บทที่ 7 : IDS/IPS Part1

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Outline

- อะไรคือ IDS/IPS ?
- ทำไมต้องมี IDS/IPS ?
- ขีดความสามารถ IDS
- ประเภทของ IDS
- การวิเคราะห์และการตรวจจับการบุกรุก
- การแจ้งเตือนภัยของ IDS

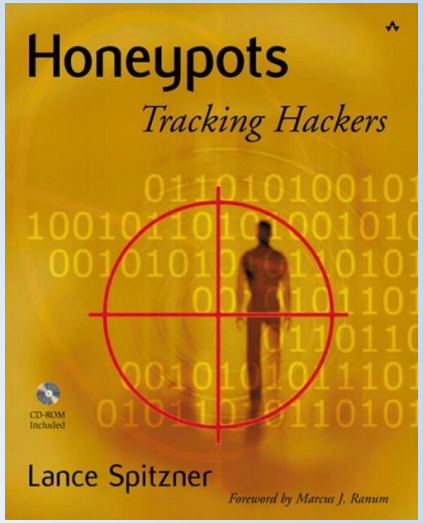
อะไรคือ IDS/IPS ?

- **IDS (Intrusion Detection System)** หมายถึงระบบตรวจจับการบุกรุก เป็นเครื่องมือรักษาความปลอดภัยที่ทุกองค์กรควรจะมีรองจากไฟร์วอลล์ ใช้ในการตรวจจับความพยายามในการบุกรุกเครือข่าย และเตือนภัยให้กับผู้ดูแลระบบได้รับทราบ
- ปกติแฮคเกอร์จะหลีกเลี่ยงการเจาะระบบที่มี IDS ติดตั้งอยู่

อะไรคือ IDS/IPS ? [2]

- ปัญหาใหญ่ของ IDS คือไม่สามารถป้องกันการบุกรุกได้แบบเรียลไทม์ในการโจมตีแบบ DDoS จึงมีการคิดค้นเทคโนโลยีใหม่ เรียกว่า **IPS (Intrusion Prevention System)**
- IPS ที่มีความฉลาดจะใช้เทคโนโลยีชั้นสูงในการวิเคราะห์ข้อมูล เช่น Neural Network, Fuzzy Logic ส่งผลให้การวิเคราะห์แม่นยำขึ้น

อะไรคือ IDS/IPS ? [3]



- อีกเครื่องมือหนึ่งที่มักใช้ร่วมกับ IDS/IPS คือ **Honeypot**
- Honeypot เป็นเป้าหมายลวง หมายถึงเครื่องเซิร์ฟเวอร์ที่เราปล่อยให้มีช่องโหว่เพื่อลวงให้แฮคเกอร์เข้ามาติดกับ
- ทำให้เรารู้วิธีการเจาะระบบของแฮคเกอร์อย่างละเอียด ตลอดจนสามารถสืบหาตัวแฮคเกอร์ได้ก่อนที่ระบบจริงจะถูกเจาะ

ทำไมต้องมี IDS/IPS ?

- เพื่อเป็นเครื่องมือในการสืบสวนหาบุคคลที่บุกรุกระบบ อาจนำไปสู่การจับกุมและลงโทษบุคคลเหล่านั้นได้
- เพื่อตรวจจับการโจมตีหรือการฝ่าฝืนคำสั่ง ที่ไม่สามารถป้องกันได้จากระบบรักษาความปลอดภัยอื่น
- เพื่อตรวจจับความพยายามที่จะบุกรุกเครือข่ายและป้องกันก่อนที่จะเกิดการโจมตีจริงๆ
- เพื่อเก็บรวบรวมสถิติเกี่ยวกับความพยายามหรือการโจมตีและนำไปวิเคราะห์ภัยคุกคามที่อาจเกิดขึ้นได้

ทำไมต้องมี IDS/IPS ? [2]

