

**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**

**Alert**

**Active**

* **Agent**

Agent chính là các máy workstation. Agent được cấu hình để kiểm quản lí file (tra tính toàn vẹn của file), kiểm tra rootkit, phân tích ventlog, quản lí Registry, đọc log, có logcollector để thu thập và gửi log về cho server.

* **Pre-decode**

Pre-decode là giai đoạn đầu tiên của quá trình phân tích log. Log nhận từ các Agent gửi đến hoặc trên local.

Những log có định dạng mà pre-decode nhận ra, sẽ được trích xuất ra các thông tin mặc định (hostname, program\_name, time, date và log message, ). Pre-decode làm cho log trông đơn giản hơn và việc decode cũng sẽ đơn giản, nhanh hơn.

Pre-decode gửi thông tin đã trích xuất từ log ban đầu sang cho decode, hoặc gửi tất cả đoạn log vì nó không đúng định dạng.

* **Decode**

Tuỳ vào mỗi loại file log sẽ có một decoder (mặc định hoặc do người dùng định nghĩa) riêng tương ứng. Decoder trích xuất các thông tin khác quan trọng (user, ip, port, protocol, …) mà pre-decode không thể làm. Các thông tin này được dùng trong rule, cây rule.

* **Rule**

Các thông tin từ việc decode, nhanh chóng được so khớp với rule, cây rule. Tuỳ theo mức độ cảnh báo mà alert hay active response được sinh ra.

* **Alert**

Là kết quả của việc áp dụng rule, alert có thể được lưu vào database hoặc gửi cho người dùng qua mail.

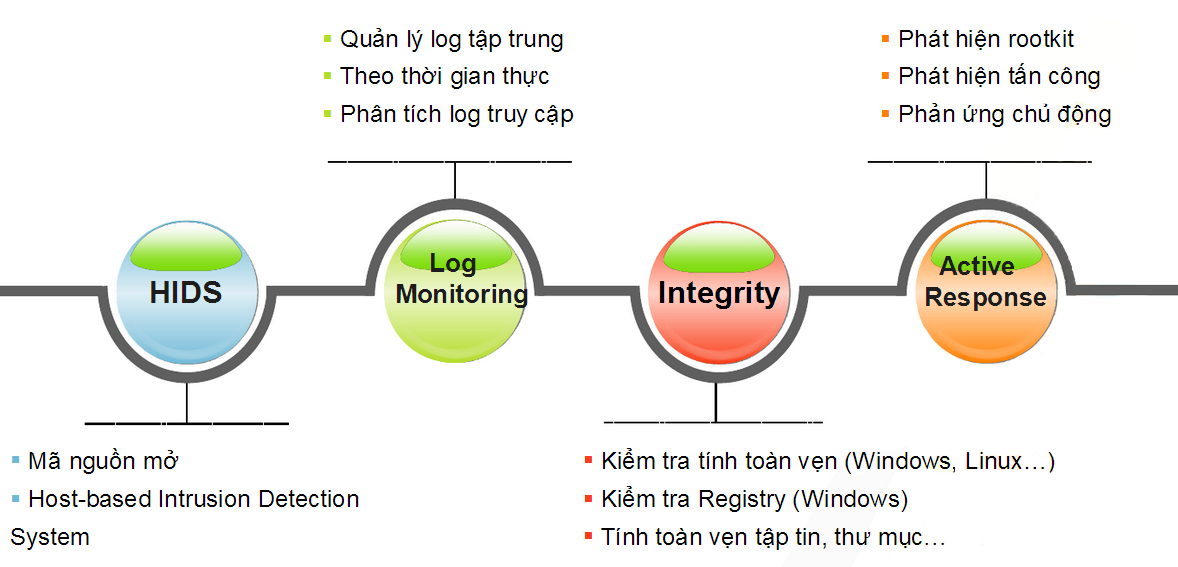
* **Active**

Thực hiện active response để ngăn chặn các hành vi trái phép ngay lập tức.

* 1. **Công nghệ thực hiện**

*Như đã ghi ở tên đề tài, công nghệ thực hiện ở đây là HIDS-OSSEC. Trong phần này, giới thiệu OSSEC là gì và làm rõ quá trình phân tích log của 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

