# พื้นฐานความปลอดภัยเครือข่าย



## เนื้อหา

1. วิธีการสำรองข้อมูล
2. การแม็บไดว์ฟ
3. การตรวจจับความปลอดภัยเครือข่าย
4. การพัฒนานโยบายความปลอดภัยเครือข่าย
5. การคุกคามความปลอดภัยเครือข่าย
6. การสนับสนุนการวัดระดับความปลอดภัย
7. การประยุกต์แก้ไขและอัพเกรดแพช
8. ไฟร์วอลล์

## วัตถุประสงค์

- อธิบายรูปแบบวิธีการสำรองข้อมูลและหลักเกณฑ์การกำหนดนโยบายการสำรองข้อมูลได้
- อธิบายวิธีการแม็บไดว์ฟได้
- อธิบายวิธีการต่างๆ ในการตรวจจับความปลอดภัยเครือข่ายได้
- อธิบายนโยบายความปลอดภัยเครือข่ายด้านต่างๆ ได้
- อธิบายการคุกคามความปลอดภัยเครือข่ายประเภทต่างๆ ได้
- อธิบายการวัดระดับความปลอดภัยของข้อมูลในระดับต่างๆ ได้
- อธิบายการประยุกต์แก้ไขและอัพเกรดแพชได้
- อธิบายไฟร์วอลล์แต่ละประเภทได้



## Network Security Basic

- ปัจจัยที่ทำให้ต้องมีการรักษาความปลอดภัยด้านเครือข่าย
  - จำนวนผู้ใช้งานในเครือข่าย
  - การเชื่อมต่อเครือข่ายกับระบบอินเทอร์เน็ต
  - ความสำคัญของข้อมูล
- มาตรการด้านการป้องกันความปลอดภัย
  - การวางแผนการรองรับความเสียหายจากปัญหาด้านฮาร์ดแวร์ (Hardware)
  - การวางแผนรองรับปัญหาการสูญหายของข้อมูล
    - การสำรองข้อมูล (Backup)
    - ระบบสำรองไฟฟ้า
    - ระบบทนทานต่อความผิดพลาด (Fault Tolerance) เป็นต้น

# 5.1 วิธีการสำรองข้อมูล (Backup Method)

- วิธีการพื้นฐานที่ง่ายที่สุดที่จะป้องกันปัญหาข้อมูลสูญหาย เมื่อข้อมูลอาจถูกทำลายไปโดยกระบวนการต่างๆ เช่น
  - ความผิดพลาดในการทำงานของเครื่องจักรกล (Mechanical Failure)
  - การโจมตีจากไวรัส (Virus Attack)
  - ความผิดพลาดของผู้ใช้เอง (User Error)
- การสำรองข้อมูลสามารถทำได้ใน 2 ลักษณะ
  - การใช้ฮาร์ดดิสก์ (Hard Disk)
  - การทำการสำรองข้อมูลด้วยเทป (Tape Backup)



# 5.1 วิธีการสำรองข้อมูล (Backup Method)

- ข้อมูลที่มีความสำคัญมากควรที่จะได้รับการสำรองไว้ตามกำหนดการเป็นรายวัน รายสัปดาห์ หรือรายเดือน ทั้งนี้ขึ้นอยู่กับความสำคัญและคุณค่าของข้อมูลที่องค์กรต้องการจัดเก็บ
- องค์กรควรจะดำเนินการสำรองข้อมูลจำนวน 2 ชุด โดยจัดเก็บเทปข้อมูลสำรองชุดหนึ่งไว้ภายในองค์กร และอีกชุดหนึ่งไว้ที่สถานที่อื่นๆ ภายนอก
- ตารางเปรียบเทียบการใช้ Hard disk และ Tape Backup ในการสำรองข้อมูล

| รายการเปรียบเทียบ | Hard Disk | Tape Backup |
|---|---|---|
| ราคาอุปกรณ์ | แพง | ถูก |
| มีการใช้อุปกรณ์เสริม | ไม่มี | มี |
| ความง่ายในการจัดการ | ง่าย | ง่าย |
| ความจุ | สูงมาก | สูง |
| ความเร็วในการทำงาน | เร็ว | ปานกลาง |

## 1. แบบ Full Backup

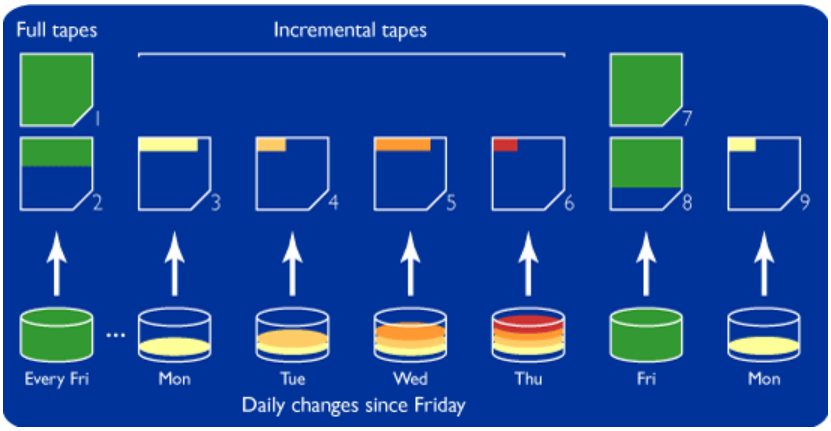
- การสำรองข้อมูลทั้งหมดบนฮาร์ดดิสก์ โดยทำสัญลักษณ์ไฟล์ที่ถูกเลือกไว้ แม้ว่าไฟล์ข้อมูลนั้น มีหรือไม่มีการเปลี่ยนแปลงหลังจากการสำรองข้อมูลครั้งล่าสุด
- การกู้คืนข้อมูล จะใช้เพียงขั้นตอนเดียวเหมือนกับขั้นตอนในการสำรองข้อมูล
- ข้อเสียของการสำรองข้อมูลแบบนี้ คือ
  - ขนาดของไฟล์สำรอง (Backup File) จะมีขนาดใหญ่
  - ใช้เวลาในการสำรองข้อมูลมาก
- การสำรองข้อมูลแบบนี้ถือเป็นรูปแบบการสำรองข้อมูลที่ง่ายที่สุด



## 2. แบบ Incremental Backup

- การสำรองข้อมูลและทำสัญลักษณ์ไฟล์ที่ถูกเลือกไว้ โดยการสำเนาข้อมูลเฉพาะไฟล์ที่ถูกแก้ไขนับตั้งแต่การทำสำเนาข้อมูลแบบ Full Backup ครั้งสุดท้ายหรือการสำรองข้อมูลแบบ Incremental Backup ครั้งล่าสุด
- เพราะฉะนั้นเมื่อทำการสำรองข้อมูลแบบ Incremental backup ติดกัน 2 ครั้ง ไฟล์ข้อมูลที่ถูกสำรองไว้ในครั้งแรกและไม่ได้ถูกแก้ไขเพิ่มเติมอีกก็จะไม่ถูกสำรองข้อมูลซ้ำ
- วิธีการกู้คืนข้อมูล
  - ในขั้นแรกจะต้องทำการกู้คืนข้อมูล Full Backup ครั้งล่าสุดก่อน
  - ตามด้วยการกู้คืนข้อมูลจาก Incremental Backup ตามเวลาที่ต้องการกู้คืนข้อมูล

# 2. แบบ Incremental Backup

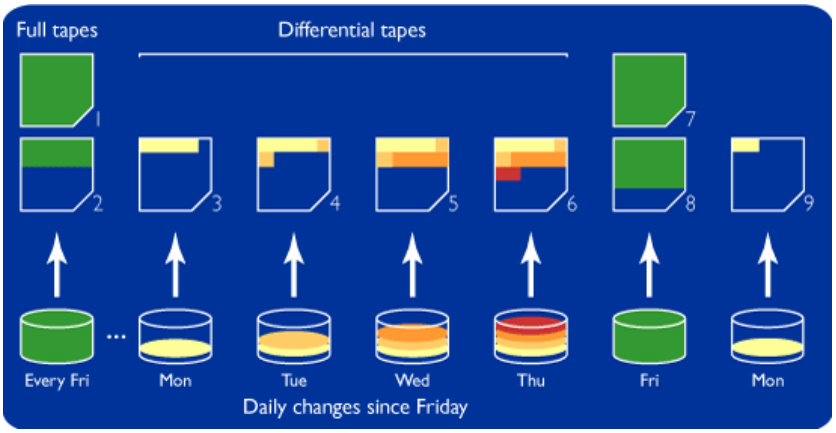





# 3. แบบ Differential Backup

- การสำรองข้อมูลโดยการสำเนาข้อมูลเฉพาะไฟล์ที่ถูกสร้างใหม่หรือแก้ไขเปลี่ยนแปลง นับตั้งแต่การทำสำเนาข้อมูลแบบ Full backup หรือ Incremental ครั้งล่าสุด โดยไม่มีการทำสัญลักษณ์ไว้ว่าได้รับการทำสำรองข้อมูลแล้ว
- เพราะฉะนั้นหากมีการสำรองข้อมูลแบบ Differential backup ติดต่อกัน 2 ครั้ง ข้อมูลที่ถูกสำรองไว้ในครั้งแรกก็จะถูกสำรองซ้ำอีกในครั้งที่สองด้วย
- วิธีการกู้คืนข้อมูลในแบบ Differential backup
  - ขั้นแรกจะต้องทำการกู้คืนข้อมูลแบบ Full backup จากเทปข้อมูลชุดล่าสุดก่อน
  - ตามด้วยการกู้คืนข้อมูลจาก Differential Backup ซึ่งข้อมูลที่ถูกแก้ไขนับตั้งแต่การทำ Full backup ครั้งล่าสุด จะอยู่ในเทปข้อมูลสำรองในรูปแบบของ Differential backup ม้วนล่าสุดทั้งหมด

# 3. แบบ Differential Backup






# นโยบายการสำรองข้อมูล

- เพื่อลดความเสี่ยงในปัญหาต่างๆ ที่อาจจะเกิดผลเสียหายต่อระบบเครือข่ายเมื่อมีภัยคุกคามเกิดขึ้นภายในระบบ
- หลักเกณฑ์ต่างๆ ที่จะใช้ในการพิจารณาเกี่ยวกับการสำรองข้อมูลที่สำคัญขององค์กร
  - การประหยัดค่าใช้จ่าย
  - การดูแลข้อมูล เช่น ตารางเวลาสำรองข้อมูล เป็นต้น
  - การเพิ่มความปลอดภัย เช่น ป้องกันผู้ใช้งานลบข้อมูลทิ้งโดยไม่ได้ตั้งใจ หรือถูกโปรแกรมไวรัสโจมตี
  - การใช้งานง่าย ผู้ใช้ไม่ต้องทำการตัดสินใจอะไรเพิ่มเติมอีกเมื่อต้องการจะสำรองข้อมูล
- สิ่งที่สำคัญสำหรับระบบสำรองข้อมูล
  - ผู้ดูแลระบบสำรองข้อมูล
  - ข้อมูลอะไรที่ต้องสำรอง
  - ตารางเวลาการสำรองข้อมูล
  - การตรวจสอบการสำรองข้อมูล
  - อุปกรณ์ที่สนับสนุนการสำรองข้อมูล

## 5.2 การแม็บไดร์ฟ (Drive Mapping)

- เป็นเทคนิคในการเข้าถึงข้อมูลเฉพาะในบริเวณพื้นที่ที่มีการอนุญาตให้ผู้ใช้เข้าถึงได้ เช่น การอ่านไฟล์ การเคลื่อนย้ายไฟล์ เป็นต้น
- เพื่อป้องกันผู้ใช้บุกรุกข้อมูลส่วนอื่นๆ นอกเหนือจากที่ผู้ให้บริการต้องการให้เข้าถึงข้อมูล
- ลักษณะของการแม็บไดร์ฟ คือ การกำหนดชื่อตัวอักษรใหม่ (A ถึง Z) ให้กับไดร์ฟ หรือโฟลด์เดอร์ ที่ต้องการแชร์ข้อมูล

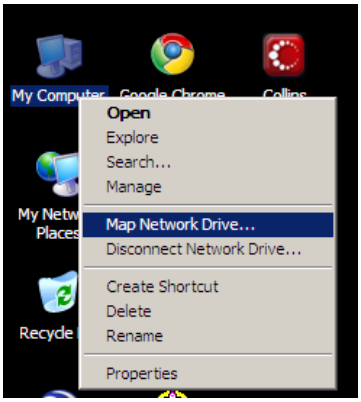


## 5.2 การแม็บไดร์ฟ (Drive Mapping)

- Universal Naming Convention (UNC) เป็นมาตรฐานสำหรับการระบุแหล่งข้อมูล server, เครื่องพิมพ์ และอื่นๆ
- ในระบบเครือข่ายระบบ UNIX ลักษณะของการระบุ path ของ UNC
  - ใช้เครื่องหมาย double slashes (//) หรือ double backslashes (\\) นำหน้าชื่อเครื่องคอมพิวเตอร์
- และระบุ path ของโฟลด์เดอร์ หรือไดร์ฟ ภายในคอมพิวเตอร์จะถูกแยกด้วย
  - เครื่องหมาย single slash (/) หรือ single backslash (\) ดังตัวอย่างต่อไปนี้
    - สำหรับระบบ UNIX //servername/path
    - สำหรับระบบ DOS/Windows \\servername\path

