอนตี้ไวรัสทั่วไปที่ไม่มีไฟล์วิน32 แอสแพ็ค(Win32 Aspack) เพื่อใช้ในการแตกไฟล์ออกมา ซับเซเวนมักจะแพร่กระจายผ่านจดหมายข่าวและทางอีเมล์ เมื่อรันไฟล์ของซับเซเวน จะได้ไฟล์ WATCHING.DLL ไปเขียนทับในรีจิสทรีย์คีย์ เมื่อโพรเซสของซับเซเวนรันในหน่วยความจำ(จะไม่เห็นในทาสก์ เมเนเจอร์) มันจะคอยมองหาพอร์ตทีซีพี/ไอพีที่เปิดไว้ เพื่อรับคำสั่งจากเครื่องไคลเอนต์ ดังนั้นซับเซเวนจะไม่มีพอร์ตที่แน่นอนในการรับส่งข้อมูลกับเครื่องไคลเอนต์

ไฟล์ที่พบ

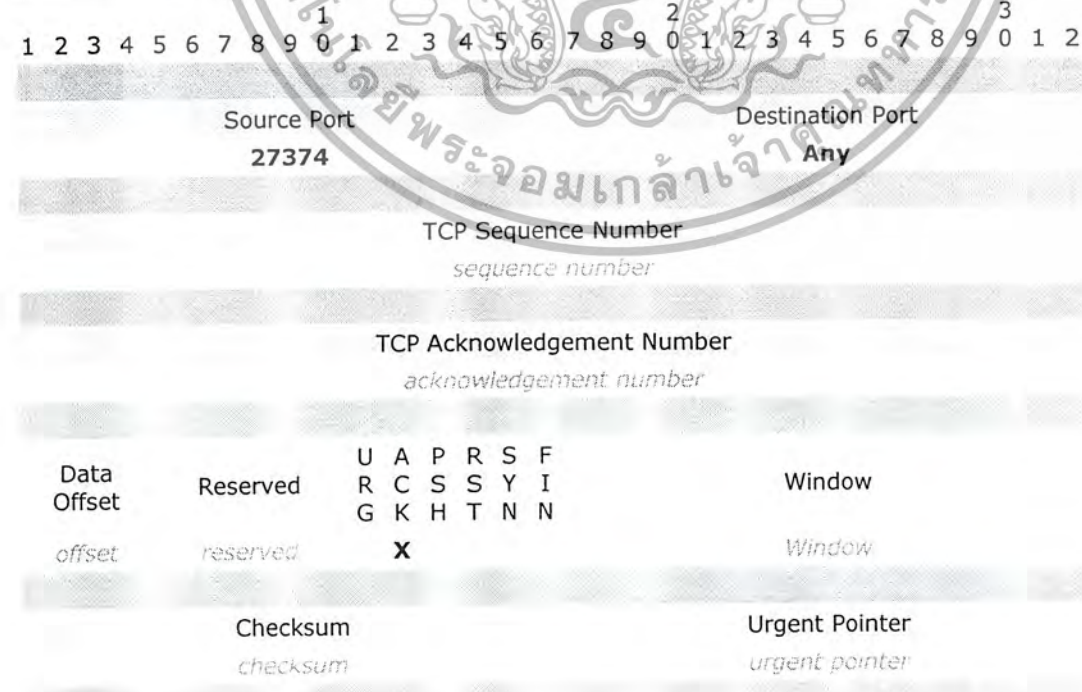
SubSeven2.2b.zip – 1,091,948 bytes SubSeven2.2b.zip – 174,905 bytes S722beta1.zip – 1,080,665 bytes Subseven2.2.zip – 2,914,603 bytes Newserver22.zip – Sub72.1unpk.zip – 482,324 bytes Sub72.2bnt.zip – 56,311 bytes Sub72.2.zip – S722.zip – Ss22.zip – Win3000.zip – 7,151 bytes Weed_skin.zip – 4,016 bytes Server.exe – 55,808 bytes Server.exe – 57,892 bytes Server.exe – 57,912 bytes Sub7.exe – 316,928 bytes Sub7.exe – 2,254,848 bytes Editserver.exe – 227,840 bytes Editserver.exe – 389,632 bytes Sin.exe – 225,792 bytes Sin.exe – 250,880 bytes Msrexe.exe – Run.exe – Windos.exe – Mueexe.exe – Ruoy.exe – Setup.cgi – 15,562 bytes Subseven.cgi – 43,920 bytes Capture.dll – 53,760 bytes Icqmapi.dll – 58,880 bytes Icqpwsteal.dll – 145,920 bytes Matrix.dll – 142,848 bytes Packet32.dll – 5,632 bytes S7advanced.dll – 174,592 bytes S7capture.dll – 90,624 bytes S7fun1.dll – 166,912 bytes S7fun2.dll – 36,352 bytes S7keys.dll – 53,248 bytes S7moreinfo.dll – 146,944 bytes S7passwords.dll – 49,664 bytes S7scanner.dll – 142,336 bytes S7sniffer.dll – 129,200 bytes S7takeover.dll – 59,392 bytes Watching.dll – Commands.cfg – 1,681 bytes Commands.cfg – 11,479 bytes Menu.cfg – 1,218 bytes Menu.cfg – 2,852 bytes Pages.cfg – 11,413 bytes Predefined.cfg – 4,458 bytes S7config.cfg – 721 bytes S7config.cfg – 2,117 bytes Zpacket.vxd – 11,380 bytes Subseven.set – 26 bytes Subseven.mem – Subseven.log – Subseven.ban –

IP HEADER



รูปที่ 3.16 แสดงไอพีเฮดเดอร์ของโทรจันซับเซเวน

TCP Packet Header



รูปที่ 3.17 แสดงทีซีพีเฮดเดอร์ของโทรจันซับเซเวน

ซับเซเวนจะสุ่มพอร์ตที่เปิดอยู่เพื่อใช้ติดต่อกับเครื่องไคลเอนต์เพื่อให้ยากในการตรวจสอบแต่จะมีลักษณะพิเศษ(signature)ในข้อมูลที่ส่งมาดังรูป

```
Banner :
< 00000000 0d0a5b52504c5d30 30320d0a          # ..[RPL]002..
```

คุณสมบัติ

คุณสมบัติทั่วไป

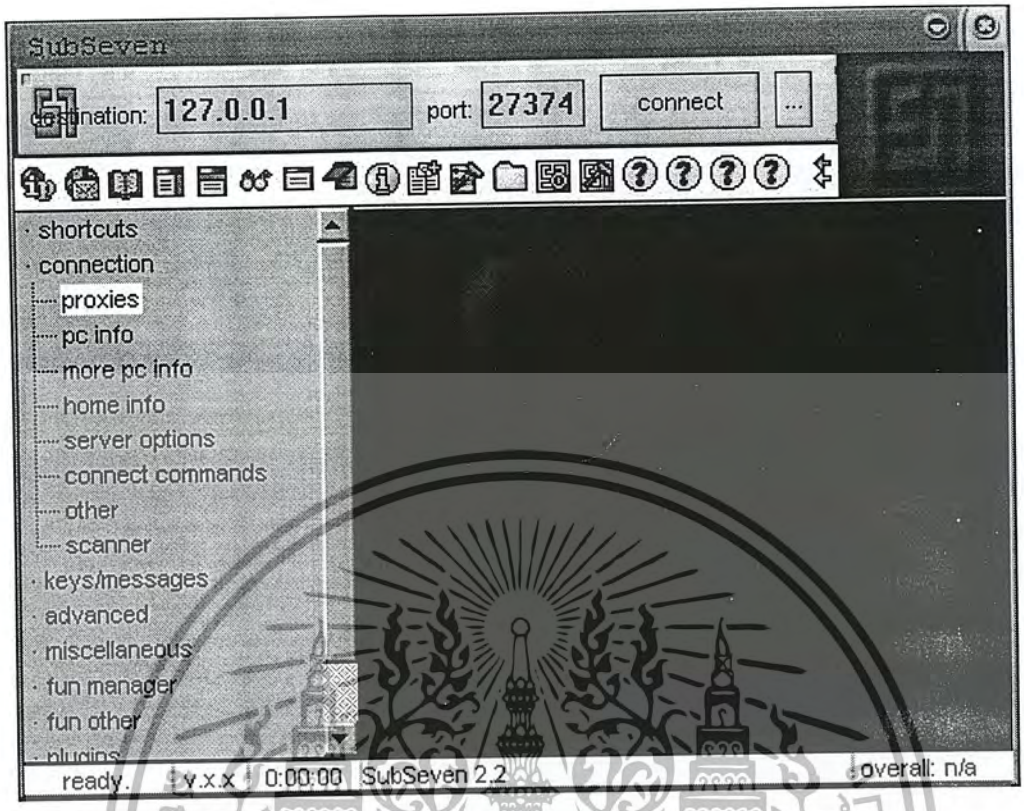
- เปิดเบราเซอร์โดยสามารถสั่งให้ไปที่ที่ต้องการได้
- รีสตาร์ทวินโดวส์
- สลับปุ่มของเมาส์
- ซ่อนเมาส์
- ตั้งค่าของเสียงใหม่
- อัดเสียงจากรีโมตไมโครโฟน
- เปลี่ยนสีของวินโดวส์
- ตัดการเชื่อมต่ออินเตอร์เน็ต
- เปลี่ยนวัน เวลา
- เปลี่ยนค่าความละเอียดของจอ
- ซ่อน/แสดงไอคอนบนเดสก์ทอป
- ซ่อน/แสดงปุ่มสตาร์ท
- ซ่อน/แสดงทาสก์บาร์
- เปิด/ปิดซีดีรอม
- เปิด/ปิดจอ
- ดิสเอเบิล/เอเนเบิล CTRL+ALT+DEL
- เปิด/ปิด สกรอลล็อค แค็ปล็อค นัมล็อค
- ดิสเอเบิลคีย์บอร์ด

คุณสมบัติเกี่ยวกับการเชื่อมต่อ

- ปิด/เปิด การเชื่อมต่ออินเตอร์เน็ต
- สแกนไอพี
- ดูชื่อเครื่อง ยูสเซอร์เนม
- ดูชื่อโฟลเดอร์ในซิสเต็ม
- ดูเวอร์ชั่นของวินโดวส์
- ดูค่าความละเอียดของจอ
- ดูเวอร์ชั่นของ ไดเร็คเอ็กซ์
- ดูผู้ผลิตซีพียูและความเร็ว
- ดูขนาดของฮาร์ดดิสก์ และพื้นที่ว่าง
- เปลี่ยนพอร์ตของเซิร์ฟเวอร์
- อัพเดทเซิร์ฟเวอร์
- ปิด/ลบ เซิร์ฟเวอร์
- ส่งข้อความวินโดวส์(Windows Popup message)
- เปลี่ยนค่าในรีจิสทรีย์
- ลบพาสเวิร์ด
- เปิดเอฟทีพีเซิร์ฟเวอร์
- ส่งเท็กซ์ไฟล์ไปที่พรินเตอร์

คุณสมบัติเกี่ยวกับไฟล์

- หาไฟล์ที่ต้องการ
- เอ็กซีคิวต์ไฟล์
- ลบไฟล์
- เซ็ทพาธ
- ดาวน์โหลด อัพโหลดไฟล์
- เล่นไฟล์*.WAV
- พรินท์ไฟล์เท็กซ์
- ฯลฯ



รูปที่ 3.18แสดงตัวควบคุมเซิร์ฟเวอร์ของโทรจันซับเซเวน

วิธีการตรวจจับคือ ดูว่าแพคเกจที่ได้รับมีพอร์ตต้นทางหมายเลข 27374 หรือไม่ และตรวจว่าในแพคเกจมีรูปแบบในแพคเกจตามที่กำหนดหรือไม่ ถ้าใช่ก็จะทำการแจ้งการตรวจจับ

รูปที่ 3.19 โฟล์วชาร์ทแสดงการตรวจจับการบุกรุกแบบซับเซเวนโทรจัน

3.2.3.7 แซสเซอร์เวอร์ม

ชื่อ : W32.Sasser.Worm

ชนิด : หนอนอินเทอร์เน็ต (worm)

ชื่ออื่นที่รู้จัก : W32/Sasser.worm, WORM_SASSER.A, Sasser

ระดับความรุนแรง : ปานกลาง

ระบบปฏิบัติการที่มีผลกระทบ : วินโดวส์ 2000(Windows 2000),วินโดวส์ เอ็กซ์พี(Windows XP)

ระบบปฏิบัติการที่ไม่มีผลกระทบ : ลินุกซ์(Linux),แมคอินทอช(Macintosh),โนเวลล์ เน็ตแวร์(Novell Netware),โอเอส ทู(OS/2), ยูนิกซ์(UNIX), วินโดวส์ 95(Windows 95),วินโดวส์ 98(Windows 98), วินโดวส์ เอ็มอี(Windows Me),วินโดวส์ เอ็นที(Windows NT),วินโดวส์ เซิร์ฟเวอร์ 2003(Windows Server 2003)

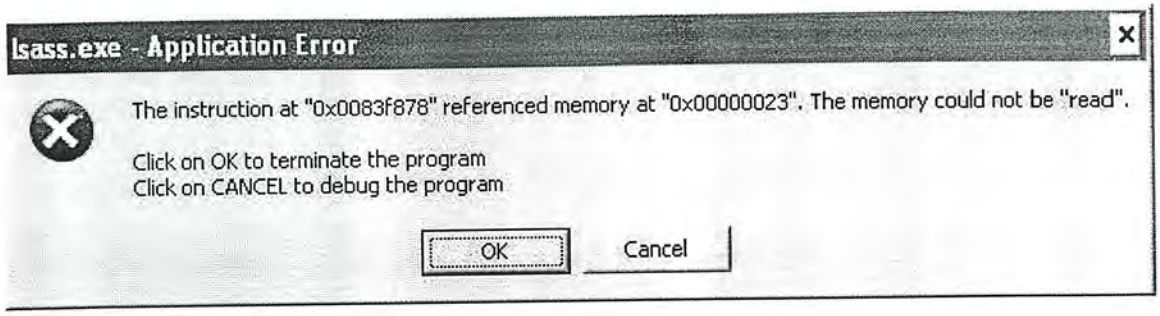
ข้อมูลทั่วไป

W32.Sasser.Worm หนอนชนิดนี้จัดเป็นโปรแกรมประเภท เอ็กซ์พลออิท(Exploit) ที่จะโจมตีช่องโหว่ของ Windows LSASS หรือ MS04-011 ผ่านพอร์ต 445/ทีซีพี นอกจากนี้หนอนยังสามารถดาวน์โหลดและรันตัวเองด้วยโปรแกรม เอฟทีพี ผ่านพอร์ต 5554/ทีซีพี ซึ่งไฟล์ของหนอนชนิดนี้มีชื่อว่า avserve.exe

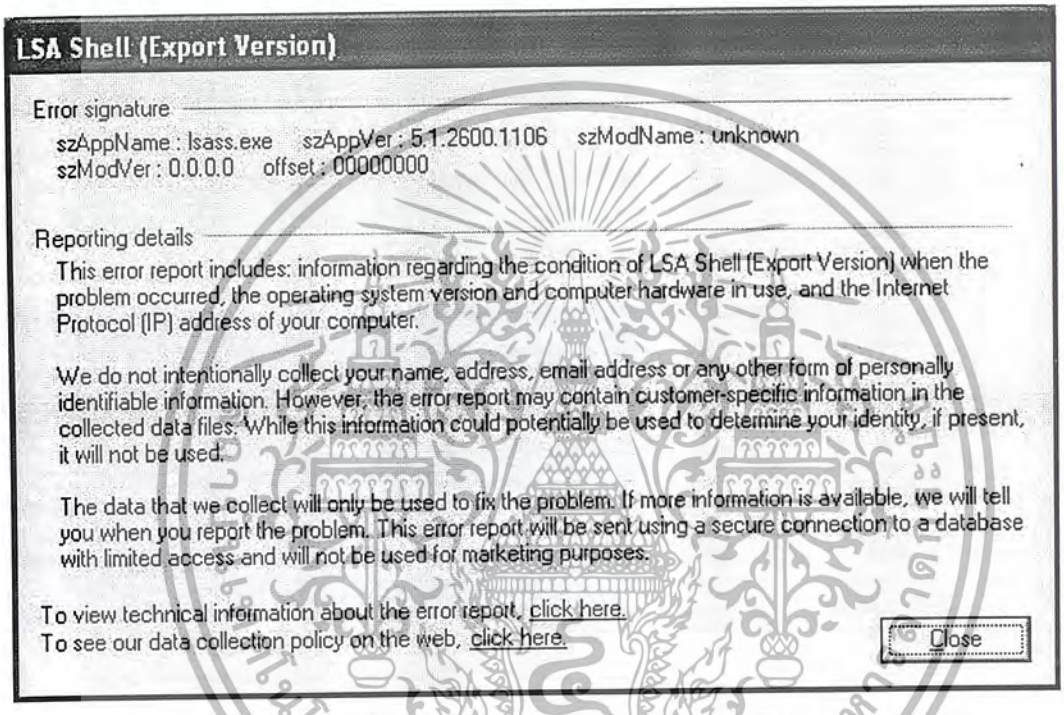
- พอร์ต 445/ทีซีพี เพราะเป็นพอร์ตที่หนอนใช้ในการโจมตี
- พอร์ต 5554/ทีซีพี เป็นพอร์ตที่ใช้ในการดาวน์โหลดไฟล์ของหนอนด้วยโปรแกรม เอฟทีพี
- พอร์ต 9996/ทีซีพี เป็น รีโมต เชล(Remote shell) ที่ถูกเปิดโดยโปรแกรมประเภท เอ็กซ์พลออิท ที่โจมตีช่องโหว่ Windows LSASS

