Ids(intrusion detection system): hệ thống phát hiện xâm nhập

* Giám sát lưu lượng mạng để phát hiện ra bất thường.
* Chỉ phát cảnh báo cho quản trị viên, k ngăn chặn
* có hai phương pháp chính:
  + phát hiện dựa trên signature
    - so sánh lưu lượng với các mẫu ( chữ kí) của các cuộc tấn công đã biết, nếu khớp sẽ cảnh báo qtv
  + phát hiện dựa trên hành vi bất thường ( anomaly-based detection)
    - xây dựng mô hình hành vi bình thường của hệ thống, nếu phát hiện hành vi bất thường so với mô hình sẽ cảnh báo.

Ips(intrusion prevention system): hệ thống ngăn chặn xâm nhập

* Tương tự như ids nhưng có them khả năng chặn các cuộc tấn công
  + Các phương pháp chính:
    - Chặn lưu lượng độc hại -> loại bỏ gói tin hoặc kết nối có dấu hiện tấncông
    - Ngắt kết nối – ngăn chặn kẻ tấn công truy cập vào hệ thống
    - Cập nhật chính sách – thay đổi các quy tắc tạm thời để tang cường bảo vệ

Idps( intrusion detection and prevention system): kết hơp giữa ids và ips

Types of intrusion detection system:

* Network based ids (nids)
  + Giám sát lưu lượng mạng của một phân đoạn mạng cụ thể và phân tích giao thức ứng dụng và mạng để phát hiện hoạt động đáng ngờ
  + Kém hiệu quả trước các cuộc tấn công Ddos vì ddos thường tạo ra 1 lưu lượng mạng khổng lồ, và hệ thống này phải kiểm tra tất cả các gói dữ liệu để xác định gói data nào là đáng ngờ
  + Thường được triển khai ở ranh giới của mạng, các host trong mạng có thể gặp nguy hiểm nếu intruder có thể bypass qua hệ thống nids này
* Wireless ids
  + tương tự như NIDS ở chỗ nó có thể phân tích lưu lượng mạng
  + Tuy nhiên, nó cũng sẽ phân tích lưu lượng truy cập dành riêng cho mạng không dây, bao gồm quét tìm người dùng bên ngoài đang cố gắng kết nối với các điểm truy cập (AP), AP giả mạo,
* Network behavior anomaly detection
  + NBAD liên tục giám sát hoạt động của mạng, bao gồm lưu lượng mạng, các kết nối, và các hoạt động của thiết bị. Nó ghi nhận các đặc điểm thông thường của mạng trong một khoảng thời gian nhất định, tạo ra một "baseline" (cơ sở dữ liệu hành vi thông thường). NBAD sẽ so sánh hoạt động mạng hiện tại với baseline này. Nếu phát hiện bất kỳ sự chênh lệch nào hoặc các hoạt động không phù hợp với hành vi thông thường, hệ thống sẽ coi đó là một sự bất thường (anomaly).
  + Các loại hành vi bất thường mà NBAD có thể phát hiện:
    - Lưu lượng mạng tăng đột biến
    - Kết nối lạ
    - Thay đổi hành vi của người dùng: Nếu một người dùng trong mạng bắt đầu thực hiện các hành động không phù hợp với thói quen thông thường của họ (ví dụ: truy cập vào dữ liệu nhạy cảm vào giữa đêm), NBAD có thể nhận diện và báo cáo hành vi này.
  + Ưu điểm
    - Phát hiện các cuộc tấn công mới: Bởi vì NBAD dựa trên việc phát hiện hành vi bất thường thay vì các chữ ký tấn công đã biết
    - Hiệu quả trong việc phát hiện nội gián: NBAD có thể phát hiện các hoạt động bất thường từ các tài khoản người dùng hợp pháp trong tổ chức, chẳng hạn như nhân viên nội bộ có hành vi xâm phạm dữ liệu.
    - Giám sát liên tục
  + Hạn chế
    - Khả năng tạo ra cảnh báo giả (false positives): Nếu baseline không được xây dựng chính xác
    - Cần thời gian để xây dựng baseline: Để hoạt động hiệu quả, NBAD cần một khoảng thời gian ban đầu để theo dõi và học hành vi thông thường của mạng.
    - Không nhận diện trực tiếp các mối đe dọa cụ thể: NBAD có thể nhận diện sự bất thường, nhưng nó không luôn luôn xác định được chính xác cuộc tấn công đang diễn ra là gì, cần phải có sự can thiệp của con người để điều tra thêm.
* Host based ids
  + phát hiện xâm nhập được triển khai trên các máy chủ hoặc thiết bị cá nhân (hosts) để giám sát và phân tích các hoạt động xảy ra trên chính thiết bị đó. Không giống như Network-based IDS (NIDS) giám sát lưu lượng mạng trên toàn bộ hệ thống, HIDS tập trung vào việc bảo vệ từng thiết bị cụ thể.
  + Khi phát hiện ra sự thay đổi bất thường hoặc một hoạt động không hợp lệ (chẳng hạn như một tệp bị thay đổi không đúng lúc, hoặc một quá trình đáng ngờ được khởi chạy), HIDS sẽ tạo ra cảnh báo để quản trị viên điều tra thêm.
  + Cơ chế bảo vệ
    - Ngắt kết nối thiết bị
    - Khôi phục tập tin bị thay đổi
    - Chặn quá trình đáng ngờ
* Protocol based ids
* Application based ids
* Hybrid ids
  + Kết hợp giữa hids và nids

