

**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.

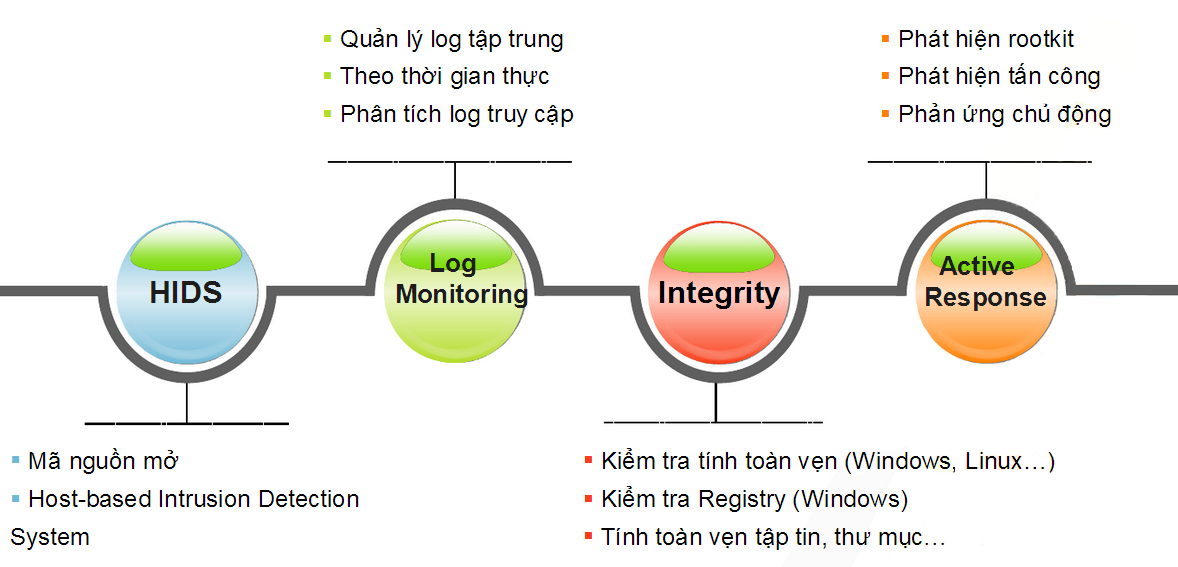
* **Active**

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

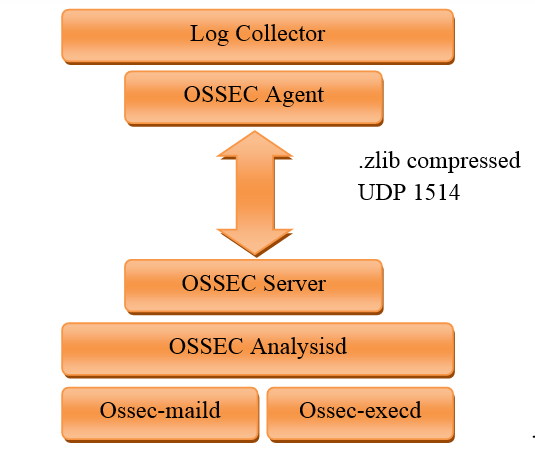
Sử dụng MD5/SHA1 checksums, hỗ trợ cấu hình file được check, tần suất, thời gian,… Mục đích của việc kiểm tra tính toàn vẹn là để phát hiện và cảnh báo các thay đổi bất thường trong hệ thống khi có một cuốc tấn công nào đó và các mạng và máy tính.

* 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:

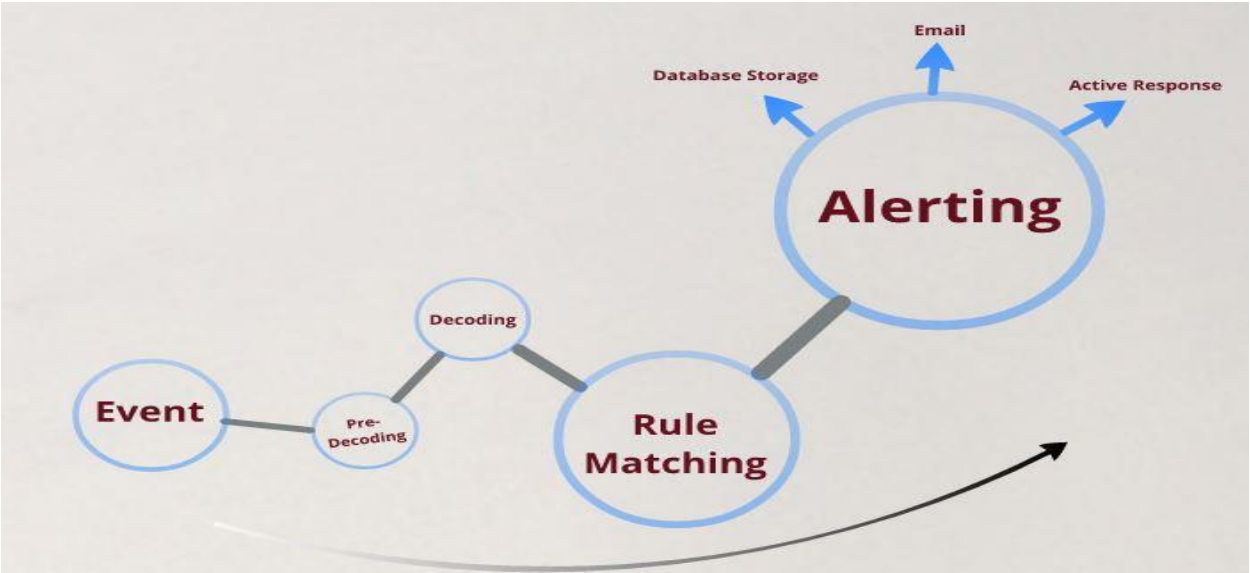
* Phần quản lý cài ở máy chủ

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 predecode chỉ để trích xuất các thông tin đơn giản của event. Predecode thường được sử dụng với các log message có định dạng được sử dụng phổ biến như syslog.

