

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 2 tháng 4 năm 2018



UIT
TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ THÔNG TIN

Mục lục

1	Giới thiệu	1
1.1	Đề tài	1
1.2	Đặt vấn đề	1
1.3	Mục tiêu	1
2	Lí thuyết IDS và Machine Learning	2
2.1	An toàn thông tin	2
2.2	Hệ thống phát hiện xâm nhập	2
2.2.1	Giới thiệu	2
2.2.2	HIDS	2
2.2.3	NIDS	2
2.2.4	Giới hạn	2
2.3	Khai thác dữ liệu	2
2.4	Máy học	2
3	Công nghệ tiếp cận	3
3.1	Snort	3
3.1.1	Giới thiệu	3
3.1.2	Kiến trúc	3
3.1.3	Cấu hình	3
3.1.4	Giới hạn	3
3.2	NSL-KDD	3
3.2.1	Giới thiệu	3
3.2.2	Đặc tính	3
3.3	Thuật toán KMeans	3
3.4	Scikit	3
3.4.1	Giới thiệu	3
4	Thử nghiệm và kết quả	4
4.1	Thiết lập dữ liệu và môi trường thử nghiệm	4
4.2	Kết quả và nhận xét	4
5	Kết luận	5
5.1	Nhận định	5
5.2	Hướng phát triển	5

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

3.1.1 Giới thiệu

3.1.2 Kiến trúc

3.1.3 Cấu hình

3.1.4 Giới hạn

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

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