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

**Mục Lục:**

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:

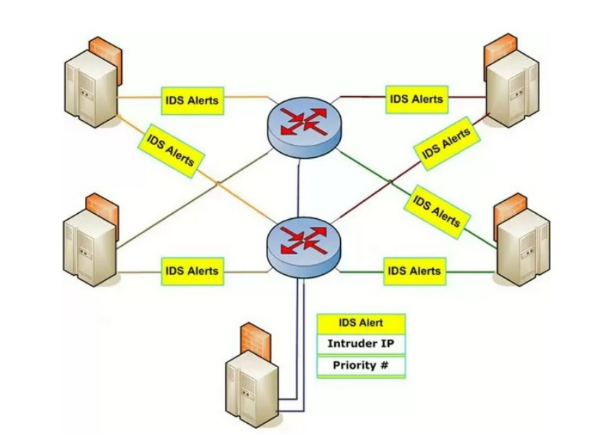
* Rule Action: cho biết các hoạt động sẽ được thực thi khi “khớp” luật (alert,log,pass,active,dynamic,drop,…)
* Protocol: Cho biết giao thức kiểm tra (TCP,UDP,ICMP,IP,..)
* IP address: cho biết thông tin về dịa chỉ IP.
* Port number: cho biết thông tin về cổng.
* Direction: Cho biết hướng của dữ liệu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

Rule options chia làm 4 danh mục:

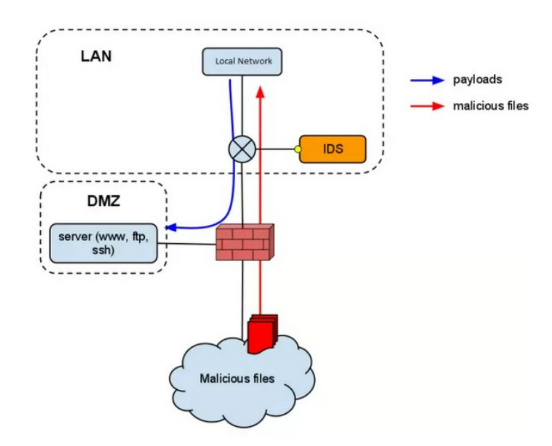
* General: cung cấp thông tin chung về luật(msg,reference,rev,classtype,…)
* Non-Payload: Tìm kiếm nội dung non-payload của gói tin(ttl,ack,id,dsize,..)
* Payload: Tìm kiếm nội dung payload của gói tin (content,offset,depth,distance,withim,..)
* Post-detection: cung cấp các phương pháp thực thi kế tiếp(logto,session,tag,..)

1. **Thiết kế:**

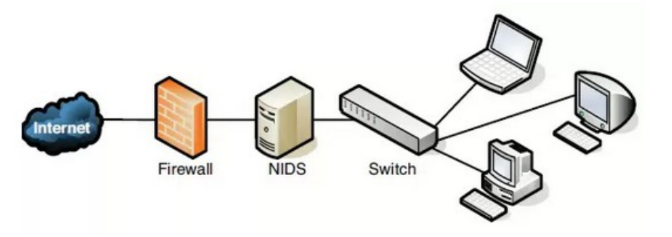
Đặt giữa router và firewall



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.

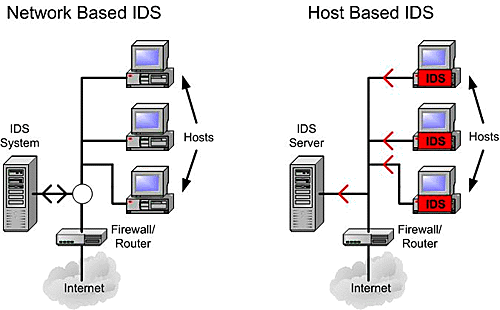
**Khác với firewall**, **IDS**không thực hiện các thao tác ngăn chặn truy nhập mà chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo cho người quản trị mạng.

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:

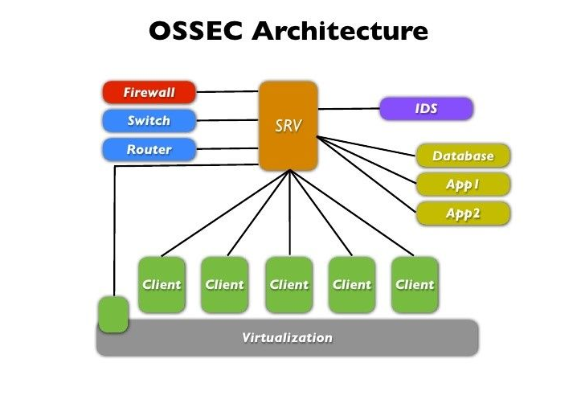
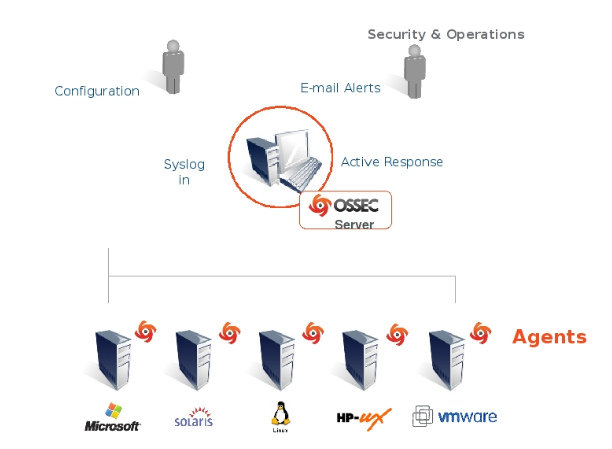
* **Network-based IDS (NIDS)**: Là những IDS giám sát trên toàn bộ mạng. Nguồn thông tin chủ yếu của NIDS là các gói dữ liệu đang lưu thông trên mạng. NIDS thường được lắp đặt tại ngõ vào của mạng, có thể đứng trước hoặc sau firewall.
* **Host-based IDS (HIDS)**: Là những IDS giám sát hoạt động của từng 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.