จากรายงานที่ได้รับ เมื่อหนอนชนิดนี้รันตัวเองแล้ว จะส่งผลให้เครื่องปิดเองโดยอัตโนมัติ คล้ายกับผลกระทบที่เกิดจาก W32.Blaster.Worm

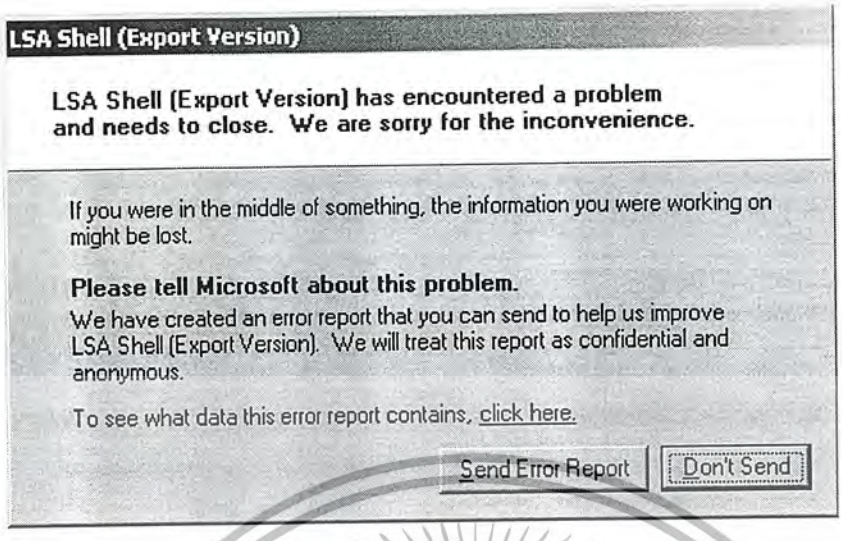
จากนั้นหนอนก็จะพยายามทำการแพร่กระจายตัวโดยสุ่มหมายเลข ไอพี เพื่อหาเครื่องคอมพิวเตอร์ที่ยังไม่ได้ทำการอัพเดต แพช(patch) MS04-011



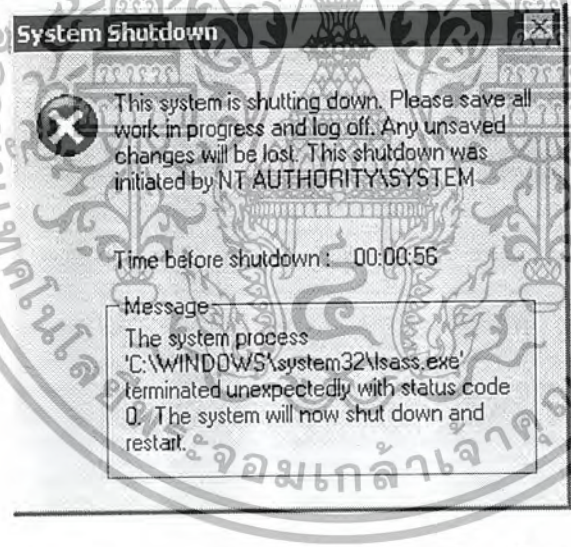
รูปที่3.20 แสดงผลหลังจากหนอนชนิดนี้แพร่กระจายในเครื่อง วินโดวส์เอ็กซ์พี



รูปที่3.21 แสดงผลหลังจากหนอนชนิดนี้แพร่กระจายในเครื่องวินโดวส์เอ็กซ์พี



รูปที่3.22 แสดงผลหลังจากหนอนชนิดนี้แพร่กระจายในเครื่อง วินโดวส์ 2000



รูปที่3.23 แสดงผลหลังจากหนอนชนิดนี้แพร่กระจายในเครื่องวินโดวส์ 2000

วิธีการแพร่กระจาย

หนอนชนิดนี้สามารถแพร่กระจายโดยเริ่มจากทำการค้นหาเครื่องตามหมายเลข ไอพี ที่ยังไม่ได้ทำการอัพเดต แพช เพื่ออุดช่องโหว่ของ Windows LSASS หรือ MS04-011 เมื่อพบแล้วหนอนจะทำการโจมตีผ่านช่องโหว่ดังกล่าวโดยใช้วิธีการทำให้บัฟเฟอร์ล้น ใน LSASS.EXE ส่งผลทำให้มีการ

เปิดพอร์ต 9996/ทีซีพี จากนั้นหนอนจะสร้างสคริปต์ชื่อ cmd.ftp เพื่อเปิดพอร์ต 5554/ทีซีพี ใช้ในการดาวน์โหลดและรันไฟล์ของหนอนเอง

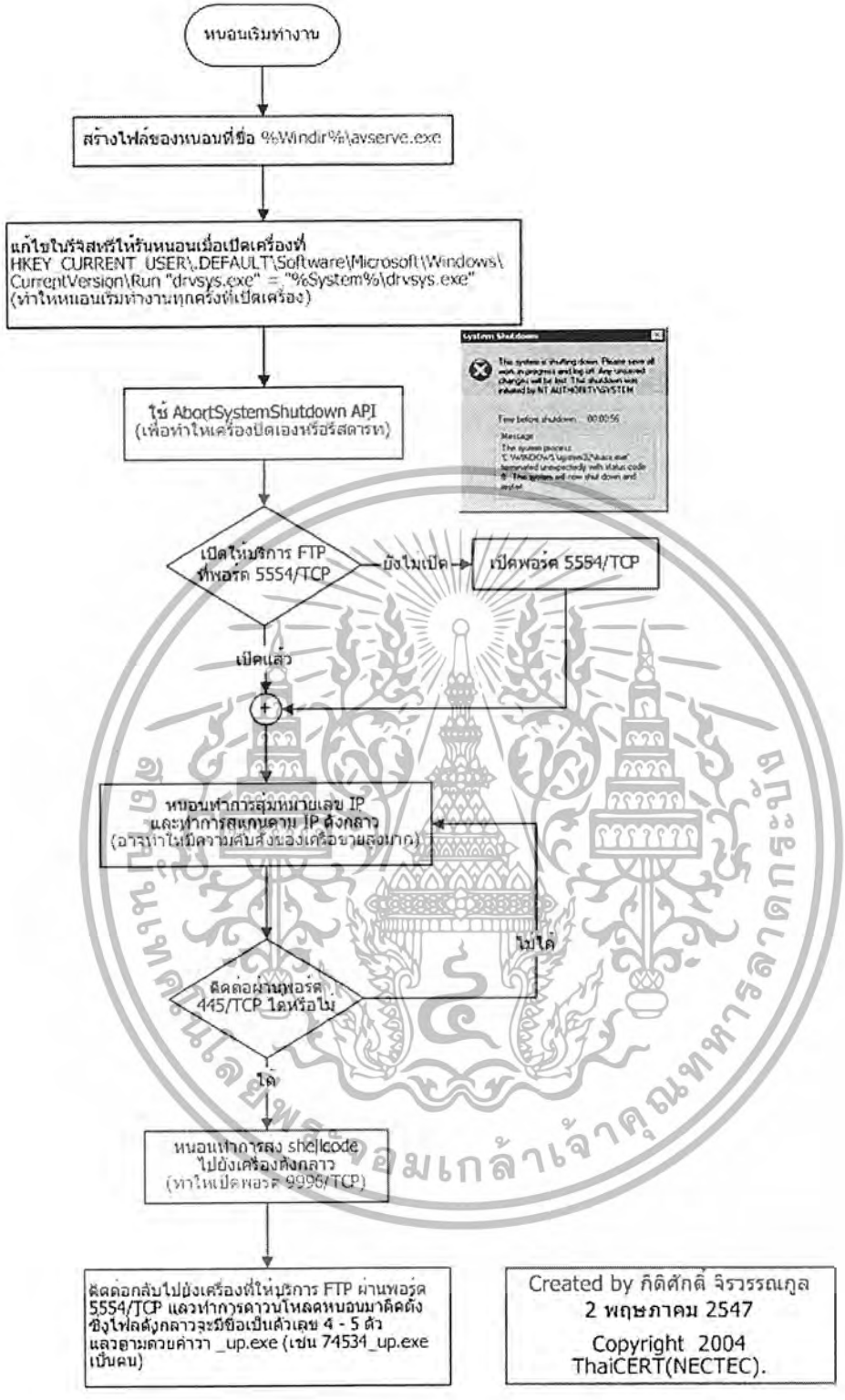
```
0000 63 68 6F 20 6F 66 66 26 65 63 68 6F 20 6F 70 65 cho off&echo ope
0010 6E 20 36 38 2E 31 34 34 2E 36 35 2E 38 30 20 35 n 68.144.65.80 5
0020 35 35 34 3E 3E 63 6D 64 2E 66 74 70 26 65 63 68 554>>cmd.ftp&ech
0030 6F 20 61 6E 6F 6E 79 6D 6F 75 73 3E 3E 63 6D 64 o anonymous>>cmd
0040 2E 66 74 70 26 65 63 68 6F 20 75 73 65 72 26 65 .ftp&echo user&e
0050 63 68 6F 20 62 69 6E 3E 3E 63 6D 64 2E 66 74 70 cho bin>>cmd.ftp
0060 26 65 63 68 6F 20 67 65 74 20 31 35 30 38 39 5F &echo get 15089_
0070 75 70 2E 65 78 65 3E 3E 63 6D 64 2E 66 74 70 26 up.exe>>cmd.ftp&
0080 65 63 68 6F 20 62 79 65 3E 3E 63 6D 64 2E 66 74 echo bye>>cmd.ft
0090 70 26 65 63 68 6F 20 6F 6E 26 66 74 70 20 2D 73 p&echo on&ftp -s
00A0 3A 63 6D 64 2E 66 74 70 26 31 35 30 38 39 5F 75 :cmd.ftp&15089_u
00B0 70 2E 65 78 65 26 65 63 68 6F 20 6F 66 66 26 64 p.exe&echo off&d
00C0 65 6C 20 63 6D 64 2E 66 74 70 26 65 63 68 6F 20 el cmd.ftp&echo
00D0 6F 6E 0A                                        on.
```

ผลกระทบที่เกิดขึ้น

- เครื่องอาจทำงานผิดพลาด : เนื่องจากหนอนจะแก้ไขไฟล์และรีจิสทรี ทำให้เครื่องทำงานผิดพลาดได้
- เปิดการเชื่อมต่อที่ผิดปกติ : หนอนจะสร้างพอร์ตที่ใช้ในการเชื่อมต่อ 5554/ทีซีพี และ 9996/ทีซีพี
- ไม่สามารถใช้งานเครือข่ายได้ : เพราะว่าหนอนจะสแกนหา ไอพี เพื่อทำการแพร่กระจาย ทำให้มีความคับคั่งของข้อมูลในเครือข่ายสูงมาก จนไม่สามารถใช้งานได้

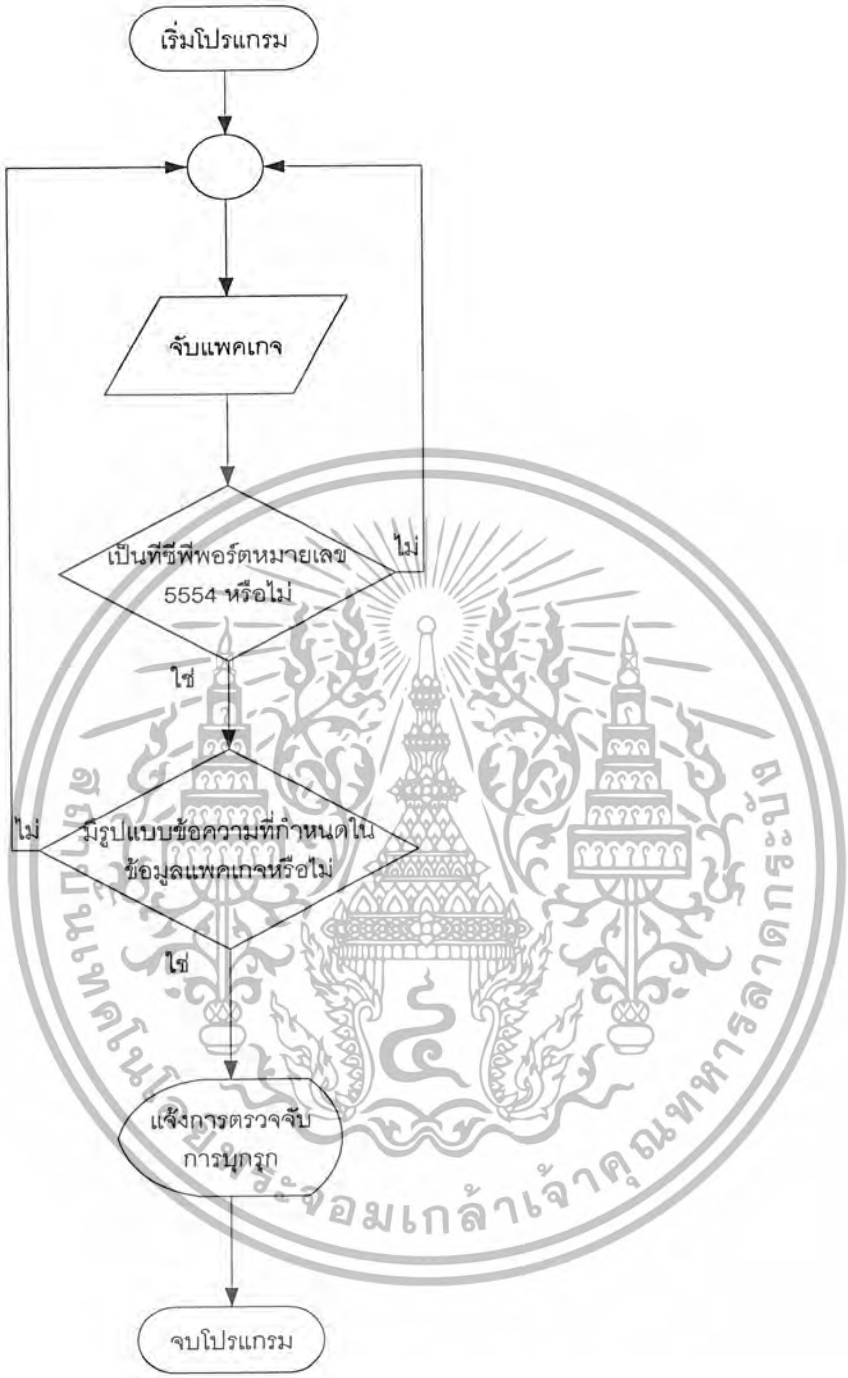
รายละเอียดทางเทคนิค

เมื่อหนอน W32.Sasser.Worm ถูกเอ็กซิคิวต์ จะมีกระบวนการดังนี้



รูปที่ 3.24 แสดงการทำงานของเวิร์ม แซสเซอร์

วิธีตรวจจับคือ ดูว่าเป็นแพคเกจทีซีพีที่มีพอร์ตปลายทางหมายเลข 5554 หรือไม่ และ มีรูปแบบข้อมูลเหมือนกับที่กำหนดไว้หรือไม่ ถ้ามีก็จะทำการแจ้งเตือนการตรวจจับ



