

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP TP. HCM**  
**KHOA CÔNG NGHỆ THÔNG TIN**

-----🙞🙜🕮🙞🙜-----

**ĐỒ ÁN 1**

**XÂY DỰNG HỆ THỐNG IPS**

**DÙNG HIDS-OSSEC**



GVHD: Nguyễn Hoà

Sinh viên thực hiện:  
1. Phạm Văn Duẩn (13037321)

2. Võ Thành Luân()

3. Mai Quốc Quy ()

4. …Vinh ()

*TP. Hồ Chí Minh, tháng 5 năm 201**6*

1. **Đặt vấn đề**

Khi mạng Internet ngày càng phát triển và các mạng nội bộ xuất hiện nhiều ở khắp mọi nơi, thách thức về các vấn đề xâm phạm và bảo mật mạng được đặt ra.

Nhiều biện pháp đã được đưa ra để bảo mật cơ sở hạ tầng mạng và truyền thông trên Internet. IDS hoặc HIDS là phương pháp bảo mật có khả năng chống lại các cuộc tấn công, các hoạt động trái phép trên hệ thống.

* 1. **Tầm quan trọng của IDS**

IDS (Intrusion Detection System – Hệ thống phát hiện xâm nhập) là một hệ thống giám sát hoạt động trên hệ thống mạng và phân tích để tìm ra các dấu hiệu vi phạm đến các quy định bảo mật máy tính, chính sách sử dụng và các tiêu chuẩn an toàn thông tin. Các dấu hiệu này xuất phát từ rất nhiều nguyên nhân khác nhau, như lây nhiễm malwares, hackers tấn công, người dùng truy nhập tráo phép vào các tài nguyên..v.v

Sử dụng IDS giúp nâng cao khả năng quản lí và bảo vệ mạng. Nó giúp hệ thống an toàn trước những nguy cơ tấn công, nó cũng cho phép nhà quản trị nhận dạng và phát hiện những nguy cơ tiềm ẩn dựa trên những phân tích và báo cáo được IDS cung cấp. Từ đó, IDS có thể góp phần giảm thiểu đáng kể những lỗ hổng bảo mật trong môi trường mạng.

* 1. **Vai trò của HIDS**
  2. **Bài toán đặt ra của đề tài**

Trong một mạng LAN có thể có rất nhiều máy Workstation. Việc quản lí các Worktation gặp phải rất nhiều khó khăn. Việc người dùng làm gì trên

Xây dựng hệ thống IPS cho mạng LAN của Windows desktop sử dụng OSSEC có hỗ trợ

1. **Mô hình hệ thống và phương pháp thực hiện**
   1. **Mô hình hệ thống**

**Agent**

Gửi log

**Pre-decode**

So khớp thông tin

Đơn giản hoá log

Lấy thông tin

**Server**

**Decode**

**Rule**

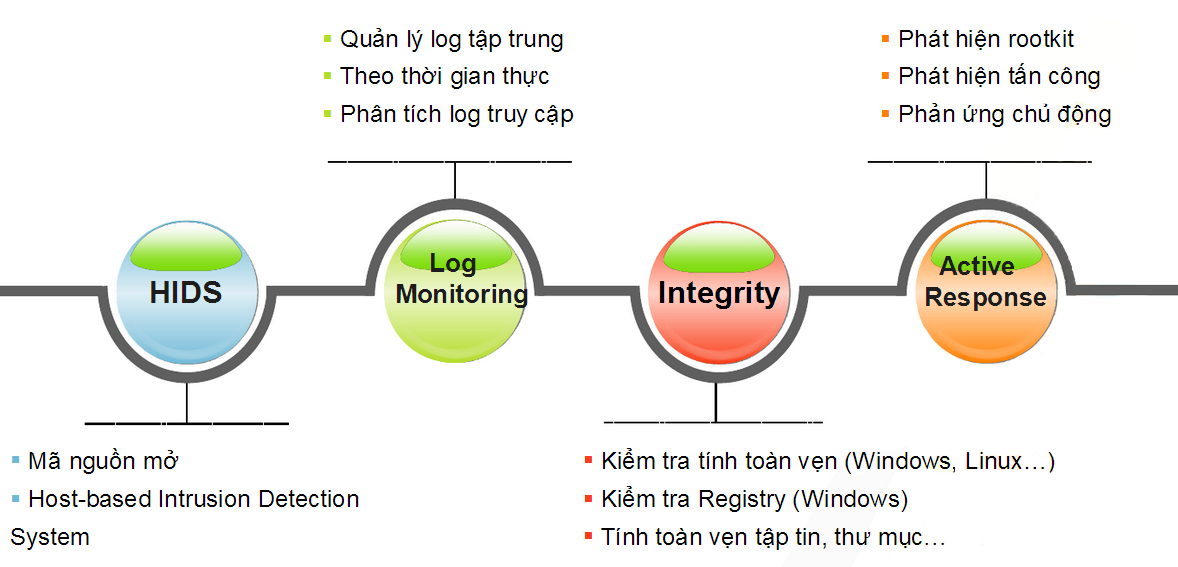
**Warning**

**Active**

* 1. **Công nghệ thực hiện**

*Như đã ghi ở tên đề tài, công nghệ thực hiện ở đây là OSSEC*

* + 1. **Giới thiệu OSSEC**

Là một chương trình để theo dõi và kiểm soát hệ thống của bạn. Nó là một phần mềmcủa HIDS (dựa trên máy chủ phát hiện xâm nhập – Host IDS), giám sát đăng nhập và cáctác vụ của hệ thống với một giải pháp mã nguồn đơn giản, mạnh mẽ. Nó cũng được hỗ trợvà hỗ trợ đầy đủ bởi Trend Micro.

