Đại Học Thủy Lợi

Khoa Công nghệ thong tin

****

**Báo cáo Bài tập lớn**

**Đề tài:Tìm hiểu và triển khai hệ thống phát hiện xâm nhập ossec**

Thành Viên:Vũ Đức Đạt-175A071221

Lê Văn Đức-175A071412

# Lời nói đầu.

Hiện nay, công nghệ liên tục đổi mới và tiến bộ kèm theo đó là nhưng dữ liệu lớn, quan trọng được lưu trên hệ thống. Vì điều đó, mọi người luôn tìm cách theo dõi và bảo mật nó trước nguy cơ bị xâm nhập và tấn công. Một trong top phần mềm mã nguồn mở được ưa chuộng trong việc phát hiện xâm nhập là hệ hệ thống là phần mềm ossec. Ossec có khả năng kiểm tra tính toàn vẹn file, giám sát chính sách, phát hiện rootkit, thời gian thực cảnh bảo và phản ứng tích cực. Đây vẫn sẽ là phần mềm hứa hẹn được tin dùng trong tương lai gần.

**Mục Lục:**

Contents

[Lời nói đầu. 2](#_Toc41471742)

[A.Tổng quan 4](#_Toc41471743)

[**I.** **Hệ thống phát hiện xâm nhập IDS(In trucsion Detetion System)** 4](#_Toc41471744)

[**1.** **Khái niệm.** 4](#_Toc41471745)

[**2.** **Các thành phần và chức năng của IDS** 4](#_Toc41471746)

[**II.** **Giới thiệu về Ossec.** 8](#_Toc41471747)

[1.Giới thiệu về ossec 8](#_Toc41471748)

[**2.** **Cài đặt ossec:** 13](#_Toc41471749)

[**3.** **Demo giao diện** 18](#_Toc41471750)

[Đăng giám sát / phân tích 19](#_Toc41471751)

[Syscheck 20](#_Toc41471752)

[B. AFQ 22](#_Toc41471753)

[Phân tích nhật ký là gì? 22](#_Toc41471754)

[Tại sao kiểm tra tính toàn vẹn? 22](#_Toc41471755)

[Nhật ký được lưu ở đâu? 23](#_Toc41471756)

[Nhật ký OSSEC có thể được lưu vào một thư mục khác không? 23](#_Toc41471757)

[Làm thế nào để bắt buộc quét syscheck ngay lập tức? 24](#_Toc41471758)

[Làm thế nào để bỏ qua một tập tin thay đổi quá thường xuyên? 24](#_Toc41471759)

[C. Tổng Kết. 24](#_Toc41471760)

# A.Tổng quan

1. **Hệ thống phát hiện xâm nhập IDS(In trucsion Detetion System)**
2. **Khái niệm.**

**IDS:** là hệ thống phần cứng hoặc phần mềm có chức năng:

* Giám sát lưu thông mạng
* Tự động theo dõi các sự kiện xảy ra trên hệ thống máy tính,phân tích để phát hiện ra các vấn đề liên quan đến an ninh,bảo mật và đưa ra cảnh báo cho nhà quản trị.
* Phản ứng lại với các lưu thông bất thường hay có hại bằng các hành động đã được thiết lập trước như khóa người dùng hay địa chỉ IP nguồn đó truy cập hệ thống mạng.

**IDS** cũng có thể phân biệt giữa:

* Những tấn công từ bên trong(từ những người trong công ty)
* Tấn công bên ngoài (hacker).

**IDS** phát hiện dựa trên các dấu hiệu đặc biệt về các nguy cơ đã biết (giống như các phần mềm diệt virus dựa vào các dấu hiệu đặc biệt để phát hiện và diệt virus) hay dựa trên so sánh lưu thông mạng hiện tại với baseline (thông số đo đạc chuẩn của hệ thống) để tìm ra các dấu hiệu khác thường.

1. **Các thành phần và chức năng của IDS**
2. **IDS bao gồm các thành phần chính:**

* **Thành phần thu thập gói tin:** thành phần này có nhiệm vị lấy các gói tin đi đến mạng . Thông thường các gói tin có địa chỉ không phải của một card mạng sẽ bị card mạng đó hủy bỏ nhưng card mạng của IDS được đặt ở chế độ thu thập tất cả.Bộ phận thu thập gói tin sẽ đọc thông tin của từng trường trong gói tin , xác điịnh chúng thuộc kiểu gói tin nào,dịch vụ gì.. các thông tin này được chuyển đến phần phát hiện tấn công.
* **Thành phần phát hiện tấn công:** các bộ cảm biến đóng vai trò quyết định. Vai trò của bộ cảm biến là dung lọc thông tin và loại bỏ những thồn tin dữ liệu không tương thích đạt được từ các sự kiện liên quan tới hệ thống bảo vệ , vì vậy có thể phát hienj được các hành động nghi ngờ.
* **Thành phần phản hồi:**khi có dấu hiệu của sự tấn công hoặc thâm nhập, các thành phần phát hiện tấn công sẽ gửi tín hiệu báo cáo (alert) có sự tấn công hoặc thâm nhập đến từng thành phần phản ứng . Lúc đó thành phần phản ứng sẽ kích hoạt tường lửa thực hiện chức năng ngăn chặn cuộc tấn công hay cảnh báo tới người quản trị.