Ips ( intrusion prevention system):

* Là quá trình vừa phát hiện xâm nhập hoặc các mối đe dọa vừa có thể quản lý một số hành động để ứng phó với với chúng.
* IPS đang theo dõi thời gian thực lưu lượng gói có hoạt động độc hại hoặc phù hợp với hồ sơ cụ thể và sẽ kích hoạt việc tạo cảnh báo và nó có thể giảm, chặn lưu lượng truy cập đó trong thời gian thực đi qua mạng.
* IPS có thể được gọi là phần mở rộng của IDS với các bài tập kiểm soát truy cập để bảo vệ máy tính xâm nhập. IPS là một thiết bị thông minh không chỉ có khả năng phát hiện các hoạt động độc hại mà còn có thể thực hiện các hành động phòng ngừa để bảo mật máy chủ hoặc mạng.
* Nói đơn giản, IDS hoàn toàn phù hợp để giám sát các cuộc tấn công mạng và cảnh báo cho quản trị viên về các tấn công mạng. IPS như là một vũ khí để ta có thể chủ động ngăn chặn những cuộc tấn công đó.
* Các chức năng chính được thực hiện bở IPS
  + IPS detects and takes preventive actions against malicious attacks
    - Phát hiện tấn công: IPS giám sát lưu lượng mạng và sử dụng các phương pháp như phát hiện dựa trên chữ ký (signature-based detection) hoặc hành vi (anomaly-based detection) để nhận diện các cuộc tấn công độc hại.
    - Hành động ngăn chặn: Sau khi phát hiện, IPS tự động thực hiện các biện pháp để ngăn chặn cuộc tấn công trước khi nó có thể gây hại. Điều này có thể bao gồm việc chặn lưu lượng tấn công, ngắt kết nối hoặc ngăn chặn các lệnh xâm nhập.
  + IPS stops the attack itself
    - Tự động ngăn chặn: Không giống như IDS (Intrusion Detection System), chỉ phát hiện và cảnh báo, IPS có khả năng tự động ngăn chặn cuộc tấn công ngay lập tức. Khi phát hiện lưu lượng mạng độc hại, IPS sẽ chặn hoặc dừng cuộc tấn công mà không cần sự can thiệp của quản trị viên.
  + IPS changes the security environment
    - Thay đổi chính sách hoặc cấu hình: Khi phát hiện mối đe dọa, IPS có thể thay đổi môi trường bảo mật để ngăn chặn các tấn công tiếp theo. Điều này có thể bao gồm thay đổi cấu hình tường lửa, áp dụng các quy tắc bảo mật mới hoặc ngăn chặn một dải địa chỉ IP.
    - Ví dụ: Nếu phát hiện một loạt cuộc tấn công từ một địa chỉ IP cụ thể, IPS có thể tự động cập nhật tường lửa để chặn địa chỉ IP đó.
  + IPS changes the attack’s contents
    - Sửa đổi hoặc loại bỏ phần độc hại: IPS có thể can thiệp vào nội dung của gói tin để loại bỏ hoặc sửa đổi phần nguy hiểm trước khi gói tin này đến được đích. Điều này giúp bảo vệ hệ thống mà vẫn cho phép lưu lượng mạng tiếp tục.
    - Ví dụ: Nếu một email có chứa mã độc hại, IPS có thể xóa mã độc đó khỏi email trước khi cho phép nó được chuyển tiếp tới người nhận.