Các thông tin được trích xuất qua giai đoạn này bao gồm:

* **hostname:** Nơi tạo ra log
* **program\_name:** Chương trình tạo ra log
* **log:** Nội dung chính của log
* **time/date:** Thời gian sinh ra event log

Ta xét một ví dụ đơn giản về ssh trong event log sau :

Log message: “Oct 28 14:21:39 atropo sshd[855]: Accepted password for piopio from 192.168.3.13 port 45018 ssh2”

Và đây là kết quả từ OSSEC-Logtest

\*\*Phase 1: Completed pre-decoding.

full event: 'Oct 28 14:21:39 atropo sshd[855]: Accepted password for piopio from 192.168.3.13 port 45018 ssh2'

hostname: 'atropo'

program\_name: 'sshd'

log: 'Accepted password for piopio from 192.168.3.13 port 45018 ssh2'

Ta có thể thấy là chỉ có các thông tin cơ bản được trích xuất. Ngoài ra các thông tin như: người dùng, process id, status, source ip,… thì lại không được hiển thị. Vậy nên cần phải thông qua một tiến trình nữa để có thể lấy được các thông tin này, đó chính là decode.

Có một vấn đề nữa ở predecode là đối với những định dạng log khác thì predecode sẽ không thể trích xuất được thông tin mà phải chuyển thẳng đến quá trình decode.

* + 1. **Giai đoạn Decoding**

Decode là tiến trình diễn ra ngay sau khi predecode. Mục đích của decode là trích xuất các thông tin từ log để sử dụng trong rule ngay sau khi decode diễn ra. Các thông tin này chính là thông tin về: người dùng, ip source, process id, status,… và các thông tin cần thiết khác.

**Bảng 2.1** : Các field được sử dụng trong decoded

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |

Dưới đây là thông tin một số option trong field *oder* dùng để gán cho từng dữ liệu trích được từ file log:

* **Location:** nơi sinh log
* **srcuser:** source user
* **dstuser:** destination user
* **srcip:** source ip
* **dstip:** destination ip
* **srcport:** source port
* **dstport:** destnation port
* **protocol:** tên giao thức
* **id:** event id
* **url:** địa chỉ
* **status:** trạng thái
* **extra-data:** dữ liệu

Từ ví dụ trên ta có được log như sau:

Log: ” 'Accepted password for piopio from 192.168.3.13 port 45018 ssh2'”

Sau quá trình Decoding ta được:

|  |  |
| --- | --- |
| **Thuộc tính** | **Kết quả** |
| *user*  *srcip* | piopio  192.168.3.13 |

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.

Ta có ví dụ về log message được sinh ra sau khi tạo chia sẽ folder trên windows:

WinEvtLog: Security: **AUDIT\_SUCCESS**(5140): Microsoft-Windows-Security-Auditing: (no user): no domain: VanDuan-PC: A network share object was accessed. Subject: Security ID: S-1-5-21-739373341-442988835-2982865765-1000 Account Name: VanDuan Account Domain: **VANDUAN-PC** Logon ID: 0x24EF400 Network Information: Object Type: File Source Address: fe80::9d4d:93cc:9f6d:c594 Source Port: 12922 Share Information: Share Name: \\\*\123 Share Path: \??\C:\WINDOWS\System32 Access Request Information: Access Mask: 0x1 Accesses: ReadData (or ListDirectory)

Ta thử trích xuất các thông tin được tô màu bên trên với decoder được viết như sau:

<decoder name=*"windows-file-share-create"*>

<prematch>\.(5140)\.</prematch>

</decoder>

<decoder name=*"windows-file-share-create-sub"*>

<parent>windows-file-share-create</parent>

<regex>^\.+:\.+: (\.+)\((\d+)\): </regex>

<regex>\.+Account Name:\s\s(\w+)\s\s\sAccount Domain:\s\s(\w+)\s\s\s</regex>

<order>status, id, user, extra\_data</order>

</decoder>

Kết quả có được:

\*\*Phase 2: Completed decoding.

decoder: 'windows-file-share-create'

status: 'AUDIT\_SUCCESS'

id: '5140'

dstuser: 'VanDuan'

extra\_data: 'VANDUAN-PC'

url: 'C:\WINDOWS\System32'

Có thể thấy được, ta dễ dàng có được các thông tin cần thiết để so khớp với rule thông qua decoder nhờ sử dụng các biểu thức regular expression.

* + 1. **Rule Matching**
       1. **Giới thiệu về rule**

Để cho hệ thống đạt được các tính năng mạnh mẽ nhất của OSSEC . Việc kết hợp các bộ giải mã (decoder) và các quy tắc (rule) với nhau sẽ làm cho hệ thống OSSEC HIDS đạt được sức mạnh của nó. Khi kết hợp chúng, chúng sẽ cho phép bạn cấu hình và chỉnh mọi cảnh báo từ OSSEC HIDS, bao gồm : Kiểm tra tính toàn vẹn của các cảnh báo,các syslog, các event log của agent và cảnh báo phát hiện rootkit.