รูปที่ 3.25 โฟล์วชาร์ทแสดงการตรวจจับการบุกรุกแบบแซสเซอร์เวอร์ม

3.2.3.8 เอสคิวแอล แสลมเมอร์ เวอร์ม

ชื่อ : W32.SQLExp.Worm

ชนิด : หนอนอินเทอร์เน็ต (worm)

ชื่ออื่นที่เป็นที่รู้จัก : SQL Slammer Worm, DDOS.SQLP1434.A, W32/SQLSlammer

ระดับความรุนแรง : สูง

ลักษณะทั่วไป

มีผลกระทบต่อเครื่องที่ติดตั้ง

1. ไมโครซอฟท์ เอสคิวแอล เซิร์ฟเวอร์ 2000 (Microsoft SQL Server 2000)
2. ไมโครซอฟท์ เดสทอป เอ็นจิน2000(Microsoft Desktop Engine (MSDE) 2000) ที่ไม่ได้ติดตั้ง Service Pack 2 และ 3

W32.SQLExp.Worm เป็นหนอนที่มุ่งโจมตีและมีผลกระทบเฉพาะเครื่องเซิร์ฟเวอร์ที่รันไมโครซอฟท์ เอสคิวแอล เท่านั้น หนอนชนิดนี้ทำงานอยู่ในหน่วยความจำเท่านั้นไม่ทำงานในฮาร์ดดิสก์ ดังนั้นจึงทำให้โปรแกรมป้องกันไวรัสไม่สามารถตรวจจับได้หนอนชนิดนี้ทำการส่งข้อมูลขนาด 376 ไบต์ไปยังพอร์ต 1434/ยูดีพี (เป็นพอร์ตบริการ เอสคิวแอลเซิร์ฟเวอร์ รีโซลูชัน (SQL Server Resolution Service Port) เป็นพอร์ตสำหรับมอนิเตอร์(Monitor port)ใช้สำหรับให้ไคลเอนต์ตรวจสอบว่าสามารถติดต่อกับเซิร์ฟเวอร์ได้หรือไม่) เป็นจำนวนมาก ระหว่างเครื่องเซิร์ฟเวอร์ที่ให้บริการ เอ็มเอส-เอสคิวแอล(MS-SQL) ทำให้ระบบเครือข่ายใช้งานไม่ได้ เป็นการโจมตีแบบปฏิเสธการให้บริการ(Denial of Service (DoS)) โดยแพ็คเก็ตที่ใช้ในการโจมตีมีลักษณะดังนี้

1.แบบสแต็กเบส(Stack base Buffer overflow)

เมื่อ เอสคิวแอล เซิร์ฟเวอร์รับแพ็คเก็ตจากพอร์ต ยูดีพี 1434 โดยไบต์แรกเซ็ตให้เป็น 0x04 ตามด้วยสตริงจำนวนมากจนมีขนาด 376 ไบต์ SQL เซิร์ฟเวอร์ ก็จะพยายามที่จะเปิดมันโดย 0x04 เป็นคำสั่งในการเปิด

HKLM\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion

โดยการเพิ่มขนาดของแพ็คเก็ต ในขณะที่สแต็คมีพื้นที่แค่ 64 ไบต์ จึงเกิดบัฟเฟอร์ โอเวอร์โฟลวแบบสแต็กเบสขึ้น ต่อมาโพรเซสเซอร์ก็จะเอ็กซีคิวต์ โคด ของผู้บุกรุกโดยไม่ต้องมีการยืนยัน (Authentication)

2.แบบฮีปเบส(Heapbase Buffer overflow)

เมื่อ เอสคิวแอล เซิร์ฟเวอร์รับแพ็คเก็ตจากพอร์ต ยูดีพี 1434 โดยไบต์แรกเซ็ตให้เป็น 0x08 ตามด้วยสตริงขนาดยาวมากๆ ตามด้วยเครื่องหมายโคลอน (:) และตามด้วยตัวเลข บัฟเฟอร์ โอเวอร์โฟลวก็จะเกิดขึ้น แต่จะนำข้อมูลที่เกินมาไปเก็บไว้ในตำแหน่งที่ตัวเลขกำหนดไว้ แต่ถ้าไม่มีเครื่องหมายโคลอน และตัวเลข จะทำให้ไม่สามารถนำข้อมูลไปเก็บไว้ที่อื่นได้ จึงเกิดโอเวอร์โฟลวแบบฮีปเบสขึ้น

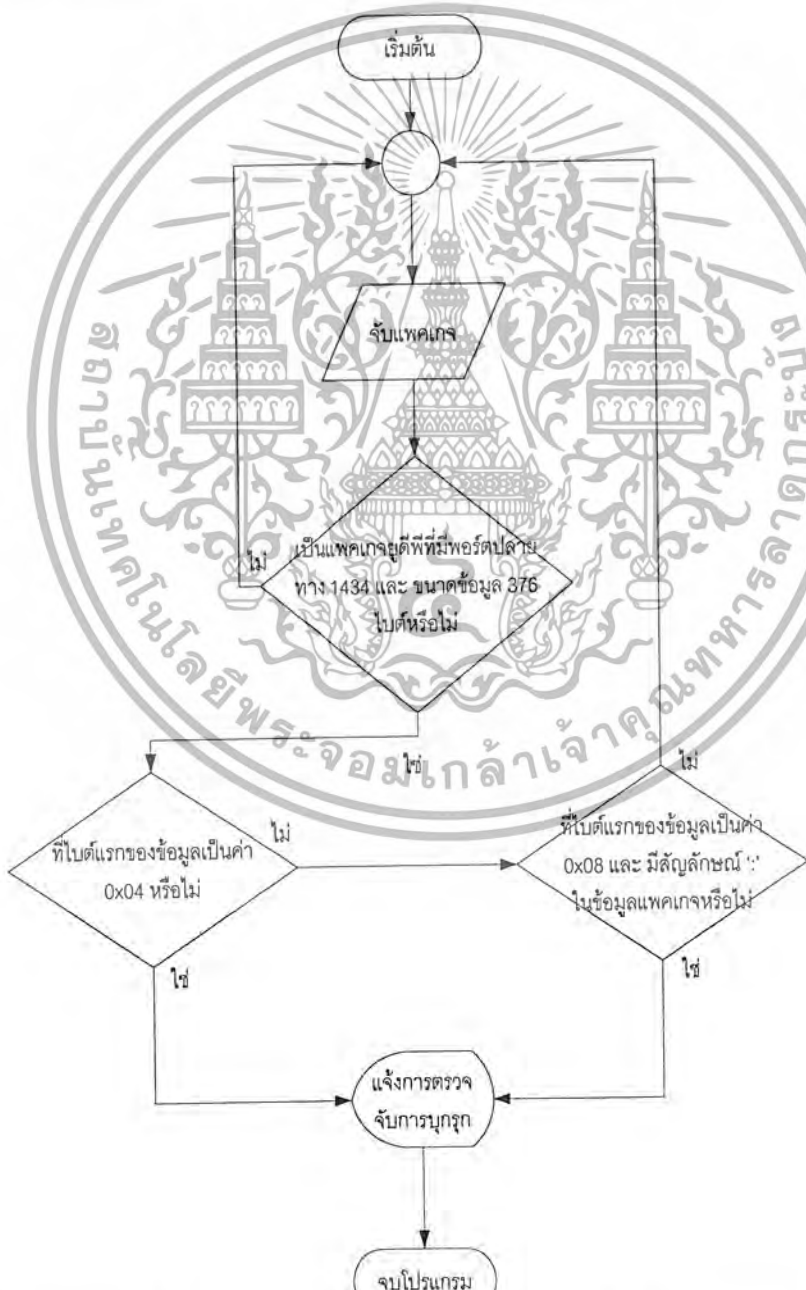
รายละเอียดทางเทคนิค

เมื่อหนอน W32.SQLExp.Worm ติดเครื่องแล้วจะมีการทำงานดังนี้

1. เปิดซ็อกเก็ตของ เน็ตไบออส(netbios) เพื่อให้หนอนทำการส่งแพ็กเก็ต
2. ใช้งานฟังก์ชั่น เอพีไอ(API) ของวินโดวส์ ที่ชื่อ เก็ททิคเคาท์(GetTickCount) เพื่อที่จะสุ่มหมายเลข ไอพี สำหรับการส่งหนอน
3. ทำการส่งตัวหนอนเองไปยังทุก ไอพี ที่สุ่มขึ้นผ่านทางพอร์ต 1434/ยูดีพี ทำให้เกิดความคับคั่งของเน็ตเวิร์กจำนวนมาก

รูปที่3.26 แสดงปริมาณการแพร่กระจายของของเวิร์ม เอสคิวแอล สแลมเมอร์

หลักการตรวจจับคือ ดูแพคเกจยูดีพีที่มีพอร์ตปลายทางหมายเลข 1434 และส่วนข้อมูลมีขนาด 376 ไบต์หรือไม่ ถ้าใช่ก็จะทำการตรวจข้อมูลในแพคเกจที่ไบต์แรกว่าเป็นค่า 0x04 หรือ 0x08 หรือไม่ถ้าเป็น 0x04 จะพบว่าเป็นการโจมตีแบบแสตกโอเว่อร์โฟลว์แล้วจะทำการแจ้งเตือน แต่ถ้าพบ 0x08 จะทำการตรวจต่อไปอีกว่าในข้อมูลมี ':' อยู่หรือไม่ ถ้าไม่มีจะพบว่าเป็นการโจมตีแบบฮีปโอเว่อร์โฟลว์ แล้วจะทำการแจ้งเตือน



รูปที่ 3.27 โฟล์วชาร์ทแสดงการตรวจจับการบุกรุกแบบเอสคิวแอล สแลมเมอร์เวอร์ม

3.2.3.9นาชิเวอร์ม

ชื่อ : W32.Nachi.Worm

ชนิด : หนอนอินเทอร์เน็ต (worm)

ชื่ออื่นที่รู้จัก : W32/Welchia.worm10240 , W32/Nachi.worm, WORM_MSBLAST.D, Lovsan.D, W32.Welchia.Worm, W32/Nachia.worm

ระดับความรุนแรง : สูง

ลักษณะทั่วไป

W32.Nachi.Worm หนอนชนิดนี้จัดเป็นโปรแกรมประเภทเอ็กซ์พลออิท(Exploit) ที่จะโจมตีช่องโหว่ของ ดีคอม อาร์พีซี(DCOM RPC) (Windows Distributed Component Object Model Remote Procedure Call) หรือ MS03-026 ซึ่งจะคล้ายกับหนอนชื่อ W32.Blaster.Worm ที่มีการโจมตีผ่านช่องโหว่ของ DCOM RPC ผ่านพอร์ต TCP/135 และหนอนชนิดนี้ยังเน้นโจมตีไปยังระบบปฏิบัติการวินโดวส์ XP มากที่สุด

หนอนจะพยายามดาวน์โหลด แพช โปรแกรม อาร์พีซี(RPC) จากเว็บไซต์ของไมโครซอฟต์ และติดตั้ง จากนั้นทำการรีสตาร์ทเครื่อง

จุดเด่นของหนอนชนิดนี้คือ จะทำการหาเครื่องที่จะแพร่กระจายต่อไปโดยการส่งแพ็กเก็ต ไอซีเอ็มพี ซึ่งส่งผลให้ความคับคั่งของข้อมูล ไอซีเอ็มพี เพิ่มขึ้นมาก

และหนอนชนิดนี้พยายามที่จะกำจัดหนอน W32.Blaster.Worm ด้วย

วิธีการแพร่กระจาย

หนอนชนิดนี้สามารถแพร่กระจายโดยอาศัยการโจมตีช่องโหว่ของไมโครซอฟต์วินโดวส์ และค้นหาเครื่องตามหมายเลข ไอพี ที่เปิดพอร์ต 135/ทีซีพี เมื่อค้นพบหนอนจะส่ง ไอซีเอ็มพี เพื่อตรวจสอบเครื่องที่จะโจมตีว่ายังอยู่ในเครือข่ายหรือไม่ เมื่อเครื่องดังกล่าว ตอบกลับ หนอนจะส่งโปรแกรมที่เป็นเอ็กพลออิท จากนั้นหนอนจะสร้าง รีโมทเชลล์ เปิดพอร์ต ทีซีพี/707 รอคำสั่งที่จะให้ดาวน์โหลดตัวหนอนผ่านโปรแกรม ทีเอฟทีพี

รายละเอียดทางเทคนิค

เมื่อหนอน W32.Nachi.Worm ถูกเอ็กซิคิวต์ หนอนจะมีกระบวนการดังนี้

1. คัดลอกตัวหนอนเองไปยัง %System%\Wins\Dllhost.exe

   หมายเหตุ %System% เป็นตัวแปร แทนโฟลเดอร์ System โดยทั่วไปแล้วจะอยู่ที่ C:\Windows\System สำหรับระบบปฏิบัติการวินโดวส์ 95/98/เอ็มอี ส่วน C:\Winnt\System32 สำหรับระบบปฏิบัติการวินโดวส์ เอ็นที/2000 และ C:\Windows\System32 สำหรับระบบปฏิบัติการวินโดวส์ เอ็กซ์พี

2. คัดลอกไฟล์ %System%\Dllcache\Tftpd.exe ไปเป็นไฟล์ %System%\Wins\svchost.exe ซึ่ง Svchost.exe เป็นโปรแกรมที่มาพร้อมกับระบบปฏิบัติการ อาจทำให้โปรแกรมป้องกันไวรัสไม่สามารถตรวจจับได้
3. สร้าง บริการ ต่อไปนี้

   Service Name: RpcTftpd
   Service Display Name: Network Connections Sharing
   Service Binary: %System%\wins\svchost.exe

   Service Name: RpcPatch
   Service Display Name: WINS Client
   Service Binary: %System%\wins\dllhost.exe

   บริการเหล่านี้ถูกตั้งค่าไว้ให้เริ่มทำงานโดยอัตโนมัติ

4. กำจัดหนอน W32.Blaster.Worm โดยการหยุดการทำงานของโพรเซสที่ชื่อ Msblast.exe และลบไฟล์ %System%\msblast.exe ที่ถูกปล่อยโดยหนอน W32.Blaster.Worm
5. หนอนจะค้นหาเป้าหมายจากหมายเลข IP ด้วยวิธีที่แตกต่างกัน 2 วิธี คือ
   - หนอนจะนับเพิ่มจาก A.B.0.0 ถ้าเครื่องที่หนอนชนิดนี้คุกคามมีหมายเลข IP เป็น A.B.C.D
   - หนอนจะสร้างหมายเลข IP โดยการสุ่มจาก hard-coded addresses หลังจากเลือกหมายเลข IP เริ่มต้นได้แล้ว หนอนจะทำการนับเพิ่มไปเรื่อยๆ และค่าจะอยู่ในช่วงของเน็ตเวิร์กคลาสซี ยกตัวอย่างเช่น ถ้าเริ่มต้นที่ A.B.0.0 หมายเลข IP จะเพิ่มขึ้นไปเรื่อยๆ จนถึง A.B.255.255

6. จากนั้นหนอนจะทำการตรวจสอบเครื่องที่หนอนคำนวนหมายเลข IP โดยการส่งแพ็กเก็ต ไอซีเอ็มพี หรือเรียกว่าปิง นั่นเอง และเมื่อหนอนพบว่ามีเครื่องยังอยู่ในเครือข่ายก็จะทำการส่งข้อมูลที่เป็นโปรแกรมประเภทเอกซพลออิท ไปโจมตีช่องโหว่ของ DCOM RPC ผ่านพอร์ต ทีซีพี/135
7. สร้างการเชื่อมต่อระยะไกลกลับไปยังเครื่องที่เป็นผู้โจมตี ผ่านพอร์ตที่สุ่มขึ้นมาระหว่าง ทีซีพี/666 ถึง ทีซีพี/765 เพื่อรอรับคำสั่ง
8. เรียกใช้งานโปรแกรม ทีเอฟทีพี เซิร์ฟเวอร์บนเครื่องที่เป็นผู้โจมตี และสั่งให้เครื่องที่ถูกหนอนโจมตีนั้นติดต่อและดาวน์โหลด Dllhost.exe และ Svchost.exe จากเครื่องที่เป็นผู้โจมตี ถ้าไฟล์ %System%\dllcache\tftpd.exe มีอยู่ในเครื่องแล้ว หนอนจะไม่ทำการดาวน์โหลด Svchost.exe
9. ตรวจสอบข้อมูลต่างๆ ของเครื่องที่ถูกโจมตี เช่นระบบปฏิบัติการที่ใช้ หมายเลขของ เซอร์วิสแพ็ค(Service Pack) และซิสเต็ม โลคอล(System Local) จากนั้นจะพยายามติดต่อไปยังเว็บไซต์สำหรับอัพเดต แพช ของไมโครซอฟต์เพื่อดาวน์โหลด แพช ของช่องโหว่ ดีคอม อาร์พีซี เว็บไซต์ที่หนอนใช้ดาวน์โหลดนั้นมีดังนี้
    - http://download.microsoft.com/download/6/9/5/6957d785-fb7a-4ac9-b1e6-cb99b62f9f2a/Windows2000-KB823980-x86-KOR.exe
    - http://download.microsoft.com/download/5/8/f/58fa7161-8db3-4af4-b576-0a56b0a9d8e6/Windows2000-KB823980-x86-CHT.exe
    - http://download.microsoft.com/download/2/8/1/281c0df6-772b-42b0-9125-6858b759e977/Windows2000-KB823980-x86-CHS.exe
    - http://download.microsoft.com/download/0/1/f/01fdd40f-efc5-433d-8ad2-b4b9d42049d5/Windows2000-KB823980-x86-ENU.exe
    - http://download.microsoft.com/download/e/3/1/e31b9d29-f650-4078-8a76-3e81eb4554f6/WindowsXP-KB823980-x86-KOR.exe
    - http://download.microsoft.com/download/2/3/6/236eaaa3-380b-4507-9ac2-6cec324b3ce8/WindowsXP-KB823980-x86-CHT.exe
    - http://download.microsoft.com/download/a/a/5/aa56d061-3a38-44af-8d48-85e42dc9d2c0/WindowsXP-KB823980-x86-CHS.exe
    - http://download.microsoft.com/download/9/8/b/98bcfad8-afbc-458f-aace-b7a52a983f01/WindowsXP-KB823980-x86-ENU.exe
10. หลังจากที่หนอนติดตั้ง แพช ให้กับเครื่องเรียบร้อยแล้ว จากนั้นจะทำการรีสตาร์ทเครื่อง ซึ่งเป็นอันสิ้นสุดกระบวนการติดตั้ง แพช

แพ็กเก็ต ไอซีเอ็มพี ที่หนอนชนิดนี้ทำการส่งออกมา

icmp: echo request (ttl 117, id 33634, len 92)

0x0000 xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx .....