1. **Chức năng.**

* **Cảnh báo thời gian thực:**là gửi các cảnh báo thời gian thực đến người quản trị để họ nắm được chi tiết các cuộc tấn công, các đặc điểm thông tin về chúng.
* **Ghi đè vào các tập tin:**các dữ liệu của gói tin sẽ được lưu trữ trong hệ thống các tập tin log.Mục đích là để những người quản trị có thể theo dõi các luồng thông tin vs là nguồn thông tin giúp cho module phát hiện các hoạt động tấn công.
* **Ngăn chặn thay đổi gói tin:**khi một gói tin khớp với dấu hiệu tấn công thì IDS sẽ phản hồi bằng cách xóa bỏ hay từ chối thay đổi nội dung gói tin làm cho gói tin trở lên không bình thường.

1. **Phân loại:**

**Network Base IDS(NIDS):**Hệ thống phát hiện xâm nhập mạng .

Hệ thống sẽ tập hợp các gói tin để phân tích sâu bên trong mà không làm thay đổi cấu trúc gói tin. NIDS có thể là phần mềm triển khai trên server hoặc dạng thiết bị tích hợp appliance.

**Host Base IDS(HIDS)** là hệ thống phát hiện xâm nhập host.

Theo dõi các hoạt động bất thường trên các host riêng biệt . HIDS được cài đặt trực tiếp trên các máy(host) cần theo dõi.

**Ựu nhược điểm của HIDS**

* **Ưu điểm:**

**+** Có khả năng xác định người dùng liên quan tới một sự kiện

+HIDS có khả năng phát hiện các cuộc tấn công diễn ra trên một máy.

+Có thể phân tích các dữ liệu mã hóa.

+Cung cấp các thông tin về host trong lúc tấn công diễn ra.

* **Nhược điểm:**

**+**Thông tin từ HIDS là không đáng tin cậy ngay khhi sự tấn công vào host này thành công.

**+**Khi hệ điều hành bị hạ do tấn công, đồng thời HIDS cũng bị hạ .

+HIDS phải được thiết lập trên từng host giám sát.

+HIDS không có khả năng phát hiện các cuộc thăm dò mạng.

+HIDS cần tài nguyên Host để hoạt động.

+Đa số chạy trên hệ điều hành Window . Tuy nhiên cũng có một số chạy trên linux chặng hạng Ubuntu

**Các hoạt động của HIDS**

Khi các lượng được truyền tải đến host chúng được phân tích và đưa qua các host nếu hệ thống không phát hiện thấy các gói tin mang mã nguy hiểm bên trong. HIDS thường được sử dụng cho các máy tính nội bộ trong khi đó NIDS được dùng cho cả một mạng . HIDS thường được sử dụng cho nền Window trong thế giời máy tính , tuy nhiên cũng có nhiều sản phẩm cũng có thể hoạt động trong môi trường UNIX và các hệ điều hành khác.

1. **Hệ thống luật**

Tập luật là thành phần quan trọng nhất của một hệ thống phát hiện xâm nhập.Đây là tập sẽ định ra dấu hiệu (Mẫu) để so sánh , đối chiếu với dữ liệu ở đầu vào. Thông thường , tập luật bao gồm rất nhiều luật, mội luật sẽ gồm 2 thành phần cơ bản: Rule Header và Rule Options.

Rule Header bao gồm các thông tin sau:

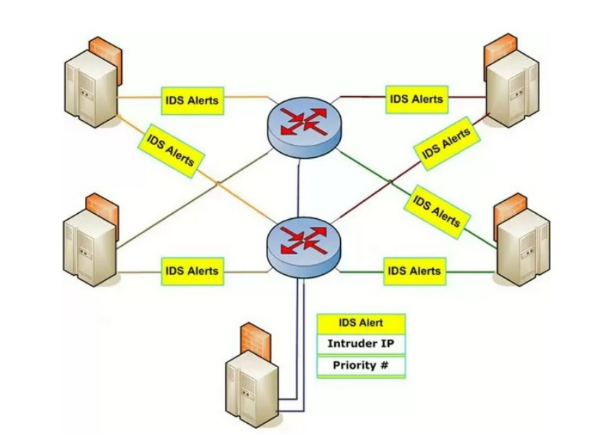
* Rule Action: cho biết các hoạt động sẽ được thực thi khi “khớp” luật (alert,log,pass,active,dynamic,drop,…)
* Protocol: Cho biết giao thức kiểm tra (TCP,UDP,ICMP,IP,..)
* IP address: cho biết thông tin về dịa chỉ IP.
* Port number: cho biết thông tin về cổng.
* Direction: Cho biết hướng của dữ liệu mà được khớp.

Rule options chia làm 4 danh mục:

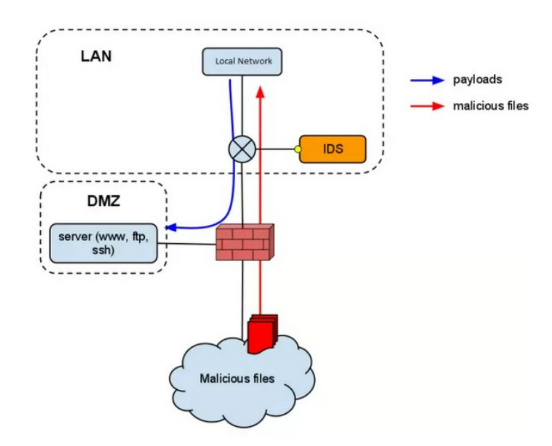
* General: cung cấp thông tin chung về luật(msg,reference,rev,classtype,…)
* Non-Payload: Tìm kiếm nội dung non-payload của gói tin(ttl,ack,id,dsize,..)
* Payload: Tìm kiếm nội dung payload của gói tin (content,offset,depth,distance,withim,..)
* Post-detection: cung cấp các phương pháp thực thi kế tiếp(logto,session,tag,..)