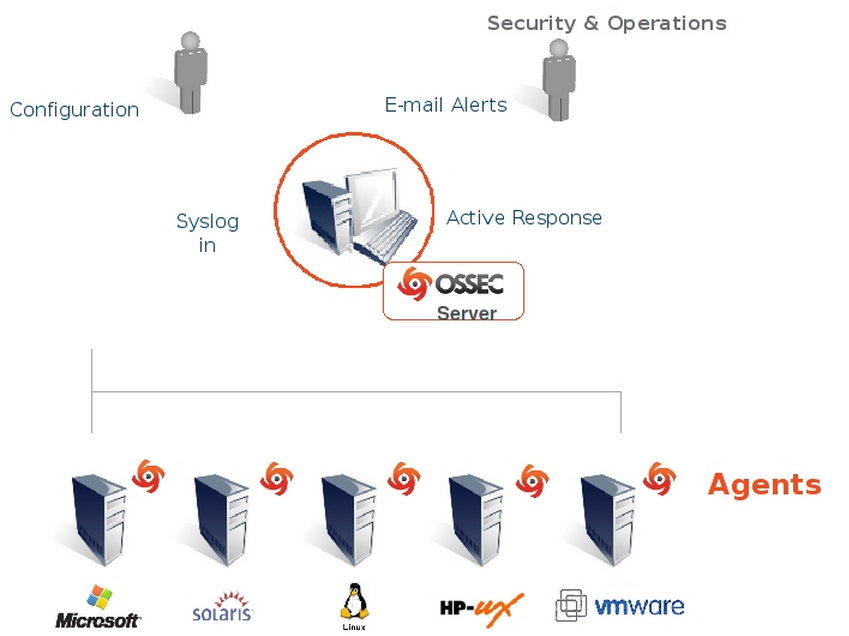
Sử dụng MD5/SHA1 checksums, hỗ trợ cấu hình file được check, tần suất, thời gian,… Mục đích của việc kiểm tra tính toàn vẹn là để phát hiện và cảnh báo các thay đổi bất thường trong hệ thống khi có một cuốc tấn công nào đó và các mạng và máy tính.

* 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:

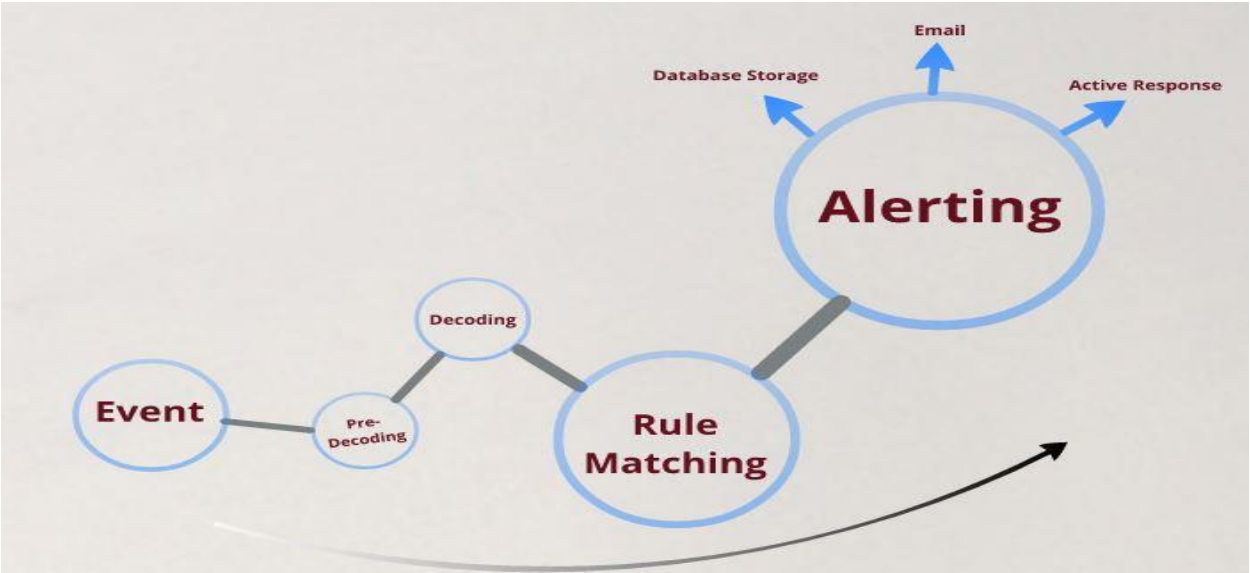
* Phần quản lý cài ở máy chủ

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. **Quá trình phân tích log của OSSEC**
     1. **Giai đoạn Pre-Decoding**

Quá trình pre-decoding là rất đơn giản, nó chỉ trích xuất thông tin tĩnh từ các thuộc tínhcủa một sự kiện. Các thông tin được trích xuất trong giai đoạn này là time, date, hostname,program name, và log message, vv. Những thông tin tĩnh quan trọng từ log được lấy ra và được thực hiện sau đó ở trong phần decoding của quá trình.

Mục đích của pre-decoding là làm cho việc decoding trờ nên đơn giản hơn.

