TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM
Khoa Mạng máy tính & Truyền thông

Giới thiệu môn học

NT204 – Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

GV: Đỗ Hoàng Hiển

hiendh@uit.edu.vn

Nội dung

Tổng quan về IDS/IPS

Hôm nay học gì?

1. Giới thiệu môn học
2. Giới thiệu về IDS/IPS

Thông tin môn học

Giới thiệu môn học

Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

Intrusion Detection and Prevention System (IDS/IPS - IDPS)

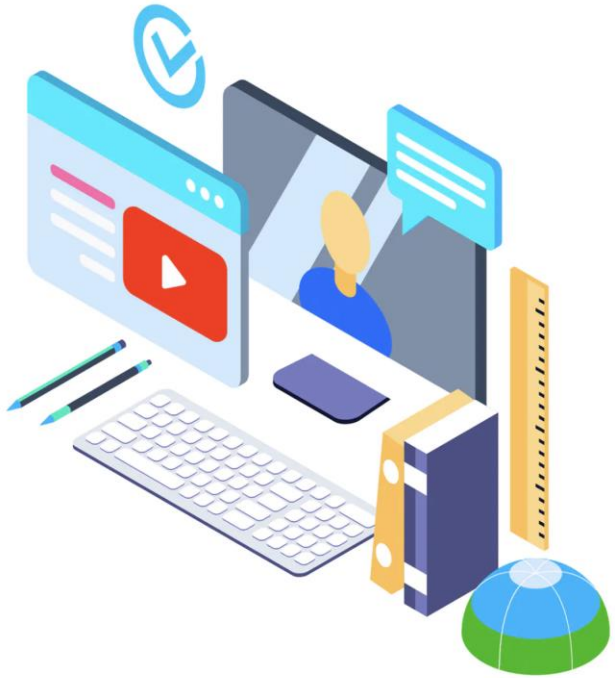
- **Môn tiên quyết**: NT101 - An toàn mạng máy tính. SV cần các kiến thức nền tảng:
  - Nguyên tắc hoạt động cơ bản của mạng máy tính (IT005).
  - Cơ bản về các tấn công mạng và phương pháp phòng thủ (NT101)
  - Kỹ năng nghiên cứu cơ bản (đọc hiểu, phân tích, hiện thực)

  ** Kinh nghiệm sử dụng Machine Learning / Deep Learning*

Quản lý khoá học

Giới thiệu môn học

- Website môn học: https://courses.uit.edu.vn/
  - Thông báo
  - Thông tin khoá học, các policy
  - Bài giảng, tài liệu tham khảo
  - Bài tập/ Assignments/ Labs



Mục tiêu môn học

Giới thiệu môn học

Sau khi kết thúc môn học, Sinh viên có thể:

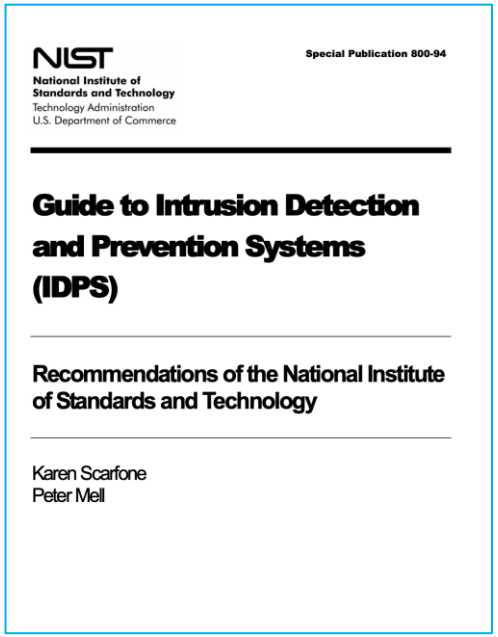
- Hiểu được cơ bản các vấn đề, khái niệm, phân loại, nguyên tắc hoạt động và các kỹ thuật trong các hệ thống IDPS.
- Hiểu được lúc nào, ở đâu, bằng cách nào và lý do khi áp dụng các công cụ IDPS và các kỹ thuật liên quan để đảm bảo an toàn mạng.
- Tiếp cận các hướng mới cho IDPS (học máy/học sâu) và cách áp dụng các công nghệ bảo mật mới vào kiến trúc mạng hiện có.
- Có thể triển khai, đánh giá, tuỳ chỉnh một IDPS cho những yêu cầu bảo mật cụ thể.