0x0010 xxxx xxxx 0800 fb60 0200 a549 aaaa aaaa .....`...I....

0x0020 aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa .....

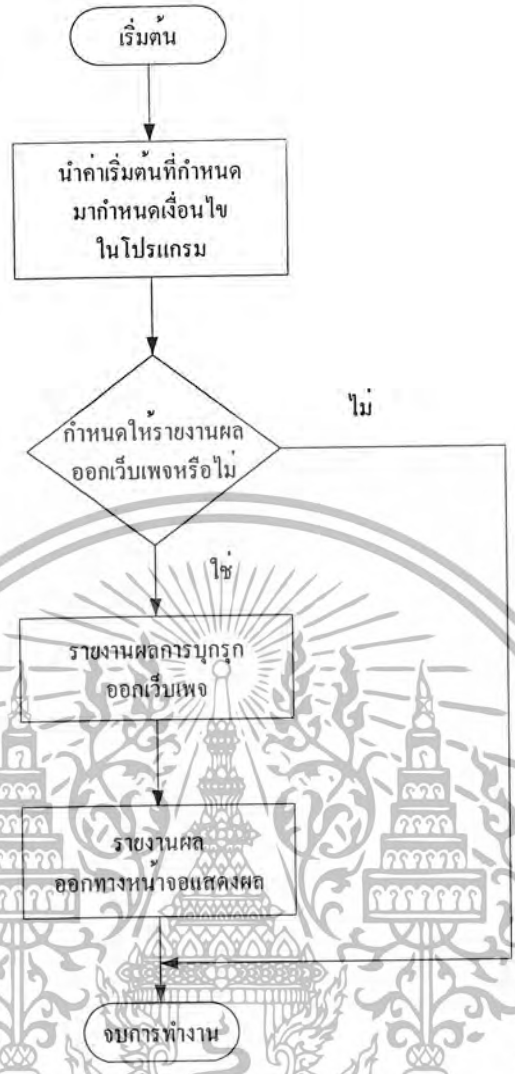
0x0030 aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa .....

0x0040 aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa .....

0x0050 aaaa aaaa aaaa aaaa aaaa aaaa .....

รูปที่ 3.28 โฟล์วชาร์ทแสดงการตรวจจับการบุกรุกแบบนาชิเวอร์ม

3.2.4 ส่วนรายงานผลต่อผู้ใช้



รูปที่ 3.29 โฟลว์ชาร์ทแสดงการแสดงการรายงานผล

บทที่ 4

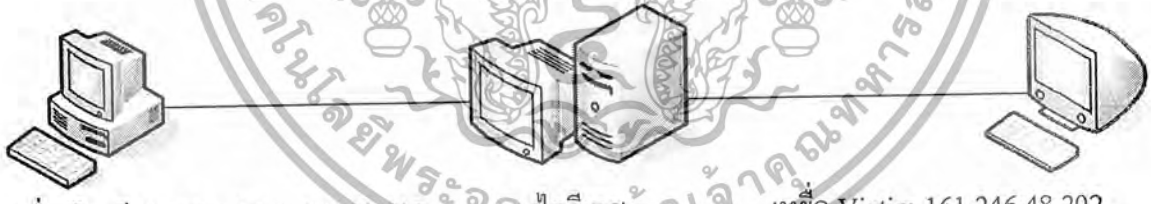
การทดลองและผลการทดลอง

4.1 อุปกรณ์การติดตั้งก่อนการทดสอบ

ขั้นตอนการทดสอบโปรแกรมไอดีเอส ได้ทำการทดสอบโดยมีรายละเอียดของคอมพิวเตอร์ที่เกี่ยวข้องที่ใช้ทดสอบดังนี้

1. เครื่องที่ติดตั้งโปรแกรม ไอดีเอส
   - การ์ดแลนความเร็ว 10/100 Mb 2ตัว

   ระบบปฏิบัติการลีนุกซ์เรดแฮท 9.0 เคอร์เนลเวอร์ชั่น 2.4.20-8
2. เครื่องที่ใช้ทำการโจมตี (Attacker)
   - การ์ดแลนความเร็ว 100 Mb
   - IP address 161.246.73.119
   - ระบบปฏิบัติการวินส์โดว์เอ็กซ์พี
3. เครื่องที่ใช้เป็นเหยื่อทดสอบ (Victim)
   - การ์ดแลนความเร็ว 100 Mb
   - IP address 161.246.73.202
   - ระบบปฏิบัติการวินส์โดว์เอ็กซ์พี



รูปที่4.1 แสดงโครงสร้างเครือข่ายในการทดสอบ

ก่อนติดตั้งระบบตรวจจับผู้บุกรุกทางเครือข่ายคอมพิวเตอร์ ผู้ติดตั้งต้องคำนึงถึงปัจจัยดังต่อไปนี้ เพื่อไม่ให้เกิดปัญหาในการติดตั้งดังนี้

1. ระบบนี้สร้างขึ้นบนระบบปฏิบัติการลีนุกซ์ เรดแฮท(Redhat 9.0) ดังนั้นจึงควรติดตั้งระบบบนระบบปฏิบัติการที่มีลักษณะใกล้เคียง หรือมีลักษณะเดียวกับระบบปฏิบัติการดังกล่าว ที่มีคอมไฟล์เลอร์ภาษาซีอยู่ด้วย
2. เครื่องที่ใช้ควรมีหน่วยความจำอย่างน้อย 400 KB (สำหรับโปรแกรมขณะทำงาน)

3. เครื่องที่ติดตั้งระบบต้องอยู่ในบรอดคาสโดเมน (Broadcast domain) เดียวกับเครื่องที่ต้องการตรวจจับ ซึ่งหมายถึงการที่สามารถรับข้อมูลแพ็กเก็ตที่ทั้งเครือข่ายนั้น ๆ ได้รับหรือ ตรวจจับภายในเครื่องเดียวกัน
4. ต้องใช้สิทธิ์รูท (root) ของระบบในการใช้งานระบบ

การติดตั้งระบบตรวจจับผู้บุกรุกทางเครือข่ายคอมพิวเตอร์นั้น สามารถทำได้โดยใช้ขั้นตอนต่อไปนี้

1. สร้างไดเรกทอรีเพื่อเก็บไฟล์ที่ใช้ในการติดตั้ง โดยใช้คำสั่ง mkdir <ชื่อไดเรกทอรี> แล้วนำไฟล์ต่างๆ ที่ใช้ในการติดตั้งไปไว้ในไดเรกทอรีที่เตรียมไว้ ซึ่งได้แก่ ไฟล์ดังต่อไปนี้

- itenid.c
- itenid.h
- Makefile
- itenid.1

2. เรียกคำสั่ง make เพื่อคอมไฟล์โปรแกรมทั้งหมด ในไดเรกทอรีที่เก็บไฟล์สำหรับการติดตั้ง

3. จากนั้นเรียกคำสั่ง make install เพื่อสร้างที่เก็บ file ต่างๆ และ copy files ไปไว้ในไดเรกทอรีที่กำหนด

เมื่อติดตั้งระบบแล้ว แต่ไม่ต้องการใช้งานระบบอีก ผู้ใช้สามารถถอดระบบออกจากเครื่องได้ โดยมีขั้นตอนดังต่อไปนี้

(1) เรียกคำสั่ง make uninstall เพื่อลบไฟล์ต่างๆ ที่ไม่จำเป็นต้องใช้ในไดเรกทอรีที่เก็บไฟล์เหล่านั้น
(2) จากนั้นเรียกคำสั่ง make clean เพื่อลบ object files ทั้งหมดออก

หากเกิดปัญหาในการใช้งานผู้ใช้สามารเรียกขอความช่วยเหลือจากระบบได้ โดยการเรียกแมนเพจขึ้นมาดู โดยใช้คำสั่ง man itenid ซึ่งนำเสนอออปชันต่างๆ ที่ให้เลือกใช้งาน และข้อมูลต่างๆ เกี่ยวกับระบบ

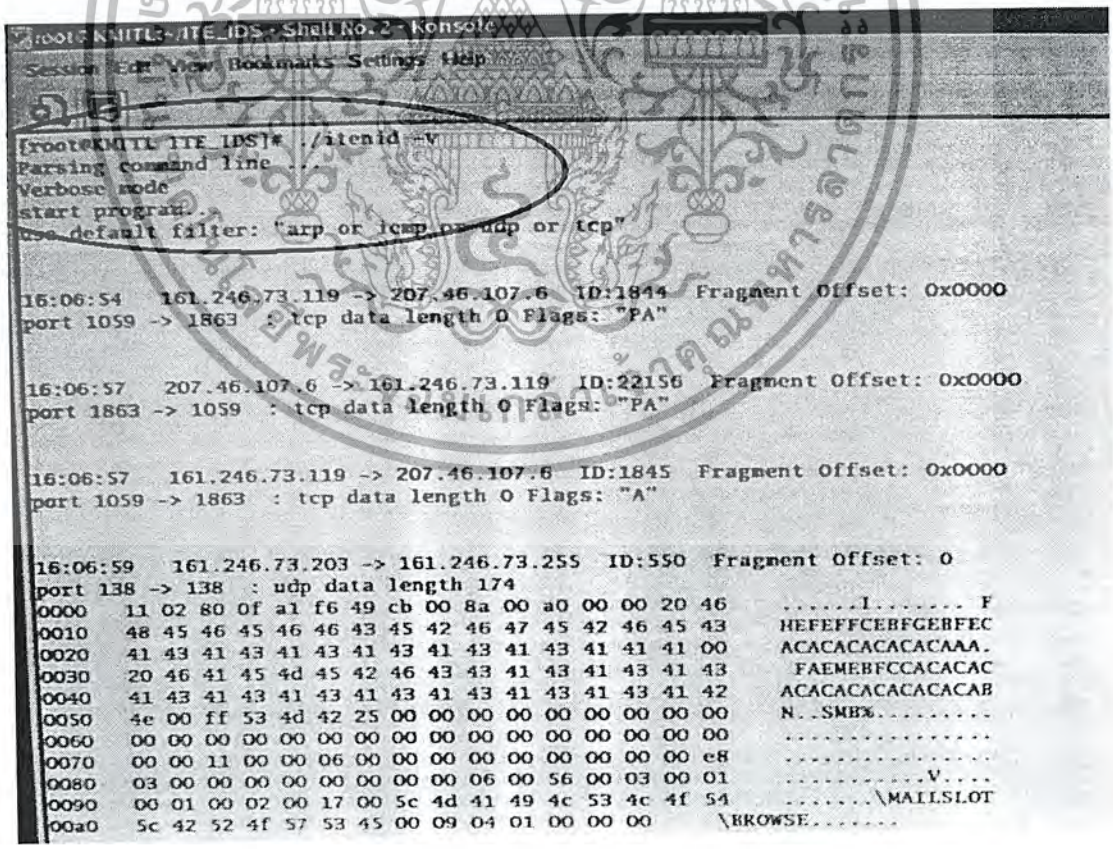
การเรียกใช้งานระบบสามารถเรียกใช้ได้บนคอมมานไลน์ที่หน้าจอเทอร์มินอลของระบบปฏิบัติการลีนุกซ์ โดยเรียกใช้คำสั่ง itenid - <option> โดยมีคำสั่งให้เลือกใช้ที่เกี่ยวข้องกับการออกแบบและการสร้างดังนี้

- v	พิมพ์ข้อมูลของแพ็กเก็ตที่เก็บได้ออกหน้าจอ
- R	ตรวจสอบการโจมตีแบบตามเวลาจริง
- l	เก็บข้อมูลแพ็กเก็ตที่จับได้ลงล็อกไฟล์

4.2การทดลองส่วนการแสดงผลข้อมูลออกทางหน้าจอ

ในขั้นตอนนี้เป็นการเก็บข้อมูลของแพ็กเก็ตที่เข้าสู่ระบบ โดยผู้ใช้อาจเลือกให้ระบบเก็บข้อมูลดังกล่าวลงล็อกไฟล์ หรือแสดงข้อมูลของแพ็กเก็ตเหล่านั้นบนหน้าจอก็ได้

กรณีต้องการดูแพ็กเก็ตโดยไม่ต้องการเก็บข้อมูลเหล่านั้นไว้ ผู้ใช้สามารถเลือกใช้ออปชัน itenid –v ตามโฟลว์ชาร์ทรูปที่ 3.1 ซึ่งเมื่อสั่งคำสั่งดังกล่าว ระบบจะแสดงข้อมูลของแพ็กเก็ตที่เข้าสู่ระบบผ่านหน้าจอเทอร์มินอล โดยแสดงข้อมูลของเฮดเดอร์ของแพ็กเก็ตทั้งของทีซีพี/ไอพี และอีเทอร์เน็ตบางส่วน รวมทั้งวันและเวลาที่แพ็กเก็ตเหล่านั้นเข้ามาด้วย ดังรูปที่ 4.2

