

**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 (13017701)

3. Mai Quốc Qui (13032721)

4. Nguyễn Hữu Vinh (13021241)

*TP. Hồ Chí Minh, tháng 5 năm 201**6*

1. **Đặt vấn đề**
   1. **Tầm quan trọng của IDS**
   2. **Vai trò của HIDS**
   3. **Bài toán đặt ra của đề tài**
2. **Mô hình hệ thống và phương pháp thực hiện**
   1. **Mô hình hệ thống**
   2. **Công nghệ thực hiện**
   3. **Phương pháp thực hiện**
3. **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**
      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 3.1:** 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:**

* *Level 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.

* *Level 1:-Không có-*
* *Level 2:* Hệ thống ưu tiên thông báo thấp

Thông báo hệ thống hoặc thông báo trạng thái không có liên quan đến ninh.

* *Level 3:* Sự kiện thành công / ủy quyền

Bao gồm đăng nhập thành công, các sự kiện mà tường lữa cho phép,vv

* *Level 4:* Hệ thống báo lỗi ưu tiên 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.

* *Level 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.

* *Level 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

* *Level 7:* So khớp “Bad word”

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.

* *Level 8:* Xuất hiện lần đầu tiên

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.

* *Level 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”.

* *Level 10:* Lỗi do nhiều người dùng tạo ra

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.

* *Level 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.

* *Level 12:* Sự kiện có tầm 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.

* *Level 13:* Lỗi không bình thường “Có tầm 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

* *Level 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.

* *Level 15:* Tấn công nghiêm trọng

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. |

* + - 1. **Ví dụ hoàn chỉnh về quá trình phân tích và thực hiện một cây rule. Cho các event log sau:**

***Cái này chắc để dành xét cái bài hoàn chỉnh xuyên suốt có luôn phân tích log nha m***

**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)

**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

**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

**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. **Alert và Active Reponse**

1. **Kết quả thực hiện**
   1. **Kết quả đạt được**
   2. **Hạn chế**
2. **Hướng phát triển**