Tên nhóm: Nguyễn Xuân Nam

Tên giải pháp: Hệ thống phát hiện xâm nhập dựa trên sự bất thường sử dụng học máy

Mô tả chung

Hệ thống IDS (hệ thông phát hiện xâm nhập) là một trong những công cụ hữu hiệu trong việc phát hiện và cản báo xâm nhập hay tấn công vào hệ thống mạng máy tính. Điểm đặc biệt của hệ thống là có thể phát hiện ra cả những loại tán công mới chưa được công bố, và vì xử dụng học máy nên hệ thống sẽ ngày càng trở nên thông minh hơn khi có nhiều dữ liệu huấn luyện. Phần lý thuyết của hệ thống đã được công bố ở hội nghị quốc tế NICS 2016 tổ chức ở Đà Nẵng.

Các chức năng

* Phát hiện, cảnh báo cho người quản trị biết khi hệ thống có dấu hiệu bị tấn công.
* Cung cấp nhiều lựa chọn về mức độ an ninh của hệ thống(mức độ càng cao thì càng khó bị tấn công, nhưng dễ sinh ra dương tính giả).
* Định kỳ huấn luyện hệ thống để hệ thống trở nên thông minh hơn