บทที่ 2

ภัยคุกคามและการโจมตี

2.1 บทนำ

เหตุการณ์หรือการกระทำที่เป็นการละเมิดความปลอดภัยของระบบคอมพิวเตอร์นั้นมีหลากหลายรูปแบบด้วยกัน ซึ่งแต่ละรูปแบบของการกระทำจะมีวิธีการและทำให้เกิดความเสียหายแตกต่างกัน บทนี้จะนำเสนอเนื้อหาเกี่ยวกับภัยคุกคามและการโจมตีในรูปแบบต่าง ๆ ที่กระทำกันในปัจจุบัน และมีผลต่อการรักษาความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย

2.2 ภัยคุกคาม (Threat) และการโจมตี (Attack)

ภัยคุกคาม [NCSC-TG-004, 1988] คือ บุคคล สิ่งของและเหตุการณ์ใด ๆ ก็ตามที่มุ่งร้ายหรือเป็นสาเหตุของภัยอันตรายต่าง ๆที่จะเกิดขึ้นกับระบบคอมพิวเตอร์ในรูปแบบของการทำลาย เปิดเผย แก้ไขข้อมูลและรวมถึงการที่ทำให้ระบบไม่สามารถให้บริการแก่ผู้ใช้ได้ โดยที่ภัยคุกคามอาจจะเกิดขึ้นโดยอุบัติเหตุ เช่น ไฟไหม้ น้ำท่วม เป็นต้น หรือเกิดขึ้นโดยเจตนาของบุคคลที่ประสงค์ร้ายต่อระบบโดยการโจมตี ซึ่งเป็นการกระทำโดยพยายามที่จะข้ามผ่าน (bypass) กระบวนการการควบคุมความปลอดภัยของระบบคอมพิวเตอร์

บุคคลที่กระทำการโจมตีหรือบุกรุกระบบหรือที่เรียกว่าผู้บุกรุก (Intruder) สามารถแบ่งได้เป็น 2 ประเภทคือ

1. ผู้บุกรุกจากภายนอก (Outsider Intruder) หมายถึง ผู้บุกรุกที่มาจากภายนอกเครือข่ายขององค์กร เช่น การโจมตีโดยผ่านเครือข่ายอินเทอร์เน็ตในรูปแบบต่าง ๆ
2. ผู้บุกรุกจากภายใน (Insider Intruder) หมายถึง ผู้บุกรุกที่เป็นผู้ใช้ซึ่งมีสิทธิในการใช้ระบบหรือเครือข่ายภายในองค์กร โดยรวมถึงผู้ใช้ที่ใช้สิทธิไปในทางที่ผิดหรือการลักลอบใช้สิทธิ์ของผู้ใช้คนอื่น ๆ

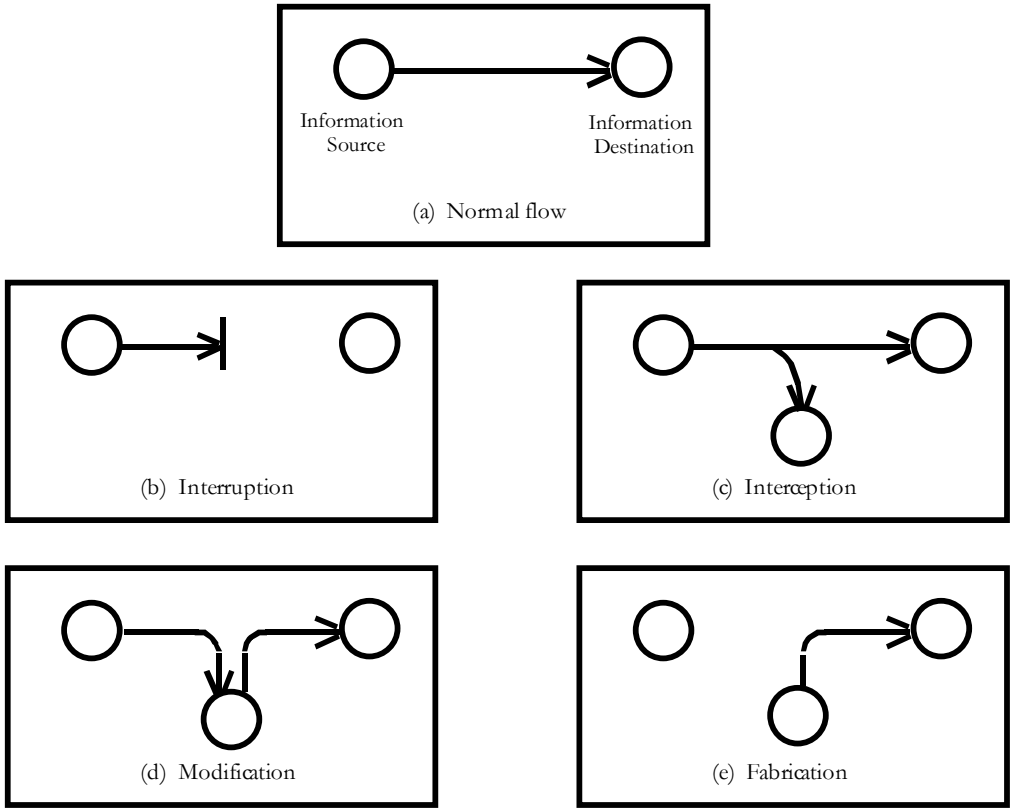
การโจมตีระบบหรือเครือข่ายนั้นผู้บุกรุกจะทำการโจมตีในลักษณะหรือรูปแบบที่แตกต่างกันทั้งนี้ขึ้นอยู่กับวัตถุประสงค์ของการโจมตี William Stallings [Stallings, 1995] ได้แบ่งประเภทการโจมตีตามลักษณะการกระทำ ได้ 4 ประเภทดังนี้

1. Interruption คือ การทำให้ทรัพยากรของระบบถูกทำลาย ทำให้ไม่สามารถให้บริการหรือไม่สามารถใช้งานได้อีก เช่น การทำลายอุปกรณ์หรือเครื่อง

คอมพิวเตอร์การตัดสายสัญญาณที่ใช้ในการติดต่อสื่อสาร การทำให้เครือข่ายท่วม (Network Flooding) เป็นต้น

2. Interception คือ การที่บุคคล โปรแกรมหรือเครื่องคอมพิวเตอร์ที่ไม่ได้รับอนุญาตสามารถเข้าถึงทรัพยากรหรือข้อมูลได้ เช่น การดักฟังสัญญาณการสื่อสาร (Wiretapping) บนสายสัญญาณสื่อสารในเครือข่าย การคัดลอกไฟล์หรือโปรแกรมโดยไม่ได้รับอนุญาต เป็นต้น
3. Modification คือ การที่บุคคลหรือโปรแกรมที่ไม่ได้รับอนุญาตสามารถเข้าถึงทรัพยากรและแก้ไขได้ด้วย เช่น การแก้ไขข้อมูลในไฟล์ การปรับเปลี่ยนโปรแกรมให้มีการทำงานที่ต่างไปจากการทำงานปกติหรือการแก้ไขข้อมูลที่รับส่งในเครือข่าย
4. Fabrication คือ การที่บุคคลหรือโปรแกรมที่ไม่ได้รับอนุญาตปลอมแปลงข้อมูลขึ้นมาในระบบ เช่น การปลอมข้อมูล ข่าวสารที่รับส่งในเครือข่าย การเพิ่มข้อมูลในไฟล์

โดยลักษณะของการโจมตีทั้ง 4 ประเภทสามารถแสดงเป็นแผนภาพได้ดังภาพประกอบ 2.1



ภาพประกอบ 2.1 แผนภาพแสดงลักษณะการโจมตี

ที่มา : Stallings, William. 1995

สำหรับการโจมตีประเภท Interception นั้น William Stallings ได้จัดให้เป็นการโจมตีแบบ passive และการโจมตีประเภท Interruption, Modification และ Fabrication เป็นการโจมตีแบบ active ซึ่งวิธีการและรูปแบบของการโจมตีแบบ active และ passive ได้กล่าวในหัวข้อ 2.3 และ 2.4 ตามลำดับ

2.3 Active Attack

การโจมตีแบบ active เป็นการโจมตีที่ทำให้เกิดการแก้ไข/เปลี่ยนแปลงของข้อมูลหรือระบบ และการสร้างข้อมูลขึ้นมาใหม่โดยการปลอมแปลง เช่น การเปลี่ยนแปลงข้อมูลในไฟล์หรือการเพิ่มไฟล์ที่ไม่ได้รับอนุญาตเข้าไปในระบบ รวมถึงการทำให้ระบบไม่สามารถให้บริการผู้ใช้ได้ การโจมตีรูปแบบนี้สามารถตรวจจับได้ง่าย เนื่องจากมีร่องรอยการกระทำที่สามารตรวจสอบดูได้ แต่การป้องกันจะทำได้ค่อนข้างยาก วิธีการโจมในรูปแบบ active โดยทั่วไปมีดังนี้

2.3.1 ไวรัส (Virus)

ไวรัสคือชุดคำสั่งหรือโปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปอยู่ในระบบคอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่น ๆ แต่ไวรัสจะไม่สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ด้วยตัวมันเอง โดยทั่วไปเกิดจากการที่ผู้ใช้เป็นพาหะ นำไวรัสจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง เช่น เมื่อผู้ใช้ส่งอีเมล์โดยแนบไฟล์ที่มีไวรัสไปด้วย การแลกเปลี่ยนไฟล์โดยใช้แผ่นดิสก์เก็ตและเมื่อผู้ใช้รับไฟล์มาใช้ไวรัสก็จะแพร่กระจายไปยังเครื่องของผู้ใช้นั้นและจะเป็นวงจรในลักษณะนี้ต่อไปเรื่อย ๆ จุดประสงค์และรายละเอียดการทำงานของไวรัสแต่ละตัวขึ้นอยู่กับผู้เขียนโปรแกรมไวรัสนั้น ๆ เช่น อาจสร้างไวรัสสำหรับไปทำลายโปรแกรมหรือข้อมูลอื่น ๆ ที่อยู่ในเครื่องคอมพิวเตอร์หรือแสดงข้อความทางจอภาพ เป็นต้น