Mỗi rule của OSSEC đều được lưu trong rules/ của thư mục cài đặt OSSEC HIDS. Điển hình như trong Linux /var/ossec/rules/. Mỗi rule được định nghĩa trong một file mở rộng .xml riêng biệt và được đặt tên cho phù hợp , mục đích là dễ nhận dạng và phân loại rule. Ví dụ, tất cả các rule của máy chủ Apache HTTP đều được đặt trong file apache\_rules.xml. Khi cài đặt OSSEC HIDS mặc định sẽ có 43 file rules được định nghĩa sẵn.

**Bảng 2.2 :** Các rule mặc định trong OSSEC HIDS

|  |  |
| --- | --- |
| Tên rule | Mô tả |
| 1. *apache\_rules.xml* | Apache HTTP server rules |
| 1. *arpwatch\_rules.xml* | Arpwatch rules |
| 1. *attack\_rules.xml* | Common attack rules |
| 1. *cisco-ios\_rules.xml* | Cisco IOS firmware rules |
| 1. *courier\_rules.xml* | Courier mail server rules |
| 1. *firewall\_rules.xml* | Common firewall rules |
| 1. *ftpd\_rules.xml* | Rules for the ftpd daemon |
| 1. *hordeimp\_rules.xml* 2. *ids\_rules.xml* 3. *imapd\_rules.xml* 4. *local\_rules.xml* 5. *mailscanner\_rules.xml* 6. *msauth\_rules.xml* 7. *ms-exchange\_rules.xml* 8. *netscreenfw\_rules.xml* 9. *ms\_ftpd\_rules.xml* 10. *mysql\_rules.xml* 11. *named\_rules.xml* 12. *ossec\_rules.xml* 13. *pam\_rules.xml* 14. *pix\_rules.xml* 15. *policy\_rules.xml* 16. *postfix\_rules.xml* 17. *postgresql\_rules.xml* 18. *proftpd\_rules.xml* 19. *pure-ftpd\_rules.xml* 20. *racoon\_rules.xml* 21. *rules\_config.xml* 22. *sendmail\_rules.xml* 23. *squid\_rules.xml* 24. *smbd\_rules.xml* 25. *sonicwall\_rules.xml* 26. *spamd\_rules.xml* 27. *sshd\_rules.xml* 28. *symantec-av\_rules.xml* 29. *symantec-ws\_rules.xml* 30. *syslog\_rules.xml* 31. *telnetd\_rules.xml* 32. *vpn\_concentrator\_rules.xml* 33. *vpopmail\_rules.xml* 34. *vsftpd\_rules.xml* 35. *web\_rules.xml* 36. *zeus\_rules.xml* | Horde Internet Messaging Program rules  Common IDS rules  Rules for the *imapd* daemon  OSSEC HIDS local, user-defined rules  Common mail scanner rules  Microsoft Authentication rules  Microsoft Exchange server rules  Juniper Netscreen firewall rules  Microsoft FTP server rules  MySQL database rules  Rules for the *named* daemon  Common OSSEC HIDS rules  Pluggable Authentication Module (PAM) rules  Cisco PIX firewall rules  Policy specific event rules  Postfix mail transfer agent rules  PostgerSQL database rules  ProFTPd FTP server rules  Pure-FTPd FTP server rules  Racoon VPN device rules  OSSEC HIDS Rules configuration rules  Sendmail mail transfer agent rules  Squid proxy server rules  Rules for the *smbd* daemon  SonicWall firewall rules  Rules for the *spamd* spam-deferral daemon  Secure Shell (SSH) network protocol rules  Symantec Antivirus rules  Symantec Web Security rules  Common syslog rules  Rules for the telnetd daemon  Cisco VPN Concentrator rules  Rules for the *vpopmail* virtual mail domain application  Rules for the vsftpd FTP server  Common web server rules  Zeus web server rules |

Mỗi rule có một ID duy nhất được gán khi lần đầu tiên được tạo ra. Cho mỗi loại log, giá trị của các rule ID phải được ghi lại để đảm bảo rằng decoder của OSSEC HIDS không bị lỗi ghi đè.

OSSEC cung cấp cho người dùng một khoảng địa chỉ ID để cho người dùng tự tạo ra quy tắc. Các quy tắc do người dùng tạo ra gọi là local rule, local rule nên nằm trong khoảng ID từ 100,000 đến 119,999. Vì nếu chọn bất kì ID khác thì có thể gây ra xung đột với các ID rule mặc định của OSSEC. Với mỗi local rule nên đặt trong file local\_rules.xml nằm trong thư mục /*var/ossec/rules/local\_rules.xml* của OSSEC HIDS.

* + - 1. **Xây dựng rule**

Các rule của OSSEC HIDS sẽ đánh giá mức độ của sự kiện để xem sự kiện này cần đưa ra một cảnh báo hoặc nólà một phần của một cảnh báo tổng hợp (với nhiều sự kiện).

Vai trò của rule:

* Kiểm tra, so khớp các thông tin.
* Lọc từng luồng dữ liệu.
* Tạo ra các điều kiện phức (cây rule).