1. **Thiết kế:**

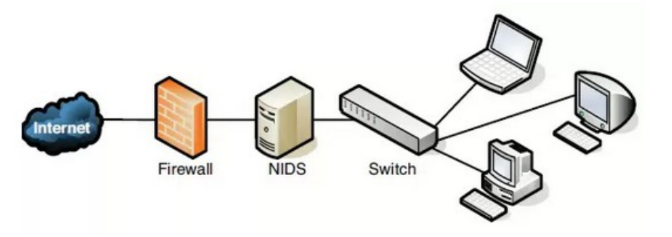
Đặt giữa router và firewall



Đặt trong miền DMZ



Đặt sau Firewall



1. **Giới thiệu về Ossec.**

### 1. Giới thiệu về ossec

a) Ossec là gì?

* Ossec là phần mềm mã nguồn mở giúp phát hiện xâm nhập dựa trên host( HIDS).
* Nó đa nền tảng, có thể mở rộng và có nhiều cơ chế bảo mật khác nhau.

\*)Ossec và IDS ( HIDS is **Host-based IDS)**

+ **IDS**là hệ thống phát hiện các dấu hiệu của tấn công xâm nhập, đồng thời có thể khởi tạo các hành động trên thiết bị khác để ngăn chặn tấn công.

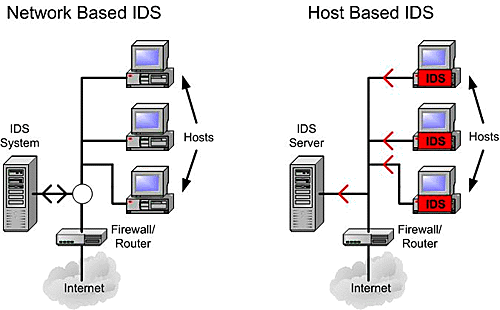
**Khác với firewall**, **IDS**không thực hiện các thao tác ngăn chặn truy nhập mà chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo cho người quản trị mạng.

Một điểm khác biệt khác đó là mặc dù cả hai đều liên quan đến bảo mật mạng

* **Firewall** theo dõi sự xâm nhập từ bên ngoài và ngăn chặn chúng xảy ra, nó giới hạn truy nhập giữa các mạng để ngăn chặn sự xâm nhập nhưng không phát hiện được cuộc tấn công từ bên trong mạng.
* **IDS**sẽ đánh giá sự xâm nhập đáng ngờ khi nó đã diễn ra đồng thời phát ra cảnh báo, nó theo dõi được cả các cuộc tấn công có nguồn gốc từ bên trong một hệ thống.

Chức năng ban đầu của IDS chỉ là phát hiện các dấu hiện xâm nhập, do đó IDS chỉ có thể tạo ra các cảnh báo tấn công khi tấn công đang diễn ra hoặc thậm chí sau khi tấn công đã hoàn tất. Càng về sau, nhiều kỹ thuật mới được tích hợp vào IDS, giúp nó có khả năng dự đoán được tấn công (prediction) và thậm chí phản ứng chủ động khi cuộc tấn công diễn ra (Active response).

\*) **HIDS và NIDS**

[](https://github.com/PhamKhahn/thuctapsinh/blob/master/KhanhPQ/Ossec/IDS.gif)

Trước khi nói về Ossec, tôi muốn bạn biết thêm về 2 khái niệm này:

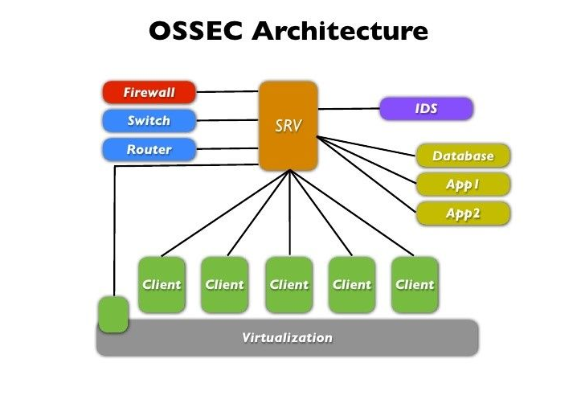
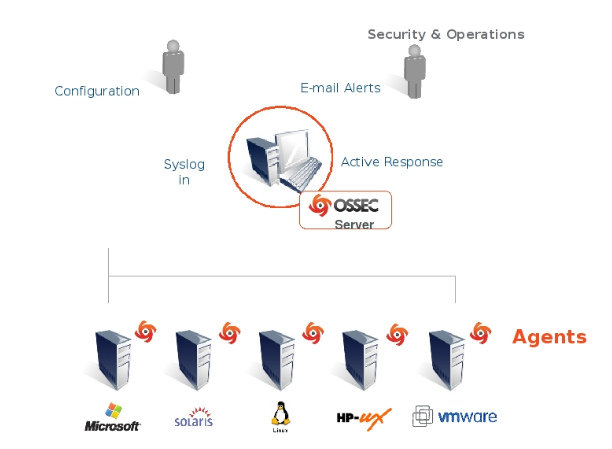
* **Network-based IDS (NIDS)**: Là những IDS giám sát trên toàn bộ mạng. Nguồn thông tin chủ yếu của NIDS là các gói dữ liệu đang lưu thông trên mạng. NIDS thường được lắp đặt tại ngõ vào của mạng, có thể đứng trước hoặc sau firewall.
* **Host-based IDS (HIDS)**: Là những IDS giám sát hoạt động của từng máy tính riêng biệt. Do vậy, nguồn thông tin chủ yếu của HIDS ngoài lưu lượng dữ liệu đến và đi từ máy chủ còn có hệ thống dữ liệu nhật ký hệ thống (system log) và kiểm tra hệ thống (system audit).

b) Các chức năng của ossec.

