Thiết kế và triển khai hệ thống phát hiện xâm nhập dựa trên kĩ thuật máy học

Nguyễn Đức Thông
Phạm Ngọc Hiếu Minh
Trần Thanh Tín

Ngày 11 tháng 4 năm 2018

UIT
TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ THÔNG TIN

Mục lục

1 Giới thiệu

1.1 Đề tài

1.2 Đặt vấn đề

1.3 Mục tiêu

2 Lí thuyết IDS và Machine Learning

2.1 An toàn thông tin

2.2 Hệ thống phát hiện xâm nhập

2.2.1 Giới thiệu

2.2.2 HIDS

2.2.3 NIDS

2.2.4 Giới hạn

2.3 Khai thác dữ liệu

2.4 Máy học

3 Công nghệ tiếp cận

3.1 Snort 3

3.1.1 Giới thiệu

3.1.2 Kiến trúc

3.1.3 Cấu hình

3.1.4 Mở rộng tính năng

3.2 NSL-KDD

3.2.1 Giới thiệu

3.2.2 Đặc tính

3.3 Thuật toán KMeans

3.4 Scikit

3.4.1 Giới thiệu

Scikit-learn (viết tắt là **sklearn**) là một thư viện mã nguồn mở trong ngành machine learning, rất mạnh mẽ và thông dụng với cộng đồng Python, được thiết kế trên nền NumPy và SciPy. Scikit-learn chứa hầu hết các thuật toán machine learning hiện đại nhất, đi kèm với comprehensive documentations. Điểm mạnh của thư viện này là nó được sử dụng phổ biến trong academia và industry, do đó nó luôn được updated và có một very active user community.

4 Thử nghiệm và kết quả

4.1 Thiết lập dữ liệu và môi trường thử nghiệm

4.2 Kết quả và nhận xét

5 Kết luận

5.1 Nhận định

5.2 Hướng phát triển

Tài liệu