Có 2 loại rule trong OSSEC HIDS là:

* Atomic rules
* Composite rules
  + - * 1. **Atomic rules**

Mỗi rule hoặc nhóm các rules phải được định nghĩa trong một thẻ *<group></group>.* Thuộc tính *name* của group cũng được định nghĩa trong cặp thẻ này.Ví dụ:

<group name=*"ms-file-share,"*>

</group>

Dấu “ , ” phân biệt hai nhóm khác nhau trong cùng 1 group

Một group có thể có nhiều rule , các rule được định nghĩa trong cặp thẻ *<rule></rule>* và bắt buộc phải có ít nhất hai thuộc tính *id* và *level*. Các *id*  là định danh duy nhất và *level* là để chỉ mức độ nghiêm trọng của các cảnh báo.

Ví dụ:

<group name=*"ms-file-share,"*>

<rule id=*"100100"* level=*"0"* noalert=*"1"*>

<id>5140|5142|5143|5144</id>

<description>WINDOWS FILE SHARE message grouped

</description>

</rule>

</group>

**Cấp độ Rules**

Các rule được phân loại ở nhiều cấp độ(*level*). Từ mức thấp nhất (00) cho đến mức tối đa là (15). Khi các rule được viết, chúng được lưu trữ theo mô hình phân cấp (tree rule).

Các rule sẽ được đọc từ mức độ cao nhất đến mức độ thấp nhất. Nhưng có trường hợp ngoại lệ là mức độ 0 sẽ được đánh giá trước các mức độ khác.

**Cụ thể các mức độ cảnh bảo trong OSSEC HIDS như sau:**

**Bảng 2.3: Các mức độ cảnh báo của OSSEC**

|  |  |  |
| --- | --- | --- |
| Level | Định nghĩa | Mô tả |
| 0 | Bỏ qua không hành động | Những rule với *level* này sẽ được quét trước tất cả những rule khác. Chúng bao gồm các sự kiện không có liên quan đến an ninh. |
| 1 | *Không có* |  |
| 2 | Hệ thống ưu tiên thông báo thấp | Thông báo hệ thống hoặc thông báo trạng thái không có liên quan đến ninh |
| 3 | Sự kiện thành công/uỷ quyền | Bao gồm đăng nhập thành công, các sự kiện mà tường lữa cho phép,v.v. |
| 4 | Lỗi hệ thống mức thấp | Lỗi liên quan đến các cấu hình xấu hoặc các thiết bị/ ứng dụng không được sử dụng. Không có liên quan đến bảo mật và thường được gây ra bởi cài đặt mặc định hoặc kiểm thử phần mềm |
| 5 | Lỗi do người dùng tạo ra | Chúng bao gồm mật khẩu bị mất, các hành động bị từ chối , bởi vì không có liên quan đến an ninh |
| 6 | Tấn công cấp thấp | Có thể là một con sâu hoặc virus mà không tạo ra mối đe dọa cho hệ thống. Chúng cũng bao gồm việc thường xuyên kích hoạt các sự kiện IDS và các sự kiện lỗi phổ biến khác |
| 7 | So sánh với những từ khoá xấu | Bao gồm các từ như “bad”, “error”,v.v. Những sự kiện này hầu hết được phân loại theo thời gian và có một số liên quan đến an ninh |
| 8 | Sự kiện xuất hiện lần đầu | Bao gồm các sự kiện được thấy lần đầu tiên. Một sự kiện IDS được phát sinh lần đầu tiên hoặc lần đầu tiên người dùng đăng nhập |
| 9 | Lỗi từ nguồn không hợp lệ | Bao gồm một nổ lực đăng nhập từ người dùng không rõ hoặc từ một nguồn không hợp lệ. Có thể có sự liên quan đến bảo mật(đặc biệt nếu lặp đi lặp lại). Ngoài ra cũng bao gồm các lỗi liên quan đến tài khoản root “admin” |
| 10 | Nhiều người dùng tạo ra lỗi | Bao gồm sai mật khẩu, đăng nhập thất bại, có thể là do một cuộc tấn công hoặc cũng có thể chỉ do người sử dụng quên thông tin của mình |
| 11 | Cảnh báo kiểm tra tính toàn vẹn | Bao gồm các thông điệp liên quan đến việc sửa đổi mã nhị phân hoặc có sự hiện diện của rootkit (bởi rootcheck). Nếu bạn chỉ sửa đổi cấu hình hệ thống của bạn, thì nên quan tâm đến các thông điệp “syscheck”, nó có khả năng là một cuộc tấn công thành công |
| 12 | Sự kiện có mức quan trọng cao | Bao gồm các thông báo lỗi hoặc các cảnh báo từ hệ thống, kernel,v.v. Chúng có thể chỉ ra một cuộc tấn công chống lại một ứng dụng cụ thể |
| 13 | Lỗi bất thường (có mức quan trọng cao) | Bao gồm các mô hình tấn công phổ biến như một nỗ lực tràn bộ nhớ đệm , một thông điệp lớn hơn syslog bình thường, hoặc một chuỗi URL lớn hơn bình thường |
| 14 | Sự kiện bảo mật có tầm quan trọng cao | Thường là kết quả tương quan của nhiều quy tắc tấn công và chỉ một cuộc tấn công |
| 15 | Tấn công thành công | Cần chú ý ngay lập tức là điều cần thiết |

OSSEC HIDS cũng có cung cấp một số subgroup cho ta định nghĩa vào các group cha sử dụng thẻ *<group></group>*

Một thẻ quan trọng là *<decoded\_as></decoded\_as>*. Điều này có nghĩa rằng rule sẽ được thực hiện chỉ khi sự kiện được decoded giãi mã.