* Log based Intrusion Detection (LIDs) and Log Monitoring:
  + Chủ động theo dõi và phân tích dữ liệu real-time từ nhiều nguồn sinh log.
  + Ngoài ra, Ossec sẽ thu thập,phân tích và kiểm tra mối tương quan các log và cho ta biết những điều đáng ngờ đang xảy ra trong hệ thống (bị tấn công, lỗi, sử dụng sai,..),các phần mềm được cài đặt thêm, các rule firewall bị đổi.
* Compliance Auditing:
  + Kiểm soát các ứng dụng và hệ thống nhằm tuân thủ các yêu cầu, tiêu chuẩn về bảo mật như PCI-DSS và CIS.
* Rootkit and Malware Detection:
  + Tin tặc thường muốn che dấu hành động và quay lại hệ thống đã xâm nhập được
  + Ossec phân tích ở cấp độ file và tiến trình nhằm phát hiện các ứng dụng độc hại, các rootkit hay các file hệ thống bị sửa đổi theo cách phổ biến với rootkit
* File Integrity Monitoring (FIM):
  + Phát hiện các thay đổi đối với hệ thống.
* Active Response:
  + Các hành vi ứng phó lại các cuộc tấn công vào hệ thống trong thời gian thực.
  + Giúp ngăn sự cố lan rộng trước khi admin có thể hành động
* System Inventory:
  + Thu thập các thông tin hệ thống như phần mềm được cài đặt, harware,…

c) Hoạt động của ossec:

Ossec hoạt động theo mô hình Server-Agent/Agentless

[](https://github.com/PhamKhahn/thuctapsinh/blob/master/KhanhPQ/Ossec/Kien_truc1.png)[](https://github.com/PhamKhahn/thuctapsinh/blob/master/KhanhPQ/Ossec/Kientruc2.png)

**c.1. Manager (Server)**

Lưu trữ cơ sở dữ liệu của việc kiểm tra tính toàn vẹn file

Kiểm tra các log, event.

Quản lý, lưu tất cả các rule, decoder (bộ giải mã), cấu hình chính. Điều này giúp dễ dàng quản lý, dù cho có lượng lớn Agent

Server không chạy trên Windows OS.

**c.2. Agent**

Bản chất thì là 1 phần mềm được cài đặt trên máy client giúp thu thập các thông tin và gửi cho Server để phân tích, thống kê.

* Chiếm lượng memory và CPU nhỏ,không đáng kể
* 1 số thông tin được thu thập theo thời gian thực
* 1 số thông tin thì lại được thu thập định kỳ

Nhưng khi nói Agent thì là để chỉ máy Client được cài gói Ossec-agent.

*Chú ý:*

* Windows OS chỉ có thể làm Agent chứ không làm Server được.

**c.3. Agentless**

Là các hệ thống không cài được gói agent

Trên các Agentless này có thể thực hiện việc kiểm tra tính toàn vẹn

Giúp monitor firewall, router hay thậm chí cả hệ thống Unix

**c.4. Ảo hóa/ VMware**

Cho phép cài đặt agent trên các guest OS (Máy ảo)

Ngoài ra cũng được cài đặt trong VMware ESX nhưng có thể dẫn đến sự cố không hỗ trợ.

Khi cài đặt trong VMware ESX giúp nhận được thời điểm các VM guest được khởi tạo, xóa đi, khởi động,.. Ossec cũng giám sát việc login,logouts và các lỗi bên trong ESX server

Ngoài ra nó cũng cảnh báo nếu bất kỳ tùy chọn cấu hình không an toàn nào được bật.

**c.5. Firewalls, switches and routers**

Chính là các Agentless

Ossec có thể nhận và phân tích nhật ký hệ thống từ nhiều firewall, switch, router.

Nó support tất cả Cisco routers, Cisco PIX, Cisco FWSM, Cisco ASA, Juniper Routers, Netscreen firewall, Checkpoint và nhiều thiết bị khác.

* 1. **Cài đặt ossec:**

Đầu tiên bạn cần cập nhật hệ thống của mình với phiên bản ổn định nhất bằng lệnh:

apt-**get** update -y

apt-**get** upgrade -y

Ossec yêu cầu cài gcc, libc, apache và Php. Có thể cài tất cả các gói bằng lệnh sau:

apt-**get** install build-essential gcc make apache2 libapache2-mod-php7.0 php7.0 php7.0-cli php7.0-common apache2-utils unzip wget sendmail inotify-tools -y

Tiếp theo tải xuống phiên bản mới nhất của ossec:

wget https://github.com/ossec/ossec-hids/archive/2.9.0.tar.gz

Giải nén tập tin vừa tải xuống:

tar -xvzf 2.9.0.tar.gz

Di chuyển đến thư mục giải nén:

cd ossec-hids-2.9.0

Chạy install.sh để cài đặt ossec:

sh install.sh

Bạn sẽ cần trả lời một số câu hỏi:

Chọn ngôn ngữ của bạn là Tiếng Anh và enter:

(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]:en

Sau khi nhấn sẽ hiện lên:

OSSEC HIDS v2.9.0 Installation Script - http://www.ossec.net

You are about to start the installation process **of** the OSSEC HIDS.