Ví dụ về pre-decoding qua đoạn log được tạo bởi chương trình *sshd*

“Apr 14 17:32:06 linux\_server sshd[1025]: Accepted password for dcid from 192.168.2.180 port 1618 ssh2”

|  |  |
| --- | --- |
| **Thuộc tính** | **Kết quả** |
| *hostname*  *program\_name*  *log*  *time/data* | linux\_server  sshd  Accepted password for dcid from 192.168.2.180 port 1618 ssh2  Apr 14 17:32:06 |

Tuy nhiên, các loại log không đúng định dạng thì quá trình pre-decoding trở nên vô nghĩa.

* + 1. **Giai đoạn Decoding**

Là bước tiếp theo trong quá trình, sau giai đoạn pre-decoding. Mục tiêu của decoding là trích xuất thông tin động, quan trọng từ các log để có thể sử dụng trong các rules sau này. Decoder sẽ trích xuất thông tin như địa chỉ IP, username, port …

Từ ví dụ trên ta có được log như sau:

Log: ”Accepted password for dcid from 192.168.2.180 port 1618 ssh2”

Sau quá trình Decoding ta được:

|  |  |
| --- | --- |
| **Thuộc tính** | **Kết quả** |
| *user*  *srcip* | dcid  192.168.2.180 |

Decoder có thể được cấu hình để lấy được tất cả những thông tin quan trọng, không phụ thuộc vào định dạng của log, từ nhiều nguồn log khác nhau.

Tất cả các decoder được cấu hình trong file */var/ossec/etc/decoder.xml*

Sử dụng Decoder với các thẻ ở bảng bên dưới

|  |  |  |  |
| --- | --- | --- | --- |
| **Tag** | **@** | **Value** | **Mô tả** |
| *decoder* |  |  |  |
| @name |  | Tên decoder duy nhất |
| *parent* |  |  | Tên của decoder cha |
| *program\_name* |  |  | Tên chương trình phải giống như ở pre-decoding |
| *prematch* |  |  | Thực hiện decode nếu trùng khớp |
| @offset | after\_parent | Bắt đầu lấy thông tin tại nơi decoder cha dừng |
| *regex* |  |  | Biểu thức dùng để trích xuất thôn tin |
| @offset | after\_parent  after\_prematch  after\_regex | Bắt đầu sau parent, prematch hoặc regex của decoder cha |
| *oder* |  | srcip, dstip,srcport, dstport, protocol, action, user, id, status, command, url, data, system\_name | Các thuộc tính tương ứng với các biểu thức trong regex theo thứ tự lần lượt |
| *type* |  | firewall, ids, syslog, web-log, squid, windows, ossec | Xác định từng loại log |

Ví dụ với đoạn log sau

“Apr 14 17:32:06 linux\_server sshd[1025]: Accepted password for dcid from 192.168.2.180 port 1618 ssh2”

Decoder:

|  |
| --- |
| <decoder name="sshd-success">  <parent>sshd</parent>  <prematch>^Accepted</prematch>  <regex offset="after\_prematch">^ \S+ for (\S+) from (\S+) port  </regex>  <order>user, srcip</order>  </decoder> |

* + 1. **Rule Matching**

Rule và decoder kết hợp với nhau giúp cho OSSEC phát huy được các tính năng mạnh mẽ của mình. Khi kết hợp chúng với nhau cho phép cấu hình và điều chỉnh các cảnh báo từ OSSEC, bao gồm kiểm tra tính toàn vẹn, syslog, cáclog events của agent và cảnh báo phát hiện rootkit.

Rule của OSSEC được lưu trữ bên trong thư mục */var/ossec/rule*. Mỗi rule được xác định với phần mở rộng là XML riêng biệt và được đặt tên phù hợp. XML được sử dụng thay vì file cấu hình (dạng text) bởi vì XML dễ đọcvà hiểu được nó dễ dàng. Có 43 file rule được cài đặt mặc định trong HIDS OSSEC.

Mỗi các rule có một Rule\_ID duy nhất, Rule\_ID do người dùng tự định nghĩa một rules nằm trong khoảng 100000 đến 119999.

Có hai loại rule trong OSSEC: atomic và composite. Atomic rule dựa trên các sự kiện đơn lẻ, không có bất kì mối quan hệ nào. Ví dụ, một thông báo có thể được sinh ra với một lần đăng nhập thất bại duy nhất. Composite rule kết hợp nhiều sự kiện với nhau. Ví dụ với 10 lần đăng nhập thất bại, từ một IP và trong khoảng thời gian 180s thì lúc này cần tới một composite rule.