ตัวอย่างไวรัสคอมพิวเตอร์ที่เป็นที่รู้จักกันโดยทั่วไป เช่น Stoned, Melissa, CIH/Chernobyl, Michelangello หรือแม้แต่ไวรัสที่ใช้ชื่อไทย เช่น ลาวดวงเดือน เป็นต้น

ประเภทของไวรัส

โปรแกรมไวรัสมีหลากหลายชนิด ซึ่งสามารถจัดประเภทของไวรัสตามการทำงานได้ดังนี้

1. Boot Sector Virus หรือ Boot Infector Virus คือไวรัสที่เก็บตัวเองอยู่ในบูตเซกเตอร์ (Boot Sector) ของดิสก์ ส่วนของบูตเซกเตอร์นี้จะถูกใช้งานเมื่อ

มีการเปิดเครื่องคอมพิวเตอร์ขึ้นมา โดยระบบอ่านข้อมูลในบูตเซกเตอร์ ซึ่งมีโปรแกรมเล็กๆ ไว้ใช้ในการเรียกระบบปฏิบัติการขึ้นมาทำงาน ดังนั้นบูตเซกเตอร์ไวรัสจะเข้าไปแทนที่โปรแกรมดังกล่าว และไวรัสประเภทนี้ถ้าไปอยู่ในฮาร์ดดิสก์ ก็จะเข้าไปอยู่บริเวณที่เรียกว่า Master Boot Sector หรือ Parition Table ของฮาร์ดดิสก์ ดังนั้นถ้าบูตเซกเตอร์ของดิสก์ใดมีไวรัสประเภทนี้อยู่ ทุกครั้งที่บูตเครื่องขึ้นมาโดยมีการเรียกระบบปฏิบัติการจากดิสก์ตัวดังกล่าว โปรแกรมไวรัสจะทำงานก่อนและจะเข้าไปฝังตัวอยู่ในหน่วยความจำเพื่อเตรียมพร้อมที่จะทำงานตามที่ได้ถูกกำหนดไว้ ไวรัสประเภทนี้ ได้แก่ ไวรัส Michelangello, Empire และ Stoned เป็นต้น

2. Program Virus หรือ File Infector Virus เป็นไวรัสอีกประเภทหนึ่งที่จะแฝงตัวอยู่กับโปรแกรมซึ่งปกติก็คือ ไฟล์ที่มีนามสกุลเป็น .COM หรือ .EXE บนระบบปฏิบัติการวินโดวส์ นอกจากนี้ไวรัสบางชนิดอาจจะถูกเก็บไว้ในโปรแกรมที่มีนามสกุลเป็น .SYS, .DLL และ .OVL ได้ด้วย ซึ่งวิธีการที่ใช้เพื่อทำการนำไวรัสไปใส่ในโปรแกรมมีอยู่สองวิธี คือ การแทรกตัวเองเข้าไปอยู่ในโปรแกรม ผลก็คือหลังจากที่โปรแกรมนั้นมีไวรัสแล้ว ขนาดของโปรแกรมจะใหญ่ขึ้นหรืออาจมีการสำเนาตัวเองเข้าไปทับส่วนของโปรแกรมที่มีอยู่เดิมซึ่งทำให้ขนาดของโปรแกรมไม่เปลี่ยน และยากที่จะซ่อมให้กลับเป็นดังเดิม การทำงานโดยทั่วไปของไวรัสชนิดนี้คือ เมื่อมีการเรียกโปรแกรมที่มีไวรัส ส่วนของไวรัสจะทำงานก่อนและจะถือโอกาสนี้ฝังตัวเข้าไปอยู่ในหน่วยความจำทันทีแล้วจึงให้โปรแกรมนั้นทำงานตามปกติต่อไป เมื่อไวรัสเข้าไปฝังตัวอยู่ในหน่วยความจำแล้ว หลังจากนี้ไปถ้ามีการเรียกโปรแกรมอื่นๆ ขึ้นมาทำงานต่อ ตัวไวรัสก็จะสำเนาตัวเองเข้าไปในโปรแกรมเหล่านั้นเป็นการแพร่ระบาดต่อไป ส่วนวิธีการแพร่ระบาดของโปรแกรมไวรัสอีกวิธีหนึ่งก็คือ เมื่อมีการเรียกโปรแกรมที่มีไวรัสอยู่ไวรัสจะเข้าไปหาโปรแกรมอื่นๆ ที่อยู่ในดิสก์เพื่อทำสำเนาตัวเอง แล้วจึงให้โปรแกรมที่ถูกเรียก นั้นทำงานตามปกติต่อไป ไวรัสประเภทนี้ ได้แก่ ไวรัส WinVir, CIH/Chernobyl และ Christmas tree เป็นต้น

3. Polymorphic Virus เป็นชื่อที่ใช้ในการเรียกไวรัสที่มีความสามารถในการแปรเปลี่ยนตัวเองได้เมื่อมีสร้างสำเนาตัวเองเกิดขึ้น ซึ่งอาจแปรเปลี่ยนได้หลากหลายรูปแบบ ผลก็คือ ทำให้ไวรัสเหล่านี้ยากต่อการถูกตรวจจับด้วยโปรแกรมตรวจหาไวรัส ไวรัสประเภทนี้ ได้แก่ ไวรัส DarkParanoid, Whale และ WildLick เป็นต้น

4. Stealth Virus เป็นชื่อที่ใช้เรียกไวรัสที่มีความสามารถในการพรางตัวต่อการตรวจจับได้ เช่น ไวรัสแบบ File Intector เมื่อไวรัสไปแฝงตัวอยู่กับโปรแกรมใดแล้วจะทำให้ขนาดของโปรแกรมนั้นใหญ่ขึ้น แต่ถ้าโปรแกรมไวรัสนั้นเป็นแบบ stealth virus จะไม่สามารถตรวจดูขนาดที่แท้จริงของโปรแกรมที่เพิ่มขึ้นได้ เนื่องจากตัวไวรัสจะเข้าไปควบคุมระบบปฏิบัติการ เมื่อมีการใช้คำสั่งแสดงข้อมูลของไฟล์ เช่น DIR หรือโปรแกรมใดก็ตามเพื่อตรวจดูขนาดของโปรแกรม ระบบปฏิบัติการก็จะแสดงขนาดเหมือนเดิม ทุกอย่างราวกับว่าไม่มีอะไรเกิดขึ้น ไวรัสประเภทนี้ ได้แก่ ไวรัส Brain, Soulfly, Shrapnel และ Pandemonium เป็นต้น
5. Macro Virus โดยทั่วไปไฟล์ข้อมูลจะไม่สามารถแพร่กระจายไวรัสได้เพราะไม่สามารถสั่งให้ไฟล์ดังกล่าวทำงานได้ แต่โปรแกรมในปัจจุบัน เช่น Microsoft Word, Excel และชุด Office ได้เพิ่มความสามารถขึ้นโดยได้เพิ่มส่วนของภาษามาโคร (Macro Language) ในการทำงานกับไฟล์ข้อมูล ซึ่งคำสั่งมาโครเหล่านี้จะทำงานโดยอัตโนมัติตามเหตุการณ์ที่กำหนด เช่น ทำงานเมื่อเปิดไฟล์ ซึ่งความสามารถดังกล่าวได้นำไปสู่การพัฒนาไวรัสในรูปแบบของ Macro Virus โดยจะแฝงอยู่กับไฟล์ข้อมูลหรือไฟล์ซึ่งใช้เป็นต้นแบบ (Template) ในการสร้างเอกสาร (ประเภท document, spreadsheet และ powerpoint เป็นต้น) หลังจากที่ต้นแบบในการใช้สร้างเอกสารมีไวรัสแล้ว ทุกๆ เอกสารที่เปิดขึ้นใช้ด้วยต้นแบบนั้นก็จะมีไวรัสด้วย ไวรัสประเภทนี้ได้แก่ ไวรัส Access.Lovely, Winword/Concept, Excel/Compat และ Word97/Melissa เป็นต้น
6. Visual Basic Script Virus ซึ่ง Visual Basic Script หรือ VBSscript เป็นภาษาหนึ่งที่ใช้เขียนร่วมกับภาษา HTML ในพัฒนาเว็บเพจ ดังนั้นไวรัสที่พัฒนาด้วย VBScript จะซ่อนตัวในเว็บไซต์ต่างๆ และเมื่อผู้ใช้งานเปิดเว็บเพจที่มีไวรัสนี้อยู่ ก็จะโจมตีเครื่องของผู้ใช้ผ่านโปรแกรม Web Browser แล้วหลังจากนั้นก็แพร่กระจายผ่านอีเมล์ โดยใช้โปรแกรม Microsoft Outlook เพื่อโจมตีหรือกระจายไวรัสไปยังผู้อื่นต่อไป โดยอาศัย mailing list หรือรายชื่ออีเมล์ที่เก็บอยู่ในเครื่องนั้นๆ นอกจากนี้ VBScript ยังสามารถเข้าถึงและทำงานกับไฟล์ระบบบนเครื่องคอมพิวเตอร์ของผู้ใช้ซึ่งเปิดเว็บเพจที่มีไวรัสนั้นได้ด้วยเช่นกัน ไวรัสประเภทนี้ได้แก่ ไวรัส VBS/Haptime, VBS/Redlof, VBS/AnnaKournikova และ JS.Fortnight เป็นต้น