You must have a C compiler pre-installed **in** your system.

- System: Linux Node1 4.4.0-45-**generic**

- User: root

- Host: localhost

-- Press ENTER to **continue** **or** Ctrl-C to abort. --

Tiếp tục nhấn enter câu hỏi hiện ra đầu tiên:

Chọn kiểu cài đặt mà bạn mong muốn, ở đây tôi chọn local.

1- What kind **of** installation **do** you want (server, agent, **local**, hybrid **or** help)? **local**

Sau đó nhấn enter và tiếp tục chọn vị trí cài đặt như sau:

- Server installation chosen.

2- Setting up the installation environment.

- Choose **where** to install the OSSEC HIDS [/var/ossec]:

Sau đó là lựa chọn có gửi vô email không? Ở đây tôi chọn n.

- Installation will be made at /**var**/ossec .

3- Configuring the OSSEC HIDS.

3.1- Do you want e-mail notification? (y/n) [y]: n

Nhấn enter để kiểm tra tính toàn vẹn deamon:

3.2- Do you want to run the integrity check daemon? (y/n) [y]:

- Running syscheck (integrity check daemon).

Nhấn enter để cho công cụ phát hiện rootkit:

3.3- Do you want to run the rootkit detection engine? (y/n) [y]:

- Running rootcheck (rootkit detection).

Nhấn enter để bật phản hồi hoạt động:

- Do you want to enable active response? (y/n) [y]:

- Active response enabled.

Nhấn enter để bật phản hồi tường lửa:

- Do you want to enable the firewall-drop response? (y/n) [y]:

- firewall-drop enabled (**local**) **for** levels >= 6

Gõ n và nhấn enter nếu bạn không muốn thêm nhiều Ip vào danh sách trắng:

- Default white list **for** the active response:

- 192.168.15.1

- Do you want to **add** more IPs to the white list? (y/n)? [n]: n

Nhấn enter để bật syslog từ xa:

3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]:

- Remote syslog enabled.

- If you want to monitor any other file, just change the

ossec.conf **and** **add** a **new** localfile entry.

Any questions about the configuration can be answered

**by** visiting us online at http://www.ossec.net .

--- Press ENTER to **continue** ---

Nhấn enter để bắt đầu cài đặt. Sau khi cài đặt xong hãy khởi động nó lên bằng lệnh:

/var/ossec/bin/ossec-control start

Để tiện lợi cho việc sử dụng và quản lí ta cần cài đặt giao diện người dùng Web ossec:

Đầu tiên ta cài đặt phiên bản mới nhất của nguồn UI ossec từ kho github:

/var/ossec/bin/ossec-control start

Giải nén nó:

unzip master.zip

Tiếp theo di chuyển thư mục giải nén đó vào thư mục gốc apache:

mv ossec-wui-master /**var**/www/html/ossec

Di chuyển đến thư mục và cài đặt ossec web UI bằng câu lệnh sau:

cd /**var**/www/html/ossec

./setup.sh

Điền thông tin vào hình dười đây gồm tên user và password:

trap: SIGHUP: bad trap

Setting up ossec ui...

Username: admin

New password:

Re-type **new** password:

Nhập tên người dùng máy chủ web của bạn là www-data

Adding password **for** user admin

Enter your web server user name (e.g. apache, www, nobody, www-data, ...)

www-data

You must restart your web server after **this** setup **is** **done**.

Setup completed successfully.

Cuối cùng khời động lại apache2:

systemctl restart apache2

Sau khi xong bạn có thể vào trình duyệt gõ: https:// Ip máy của bạn/ossec nhấn enter:

* 1. **Demo giao diện**

**Rules Syntax (Quy tắc cú pháp)**

Đầu tiên, các quy tắc có 0 cấp được thử, và sau đó tất cả các quy tắc khác theo thứ tự giảm dần theo cấp độ của chúng. Nếu mức độ giống nhau, thứ tự sẽ được quyết định dựa trên danh sách quy tắc trong tệp /var/ossec/etc/ossec.conf. Lưu ý, đối với các quy tắc có một số yêu cầu (ví dụ if\_sid), yêu cầu này được thử trước tiên.