Hint: Nhiều assignment, bài tập vận dụng, bài tập nghiên cứu có thể dùng để đánh giá các **mục tiêu môn học** này!

Giáo trình, tài liệu

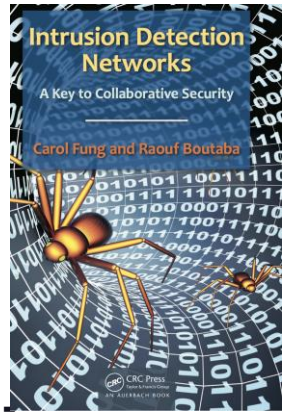
Giới thiệu môn học

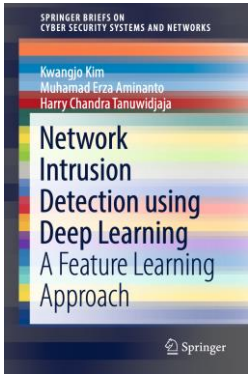
- **Giáo trình**:
  - **Không có giáo trình!**
  - **Nội dung môn học dựa trên một số bài báo khoa học gần đây trong nhiều hội nghị hoặc tạp chí chuyên ngành; các hướng dẫn và tài liệu của các công cụ IDPS**



Tài liệu tham khảo thêm:

- Karen Scarfone and Peter Mell, **Guide to Intrusion Detection and Prevention Systems (IDPS),** *Recommendations of the National Institute of Standards and Technology, 2007*
- Carol Fung and Raouf Boutaba, **Intrusion Detection Networks – A Key to Collaborative Security,** CRC Press, 2013
- *Một số bài báo khoa học liên quan (sẽ được cung cấp tương ứng trong các buổi học)*





Nội dung từng tuần (dự kiến)

Giới thiệu môn học

Tuần 1: **Giới thiệu môn học**

Tuần 2: **Ôn tập về tấn công mạng, tổng quan IDPS**

Tuần 3 - 4: **Network-based IDPS**

Tuần 5: **Host-based IDPS**

Tuần 6: **Security Monitoring, Log analysis, SIEM/SOC**

Tuần 7**:** *Báo cáo đồ án (Giữa kỳ)*

Tuần 8**: Đánh giá và đánh lừa IDPS**

Tuần 9 – 10: **Học máy cho IDS**

Tuần 11: **Bảo mật cho Học máy**

Tuần 12 – 15: **Báo cáo đồ án (cuối kỳ)**

Đánh giá

Giới thiệu môn học

30% quá trình/đồ án + **20%** thực hành + **50%** cuối kỳ

- **Quá trình**
  - Quiz, câu hỏi trên lớp, các bài tập nghiên cứu tài liệu
  - Bài tập assignment
  - Dự kiến giao bài tập mỗi 1-3 tuần
- **Không thi giữa kỳ!**
- **Đồ án**
  - Thực hiện theo nhóm, **3-4 sinh viên/nhóm**
  - Danh sách topics và đăng ký đồ án: thông báo sau
- **Cuối kỳ**

Yêu cầu

Giới thiệu môn học

- **Quy định trong lớp:**
  - Đến lớp đúng giờ. Có thể ghi nhận điểm *(cộng điểm điểm danh hoặc cộng điểm các bài tập/quiz trên lớp)*
  - Không làm việc riêng trong giờ học (ăn uống, sử dụng điện thoại hoặc laptop vào để làm các việc không liên quan đến nội dung buổi học).
- **Trong bối cảnh dịch bệnh:**
  - Khi học offline:
    - Đeo khẩu trang, chú ý giữ khoảng cách, rửa tay thường xuyên.
    - Giữa khoảng cách an toàn với những người có biểu hiện ho hoặc hắt hơi.
    - Ở nhà nếu cảm thấy không khoẻ *(nhớ gửi email cho GV trước).*
  - Học online nếu điều kiện không cho phép.