# วิธีการแม็บไดร์ฟ (Drive Mapping)

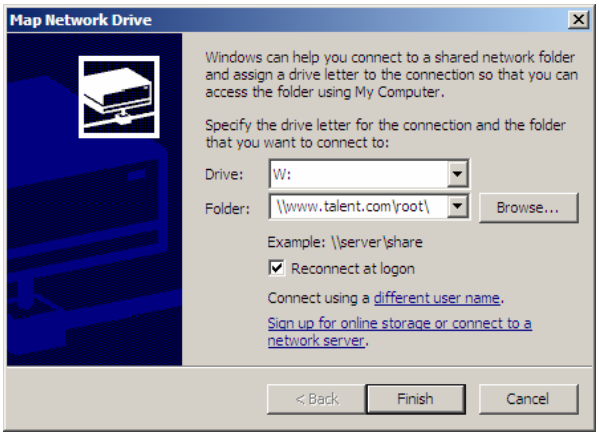
1. คลิกขวาที่ My Computer






# วิธีการแม็บไดร์ฟ (Drive Mapping)

2. ระบุชื่อ Drive และเลือก Folder



# วิธีการแม็บไดร์ฟ (Drive Mapping)

- การกำหนดเกี่ยวกับชื่อไดร์ฟ เพื่อป้องกันการชนกันของชื่อไดร์ฟ ได้มีการกำหนดการให้บริการด้าน IT เกี่ยวกับนโยบายการแม็บไดร์ฟโดยกำหนดการใช้ตัวอักษรในช่วงท้ายๆ โดยเริ่มจาก Z และย้อนขึ้นไป ดังนี้
  - Drive Z: User File store
  - Drive Y: Central Software
  - Drive X: Department File Store
  - Drive W: Reserved for mapping to the web server
  - Drive V: Reserved for SoftGrid Development
  - Drive U: Reserved for Future use
  - Drive T: Reserved for Future use



# วิธีการแม็บไดร์ฟ (Drive Mapping)

| Name | Type |
|---|---|
| **Hard Disk Drives** | |
| WINDOWS (C:) | Local Disk |
| DATA (D:) | Local Disk |
| **Devices with Removable Storage** | |
| 3½ Floppy (A:) | 3½-Inch Floppy Disk |
| DVD Drive (E:) | CD Drive |
| **Network Drives** | |
| Root (W:) | Disconnected Network Drive |
| X drive (X:) | Network Drive |
| Software (Y:) | Network Drive |
| Z drive (Z:) | Network Drive |

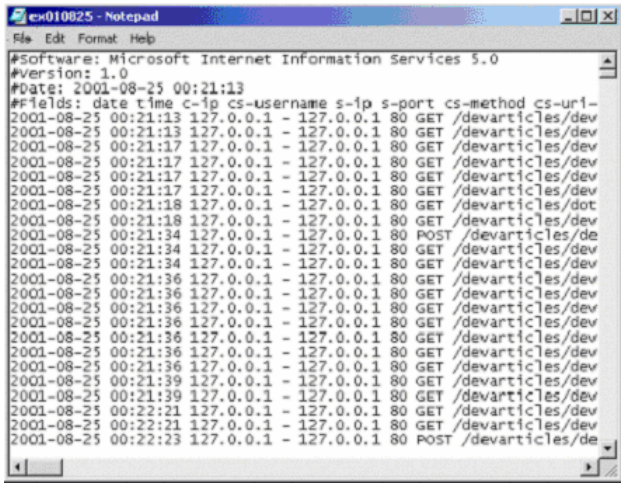
แสดงการเปิดไดร์ฟที่ถูกแม็ป

# 5.3 การตรวจจับความปลอดภัยเครือข่าย (Network Security Monitoring)

- ภัยคุกคามแบ่งเป็น
  - ภัยจากภายนอกเข้าสู่ภายในระบบเครือข่าย (Intrusion)
  - ภัยจากภายในออกสู่ภายนอกระบบเครือข่าย (Extrusion)
- การรักษาความปลอดภัยของข้อมูลจึงต้องพิจารณาและป้องกันในทุกส่วนของระบบอย่างเต็มที่
- การใช้เครื่องมือช่วยในการป้องกันภัยคุกคามระบบเครือข่ายมีมากมาย เช่น
  - ไฟร์วอลล์ (Firewall)
  - การทำระบบตรวจจับผู้บุกรุก (Intrusion Detection System) เป็นต้น
- การตรวจจับความปลอดภัยเครือข่าย เป็นการเฝ้าติดตามการจราจรของระบบเครือข่าย (Monitoring Network Traffic) ดูเส้นทางการลำเลียงข้อมูลเพื่อใช้ในการสืบหาการกระทำผิดทางอาชญากรรมคอมพิวเตอร์ (Network Forensics) ข้อมูลของ Log ที่เกิดขึ้นจากอุปกรณ์ต่างๆ



# 5.3 การตรวจจับความปลอดภัยเครือข่าย (Network Security Monitoring)




แสดงตัวอย่างข้อมูล Log file

## 5.3 การตรวจจับความปลอดภัยเครือข่าย (Network Security Monitoring)

- **การทำ Hardening** คือ การสร้างความแข็งแกร่งให้กับเครื่องเซิร์ฟเวอร์ (Server) และเครื่องไคลเอนต์ (Client) ภายในขององค์กร
  - การ Hardening จากผลการทำ Security Assessment โดยการสแกนหาช่องโหว่ที่เกิดขึ้นในเครือข่าย (Vulnerability) และทำการเปิด service และ patch ในส่วนที่อ่อนแอ
  - การ Hardening โดยทำตาม checklist สำหรับเครื่องเซิร์ฟเวอร์ที่สำคัญ
  - การ Update Patch โดยการ Patch ในส่วนของระบบปฏิบัติการ โปรแกรมประยุกต์ และข่าวสารใหม่ๆ ในวงการความปลอดภัยด้านสารสนเทศ



## 5.3 การตรวจจับความปลอดภัยเครือข่าย (Network Security Monitoring)

- **การเฝ้าตรวจระบบเครือข่ายองค์กร** คือ การเฝ้าตรวจระบบเครือข่ายเพื่อตรวจดูสิ่งผิดปกติที่เกิดขึ้นในระบบเครือข่ายขององค์กร ทั้งการโจมตีจากภายนอกเครือข่ายและการโจมตีจากภายในเครือข่าย ตลอดจนภัยคุกคามที่แฝงมากับความผิดพลาดจากการใช้งานระบบของผู้ใช้ (Human error) ซึ่งมีวิธีการต่างๆ ดังต่อไปนี้

## 5.3 การตรวจจับความปลอดภัยเครือข่าย (Network Security Monitoring)

- การติดตั้งระบบตรวจจับผู้บุกรุก (Intrusion Detection System)
  - เพื่อตรวจจับผู้บุกรุกโดยดูการเข้าออกของแพ็กเก็ต (packet) ในส่วนของข้อมูลที่เข้าออกในระบบเครือข่าย เปรียบเสมือนสนิฟเฟอร์(Sniffer) ที่ใช้ในการดักดูแพ็กเก็ตในระบบเครือข่าย แต่มีฐานข้อมูล(Database) สำหรับเก็บวิธีการโจมตี ในส่วนนี้จะเรียกว่า Network Full Content Data Monitoring ซึ่งจะเก็บวิธีการโจมตีทั้งหมด
- การตรวจจับเน็ตเวิร์คทราฟฟิก (Network Traffic)
  - เพื่อดูจำนวนการใช้งานต่างๆ บนระบบเครือข่าย ส่วนนี้จะเรียกว่า Session Data Monitoring



## 5.3 การตรวจจับความปลอดภัยเครือข่าย (Network Security Monitoring)

- การตรวจจับสิ่งผิดปกติที่วัดจากสถิติ
  - โดยการประมาณการว่าอาจจะเป็นไปได้หรือไม่ว่าระบบเครือข่ายขณะนี้มีปัญหา
  - โดยเครื่องมือที่ใช้ เช่น NetFlow จากเราท์เตอร์ (router) และอุปกรณ์อื่นๆ ที่สามารถเรียกดูสถิติการเข้าออกภายในระบบเครือข่ายได้ ส่วนนี้จะเรียกว่า Anomaly Data
- การเก็บล็อกไฟล์ (log file) ที่มีอยู่ในเครื่องเซิร์ฟเวอร์และอุปกรณ์เครือข่ายเพื่อทำการ correlation log ทั้งหมด เพื่อตรวจหาสิ่งผิดปกติที่เกิดขึ้น เพื่อใช้ในการสืบหาการกระทำผิดทางอาชญากรรมคอมพิวเตอร์ ส่วนนี้จะเรียกว่า Data Collection Monitoring

## การจัดการระบบความปลอดภัย

- ***การจัดการกฎพื้นฐาน (Rule base)***
  - 1.) กฎพื้นฐานไฟร์วอลล์ (Rule base Firewall) การกำหนดทางเข้าทางออกผ่านกฎเกณฑ์ที่เหมาะสม และสามารถที่จะ block content ในระดับ Application ในส่วนการโจมตีที่ต่อเนื่องจากผู้บุกรุกได้ (Denial of Service)
  - 2.) Rule Access Control List ในอุปกรณ์เราท์เตอร์ มองระดับเน็ตเวิร์กเลเยอร์ (Network Layer) การเข้าออกของ IP และ Port
  - 3.) กฎพื้นฐานในระบบตรวจจับผู้บุกรุก (Intrusion Detection System) ควรมีการจัดการในส่วน update signature ใหม่ๆ ที่เกิดขึ้น และสามารถวิจัยการโจมตีใหม่ๆ ได้ เพื่อสร้าง Rule base ใหม่เพื่อจดจำในการใช้งานต่อไป
  - 4.) กฎพื้นฐานในการทำการสแกนหาช่องโหว่ที่เกิดขึ้นในเครือข่าย (Vulnerability Scan) และมีการจัดการในส่วนของเครื่องมือ ในการตรวจสอบระบบเครือข่าย โดยมีการตั้งค่าให้ทำงานในช่วงเวลาใดเวลาหนึ่งและทำเป็นแผนงาน เมื่อพบช่องโหว่ก็สามารถที่จะระบุผู้ปฏิบัติงานได้ว่าควรจะปิดส่วนไหน และมีการ update signature ในการทำการตรวจสอบอย่างสม่ำเสมอ



## การจัดการระบบความปลอดภัย

- ***การกำหนดค่าการสำรองข้อมูล (Backup data)*** ในการทำการตรวจจับความปลอดภัยเครือข่าย คือการสำรองข้อมูลและเก็บบันทึกไว้เพื่อใช้ตรวจสอบย้อนหลัง
- ***การกำหนดสิทธิของผู้ใช้งาน*** ว่าเป็นระดับผู้ใช้ (User) หรือผู้บริหารระบบ (System administrator) โดยแบ่งเป็น 2 ส่วน คือ การกำหนดสิทธิผู้ใช้ในการทำงาน และการเข้าถึงระยะไกล (remote access) และการกำหนดสิทธิผู้บริหารระบบในการทำงานและการเข้าถึงระยะไกล
- ***การกำหนดนโยบายความปลอดภัย (Security Policy)*** โดยการจัดทำนโยบายด้านความปลอดภัย ซึ่งอ้างอิงกับมาตรฐานสากล เช่น มาตรฐาน ISO เป็นต้น
- ***การสร้างความตระหนักถึงความปลอดภัย (Security Awareness)*** ในการใช้งานข้อมูลสารสนเทศ และกระตุ้นให้พนักงานในองค์กรมีความรู้ด้านการป้องกันภัยระบบสารสนเทศ

# 5.4 การพัฒนานโยบายความปลอดภัยเครือข่าย

- **นโยบายด้านความปลอดภัยไอทีทั่วไป** วัตถุประสงค์ดังนี้
  - การป้องกันแหล่งทรัพยากร กำหนดขึ้นเพื่อรับรองว่าผู้ใช้ที่ได้รับอนุญาตแล้วเท่านั้นที่สามารถเข้าสู่ระบบและใช้งานทรัพยากรภายในระบบได้
  - การรับรองหรือการแสดงที่มาที่ไว้ใจได้ ทำให้ระบบสามารถที่จะป้องกันต่อความเสี่ยงของการปลอมตัวในการเข้าถึงระบบได้
  - การอนุญาต เป็นการรับรองว่าผู้ใช้งานหรือเครื่องคอมพิวเตอร์ใดที่อยู่ห่างไกลจะได้รับอนุญาตให้กระทำการใดๆ ในระบบได้
  - การทำให้สมบูรณ์ คือ ความมั่นคงของข้อมูลที่ได้รับการปกป้องจากการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต หรือได้รับการป้องกันข้อมูลจากการถูกสอดแนมและการถอดรหัส
  - การเก็บเป็นความลับ สำหรับข้อมูลที่เป็นความลับจะต้องมีการรักษาความลับให้ได้ เช่นการเข้ารหัสข้อมูล เป็นต้น



# 5.4 การพัฒนานโยบายความปลอดภัยเครือข่าย

- ***นโยบายด้านผู้ใช้*** คือ การกำหนดว่าผู้ใช้สามารถที่จะทำอะไรได้ เมื่อเข้าใช้งานระบบเครือข่ายหรือข้อมูลขององค์กร
  - *การตั้งรหัสผ่าน* วิธีนี้จะช่วยรักษาข้อมูลส่วนตัวของผู้ใช้ให้ปลอดภัยจากภัยอันตรายต่างๆ
  - *การใช้ข้อมูลส่วนตัว* คือ การอนุญาตให้ใช้ข้อมูลส่วนตัวของผู้ใช้ โดยการกำหนดว่าควรเก็บที่ใด
  - *การใช้อินเทอร์เน็ต* คือ การกำหนดว่าผู้ใช้จะสามารถใช้อะไรได้บ้างในระบบเครือข่ายอินเทอร์เน็ต เช่น ให้ใช้อีเมล์ได้แต่ไม่ให้ใช้โทรศัพท์อินเทอร์เน็ต
  - *การเข้าใช้ระบบ* หมายความว่า เมื่อเข้าสู่ระบบแล้วผู้ใช้จะสามารถจัดการกับระบบได้ เช่น ผู้ใช้สามารถติดตั้งโปรแกรม หรือเข้าใช้ฐานข้อมูลส่วนตัว เป็นต้น
  - *การเข้าถึงระยะไกล* เป็นการอนุญาตให้ผู้ใช้สามารถควบคุมเครื่องระยะไกลได้ (Remote Access) โดยการใช้โปรแกรม Telnet
  - *การใช้อุปกรณ์* หมายถึง การอนุญาตให้ผู้ใช้สามารถใช้งานอุปกรณ์ที่เกี่ยวข้องกับการทำงานของระบบคอมพิวเตอร์ได้ เพื่อป้องกันการเกิดปัญหากับระบบ เช่น ป้องกันไวรัสจากการใช้อุปกรณ์ Flash Drive เป็นต้น