- เพื่อเป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันของระบบรักษาความปลอดภัยอื่น เช่น ไฟร์วอลล์ เป็นต้น
- เพื่อเป็นข้อมูลที่เป็นประโยชน์เมื่อมีการบุกรุกจริงๆ ซึ่งจะช่วยค้นหาส่วนที่ถูกโจมตี การกู้คืน และการแก้ไขผลเสีย รวมไปถึงการป้องกันในอนาคต

ขีดความสามารถของ IDS

IDS สามารถทำสิ่งต่อไปนี้ได้ดี

- มอนิเตอร์และวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบรวมถึงพฤติกรรมของผู้ใช้
- ทดสอบระดับความปลอดภัยของระบบ
- เรียนรู้ลำดับเหตุการณ์ของระบบที่แตกต่างจากเหตุการณ์ปกติหรือเกิดจากการโจมตีที่รู้ล่วงหน้า
- จัดการข้อมูล Event Log และ Audit Log ของระบบปฏิบัติการ
- รายงานข้อมูลเกี่ยวกับนโยบายการรักษาความปลอดภัยพื้นฐาน

ขีดความสามารถของ IDS [2]

IDS ไม่สามารถทำหน้าที่ต่อไปนี้ได้

- ไม่สามารถปิดช่องโหว่ของระบบที่ไม่ได้ป้องกันโดยระบบรักษาความปลอดภัยอื่น เช่นไฟร์วอลล์หรือแอนตี้ไวรัส
- ไม่สามารถตรวจจับ รายงาน และตอบโต้การโจมตีได้ในช่วงเวลาที่มีการใช้เครือข่ายหนาแน่นมากเกินไป
- ไม่สามารถตรวจจับการโจมตีแบบใหม่ หรือการโจมตีแบบเก่าแต่เปลี่ยนรูปแบบการโจมตี

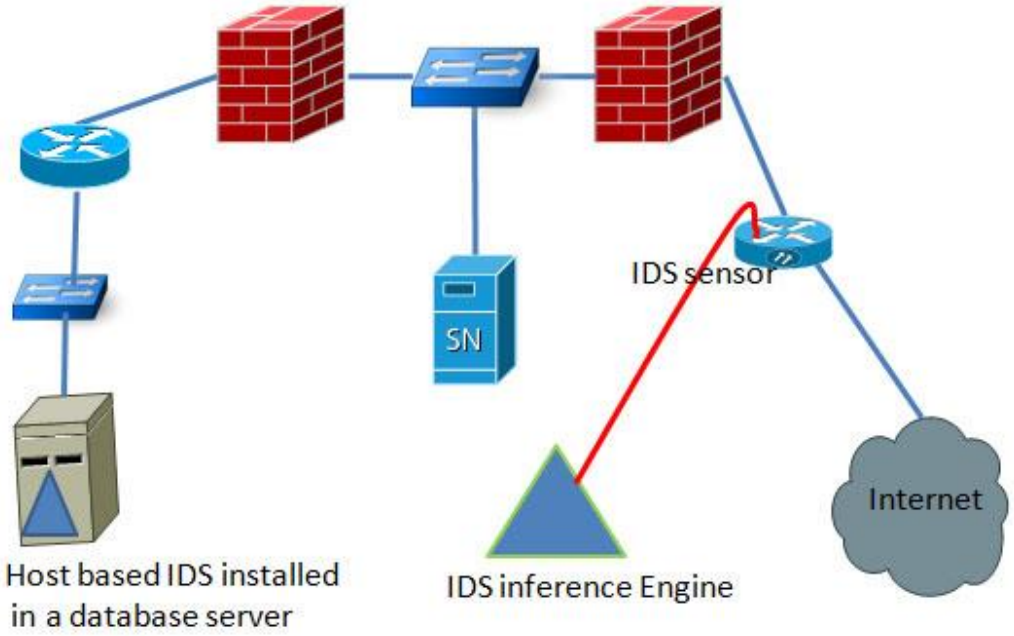
ขีดความสามารถของ IDS [3]