7. Companion Virus เป็นไวรัสที่อาศัยจุดอ่อนในเรื่องลำดับความสำคัญในการทำงานของนามสกุลไฟล์โปรแกรม โดยทั่วไปเมื่อผู้ใช้พิมพ์ชื่อโปรแกรมที่ต้องการทำงาน ระบบจะตรวจสอบว่ามีชื่อไฟล์โปรแกรมที่ต้องการและนามสกุลเป็น .com ก่อน แต่หากไม่มีแล้วจึงจะหาชื่อไฟล์โปรแกรมที่มีนามสกุลเป็น .exe ต่อในภายหลัง หลักการทำงานไวรัสประเภทนี้คือหาไฟล์โปรแกรมที่มีนามสกุลเป็น .exe และสร้างไฟล์ที่เป็นไวรัสให้มีชื่อเหมือนกันกับชื่อไฟล์ดังกล่าว แต่มีนามสกุลเป็น .com ดังนั้นเมื่อผู้ใช้พิมพ์คำสั่งเรียกใช้โปรแกรม โปรแกรมที่เป็นไวรัสก็จะถูกสั่งให้ทำงานก่อน แล้วจึงส่งการทำงานไปยังไฟล์โปรแกรมที่เป็น .exe ในภายหลัง ดังนั้นหากในระบบมีไวรัสประเภทนี้อยู่ สามารถสังเกตได้ง่ายคือ มีไฟล์ที่มีนามสกุล .com มากเป็นพิเศษและมีไฟล์ที่มีชื่อเหมือนกันโดยมีทั้งนามสกุล .com และ .exe กัน ไวรัสประเภทนี้ได้แก่ ไวรัส W32/Parrot-A, W32/Lovgate, Win95.Companion และ Sandrine เป็นต้น
8. Cluster Virus / Directory Virus ไวรัสประเภทนี้ทำงานโดยการเปลี่ยนแปลงข้อมูลเกี่ยวกับไดเรคตอรี่ของไฟล์ต่าง ๆให้ชี้ไปยังตำแหน่งที่เก็บโปรแกรมไวรัสแทนที่จะชี้ไปยังตำแหน่งที่เก็บไฟล์โปรแกรมปกติ ดังนั้นเมื่อสั่งให้ไฟล์โปรแกรมทำงาน ไวรัสก็จะทำงานก่อนแล้วจึงสั่งให้โปรแกรมที่ต้องการทำงานในภายหลัง ไวรัสประเภทนี้ได้แก่ ไวรัส DIR-II และ Byway เป็นต้น
9. Hoax หรือ ข่าวไวรัสหลอกลวง เป็นรูปแบบหนึ่งของการก่อกวนที่มีผลต่อผู้ใช้คอมพิวเตอร์จำนวนมาก โดยไวรัสหลอกลวงพวกนี้จะมาในรูปของอีเมล์ การส่งข้อความต่อ ๆ กันไปผ่านทางโปรแกรมรับส่งข้อความหรือห้องสนทนาต่าง ๆ ซึ่งสามารถสร้างความวุ่นวายให้เกิดขึ้นได้มากหรือน้อยเพียงใดนั้นขึ้นกับเทคนิคและการใช้จิตวิทยาของผู้สร้างข่าวขึ้นมา โดยส่วนใหญ่อีเมล์ประเภทนี้จะมีหัวข้อที่ชวนเชื่อ อ้างแหล่งข้อมูลและบริษัทใหญ่ ๆ เป็นการสร้างความเชื่อมั่นและเมื่อผู้รับส่งต่อไปยังเพื่อนสนิทและคนคุ้นเคยก็ยิ่งสร้างความเชื่อมั่นมากขึ้น จากนั้นผู้รับก็จะทำตัวเป็นผู้ส่งต่อไปอีกหลาย ๆทอด ซึ่งเป็นลักษณะเด่นของข่าวไวรัสหลอกลวง หากได้รับจดหมายประเภทนี้ก็ไม่ควรที่จะส่งไปต่อ แต่ควรตรวจสอบจากแหล่งข้อมูลที่ถูกต้องก่อนทำการส่งต่อไป ส่วนเหตุผลที่ทำให้ข่าวไวรัสหลอกลวงถูกจัดว่าเข้าข่ายไวรัสคอมพิวเตอร์ เพราะว่าเป็นการเอาจุดเด่นในด้านพฤติกรรมของผู้ใช้อีเมล์ที่สามารถส่งจดหมายหรือข้อความที่เข้าถึงคนหมู่มากได้ในเวลาอันรวดเร็ว มาเป็นเครื่องมือ

ในการสร้างความเสียหาย ซึ่งลักษณะนี้เปรียบได้กับไวรัสที่มีการระบาดและกระจายตัวไปอย่างรวดเร็ว ซึ่งบุคคลที่ส่งอีเมล์ดังกล่าวออกไป ก็เปรียบเสมือนพาหะของไวรัส ซึ่งวิธีการป้องกัน คือ หากได้รับอีเมล์ที่มีข้อความในทำนองที่กล่าวข้างต้น ควรลบทิ้งทันทีและไม่ควรส่งต่อให้ผู้อื่น เนื่องจากเป็นข่าวที่ไม่เป็นความจริง แล้วยังเป็นการเพิ่มภาระให้กับระบบเครือข่ายอีกด้วย

2.3.2 ม้าโทรจัน (Trojan Horse)

เป็นการโจมตีที่ได้รับการตั้งชื่อตามตำนานม้าโทรจัน โดยที่ในทางคอมพิวเตอร์นั้นม้าโทรจันหมายถึงโปรแกรมที่มุ่งประสงค์ร้ายต่อระบบแต่ได้ปลอมหรือหลอกผู้ใช้ให้เข้าใจว่าเป็นโปรแกรมที่ดีมีประโยชน์ไม่มีอันตรายใด ๆ แต่เมื่อโปรแกรมถูกนำเข้าและทำงานก็จะปฏิบัติการอื่น ๆ นอกจากหน้าที่เดิม เช่น การขโมยข้อมูลความลับต่าง ๆ เช่น บัญชีผู้ใช้และรหัสผ่าน เป็นต้น การยึดเป็นฐานที่มั่นเพื่อโจมตีคอมพิวเตอร์เครื่องอื่น หรือเมื่อผู้ใช้เปิดโปรแกรมม้าโทรจันขึ้นมาก็จะเป็นการเปิดช่องทางให้บุคคลอื่นที่มีโปรแกรมควบคุมเข้ามากระทำการมิชอบที่เครื่องของของตนเองได้

โปรแกรมม้าโทรจันถือเป็นโปรแกรมที่ไม่มีคำสั่งหรือการทำงานที่เป็นอันตรายต่อคอมพิวเตอร์โดยตรงและเป็นโปรแกรมที่ไม่สามารถแพร่กระจายได้ ซึ่งจะไม่เหมือนกับไวรัสที่สามารถแพร่กระจายไปยังโปรแกรมหรือไฟล์อื่น ๆ บนเครื่องได้ สามารถแบ่งโปรแกรมม้าโทรจันออกเป็นหลายประเภทตามลักษณะการคุกคามและการทำงาน เช่น

- Client/Server เป็นโปรแกรมม้าโทรจันที่ประกอบด้วยโปรแกรม 2 ส่วน โดยโปรแกรมส่วนที่ถูกส่งไปทำงานบนเครื่องปลายทางที่ต้องการจะเรียกว่า เซิร์ฟเวอร์ (Server) และเมื่อโปรแกรมส่วนนี้ถูกติดตั้งและทำงานแล้วก็จะเปิดช่องทางให้โปรแกรมอีกส่วนที่ทำงานอยู่บนเครื่องของผู้บุกรุก ซึ่งจะเรียกว่า ไคลเอ็นต์ (Client) สามารถควบคุมเครื่องดังกล่าวได้จากระยะไกล โปรแกมม้าโทรมันประเภทนี้ ได้แก่ Back Orifice, Subseven และ Netbus เป็นต้น
- Keylogger โปรแกรมประเภทนี้จะทำหน้าที่บันทึกการกดคีย์ต่าง ๆ ในขณะที่กำลังใช้คอมพิวเตอร์ ซึ่งรวมถึงการกดคีย์เพื่อใส่ข้อมูลบัญชีผู้ใช้และรหัสผ่านด้วย แล้วบันทึกหรือส่งข้อมูลนี้ไปยังผู้บุกรุก เพื่อให้ผู้บุกรุกสามารถนำข้อมูลเหล่านี้มาใช้เป็นประโยชน์ในการบุกรุกในภายหลัง

โปรแกรมม้าโทรจันส่วนใหญ่จะแฝงตัวมาในรูปแบบของโปรแกรมเกมส์ การ์ดอวยพร รูปภาพสกรีนเซฟเวอร์ (screen saver) และรูปแบบอื่น ๆ ที่ทำให้มีความน่าสนใจที่จะสั่งให้ทำงาน ดังนั้นแนวทางการป้องกันก็คือ จะต้องไม่เปิดหรือสั่งงานโปรแกรมใดก็ตาม ที่ได้

รับมาจากแหล่งที่ไม่มีความน่าเชื่อถือหรือไม่รู้จัก และควรจะต้องมีการตรวจสอบความถูกต้องสมบูรณ์ของโปรแกรมก่อนการใช้งาน

2.3.3 แบคทีเรียม (Bacterium)