Một số điểm cần lưu ý

Giới thiệu môn học

- **Luôn trung thực, cố gắng**
  - Trung thực trong quá trình học – *đừng dễ bị cám dỗ*
  - Các bài nộp cần đảm bảo là **100% công sức** của chính mình, cần **trích dẫn rõ ràng** các nguồn tài liệu đã tham khảo
  - *Hãy nộp bài làm mà mình cảm thấy hài lòng* – đừng làm ẩu hay lười biếng!
  - **Không "thử nghiệm" với các hệ thống trái phép**
- **Tìm tòi và thực nghiệm**
  - Các hoạt động thực nghiệm cần sử dụng containers hoặc máy ảo
  - **Nhắc lại:** Chỉ thực nghiệm trên các hệ thống được cho phép

Không chia sẻ các tài liệu học *(slides, assignments, labs,…)* **ra ngoài lớp học mà không có sự cho phép của GV!**

Chỉ lưu hành nội bộ

Liên hệ Giảng viên

Giới thiệu môn học

- **Best way!!** Gửi email đến **hiendh@uit.edu.vn**
  - Nhớ thêm mã lớp **"NT204.XXX.YYYY"** trên tiêu đề email.
- Gặp trực tiếp: Phòng E8.1, UIT (Phòng thí nghiệm An toàn thông tin)
  - Nhớ gửi email trước khi gặp trực tiếp

Câu hỏi/thắc mắc nếu có?

Giới thiệu môn học

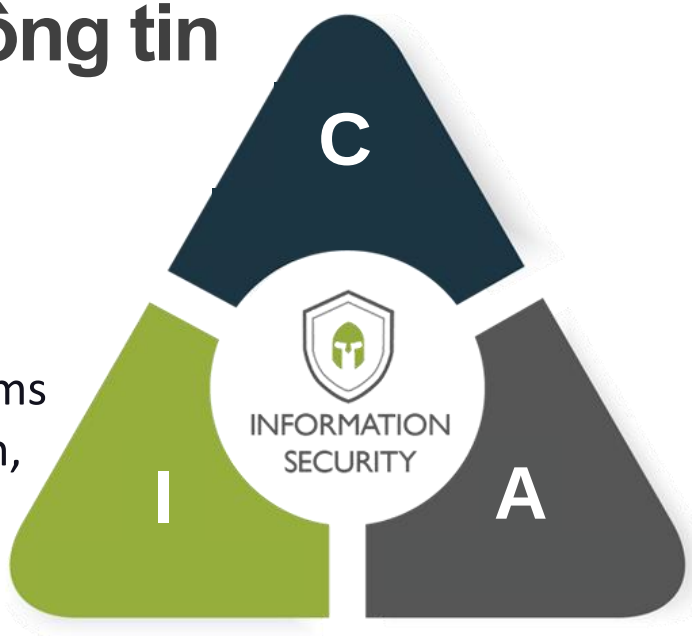
IDS/IPS

Giới thiệu

NT204 – IDS/IPS

Nhắc lại cơ bản về An toàn thông tin

An toàn thông tin là gì?



Định nghĩa **An toàn thông tin (Information Security)** (NIST):

> "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **confidentiality, integrity,** and **availability**."

Bộ ba CIA?

3 "mục tiêu lớn" của an toàn thông tin:

- **Confidentiality (bảo mật)**: tránh để lộ thông tin trái phép
- **Integrity (toàn vẹn)**: tránh để thông tin bị thay đổi trái phép

Mục tiêu về thông tin → kiểm soát dựa trên thông tin

- **Availability (sẵn sàng)**: đảm bảo những người dùng hợp lệ luôn có thể truy cập đến thông tin và hệ thống

mục tiêu về hệ thống – không thể chỉ xem xét thông tin

[1] https://csrc.nist.gov/glossary/term/information-security

Intrusions là gì? Xâm nhập là gì?