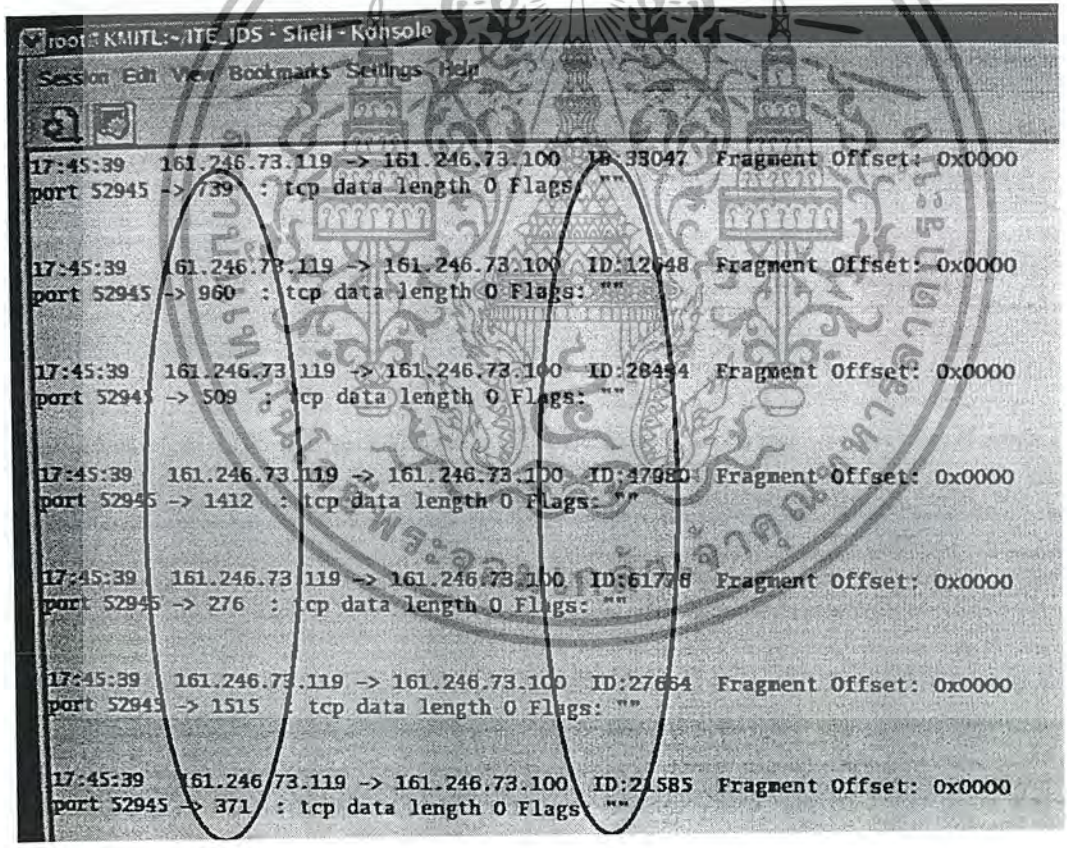


รูปที่ 4.2 แสดงการแสดงผลข้อมูลแพ็กเก็ตผ่านหน้าจอเทอร์มินอล

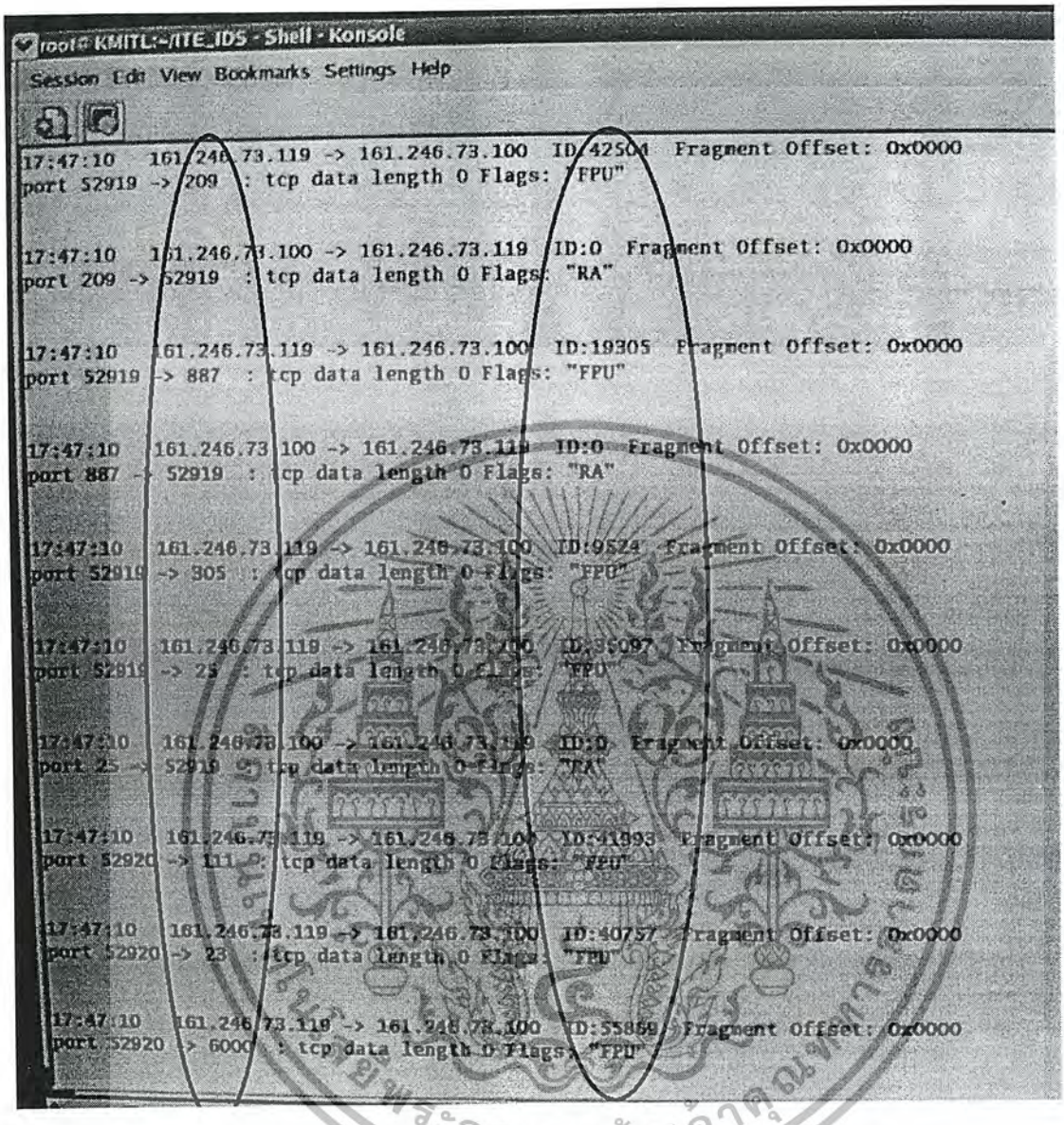
ในลักษณะการทำงานแบบนี้จะไม่มีการตรวจสอบการบุกรุก แต่จะเป็นเพียงการแสดงผลข้อมูลที่วิ่งผ่านเครือข่าย การดูข้อมูลของแพ็กเก็ตในลักษณะนี้มีข้อดีที่ไม่ต้องเปลืองเนื้อที่ในการเก็บข้อมูล แต่เป็นเพียงการเรียกดูข้อมูลอย่างเดียว ไม่ได้มีการเก็บข้อมูลของแพ็กเก็ตที่เข้ามาในระบบไว้เลย

4.2.1 การทดลองการโจมตีแบบสแกนพอร์ต (Port Scan)

ทำการทดลองการโจมตีจากเครื่องที่ใช้ทำการโจมตีโดยมีหมายเลขไอพี 161.246.73.119 โดยใช้การโจมตีแบบ นูล์สแกน และ คริสต์มาสทรีสแกน โดยโจมตีไปยังเครื่องที่ใช้เป็นเหยื่อทดสอบหมายเลขไอพี 161.246.73.100 โดยใช้เครื่องที่ติดตั้งโปรแกรมไอดีเอสหมายเลขไอพี 161.246.73.100 ผลที่ได้จากจะแสดงดังรูป 4.3 และ 4.4 ตามลำดับ



รูปที่ 4.3 แสดงการจับแพ็กเก็ตการโจมตีแบบนูล์สแกน (Null Scan)

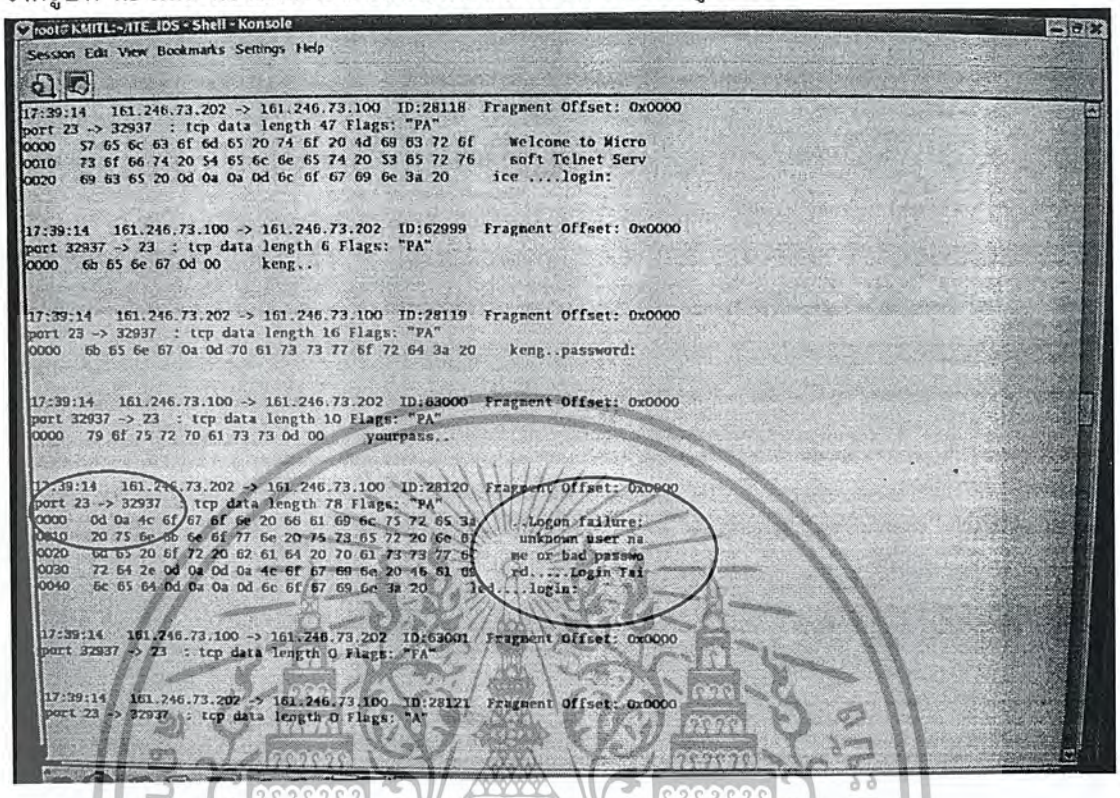


รูปที่ 4.4 แสดงผลการดักจับแพ็กเก็ตการโจมตีแบบคริสต์มาสทรีสแกน(Xmas Scan)

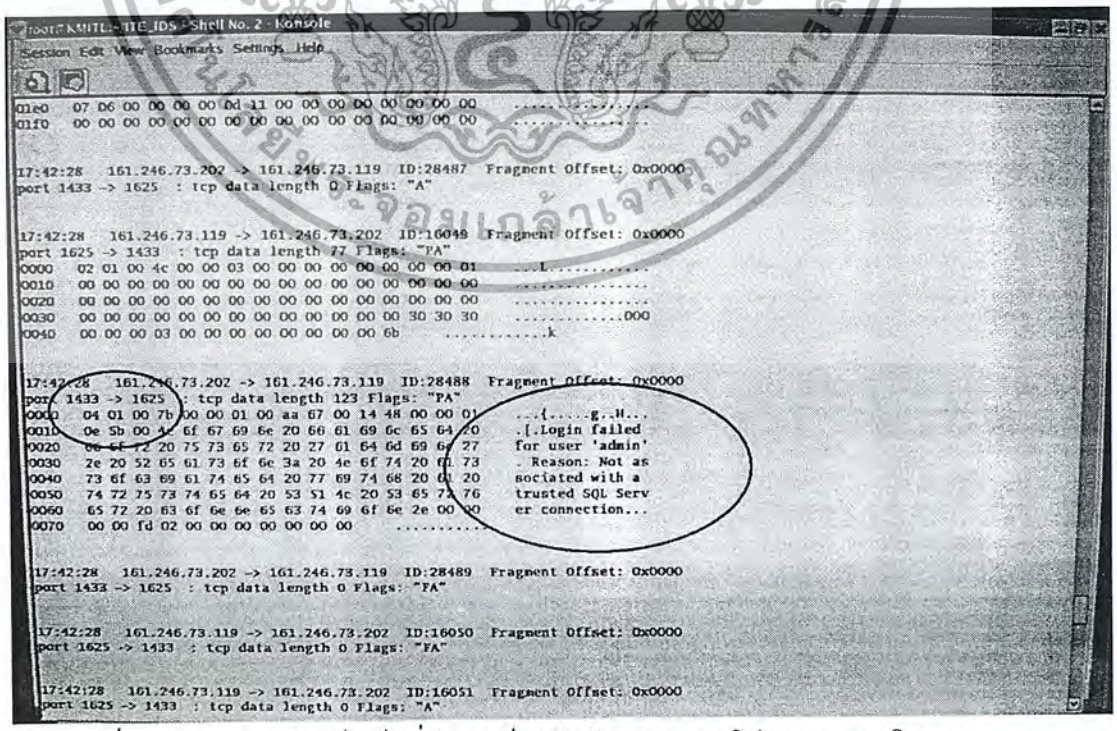
จากผลการทดลองจะเห็นได้ว่าเครื่องที่ทำการโจมตีจะทำการขอติดต่อเครื่องเหยื่อไปที่พอร์ตหมายเลขต่างๆโดยใช้แฟรกตามวิธีที่โจมตี

4.2.2 การทดลองการโจมตีแบบบรูทฟอร์ซ(Bruteforce Attack)

จากรูปที่ 4.5 และ 4.6 เป็นการจับแพ็กเก็ตของการโจมตีแบบบรูทฟอร์ซ



รูปที่ 4.5 แสดงการจับแพ็กเก็ตที่ทำการล็อกอินผิดพลาดของโปรแกรมเทลเน็ต



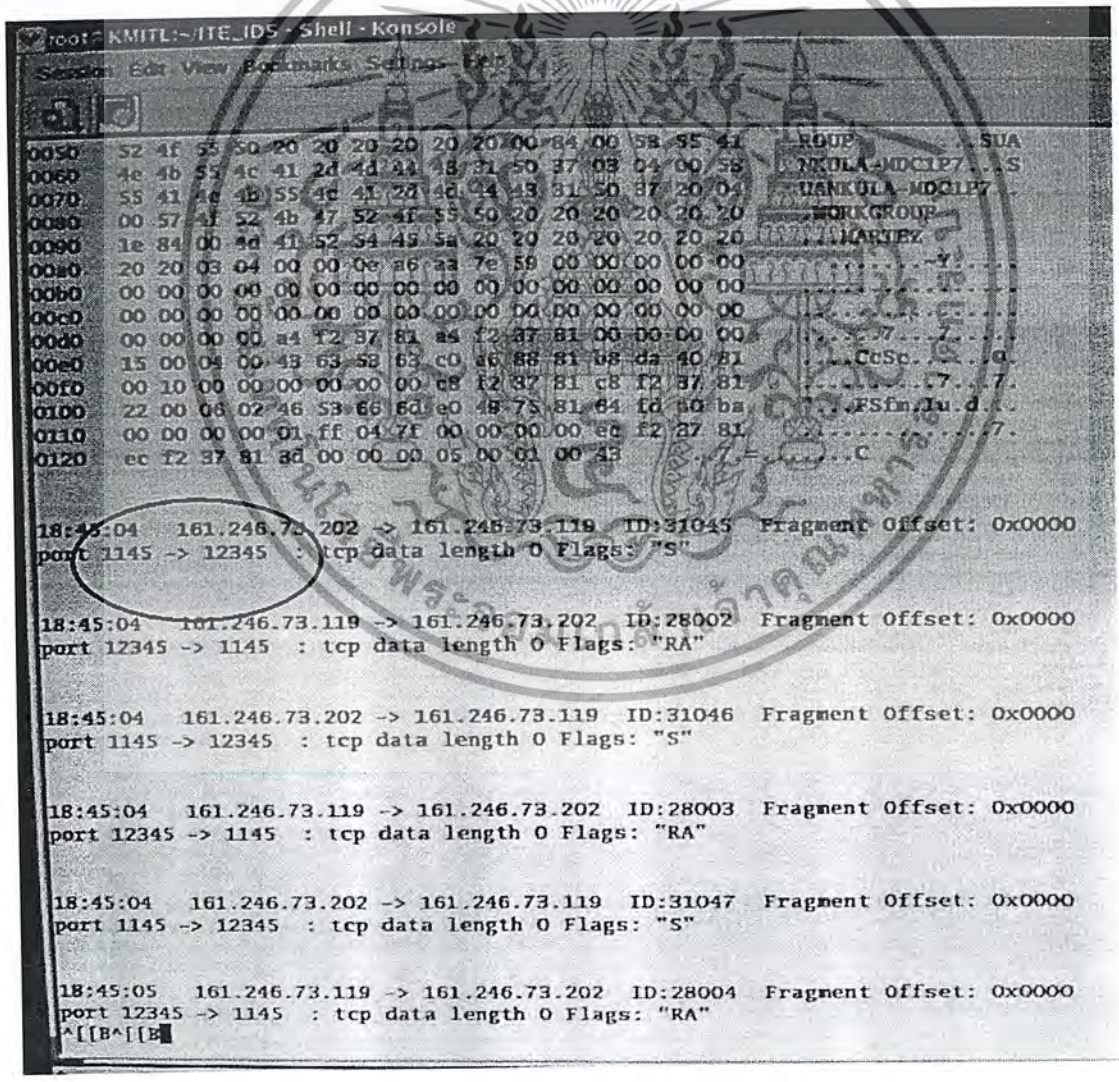
รูปที่ 4.6 แสดงการจับแพ็กเก็ตที่ทำการล็อกอินผิดพลาดของโปรแกรมเอสคิวแอล