Ví dụ:

<rule id=*"100123"* level=*"5"* >

<decoded\_as>ssh</decoded\_as>

<description>Logging every decoded ssh message

</description>

</rule>

Lấy một ví dụ từ chương trình *ssh,* chúng ta có thể thấy rule sẽ thực hiện chỉ khi nếu sự kiện được giải mã bởi decoded *ssh*.

Xét ví dụ:

<rule id=*"100100"* level=*"0"* noalert=*"1"*>

<id>5140|5142|5143|5144</id>

<description>WINDOWS FILE SHARE message grouped

</description>

</rule>

Ngoài ra bạn cũng có thể thấy rằng rule này cũng sẽ thực hiện nếu như giá trị trong thẻ *<id></id>* phù hợp với giá trị ID được trích ra từ quá trình decoded.

Thẻ *<description></description>* dùng để mô tả mục đích là để bạn phân biệt giữa các rule được tạo ra.

Các quy tắc đã tạo ra không nhất thiết phải là một quy tắc hữu ích . Tuy nhiên, ta cũng có thể mở rộng một chút nữa bằng thẻ *<match></match>* để kiểm tra ,so khớp các thành phần của log.

Ví dụ:

Ta có event log sau :

WinEvtLog: Security: AUDIT\_SUCCESS(5140): Microsoft-Windows-Security-Auditing: (no user): no domain: VanDuan-PC: A network share object was accessed. Subject: Security ID: S-1-5-21-739373341-442988835-2982865765-1000 Account Name: VanDuan Account Domain: VANDUAN-PC Logon ID: 0x24EF400 Network Information: Object Type: File Source Address: fe80::9d4d:93cc:9f6d:c594 Source Port: 12922 Share Information: Share Name: \\\*\123 Share Path: \??\C:\WINDOWS\System32 Access Request Information: Access Mask: 0x1 Accesses: ReadData (or ListDirectory)

Ngoài việc ta có thể nhận biết đó là log chia sẽ File WinDows

Mà khi ta sử dụng thẻ *<match></match>* để kiểm tra log như :

<rule id=*"100110"* level=*"8"*>

<if\_sid>100100</if\_sid>

<match>A network share object was accessed</match>

<description>Nguoi dung chia se thu muc</description>

<options>alert\_by\_mail</options>

</rule>

Nếu chuỗi trong thẻ *<match></match>* thỏa thì rule này sẽ thực thi cảnh báo và ta cũng có thể biết được hành động liên quan đến chia sẽ thư mục đó là gì.

Để làm việc đúng cách, bạn phải sử dụng thẻ *<if\_sid></if\_sid>*. Thẻ này cho biết thêm một quy tắc để tạo cây rules.

Như ví dụ trên ta có thể thấy rule có id= “100110” sẽ là rule con của rule cha id= “100100” trong cây.

Thẻ *<options></options>* có 3 giá trị là : no\_email\_alert , alert\_by\_emai, no\_log. Dùng để chỉ hành động xảy ra sau khi rule thực hiện.

* + - 1. **Composite Rules**

Đến hiện tại chúng ta đã có các tùy chọn cho cac sự kiện là duy nhất. Nếu chúng ta muốn có sự tương quan giữa nhiều sự kiện , thì cũng có một vài các tùy chọn khác mà ta cần hiểu nó với Composite Rules(CR).

Composite rules phải phù hợp với các events hiện tại với những gì đã nhận được OSSEC HIDS. Để có được quy tắc đối với CR chúng ta phải bổ sung hai tùy chọn là *frequency* và *timeframe* . *Frequency* xác định bao nhiêu lần một event phải xảy ra trước khi các rule sinh ra cảnh báo. *Timeframe* cho HIDS OSSEC bao lâu thì trở lại, xác định trong khoảng thời gian nào đó nó sẽ đưa ra cảnh báo.

Ví dụ:

<rule id=*"100114"* level=*"10" frequence=”3” timeframe=”600”*

<if\_matched\_sid>100110</if\_matched\_sid>

<same\_user/>

<description>Nguoi dung lien tuc chia se thu muc trong 10p </description>

<options>alert\_by\_mail</options>

</rule>

Rule này tạo ra với dụng ý là khi cùng một người dùng thể hiện qua thẻ *</same\_user/>* liên tục chia sẽ thư mục 3 lần trong khoảng thời gian là 10 phút thì nó sẽ đưa ra một cảnh báo.

Khác với Atomic rules sử dụng một số thẻ như: *<if\_sid></if\_sid>, <group></group> , <regex></regex>*

Thì ở đây ta cũng có lần lượt 3 thẻ thay thế chỉ được sử dụng cho riêng *Composite rules* là :

*<if\_matched\_sid></if\_matched\_sid>,*

*<if\_matched\_group></if\_matched\_group>,*

*<if\_matched\_regex></if\_matched\_regex>*

Ngoài ra còn có một số thẻ bổ sung mà ta có thể sử dụng để tạo các composite rules chi tiết hơn: Những tùy chọn này được thế hiện trong bảng sau:

**Bảng 3.2.** Các thẻ tùy chọn trong Composite rules

|  |  |
| --- | --- |
| Thẻ | Mô tả |
| same\_source\_ip  same\_dest\_ip  same\_src\_port  same\_dst\_port  same\_location  same\_user  same\_id | Quy định rằng các địa chỉ IP nguồn phải giống nhau  Quy định rằng các địa chỉ IP đích phải giống nhau  Quy định rằng các port nguồn phải giống nhau.  Quy định rằng các port đích phải giống nhau  Xác định rằng vị trí (hostname hoặc agent\_name) phải giống nhau.  Xác định rằng username được decode phải giống nhau.  Xác định rằng id được decode phải giống nhau. |

Ngoài ra để nâng cao khả năng kiểm tra và lọc dữ liệu, thì còn có rất nhiều cặp thẻ.