**Các mức độ cảnh báo của OSSEC**

|  |  |
| --- | --- |
| **Level** | **Định nghĩa** |
| **0** | Bỏ qua, không quan tâm |
| **1** | None |
| **2** | Thông báo của hệ thống mức thấp |
| **3** | Sự kiện thành công/uỷ quyền |
| **4** | Lỗi hệ thống mức thấp |
| **5** | Lỗi do người dùng tạo ra |
| **6** | Tấn công cấp thấp |
| **7** | So sánh với những từ khoá xấu |
| **8** | Sự kiện xuất hiện lần đầu |
| **9** | Lỗi từ nguồn không hợp lệ |
| **10** | Nhiều người dùng tạo ra lỗi |
| **11** | Cảnh báo kiểm tra tính toàn vẹn |
| **12** | Sự kiện có mức quan trọng cao |
| **13** | Lỗi bất thường (quan trọng cao) |
| **14** | Sự kiện bảo mật có tầm quan trong cao |
| **15** | Tấn công thành công |

Rule được sử dụng với các thẻ ở bảng bên dưới

|  |  |  |  |
| --- | --- | --- | --- |
| **Tag** | **@** | **Value** | **Mô tả** |
| *group* |  |  | Thẻ nhóm các rule |
|  | @name |  | Tên theo ngữ cảnh |
| *rule* |  |  |  |
| @id |  | Duy nhất |
| @level | (number) | Từ 0 tới 15 |
| @maxsize | (number) | Kích thước tối đa của log |
| @frequency | (number) | Số lần rule trùng khớp |
| @accuracy | 0/1 | 0 = no, 1 = yes |
| @noalert | 0/1 |  |
| @ignore | (number) | Bao nhiêu lần rule xảy ra được bỏ qua |
| @overwrite | yes/no | Chỉnh sửa lại rule mặc định |
| @timefarm | (seconds) |  |
| *description* |  |  | Bắt buộc |
| *cve/infor* |  |  |  |
| *action/status* |  |  | Decode bởi decoder |
| *group* |  | invalid\_login, authenication\_success,  authentication\_failed,  attacks, sshd, ids,(…) | Nhóm ứng dụng độc lập |
| *decoded\_as* |  |  | Khớp với tên decoder |
| *match* |  |  | So sánh nhanh chuỗi với mẫu bất kì |
| *regex* |  |  | Giống như ở decoder |
| *if\_sid*  *if\_group*  *if\_level* |  |  | Rule chỉ đúng nếu trùng id/group/level |
| *hostname* |  |  | Giống với decode ở pre-decoder |
| *srcip/dstip/*  *srcport/dstport/*  *user/id/url* |  |  | Giống với decode bằng decoder |
| *program\_name* |  |  | Giống với decode ở pre-decoder |
| *category* |  | firewall, ids, syslog, web-log, squid, windows, ossec | Giống với kiểu đã khai báo ở decoder |
| *weekday* |  | sunday, sun, monday, mon, tuesday, tue, wednesday, wed, thursday, thu, friday, fri, saturday, sat, weekdays, weekends | Dành cho chính sách. Ngày trong tuần |
| *time* |  | hh:mm – hh:mm or hh:mm am – hh:mm pm | Dành cho chính sách |
| *options* |  | alert\_by\_email,  no\_email\_alert,  no\_log |  |
| *extra\_data* |  |  | Được trích xuất bởi decode (data) |
| *if\_matched\_sid*  *if\_matched\_group*  *if\_matched\_regex* |  |  | Composite rule: rule chắc chắn trùng khớp với id/group/regex |
| *same\_source\_ip*  *same\_src\_port*  *same\_dst\_port*  *same\_user/same\_location*  *same\_id/different\_url* |  |  | Composite rule: quy định các giá trị trong từng thuộc tính phái giống nhau (ip đến từ 1 nguồn,…) |

Ví dụ rule:

|  |
| --- |
| <group name=“syslog,sshd,”>  <rule id=“100123” level=“2”>  <decoded\_as>sshd</decoded\_as>  <description>Logging every decoded sshd message</description>  </rule>  <rule id=“100124” level=“7”>  <if\_sid>100123</if\_sid>  <match>^Failed password</match>  <group>authentication\_failure</group>  <description>Failed SSHD password attempt</description>  </rule>  <rule id=“100125” level=“3”>  <if\_sid>100123</if\_sid>  <match>^Accepted password</match>  <group>authentication\_success</group>  <description>Successful SSHD password attempt</description>  </rule>  </group> |

Cây rule của ví dụ trên

Rule 100123

Rule 100124

Rule 100125

* 1. **Quy trình thực hiện của đề tài**

*Phuơng pháp thực hiện bao gồm các giai đoạn trong quá trình phân tích log của HIDS-OSSEC, và bổ sung thêm quá trình nhận dạng log và lấy log từ workstation.*

* + 1. **Nhận dạng log**

Mỗi sự kiện

* + 1. **Lấy log từ workstation**
    2. **Decode log**
    3. **Rule**
    4. **Alert và Active Reponse**

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 Matching**
   5. **Alert và Active Reponse**
2. **Kết quả thực hiện**
   1. **Kết quả đạt được**
   2. **Hạn chế**
3. **Hướng phát triển**