## 5.4 การพัฒนานโยบายความปลอดภัยเครือข่าย

- ***นโยบายด้านสารสนเทศ*** เพื่อให้สามารถบริหารระบบเครือข่ายได้อย่างปลอดภัยและมีความมั่นคงสูงสุด
  - *ด้านระบบรักษาความปลอดภัย* คือ การตรวจหาการบุกรุก การยับยั้งและการกำจัดผู้ที่ไม่หวังดีที่ต้องการเข้าสู่ระบบเครือข่าย
    - การเตรียมพร้อม การระบุชี้ชัด การยับยั้ง การกำจัด การฟื้นฟู การสรุปข้อมูลการถูกโจมตี
  - *ด้านการสำรองข้อมูล* คือ การกำหนดว่าองค์กรจะสำรองข้อมูลอะไร ใครเป็นผู้ดูแลรับผิดชอบข้อมูลจะถูกสำรองไว้ที่ใด การเก็บรักษาจะไว้นานเท่าใด และควรใช้โปรแกรมอะไรในการสำรองข้อมูล
  - *ด้านการทำให้ข้อมูลทันสมัย* คือ การดำเนินการในกรณีที่มีการเปลี่ยนแปลงของข้อมูลสารสนเทศเป็นระยะๆ จึงจำเป็นที่จะต้องมีการปรับปรุงข้อมูลให้ทันสมัย โดยการกำหนดว่าควรจะใช้วิธีการและเครื่องมือใดบ้างในการปรับปรุงข้อมูล
  - *ด้านการใช้ไฟร์วอลล์* เพื่อป้องกันการโจมตีระบบเครือข่าย โดยไฟร์วอลล์ที่ใช้ป้องกันอาจจะเป็นอุปกรณ์ประเภทฮาร์ดแวร์หรือซอฟต์แวร์ก็ได้ โดยอาจจะกำหนดเป็นชั้นเดียวหรือหลายชั้น



## 5.4 การพัฒนานโยบายความปลอดภัยเครือข่าย

- ***นโยบายทั่วไป*** คือ การกำหนดนโยบายที่จะช่วยเสริมสร้างมาตรฐานสำหรับการป้องกันแหล่งทรัพยากรทาง
- เพื่อการยอมรับและปฏิบัติตามทั่วทั้งองค์กร ตลอดจนมีความยืดหยุ่นเพียงพอที่จะปรับให้เข้ากับกิจกรรมและทรัพยากรที่มีอยู่ได้ เช่น
  - *การวางแผนความต่อเนื่อง* คือ การวางแนวทางเพื่อรักษาความปลอดภัยให้กับองค์กรหรือหน่วยงาน เพื่อให้สามารถผ่านพ้นช่วงเวลาวิกฤติที่เป็นผลจากการคุกคามของผู้ไม่หวังดีต่อองค์กร
  - *การกู้คืนจากภาวะถูกคุกคาม* เช่น การกู้คืนเครื่องคอมพิวเตอร์แม่ข่าย การกู้คืนข้อมูล การกู้คืนระบบโทรศัพท์ เป็นต้น

## 5.4 การพัฒนานโยบายความปลอดภัยเครือข่าย

- นโยบายเฉพาะประเด็นในด้านความปลอดภัยไอที
  - ความหมายและองค์ประกอบ เป็นการกำหนดนโยบายในการรักษาความปลอดภัยไอทีขององค์กร โดยการดำเนินการจัดหาอุปกรณ์เทคโนโลยีให้แก่องค์กรและให้ความรู้แก่พนักงานเพื่อให้ใช้เครื่องมือในสำนักงานได้อย่างเหมาะสมและปลอดภัย
  - คำแถลงนโยบาย เป็นการเริ่มต้นการรายงานความชัดเจนของวัตถุประสงค์ของนโยบายครอบคลุมความปลอดภัยสำหรับผู้ใช้เว็บและอินเทอร์เน็ต
  - การอนุญาตให้เข้าถึงข้อมูลและการใช้อุปกรณ์
  - ข้อห้ามในการใช้อุปกรณ์



## 5.4 การพัฒนานโยบายความปลอดภัยเครือข่าย

- นโยบายเฉพาะประเด็นในด้านความปลอดภัยไอที
  - ข้อห้ามในการใช้อุปกรณ์
    - การละเมิดทรัพย์สินทางปัญญา ความหมายของทรัพย์สินทางปัญญา คือผลงานอันเกิดจากความสร้างสรรค์ของมนุษย์ เช่น
    - ลิขสิทธิ์ คือ สิทธิแต่เพียงผู้เดียวที่จะกระทำการใดๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น การคุ้มครองลิขสิทธิ์และข้อห้าม เช่น ห้ามทำซ้ำหรือดัดแปลง คัดลอก ทำสำเนา หรือแปล ห้ามนำผลงานผู้อื่นมาเผยแพร่ต่อสาธารณะชนโดยไม่ได้รับอนุญาต เป็นต้น
    - สิทธิบัตร คือ หนังสือสำคัญที่ออกให้แก่ผู้ประดิษฐ์ คิดค้น หรือออกแบบผลิตภัณฑ์ใหม่ๆ การคุ้มครองสิทธิบัตรและข้อห้าม ได้รับการคุ้มครองในการผลิตสินค้าที่เปิดเผยไว้แต่เพียงผู้เดียว ตัวอย่างสิทธิบัตร เช่น สิทธิบัตรไฟร์วอลล์(Firewall) เป็นต้น

## 5.4 การพัฒนานโยบายความปลอดภัยเครือข่าย

- นโยบายเฉพาะประเด็นในด้านความปลอดภัยไอที
  - การจัดการระบบ (Systems Management)
  - การละเมิดนโยบาย
  - การตรวจสอบทบทวนและแก้ไขนโยบาย
  - ข้อจำกัดความรับผิดชอบ



## 5.4 การพัฒนานโยบายความปลอดภัยเครือข่าย

- นโยบายความปลอดภัยไอทีที่เกี่ยวกับระบบ
  - นโยบายการควบคุมสิทธิการเข้าถึง (ACL = Access Control List Policies) คือกฎระเบียบที่ใช้ในการควบคุมสิทธิการเข้าถึงระบบของบุคคลแต่ละคนและลำดับชั้นข้อมูลความลับ เช่น การควบคุมการเข้าถึงของขั้นตอน การจัดเก็บ การเรียกใช้ การถ่ายโอน และการเปลี่ยนแปลงข้อมูล หรือการใช้อุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ต่างๆ ในการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ต
  - นโยบายด้านกฎเกณฑ์ การกำหนดกฎเกณฑ์ในลักษณะเฉพาะเจาะจงมากกว่าการควบคุมสิทธิการเข้าถึง (ACL) และอาจไม่เกี่ยวข้องกับผู้ใช้โดยตรง
    - เช่น การใช้ไฟร์วอลล์(Firewalls) โดยที่ผู้ใช้สามารถตั้งค่าตัวแปรในการควบคุมไฟร์วอลล์ได้เอง รวมไปถึงค่าตัวแปรในระดับเครือข่ายด้วย ทำให้สามารถช่วยป้องกันการบุกรุกจากผู้ไม่หวังดี

## 5.5 การคุกคามความปลอดภัยเครือข่าย

- **การคุมคามจากโปรแกรม** ลักษณะการคุกคามจากโปรแกรมจะทำให้ระบบเครือข่ายให้บริการที่ผิดพลาด ซึ่งอาจส่งผลให้เครื่องผู้ใช้บริการรับผลจากความผิดพลาดนั้นไปด้วย
- **การคุมคามจากแฮกเกอร์** แฮกเกอร์ (Hacker) หมายถึงผู้บุกรุกที่พยายามเข้าสู่ระบบเครือข่ายที่มีระบบการป้องกัน เพื่อที่จะเข้าไปดูข้อมูลภายในระบบ โดยไม่มีการเปลี่ยนแปลงหรือแก้ไขข้อมูลใดๆ หากผู้บุกรุกพยายามเปลี่ยนแปลงแก้ไขข้อมูลใดๆ แล้ว ผู้บุกรุกในลักษณะดังกล่าวจะถูกเรียกว่า แคร็กเกอร์ (Cracker)



## 1. การคุกคามจากโปรแกรม

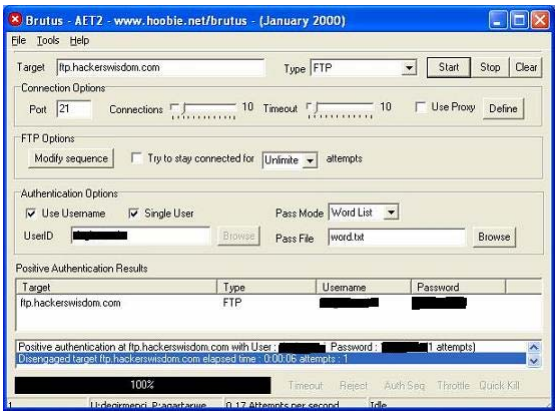
- ***ไวรัส (Virus)*** คือ โปรแกรมที่ทำลายระบบการทำงานของคอมพิวเตอร์ โดยเมื่อไวรัสเข้าสู่เครื่องคอมพิวเตอร์แล้วจะแพร่กระจายไปในโปรแกรมอื่นๆ ภายในเครื่องเท่านั้น ไวรัสจะไม่สามารถแพร่ กระจายตัวเองไปในเครื่องคอมพิวเตอร์อื่นได้ นอกจากจะมีผู้ใช้นำโปรแกรมที่ติดไวรัสดังกล่าวไปใช้ยังเครื่องคอมพิวเตอร์อื่น ไวรัสบางชนิดอาจเพียงรบกวนการทำงานของผู้ใช้เท่านั้น แต่บางชนิดสามารถที่จะทำลายข้อมูลทั้งหมดในฮาร์ดดิสก์ (Hard disk)
- ***เวิร์ม (Worm)*** คือ โปรแกรมที่ทำลายระบบการทำงานของคอมพิวเตอร์ที่มีลักษณะคล้ายไวรัส แต่มีระดับความรุนแรงในการทำลายระบบมากกว่า เพราะนอกจากจะแพร่กระจายเพื่อทำลายระบบการทำงานของเครื่องคอมพิวเตอร์แล้ว เวิร์มยังสามารถแพร่กระจายผ่านระบบเครือข่ายเข้าไปทำลายคอมพิวเตอร์เครื่องอื่นๆ ได้ด้วยตัวเอง
- ม้าโทรจัน (Trojan Horse) คือโปรแกรมที่ทำลายระบบคอมพิวเตอร์ที่แฝงมากับโปรแกรมประเภทอื่นๆ เช่น เกม และโปรแกรมอำนวยความสะดวกต่างๆ เป็นต้น ลักษณะการทำงานของม้าโทรจัน เมื่อผู้ใช้ทำการติดตั้งโปรแกรมที่ต้องการแล้วเริ่มใช้งาน โปรแกรมม้าโทรจันที่แฝงมาจะเข้าทำลายระบบของเครื่องคอมพิวเตอร์โดยใช้วิธีการต่างๆ เช่น การลบไฟล์ ซ่อนไฟล์ต่างๆ ภายในเครื่อง หรือที่รุนแรงกว่านั้นคือโปรแกรมม้าโทรจันจะสร้างทางเข้าประตูหลัง (Back door) ให้กับโปรแกรมประเภทอื่นๆ ที่มุ่งหวังบุกรุกเพื่อเข้ามาทำลายระบบ หรือลักลอบขโมยข้อมูล เป็นต้น

## 2. การคุกคามจากแฮกเกอร์

- การโจมตีรหัสผ่าน (Password Attacks) *เป็นวิธีการเข้าโจมตีระบบเครือข่ายโดยที่ผู้บุกรุกได้พยายามทดลองใช้รหัสผ่านเข้าสู่ระบบที่ได้จากการคาดเดา เพื่อหวังเข้าใช้งานในระบบเครือข่ายให้เหมือนกับเป็นผู้ใช้งานในระบบนั้นจริงๆ*



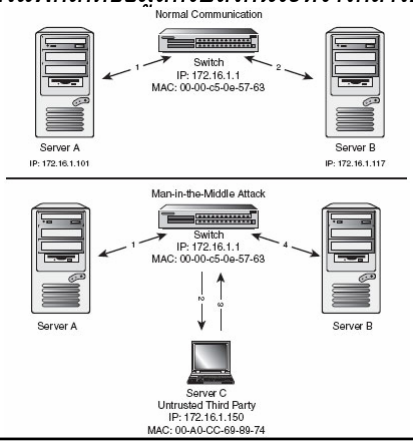
## 2. การคุกคามจากแฮกเกอร์




การโจมตีรหัสผ่าน (Password Attacks)