IDS ไม่สามารถทำหน้าที่ต่อไปนี้ได้ (ต่อ)

- ไม่สามารถตอบโต้การโจมตีได้อย่างมีประสิทธิภาพ หากผู้โจมตีมีความชำนาญสูง
- ไม่สามารถสืบหาผู้บุกรุกได้โดยอัตโนมัติ ต้องอาศัยคนในการช่วยวิเคราะห์
- ไม่สามารถขัดขวางไม่ให้เกิดการโจมตี IDS เอง
- ไม่สามารถป้องกันปัญหาเกี่ยวกับความถูกต้องของแหล่งข้อมูล
- ไม่สามารถทำงานได้ดีในระบบเครือข่ายที่ใช้สวิตช์

ประเภทของ IDS

- แบ่งเป็น 2 ประเภท คือ
  - Host-Based IDS
  - Network-Based IDS



Network based IDS analyzing all incoming traffic outside the Perimeter network

ประเภทของ IDS

: Host-Based IDS

- เป็นซอฟต์แวร์ที่รันบนโฮสต์
- ปกติจะวิเคราะห์ Log เพื่อค้นหาข้อมูลเกี่ยวกับการบุกรุก โดยจะอ่านเหตุการณ์ใหม่ที่เกิดขึ้นใน Log และเปรียบเทียบกับกฎที่ตั้งไว้ก่อนหน้า ถ้าตรงกับกฎก็จะแจ้งเตือนทันที
- มีการตรวจสอบ Checksum ของไฟล์เพื่อตรวจสอบความคงสภาพ

ประเภทของ IDS

: Host-Based IDS [2]

ข้อดี

- สามารถตรวจพบการบุกรุกกับโฮสต์นั้นๆได้เสมอ ถ้าระบบสามารถบันทึกเหตุการณ์ไว้ใน Log ได้
- สามารถบอกได้ว่าการบุกรุกครั้งนั้นสำเร็จหรือไม่ โดยวิเคราะห์จากข้อความใน Log หรือการแก้ไขไฟล์สำคัญ
- สามารถระบุได้ว่ามีการเข้าใช้งานอย่างผิดปกติโดยผู้ใช้ระบบเอง

ประเภทของ IDS

: Host-Based IDS [3]