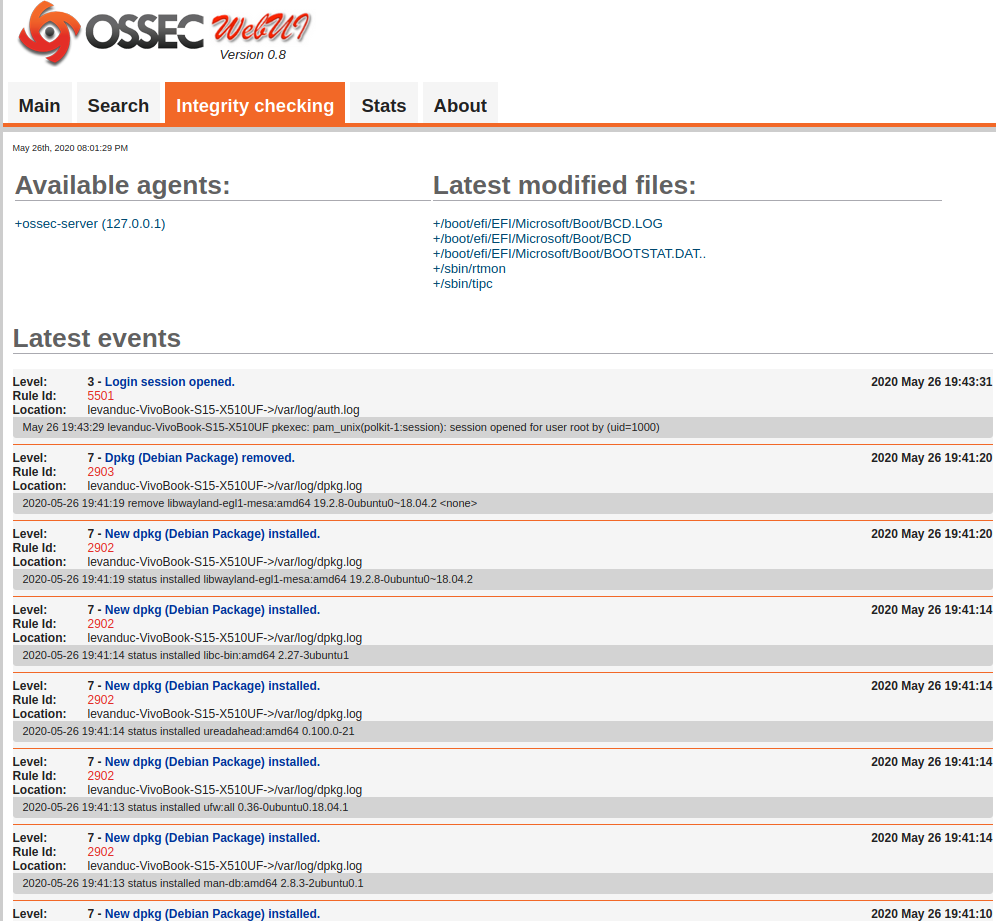
**Thuộc Tính:**

* **Level :** Chỉ định cấp độ của quy tắc. Cảnh báo và phản hồi sử dụng giá trị này. Được phép: Bất kỳ số nào (0 đến 16)
* **Location**: Vị trí
* **Rule Id:** Chỉ định ID của quy tắc.Được phép: Bất kỳ số nào từ 100 đến 99999

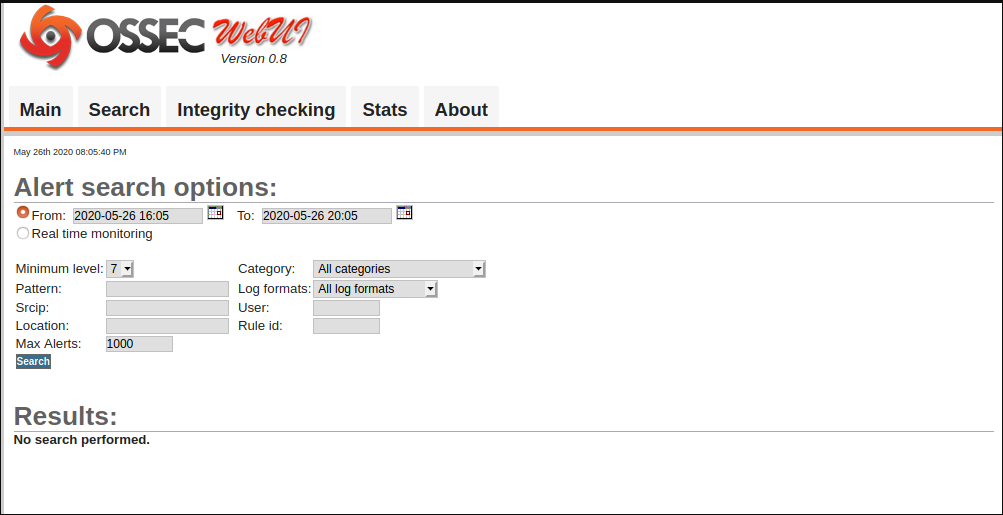
# Đăng giám sát / phân tích

Phân tích nhật ký (hoặc kiểm tra nhật ký) được thực hiện bên trong OSSEC bởi các quy trình logcollector và phân tích. Cái đầu tiên thu thập các sự kiện và cái thứ hai phân tích (giải mã, lọc và phân loại) chúng.

Nó được thực hiện trong thời gian thực, vì vậy ngay khi một sự kiện được viết, OSSEC sẽ xử lý chúng. OSSEC có thể đọc các sự kiện từ các tệp nhật ký nội bộ, từ nhật ký sự kiện Windows và cũng có thể nhận chúng trực tiếp qua syslog từ xa.