## 2. การดักฟังจากแฮกเกอร์

- การโจมตีแบบ Man-in-the-Middle *เป็นวิธีการที่ผู้บุกรุกสามารถผ่านเข้าถึงแพ็กเก็ตข้อมูลที่รับส่งกันระหว่างกลางบนเครือข่ายได้*

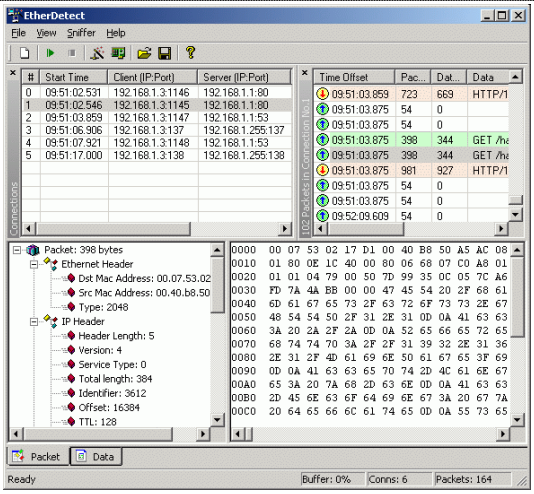





## 2. การดักฟังจากแฮกเกอร์

- แพ็กเก็ตสนิฟเฟอร์ (packet sniffer) *เป็นอุปกรณ์หรือซอฟต์แวร์ที่สามารถอ่านแพ็กเก็ตที่รับส่งในระบบเครือข่ายได้ การสนิฟแพ็กเก็ตเป็นเทคนิคการดักจับแบบเงียบๆ ที่ยากต่อการจับ ซึ่งในปัจจุบันโปรแกรมประเภทนี้สามารถหาดาวน์โหลดได้ง่าย เนื่องจากบุคคลบางกลุ่มได้ทำการลักลอบพัฒนาโปรแกรมจากคุณสมบัติของโปรโตคอล* ***TCP/IP*** *ให้สามารถตรวจจับทุกแพ็กเก็ตเพื่อค้นหาชื่อผู้ใช้และรหัสผ่านได้ จากนั้นผู้บุกรุกก็จะใช้รหัสผ่านที่ตรวจจับได้ในแพ็กเก็ตนั้นแล้วนำมาล็อกอินเข้าสู่ระบบเครือข่าย ซึ่งทำให้เกิดความเสียหายแก่ระบบได้มากมาย เช่น การเปลี่ยนรหัสผ่านในระบบ ซึ่งทำให้ผู้ใช้งานจริงไม่สามารถล็อกอินเข้าสู่ระบบได้ เป็นต้น*

# 2. การดักตามจากแฮกเกอร์



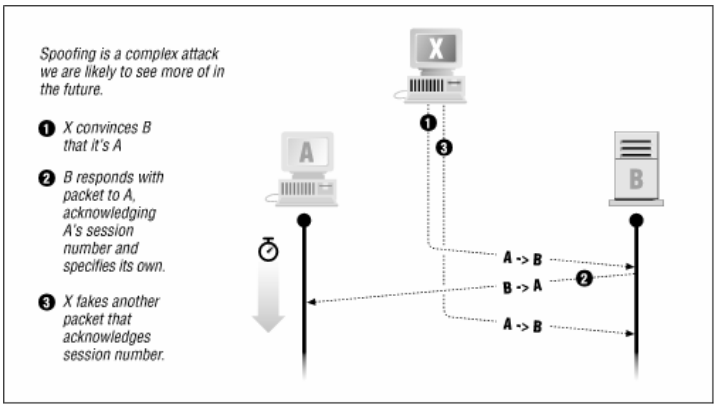

แพ็กเก็ตสนิฟเฟอร์ (packet sniffer)



# 2. การดักตามจากแฮกเกอร์

- ไอพีสปูฟฟิง (IP Spoofing) *วิธีการที่ผู้บุกรุกจากภายนอกทำการสร้างข้อมูลปลอมที่เชื่อถือได้ เช่น การใช้ค่าไอพีแอดเดรสปลอมเหมือนกับค่าไอพีในเครือข่าย และนำมาขอใช้บริการในระบบเครือข่ายนั้น ทำให้ระบบเครือข่ายนั้นอนุญาตให้ใช้ทรัพยากรต่างๆ ในเครือข่ายได้*

## 2. การคุกคามจากแฮกเกอร์



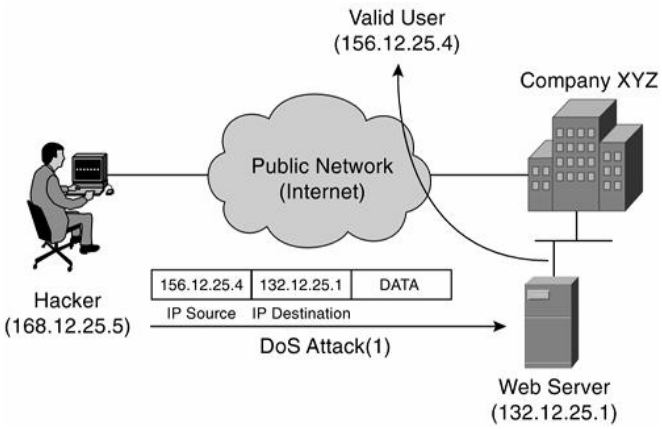

ไอพีสปูฟฟิง (IP Spoofing)



## 2. การคุกคามจากแฮกเกอร์

- การโจมตีแบบ DoS (Denial-of-Service) *เป็นวิธีการเข้าโจมตีเครื่องเซิร์ฟเวอร์ โดยการทำให้ระบบการให้บริการของเครื่องเซิร์ฟเวอร์เกิดการใช้บริการข้อมูลจนถึงขีดจำกัด จนเครื่องเซิร์ฟเวอร์ไม่สามารถให้บริการแก่เครื่องอื่นๆ ได้ การโจมตีแบบนี้ทำได้โดยการร้องขอการใช้บริการกับเครื่องเซิร์ฟเวอร์จนถึงขีดสุดของเซิร์ฟเวอร์ โดยอาจใช้โปรโตคอล* ***TCP*** *เป็นเครื่องมือในการโจมตีที่จุดอ่อนของระบบเครือข่าย หรือระบบรักษาความปลอดภัยของเครือข่าย*

## 2. การคุกคามจากแฮกเกอร์




การโจมตีแบบ DoS (Denial-of-Service)



## 2. การคุกคามจากแฮกเกอร์

- การโจมตีแบบ Distributed Denial of Service (DDoS)
- นำเครื่องมือที่จะใช้ในการโจมตีไปติดตั้งบนเครื่องที่ถูกเจาะไว้
  - จากนั้นจึงจะระดมส่งข้อมูลในรูปแบบที่ควบคุมได้โดยผู้ควบคุมการโจมตีไปยังเหยื่อหรือเป้าหมายที่ต้องการ
- การโจมตีรูปแบบนี้มักจะก่อให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่จนผู้อื่นไม่สามารถใช้งานได้ตามปกติ
  - หรือทำให้ระบบที่ถูกโจมตีไม่มีทรัพยากรเหลือพอที่จะให้บริการผู้ใช้ธรรมดาได้
- การป้องกันการโจมตีแบบ DoS นั้น
  - จะสามารถทำได้ก็ต่อเมื่อทราบวิธีของการโจมตีก่อน และการป้องกันการโจมตีในบางครั้งก็ไม่สามารถทำได้ในครั้งเดียว ขึ้นอยู่กับรูปแบบการโจมตี สถาปัตยกรรมของเป้าหมายที่ถูกโจมตี

## 2. การคุกคามจากแฮกเกอร์

- รูปแบบการโจมตีที่นิยมใช้กันก็มีอย่าง SYN flood, UDP flood, ICMP flood, Smurf, Fraggle เป็นต้น
- SYN Flood
  - เป็นการโจมตีโดยการส่งแพ็คเก็ต TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ source address ได้)
  - เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายัง source ip address ที่ระบุไว้
  - ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน source ip address ไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิดสภาวะ half-open ขึ้นที่เครื่องเป้าหมาย
  - หากมีการส่ง SYN flood จำนวนมาก ก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม ทำให้ไม่สามารถให้บริการตามปกติได้



## 2. การคุกคามจากแฮกเกอร์

- SYN Flood
  - การป้องกัน Cisco Router
  - เราเตอร์ของ Cisco มีฟังก์ชันการทำงานชื่อ TCP Intercept ซึ่งถูกออกแบบมาเพื่อต่อต้านการโจมตีแบบ SYN flood
  - โดย TCP intercept software จะพยายามสร้างการเชื่อมต่อกับ client หากสำเร็จการเชื่อมต่อดังกล่าวก็จะถูกส่งไปให้กับเครื่องให้บริการต่อไป
  - ดังนั้นการโจมตีแบบ SYN flood จะไม่สามารถเข้าไปถึงเครื่องเป้าหมายจริงๆ ได้
  - ข้อเสียคือจะทำให้เราเตอร์ใช้ทรัพยากรมากกว่าปกติ

## 2. การคุกคามจากแฮกเกอร์

- ICMP Flood
  - เป็นการส่งแพ็คเก็ต ICMP จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่
- **การป้องกัน**
  - ระบบส่วนใหญ่สามารถทำงานได้โดยไม่ต้องใช้ ICMP Echo Request ซึ่งสามารถป้องกันการใช้งานได้โดยใช้คำสั่งที่เราเตอร์หรืออุปกรณ์กรองแพ็คเก็ตอื่นๆ



## 2. การคุกคามจากแฮกเกอร์

- UDP Flood
  - เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่และ/หรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด โดยจะส่ง UDP packet ไปยัง port ที่กำหนดไว้ เช่น 53 (DNS)
- **การป้องกัน**
  - เราเตอร์และอุปกรณ์กรองแพ็คเก็ตอื่นๆ สามารถ drop แพ็คเก็ตที่มุ่งโจมตีมายัง port ที่ไม่เป็นที่ต้องการได้
  - เช่น โจมตีมายัง port ที่ไม่ได้ให้บริการใน port ดังกล่าว ในกรณีที่เป็นการโจมตีเฉพาะ port ที่เปิดให้บริการ เช่น port 53 ก็สามารถป้องกันระบบเป้าหมายได้โดยใช้ CAR เพื่อจำกัดจำนวนข้อมูล
  - ฟังก์ชันชื่อ Committed Access Rate (CAR) ซึ่งใช้ในการจำกัดแบนด์วิดธ์ที่ใช้สำหรับแต่ละบริการได้

## 2. การคุกคามจากแฮกเกอร์

- Smurf
  - ผู้โจมตีจะส่ง ICMP Echo Request ไปยัง broadcast address ในเครือข่ายที่เป็นตัวกลาง(ปกติจะเรียกว่า amplifier)
  - โดยปลอม source ip address เป็น ip address ของระบบที่ต้องการโจมตี ซึ่งจะทำให้เครือข่ายที่เป็นตัวกลางส่ง ICMP Echo Reply กลับไปยัง ip address ของเป้าหมายทันที ซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่
- **การป้องกัน**
  - เช่นเดียวกันกับการโจมตีแบบ ICMP flood เราเตอร์และอุปกรณ์กรองแพ็คเก็ตอื่นๆ สามารถ drop ICMP Echo Reply ซึ่งในกรณีนี้ควร drop ICMP Echo Reply ที่ส่งเข้ามาโดยไม่ได้มีการส่ง ICMP Echo Request ออกไปก่อน
  - การทำงานลักษณะนี้อาจจะทำให้อุปกรณ์ packet filtering ใช้ทรัพยากรเพิ่มขึ้น และในกรณีที่เกิดการโจมตีขึ้นแล้วยังสามารถบล็อก source ip address ของ ICMP Echo Reply ได้ เพราะผู้โจมตีไม่สามารถเปลี่ยนแปลงข้อมูลส่วนนี้ได้



## 2. การคุกคามจากแฮกเกอร์

- Fraggle
  - เป็นอีกรูปแบบหนึ่งของการโจมตีแบบ Smurf โดยผู้โจมตีจะส่ง UDP Echo Request (UDP port 7) ไปยัง broadcast address ของ amplifier network โดยปลอม source ip address ไปเป็น ip address ของเป้าหมาย
  - ซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่ และ/หรือทำให้มีการใช้ทรัพยากรของเป้าหมายจนหมดไป ซึ่งการโจมตียังสามารถใช้ได้กับ UDP, TCP services อื่น
- **การป้องกัน**
  - สามารถป้องกันได้คล้ายๆ กับการป้องกันการโจมตีแบบ Smurf attack โดยใช้เราเตอร์หรืออุปกรณ์กรองแพ็คเก็ตอื่นๆ drop แพ็คเก็ต UDP/TCP ที่ใช้โจมตีเข้ามา หรืออาจจะใช้วิธีบล็อก source ip address ได้เช่นเดียวกัน

## 2. การคุกคามจากแฮกเกอร์

- โดยปกติการโจมตีแบบ DoS ผู้โจมตีมักจะโจมตีไปยังเป้าหมายโดยระบุเป็น ip address โดยตรง ไม่ได้ผ่านการทำ DNS lookup มาก่อน
- ดังนั้น เมื่อเกิดการโจมตีขึ้น ยังสามารถหาหนทางหลบหลีกการโจมตีดังกล่าวได้ 2 วิธีคือ
  - 1. เปลี่ยน ip address เมื่อเกิดการโจมตี
  - 2. เปลี่ยน ip address ไปเรื่อยๆ แม้จะไม่มีการโจมตี
- ซึ่งการกระทำทั้งสองรูปแบบก็มีข้อดีข้อเสียต่างกัน
  - ในรูปแบบแรกจะต้องมีระบบตรวจจับที่ดี สามารถแจ้งเตือนผู้ดูแลระบบให้สามารถปรับเปลี่ยน ip address ได้อย่างรวดเร็ว จะเห็นว่ามีช่องว่างระหว่างการดำเนินงานอยู่ แต่ก็มียังมีข้อดีที่ผู้โจมตีจะไม่สามารถรู้แทกติกนี้จนกว่าจะเริ่มโจมตี
  - ในขณะที่วิธีที่สองจะมีความยากลำบากในการเริ่มโจมตีมากกว่า