* + 1. **Lợi ích của OSSEC**
* Đáp ứng được các tiêu chuẩn quốc tế

OSSEC cho phép bạn phát hiện và cảnh báo những thay đổi hệ thống tập tin và nhữnghành vi nguy hiểm nhúng trong các file log của các sản phẩm, cũng như các ứng dụng tùychỉnh. Nó bao gồm các phần giám sát tính toàn vẹn file kiểm tra đăng nhập, giám sát vàthực thi chính sách kiểm tra. Tuân thủ các tiêu chuẩn như PCI (Payment Card Industry),HIPAA (Health Insurance Portability and Accountability Act)

* Là một hệ thống đa nền tảng

Có thể thực hiện một hệ thống IPS dựa trên các chính sách riêng trên nhiều nền tảng khác nhau. Tuy nhiên, chỉ cần quan tâm Windown.

* Xây dựng cảnh báo theo thời gian thực

Cho phép khách hàng cấu hình những cái họ muốn được cảnh báo, họ có thể tập trungvào các sự cố quan trọng trong hệ thống hơn là những thứ khác. Tích hợp với SMTP, sms và syslog cho phép khách hàng có các cảnh báo trên bằng việc gửi trên e-mail và cách thiết bị cầm tay như điện thoại di động. Các hoạt động active response cũng có sẵn để ngăn chặn một cuộc tấn công ngay lập tức.

* Quản lí tập trung

OSSEC cung cấp một server chính quản lý tập trung các chính sách cho nhiều máy chủ sử dụng nhiều hệ điều hành khác nhau. Ngoài ra nó còn cho phép khách hàng có thể định nghĩa những chính sách riêng cho từng server cụ thể nhằm tối ưu hóa cho các chính sách.

* + 1. **Các chức năng chính của OSSEC**
* Kiểm tra tính toàn vẹn của tập tin

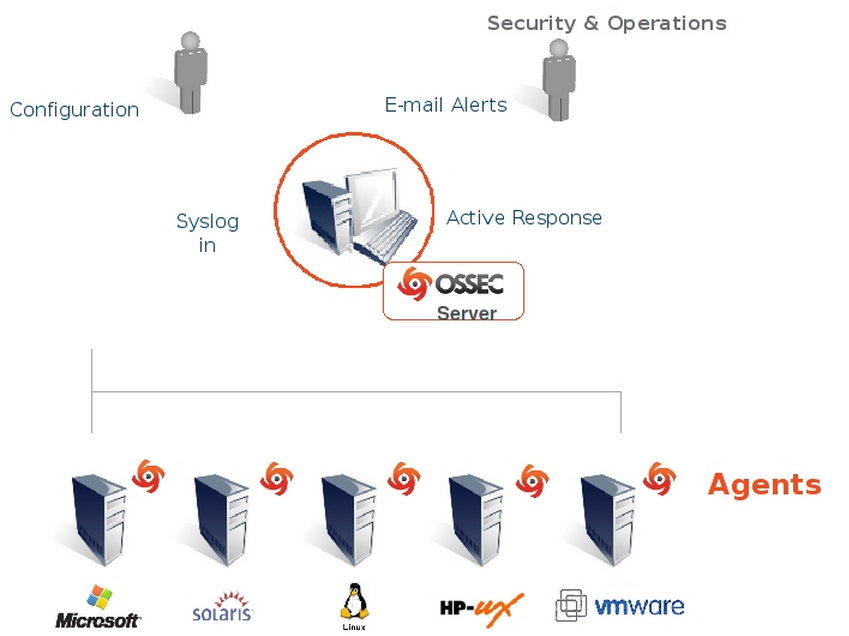
Sử dụng MD5/SHA1 checksums, hỗ trợ cấu hình file được check, tần suất, thời gian,… Mục đích của việc kiểm tra tính toàn vẹn là để phát hiện và cảnh báo các thay đổi bất thường trong hệ thống khi có một cuốc tấn công nào đó và các mạng và máy tính.

* Phát hiện rootkit

Chúng là công cụ phần mềm được cài đặt bởi Hacker để ẩn giấu một số file và tiến trình chạy ngầm khi tấn công vào hệ thống. Việc sử dụng OSSEC sẽ phát hiện rootkit, tự động kiểm tra sau một khoảng thời gian nhất định do người dùng định nghĩa, dựa trên việc so sánh với cơ sở dữ liệu mà các rootkit bị phát hiện và được thông báo.

* Kiểm tra Registry (Windows)

Registry trên Windows là một phần khá nhạy cảm vì dễ bị tấn công. Việc kiểm tra sẽ giúp phát hiện những thay đổi nhỏ đôi khi có thể gây nguy hiểm toàn hệ thống.

* + 1. **Kiến trúc hệ thống**

Cài đặt và hoạt động trực tiếp trên một máy local

Dạng Client-Server gồm:

* Phần quản lý cài ở máy chủ

Có thể nhận log từ Firewalls, switches and routers

* Agent:

Agent có thể cài ở máy client hoặc cũng hổ trợ tính năng agentless

Agent có thể cài được trên máy ảo

* 1. **Phương pháp thực hiện**

*Phuơng pháp thực hiện tương ứng với các giai đoạn trong quá trình phân tích của HIDS-OSSEC*

1. **Các module phân tích và xử lý log của đề tài**
   1. **Nhận dạng log**
   2. **Lấy log từ workstation**
   3. **Decode log**
   4. **Rule**
   5. **Alert và Active Reponse**
2. **Kết quả thực hiện**
   1. **Kết quả đạt được**
   2. **Hạn chế**
3. **Hướng phát triển**