ข้อเสีย

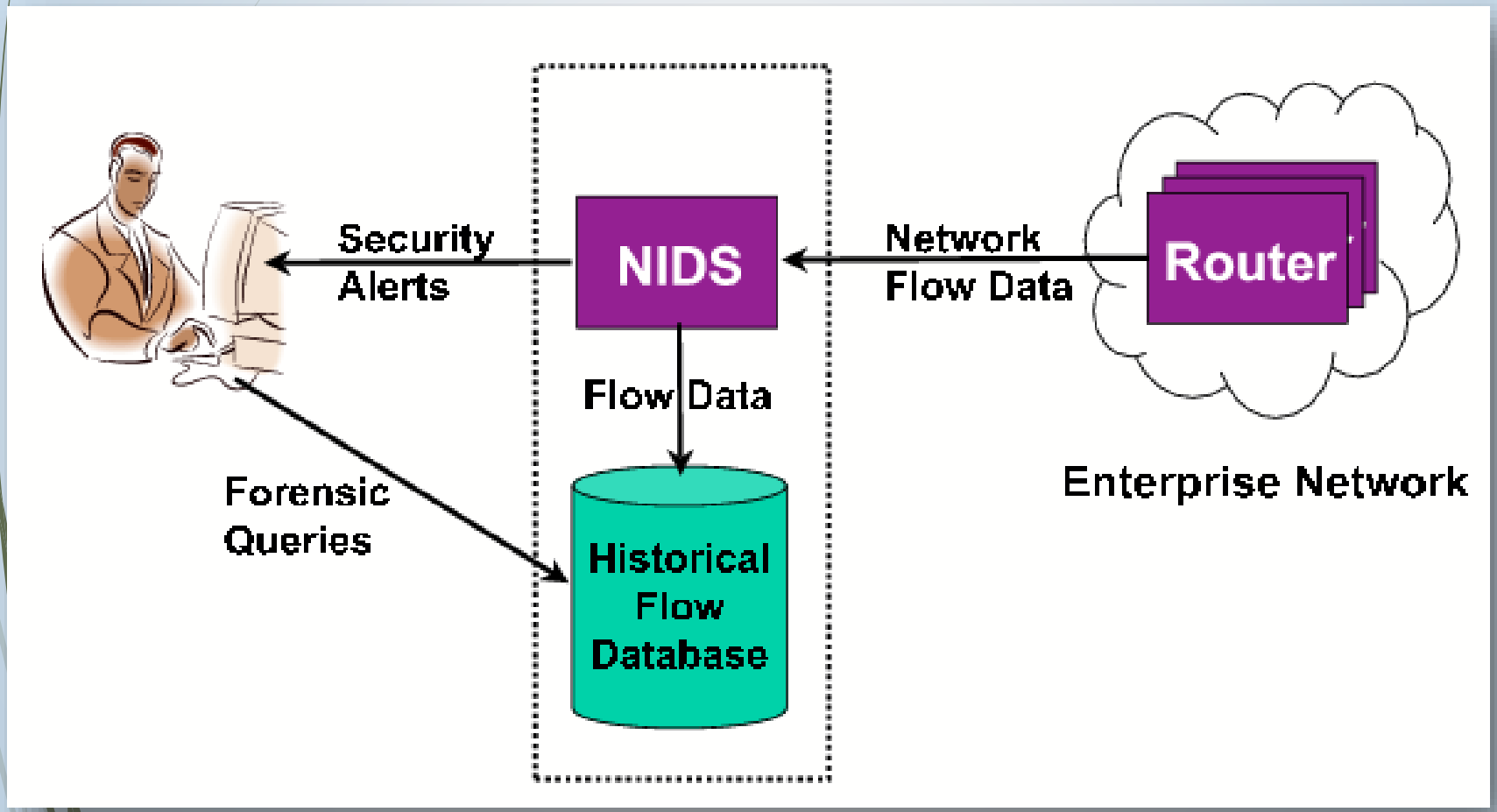
- โปรเซสของ IDS อาจถูกโจมตีเองจนไม่สามารถแจ้งเตือนได้
- โฮสต์เบสไอดีเอสจะแจ้งเตือนก็ต่อเมื่อเกิดเหตุการณ์ตรงกับที่กำหนดไว้ก่อนหน้า จึงไม่สามารถแจ้งเตือนการบุกรุกด้วยเทคนิคใหม่ๆได้
- การทำงานของไอดีเอสจะมีผลกระทบต่อประสิทธิภาพของโฮสต์ เนื่องจากต้องตรวจสอบ Log File อยู่เสมอ

ประเภทของ IDS

: Network-Based IDS

- เป็นซอฟต์แวร์พิเศษที่รันบนคอมพิวเตอร์เครื่องหนึ่งต่างหาก
- มีเน็ตเวิร์คการ์ดที่รับทุกๆแพ็คเก็ตที่วิ่งอยู่บนเครือข่าย แล้ววิเคราะห์ข้อมูลในแพ็คเก็ตเหล่านั้นกับข้อมูลที่เป็นรูปแบบการบุกรุกที่เก็บไว้ในฐานข้อมูลก่อนหน้า ถ้าตรงกับรูปแบบดังกล่าว IDS จะแจ้งเตือนทันที

แผนผังการทำงานของ Network-based IDS



ประเภทของ IDS

: Network-Based IDS [2]