## 2. การคุกคามจากแฮกเกอร์

- การแก้ไข DNS
  - การแก้ไข DNS entries โดยเปลี่ยน ip address ของระบบที่กำลังถูกโจมตีไปเป็น ip address ใหม่ ให้พยายามลดค่า TTL ของ DNS record ให้น้อยที่สุดเท่าที่จะเป็นไปได้ และพิจารณาว่าควรย้าย DNS server ไปยังลิ้งค์อื่นที่ไม่ใช่ลิ้งค์เดียวกันกับระบบที่กำลังถูกโจมตี โดยพิจารณาได้จาก traffic ที่จะเกิดขึ้นจาก DNS server เครื่องนี้
  - นอกจากนี้ควรตรวจสอบ secondary DNS server ด้วยว่ามีความพร้อมในการทำงานหรือไม่หาก primary DNS server มีปัญหา
- Network Address Translation
  - หากระบบที่ถูกโจมตีสามารถใช้งาน NAT ได้ ก็จะทำให้ง่ายในการเปลี่ยน ip address หากไม่มี NAT ถูกติดตั้งในระบบไว้แล้ว ก็ควรติดตั้งเพิ่มเติม โดยปกติแล้วเราเตอร์ก็มีความสามารถนี้ นอกจากนี้ควรพิจารณาถึงระบบที่สามารถทำ load balancing ได้ เพื่อกระจายภาระงานให้ทั่วถึง

## 2. การคุกคามจากแฮกเกอร์

- filter ค่า ip address เดิม
  - traffic ที่เข้ามายัง ip address ตัวเดิมจะมีแค่ traffic ที่เกิดจากการโจมตีและจากผู้ใช้ที่ยังใช้ค่า DNS entry เก่าเท่านั้น(ซึ่งเกิดจากการกระจายตัวของ DNS entry นั้นจะต้องใช้เวลาซักระยะ)
  - ดังนั้นจึงสามารถบล็อก traffic สำหรับ ip address นี้ได้ หากไม่ต้องการให้ traffic ของ ip address ชุดเดิมเข้ามาภายในระบบก็สามารถทำได้โดยการยกเลิก routing สำหรับ ip address เดิมเสีย
- ใช้ ip address ชุดใหม่และลิ้งค์ที่แตกต่าง
  - มีวิธีแก้ไขที่ได้ผลอีกวิธีคือ การเปลี่ยนไปใช้ลิ้งค์ชุดใหม่และ ip address บล็อกใหม่ทั้งหมด หากผู้โจมตีหยุดการโจมตีและเปลี่ยนเป้าหมายเป็น ip address ชุดใหม่ ผู้ดูแลระบบก็สามารถเปลี่ยน ip address และลิ้งค์กลับไปเป็นลิ้งค์เดิมได้

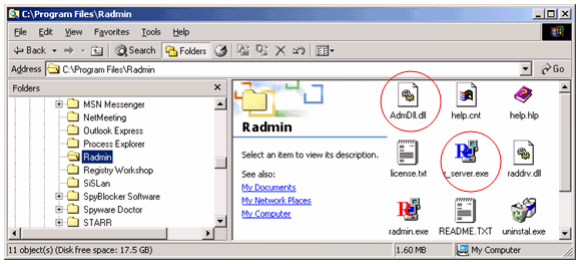


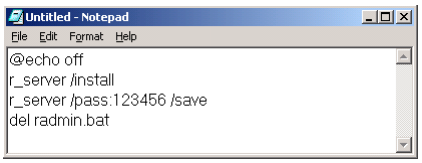
## 2. การคุกคามจากแฮกเกอร์

- **การปิดบังอำพราง** *(Covering)*
- เวลาเสร็จงานโจรกรรมต่างๆแล้วก็ต้องมีการทำลายหลักฐาน
- คุณแค่ลบไฟล์ ที่เป็นไฟล์ log ที่เก็บข้อมูลต่างๆเท่านั้นก็เพียงพอแล้ว และไฟล์ที่คุณได้ส่งเข้าไป หรือสร้างขึ้นมาบนเครื่องเหยื่อ ถ้ามันหมดประโยชน์แล้วก็ควรกำจัดทิ้งไปด้วย
- โปรแกรม Clearevent log.exe ซึ่งโปรแกรมนี้จะคอยลบไฟล์ต่างๆใน log ให้หมดสิ้นไป
  - โปรแกรมกำจัด log ไฟล์ต่างๆ (โปรแกรมประเภทที่ไม่จำเป็นต้องติดตั้งที่เครื่องเหยื่อ) ที่สามารถรันได้เลยจะยิ่งดี เพราะมันจะทำการเคลียร์ ลบ หลักฐานต่างๆที่เราเข้าไปเจาะ ซึ่งบางทีมันอาจเก็บค่า IP รวมไปถึงการกระทำต่างๆ และเวลา ที่คุณได้กระทำเอาไว้

## 2. การดูกตามจากแฮกเกอร์

- การสร้างประตูลับ *(Back doors)*






## 2. การดูกตามจากแฮกเกอร์

- **Port Scanning** เป็นหนึ่งในเทคนิคที่โด่งดังที่สุดที่ผู้โจมตีใช้ในการค้นหาบริการ Service ที่พวกเขาจะสามารถเจาะผ่านเข้าไปยังระบบๆได้ โดยปกติแล้วทุก ๆ ระบบที่ต่อเข้าสู่ระบบ LAN หรือระบบอินเทอร์เน็ตจะเปิด service อยู่บน port ที่เปิดเป็นตัวเลขต่างๆ

## 2. การคุกคามจากแฮกเกอร์

- ถึงแม้ว่า Port Scans สามารถเกิดขึ้นกับระบบของคุณ แต่ก็สามารถตรวจจับได้และก็สามารถใช้เครื่องมือที่เหมาะสมมาจำกัดจำนวนของข้อมูลเกี่ยวกับบริการที่เปิดได้ ทุกๆระบบที่เปิด สู่สาธารณะจะมีพอร์ตหลายพอร์ตที่เปิดและพร้อมให้ใช้งานได้ (ต้องรู้ว่าแต่ละ port ที่เปิดนั้นคือบริการอะไร)
- ต้องทำการกำหนดสิทธิ์ต่างในแต่ละ port และจำกัดจำนวนพอร์ตที่จะเปิดให้แก่ผู้ใช้ที่ได้รับอนุญาตและปฏิเสธการเข้าถึงมายังพอร์ตที่ปิด



## 2. การคุกคามจากแฮกเกอร์

- เทคนิคของ Port Scanning อยู่มากมายหลายรูปแบบ ซึ่งมีเครื่องมือ Port Scanning ที่ทำงานโดยอัตโนมัติ เช่น Nmap และ Nessus
- **รูปแบบมาตรฐานสำหรับ Nmap และ Nessus**

## 2. การดุกตามจากแฮกเกอร์

- **1. Address Resolution Protocol (ARP)** scans จะตรวจหาอุปกรณ์ที่ทำงานในเครือข่ายโดยการส่งชุดของ ARP broadcasts และเพิ่มค่าของฟิลด์ที่บรรจุ IP address ของเป้าหมายในแต่ละ broadcast packet การ scan ชนิดนี้จะได้รับผลตอบสนองจากอุปกรณ์ที่มี IP บนเครือข่ายออกมาในรูปแบบของ IP address ของแต่ละอุปกรณ์ การ scan แบบนี้จึงทำการ map out ได้ทั้งเครือข่ายอย่างมีประสิทธิภาพ
- **2.The Vanilla TCP connect scan** เป็นเทคนิคการ scan แบบพื้นฐานและง่ายที่สุด คือจะใช้ connect system call ของระบบปฏิบัติการไปบนระบบเป้าหมายเพื่อเปิดการเชื่อมต่อไปยังทุก ๆ พอร์ตที่เปิดอยู่ การ scan ชนิดนี้สามารถจับได้ง่ายมาก โดยล็อก (log) ต่าง ๆ ของระบบที่เป็นเป้าหมายจะแสดงการร้องขอการเชื่อมต่อ (connection requests ) และข้อความแสดงข้อผิดพลาด (error messages) สำหรับบริการที่ตอบรับการเชื่อมต่อนั้น



## 2. การดุกตามจากแฮกเกอร์

- **3.The TCP SYN (Half Open) scans** เทคนิคนี้บางครั้งถูกเรียกว่า half open เพราะว่าระบบที่ทำการโจมตีไม่ได้ปิดการเชื่อมต่อที่ได้เปิดไว้ scanner จะส่ง SYN packet ไปยังเป้าหมายและรอการตอบสนอง ถ้าพอร์ตถูกเปิดไว้เป้าหมายก็จะส่ง SYN/ACK กลับมา แต่ถ้าพอร์ตถูกปิดอยู่ เป้าหมายก็จะส่ง RST กลับมา วิธีการ scan รูปแบบนี้ยากต่อการตรวจจับ ปกติเครื่องที่เป็นเป้าหมายจะทำหน้าที่ปิดการเชื่อมต่อที่เปิดไว้ และส่วนใหญ่จะไม่มีระบบการล็อกที่เหมาะสมในการตรวจจับการ scan ชนิดนี้
- **4.The TCP FIN scan** เทคนิคนี้สามารถที่จะทะลุผ่านไฟล์วอลล์ ส่วนใหญ่, packet filters , ละโปรแกรมตรวจจับการ scan ไปได้โดยไม่ถูกตรวจพบ เพราะระบบที่ทำการโจมตีจะส่ง FIN packets ไปยังระบบของเป้าหมาย สำหรับพอร์ตต่าง ๆ ที่ปิดอยู่จะตอบสนองกลับไปด้วย RST ส่วนพอร์ตที่เปิดจะไม่สนใจ packets เหล่านั้นเลย ดังนั้นเครื่องที่ทำการโจมตีก็จะได้ข้อมูลว่ามันได้รับ RST จากพอร์ตไหนบ้างและไม่ได้ RST จากพอร์ตไหนบ้าง

## 2. การคุกคามจากแฮกเกอร์

- **5.The TCP Reverse Ident scan** เป็นเทคนิคที่สามารถตรวจหาชื่อของเจ้าของแต่ละโพรเซสที่เป็นการเชื่อมต่อด้วย TCP บนเครื่องเป้าหมาย การ scan ชนิดนี้จะทำให้ระบบที่ทำการโจมตีสามารถเชื่อมต่อเข้าไปยังพอร์ตที่เปิดอยู่และใช้ ident protocol ในการค้นหาว่าใครเป็นเจ้าของโพรเซสบนเครื่องเป้าหมายได้
- **6.The TCP XMAS** ถูกใช้เพื่อหาพอร์ตบนเครื่องเป้าหมายที่อยู่ในสถานะ listening โดยจะส่ง TCP packet ที่มี flag เป็น URG, PSH และ FIN ใน TCP header ไปยังพอร์ตของเครื่องเป้าหมาย ถ้าพอร์ต TCP ของเครื่องเป้าหมายปิดอยู่ พอร์ตนั้นก็จะส่ง RST กลับมา แต่ถ้าพอร์ตเปิดอยู่ก็จะไม่สนใจ packet นั้นเลย
- **7.The TCP NULL scan** เทคนิคนี้จะส่ง TCP packet ที่มี sequence number แต่ไม่มี flag ออกไปยังเครื่องเป้าหมาย ถ้าพอร์ตปิดอยู่จะส่ง กลับมา RST packet กลับมา แต่ถ้าพอร์ตเปิดอยู่ ก็จะไม่สนใจ packet นั้นเลย



## 2. การคุกคามจากแฮกเกอร์

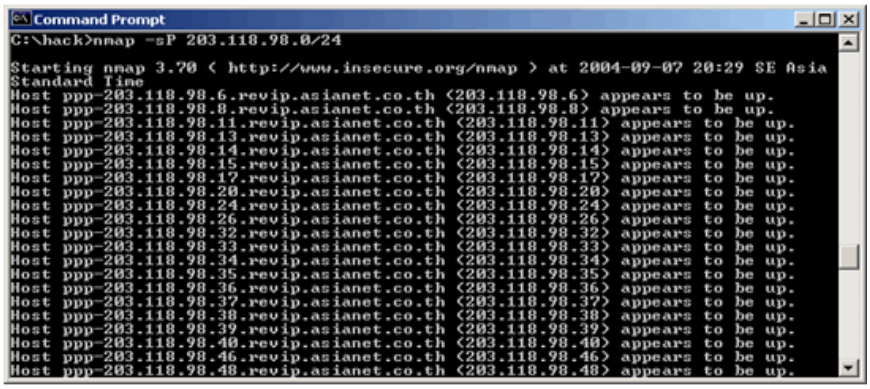
- **8.The TCP ACK scan** เป็นเทคนิคที่ใช้ค้นหาเว็บไซต์ที่เปิดบริการอยู่ แต่ปฏิเสธการตอบสนองต่อ ICMP ping หรือค้นหากฎ (rule) หรือนโยบาย ( policy) ต่าง ๆ ที่ตั้งไว้ที่ไฟล์วอลล์เพื่อตรวจสอบดูว่าไฟล์วอลล์สามารถกรอง packet อย่างง่าย ๆ หรือเทคนิคชั้นสูง โดยการ scan แบบนี้จะใช้ TCP packet ที่มี flag เป็น ACK ส่งไปยังพอร์ตเครื่องปลายทาง ถ้าพอร์ตเปิดอยู่ เครื่องเป้าหมายจะส่ง RST กลับมา แต่ถ้าปิดอยู่ก็จะไม่สนใจ packet นั้น
- **9.The FTP Bounce Attack** ใช้โพรโตคอล ftp สำหรับสร้างการเชื่อมต่อบริการ ftp ของ proxy วิธีการ scan แบบนี้ ผู้โจมตีจะสามารถซ่อนตัวอยู่หลัง ftp server และ scan เป้าหมายอื่น ๆ ได้โดยไม่ถูกตรวจจับ ดังนั้น ftp servers ส่วนใหญ่จะมีการ disable บริการของ ftp เพื่อความปลอดภัยของระบบ
- **10.The UDP ICMP port scan** ใช้โพรโตคอล UDP ในการ scan หาพอร์ตหมายเลขสูง ๆ โดยเฉพาะในระบบ Solaris แต่จะช้าและไม่น่าเชื่อถือ
- **11.The ICMP ping-sweeping scan** จะใช้คำสั่ง ping เพื่อกวาดดูว่ามีระบบไหนที่เปิดใช้งานอยู่ เครือข่ายส่วนใหญ่จึงมีการกรองหรือ disabled โพรโตคอล ICMP เพื่อความปลอดภัยของระบบ