**Bảng 2.4** : Các thẻ có thể sử dụng khi tạo rule

|  |  |  |  |
| --- | --- | --- | --- |
| **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 một tree rule đơn giản:

|  |
| --- |
| <group name=*"ms-file-share,"*>  <rule id=*"100100"* level=*"0"* noalert=*"1"*>  <id>5140|5142|5143|5144</id>  <description>WINDOWS FILE SHARE message grouped</description>  </rule>    <rule id=*"100110"* level=*"8"*>  <if\_sid>100100</if\_sid>  <id>5140</id>  <match>A network share object was accessed</match>  <description>Nguoi dung chia se thu muc</description>  <options>alert\_by\_mail</options>  </rule>  <rule id=*"100114"* level=*"10" frequence=”3” timeframe=”600”*  <if\_matched\_sid>100110</if\_matched\_sid>  <same\_user/>  <description>Nguoi dung lien tuc chia se thu muc trong 10p</description>  <options>alert\_by\_mail</options>  </rule>  </group> |

Cây rule của ví dụ trên

Người dùng chia sẽ thư mục liên tiếp 3 lần trong 10 phút

Rule nhận biết hành động liên quan chia sẽ file windows

Người dùng chia sẽ thư mục

Rule 100100

Rule 100110

Rule 100114

* 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**

Bước đầu tiên của quá trình là nhận diện log. Nó bao gồm việc chọn sự kiện an ninh nào trên Windows được quan tâm và phân tích log được sinh ra. Các sự kiện an ninh trên Windows như đăng nhập, chia sẻ file, cài đặt phần mềm, … Xác định được những trường hợp sinh ra log có biểu hiện bình thường/bất thường, từ đó quyết định xem những thuộc tính nào nên được trích xuất trong quá trình Decode.

Các chính sách ( trong Group policy) trên Windows nên được thiết lập để ghi lại log.

* + 1. **Lấy log từ workstation**

OSSEC trên agent sẽ được cấu hình để log (toàn bộ hoặc chỉ những log quan tâm) gửi tới server.

* + 1. **Decode log**

Việc decode log dựa trên kết quả của nhận dạng log. Từ những thuộc tính quan trọng cần được trích xuất, các decoder được viết để lấy ra các thông tin đó.

* + 1. **Rule**

Các trường hợp bình thường/bất thường được sử dụng để viết rule và cây rule.

Các thông tin từ quá trình decode được so khớp với cây rule để sinh ra alert và active response.

* + 1. **Alert và Active Reponse**

Alert được sinh ra từ việc so khớp rule. Tuỳ vào mức độ quan trọng, alert được cấu hình để thông báo cho từng người cụ thể bằng mail hoặc chỉ lưu vào database.

Trong đồ án một Active Response không được nhắc đến.

1. **Bài tập ví dụ thực hiện tuần tự các module phân tích và xử lý log của đề tài trong hệ thống OSSEC HIDS**
   1. **Nhận dạng log**

Trên Windows có rất nhiều log khác nhau phát sinh từ nhiều sự kiện khác nhau. Tuy nhiên, chúng ta chỉ quan tâm tới loại log nào có liên quan tới an ninh. Nhóm các sự kiện cần quan tâm được liệt kê trong bảng bên dưới.

|  |  |  |
| --- | --- | --- |
| **STT** | **Nhóm các sự kiện** | **Mô tả** |
| 1 | Accout Logon | Các sự kiện đăng nhập bằng tài khoản |
| 2 | Accout Management | Các sự kiện quản lí tài khoản |
| 3 | Directory Servive | Các sự kiện dịch vụ thư mục |
| 4 | Logon/Logoff | Các sự kiện đăng nhập/đăng xuất |
| 5 | Non Audit (Event Log) | Các sự kiện trên eventlog |
| 6 | Object Access | Các sự kiện quyền truy cập đối tượng |
| 7 | Policy Change | Các sự kiện khi thay đổi chính sách |
| 8 | Privilege Use | Các sự kiện quyền người dùng |
| 9 | Process Tracking/  Detailed Tracking | Các sự kiện theo dõi tiến trình hoặc chi tiết |
| 10 | System | Các sự kiện từ hệ thống |

Ví dụ

* 1. **Lấy log từ workstation**

Mày ghi thêm cái gì đó vào đây nha

Ta sẽ nhận được cái log event sau

**Log Event**

* + 1. **A network share object was accessed**

WinEvtLog: Security: AUDIT\_SUCCESS(5140): Microsoft-Windows-Security-Auditing: (no user): no domain: VanDuan-PC: A network share object was accessed. Subject: Security ID: S-1-5-21-739373341-442988835-2982865765-1000 Account Name: VanDuan Account Domain: VANDUAN-PC Logon ID: 0x24EF400 Network Information: Object Type: File Source Address: fe80::9d4d:93cc:9f6d:c594 Source Port: 12922 Share Information: Share Name: \\\*\123 Share Path: \??\C:\WINDOWS\System32 Access Request Information: Access Mask: 0x1 Accesses: ReadData (or ListDirectory)