- ส่วนใหญ่ IDS ประเภทนี้จะมีเน็ตเวิร์คการ์ด 2 ตัว ทำหน้าที่
  - ตัวแรกใช้เชื่อมต่อเข้ากับเครือข่ายที่ต้องเฝ้าระวัง โดยการ์ดนี้จะไม่มีหมายเลขไอพี เพื่อป้องกันเครื่องอื่นมองเห็น
  - ตัวที่สองจะเชื่อมต่อเข้ากับอีกเครือข่ายหนึ่ง เพื่อใช้แจ้งเตือนไปยังเซิร์ฟเวอร์
- สาเหตุที่ต้องทำเช่นนี้ก็เพื่อการป้องกัน IDS ถูกโจมตีเสียเอง

ประเภทของ IDS

: Network-Based IDS [3]

ข้อดี

- NIDS จะถูกซ่อนในเครือข่าย ทำให้ผู้บุกรุกไม่รู้ว่ากำลังถูกเฝ้ามอง
- NIDS หนึ่งเครื่องสามารถใช้เฝ้าระวังการบุกรุกได้หลายระดับและหลายโฮสต์
- สามารถตรวจจับทุกๆแพ็คเก็ตที่วิ่งไปยังระบบที่เฝ้าระวังอยู่

ประเภทของ IDS

: Network-Based IDS [4]

ข้อเสีย

- จะแจ้งเตือนก็ต่อเมื่อตรวจพบแพ็คเก็ตที่ตรงกับฐานข้อมูลที่กำหนดไว้ก่อนหน้าเท่านั้น
- ไม่สามารถตรวจจับแพ็คเก็ตได้ทั้งหมด เมื่อมีการใช้เครือข่ายหนาแน่น
- ไม่สามารถระบุได้ว่าการบุกรุกนั้นสำเร็จหรือไม่
- ไม่สามารถวิเคราะห์แพ็คเก็ตที่เข้ารหัสไว้ได้

ประเภทของ IDS

: การเลือกใช้ HIDS และ NIDS

- NIDS สามารถใช้เฝ้าระวังได้ครอบคลุมเครือข่ายมากกว่า จึงเป็นทางเลือกที่ประหยัดกว่า
- HIDS เหมาะสำหรับการเฝ้าระวังที่อาจเกิดจากผู้ใช้งานในเครือข่ายเอง
- ดังนั้นการเลือก IDS ให้เหมาะสมจึงขึ้นอยู่กับภัยที่คุกคามเครือข่ายขององค์กร

การวิเคราะห์และการตรวจจับการบุกรุก

- IDS จะใช้ 2 วิธีหลักในการวิเคราะห์เพื่อตรวจจับการพยายามบุกรุก คือ
  - การตรวจจับการใช้งานในทางที่ผิด (Misuse Detection)
  - การตรวจจับเหตุการณ์ผิดปกติ (Anomaly Detection)

การวิเคราะห์และการตรวจจับการบุกรุก : Misuse Detection

- คือการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบ เพื่อค้นหาเหตุการณ์ที่กำหนดไว้ว่าเป็นการโจมตี
- ข้อมูลที่เป็นเหตุการณ์ที่เป็นการโจมตี เรียกว่า “Signature”
- การตรวจจับการบุกรุกด้วยวิธีนี้จึงเรียกว่า **“Signature-based Detection”**

การวิเคราะห์และการตรวจจับการบุกรุก

: Anomaly Detection

- แนวคิดการตรวจจับแบบนี้ตั้งอยู่บนสมมติฐานที่ว่า *“การโจมตีคือการกระทำที่ถือว่าเป็นการทำงานผิดปกติ”*
- เทคนิคการตรวจจับในเชิงพาณิชย์ คือ
  - **Threshold Detection** คือการนับจำนวนครั้งของบางเหตุการณ์เพื่อเปรียบเทียบกับจำนวนครั้งที่อยู่ในเกณฑ์ปกติ
  - **Statistical Measure** การวัดค่าความกระจายของคุณสมบัติของโพรไฟล์ โดยเทียบกับค่าคงที่หรือค่าที่วัดได้ในอดีต
- ข้อดีของวิธีการวิเคราะห์แบบนี้คือสามารถตรวจจับการบุกรุกโดยใช้เทคนิคใหม่ๆได้