## 2. การดุกตามจากแฮกเกอร์

- **เทคนิคการ Ping Sweep**
- การแสกนว่ามีเรื่องไหนยัง login อยู่หรือกำลังใช้งาน และ port ต่างที่เครื่องเหยื่อได้เปิดเอาไว้ จากบทความของผม เวลา**คุณจะต้องสนใจเครื่องของเหยื่อที่ port 139 กับ 445 เท่านั้น** เพราะเป็นส่วนจำเป็นในการ Hack Window
- คือการ ping ไปยังเครื่องเป้าหมายที่จำนวนมากๆ ในวง Network ที่คุณใช้อยู่ หรือวง lan นั่นเอง (ใน Internet ก็ใช้ได้) โดยแสกนพร้อมๆกันคล้ายกับการกราดยิง เพื่อตรวจสอบว่าเครื่องปลายทางได้เปิดอยู่หรือไม่ก็ตาม เช่น คุณมี IP **x.y.z.6** ตรง **x.y.z** อาจเป็นตัวเลขใดๆก็ได้ แต่เลข 6 คือเลขชุดหลังของ ip คุณ เวลาคุณแสกนหาให้เขียนลงไปดังนี้ **x.y.z.0/24** จากตรงเลข 6 เปลี่ยนเป็น **0/24** หมายความว่าเป็นการแสกน IP ตั้งแต่ **x.y.z.1- x.y.z.255**



## 2. การดุกตามจากแฮกเกอร์



## 2. การคุกคามจากแฮกเกอร์

- **เทคนิคการแสกนหลบ เมื่อเครื่องปลายทาง block ICMP**
  - จะเป็นการ Ping Sweep ขั้นสูงที่เรียกว่า TCP Ping scan โดยการใช้พารามิเตอร์ –PT พร้อมกับระบุหมายเลข port ต่างๆเข้าไป ซึ่งการระบุเลข port นั้นจะต้องทราบว่าเครื่องส่วนใหญ่นั้นจะต้องเปิดเอาไว้เพื่อติดต่อสื่อสารกับเครื่องอื่นๆ เช่น http 80 , SMTP 25 , POP 110 , IMAP 143 และอื่นอีกมาก ซึ่งปรกติจะต้องเปิดไว้คือ http 80 ซึ่งอาจทะลุผ่าน firewall ได้ถ้ามีการกำหนด firewall ได้ไม่ดี

## 5.6 การสนับสนุนการวัดระดับความปลอดภัย

- การสนับสนุนการวัดระดับความปลอดภัย (Implementing Security Measures) ด้วยวิธีการของการวัดระดับความปลอดภัยของข้อมูลในเครื่องคอมพิวเตอร์ที่เรียกว่า Orange Book ซึ่งเป็นมาตรฐานการรักษาความปลอดภัยที่กำหนดโดยกระทรวงกลาโหมสหรัฐอเมริกา และได้จัดแบ่งระดับความปลอดภัยออกเป็น 4 ระดับใหญ่ๆ ได้แก่ ระดับ D, C, B และ A เรียงลำดับ จากระดับความปลอดภัยที่น้อยที่สุดจนไปถึงระดับความปลอดภัยที่มากที่สุด



## 5.6 การสนับสนุนการวัดระดับความปลอดภัย

- **ระดับความปลอดภัย D**
- เป็นระดับที่มีความปลอดภัยต่ำที่สุด คือไม่มีการป้องกันรักษาความปลอดภัยโดยพื้นฐานเลย เช่น ไม่มีการกำหนดรหัสผ่านใดๆ สำหรับการเข้าสู่ระบบแก่เครื่องผู้ใช้ ระบบที่มีความปลอดภัยอยู่ในระดับ D จะมีการควบคุมการเข้าถึงไฟล์เพียงเล็กน้อยหรือไม่มีเลย ตัวอย่างระบบปฏิบัติการที่มีความปลอดภัยอยู่ในระดับ D ได้แก่ ระบบปฏิบัติการ MS-DOS เป็นต้น

# 5.6 การสนับสนุนการวัดระดับความปลอดภัย

- **ระดับความปลอดภัย C**
- ***ระดับความปลอดภัย C1*** บางครั้งจะเรียกว่า Discretionary Security Protection ระดับ C1 จะเป็นระดับความปลอดภัยที่ระบบคอมพิวเตอร์มีการรักษาความปลอดภัยในเบื้องต้น ได้แก่ การระบุชื่อผู้ใช้งาน และการใส่รหัสผ่านก่อนที่จะเข้าใช้งานระบบ รวมไปถึงการกำหนดสิทธิ์ในการเข้าใช้งานของผู้ใช้แต่ละคน แต่อย่างไรก็ตาม การรักษาความปลอดภัยในระดับนี้ยังไม่ได้แยกแยะและระบุหน้าที่ว่าใครเป็นผู้ดูแลระบบ หรือผู้ใช้งานทั่วไป คำว่า Discretionary จะหมายถึงการเข้าถึงที่ถูกกำหนดอยู่ในเกณฑ์ของ "need-to-know" ตัวอย่างของระบบปฏิบัติการที่มีความปลอดภัยระดับ C1 ได้แก่ ระบบปฏิบัติการ UNIX เป็นต้น
- ระดับความปลอดภัย C2 บางครั้งเรียกว่า Controlled Access Protection ซึ่งจะหมายถึงการบันทึกและเพิ่มการพิสูจน์ตัว ซึ่งจะเป็นส่วนที่เพิ่มขึ้นมาจากการรักษาความปลอดภัยระดับ C1 นั่นคือนอกจากจะมีการระบุชื่อและรหัสผ่านก่อนเข้าใช้ระบบแล้ว ยังสามารถที่จะแยกหน้าที่และอำนาจของผู้ใช้แต่ละคนออกจากกันด้วยและบันทึกการทำงานของผู้ใช้แต่ละคนเพื่อให้ผู้ดูแลระบบสามารถตรวจสอบได้ในภายหลัง



# 5.6 การสนับสนุนการวัดระดับความปลอดภัย

- **ระดับความปลอดภัย B**
- ***ระดับความปลอดภัย B1*** ความปลอดภัยในระดับนี้ เพิ่มส่วนที่ควบคุมการใช้งานที่เรียกว่า Label ขึ้น ซึ่งส่วนนี้จะกำหนดค่าความปลอดภัยให้กับข้อมูล และอุปกรณ์ต่างๆ เฉพาะในส่วนที่สำคัญๆ เท่านั้น ซึ่งผู้ที่ต้องการใช้ข้อมูล และอุปกรณ์ต้องมีสิทธิในการเรียกใช้ข้อมูลและอุปกรณ์ไม่น้อยไปกว่า Label
- ***ระดับความปลอดภัย B2*** มีการเพิ่มส่วนควบคุมจากระดับ B1 ซึ่งจะกำหนดให้ทุกๆ ข้อมูล และทุกอุปกรณ์ต้องมี Label กำกับการใช้งานไม่ใช่แต่เฉพาะอุปกรณ์สำคัญเท่านั้น
- ***ระดับความปลอดภัย B3*** เป็นระดับการรักษาความปลอดภัยที่สูงมาก จะมีส่วนที่เพิ่มจากระดับ B2 คือ มีการป้องกันการบุกรุกระบบ และป้องกันการขโมยข้อมูลไปใช้โดยเฉพาะ มีการรักษาความปลอดภัยในการเข้าใช้ระบบปฏิบัติการ และเครือข่ายอย่างเข้มงวด ตั้งแต่การออกแบบระบบ การใช้งาน และการตรวจสอบรวมทั้งการแก้ไขเมื่อระบบหยุดทำงาน ระบบปฏิบัติการในปัจจุบันยังไม่มีระบบไหนที่พัฒนาไปถึงระดับนี้ได้

# 5.6 การสนับสนุนการวัดระดับความปลอดภัย

- **ระดับความปลอดภัย A**
- เป็นระดับความปลอดภัยที่สูงที่สุด มีคุณสมบัติเหมือนกับระดับ B3 แต่แตกต่างกันเพียงจุดประสงค์ของการออกแบบ และการนำไปใช้งานจริงจะมีการตรวจสอบทุกขั้นตอนเพื่อให้มั่นใจว่าระดับความปลอดภัยระดับนี้จะมีผลในการนำไปใช้งานจริง



# 5.6 การสนับสนุนการวัดระดับความปลอดภัย

| | D | C | B | A |
|---|---|---|---|---|
| **Labels** | N | N | Y | Y |
| **Discretionary Access Control** | N | Y | Y | Y |
| **Mandatory Access Control** | N | N | Y | Y |
| **Identification** | N | Y | Y | Y |
| **Authentication** | N | Y | Y | Y |
| **Auditing** | N | N* | Y | Y |
| **Trusted Path** | N | N | Y | Y |

## 5.6 การสนับสนุนการวัดระดับความปลอดภัย

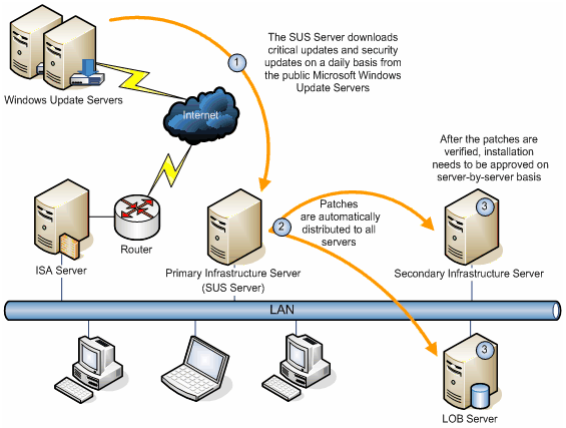
- การรักษาความปลอดภัยในระดับที่สูงขึ้น จะมีค่าใช้จ่ายในการดำเนินการและการดูแลรักษามากขึ้นตามลำดับ ปัจจัยสำหรับการตัดสินใจที่จะเลือกระดับการรักษาความปลอดภัยที่ต้องการมี 3 ประการ คือ ส่วนใดในระบบที่ต้องการป้องกัน อะไรจากระบบใดที่ต้องการการป้องกัน และเวลาที่ใช้และค่าใช้จ่ายที่จะเกิดขึ้นในการป้องกันระบบ



## 5.6 การประยุกต์แก้ไขและอัพเกรด

- การซ่อมแซมช่องโหว่ของระบบ (Patch Management) หมายถึง การบริหารจัดการติดตั้งระบบ patch ให้กับระบบคอมพิวเตอร์ในองค์กรอย่างเป็นระบบ เพื่อปิดช่องโหว่ (Vulnerabilities) ที่อาจถูกโจมตีด้วย Exploit หรือ Worm
- กระบวนการจัดการ patch จะประกอบด้วย 2 มุมมอง คือ ด้านเทคโนโลยี และด้านกระบวนการ
- มุมมองทางด้านเทคโนโลยีจะเน้นในเรื่องของการลดเวลาในการติดตั้ง patch ภายในองค์กร รวมไปถึงการลดแบนด์วิธ (bandwidth) ที่ใช้ในการปรับปรุง Patch
  - เทคโนโลยีเหล่านี้จะดำเนินการ download patch จากผู้ค้ารายต่างๆ มาเก็บไว้ที่เครื่องให้บริการหลักภายในองค์กร จากนั้นจึงทดสอบ patch และกระจาย patch ดังกล่าวไปยังเครื่องแม่ข่ายและลูกข่ายต่างๆ ทั่วทั้งองค์กรผ่านเครือข่ายภายในขององค์กร ซึ่งทำให้มีการใช้ Internet bandwidth ลดลง รวมไปถึงใช้เวลาในการติดตั้ง patch ต่างๆ ลดลงอีกด้วย