แบคทีเรียมเป็นโปรแกรมคอมพิวเตอร์ที่จะทำการคัดลอกตัวเอง (replicate) ภายในระบบคอมพิวเตอร์ที่อาศัยอยู่ จนกระทั่งครอบครองการทำการงานของหน่วยประมวลผล หน่วยความจำหรือพื้นที่ของดิสก์หรือทรัพยากรอื่นๆ ของระบบ จนทำให้ระบบทำงานช้าลงและไม่สามารถให้บริการได้ในที่สุด สำหรับการแพร่กระจายของแบคทีเรียมภายในเครื่องคอมพิวเตอร์แต่ละเครื่องนั้นสามารถทำได้ด้วยตัวเอง ในลักษณะของการคัดลอกตัวเองขึ้นมา ต่างจากไวรัสที่ต้องไปอาศัยหรือแฝงตัวกับไฟล์หรือโปรแกรมอื่นๆ แต่อย่างไรก็ตามสำหรับการแพร่กระจายไปยังเครื่องอื่นๆ ต้องอาศัยผู้ใช้เป็นพาหนะเช่นเดียวกับไวรัส

2.3.4 เวิร์ม (Worm)

เวิร์มเป็นโปรแกรมคอมพิวเตอร์ ที่สามารถแพร่กระจายได้ด้วยตัวเองผ่านเครือข่ายไปยังคอมพิวเตอร์หรืออุปกรณ์อื่นๆ ที่ต่ออยู่บนเครือข่ายด้วยกัน ลักษณะการแพร่กระจายคล้ายตัวหนอนที่เจาะไชไปยังเครื่องคอมพิวเตอร์ต่างๆ แพร่พันธุ์ด้วยการคัดลอกตัวเองออกเป็นหลายๆ โปรแกรมและส่งต่อผ่านเครือข่ายออกไป

กำเนิดของเวิร์มเกิดขึ้นในปี ค.ศ. 1988 โดยโรเบิร์ต มอริส (Robert Morris, Jr.) ซึ่งประวัติของเวิร์มดูได้จาก [Schmidt and Darby, 2001] เวิร์มถือว่าเป็นโปรแกรมคอมพิวเตอร์ชนิดหนึ่งที่แพร่ระบาดได้ด้วยตัวเองจากเครื่องคอมพิวเตอร์หนึ่งสู่เครื่องคอมพิวเตอร์หนึ่งโดยไม่ทำลายไฟล์หรือข้อมูล ต่างจากไวรัสที่อาจจะมีการทำลายไฟล์หรือข้อมูลต่างๆในระบบ และไวรัสจะต้องมีพาหะในแพร่ระบาดไปยังเครื่องอื่นๆ ในปัจจุบันเวิร์มจะมาในรูปแบบของอีเมล์ โดยเมื่อมีผู้ส่งจดหมายอิเล็กทรอนิกส์และแนบโปรแกรมติดมาด้วยในส่วนของไฟล์ที่แนบมาด้วย (attached file) และสำหรับผู้ใช้บนระบบปฏิบัติการวินโดวส์สามารถคลิกไฟล์เหล่านั้นเพื่อเรียกใช้หรืออ่านไฟล์ได้ ซึ่งเท่ากับเป็นการเรียกโปรแกรมที่ส่งมาให้ทำงาน ถ้าสิ่งที่ส่งมานี้เป็นเวิร์ม ก็จะเป็นการเริ่มต้นการทำงาน โดยจะคัดลอกตัวเองและส่งจดหมายอิเล็กทรอนิกส์ไปให้ผู้อื่นอีก ตัวอย่างเวิร์มที่แพร่กระจายผ่านจดหมายอิเล็กทรอนิกส์ที่รู้จักกันแพร่หลายคือ Love BUG/Love Letter ซึ่งระบาดเมื่อ 4 พฤษภาคม 2543 [CERT Advisory CA-2000-04, 2000] สร้างความเสียหายกับข้อมูลจำนวนมหาศาล ความจริงการแพร่ขยายระบาดของเวิร์มมีมาหลายครั้งแล้ว แต่

เวิร์มหลายตัวไม่ได้สร้างความเสียหายมากนัก เพราะไม่ได้ทำลายระบบคอมพิวเตอร์หรือข้อมูล แต่เวิร์ม Love BUG/Love Letter ได้เข้าไปทำลายข้อมูลในเครื่องของผู้ใช้ สำหรับเวิร์มตัวนี้เขียนขึ้นเป็นไฟล์ .vbs (Visual Basic Script) ซึ่งสามารถเรียกใช้งานได้ทันทีเหมือนไฟล์โปรแกรม

2.3.5 ประตูลับ (Trapdoor/Backdoor)

ประตูลับเป็นกลไกทางด้านซอฟต์แวร์หรือฮาร์ดแวร์ โดยผู้พัฒนาทำขึ้นเพื่อผ่านระบบการป้องกันเข้าไปทำงาน ซึ่งประตูลับเป็นวิธีการในผ่านการควบคุมและได้มาซึ่งสิทธิระดับผู้ดูแลระบบหรือ superuser ซึ่งเดิมผู้พัฒนาโปรแกรมจะใช้ในการติดตามและทดสอบโปรแกรมโดยที่สามารถไปยังจุดที่ต้องการได้ถ้ามีปัญหาที่ต้องแก้ไข ส่วนใหญ่ backdoor จะถูกเอาออกก่อนที่ส่งโปรแกรมไปยังลูกค้า แต่ก็ไม่เสมอไปและในบางครั้งประตูลับจะถูกสร้างหรือติดตั้งโดยโปรแกรมที่มุ่งประสงค์ร้าย เช่น ไวรัส ม้าโทรจัน เป็นต้น

ในเชิงประวัติศาสตร์แล้วประตูลับนั้นมีมานานแล้ว ซึ่งจากเอกสารเรื่อง "Reflections on Trusting Trust" โดย Ken Thompson [Thompson, 1984] ได้เปิดเผยประตูลับที่มีอยู่ในยูนิกซ์รุ่นต้นๆ ที่อาจถือว่าเป็นการเจาะระบบความปลอดภัยด้วยเช่นกัน

ปัจจุบันมีการนำเอาลักษณะการทำงานของประตูลับไปใช้ร่วมกับการโจมตีวิธีการอื่นด้วย โดยเฉพาะการนำไปใช้ร่วมกับโปรแกรมประเภทม้าโทรจัน เพื่อสร้างช่องทางให้ผู้บุกรุกสามารถมาควบคุมเครื่องคอมพิวเตอร์ที่ถูกโจมตีได้จากระยะไกล ตัวอย่างโปรแกรมที่มีการทำงานในลักษณะนี้ เช่น Back Orifice, Subseven และ NetBus เป็นต้น นอกจากนี้เวิร์มบางตัวก็จะมีการติดตั้งประตูลับไว้ในเครื่องคอมพิวเตอร์ที่เวิร์มแฝงตัวอยู่ด้วยเช่นกัน เช่น SoBig, Mydoom เป็นต้น

2.3.6 Logic Bomb/Time Bomb

Logic Bomb และ Time Bomb เป็นโปรแกรมที่มุ่งประสงค์ร้ายจำพวกไวรัสหรือเวิร์มที่พัฒนาขึ้นโดยมีการกำหนดเงื่อนไขในการทำงานของตัวเองอยู่ ซึ่ง Time Bomb จะทำงานโดยใช้เงื่อนไขของวันที่และเวลา นั่นคือโปรแกรมจะทำงานก็ต่อเมื่อถึงวันที่หรือเวลาที่กำหนดไว้เท่านั้น ส่วน Logic Bomb จะทำงานก็ต่อเมื่อมีเงื่อนไขหรือสภาพการณ์ตามที่ผู้สร้างโปรแกรมกำหนดขึ้น เช่น เงื่อนไขการมีไฟล์หรือไม่มีไฟล์ที่กำหนดในระบบหรือทำงานเมื่อผู้ใช้มีการเรียกใช้งานโปรแกรมที่กำหนดไว้ เป็นต้น

ตัวอย่างการทำงานของ Time Bomb เช่น ไวรัส Friday 13th จะมีการทำลายไฟล์ข้อมูลในเครื่องคอมพิวเตอร์ในทุกวันศุกร์ที่ 13 เป็นต้น โปรแกรมที่ทำงานในลักษณะของ Logic

Bomb และ Time Bomb นี้จะไม่เหมือนกับไวรัสเพราะว่า Logic Bomb นั้นทำงานครั้งเดียวหรือที่ช่วงเวลาใดเวลาหนึ่งเท่านั้น แต่การกระทำของไวรัสนั้นทำงานอย่างต่อเนื่องตลอดเวลา

2.3.7 การปลอมแปลง (Masquerade)

การปลอมแปลง คือการที่เอนทิตี้ (entity) หนึ่งได้แอบอ้างว่าเป็นอีกเอนติตี้หนึ่ง โดยที่เอนติตี้ในที่นี้อาจจะเป็น ผู้ใช้ โปรเซส หรือเครื่องคอมพิวเตอร์ในเครือข่าย ก็ได้ ซึ่งวัตถุประสงค์ของการปลอมแปลงก็เพื่อให้สามารถเข้าถึงหรือใช้งานระบบคอมพิวเตอร์ที่ต้องการได้ ส่วนใหญ่วิธีการนี้จะใช้ร่วมกับการโจมตีในลักษณะ active attack วิธีการอื่น เช่น การปลอมหมายเลข IP ของผู้ส่งข้อความผ่านเครือข่าย เป็นต้น

2.3.8 Denial of Service (DoS)

การโจมตีแบบ DoS โดยทั่วไปมีจุดประสงค์เพื่อป้องกันไม่ให้ผู้ใช้ที่มีสิทธิใช้งานตามปกติสามารถใช้งานได้หรือทำให้เกิดความเสียหายต่อการใช้งานคอมพิวเตอร์หรือทรัพยากรของระบบเครือข่าย ระบบที่เชื่อมต่อกับอินเทอร์เน็ตมักจะถูกโจมตีแบบ DoS ก็เนื่องมาจากเครือข่ายอินเทอร์เน็ตประกอบไปด้วยทรัพยากรที่มีอยู่อย่างจำกัด โครงสร้างพื้นฐานของการเชื่อมต่อในโลกของอินเทอร์เน็ตนั้นประกอบไปด้วยทรัพยากรที่มีอยู่อย่างจำกัด เช่น แบนด์วิดธ์ (Bandwidth) พลังในการประมวลผล (processing power) และพื้นที่ที่จำกัดของการเก็บข้อมูล ล้วนแต่เป็นเป้าหมายในการโจมตีแบบ DoS ซึ่งมีวัตถุประสงค์คือให้มีการใช้งานทรัพยากรที่มีอยู่จนถึงขั้นที่ทำให้ระบบมีปัญหาได้

