**Báo cáo IPDS**

1. **Một số loại tấn công mạng phổ biến**
   1. **Tấn công từ chối dịch vụ phân tán (DDos – Distributed reflection Denial of Service):**

* Mục tiêu là làm quá tải tài nguyên của hệ thống (máy chủ, dịch vụ, mạng) bằng cách gửi lượng lớn yêu cầu từ nhiều nguồn khác nhau, khiến hệ thống không thể phục vụ người dùng hợp lệ.
* Phát hiện: IDPS có thể nhận diện lưu lượng mạng bất thường, chẳng hạn như lưu lượng cao đột ngột từ nhiều nguồn khác nhau tấn công vào một mục tiêu.
* Phòng chống: Hạn chế băng thông cho các nguồn nghi vấn, chặn lưu lượng từ các IP có dấu hiệu bất thường, hoặc sử dụng kỹ thuật lọc lưu lượng.
  1. **Tấn công cơ sở dữ liệu (SQL Injection):**
     + Tấn công này khai thác lỗ hổng trong các ứng dụng web để chèn mã SQL độc hại vào các truy vấn cơ sở dữ liệu, cho phép kẻ tấn công truy cập, sửa đổi hoặc xóa dữ liệu.
     + Công cụ: sqlmap, sử dụng các payload đơn giản như ' OR 1=1 --.
     + Phát hiện: IDPS có thể phát hiện các chuỗi ký tự hoặc mẫu truy vấn SQL độc hại trong các yêu cầu HTTP đến máy chủ web.
  2. **Tấn công khai thác lỗ hỏng bảo mật - Exploit attack**
     + Đây là kiểu tấn công khai thác lỗ hổng bảo mật chưa được biết đến hoặc chưa được vá bởi nhà cung cấp phần mềm.
  3. **Tấn công mật khẩu – password attack**
     + **Brute force attack – tấn công dò mật khẩu:** Đây là một kiểu tấn công mà kẻ tấn công thử mọi kết hợp có thể của mật khẩu hoặc khóa để bẻ khóa tài khoản hoặc mã hóa.

Phát hiện: IDPS có thể giám sát các nỗ lực đăng nhập thất bại liên tiếp từ một địa chỉ IP cụ thể. Nếu phát hiện quá nhiều lần thử không thành công trong một khoảng thời gian ngắn, IDPS có thể đánh dấu đây là một cuộc tấn công brute force.

* + - **Dictionary Attack (tấn công từ điển**): là một biến thể của Brute Force Attack, tuy nhiên kẻ tấn công nhắm vào các từ có nghĩa thay vì thử tất cả mọi khả năng, nhiều người dùng có xu hướng đặt mật khẩu là những từ đơn giản VD: password, motconvit,… -> tỉ lệ thành công cao hơn.
    - **Key Logger Attack (tấn công Key Logger):** ưu lại lịch sử các phím mà nạn nhân gõ, bao gồm ID, password hay nhiều nội dung khác. Nguy hiểm vì dù có đặc mật khẩu phức tạp cũng không tác dụng.
  1. A diagram of a computer hacker

     Description automatically generated**Tấn công Man-in-the-Middle Attack:** Tấn công này xảy ra khi kẻ tấn công chen ngang vào giao tiếp giữa hai bên (ví dụ: giữa người dùng và trang web), cho phép họ đọc, thay đổi hoặc chặn dữ liệu trao đổi.

Phát hiện: IDPS có thể phát hiện các thay đổi bất thường trong lưu lượng mạng, chẳng hạn như các thông báo giả mạo ARP, DNS hoặc SSL/TLS.

* **ARP (Address Resolution Protocol) là giao thức được sử dụng để chuyển đổi địa chỉ IP thành địa chỉ MAC trên mạng nội bộ. Kẻ tấn công có thể giả mạo thông báo ARP để đánh lừa các thiết bị trong mạng gửi dữ liệu cho kẻ tấn công thay vì thiết bị hợp pháp.**
* **DNS (Domain Name System) là hệ thống dịch địa chỉ IP thành tên miền (ví dụ: chuyển 192.168.1.1 thành example.com). Kẻ tấn công có thể gửi các thông báo DNS giả mạo để chuyển hướng người dùng đến một trang web lừa đảo thay vì trang hợp pháp.**
* **SSL/TLS (Secure Sockets Layer/Transport Layer Security) là giao thức bảo mật được sử dụng để mã hóa dữ liệu khi truyền tải giữa người dùng và máy chủ. Kẻ tấn công có thể giả mạo hoặc thay thế chứng chỉ SSL/TLS để nghe lén hoặc chiếm quyền truy cập vào kết nối bảo mật.**
  1. A computer screen with text and icons

     Description automatically generatedTấn công giả mạo – Phishing attack: Phishing là hình thức tấn công hacker giả mạo thành một đơn vị/cá nhân uy tín để chiếm lòng tin của người dùng, thông thường qua email. Mục đích của tấn công giả mạo (phishing) là đánh cắp dữ liệu nhạy cảm như thông tin thẻ tín dụng, mật khẩu, đôi khi phishing là một hình thức để lừa người dùng cài đặt malware vào thiết bị của họ

Phát hiện: IDPS có thể nhận diện các URL hoặc nội dung trong lưu lượng mạng liên quan đến các trang web lừa đảo hoặc giả mạo.

* 1. A diagram of a computer network

     Description automatically generated**Tấn công chiếm đoạt phiên (Session Hijacking attack)** : Tấn công chiếm đoạn phiên (Session Hijacking) là một loại tấn công mạng trong đó kẻ tấn công chiếm quyền điều khiển một phiên kết nối đang diễn ra giữa hai hệ thống, chẳng hạn giữa một người dùng và máy chủ.

Mục tiêu của tấn công chiếm đoạn phiên là giành quyền truy cập vào thông tin, tài khoản, hoặc tài nguyên mà người dùng hợp pháp đang sử dụng.

* 1. **Social Engineering:** Đây là hình thức tấn công dựa vào việc lừa gạt con người, như dụ dỗ họ cung cấp thông tin nhạy cảm hoặc thực hiện hành động không mong muốn.

Phát hiện: IDPS có thể phát hiện các hoạt động lừa đảo hoặc tấn công xã hội thông qua giám sát nội dung email, liên kết, và yêu cầu truy cập.

Phòng chống: Cảnh báo người dùng về các liên kết hoặc email nguy hiểm, đồng thời ngăn chặn các truy cập từ các nguồn đáng ngờ.

* 1. Tấn công quét cổng (Port Scanning) là kỹ thuật mà kẻ tấn công sử dụng để khám phá các cổng mở hoặc các dịch vụ đang chạy trên máy chủ hoặc mạng mục tiêu. Quá trình này giúp kẻ tấn công xác định các điểm yếu trong hệ thống và từ đó có thể thực hiện các cuộc tấn công khác như xâm nhập trái phép hoặc khai thác lỗ hổng bảo mật.
  2. Tấn công bằng phần mềm độc hại (Malware Attack): tấn công bằng phần mềm độc hại (malware)

Phát hiện: IDPS có thể phát hiện các mẫu mã độc hại thông qua dấu vết của nó trong lưu lượng mạng hoặc trên các tệp tin truyền qua

* Một số mô hình máy học để huấn luyện