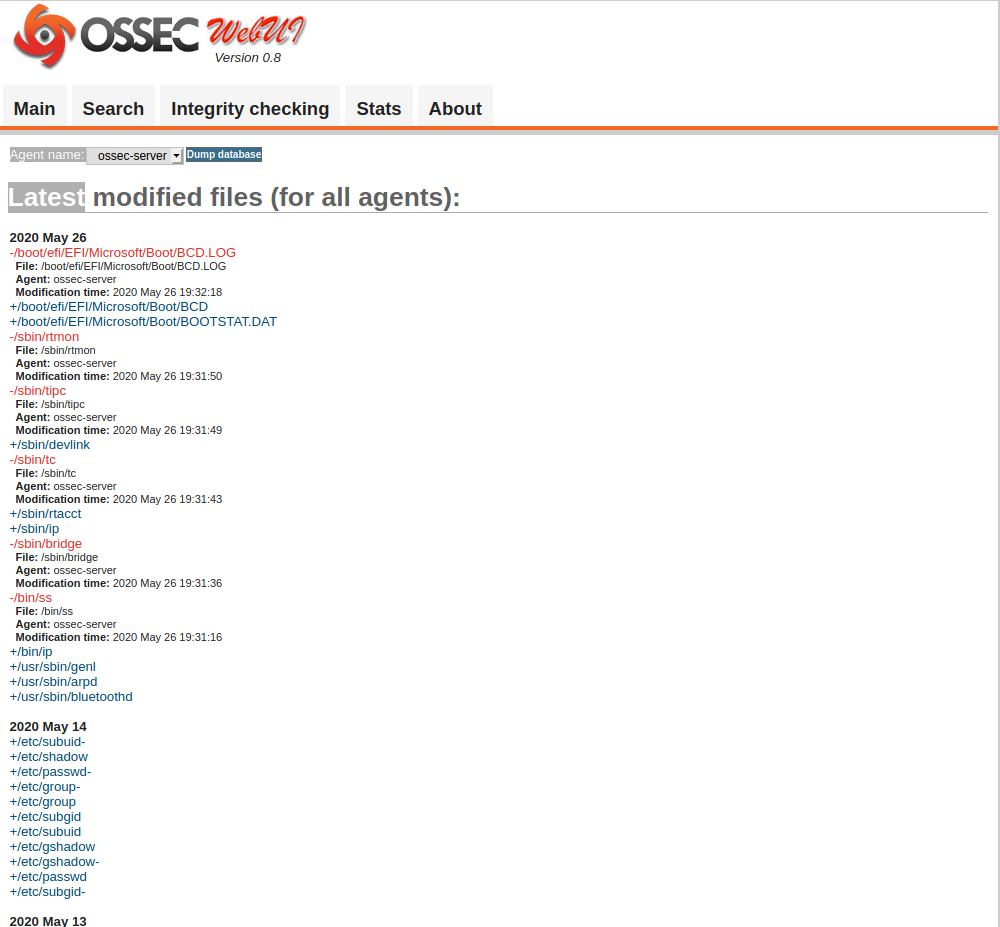


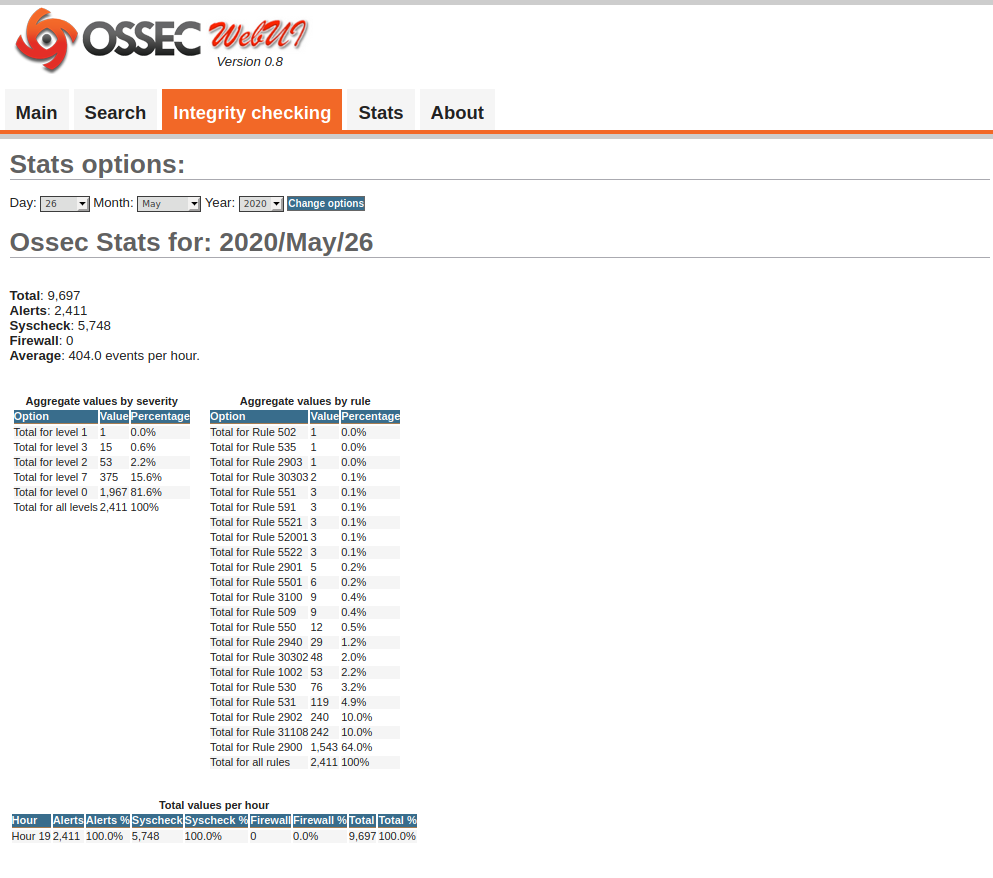
Tiếp theo là tìm kiếm trên giao diện: Dùng để kiểm tra và tìm kiếm lại các thông báo cũ theo các ngày trong khoảng thời gian hoặc thuộc tính nào đó:



# Syscheck

Syscheck là tên của quy trình kiểm tra tính toàn vẹn bên trong OSSEC. Nó chạy định kỳ để kiểm tra xem bất kỳ tệp được cấu hình





# B. FAQ

## Phân tích nhật ký là gì?

Trong OSSEC, chúng tôi gọi phân tích nhật ký là LIDS hoặc phát hiện xâm nhập dựa trên nhật ký. Mục tiêu là phát hiện các cuộc tấn công, sử dụng sai hoặc lỗi hệ thống bằng cách sử dụng nhật ký.