การโจมตีแบบ DoS นั้นเป็นการโจมตีที่จะพยายามทำให้งานที่ทำหรือบริการต่าง ๆ ที่ทำงานอยู่บนเครื่องเป้าหมายไม่สามารถทำงานได้โดยการส่งคำร้องขอ (requests) ไปยังเครื่องเป้าหมายเป็นจำนวนมากจนเกินความสามารถที่เครื่องนั้นจะให้บริการได้ จนหยุดการทำงานหรือไม่สามารถให้บริการได้ตามปกติ ซึ่งวิธีการโจมตี เช่น

- การทำให้เครือข่ายท่วม เป็นการพยายามทำให้เครือข่ายเต็มไปด้วยข้อมูลที่ไม่มีประโยชน์ต่อผู้ใด โดยเป้าหมายเพียงให้ข้อมูลที่ใช้งานปกติไม่สามารถส่งผ่านไปยังต้นทางและปลายทาง ซึ่งในกรณีนี้ทั้งเซิร์ฟเวอร์ต้นทางและไคลเอ็นต์ปลายทางต่างก็ยังทำงานได้ตามปกติ แต่ช่องทางการสื่อสารถูกปิดกั้นไว้ ซึ่งในที่สุดการให้บริการและการใช้บริการระหว่างเซิร์ฟเวอร์และไคลเอ็นต์ก็จะไม่สามารถทำได้
- การตัดการสื่อสารที่สำคัญของระบบ เช่น สำหรับเว็บไซต์ที่จะต้องทำการอ่านข้อมูลจากเครื่องที่ทำหน้าที่ให้บริการฐานข้อมูลหรือดาต้าเบสเซิร์ฟเวอร์ (Database

Server) เพื่อนำข้อมูลมาแสดงบนเว็บเพจ แทนที่ผู้โจมตีจะทำการโจมตีเว็บเซิร์ฟเวอร์หรือดาต้าเบสเซิร์ฟเวอร์ซึ่งอาจจะมีการป้องกันที่ดี ก็ทำการโจมตีจุดเชื่อมต่อระหว่างเซิร์ฟเวอร์ทั้งคู่ไม่ให้สามารถสื่อสารกันได้ ทำให้เว็บเซิร์ฟเวอร์ไม่สามารถนำข้อมูลมาแสดงผลได้และเว็บไซต์ก็ไม่สามารถให้บริการได้ในที่สุด รวมทั้งการพยายามทำให้การสื่อสารระหว่างเครื่อง 2 เครื่องเป็นไปด้วยความยากลำบาก

- การขัดขวางไม่ให้ผู้ใช้ปกติสามารถใช้บริการได้ เช่น การพยายามสร้างการเชื่อมต่อปลอมระหว่างเว็บเซิร์ฟเวอร์กับเครื่องของผู้โจมตีให้มากที่สุด ซึ่งหากระบบที่ถูกโจมตีแบบ DoS นั้นมีข้อจำกัดของจำนวนการเชื่อมต่อที่สามารถรองรับได้ไม่มากนัก ก็จะทำให้ไม่สามารถให้บริการผู้ใช้ปกติที่เข้ามาในภายหลังได้ เนื่องจากเว็บเซิร์ฟเวอร์ได้ใช้ทรัพยากรไปบริการการเชื่อมต่อปลอมนั้นจนหมด

รูปแบบการโจมตีแบบ DoS

อะนอมาลัสแพ็กเก็ต (Anomalous Packet)

อะนอมาลัสแพ็กเก็ต หมายถึงแพ็กเก็ตที่มีความผิดปกติซึ่งไม่มีโอกาสเกิดขึ้นในสภาวะการทำงานปกติได้ แพ็กเก็ตประเภทนี้เป็นการจงใจเปลี่ยนข้อมูลสำคัญที่ใช้ควบคุมการสื่อสารข้อมูลให้ผิดปกติ ผิดธรรมชาติของการสื่อสารข้อมูลธรรมดา ตามปกติแต่ละโปรโตคอล เช่น IP TCP UDP ย่อมมีค่าในเฮดเดอร์ที่จะใช้เป็นกลไกการควบคุมการสื่อสารข้อมูล โดยในสภาวะปกติแล้วค่าเฮดเดอร์เหล่านี้จะมีค่าขอบเขตและคาดหมายได้ แต่อะนอมาลัสแพ็กเก็ตเหล่านี้จะเป็นแพ็กเก็ตที่ถูกดัดแปลงด้วยเทคนิคของการควบคุมระดับ Network Layer โดยตรงแบบไม่ผ่านโปรโตคอล ซึ่งเป็นช่องทางให้ผู้โจมตีนำมาใช้โจมตีเป้าหมายให้ทำงานผิดพลาด เพราะต้องจัดการกับแพ็กเก็ตที่ไม่ได้ระบุอยู่ในโปรโตคอลหรืออาจจะใช้เพื่อปกปิดตนเองในการสำรวจเครื่องเป้าหมายที่ต้องการโจมตี เป็นต้น

เนื่องจากอะนอมาลัสแพ็กเก็ตเหล่านี้เปรียบเสมือนการกำหนดให้ระบบปฏิบัติการให้ทำงานนอกเหนือจากเงื่อนไขที่ได้กำหนดไว้ตามปกติ ดังนั้นผลที่ได้จึงแตกต่างกันโดยขึ้นอยู่กับระบบปฏิบัติการแต่ละชนิด หากระบบปฏิบัติการสามารถจัดการกับแพ็กเก็ตประเภทนี้ได้ก็อาจจะไม่มีผลกระทบใด ๆมากนัก แต่หากระบบปฏิบัติการไม่สามารถจัดการกับกรณีของแพ็กเก็ตประหลาดเช่นนี้ได้อย่างเหมาะสม ก็จะส่งผลกระทบอย่างรุนแรงได้ ดังนั้นผู้บุกรุกก็จะใช้คุณสมบัติเหล่านี้ของอะนอมาลัสแพ็กเก็ตเพื่อทำการโจมตีเครื่องเป้าหมายให้หยุดการบริการได้

Ping Flood

Ping Flood เป็นการโจมตีที่ใช้กันในยุคแรกๆ ของ DoS เป็นการโจมตีที่ไม่ได้อาศัยเทคนิคที่ซับซ้อนแต่อย่างใด อาศัยปริมาณแพ็กเก็ตมากๆ เพียงอย่างเดียว แต่ก็สามารถสร้างความเสียหายได้ โดยหลักการโจมตีของ Ping Flood คือการส่งแพ็กเก็ต ICMP Echo Request ซึ่งเป็นแพ็กเก็ตแบบเดียวกับที่ได้จากคำสั่ง Ping ไปยังเครื่องที่ต้องการโจมตีเป็นปริมาณมากๆ อย่างรวดเร็ว ทำให้เครื่องนั้นจะต้องคอยตอบ ICMP Echo Reply ตลอดเวลาจนแทบไม่มีเวลาจะทำงานอื่น ความรุนแรงของการโจมตีจะมากหรือน้อยแปรผันตามความเร็วในการส่ง ICMP เป็นหลัก หากผู้โจมตีมีแบนวิดธ์ขนาดใหญ่ และมีเครื่องที่มีสมรรถนะสูงซึ่งสามารถสร้างแพ็กเก็ต ICMP ได้ในปริมาณมากในเวลาอันสั้น เครื่องเป้าหมายก็จะหยุดทำงานได้

นอกจากการสร้างความเสียหายแก่เครื่องคอมพิวเตอร์เป้าหมายแล้ว Ping Flood ยังสร้างความเสียหายให้แก่เครือข่ายที่เครื่องคอมพิวเตอร์เป้าหมายตั้งอยู่ด้วย โดยความเสียหายจะมากหรือน้อยขึ้นอยู่กับการลักษณะการออกแบบของเครือข่ายนั้นๆ โดยเฉพาะเครือข่ายแบบ Ethernet ซึ่งแต่ละเครื่องมีการใช้ช่องทางในการสื่อสารร่วมกัน ดังนั้นเมื่อแพ็กเก็ตจำนวนมากถูกส่งมายังเครื่องเป้าหมาย นอกจากจะทำให้เครื่องเป้าหมายเสียหายแล้วเครือข่ายที่เป็นทางผ่านก็จะเต็มไปด้วยแพ็กเก็ตนี้เช่นกัน โดยลักษณะเช่นนี้จะเกิดขึ้นบนเครือข่ายที่มีการใช้การช่องทางการสื่อสารร่วมกัน เช่น 10Base-5 หรือ 10Base-T ที่ใช้ฮับ (Hub) เป็นตัวกระจายสัญญาณ

การโจมตีแบบนี้จะต้องกระทำควบคู่กับการปลอมหมายเลข IP ของเครื่องต้นทาง เนื่องจากการส่ง ICMP Echo Request ไปแล้วก็จะได้รับ ICMP Echo Reply กลับมาเสมอ ดังนั้นหากไม่มีการปลอม IP ต้นทาง แพ็กเก็ต ICMP Echo Reply ก็จะสะท้อนกลับมายังผู้โจมตีในจำนวนเท่ากับที่ส่งไปโจมตี ซึ่งอาจทำให้ผู้โจมตีได้รับผลกระทบด้วยเช่นกัน