Khái niệm

"**Intrusion** is the act of thrusting in, or of entering into a place or state without invitation, right, or welcome"

NIST[1] định nghĩa:

- ***"intrusion" - xâm nhập*** là một hành vi cố gắng xâm phạm CIA, hoặc qua mặt cơ chế bảo mật của một máy tính hoặc mạng máy tính.
- Có thể có nhiều nguyên nhân:
  - malware (ví dụ, worms, spyware),
  - kẻ tấn công truy cập trái phép vào hệ thống qua mạng Internet,
  - người dùng hợp lệ của hệ thống lợi dụng quyền hạn hoặc cố chiếm thêm quyền không được phép

[1] https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps?pub_id=50951

Các tấn công mạng – intrusion phổ biến

Ôn lại một số tấn công…

Ví dụ một số tấn công mạng

- Truy cập trái phép vào tài nguyên nào đó
  - Tiết lộ, thay đổi hoặc phá huỷ tài nguyên
- Distributed Denial of Service (DDoS) Attacks (ví dụ: Mirai botnet)
- Malware (Virus, worms, trojan, ransomware, spyware) (Ví dụ: WannaCry)
- Theo dõi và bắt lưu lượng mạng
  - User IDs, passwords, và các thông tin khác có thể bị đánh cắp qua Internet
- Khai thác các lỗ hổng phần mềm (ví dụ: buffer overflow)
- Giả dạng người dùng hợp lệ hoặc hệ thống đầu cuối
- Tấn công Web (SQLi, XSS, CSRF,…)
- DNS Attack

Dấu hiệu chung của intrusion – xâm nhập

Tổng quan

- Log ngắn và không đầy đủ
- Hiệu suất hệ thống thấp bất thường
- Các tiến trình bất thường
- Hệ thống bị crash hoặc reboot
- Hiển thị hình ảnh hoặc đoạn tin nhắn bất thường
- …

Xâm nhập hệ thống	Xâm nhập mạng
▪ Xuất hiện **các file** hoặc **chương trình lạ** ▪ Các **quyền truy cập** file bị thay đổi ▪ Kích thước file bị **thay đổi bất thường** ▪ Những **tên file lạ** trong các **thư mục** ▪ **Thiếu** file	▪ **Thăm dò** liên tục các service trên các máy tính ▪ Kết nối từ các **vị trí bất thường** ▪ Cố gắng **đăng nhập liên tục** từ host ở xa ▪ **Dữ liệu bất thường** trong các file log, dấu hiệu của DoS hoặc hướng tới crash dịch vụ

Nguồn: CEHv9

Intrusion Detection and Prevention

Khái niệm

- ***"intrusion detection" – phát hiện xâm nhập*** là quy trình **theo dõi** các sự kiện diễn ra trong một hệ thống máy tính hoặc mạng máy tính và **phân tích** để nhận biết các dấu hiệu của sự bất thường (hành vi xâm nhập - intrusion).
- ***"Intrusion Detection System" (IDS) – hệ thống phát hiện xâm nhập*** là hệ thống phần mềm hoặc phần cứng **tự động** thực hiện quy trình phát hiện xâm nhập.
- ***"Intrusion Prevention System" (IPS) – hệ thống ngăn chặn xâm nhập*** là hệ thống **có tất cả chức năng của IDS**, **và** có thể **dừng** sự xâm nhập.

Intrusion detection and prevention systems (IDPS) = *IDS + IPS*

[1] https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps?pub_id=50951

Sử dụng IDPS

Tổng quan

- **IDPS** thường tập trung **xác định các sự cố có thể xảy ra** và **hỗ trợ ứng phó với sự cố**

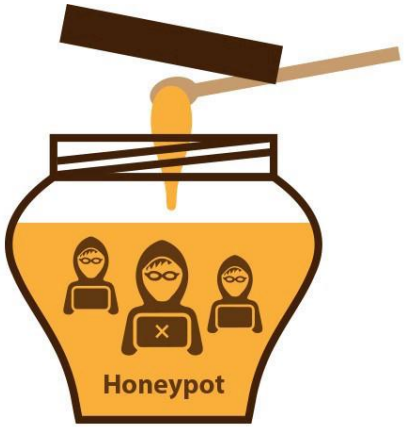
  *Ví dụ: phát hiện khi có attacker đã chiếm thành công một hệ thống bằng cách **khai thác một lỗ hổng** trên hệ thống đó*