จากรูปภาพทั้งสองภาพคือการตอบกลับจากเครื่องเซิฟเวอร์เทลเนตและเอสคิวแอลตามลำดับ เมื่อเครื่องไคลเอนท์ทำการล็อกอินผิดพลาด

4.2.3 การทดลองการโจมตีของโทรจันแบบต่างๆ

4.2.3.1 การติดต่อกับพอร์ตโทรจัน

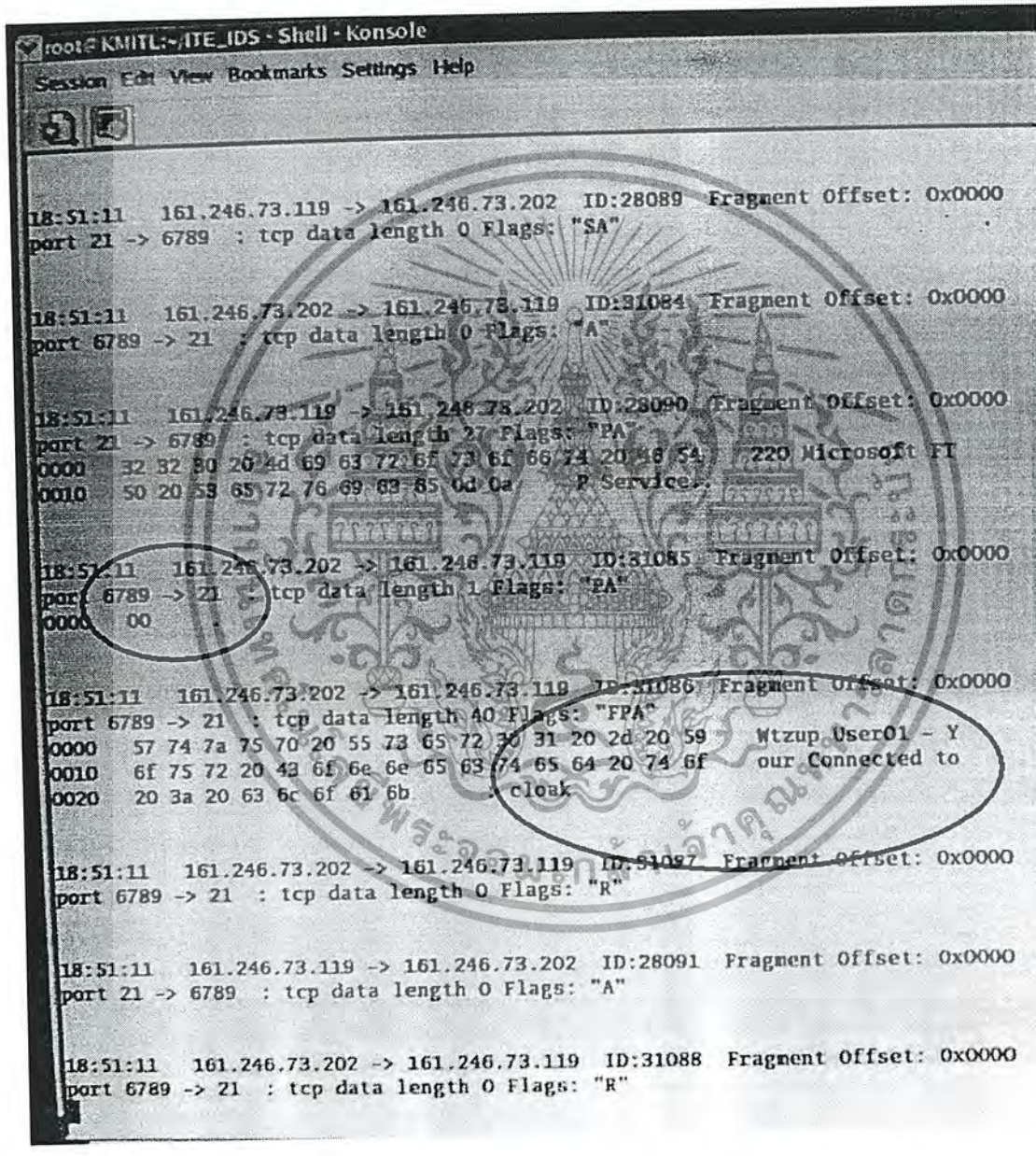
รูปที่ 4.7 นี้เป็นรูปที่แสดงการจับแพ็กเก็ตของการโจมตีแบบพยามยามติดต่อพอร์ตแบล็กดอร์โดยในรูปเป็นการพยายามขอทำการเชื่อมต่อไปที่พอร์ต 12345 ซึ่งเป็นพอร์ตที่อยู่ในแบ็กดอร์พอร์ตลิสต์



รูปที่ 4.7 แสดงการจับแพ็กเก็ตของการโจมตีแบบพอร์ตแบ็คดอร์

4.2.3.2 การโจมตีแบบโดลีโทรจัน

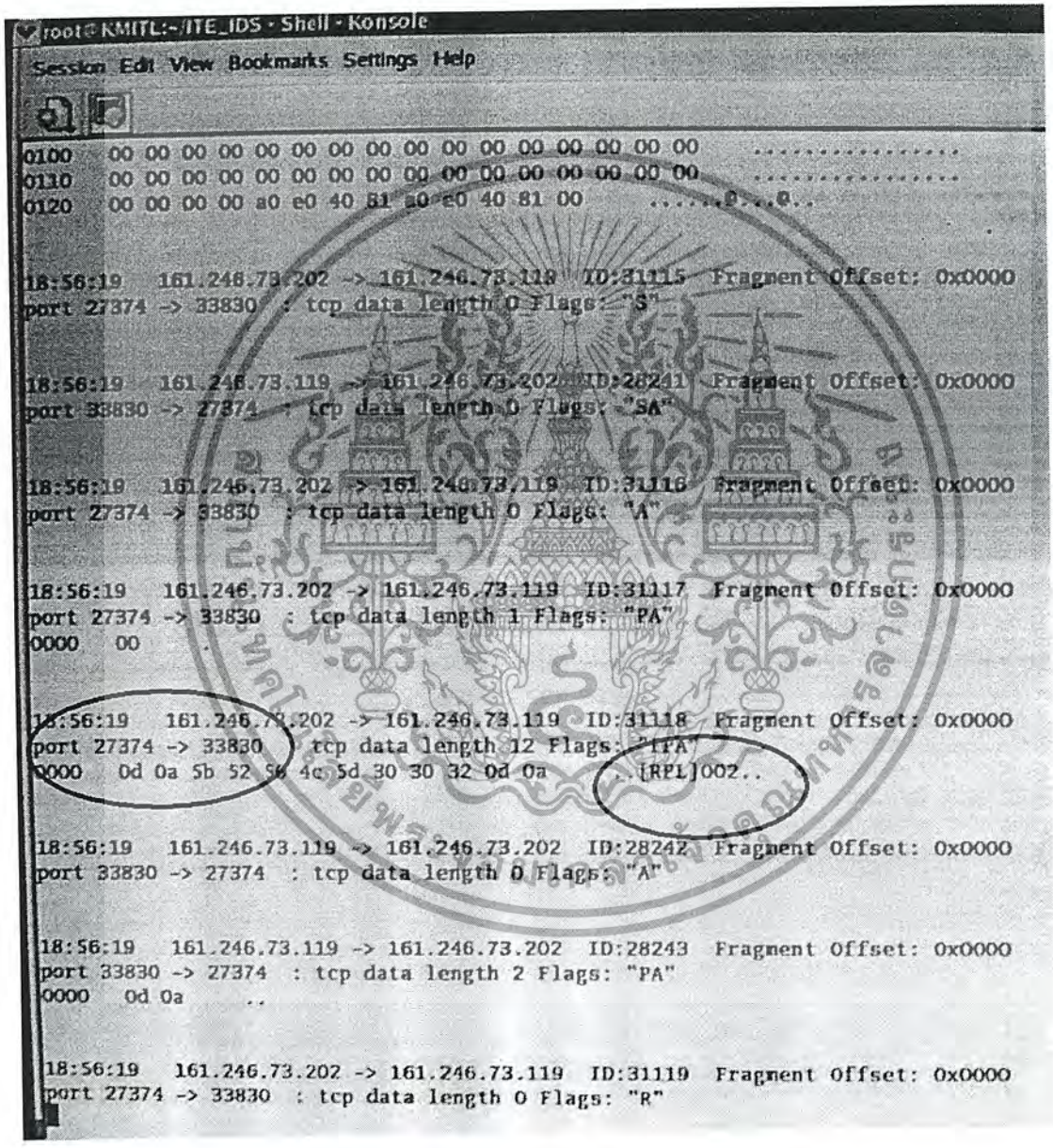
จากรูปที่ 4.8 เป็นการแสดงผลการจับแพ็กเก็ตของการโจมตีโดลีโทรจันซึ่งจะเห็นได้ว่าเครื่องที่ทำการโจมตีจะขอติดต่อไปยังเครื่องเหยื่อที่พอร์ต 21 ซึ่งเหมือนจะเป็นการขอติดต่อเอฟทีพีเซิฟเวอร์ธรรมดา และพอเชื่อมต่อได้ก็จะทำการส่งข้อมูลที่เป็นสัญลักษณ์ของโดลีโทรจันไป



รูปที่ 4.8 แสดงการจับแพ็กเก็ตการโจมตีแบบโดลีโทรจัน

4.2.3.3 การทดลองการโจมตีแบบซับเซเวนโทรจัน

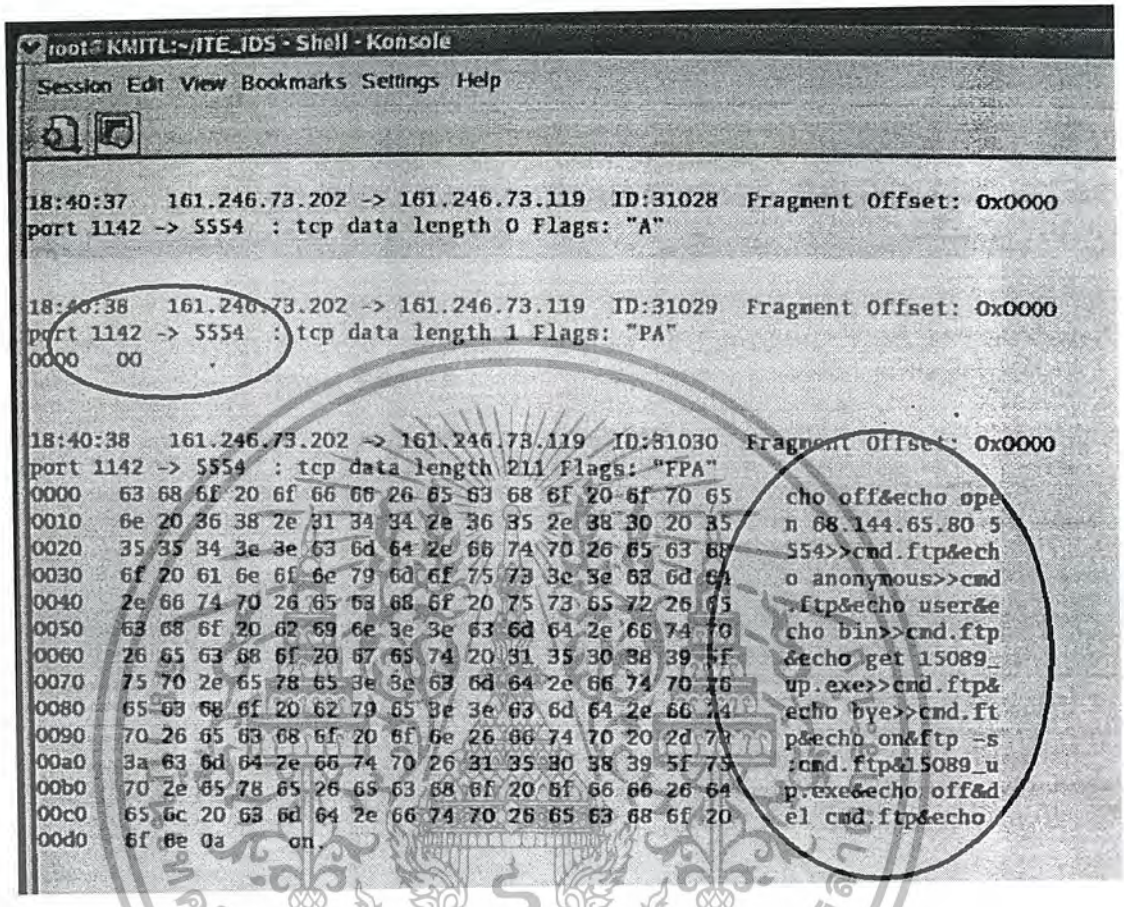
จากรูปที่ 4.9 จะเห็นว่าการโจมตีแบบซับเซเว่นนี้ เครื่องโจมตีจะใช้พอร์ตต้นทางเป็นพอร์ต 27374 ติดต่อไปที่เครื่องที่ถูกโจมตีซึ่งได้ทำการถูกฝังโปรแกรมไว้ที่เครื่องเรียบร้อยแล้ว และเมื่อทำการติดต่อได้ก็จะทำการส่งข้อมูลตามรูปแบบการโจมตีนั้น



รูปที่ 4.9 แสดงการจับแพ็กเก็ตการโจมตีแบบซับเซเว่นโทรจัน

4.2.4 การทดลองการโจมตีแบบตัวหนอน (Worm)