WinEvtLog: Security: AUDIT\_SUCCESS(5140): Microsoft-Windows-Security-Auditing: (no user): no domain: VanDuan-PC: A network share object was accessed. Subject: Security ID: S-1-5-21-739373341-442988835-2982865765-1000 Account Name: VanDuan Account Domain: VANDUAN-PC Logon ID: 0x6D0388 Network Information: Object Type: File Source Address: fe80::9d4d:93cc:9f6d:c594 Source Port: 8545 Share Information: Share Name: \\\*\Share Folder Share Path: \??\D:\Share Folder Access Request Information: Access Mask: 0x1 Accesses: ReadData (or ListDirectory)

* + 1. **A network share object was added**

WinEvtLog: Security: AUDIT\_SUCCESS(5142): Microsoft-Windows-Security-Auditing: (no user): no domain: VanDuan-PC: A network share object was added. Subject: Security ID: S-1-5-21-739373341-442988835-2982865765-1000 Account Name: VanDuan Account Domain: VANDUAN-PC Logon ID: 0x182BBCF Share Information: Share Name: \\\*\Ebook456 Share Path: D:\DA OSSEC\EBook

* + 1. **A network share object was modified**

WinEvtLog: Security: AUDIT\_SUCCESS(5143): Microsoft-Windows-Security-Auditing: (no user): no domain: VanDuan-PC: A network share object was modified. Subject: Security ID: S-1-5-21-739373341-442988835-2982865765-1000 Account Name: VanDuan Account Domain: VANDUAN-PC Logon ID: 0x24EF3C4 Share Information: Object Type: Directory Share Name: \\\*\Share Folder Share Path: D:\Share Folder Old Remark: N/A New Remark: N/A Old MaxUsers: 0xFFFFFFFF New Maxusers: 0xFFFFFFFF Old ShareFlags: 0x0 New ShareFlags: 0x0 Old SD: O:BAG:S-1-5-21-739373341-442988835-2982865765-1000D:(A;;FA;;;S-1-5-21-739373341-442988835-2982865765-500)(A;;0x1200a9;;;WD) New SD: O:BAG:S-1-5-21-739373341-442988835-2982865765-1000D:(A;;0x1200a9;;;WD)(A;;FA;;;S-1-5-21-739373341-442988835-29828

* 1. **A network share object was deleted**

WinEvtLog: Security: AUDIT\_SUCCESS(5144): Microsoft-Windows-Security-Auditing: (no user): no domain: VanDuan-PC: A network share object was deleted. Subject: Security ID: S-1-5-21-739373341-442988835-2982865765-1000 Account Name: VanDuan Account Domain: VANDUAN-PC Logon ID: 0x6D0353 Share Information: Share Name: \\\*\Share Folder Share Path: D:\Share Folder

* 1. **Decode log**

Thực hiện quá trình viết decoded

<!--File Share Create-->

<decoder name=*"windows-file-share-create"*>

<prematch>\.(5140)\.</prematch>

</decoder>

<decoder name=*"windows-file-share-create-sub"*>

<parent>windows-file-share-create</parent>

<regex>^\.+:\.+: (\.+)\((\d+)\): </regex>

<regex>\.+Account Name:\s\s(\w+)\s\s\sAccount Domain:\s\s(\w+)\s\s\s</regex>

<order>status, id, user, extra\_data</order>

</decoder>

<decoder name=*"windows-file-share-create-sub"*>

<parent>windows-file-share-create</parent>

<regex>\.+Share Path:\s\s\\\p+\\(\.+)\s\s\s</regex>

<order>url</order>

</decoder>

<!--File Share Delete-->

<decoder name=*"windows-file-share-delete"*>

<prematch>\.(5144)\.</prematch>

</decoder>

<decoder name=*"windows-file-share-delete-sub"*>

<parent>windows-file-share-delete</parent>

<regex>^\.+:\.+: (\.+)\((\d+)\): </regex>

<regex>\.+Account Name:\s\s(\w+)\s\s\sAccount Domain:\s\s(\w+)\s\s\s</regex>

<order>status, id, user, extra\_data</order>

</decoder>

<decoder name=*"windows-file-share-delete-sub"*>

<parent>windows-file-share-delete</parent>

<regex>\.+Share Path:\s\s(\.+)</regex>

<order>url</order>

</decoder>

<!--File Share Add-->

<decoder name=*"windows-file-share-add"*>

<prematch>\.(5142)\.</prematch>

</decoder>

<decoder name=*"windows-file-share-add-sub"*>

<parent>windows-file-share-add</parent>

<regex>^\.+:\.+: (\.+)\((\d+)\): </regex>

<regex>\.+Account Name:\s\s(\w+)\s\s\sAccount Domain:\s\s(\w+)\s\s\s</regex>

<order>status, id, user, extra\_data</order>

</decoder>

<decoder name=*"windows-file-share-add-sub"*>

<parent>windows-file-share-add</parent>

<regex>\.+Share Path:\s\s(\.+)</regex>

<order>url</order>

</decoder>

<!--File Share Modified-->

<decoder name=*"windows-file-share-modified"*>

<prematch>\.(5143)\.</prematch>

</decoder>

<decoder name=*"windows-file-share-modified-sub"*>

<parent>windows-file-share-modified</parent>

<regex>^\.+:\.+: (\.+)\((\d+)\): </regex>

<regex>\.+Account Name:\s\s(\w+)\s\s\sAccount Domain:\s\s(\w+)\s\s\s</regex>

<order>status, id, user, extra\_data</order>

</decoder>

<decoder name=*"windows-file-share-modified-sub"*>

<parent>windows-file-share-modified</parent>

<regex>\.+Share Path:\s\s(\.+)\s\s\s</regex>

<order>url</order>

</decoder>

Mày thêm 1 cái logtest vào đây nha Duẫn

* 1. **Rule Matching**

Thực hiện viết các rule lọc các luồng dữ liệu đưa vào các mức độ cảnh báo khác nhau.