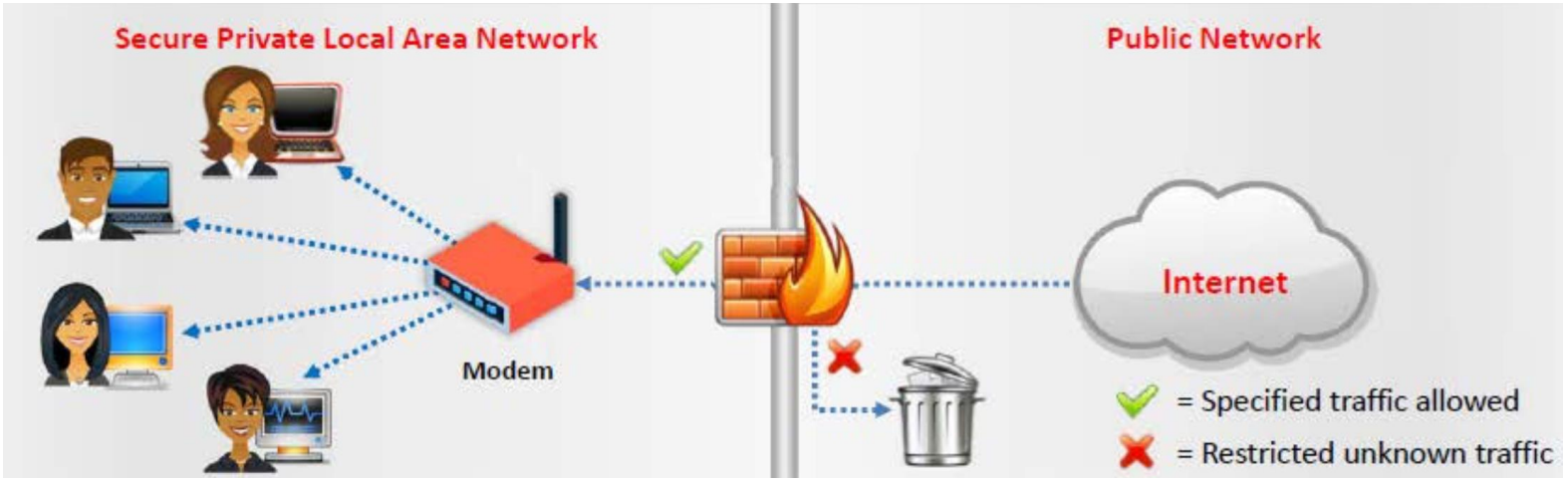
  - **Ghi log** các thông tin có thể được attacker sử dụng
  - **Nhận biết** các hành vi vi phạm chính sách bảo mật
  - **Theo dõi** việc truyền file và xác định các file đáng ngờ
- **Xác định, chặn các hoạt động do thám,** vốn có thể là dấu hiệu sắp có tấn công (cảnh báo sớm) và thông báo cho quản trị viên
- **Xác định các vấn đề trong chính sách bảo mật**
- **Tài liệu hoá các mối đe doạ hiện có đối với 1 tổ chức**
- **Răn đe các cá nhân vi phạm chính sách bảo mật**