4.2.4.1 การทดลองการโจมตีของแซสเซอร์

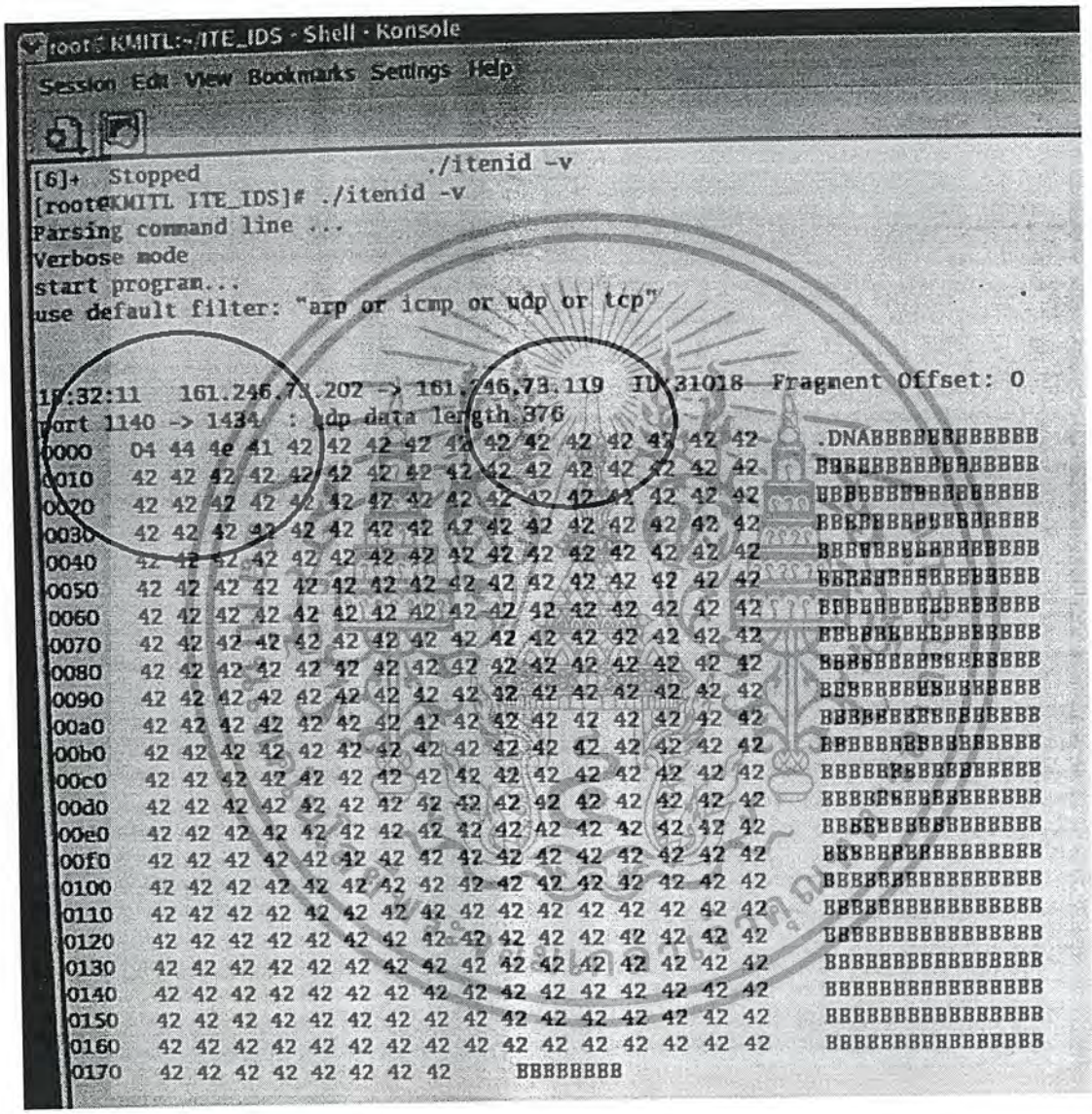


รูปที่ 4.10 แสดงการจับแพ็กเก็ตการโจมตีแบบแซสเซอร์

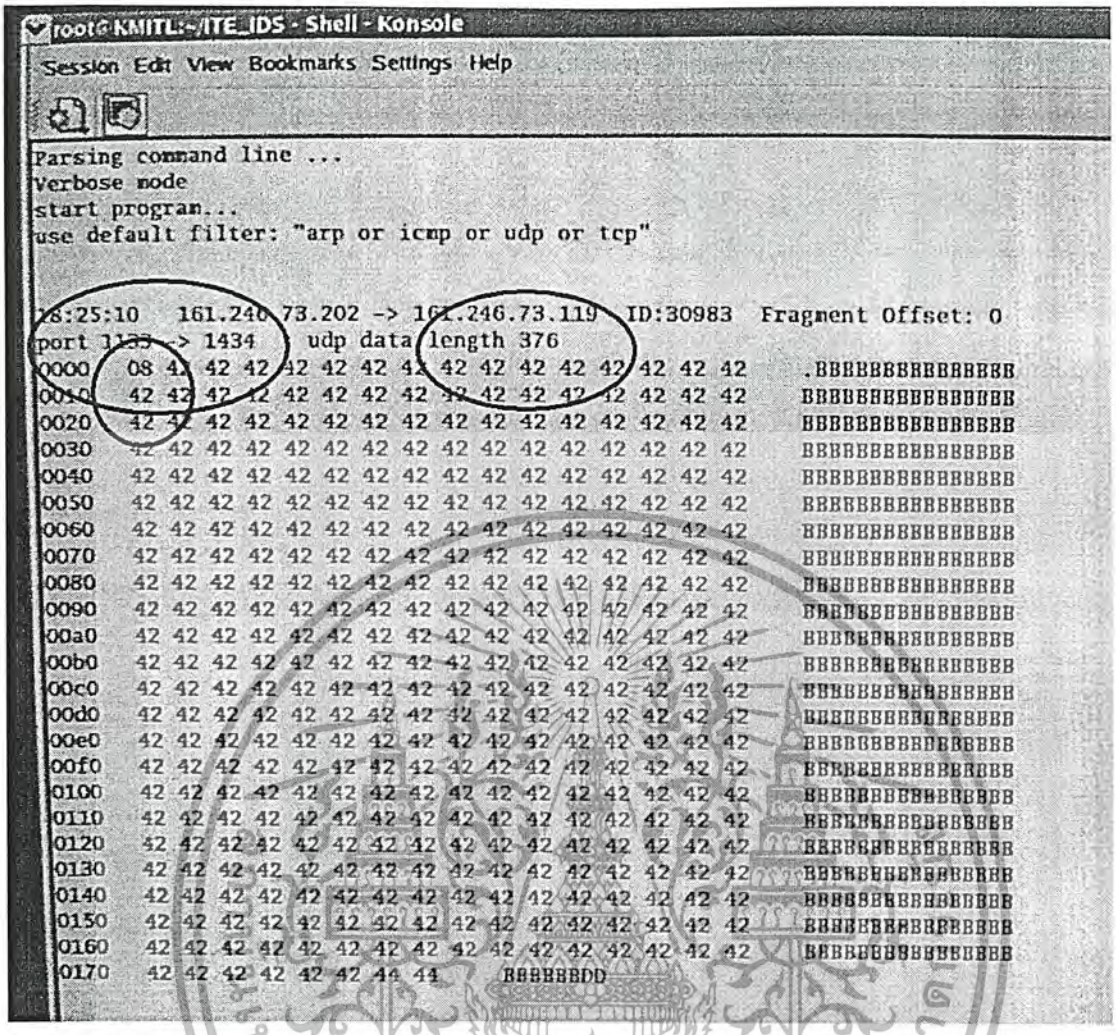
จากรูปจะเห็นได้ว่าเครื่องโจมตีจะทำการเชื่อมต่อไปยังเครื่องเหยื่อที่พอร์ต 5554 หลังจากนั้นจะส่งข้อมูลที่เป็นไปตามรูปแบบของแซสเซอร์ ดังในรูป

4.2.4.2 การทดลองการโจมตีของสแลมเมอร์

ในการทดลองการโจมตีนี้จะมีอยู่สองตัวอย่างด้วยกันคือ โจมตีแบบสแตกโอเว่อร์โฟลว์ และ ฮีปโอเว่อร์โฟลว์ ตามลำดับ



รูปที่ 4.11 แสดงการจับแพ็กเก็ตของการโจมตีแบบสแตกโอเวอร์โฟลว์

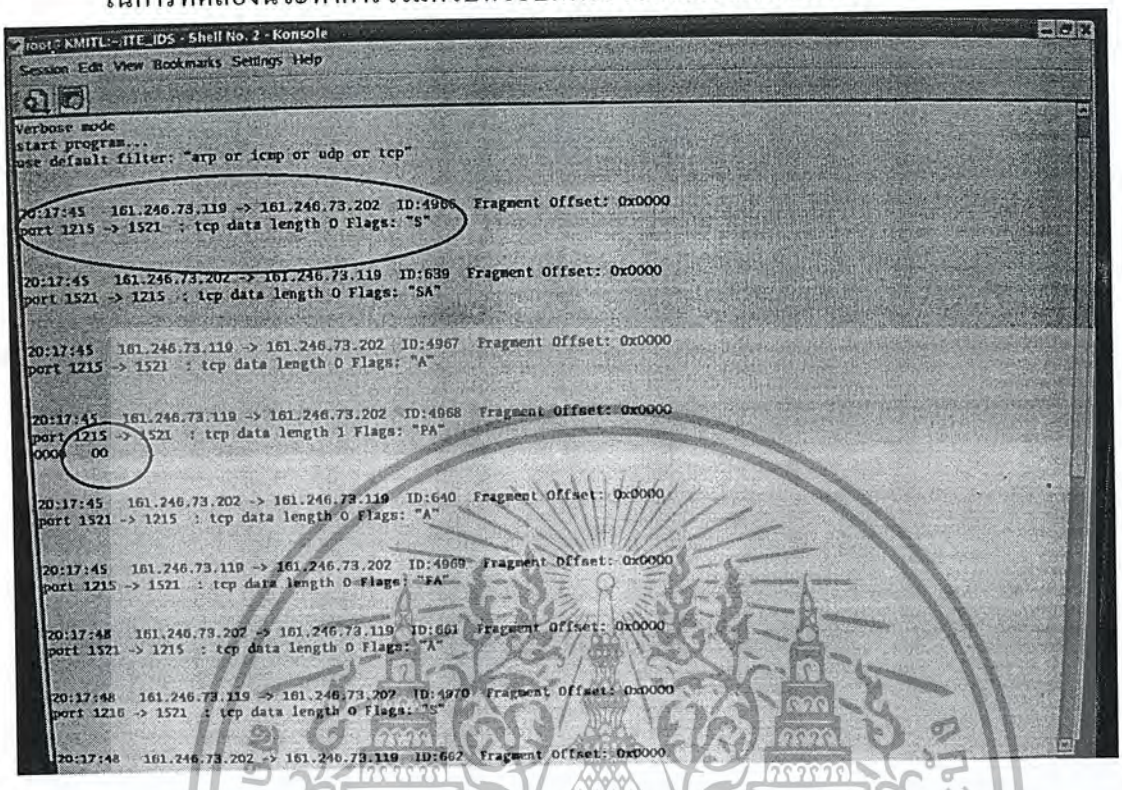


รูปที่ 4.12 แสดงการจับการโจมตีแบบฮีปโอเวอร์โฟว์

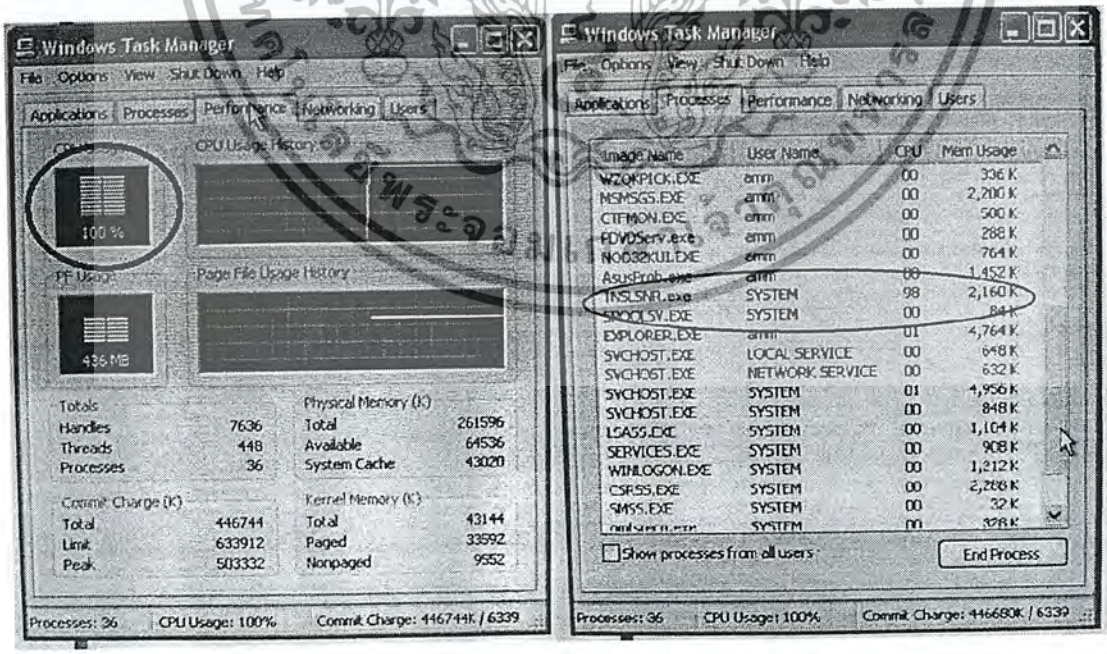
จากทั้งสองภาพจะเห็นได้ว่าการโจมตีนี้ ผู้โจมตีจะส่งแพ็กเก็ตยูดีพีไปที่พอร์ต 1434 และส่งข้อมูลขนาด 376 ไบต์ไป โดยถ้าเป็นวิธี สแตกโอเว่อร์โฟลว์ข้อมูลข้างในที่ไบต์แรกจะมีค่า 04 ระบบเลขฐานสิบหก แต่ ฮีปโอเว่อร์โฟลว์จะส่งค่า 08 ในระบบเลขฐานสิบหกแทน

4.2.5 การทดลองการโจมตีข้อบกพร่องของแอพพลิเคชัน

ในการทดลองนี้จะทำการโจมตีไปที่ข้อบกพร่องของออราเคิลเซิฟเว่อร์



รูปที่ 4.13 แสดงการจับแพ็กเก็ตการโจมตีข้อบกพร่องของออราเคิลเซิฟเว่อร์

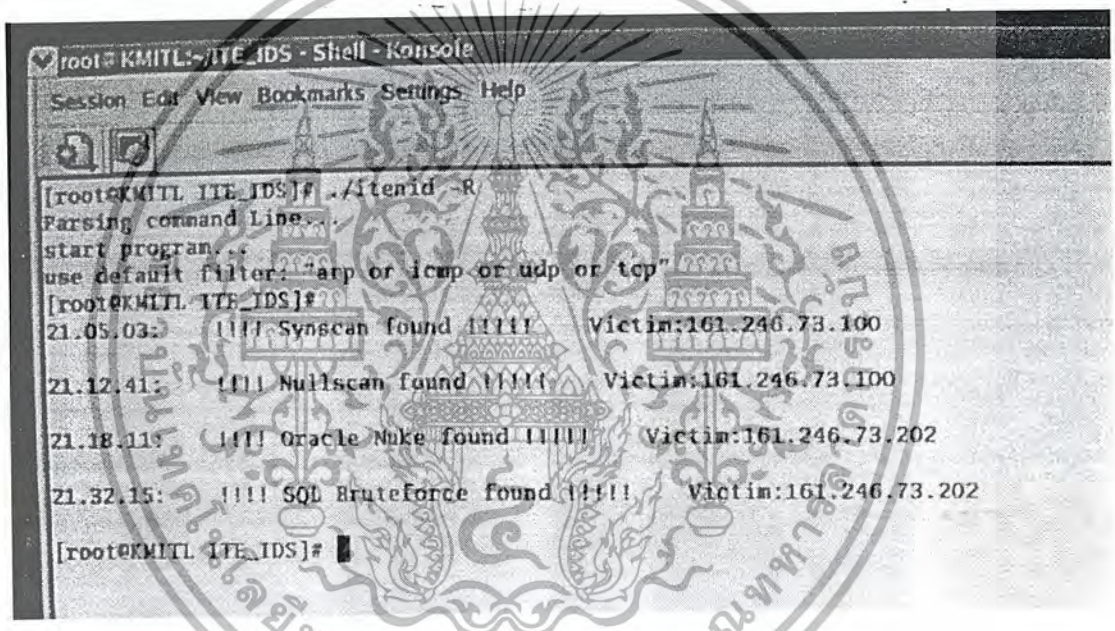


รูปที่ 4.14 แสดงประสิทธิภาพของเครื่องที่โดนโจมตีแล้ว

จากรูปจะเห็นว่าผู้โจมตีแค่ส่งแพ็กเก็ตทีซีพีขนาด 1 ไบต์ไปที่เครื่องเหยื่อเท่านั้นก็สามารถทำให้เครื่องเหยื่อใช้รีซอร์สต่างๆของเครื่องอย่างเต็มประสิทธิภาพได้

4.3 การทดลองส่วนการวิเคราะห์การบุกรุก

ในผลการทดลองส่วนนี้เป็นการนำข้อมูลของแพ็กเก็ตที่เข้ามาขณะนั้น มาวิเคราะห์ในขณะนั้นเลย โดยเรียกใช้คำสั่ง itenid –R ตามโฟลว์ชาร์ทรูปที่ 3.2 ทำให้ได้ข้อมูลการโจมตีตามเวลาจริง ซึ่งแสดงผลออกมาผ่านหน้าจอเทอร์มินอล โดยจะแสดงผลทั้งเครื่องเป้าหมายที่ถูกโจมตี วันและช่วงเวลาที่ถูกโจมตี และชนิดของการโจมตีด้วย ดังรูปที่ 4.15



รูปที่ 4.15 แสดงผลการรันโปรแกรมในโหมดตรวจจับผู้บุกรุก

บทที่ 5
สรุปผลการทดลอง

5.1 สรุปผลการทดลอง

จากการศึกษาเกี่ยวกับระบบตรวจจับผู้บุกรุก พบว่าหัวใจสำคัญในการพัฒนา คือต้องพยายามเข้าใจให้ได้ว่าลักษณะพิเศษ(Signature) ของตัวที่เราต้องการจะตรวจจับคืออะไร ในขณะที่งานมางด้านโปรแกรมมิ่งจะคล้ายคลึงกันเกือบทุกตัว ดังนั้นสรุปก็คือระบบตรวจจับผู้บุกรุกที่ดี คือมีข้อมูลที่ทันสมัย ก็จะสามารถป้องกันระบบเครือข่ายได้ดีที่สุด

5.2 ปัญหาและอุปสรรค

1. ความยากในการหาข้อมูลในส่วนลึก ของโปรแกรมที่ใช้โจมตี(malicious program) ชนิดต่างๆซึ่งโดยส่วนมากมักจะมีเพียงคร่าวๆ แต่จะเน้นหนักไปทางวิธีการแก้ไข

2. แอปพลิเคชั่นที่ใช้ทดลองหาได้ยากมาก จนในบางตัวต้องเขียนตัวจำลองขึ้นเองเพื่อใช้ในการทดลอง

3.เมื่อแพ็คเก็ตที่มีเข้ามาในขณะใดขณะหนึ่งมีเป็นจำนวนมาก อาจทำให้บางแพ็คเก็ตถูกละเลยการตรวจสอบได้

5.3 แนวทางการวิจัยและพัฒนาต่อ

1. สามารถตรวจจับและวิเคราะห์ได้ทันโดยไม่ต้องดรอปทิ้งเมื่อโดนโจมตีด้วยแพ็กเก็ตปริมาณมาก และความเร็วสูง

2. สามารถตรวจจับการโจมตีได้หลากหลายชนิดเพิ่มขึ้น

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] จตุชัย แพงจันทร์, อนุโชต วุฒิพรพงษ์ , "เจาะระบบ Network ฉบับสมบูรณ์" บริษัท ไอดีซี อิโฟ ดิส-ทริบิวเตอร์ เซ็นเตอร์ จำกัด ,2546 .