SYN Flood Attack

คุณสมบัติสำคัญของการสื่อสารโดยใช้โปรโตคอล TCP คือการเชื่อมต่อที่มีเสถียรภาพ การเริ่มต้นเชื่อมต่อแบบ TCP นั้นจะเป็นการตรวจสอบซึ่งกันและกันทั้ง 2 ฝ่ายที่เรียกว่า 3-way handshake โดยเริ่มต้นจากเครื่องไคลเอ็นต์ที่ต้องการติดต่อส่งสัญญาณ SYN มายังเซิร์ฟเวอร์แล้วเซิร์ฟเวอร์จะต้องตอบกลับด้วยสัญญาณ SYN ACK กลับไปยังเครื่องไคลเอ็นต์ จากนั้นต้องรอการตอบรับสัญญาณ ACK อีกครั้งหนึ่งจากเครื่องไคลเอนต์ จึงจะจบกระบวนการ ดังนั้นเพื่อให้การเชื่อมต่อเป็นไปอย่างต่อเนื่อง โปรแกรมที่จัดการ 3-way handshake ของเซิร์ฟเวอร์จะต้องจัดสรรหน่วยความจำจำนวนหนึ่งเพื่อรองรับการเชื่อมต่อแต่ละครั้งจนกว่าการทำ 3-way handshake จะสิ้นสุดลง โดยที่เซิร์ฟเวอร์เองก็ไม่มีทางรู้ได้เลยว่าไคลเอ็นต์จะส่งสัญญาณ ACK กลับมาเพื่อจบการเชื่อมต่อนั้นของ 3-way handshake เมื่อใด โดยที่เซิร์ฟเวอร์เองก็จะมี

เวลาค่าหนึ่งที่จะรอให้ได้สัญญาณ ACK ตอบกลับมา หากถึงเวลาที่กำหนดแล้วไม่มีแพ็กเก็ตของ ACK กลับมาเซิร์ฟเวอร์จะต้องยุติการรอนั้นและคืนหน่วยความจำให้แก่ระบบปฏิบัติการ

ลักษณะสำคัญของการโจมตีแบบนี้ก็คือ ผู้โจมตีจะสร้างแพ็กเก็ต TCP ที่ตั้งค่า SYN เพื่อขอเริ่มการเชื่อมต่อพร้อมทั้งทำการปลอมหมายเลข IP ต้นทางให้เป็นของเครื่องที่ไม่มีอยู่จริงด้วย แล้วจึงส่งแพ็กเก็ตดังกล่าวในปริมาณมากไปยังเครื่องเป้าหมาย หลังจากนั้นเครื่องเป้าหมายก็จะส่งสัญญาณ SYN ACK ตอบกลับมาที่เครื่องต้นทาง แต่เนื่องจากเครื่องต้นทางนั้นไม่มีอยู่จริง จึงไม่มีการส่งสัญญาณ ACK กลับไปยังเครื่องเป้าหมาย จึงทำให้เกิดสภาวะเปิดการเชื่อมต่อแบบครึ่งเดียว (Half Open) ขึ้นที่เครื่องเป้าหมายและระบบปฏิบัติการก็จะจัดสรรหน่วยความจำสำหรับการเชื่อมต่อดังกล่าวด้วย โดยเครื่องเป้าหมายจะรอสัญญาณ ACK จนถึงเวลาที่กำหนดแล้วจึงจะยุติการเชื่อมต่อและคืนหน่วยความจำ แต่หากผู้โจมตีส่งแพ็กเก็ต TCP SYN จำนวนมากๆ อย่างต่อเนื่อง ก็จะส่งผลกระทบโดยตรงต่อการบริการของเครื่องเป้าหมาย และหากระบบปฏิบัติการของเครื่องนั้นจัดการหน่วยความจำได้ไม่มีประสิทธิภาพเพียงพอ ก็อาจจะส่งผลให้เครื่องหยุดทำงานได้

Land Attack

Land Attack เป็นวิธีการที่ผู้โจมตีจะทำการสร้างแพ็กเก็ต ที่มีหมายเลข IP ต้นทางเหมือนกับหมายเลข IP ปลายทางและหมายเลขพอร์ตต้นทางเท่ากับหมายเลขพอร์ตปลายทาง มีการกำหนด SYN Flag เพื่อขอเริ่มต้นการเชื่อมต่อ แล้วส่งแพ็กเก็ตเหล่านี้ไปยังเครื่องเป้าหมาย ปกติข้อกำหนดของ TCP เมื่อมีการส่งสัญญาณ SYN เพื่อขอการเชื่อมต่อไปยังเครื่องเป้าหมาย เครื่องนั้นก็จะต้องตอบรับกลับไปยังผู้ส่งด้วย SYN ACK ตามหมายเลขพอร์ตและหมายเลข IP ต้นทาง แต่สำหรับการโจมตีแบบนี้หมายเลข IP ต้นทางเท่ากับ IP ปลายทางและหมายเลขพอร์ตต้นทางเท่ากับหมายเลขพอร์ตปลายทาง ดังนั้นการตอบกลับด้วย SYN ACK ก็จะตอบกลับไปที่ปลายทางเดิม ซึ่งกรณีนี้ไม่มีข้อกำหนดอยู่ในโปรโตคอลว่าควรทำอย่างไร ดังนั้นเครื่องจึงพยายามตอบสนองตามข้อกำหนดเท่าที่มีอยู่โดยการตอบกลับไปที่หมายเลข IP และพอร์ตต้นทางที่ส่งมานั่นคือการตอบกลับเข้ามายังตนเอง ซึ่งจะทำให้มีการตอบกลับไปมาของ TCP วนรอบอยู่ในตัวเองด้วยความเร็วสูง ทำให้คอมพิวเตอร์ต้องใช้ทรัพยากรที่มีอยู่ทั้งหมด เพื่อคอยจัดการกับ TCP ที่ตอบกลับไปมาดังกล่าว จนไม่อาจจะไปทำงานอื่นๆ ได้อีกอาจจะถึงขั้นหยุดทำงานไปเลย

Smurf Attack

Smurf attack เป็นการปรับปรุงวิธีการโจมตีแบบ Ping Flood โดยที่ผู้โจมตีจะปลอมหมายเลข IP ต้นทางเป็นหมายเลข IP ของระบบหรือเครื่องที่ต้องการโจมตีและส่ง

ICMP Echo Request ไปยัง Broadcast Address ซึ่งหมายถึงเครื่องทุกเครื่องในเครือข่ายที่เป็นตัวกลางซึ่งจะทำให้เกิดปรากฏการณ์ที่จะเรียกว่าการขยายสัญญาณ (amplifier) ซึ่งจะทำให้เครื่องต่าง ๆ ที่อยู่ในเครือข่ายที่เป็นตัวกลางจะส่ง ICMP Echo Reply กลับไปยังหมายเลข IP ของเครื่องเป้าหมายทันที ซึ่งทำให้เครื่องเป้าหมายได้รับ ICMP Echo Reply จำนวนมากจนไม่สามารถสื่อสารกับผู้อื่นได้หรือเครื่องหยุดทำงานไปเลย นอกจากนี้อาจจะเกิดผลเสียหายแก่เครือข่ายได้ หากผู้โจมตีส่งแพ็กเก็ตที่ใช้ในการโจมตีอย่างต่อเนื่องและอัตราสูงก็จะทำให้เครือข่ายเต็มไปด้วยแพ็กเก็ตของ ICMP Echo Reply ซึ่งทำให้แพ็กเก็ตอื่น ๆสำหรับใช้งานปกติไม่สามารถรับส่งข้อมูลกันได้

Ping of Death Attack

การโจมตีวิธีนี้อาศัยข้อบกพร่องของการแบ่งข้อมูลออกเป็นส่วนย่อย ๆ หรือที่เรียกกันว่าการทำแฟร็กเมนต์ (fragment) ซึ่งปกติดาต้าแกรมของ IP จะมีขนาดสูงสุดได้ไม่เกิน 65535 ไบต์ [RFC-791] เมื่อเครื่องต้นทางส่งดาต้าแกรมที่ถูกแฟร็กเมนต์ไปถึงเครื่องปลายทางแล้ว เครื่องปลายทางก็จะมีกลไกในการรวม (assemble) เอาส่วนของดาต้าแกรมที่ถูกแฟร็กเมนต์เหล่านั้นเข้าเป็นดาต้าแกรมที่สมบูรณ์อันเดียว ดังนั้นโอกาสที่จะทำให้ขนาดของดาต้าแกรมที่สมบูรณ์นั้นสูงกว่า 65535 ไบต์ก็เป็นไปได้

ด้วยข้อบกพร่องดังกล่าวจึงเป็นที่มาของการโจมตีแบบ Ping of Death โดยการส่งดาต้าแกรมของ ICMP Echo Request ที่ถูกแฟร็กเมนต์ไปยังเป้าหมายเสมือนการใช้คำสั่ง Ping ปกติ แต่จงใจทำให้ผลรวมของดาต้าแกรมที่ถูกแฟร็กเมนต์นั้นเกินขนาด 65535 ไบต์ ซึ่งขนาด 65535 ไบต์เป็นขนาดที่ระบบปฏิบัติการจัดสรรหน่วยความจำไว้รองรับอยู่แล้ว แต่หากระบบปฏิบัติการไม่ได้ตรวจสอบให้ดีก่อนการรวมดาต้าแกรมเข้าเป็นอันเดียวกันแล้วนำไปใส่หน่วยความจำปกติเลย ก็จะส่งผลทำให้ข้อมูลล้นออกมานอกหน่วยความจำที่จัดสรรไว้ อาการในลักษณะนี้เรียกว่า Buffer Overflow แล้วหลังจากนั้นส่วนที่เกินออกมาก็จะไปตกที่ตำแหน่งของโปรแกรมอื่นที่ใช้งานอยู่ ก็จะทำให้โปรแกรมนั้นทำงานผิดพลาดไปจากปกติ