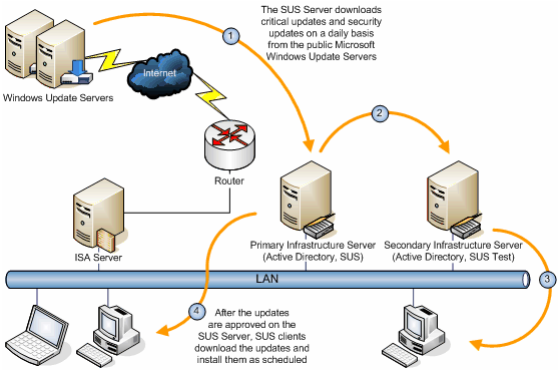
# 5.6 การประยุกต์แก้ไขและอัพเกรด




แสดงลักษณะการ Patch แบบ Server Patch Management



# 5.6 การประยุกต์แก้ไขและอัพเกรด




แสดงลักษณะการ Patch แบบ Client Patch Management

## 5.6 การประยุกต์แก้ไขและอัพเกรด

- มุมมองทางด้านกระบวนการนั้น จะเน้นกระบวนการในการทดสอบ patch เป็นหลัก โดยนำเครื่องลูกข่ายและแม่ข่าย (clients and servers) ของโปรแกรมหลักๆ มาทดสอบและติดตั้ง patch ก่อนการติดตั้ง patch จริงลงในเครื่องที่ใช้งานจริงทั้งเครื่องลูกข่ายและแม่ข่าย



## 5.6 การประยุกต์แก้ไขและอัพเกรด

- **หลักการทำงานของไฟล์ Patch**
- เมื่อทำการรันไฟล์ patch จะมีส่วนที่ทำการตรวจสอบรหัส (code) ของโปรแกรมที่ใช้อยู่กับรหัสในไฟล์ patch โดยขั้นตอนการเปรียบเทียบนั้นไม่ได้เปรียบเทียบที่ วัน เวลา ที่สร้างไฟล์ หรือขนาดของไฟล์เท่านั้น แต่จะเป็นการเปรียบเทียบแบบเป็นรูปแบบ (pattern) คือมองตั้งแต่การไม่ตรงแนวของ code การเว้นวรรค โดยโปรแกรมที่ทำการตรวจสอบนั้น เมื่อพบรูปแบบที่แตกต่างกัน โปรแกรมที่จัดการ patch นั้นจะทำการสำเนารหัสในส่วนที่ไฟล์ในเครื่องคอมพิวเตอร์ไม่มีลงมาให้

## Windows XP Service Pack 3 (SP3)

- **มีอะไรใหม่ใน Windows XP Service Pack 3 (SP3)**
  Patch ต่างๆใน SP3 ส่วนมากเป็นการแก้ไขข้อผิดพลาด แต่ก็ยังมีคุณสมบัติใหม่บางอย่างทางด้านความปลอดภัย การบริหารระบบ และเน็ตเวิร์ก ที่ไมโครซอฟท์ใส่เข้ามาเพื่อให้เครื่องที่ยังจำเป็นต้องใช้ XP ไม่อัพเกรดไปเป็น Vista สามารถทำงานได้อย่างราบรื่น ซึ่งสรุปคุณสมบัติใหม่เฉพาะที่สำคัญใน SP3 (รวมทั้ง Patch ที่ออกมาหลัง SP2 แต่ก่อนหน้า SP3)ได้ดังนี้



## Windows XP Service Pack 3 (SP3)

- **Patch ที่ออกมาหลัง SP2 แต่ก่อนหน้า SP3**
- ด้านการบริหารระบบ
  - **Microsoft Management Console (MMC) 3.0**
    เป็น โปรแกรมที่รวมเครื่องมือในการบริหารระบบของ Windows ไว้ที่เดียวกัน โดยสามารถสร้างเครื่องมือย่อยๆแต่ละอย่างมาติดตั้งเพิ่มให้ทำงานภายใต้ MMC ได้ (เรียกว่า Snap-in) โดย patch นี้เป็นการอัพเกรด MMC ให้เป็นเวอร์ชั่น 3.0

## Windows XP Service Pack 3 (SP3)

- ด้าน Network
  - **Background Intelligent Transfer Service (BITS) 2.5** เป็น โปรแกรมส่วนที่ใช้ในการรับส่งข้อมูล เช่นการดาวน์โหลดอัพเดทต่างๆจากไมโครซอฟท์ ซึ่งในเวอร์ชั่น 2.5 นี้มีการปรับปรุงเรื่องความปลอดภัยให้ดีขึ้น
  - **IPSec Simple Policy Update for Windows Server 2003 and Windows XP** ปรับ ปรุงการทำงานที่สนับสนุนโปรโตคอล IPSec (IP Security คือโปรโตคอลที่ทำการรับส่งข้อมูลแบบปลอดภัยผ่าน Internet Protocol หรือ IP อีกทีหนึ่ง)
  - **Digital Identity Management Service (DIMS)** ช่วยให้ผู้ใช้ที่ทำการ logon เข้ามาในคอมพิวเตอร์เครื่องใดก็ได้ที่ join กับโดเมนไว้สามารถเข้าใช้ใบรับรองดิจิตอล (certificate) และ private key (ที่ใช้ในการถอดรหัสข้อมูลที่เข้ารหัสมาด้วย public key ของผู้รับ) ได้โดยไม่มีการเตือนใดๆ



## Windows XP Service Pack 3 (SP3)

- ด้าน Network
  - **Peer Name Resolution Protocol (PNRP) 2.1** ทำให้โปรแกรมบน Windows XP สามารถใช้โปรโตคอล PNRP นี้ติดต่อกับโปรแกรมที่ใช้โปรโตคอลเดียวกันบนเครื่องที่รัน Windows Vista ได้
  - **Remote Desktop Protocol (RDP) 6.1** เป็น การปรับรุ่นของโปรโตคอล RDP ที่ใช้ติดต่อระหว่างเครื่องที่ทำหน้าที่เป็น Terminal Server กับ Terminal Client เช่นในกรณีของการใช้โปรแกรม Remote Desktop Connection ล็อกอินจากหน้าจอของเครื่องที่เราใช้อยู่เข้าไปใช้งานอีกเครื่องหนึ่งที่ต่อ กันผ่านเน็ตเวิร์กเสมือนไปนั่งอยู่หน้าเครื่องนั้น ซึ่งโปรโตคอล RDP นี้จะทำงานบน TCP อีกทีหนึ่ง การปรับรุ่นนี้จะทำให้การเชื่อมต่อแบบ remote นี้ระหว่างเครื่องที่ใช้ Windows XP กับ Vista ทำงานได้ดีขึ้น
  - **Wi-Fi Protected Access 2 (WPA2)** เป็น การปรับรุ่นของระบบความปลอดภัยสำหรับ Wireless LAN เพื่อป้องกันการเข้าใช้เครือข่ายโดยไม่ได้รับอนุญาต จากที่ Windows XP เคยมีแค่มาตรฐานเดิมคือ WEP (Wired Equivalent Privacy ซึ่งจัดว่าไม่ปลอดภัยที่จะใช้แล้วในปัจจุบัน เพราะเจาะได้ง่าย) และ WPA รุ่นแรก ก็เพิ่มมาตรฐานใหม่คือ WPA2 เพื่อให้เป็นไปตามมาตรฐานความปลอดภัยล่าสุดของ IEEE 801.11i

## Windows XP Service Pack 3 (SP3)

- **Patch เฉพาะที่เพิ่มมาใหม่ใน SP3**
- **ด้าน Network**
  - **ความสามารถในการตรวจจับ Router ที่ทำตัวเหมือนหลุมดำ** (Black Hole Router คือ router ที่ทิ้งข้อมูลบางส่วนที่ส่งผ่านไปเฉยๆ) และพยายามส่งข้อมูลอ้อมไปทางอื่นแทน
  - **Network Access Protection (NAP)** เพิ่ม ความสามารถให้เทียบเท่ากับ Windows Vista และ Windows Server 2008 ในการป้องกันไม่ให้เครื่องคอมพิวเตอร์ที่มีคุณสมบัติไม่ครบถ้วนเพียงพอ เข้ามาใช้ทรัพยากรในเน็ตเวิร์กได้ ซึ่งผู้ดูแลระบบสามารถตั้งเงื่อนไขในการตรวจสอบ รวมถึงการจำกัดระดับการอนุญาตให้ติดต่อกับเครื่องอื่นๆในกรณีที่เครื่องนั้น มีคุณสมบัติไม่ตรงตามเงื่อนไข



## Windows XP Service Pack 3 (SP3)

- **Patch เฉพาะที่เพิ่มมาใหม่ใน SP3**
- **ด้านความปลอดภัย (Security)**
  - **CredSSP Security Service Provider** เป็น มาตรฐานใหม่ในการติดต่อเพื่อโอนหน้าที่การตรวจสอบชื่อและข้อมูลผู้ใช้ (user credential) จากเครื่องที่ผู้ใช้นั้น logon เข้าใช้งาน ไปยังเครื่องเซิร์ฟเวอร์อื่นๆที่ต้องการได้
  - **มีคำอธิบาย Security Options ที่ละเอียดขึ้น**
  - **Microsoft Cryptographic Module** ปรับ ปรุงโปรแกรมส่วนที่ทำการเข้าและถอดรหัสให้สอดคล้องกับการเปลี่ยนมาตรฐานของ รัฐบาลสหรัฐ จาก FIPS (Federal Information Processing Standard) 140-1 เป็น 140-2 โดยสามารถทำ hashing แบบ SHA2 (SHA256, SAH384 และ SHA512) ในไฟล์ rsaenh.dll

## Windows XP Service Pack 3 (SP3)

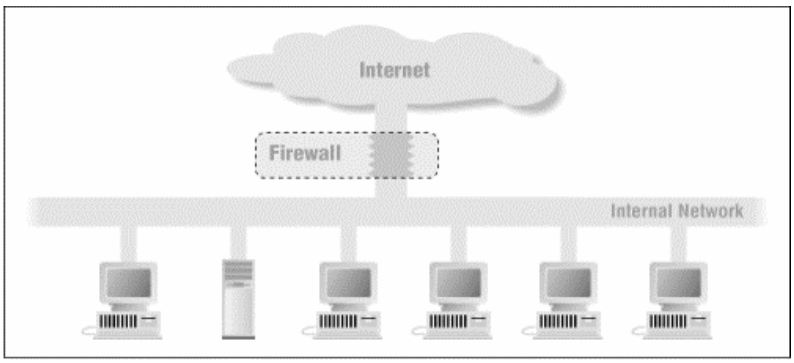
- **Patch เฉพาะที่เพิ่มมาใหม่ใน SP3**
- **ด้านการติดตั้ง (Setup)**
  - **Windows Product Activation** การ activate Windows เปลี่ยนมาใช้ขั้นตอนเหมือน Windows Server 2003 SP2 และ Windows Vista คือยอมให้ผู้ใช้สามารถติดตั้ง Windows XP ที่เป็น SP3 ในตัวอยู่แล้วในแบบ Full Install ไปจนเสร็จได้โดยไม่ต้องใส่ Product Key แล้วค่อยมาถามให้กรอก Product key ทีหลังตอนตรวจสอบลิขสิทธิ์ (ส่วนการติดตั้งหรืออัพเกรดโดยดาวน์โหลดผ่าน Windows Update นั้นไม่ต้องใช้ key อยู่แล้ว) แต่ทั้งนี้ไม่ได้เปลี่ยนวิธีในการ Activate แต่อย่างใด



## 5.7 ไฟร์วอลล์ (Firewall)

- ไฟร์วอลล์ (Firewall) เป็นระบบที่ทำหน้าที่ตรวจสอบการผ่านเข้าออกของข้อมูลระหว่างระบบเครือข่ายภายในและภายนอก เพื่อป้องกันการคุกคามระบบเครือข่ายภายในจากผู้บุกรุกภายนอก ขณะเดียวกันไฟร์วอลล์ยังสามารถควบคุมการใช้งานภายในเครือข่ายได้โดยการกำหนดสิทธิ์ของผู้ใช้แต่ละคนให้ผ่านเข้าออกได้อย่างปลอดภัย เมื่อมีการเชื่อมต่อกับระบบอินเทอร์เน็ต ดังนั้นไฟร์วอลล์จึงเป็นตัวช่วยป้องกันระบบเครือข่ายที่สำคัญที่ใช้ในการรักษาความปลอดภัยให้แก่ระบบเครือข่าย

# 5.7 ไฟร์วอลล์ (Firewall)






# 5.7 ไฟร์วอลล์ (Firewall)

- **คุณสมบัติทั่วไปของไฟร์วอลล์**
  - ไฟร์วอลล์เป็นเครื่องมือรักษาความปลอดภัยที่ทำหน้าที่ควบคุมการเข้าถึงระบบเครือข่าย โดยทำการตรวจสอบแพ็กเก็ตใดๆ ว่าสามารถผ่านเข้าออกไฟร์วอลล์ได้หรือไม่ โดยอาศัยกฎเกณฑ์เป็นพื้นฐานในการตรวจสอบ เนื่องจากไฟร์วอลล์เองไม่สามารถทราบได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ปลอดภัยหรือไม่ปลอดภัย ดังนั้นไฟร์วอลล์จะรู้จักเฉพาะแพ็กเก็ตที่ได้รับอนุญาตและไม่ได้รับอนุญาตตามกฎเกณฑ์ที่ระบุไว้เท่านั้น

# 5.7 ไฟร์วอลล์ (Firewall)

- **ประเภทของไฟร์วอลล์**
  - สามารถแบ่งประเภทของไฟร์วอลล์ได้ 2 แนวทาง คือ แบ่งตามเทคโนโลยี และแบ่งตามลักษณะเทคนิคของการทำงาน
- การจัดประเภทไฟร์วอลล์ตามเทคโนโลยีนั้น แบ่งออกเป็น 2 ประเภท ได้แก่
  - Hardware-based Firewall เป็นลักษณะของการใช้เราท์เตอร์ (Router) ทำหน้าที่เป็นไฟร์วอลล์เพื่อควบคุมการสื่อสารของระบบเครือข่าย
  - Software-based Firewall เป็นลักษณะของการใช้เครื่องคอมพิวเตอร์ที่มีซอฟต์แวร์ไฟร์วอลล์ในการป้องกันระบบเครือข่าย
- การจัดประเภทของไฟร์วอลล์ตามลักษณะเทคนิคของการทำงาน แบ่งออกเป็น 3 ประเภทหลัก
  - สกรีนนิ่งเราท์เตอร์ (Screening Router) หรือ แพ็กเก็ตฟิลเตอร์ (Packet Filters)
  - พร็อกซีเซิร์ฟเวอร์เกตเวย์ (Proxy Server Gateways)
  - เทคนิคสเตทฟูล อินสเปกชัน (Stateful Inspection)