Các cơ chế bảo mật Internet đã có

Tổng quan

- Firewall – Tường lửa
- Honeypot
- Phần mềm Antivirus

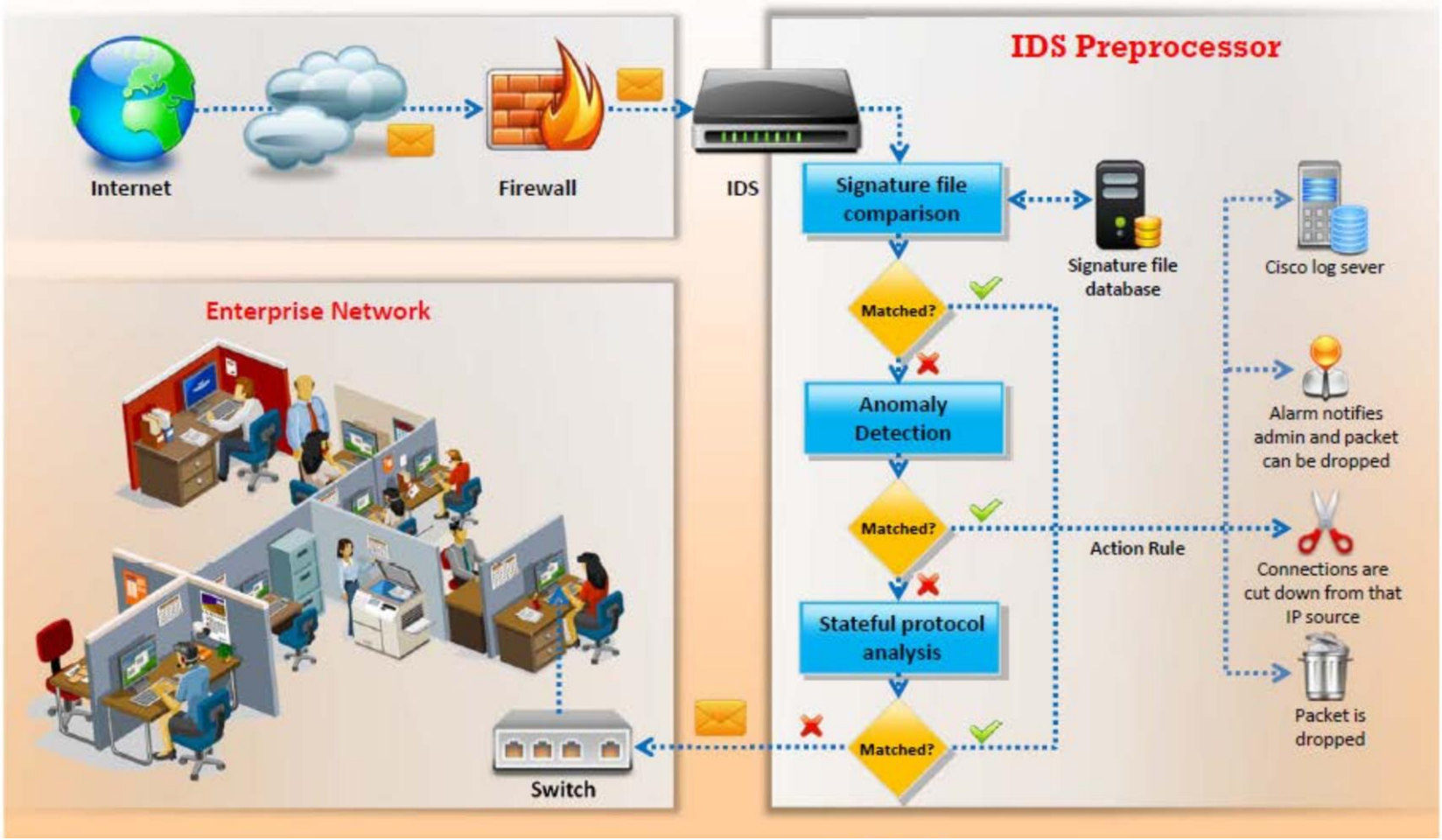




Source: CEHv9

Cách IDS hoạt động?

Tổng quan



Source: CEHv9

Cách IPS ngăn chặn xâm nhập?

Tổng quan

1. IPS dừng hoạt động tấn công

- Ngắt kết nối (mạng) hoặc phiên làm việc đang bị sử dụng để tấn công
- Chặn truy cập vào mục tiêu (hoặc các máy có khả năng là mục tiêu) từ tài khoản người dùng, địa chỉ IP hoặc các yếu tố tấn công khác
- Chặn tất cả các truy cập đến host, dịch vụ, ứng dụng hoặc các tài nguyên khác là mục tiêu

2. IPS thay đổi môi trường bảo mật

- Tái cấu hình một thiết bị mạng (ví dụ tường lửa, router, switch) để chặn truy cập từ attacker hoặc truy cập đến mục tiêu
- Vá các lỗ hổng đang có trên host

3. IPS thay đổi nội dung của hoạt động tấn công

- Loại bỏ hoặc thay thế những phần độc hại của tấn công để nó thành bình thường
- Hoạt động như proxy và *bình thường hoá* các yêu cầu được gửi đến (đóng gói lại payloads của yêu cầu, bỏ các thông tin header…)

IDPS có phải lúc nào cũng phát hiện đúng?