การแจ้งเตือนภัยของ IDS

- หลายองค์กรติดตั้ง IDS เพื่อเป็นเครื่องมือเสริมประสิทธิภาพให้กับระบบการรักษาความปลอดภัย
- เทคนิคการแจ้งเตือนของ IDS แต่ละผลิตภัณฑ์ จะมีพื้นฐานคล้ายๆกัน หากผู้ใช้เข้าใจหลักการรายงานพื้นฐานจะสามารถเรียนรู้การใช้ IDS ได้อย่างรวดเร็ว

การแจ้งเตือนภัยของ IDS

: การโจมตีที่มักจะถูกรายงานโดย IDS

- Scanning Attack (การโจมตีโดยการสแกนระบบ)
- Denial of Service Attack (การโจมตีแบบปฏิเสธการให้บริการ)
- Penetration Attack (การโจมตีแบบเจาะเข้าระบบ)
- Remote vs Local Attack (การโจมตีจากภายนอกและภายใน)

การแจ้งเตือนภัยของ IDS

: การโจมตีที่มักจะถูกรายงานโดย IDS [2]

- **Scanning Attack** หรือการสแกนระบบ หมายถึงการทดสอบว่าระบบว่าใช้งานอะไรได้บ้างก่อนที่จะลงมือโจมตีจริงๆ
- ทำได้โดยการส่งแพ็คเก็ตต่างๆไปยังระบบ และดูข้อมูลที่ได้จากการตอบกลับ
- ในการแจ้งเตือน IDS จะต้องแยกแยะให้ได้ว่าการสแกนนั้นเป็นการสแกนเพื่อประสงค์ร้าย หรือเป็นการสแกนปกติ เช่น Search Engine Scan เป็นต้น

การแจ้งเตือนภัยของ IDS

: การโจมตีที่มักจะถูกรายงานโดย IDS [3]

- **Denial of Service Attack** หรือการโจมตีแบบปฏิเสธการให้บริการ เป็นความพยายามที่จะทำให้ระบบเป้าหมายทำงานช้าลงหรือให้บริการไม่ได้เลย
- มี 2 ประเภท คือ
  - **การโจมตีช่องโหว่** (Flaw Exploitation) เป็นการโจมตีช่องโหว่ของระบบเพื่อให้เกิดข้อผิดพลาด หรือทำให้ทรัพยากรถูกใช้งานจนหมด
  - **การฟลัดดิง** (Flooding) เป็นการส่งข้อมูลไปยังระบบจนเกินกว่าที่ระบบจะรับไหว

การแจ้งเตือนภัยของ IDS

: การโจมตีที่มักจะถูกรายงานโดย IDS [4]

- Penetration Attack เป็นการเข้ามาในระบบโดยที่ไม่ได้รับอนุญาต และเปลี่ยนแปลงสิทธิ์ หรือข้อมูลที่อยู่ในระบบ
- ผู้บุกรุกจะอาศัยการเจาะช่องโหว่ของซอฟต์แวร์เพื่อเข้ามาทำลายระบบ

การแจ้งเตือนภัยของ IDS

: การโจมตีที่มักจะถูกรายงานโดย IDS [5]

- **Remote vs Local Attack** เป็นแหล่งที่มาของการโจมตีแบบ DoS และการเจาะระบบ
- **การโจมตีจากภายใน** จะเป็นการเปลี่ยนสิทธิ์ในการเข้าใช้ระบบให้มากขึ้น
- **การโจมตีจากภายนอก** จะเริ่มต้นโจมตีจากเครื่องรีโมทโดยช่องทางที่ระบบเปิดไว้ให้ หรือเป็นช่องโหว่ของระบบเอง
- รูปแบบการโจมตีที่เกิดขึ้นบ่อยคือผู้บุกรุกภายนอกจะเจาะระบบเพื่อให้สามารถเข้าใช้ระบบได้ แล้วเปลี่ยนสิทธิ์ของตนเองให้เป็นผู้ใช้ระบบ