LIDS - Phát hiện xâm nhập dựa trên nhật ký hoặc phân tích nhật ký bảo mật là các quy trình hoặc kỹ thuật được sử dụng để phát hiện các cuộc tấn công vào một mạng, hệ thống hoặc ứng dụng cụ thể sử dụng nhật ký làm nguồn thông tin chính. Nó cũng rất hữu ích để phát hiện lạm dụng phần mềm, vi phạm chính sách và các hình thức hoạt động không phù hợp khác.

## Tại sao kiểm tra tính toàn vẹn?

Có nhiều loại tấn công và nhiều vectơ tấn công, nhưng có một điều duy nhất về tất cả chúng: chúng để lại dấu vết và luôn thay đổi hệ thống theo một cách nào đó. Từ các virus sửa đổi một vài tệp, đến các rootkit cấp kernel làm thay đổi kernel, luôn có một số thay đổi về tính toàn vẹn của hệ thống.

Kiểm tra tính toàn vẹn là một phần thiết yếu của phát hiện xâm nhập, giúp phát hiện các thay đổi về tính toàn vẹn của hệ thống. OSSEC thực hiện điều đó bằng cách tìm kiếm các thay đổi trong tổng kiểm MD5 / SHA1 của các tệp chính trong hệ thống và trên sổ đăng ký Windows.

Cách thức hoạt động là nhân viên quét hệ thống cứ sau vài giờ (do người dùng xác định) và gửi tất cả tổng kiểm tra đến máy chủ. Máy chủ lưu trữ tổng kiểm tra và tìm kiếm sửa đổi trên chúng. Một cảnh báo được gửi nếu có gì thay đổ

Số liệu thống kê của ossec trên Stats:

## Nhật ký được lưu ở đâu?

Trên máy chủ OSSEC và cài đặt cục bộ, có một số loại nhật ký OSSEC. Có các nhật ký được tạo bởi các daemon OSSEC, các thông điệp tường trình từ các tác nhân và các cảnh báo. Cài đặt tác nhân không có nhật ký từ các tác nhân hoặc cảnh báo khác, nhưng có nhật ký được tạo bởi các quy trình OSSEC.

Tất cả các bản ghi được lưu trữ trong thư mục con của /var/ossec/logs. Thông điệp nhật ký OSSEC và được lưu trữ trong /var/ossec/logs/ossec.log

Thông điệp tường trình từ các tác nhân không được lưu trữ theo mặc định. Sau khi phân tích, chúng sẽ bị xóa trừ khi tùy chọn <logall> được bao gồm trong trình quản lý, ossec.conf. Nếu được đặt, tất cả các thông điệp tường trình được gửi tới người quản lý sẽ được lưu trữ trong /var/ossec/logs/archives/archives.log và được xoay vòng hàng ngày.

Cảnh báo được lưu trữ trong /var/ossec/logs/alerts/alerts.log.log và được luân chuyển hàng ngày.

## Nhật ký OSSEC có thể được lưu vào một thư mục khác không?

Là một cơ chế bảo vệ, OSSEC chroots hầu hết các quy trình của nó vào thư mục cài đặt (thường là /var/ossec). Do chroot này, các bản ghi phải được lưu vào một vị trí dưới /var/ossec. OSSEC không xoay vòng các bản ghi của nó, nhưng sẽ không thể di chuyển chúng từ /var/ossec.

Hãy chắc chắn phân bổ đủ không gian cho /var/ossec.

## Làm thế nào để bắt buộc quét syscheck ngay lập tức?

Chạy công cụ kiểm soát tác nhân để thực hiện kiểm tra tính toàn vẹn ngay lập tức (tùy chọn -a để chạy trên tất cả các tác nhân và -u để chỉ định id tác nhân)

**#** /var/ossec/bin/agent\_control -r -a

**#** /var/ossec/bin/agent\_control -r -u <agent\_id>

## Làm thế nào để bỏ qua một tập tin thay đổi quá thường xuyên?

Đặt tên tệp / thư mục trong tùy chọn <ign> hoặc tạo quy tắc cục bộ đơn giản.

Cái sau sẽ bỏ qua các tập tin / etc / a và / etc / b và thư mục / etc / dir cho các tác nhân mswin1 và ub Ubuntu-dns:

**<rule** id="100345" level="0" **>**

**<if\_group>**syscheck**</if\_group>**

**<description>**Changes ignored.**</description>**

**<match>**/etc/a|/etc/b|/etc/dir**</match>**

**<hostname>**mswin1|ubuntu-dns**</hostname>**

**</rule>**

# C. Tổng Kết.

Trên đây mới chỉ là những cái nhìn tổng quát nhất về những khái niệm, kiến trúc và cách thức hoạt động của một hệ thống phát hiện xấm nhập OSSEC, Hy vọng các bạn có thể tự cài đặt và cấu hình được một hệ thống phát hiện xâm nhập OSSEC trên hệ thống của mình. Xin cảm ơn!

**Đề tài:Tìm hiểu và triển khai hệ thống phát hiện xâm nhập ossec**

**Bảng phân chia công việc.**

|  |  |  |  |
| --- | --- | --- | --- |
| Họ Và Tên | MSV | Công việc | Tiến Độ |
| Lê Văn Đức | 175A071214 | - Cài đặt demo giao diện  - Hướng dẫn sử dụng  - Tổng quan về Ossec | Xong |
| Vũ Đức Đạt | 175A071221 | -So sánh ưu nhược điểm của NIDS và HIDS  - Triển khai và sử dụng Ossec  - FAQ | Xong |