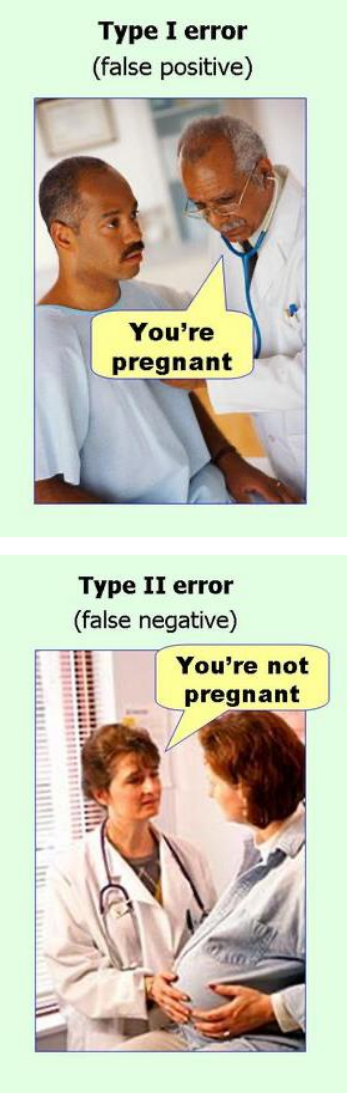
Tổng quan

Không!

- **False positive – dương tính giả:** khi IDPS xác định nhầm hoạt động bình thường là hoạt động đáng ngờ
- **False negative – âm tính giả:** khi IDPS không thể xác định 1 hoạt động là đáng ngờ

➔ **Mục tiêu: Tuỳ chỉnh IDPS để giảm tỉ lệ thông báo false (*giảm FP và FN*)**

Thực tế: *Giảm 1 tỷ lệ sẽ làm tăng tỷ lệ còn lại*
Vậy chúng ta cần làm gì?



IDPS: có thể và không thể làm gì?

Tổng quan

- **IDS có thể làm gì?**
  - IDPS có thể liên tục theo dõi các gói tin trong mạng, hiểu ở dạng nhị phân, và cảnh báo nếu xảy ra bất thường khớp với signature đã biết
  - IDPS tạo ra lượng lớn dữ liệu dù được điều chỉnh tốt như thế nào

  Một IDS mới giống như 1 đứa bé, cần chăm sóc và nuôi dưỡng để trưởng thành khoẻ mạnh và hiệu quả

  - Hỗ trợ các cơ chế phòng thủ mạng khác, hợp tác để hiện thực chiến lược **phòng thủ theo chiều sâu (defense-in-depth)**
- **IDS không thể làm gì?**
  - Không có IDS nào có thể thay thế sự cần thiết của đội ngũ nhân viên am hiểu về an toàn thông tin
  - Không có IDS nào có thể bắt tất cả các tấn công xảy ra, hoặc chặn người khác cố gắng tấn công chúng ta

Một vài từ khoá

Cần nhớ

- Intrusion (xâm nhập), Incident (sự cố); exploit (khai thác), vulnerability (lỗ hổng)
- Intrusion detection (phát hiện xâm nhập), Intrusion prevention (ngăn chặn xâm nhập), IDS, IPS
- False positive, False negative
- Tuỳ chỉnh (tuning) IDPS

Thảo luận

Xem lại…

1. **IDPS có quan trọng không?**
2. **Khác biệt giữa IDS và IPS?**
3. **Giả sử đã có 1 firewall, vậy có cần thêm IDPS? Firewall có thể hoạt động như IDPS không?**

Tuần sau:

1. **Có bao nhiêu loại IDPS?**
   (Tài liệu: paper "IDPS Taxonomy: traditional and state-of-the-art")
2. **IDPS có thể được đặt ở đâu trong mạng?**
3. **IDPS hoạt động như thế nào?**

Chuẩn bị cho tuần sau…

Looking ahead

- Hôm nay: **Giới thiệu môn học**
- Tuần sau: **Tổng quan về IDPS**
  - Nên sớm lập nhóm đồ án tối đa 4 sinh viên (có thể đăng ký tuần sau)
  - **Đọc thêm** (bài tập về nhà):
    1. Xem lại nội dung TCP/IP attack của môn NT101 – An toàn mạng máy tính
    2. G. Fernandes, J. J. P. C. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi, and M. L. Proença, "**A comprehensive survey on network anomaly detection**," *Telecommunication Systems*, vol. 70, no. 3, pp. 447–489, 2019 - https://rdcu.be/2WNT (Phần **1** - **4**)
    3. K. Scarfone and M. Peter, **Guide to Intrusion Detection and Prevention Systems (IDPS).** NIST**,** 2007. - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (Chương 2, 3)

Today end, **See you next week!**