# 5.7 ไฟร์วอลล์ (Firewall)

- ***สกรีนนิ่งเราท์เตอร์ (Screening Router)*** อุปกรณ์เราท์เตอร์จะเชื่อมต่อสองเครือข่ายเข้าด้วยกันและทำการกรอง (Filter) แต่ละแพ็กเก็ตเพื่อควบคุมทราฟฟิก (Traffic) ระหว่างเครือข่าย
  - ตรวจสอบข้อมูลที่ปรากฏอยู่ในแพ็กเก็ต(Packet) เทียบกับกฎเกณฑ์ (Rules) ที่กำหนดไว้และตัดสินใจว่าระบบควรจะโยนทิ้ง (drop) หรือว่าจะอนุญาต(allow) ให้แพ็กเก็ตนั้นผ่านไปได้
  - ข้อมูลภายในของแต่ละแพ็กเก็ตนั้นจะประกอบด้วยข้อมูลที่สำคัญสำหรับการตรวจสอบในระดับของเลเยอร์อินเทอร์เน็ต (Internet layer) และเลเยอร์ขนส่ง (Transport layer) ดังนี้
    - Source IP Address หมายถึง IP Address ต้นทางที่ส่งแพ็กเก็ต
    - Destination IP Address หมายถึง IP Address ปลายทางที่รับแพ็กเก็ต
    - Protocol ชนิดของโปรโตคอลที่อยู่ในแพ็กเก็ต
    - Source Port พอร์ตต้นทางสำหรับโปรโตคอลที่ใช้พอร์ต
    - Destination Port พอร์ตปลายทางที่แพ็กเก็ตต้องการติดต่อด้วยสำหรับโปรโตคอลที่ใช้พอร์ต
    - Options ข้อมูลสำคัญอื่นๆ ตามชนิดโปรโตคอล เช่น ICMP Message เป็นต้น

# 5.7 ไฟร์วอลล์ (Firewall)

- ซึ่งข้อมูลข้างต้นเหล่านี้จะถูกนำมาใช้เป็นเงื่อนไขควบคุมการผ่านเข้าออกของข้อมูลตามกฎเกณฑ์ที่ได้ระบุไว้ในไฟร์วอลล์ ที่เรียกว่า แอคเซสรูล (Access Rules) รูปแบบทั่วไปของแอคเซสรูลเบื้องต้นที่ใช้เปรียบเทียบกับข้อมูลทั้งหมดในแพ็กเก็ตทีละค่าจะประกอบด้วยรายการต่างๆ ดังนี้
  - Source Address
  - Destination Address
  - Protocol
  - Destination Port
  - Action
- โดยในฟิลด์สุดท้ายไฟร์วอลล์จะกำหนดผลลัพธ์เมื่อค่าในแพ็กเก็ตนั้นตรงตามเงื่อนไขในกฎเกณฑ์ที่ได้กำหนดไว้
- ดังนั้นสิ่งที่ไฟร์วอลล์จะกระทำคือ ถ้ามีกฎเกณฑ์ข้อใดไม่ได้ระบุไว้ว่าอนุญาต ให้ถือว่าไม่อนุญาต และถ้าไม่มีกฎเกณฑ์ข้อใดไม่ได้ระบุไว้ว่าไม่อนุญาต ให้ถือว่าอนุญาต

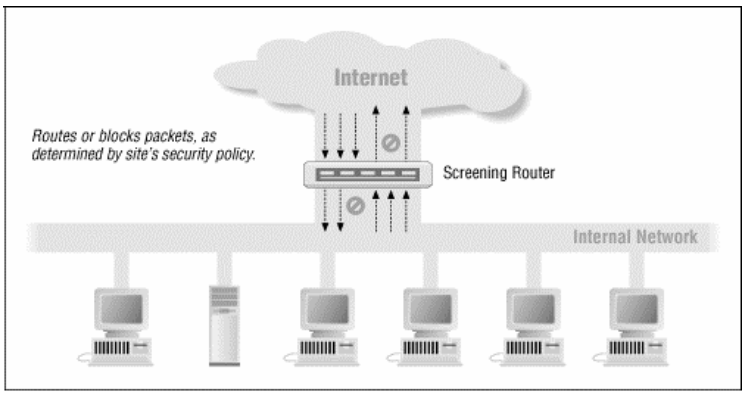


# 5.7 ไฟร์วอลล์ (Firewall)

- สกรีนนิ่งเราท์เตอร์อาจจะเป็นอุปกรณ์เราท์เตอร์เดี่ยวๆ หรือการนำเอาเครื่องคอมพิวเตอร์มาทำเป็นเราท์เตอร์เพื่อให้ทำหน้าที่เป็นแพ็กเก็ตฟิลเตอร์ริ่ง (Packet Filtering) โดยสามารถกำหนดกฎเกณฑ์ต่างๆ ให้ยืดหยุ่นได้และไม่จำกัด แต่ประสิทธิภาพการทำงานขึ้นอยู่กับระบบปฏิบัติการที่ใช้ ดังตารางเปรียบเทียบด้านล่างนี้

| อุปกรณ์ | ข้อดี | ข้อเสีย |
|---|---|---|
| เราท์เตอร์ | ประสิทธิภาพสูง มีจำนวนอินเตอร์เฟสมาก | เพิ่มเติมฟังก์ชันการทำงานได้ยาก อาจต้องการหน่วยความจำมาก |
| คอมพิวเตอร์ที่ทำหน้าที่เป็นเราท์เตอร์ | เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด | ประสิทธิภาพปานกลาง จำนวนอินเตอร์เฟสน้อยและอาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้ |

# 5.7 ไฟร์วอลล์ (Firewall)

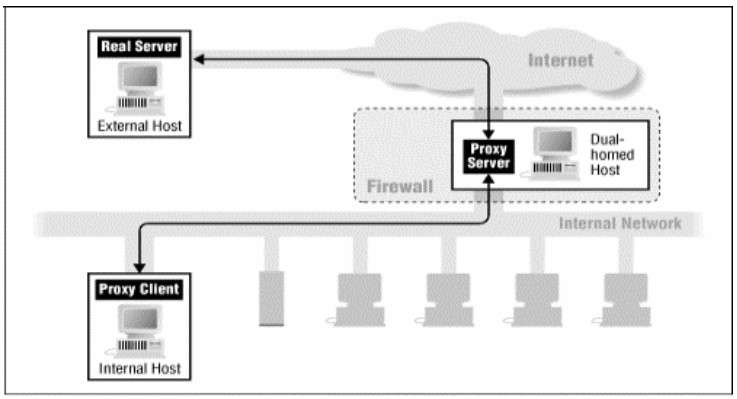





# 5.7 ไฟร์วอลล์ (Firewall)

- **พร็อกซีเซิร์ฟเวอร์เกตเวย์** จะทำงานในระดับที่สูงขึ้นไปในเน็ตเวิร์คโปรโตคอลสแต็ก(Network Protocol Stack) ซึ่งจะสูงกว่าสกรีนนิ่งเราท์เตอร์ ดังนั้นพร็อกซีจึงมีโอกาสสูงกว่าในการมอนิเตอร์ (monitor) และควบคุมการเข้าถึงระหว่างระบบเครือข่าย โดยพร็อกซีจะทำหน้าที่คอยส่งผ่านเมสเสจ (message) จากเครื่องไคลเอ็นต์ (client) ภายในไปยังบริการ (services) ต่างๆ ภายนอก ดังนั้นพร็อกซีจึงทำงานเปรียบเสมือนเป็นตัวกลางระหว่างเครื่องไคลเอ็นต์กับระบบอินเทอร์เน็ต พร็อกซีเซิร์ฟเวอร์ (proxy server) จะมี 2 ประเภทดังนี้

# 5.7 ไฟร์วอลล์ (Firewall)






# 5.7 ไฟร์วอลล์ (Firewall)

- ***เซอร์กิตเลเวลเกตเวย์ (Circuit-level gateways)***
- ทำงานที่ระดับเซสชันเลเยอร์ (Session Layer) ตาม ISO Model
- โดยจะให้การเชื่อมต่อระบบเครือข่ายที่ได้รับการควบคุมระหว่างระบบภายในและภายนอก วงจรเสมือน (virtual circuit) จะถูกสร้างขึ้นระหว่างเครื่องไคลเอนต์ภายในกับพร็อกซีเซิร์ฟเวอร์
- การร้องขอการบริการไปยังอินเทอร์เน็ตจะวิ่งผ่านวงจรนี้ไปยังพร็อกซีเซิร์ฟเวอร์ และพร็อกซีเซิร์ฟเวอร์จะทำการเปลี่ยนไอพีแอดเดรส (IP Address) แล้วจึงส่งการร้องขอบริการไปยังอินเทอร์เน็ต ดังนั้นผู้ใช้ภายนอกจะมองเห็นเฉพาะไอพีแอดเดรสของพร็อกซีเซิร์ฟเวอร์ การตอบสนอง (response) จะถูกส่งกลับมายังพร็อกซีเซิร์ฟเวอร์และถูกส่งต่อกลับไปยังเครื่องไคลเอนต์

# 5.7 ไฟร์วอลล์ (Firewall)

- ***แอปพลิเคชันเลเวลเกตเวย์ (Application-level gateways)***
- ทำหน้าที่ควบคุมการเดินทางของข้อมูลในระดับแอพพลิเคชันเลเยอร์ (application layer) ตาม ISO Model
- ทำหน้าที่เป็นตัวกลางและป้องกันการติดต่อสื่อสารโดยตรงระหว่างเครื่องเซิร์ฟเวอร์และเครื่องไคลเอ็นต์ เมื่อเครื่องไคลเอ็นต์ต้องการที่จะใช้บริการจากภายนอก เครื่องไคลเอ็นต์จะทำการติดต่อไปยังพร็อกซีก่อน เพื่อเจรจาให้พร็อกซีติดต่อไปยังเครื่องปลายทาง และเมื่อพร็อกซีติดต่อไปยังเครื่องปลายทางแล้วจึงจะมีการเชื่อมต่อเกิดขึ้น 2 การเชื่อมต่อ คือ เครื่องไคลเอ็นต์กับพร็อกซี และพร็อกซีกับเครื่องปลายทาง
- โดยที่พร็อกซีจะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้พร็อกซีจะทำหน้าที่ในการตัดสินใจด้วยว่า จะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่ แอปพลิเคชันเลเวลเกตเวย์ทั่วๆ ไปสามารถที่จะให้พร็อกซีเซอร์วิสสำหรับแอปพลิเคชันและโปรโตคอล เช่น Telnet, FTP (file transfer), HTTP (Web Services) และ SMTP (e-mail) เป็นต้น



# 5.7 ไฟร์วอลล์ (Firewall)

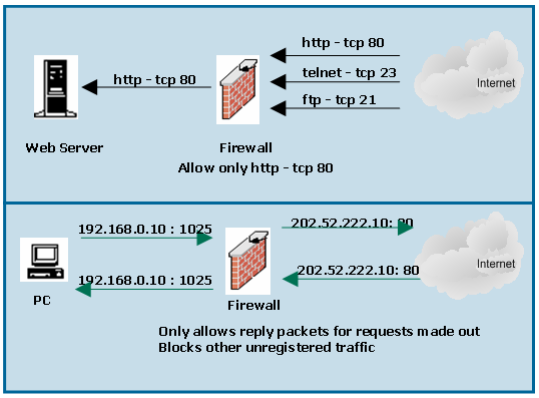
- ***สเตทฟูล อินสเปกชัน (Stateful Inspection)***
- เป็นขั้นตอนที่มีลักษณะการวิเคราะห์ความต่อเนื่องของแพ็กเก็ตในโปรโตคอลที่เพิ่มเข้าไปในแพ็กเก็ตฟิลเตอร์ริ่ง (Packet Filtering)
- เนื่องจากปกติแล้วแพ็กเก็ตฟิลเตอร์ริ่งแบบ Stateless ที่อยู่ในเราท์เตอร์ทั่วไป จะควบคุมการเข้าออกของแพ็กเก็ตโดยพิจารณาข้อมูลจากเฮดเดอร์ (Header) ของแต่ละแพ็กเก็ต แล้วนำมาเทียบกับกฎเกณฑ์ที่มีอยู่ซึ่งสร้างมาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์เท่านั้น

# 5.7 ไฟร์วอลล์ (Firewall)

- ***สเตทฟูล อินสเปกชัน (Stateful Inspection)***
- ดังนั้นในขั้นตอนของแพ็กเก็ตฟิลเตอร์ริ่งแบบธรรมดาจึงไม่สามารถทราบได้ว่าแพ็กเก็ตนี้อยู่ในส่วนใดของการเชื่อมต่อหรือเป็นแพ็กเก็ตที่เข้ามาติดต่อใหม่ หรือว่าเป็นแพ็กเก็ตที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น
- ดังนั้นขั้นตอนของสเตทฟูล อินสเปกชันจะนำเอารายละเอียดข้อมูลของ แพ็กเก็ต (message content) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว



# 5.7 ไฟร์วอลล์ (Firewall)



# 5.7 ไฟร์วอลล์ (Firewall)