ips đã có đủ nhận dạng cũng như ngăn chặn vậy tại sao lại có hệ thống kết hợp giữa ips và ids (idps)

* IDS (Intrusion Detection System): Tập trung vào việc phân tích lưu lượng mạng một cách chi tiết và tạo ra cảnh báo khi phát hiện các hành vi bất thường hoặc các cuộc tấn công. IDS có khả năng giám sát toàn bộ mạng và cung cấp cho quản trị viên thông tin chi tiết về các sự kiện bảo mật.
* IPS (Intrusion Prevention System): Ngoài việc phát hiện tấn công, IPS còn có khả năng ngăn chặn các mối đe dọa ngay lập tức. Tuy nhiên, khi IPS tự động ngăn chặn, nó có thể bỏ qua việc phân tích chi tiết và chỉ tập trung vào việc bảo vệ hệ thống. Điều này có thể dẫn đến việc bỏ sót các thông tin quan trọng mà IDS có thể cung cấp.
* Cân bằng giữa phát hiện và ngăn chặn:
  + IDPS (Intrusion Detection and Prevention System): Kết hợp cả khả năng phát hiện mạnh mẽ của IDS và khả năng ngăn chặn tự động của IPS. Hệ thống IDPS cho phép bạn lựa chọn giữa việc chỉ phát hiện hoặc vừa phát hiện vừa ngăn chặn.
* Giảm thiểu cảnh báo giả và ngăn chặn sai lầm:
  + IPS: Do tập trung vào việc ngăn chặn tự động, IPS có thể dẫn đến cảnh báo giả (false positives) và trong một số trường hợp, nó có thể ngăn chặn sai lầm, làm gián đoạn các hoạt động hợp pháp của hệ thống.
  + IDPS: Với IDPS, bạn có thể kiểm tra và phân tích các cảnh báo từ IDS trước khi thực hiện hành động ngăn chặn, giảm thiểu nguy cơ ngăn chặn nhầm. Điều này tạo ra sự cân bằng giữa an toàn và hiệu quả hoạt động của hệ thống.
* Khả năng phản hồi tùy biến:
  + IDPS: Cho phép bạn thiết lập phản hồi tùy biến dựa trên mức độ nghiêm trọng của tấn công. Ví dụ, với một số loại tấn công ít nghiêm trọng, hệ thống có thể chỉ phát hiện và cảnh báo mà không ngăn chặn. Trong khi với các mối đe dọa nguy hiểm hơn, hệ thống có thể tự động ngăn chặn ngay lập tức.
  + IPS: Thường thực hiện các hành động ngăn chặn tự động mà không có nhiều tùy chỉnh trong quá trình phát hiện.

Thu thập dữ liệu: -> Tiền xử lý dữ liệu -> Chọn thuật toán học máy (Random Forest, Support Vector Machines, Neural Networks) -> Huấn luyện mô hình -> Tích hợp mô hình vào IDPS

Tìm hiểu tất cả loại tcm ddos, sql injection

Tìm hiểu một số mô hình Snort, Suricata, hoặc Bro (Zeek)

Dataset, tiền sử lí dữ liệu

Mô hình mình sử dụng, mhoc hoac deeplearning tại sao lại dùng