# **I. Tổng quan về hệ thống phát hiện xâm nhập OSSEC:**

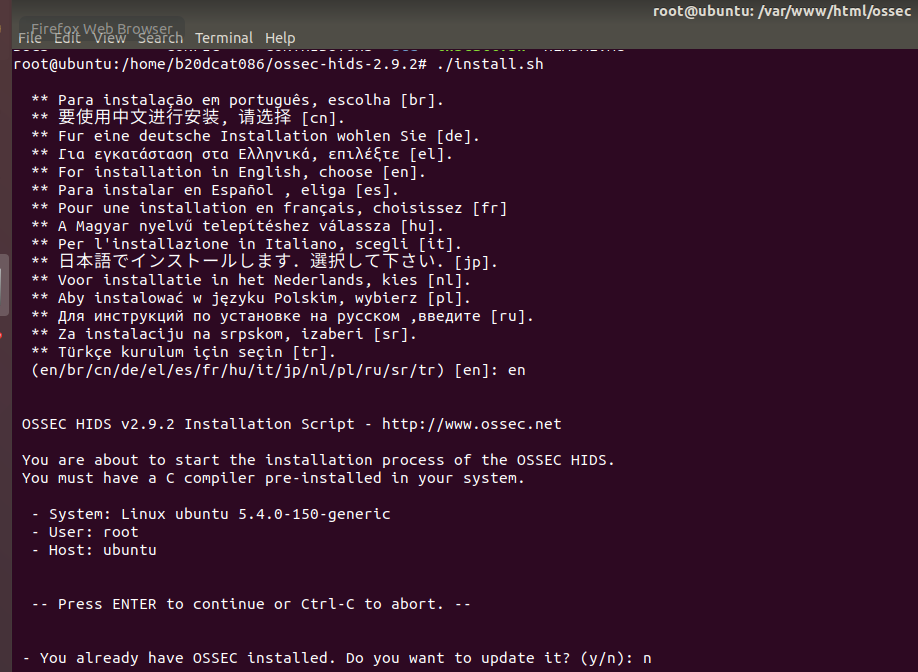
## 1. Giới thiệu:

OSSEC là hệ thống phát hiện xâm nhập dựa trên host (HIDS) dựa trên log mã nguồn mở, miễn phí, đa nền tảng có thể mở rộng và có nhiều cơ chế bảo mật khác nhau. OSSEC có thể phát hiện xâm nhập bằng cả chữ ký hoặc dấu hiệu bất thường. Các dấu hiệu bình thường và bất thường được mô tả trong bộ luật của OSSEC. OSSEC có một công cụ phân tích và tương quan mạnh mẽ, tích hợp giám sát và phân tích log, kiểm tra tính toàn vẹn của file, kiểm tra registry của Windows, thực thi chính sách tập trung, giám sát chính sách, phát hiện rootkit, cảnh báo thời gian thực và phản ứng một cách chủ động cuộc tấn công đang diễn ra.