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

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

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

ภาคผนวก ก.

รายชื่อพอร์ตโทรจัน

1 (UDP) - Sockets des Troie

2 Death

20 Senna Spy FTP server

21 Back Construction, Blade Runner, Cattivik FTP Server, CC Invader, Dark FTP, Doly Trojan, Fore, Invisible FTP, Juggernaut 42, Larva, MotIv FTP, Net Administrator, Ramen, Senna Spy FTP server, The Flu, Traitor 21, WebEx, WinCrash

22 Shaft

23 Fire HacKer, Tiny Telnet Server - TTS, Truva Atl

25 Ajan, Antigen, Barok, Email Password Sender - EPS, EPS II, Gip, Gris, Happy99, Hpteam mail, Hybris, I love you, Kuang2, Magic Horse, MBT (Mail Bombing Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth, Tapiras, Terminator, WinPC, WinSpy

30 Agent 40421

31 Agent 31, Hackers Paradise, Masters Paradise

41 Deep Throat, Foreplay

48 DRAT

50 DRAT

58 DMSetup

59 DMSetup

79 CDK, Firehotcker

80 711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Executor, God Message, God Message Creator, Hooker, IISworm, MTX, NCX, Reverse WWW Tunnel Backdoor, RingZero, Seeker, WAN Remote, Web Server CT, WebDownloader

81 RemoConChubo

99 Hidden Port, NCX

110 ProMail trojan

113 Invisible Identd Deamon, Kazimas

119 Happy99

121 Attack Bot, God Message, JammerKillah

123 Net Controller

133 Farnaz

137 Chode

137 (UDP) - Msinit

138 Chode

139 Chode, God Message worm, Msinit, Netlog, Network, Qaz

142 NetTaxi

146 Infector

146 (UDP) - Infector

170 A-trojan

334 Backage

411 Backage

420 Breach, Incognito

421 TCP Wrappers trojan

455 Fatal Connections

456 Hackers Paradise

513 Grlogin

514 RPC Backdoor

531 Net666, Rasmin

555 711 trojan (Seven Eleven), Ini-Killer, Net Administrator, Phase Zero, Phase-0, Stealth Spy

605 Secret Service

666 Attack FTP, Back Construction, BLA trojan, Cain & Abel, NokNok, Satans Back Door - SBD, ServU, Shadow Phyre, th3r1pp3rz (= Therippers)

667 SniperNet

669 DP trojan

692 GayOL

777 AimSpy, Undetected

808 WinHole

911 Dark Shadow

999 Deep Throat, Foreplay, WinSatan

1000 Der Späher / Der Spaeher, Direct Connection

1001 Der Späher / Der Spaeher, Le Guardien, Silencer, WebEx

1010 Doly Trojan

1011 Doly Trojan

1012 Doly Trojan

1015 Doly Trojan

1016 Doly Trojan

1020 Vampire

1024 Jade, Latinus, NetSpy

1025 Remote Storm

1025 (UDP) - Remote Storm

1035 Multidropper

1042 BLA trojan

1045 Rasmin

1049 /sbin/initd

1050 MiniCommand

1053 The Thief

1054 AckCmd

1080 WinHole

1081 WinHole

1082 WinHole

1083 WinHole

1090 Xtreme

1095 Remote Administration Tool - RAT

1097 Remote Administration Tool - RAT

1098 Remote Administration Tool - RAT

1099 Blood Fest Evolution, Remote Administration Tool - RAT

1150 Orion

1151 Orion

1170 Psyber Stream Server - PSS, Streaming Audio Server, Voice

1200 (UDP) - NoBackO

1201 (UDP) - NoBackO

1207 SoftWAR

1208 Infector

1212 Kaos

1234 SubSeven Java client, Ultors Trojan

1243 BackDoor-G, SubSeven, SubSeven Apocalypse, Tiles

1245 VooDoo Doll

1255 Scarab

1256 Project nEXT

1269 Matrix

1272 The Matrix

1313 NETrojan

1338 Millenium Worm

1349 Bo dll

1394 GoFriller, Backdoor G-1

1441 Remote Storm

1492 FTP99CMP

1524 Trinoo

1568 Remote Hack

1600 Direct Connection, Shivka-Burka

1703 Exploiter

1777 Scarab

1807 SpySender

1966 Fake FTP

1967 WM FTP Server

1969 OpC BO

1981 Bowl, Shockrave

1999 Back Door, SubSeven, TransScout

2000 Der Späher / Der Spaeher, Insane Network, Last 2000, Remote Explorer 2000, Senna Spy Trojan Generator

2001 Der Späher / Der Spaeher, Trojan Cow

2023 Ripper Pro

2080 WinHole

2115 Bugs

2130 (UDP) - Mini Backlash

2140 The Invasor

2140 (UDP) - Deep Throat, Foreplay

2155 Illusion Mailer

2255 Nirvana

2283 Hvl RAT

2300 Xplorer

2311 Studio 54

2330 Contact

2331 Contact

2332 Contact

2333 Contact

2334 Contact

2335 Contact

2336 Contact

2337 Contact

2338 Contact

2339 Contact, Voice Spy

2339 (UDP) - Voice Spy

2345 Doly Trojan

2565 Striker trojan

2583 WinCrash

2600 Digital RootBeer

2716 The Prayer

2773 SubSeven, SubSeven 2.1 Gold

2774 SubSeven, SubSeven 2.1 Gold

2801 Phineas Phucker

2989 (UDP) - Remote Administration Tool - RAT

3000 Remote Shut

3024 WinCrash

3031 Microspy

3128 Reverse WWW Tunnel Backdoor, RingZero

3129 Masters Paradise

3150 The Invasor

3150 (UDP) - Deep Throat, Foreplay, Mini Backlash

3456 Terror trojan

3459 Eclipse 2000, Sanctuary

3700 Portal of Doom

3777 PsychWard

3791 Total Solar Eclypse

3801 Total Solar Eclypse

4000 SkyDance

4092 WinCrash

4242 Virtual Hacking Machine - VHM

4321 BoBo

4444 Prosiak, Swift Remote

4567 File Nail

4590 ICQ Trojan

4950 ICQ Trogen (Lm)

5000 Back Door Setup, Blazer5, Bubbel, ICKiller, Ra1d, Sockets des Troie

5001 Back Door Setup, Sockets des Troie

5002 cd00r, Shaft

5010 Solo

5011 One of the Last Trojans - OOTLT, One of the Last Trojans - OOTLT, modified

5025 WM Remote KeyLogger

5031 Net Metropolitan

5032 Net Metropolitan

5321 Firehotcker

5333 Backage, NetDemon

5343 wCrat - WC Remote Administration Tool

5400 Back Construction, Blade Runner

5401 Back Construction, Blade Runner

5402 Back Construction, Blade Runner

5512 Illusion Mailer

5534 The Flu

5550 Xtcp

5555 ServeMe

5556 BO Facil

5557 BO Facil

5569 Robo-Hack

5637 PC Crasher

5638 PC Crasher

5742 WinCrash

5760 Portmap Remote Root Linux Exploit

5880 Y3K RAT

5882 Y3K RAT

5882 (UDP) - Y3K RAT

5888 Y3K RAT

5888 (UDP) - Y3K RAT

5889 Y3K RAT

6000 The Thing

6006 Bad Blood

6272 Secret Service

6400 The Thing

6661 TEMan, Weia-Meia

6666 Dark Connection Inside, NetBus worm

6667 Dark FTP, ScheduleAgent, SubSeven, Subseven 2.1.4 DefCon 8, Trinity, WinSatan

6669 Host Control, Vampire

6670 BackWeb Server, Deep Throat, Foreplay, WinNuke eXtreame

6711 BackDoor-G, SubSeven, VP Killer

6712 Funny trojan, SubSeven

6713 SubSeven

6723 Mstream

6771 Deep Throat, Foreplay

6776 2000 Cracks, BackDoor-G, SubSeven, VP Killer

6838 (UDP) - Mstream

6883 Delta Source DarkStar (??)

6912 Shit Heep

6939 Indoctrination

6969 GateCrasher, IRC 3, Net Controller, Priority

6970 GateCrasher

7000 Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold

7001 Freak88, Freak2k

7215 SubSeven, SubSeven 2.1 Gold

7300 NetMonitor

7301 NetMonitor

7306 NetMonitor

7307 NetMonitor

7308 NetMonitor

7424 Host Control

7424 (UDP) - Host Control

7597 Qaz

7626 Glacier

7777 God Message, Tini

7789 Back Door Setup, ICKiller

7891 The ReVeNgEr

7983 Mstream

8080 Brown Orifice, RemoConChubo, Reverse WWW Tunnel Backdoor, RingZero

8787 Back Orifice 2000

8988 BacHack

8989 Rcon, Recon, Xcon

9000 Netministrator

9325 (UDP) - Mstream

9400 InCommand

9872 Portal of Doom

9873 Portal of Doom

9874 Portal of Doom

9875 Portal of Doom

9876 Cyber Attacker, Rux

9878 TransScout

9989 Ini-Killer

9999 The Prayer

10000 OpwinTRojan

10005 OpwinTRojan

10067 (UDP) - Portal of Doom

10085 Syphillis

10086 Syphillis

10100 Control Total, Gift trojan

10101 BrainSpy, Silencer

10167 (UDP) - Portal of Doom

10520 Acid Shivers

10528 Host Control

10607 Coma

10666 (UDP) - Ambush

11000 Senna Spy Trojan Generator

11050 Host Control

11051 Host Control

11223 Progenic trojan, Secret Agent

12076 Gjamer

12223 Hack'99 KeyLogger

12345 Ashley, cron / crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill

12346 Fat Bitch trojan, GabanBus, NetBus, X-bill

12349 BioNet

12361 Whack-a-mole

12362 Whack-a-mole

12363 Whack-a-mole

12623 (UDP) - DUN Control

12624 ButtMan

12631 Whack Job

12754 Mstream

13000 Senna Spy Trojan Generator, Senna Spy Trojan Generator

13010 Hacker Brasil - HBR

13013 PsychWard

13014 PsychWard

13223 Hack'99 KeyLogger

13473 Chupacabra

14500 PC Invader

14501 PC Invader

14502 PC Invader

14503 PC Invader

15000 NetDemon

15092 Host Control

15104 Mstream

15382 SubZero

15858 CDK

16484 Mosucker

16660 Stacheldraht

16772 ICQ Revenge

16959 SubSeven, Subseven 2.1.4 DefCon 8

16969 Priority

17166 Mosaic

17300 Kuang2 the virus

17449 Kid Terror

17499 CrazzyNet

17500 CrazzyNet

17569 Infector

17593 Audiodoor

17777 Nephron

18753 (UDP) - Shaft

19864 ICQ Revenge

20000 Millenium

20001 Millenium, Millenium (Lm)

20002 AcidkoR

20005 Mosucker

20023 VP Killer

20034 NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job

20203 Chupacabra

20331 BLA trojan

20432 Shaft

20433 (UDP) - Shaft

21544 GirlFriend, Kid Terror

21554 Exploiter, Kid Terror, Schwindler, Winsp00fer

22222 Donald Dick, Prosiak, Ruler, RUX The TIc.K

23005 NetTrash

23006 NetTrash

23023 Logged

23032 Amanda

23432 Asylum

23456 Evil FTP, Ugly FTP, Whack Job

23476 Donald Dick

23476 (UDP) - Donald Dick

23477 Donald Dick

23777 InetSpy

24000 Infector

25685 Moonpie

25686 Moonpie

25982 Moonpie

26274 (UDP) - Delta Source

26681 Voice Spy

27374 Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader

27444 (UDP) - Trinoo

27573 SubSeven

27665 Trinoo

28678 Exploiter

29104 NetTrojan

29369 ovasOn

29891 The Unexplained

30000 Infector

30001 ErrOr32

30003 Lamers Death

30029 AOL trojan

30100 NetSphere

30101 NetSphere

30102 NetSphere

30103 NetSphere

30103 (UDP) - NetSphere

30133 NetSphere

30303 Sockets des Troie

30947 Intruse

30999 Kuang2

31335 Trinoo

31336 Bo Whack, Butt Funnel

31337 Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, cron / crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini

31337 (UDP) - Back Orifice, Deep BO

31338 Back Orifice, Butt Funnel, NetSpy (DK)

31338 (UDP) - Deep BO

31339 NetSpy (DK)

31666 BOWhack

31785 Hack'a'Tack

31787 Hack´a´Tack

31788 Hack´a´Tack

31789 (UDP) - Hack´a´Tack

31790 Hack´a´Tack

31791 (UDP) - Hack´a´Tack

31792 Hack´a´Tack

32001 Donald Dick

32100 Peanut Brittle, Project nEXT

32418 Acid Battery

33270 Trinity

33333 Blakharaz, Prosiak

33577 Son of PsychWard

33777 Son of PsychWard

33911 Spirit 2000, Spirit 2001

34324 Big Gluck, TN

34444 Donald Dick

34555 (UDP) - Trinoo (for Windows)

35555 (UDP) - Trinoo (for Windows)

37237 Mantis

37651 Yet Another Trojan - YAT

40412 The Spy

40421 Agent 40421, Masters Paradise

40422 Masters Paradise

40423 Masters Paradise

40425 Masters Paradise

40426 Masters Paradise

41337 Storm

41666 Remote Boot Tool - RBT, Remote Boot Tool - RBT

44444 Prosiak

44575 Exploiter

47262 (UDP) - Delta Source

49301 OnLine KeyLogger

50130 Enterprise

50505 Sockets des Troie

50766 Fore, Schwindler

51966 Cafeini

52317 Acid Battery 2000

53001 Remote Windows Shutdown - RWS

54283 SubSeven, SubSeven 2.1 Gold

54320 Back Orifice 2000

54321 Back Orifice 2000, School Bus

55165 File Manager trojan, File Manager trojan, WM Trojan Generator

55166 WM Trojan Generator

57341 NetRaider

58339 Butt Funnel

60000 Deep Throat, Foreplay, Sockets des Troie

60001 Trinity

60068 Xzip 6000068

60411 Connection

61348 Bunker-Hill

61466 TeleCommando

61603 Bunker-Hill

63485 Bunker-Hill

64101 Taskman

65000 Devil, Sockets des Troie, Stacheldraht

65390 Eclypse

65421 Jade

65432 The Traitor (= th3tr41t0r)

65432 (UDP) - The Traitor (= th3tr41t0r)

65534 /sbin/initd

65535 RC1 trojan