Tribe Flood Network(TFN)

TFN เป็นวิธีการโจมตีที่ใช้ ICMP เป็นคำสั่งสำหรับสั่งงานเครื่องหลาย ๆ เครื่องให้ทำการโจมตีเครื่องเป้าหมายพร้อม ๆ กัน โดยลักษณะการโจมตีแบบนี้จะเรียกว่า การโจมตีแบบ DDoS (Distributed Denial of Service) ซึ่งเป็นการผสมผสานการโจมตีแบบ DoS กับการทำงานของโปรแกรมประเภทม้าโทรจัน โดยผู้โจมตีจะพยายามติดตั้งโปรแกรมม้าโทรจันในเครื่องต่าง ๆ ที่อยู่ในเครือข่ายอินเทอร์เน็ตให้มากที่สุด โดยหน้าที่ของโปรแกรมม้าโทรจันเหล่านี้ก็คือ จะทำการโจมตีแบบ DoS ไปยังเครื่องเป้าหมายตามการสั่งการจากโปรแกรมที่หน้าที่เป็น

ศูนย์ควบคุม เมื่อถึงเวลาที่จะโจมตี ผู้โจมตีก็เพียงแต่ส่งสัญญาณจากศูนย์ควบคุมไปยังเครื่องที่มีโปรแกรมม้าโทรจันเหล่านั้นอยู่ จากนั้นทุกเครื่องก็จะทำการส่งแพ็กเก็ตจำนวนมากไปยังเครื่องเป้าหมายหรือเครือข่ายที่ต้องการพร้อมๆ กัน จนช่องทางการสื่อสารเต็มไปด้วยแพ็กเก็ตเหล่านี้และเครื่องเป้าหมายก็จะไม่สามารถให้บริการได้ในที่สุด

สำหรับการโจมตีด้วยวิธีการ TFN ผู้โจมตีจะต้องพยายามนำโปรแกรมเล็กๆ ซึ่งจะเป็นตัวที่ใช้ในการรับสัญญาณและส่งแพ็กเก็ตโจมตี หรือที่เรียกว่า TFN Daemon ไปติดตั้งไว้ในเครื่องต่างๆ ให้มากที่สุด เมื่อเครื่องเหล่านั้นเปิดขึ้นมาใช้งานและ TFN Daemon ได้ทำงานเรียบร้อยแล้ว ในเครื่องของผู้โจมตีจะมีโปรแกรมที่สามารถสื่อสารและสั่งการไปยัง TFN Daemon ซึ่งจะโปรแกรมนี้ว่า TFN Master และเมื่อถึงเวลาที่ต้องการ TFN Master ก็จะส่งสัญญาณให้ TFN Daemon ทั้งหมดทำการโจมตีพร้อมๆ กัน และเพื่อเป็นการหลบหลีกการตรวจจับหรือการป้องกันของไฟร์วอลล์ (Firewall) TFN จะใช้ ICMP Echo Reply เป็นช่องทางในการสื่อสาร ซึ่งโดยทั่วไปแล้ว ICMP มักจะไม่ค่อยเป็นที่สังเกตของผู้ดูแลระบบ หรือโปรแกรมที่ทำหน้าที่เป็นไฟร์วอลล์ จึงทำให้คำสั่งของ TFN ที่แฝงมากับ ICMP Echo Reply นั้นสามารถผ่านเข้าไปถึง TFN Daemon

นอกจาก TFN แล้วยังได้มีเครื่องมืออื่นๆ ที่ใช้สำหรับการโจมตีในลักษณะ DDoS อีกด้วย เช่น trinoo, TFN2K, stacheldraht และ shaft เป็นต้น

2.3.9 Brute-force Attack

เป็นวิธีหนึ่งในการพยายามถอดรหัสข้อความที่มีการเข้ารหัสไว้ ซึ่งส่วนใหญ่ก็คือรหัสผ่านของผู้ใช้ วิธีการนี้จะเป็นการถอดรหัสข้อความที่ถูกเข้ารหัสไว้ โดยการพยายามใช้ทุกๆ key (ค่าที่ต้องใส่ไปในอัลกอริทึมเพื่อถอดรหัสข้อความที่เข้ารหัสไว้เพื่อสร้างข้อความเดิมก่อนเข้ารหัส) ที่เป็นไปได้ ยิ่งใช้วิธี brute force attack ในการถอดรหัสได้สำเร็จเร็วเท่าไหร่ ก็แสดงให้เห็นถึงความบกพร่องของรหัสลับนั้น ความสำเร็จของการโจมตีด้วยวิธีนี้ขึ้นอยู่กับความยาวของคีย์ที่ใช้ในการเข้ารหัสข้อความ และพลังในการประมวลผลของผู้โจมตี การโจมตีแบบนี้จะใช้ไม่ได้ผลกับรหัสลับที่มีขนาดของคีย์ที่ไม่แน่นอน เช่น รหัสผ่านแบบใช้ครั้งเดียว (one-time pad cipher)

2.4 Passive Attack

การโจมตีแบบ passive attack เป็นการโจมตีที่ไม่ได้ทำให้เกิดการเปลี่ยนแปลงของข้อมูลต่างๆ แต่ผู้โจมตีสามารถเข้าถึงข้อมูลได้โดยไม่ได้รับอนุญาต เช่น การแอบดักจับข้อมูลในสายสัญญาณของเครือข่ายสื่อสาร เป็นต้น ดังนั้นการโจมตีในแบบนี้สามารถตรวจจับได้ยาก แต่

การป้องกันได้ง่าย เช่น การเข้ารหัสข้อมูลที่รับและส่งในเครือข่าย เป็นต้น ซึ่งรายละเอียดวิธีการโจมตีต่าง ๆ ที่จัดอยู่ในรูปแบบ passive attack มีดังนี้

2.4.1 Eavesdropping

สายส่งหรือคลื่นสัญญาณของเครือข่ายเป็นทรัพยากรที่ถูกใช้ร่วมกันระหว่างผู้ใช้ต่าง ๆ ในเครือข่าย ดังนั้นจึงมีความเสี่ยงที่จะถูกลอบฟัง นั่นหมายความว่าผู้ใช้อื่น ๆ ของสายส่งและคลื่นสัญญาณเหล่านี้อาจจะสามารถที่จะเข้าถึง มองเห็นหรือถอดรหัสข้อมูลที่ไปในคลื่นสัญญาณที่ส่งไปได้ โดยความเสี่ยงของการถูกลอบฟังเหล่านี้ไม่ได้มีเพียงในเครือข่ายคลื่นสัญญาณเท่านั้น แต่ในอินเทอร์เน็ตและบริการอื่น ๆ ที่มีการทำงานในลักษณะของการบริการคลื่นสัญญาณก็มีความเสี่ยงเช่นกัน ดังนั้นผู้ใช้จึงไม่ควรส่งข้อมูลที่เป็นความลับ เช่น หมายเลขบัตรเครดิต หรือข้อมูลทางการเงิน ข้อมูลทางการแพทย์ หรือ ความลับทางการค้า ไปบนเครือข่ายคลื่นสัญญาณโดยไม่ได้ทำการเข้ารหัส

2.4.2 สนิฟเฟอร์ (Sniffer)

คำว่า Sniffer (ตัวอักษร S เป็นตัวพิมพ์ใหญ่) เป็นเครื่องหมายทางการค้าซึ่งจดทะเบียนโดยบริษัท Network Associates Inc. ในสหรัฐอเมริกา เพื่อใช้ในผลิตภัณฑ์ของบริษัทที่ชื่อว่า Sniffer Network Analyzer ซึ่งเป็นโปรแกรมวิเคราะห์เครือข่าย โดยอาศัยการดักอ่านข้อมูลทั้งหมดบนเครือข่ายมาทำการวิเคราะห์แยกแยะการใช้งานเครือข่ายออกไปตามโปรโตคอลที่ใช้งานกันอยู่ เพื่อช่วยในการวางแผน ตรวจสอบและแก้ไขข้อบกพร่องที่อาจเกิดขึ้นในเครือข่าย แต่หากเขียนเป็น sniffer (ตัวอักษร s เป็นตัวพิมพ์เล็ก) จะหมายถึงโปรแกรมที่เป็นเครื่องมือที่ดักจับข้อมูลบนเครือข่าย สำหรับการตรวจสอบและวิเคราะห์ข้อมูลการจราจรในเครือข่าย

สนิฟเฟอร์สามารถดักจับข้อมูลที่อยู่ในเครือข่ายได้ก็เพราะว่าอาศัยหลักการของการทำงานของเครือข่ายแบบอีเทอร์เน็ต (Ethernet Based Network) ที่มีการกระจายข้อมูลไปยังทุกเครื่องในเครือข่ายและอาศัยเครื่องแต่ละตัวทำหน้าที่จำแนกการสื่อสารของตัวเอง ซึ่งก็หมายความว่าข้อมูลทุกแพ็กเก็ตที่ใช้สื่อสารนั้นได้ถูกส่งไปยังเครื่องทุกเครื่องให้ได้รับพร้อมกันและเหมือนกัน เพียงแต่จะอาศัยกระบวนการที่เครื่องแต่ละตัวใช้ในการระบุว่าข้อมูลแพ็กเก็ตไหนเป็นของตัวเองก็รับไป และถ้าข้อมูลแพ็กเก็ตไหนไม่ใช่ของตัวเองก็ไม่ต้องสนใจ ปกติแล้วในทุก ๆ แพ็กเก็ตที่กระจายไปบนเครือข่ายนั้นจะมีหมายเลขระบุชัดเจนคือ แมคแอดเดรส (Mac Address) ซึ่งจะเป็นสิ่งที่บอกว่าแพ็กเก็ตมาจากฮาร์ดแวร์เครื่องใดในเครือข่าย ทำให้สามารถระบุได้ว่าแพ็กเก็ตนั้นถูกส่งมาจากเครื่องไหนและต้องการส่งไปให้เครื่องไหน