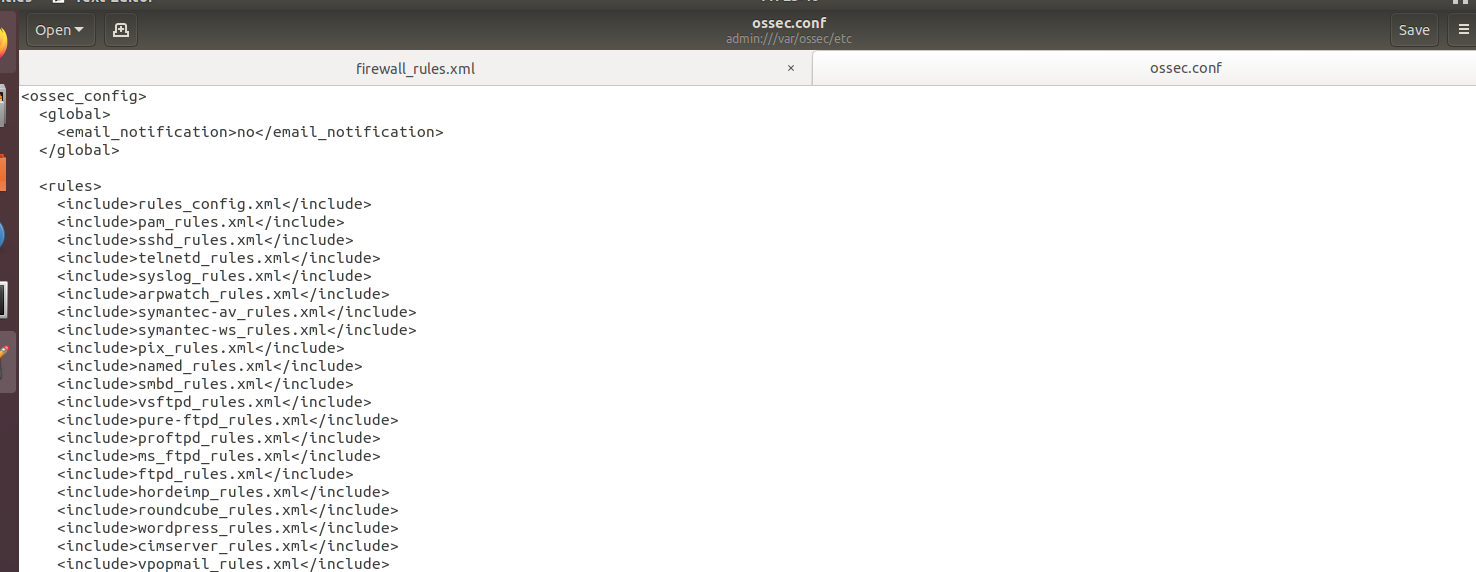
* Ưu điểm của HIDS:  
  HIDS có một số điểm cải tiến hơn so với NIDS:
  + Phù hợp với môi trường dữ liệu mã hóa ngày càng phổ biến. HIDS có khả năng đọc được các dữ liệu (log) được mã hóa tại server nhận.
  + Theo dõi được các tiến trình sử dụng của người dùng tại máy chủ.
  + Có khả năng phát hiện và phản ứng với thời gian thực.
  + Khắc phục các cuộc tấn công mà NIDS không thể cảnh báo được như tấn công phân mảnh hay ghép nối phiên.  
    **=>** Vì những lý do như vậy mà OSSEC được phát triển theo HIDS chứ không phải NIDS.
* Các tính năng nổi bật của OSSEC là:
  + **Theo dõi và phân tích các log:** OSSEC thu thập log theo thời gian thực từ nhiều nguồn khác nhau để phân tích (giải mã, lọc và phân loại) và đưa ra cảnh báo dựa trên bộ luật được xây dựng trước.
  + **Kiểm tra tính toàn vẹn của file:** Sử dụng hàm băm mật mã, có thể tính toán giá trị băm của mỗi file trong hệ điều hành dựa trên tên file, nội dung file và giá trị băm này là duy nhất. OSSEC có thể giám sát các ổ đĩa để phát hiện các thay đổi của giá trị băm này khi có ai đó, hoặc điều gì đó, sửa đổi nội dung của file hoặc thay thế phiên bản file này bằng một phiên bản file khác.

**II. Demo:**

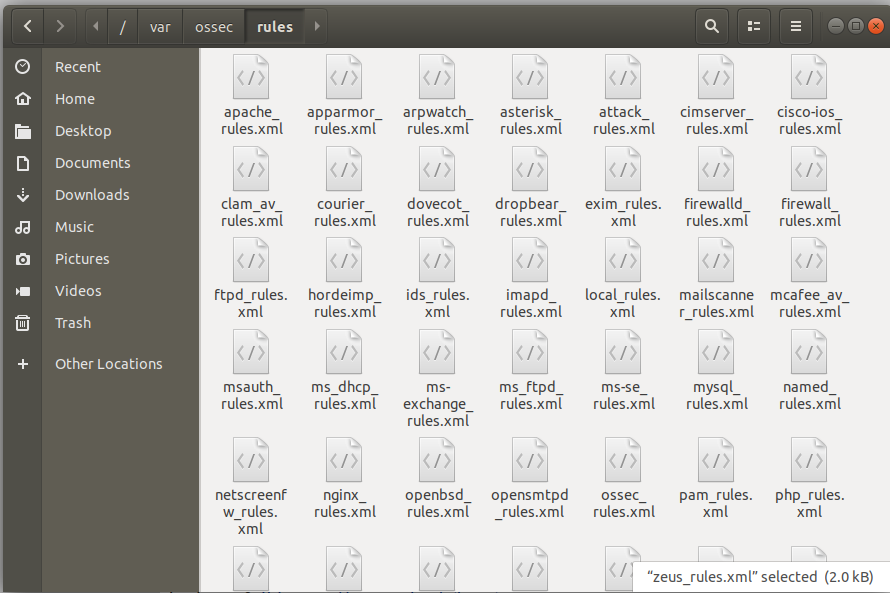
* Cài đặt OSSEC:



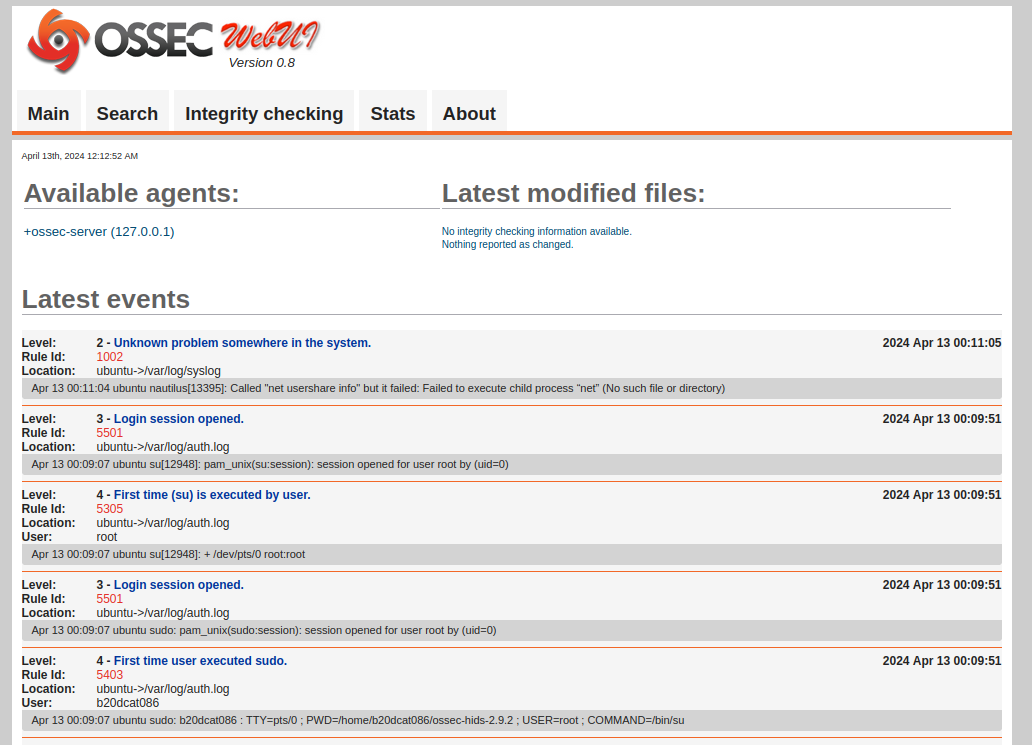
* Cấu hình file ossec.conf:



* Các luật phòng chống tấn công:



* Cảnh báo sẽ được hiển thị trên web:



# **Phát hiện quét cổng bằng OSSEC và iplog :**

* iplog là trình ghi lưu lượng truy cập TCP/IP. Hiện tại, nó có khả năng ghi lại lưu lượng TCP, UDP và ICMP. iplog có thể phát hiện các lần quét cổng TCP, quét null TCP, quét FIN, tấn công “smurf” UDP và ICMP, cờ TCP giả, quét TCP SYN, quét TCP “Xmas”, lũ ping ICMP, quét UDP và tấn công phân đoạn IP.
* iplog có thể chạy ở chế độ promiscuous và giám sát lưu lượng truy cập đến tất cả các máy chủ trên mạng. iplog sử dụng libpcap để đọc dữ liệu từ mạng và có thể được chuyển sang bất kỳ hệ thống nào hỗ trợ pthread và libpcap sẽ hoạt động trên đó.

## iplog: Scan and attack responses

## Connect Scan and SYN scan:

## 

## Iplog response:

## 

## FIN Stealth Scan:

## 

## Iplog response:

## 

## Triển khai OSSEC (HIDS) + iplog (cảm biến):

## -Thêm bộ giải mã (decoder) :

## 

## quy tắc iplog:

## -tạo file luật iplog\_rules.xml:

## 

## -thêm luật vào ossec.conf :

## 

## -và đường dẫn đến iplog:

## 

## -khởi động lại iplog.

## 

## -khởi động lại ossec.

## 

## Firewall Drop:

## Thêm vào tập lệnh ipfw:

## 

## /var/ossec/active-response/bin/firewall-drop.sh:

## 

## Thêm vào ossec.conf:

## 

## Khởi động lại ossec.

## Kiểm tra với nmap:

## .