<group name=*"ms-file-share,"*>

<rule id=*"100100"* level=*"0"* noalert=*"1"*>

<id>5140|5142|5143|5144</id>

<description>WINDOWS FILE SHARE message grouped</description>

</rule>

<rule id=*"100110"* level=*"8"*>

<if\_sid>100100</if\_sid>

<id>5140</id>

<match>A network share object was accessed</match>

<description>Nguoi dung chia se thu muc</description>

<options>alert\_by\_mail</options>

</rule>

<rule id=*"100111"* level=*"10"*>

<if\_sid>100110</if\_sid>

<url>^C:</url>

<description>Nguoi dung chia se thu muc trong o dia he thong</description>

<options>alert\_by\_mail</options>

</rule>

<rule id=*"100112"* level=*"12"*>

<if\_sid>100111</if\_sid>

<url>^C:\Windows|^C:\windows|^C:\WINDOWS</url>

<description>Nguoi dung chia se thu muc trong C:\Windows</description>

<options>alert\_by\_mail</options>

</rule>

<rule id=*"100113"* level=*"12"*>

<if\_sid>100111</if\_sid>

<url>^C:\Users|^C:\users|^C:\USERS</url>

<description>Nguoi dung chia se thu muc trong C:\Users</description>

<options>alert\_by\_mail</options>

</rule>

<rule id=*"100114"* level=*"10" frequence=”3” timeframe=”600”*

<if\_matched\_sid>100110</if\_matched\_sid>

<same\_user/>

<description>Nguoi dung lien tuc chia se thu muc trong 10p</description>

<options>alert\_by\_mail</options>

</rule>

<rule id=*"100120"* level=*"8"*>

<if\_sid>100100</if\_sid>

<id>5142</id>

<match>A network share object was added</match>

<description>Nguoi dung them thu muc chia se</description>

<options>alert\_by\_mail</options>

</rule>

<rule id=*"100130"* level=*"8"*>

<if\_sid>100100</if\_sid>

<id>5143</id>

<match>A network share object was modified</match>

<description>Nguoi dung chinh sua thu muc chia se</description>

<options>alert\_by\_mail</options>

</rule>

<rule id=*"100140"* level=*"8"*>

<if\_sid>100100</if\_sid>

<id>5144</id>

<match>A network share object was deleted</match>

<description>Nguoi dung xoa thu muc chia se</description>

<options>alert\_by\_mail</options>

</rule>

</group>

**Mô hình cây rule tổng quát**

10

12

10

8

0

8

8

8

12

Người dùng xóa thư mục chia sẽ

Người dùng chỉnh sữa thư mục chia sẽ

Người dùng thêm thư mục chia sẽ

Một User liên tục chia sẽ 3 thư mục trong 10p

Chia sẽ ổ dịa hệ thống

Chia sẽ thư mục

C:\Users

Chia sẽ thư mục trong ổ C:\Windows

Người dùng chia sẽ thư mục thành công

Rule cha của cây rule share thư mục

* 1. **Alert và Active Reponse**

1. **Kết quả thực hiện**
   1. **Kết quả đạt được**

Sau một thời gian thực hiện đồ án dưới sự hướng dẫn của thầy Nguyễn Hòa. Nhóm đã hiểu được cơ cấu tổ chức và cách thức hoạt động của hệ thống phát hiện và chống xâm nhập sử dụng công nghệ OSSEC trên nền HIDS . Đặc biệt nhóm đã biết cấu hình thực hiện việc gữi nhận log, phân loại log: lấy log nào và không lấy log nào. Đồng thời sau khi nhận được log nhóm đã biết viết các decoded để phân tích log lấy các dữ liệu cần thiết của từng loại log của các chương trình khác nhau. Sau đó thực hiện viết các quy tắc phức (cây rule) để kiểm tra và lọc các loại dữ liệu log để đưa chung vào các cảnh báo phù hợp, và nhóm cũng đã thực hiện được việc thực hiện cảnh báo của OSSEC vào Email của người quản trị để người quản trị có thể ngăn ngừa kịp thời.

* 1. **Hạn chế**

Vì đây là đồ án 1 của nhóm , nên nhóm cũng mới bắt đầu tìm hiểu về đề tài. Điều đó dẫn đến còn nhiều chức năng, cách quản lý, và cách phòng chống , ngăn chặn của hệ thống OSSEC mà nhóm chưa nắm bắt được.

Nhóm chưa thực hiện được việc cấu hình kích hoạt Active Reponse của hệ thống. Việc này nhóm sẽ thực hiện được tốt trong việc tiếp tục tìm hiểu và phát triển hệ thống OSSEC của một hệ thống mạng thông qua đồ án 2.

1. **Hướng phát triển**

Mục tiêu đặt ra của nhóm khi thực hiện đề tài này, và qua sự hướng dẫn của thầy Nguyễn Hòa là nhóm phải thực hiện được một hệ thống phát hiện xâm nhập cơ bản từ nhận log cho đến cảnh báo và thực thi hành động. Sau đó phát triển hệ thống ngăn chặn các tấn công mạnh từ bên ngoài ví dụ như : rootkit ; ta sử dụng rootcheck. Sau đó sẽ thực hiện trên Cloud nhờ sự hướng dẫn của giảng viên.