จากลักษณะการทำงานดังกล่าว โดยปกติเน็ตเวิร์กอะแดปเตอร์แบบอีเทอร์เน็ตจะรับเอาแพ็กเก็ตบนเครือข่ายเข้ามาก็ต่อเมื่อในแพ็กเก็ตนั้นมีแมคแอดเดรสปลายทางเป็นของตนเองหรือเป็นแอดเดรสพิเศษที่เรียกว่า บรอดคาสแอดเดรส (Broadcast Address) เท่านั้น และจะไม่สนใจแพ็กเก็ตอื่น ๆ ที่ไม่ได้อยู่ในเงื่อนไขนี้เลย ดังนั้นโปรแกรมสนิฟเฟอร์จะต้องมีการกำหนดให้เน็ตเวิร์กอะแดปเตอร์อยู่ในโหมดการทำงานพิเศษที่เรียกว่า โพรมิสคูอัสโหมด (Promiscuous Mode) ซึ่งจะทำให้สนิฟเฟอร์สามารถดักจับและวิเคราะห์แพ็กเก็ตได้ทุกแพ็กเก็ตที่วิ่งไปมาในเครือข่ายที่มันถูกติดตั้งไว้ได้ แต่ก็มีข้อจำกัดอยู่เหมือนกัน นั่นคือสนิฟเฟอร์จะไม่สามารถทำงานข้ามเครือข่ายได้ ถ้ามีอุปกรณ์สื่อสารอย่างเช่น บริดจ์ (Bridge) สวิตซ์ (Switch) หรือเราท์เตอร์ (Router) คั่นระหว่างเครือข่ายอยู่ มันก็จะดักจับแพ็กเก็ตได้เฉพาะภายในเครือข่ายนั้น

การถูกดักอ่านข้อมูลโดยสนิฟเฟอร์นั้นตรวจสอบได้ยาก เนื่องจากการมีสนิฟเฟอร์ติดตั้งอยู่ในเครือข่ายนั้นไม่ได้ส่งผลกระทบใด ๆ กับเครือข่าย จึงมีโอกาสน้อยมากที่ทราบว่ามีการนำสนิฟเฟอร์มาติดตั้งในเครือข่ายจากการตรวจสอบภายนอก เว้นเสียแต่ว่าจะเข้าไปตรวจสอบโหมดการทำงานของเน็ตเวิร์กอะแดปเตอร์ในทุก ๆ เครื่องที่อยู่ในเครือข่าย ซึ่งโดยปกติแล้วเน็ตเวิร์กอะแดปเตอร์จะไม่ทำงานอยู่ในโพรมิสคูอัสโหมด ดังนั้นหากพบว่าเครื่องใดทำงานอยู่ในโหมดนี้ก็อาจจะเป็นไปได้ว่าเครื่องนั้นได้ทำงานเป็นสนิฟเฟอร์คอยดักอ่านข้อมูลผู้อื่นอยู่

โดยทั่วไปข้อมูลที่รับส่งในเครือข่ายจะไม่มีการเข้ารหัสข้อมูล เป็นข้อมูลที่สามารถอ่านได้ (clear-text) รวมถึงข้อมูลเกี่ยวกับบัญชีผู้ใช้และรหัสผ่านด้วยเช่นกัน ดังนั้นวิธีการป้องกันการดักอ่านข้อมูลด้วยสนิฟเฟอร์ก็คือ การหลีกเลี่ยงการใช้งานโปรแกรมประยุกต์ที่รับส่งข้อมูลโดยไม่ได้เข้ารหัสข้อมูล เช่น Telnet, FTP และเปลี่ยนมาใช้โปรแกรมประยุกต์ที่มีการเข้ารหัสข้อมูลในการรับส่งมาใช้แทน เช่น โปรแกรม Secure Shell แทนโปรแกรม Telnet เป็นต้น นอกจากนี้ผู้ดูแลระบบก็ควรจะปรับเปลี่ยนโครงสร้างการเชื่อมต่อเครือข่ายให้เป็นแบบที่ใช้สวิตซ์ (Switched Ethernet) ซึ่งข้อมูลจะไม่กระจายแต่จะวิ่งจากต้นทางไปยังปลายทางที่ระบุเลย ทำให้ช่วยลดความเสี่ยงของการถูกดักจับข้อมูลได้มาก แทนที่จะใช้การเชื่อมต่อเครือข่ายแบบฮับ (Hub Ethernet) ซึ่งข้อมูลจะกระจายไปทั่วเครือข่ายเมื่อมีการรับส่งข้อมูล จึงเสี่ยงที่จะถูกสนิฟเฟอร์ดักจับข้อมูลไป

2.4.3 Wiretap

Wiretapping เป็นการลักลอบดักฟังสัญญาณการสื่อสารโดยเจตนาที่จะได้รับประโยชน์จากการเข้าถึงข้อมูลที่รับส่งผ่านเครือข่ายที่ใช้ในการสื่อสาร โดยเฉพาะช่องสัญญาณสำหรับการสื่อสารแบบไร้สายสมควรจะได้รับการพิจารณาเป็นพิเศษ การเกิดขึ้นไม่นานและความนิยมที่เพิ่มขึ้นของเครือข่ายไร้สาย (Wireless LAN) ซึ่งใช้มาตราฐาน IEEE802.11 ในการสื่อสารเนื่องจากข้อมูลเผยแพร่บนความถี่วิทยุที่รู้กันโดยทั่วไป จึงทำให้ผู้โจมตีสามารถรับข้อมูลที่

ส่งเหล่านี้ได้ง่าย ถึงแม้ว่าหลาย ๆช่องสัญญาณนั้นจะมีการป้องกันโดยการเข้ารหัสข้อมูล แต่หากมีการเข้ารหัสนั้นมีประสิทธิภาพต่ำ ก็จะทำให้ผู้โจมตีสามารถถอดรหัสได้เช่นกัน

2.4.4 Social Engineering

เป็นเทคนิคในการเข้าถึงข้อมูลในระบบโดยการหลอกลวงหรือหลอกล่อให้หลงเชื่อ โดยมักเกิดขึ้นผ่านทางการสนทนาระหว่างมนุษย์ด้วยกันหรือการติดต่อกันวิธีอื่น พาหะที่มักถูกใช้ติดต่อกันมักจะเป็น การโทรศัพท์พูดคุยกัน แต่อาจจะเป็นอย่างอื่น เช่น การรับส่งผ่านจดหมายอิเล็กทรอนิกส์ การโฆษณาผ่านสื่อวิทยุ โทรศัพท์หรือพาหะอื่น ๆ อีกมากที่ทำให้มนุษย์พบปะติดต่อกันได้ เช่น การปลอมแปลงจดหมายอิเล็กทรอนิกส์โดยระบุว่าส่งมาจากผู้ดูแลระบบไปยังผู้ใช้ที่ต้องการ แล้วระบุให้ส่งรหัสผ่าน ตอบกลับมายังผู้ส่ง ซึ่งหากผู้ใช้คนใดหลงเชื่อจดหมายดังกล่าวและส่งรหัสผ่านตอบกลับไป ก็จะทำให้ผู้โจมตีได้รหัสผ่านของผู้ใช้คนนั้นไปในที่สุด

2.4.5 Port Scanning

Port Scanning เป็นหนึ่งในเทคนิคที่รู้จักกันแพร่หลายที่ผู้โจมตีใช้ในการค้นหาบริการที่จะสามารถบุกรุกหรือข้ามผ่านเข้าไปยังระบบได้ โดยปกติแล้วทุก ๆ ระบบที่ต่อเข้าสู่ระบบเครือข่ายหรือระบบอินเทอร์เน็ตจะเปิดบริการต่าง ๆ ซึ่งทำงานอยู่บนพอร์ตที่เป็นที่รู้จักและที่ไม่เป็นที่รู้จัก สำหรับการทำ Port Scanning นั้น ผู้โจมตีจะสามารถค้นหาข้อมูลได้มากมายจากระบบเป้าหมาย ได้แก่ บริการอะไรบ้างที่กำลังทำงานอยู่ ผู้ใช้คนไหนเป็นเจ้าของบริการเหล่านั้น สนับสนุนการใช้งานผ่านบัญชีผู้ใช้ anonymous หรือไม่ เป็นต้น

การทำ Port Scanning ทำได้โดยการส่งข้อความหนึ่งไปยังแต่ละพอร์ตที่ต้องการ ซึ่งผลลัพธ์ที่ตอบสนองออกมาจะแสดงให้เห็นว่าพอร์ตนั้น ๆ ถูกใช้อยู่หรือไม่และสามารถทดสอบดูเพื่อหาจุดอ่อนต่อไปได้ แต่อย่างไรก็ตาม Port Scanning ก็มีประโยชน์กับผู้ดูแลระบบด้วยเช่นกันเพราะว่าทำให้สามารถตรวจสอบและค้นหาจุดอ่อนด้านความปลอดภัยของระบบที่ดูแลอยู่ได้

2.5 สรุป

การโจมตีระบบคอมพิวเตอร์และเครือข่ายนั้นสามารถแบ่งออกได้ 2 ประเภท คือ active attack และ passive attack ซึ่งการโจมตีลักษณะ active attack สามารถตรวจสอบจับได้ง่ายกว่า passive attack เนื่องจากมีการแก้ไขหรือเปลี่ยนแปลงข้อมูลในระบบ จึงทำให้เกิดร่องรอยการกระทำต่าง ๆ เกิดขึ้นในล็อกไฟล์ที่ใช้บันทึกการทำงานของระบบ และข้อมูลเหล่านี้จะถูกนำไปใช้ในการตรวจจับในระบบตรวจจับการบุกรุกที่จะกล่าวถึงในบทที่ 3