**CÀI ĐẶT HỆ THỐNG GIÁM SÁT AN NINH MẠNG ALIENVAULT**

Bài thực hành này sinh viên phải cấu hình các máy tính liên quan kết nối được với nhau trước khi cài các phần mềm.

Đối với máy chủ chạy hệ thống giám sát trung tâm AlienVault cần phải có cấu hình mạnh để hiện thị thông tin giám sát.

* 1. **Mô tả**

Để phát hiện kịp thời các cuộc tấn công mạng, cung cấp nguồn dữ liệu khi điều tra xử lý sự cố an toàn thông tin thì hệ thống giám sát an ninh mạng là một giải pháp tối ưu.

Bộ công cụ giám sát an ninh mạng mã nguồn mở AlienVault đáp ứng được hầu hết các yêu cầu của hệ thống. Do đó nó có thể được sử dụng trong học tập và nghiên cứu.

Trong nội dung bài thực hành này ứng dụng AlienVault để thu thập và phát hiện tấn công cho máy chủ chạy hệ điều hành Windows Server và Linux web server.

* 1. **Chuẩn bị**

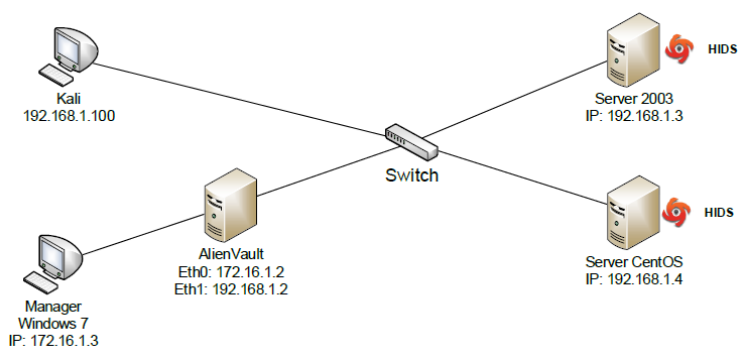
Mô hình này cần phải có 03 máy tính vật lý. Mỗi máy có chức năng như sau

+ Máy tính 01: Tạo máy ảo có RAM > 3GB. Để chạy hệ điều hành giám sát AlienVaut.

+ Máy tính 02: Tạo 02 máy ảo: Máy ảo chạy hệ điều hành Windows Server 2012 có mở cổng 3389 (Remote Desktop). Máy ảo chạy hệ điều hành Linux Ubuntu có cài đặt website.

+ Máy tính 03: Chạy máy ảo Kali Linux để tấn công, và cài đặt phần mềm Acunetix trên máy XP để quét lỗ hổng website

* 1. **Mô hình cài đặt**



Trong mô hình trên: máy chủ chạy hệ điều hành giám sát AlienVaul được kết nối vào mạng nội bộ. Và kết nối với máy vật lý Windows 7 để quản trị.

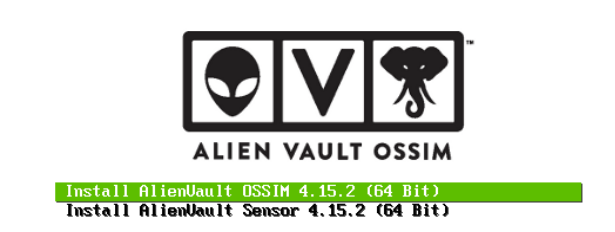
Máy Kali kết nối vào cùng mạng để tấn công.

Máy Server 2003 và CentOS chạy các dịch vụ Remote Desktop và web.

* 1. **Cài đặt máy chủ AlienVault**

Phần mềm máy chủ AlienVault đã được hãng sản xuất đóng gói thành bản ISO để cài đặt như hệ điều hành Linux.

Sau khi chèn đĩa cài đặt (file ISO) vào máy ảo, khởi động máy sẽ xuất hiện như hình sau:

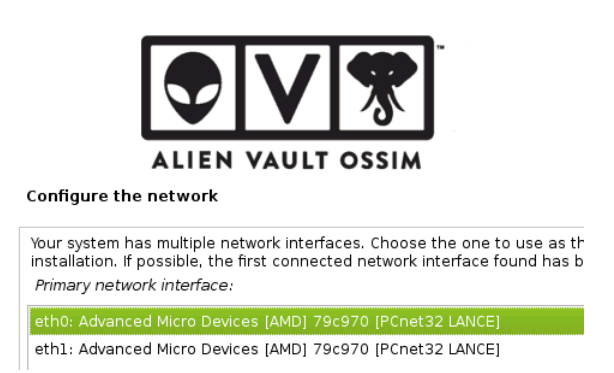


Nhấn Enter để bắt đầu cài đặt.

- Trong giao diện lựa chọn ngôn ngữ chọn English.

- Các giao diện tiếp theo chọn mặc định.

- Đến giao diện cấu hình mạng. Lựa chọn Interface mà kết nối với máy tính quản trị. Trong bài thực hành này chọn Eth0.



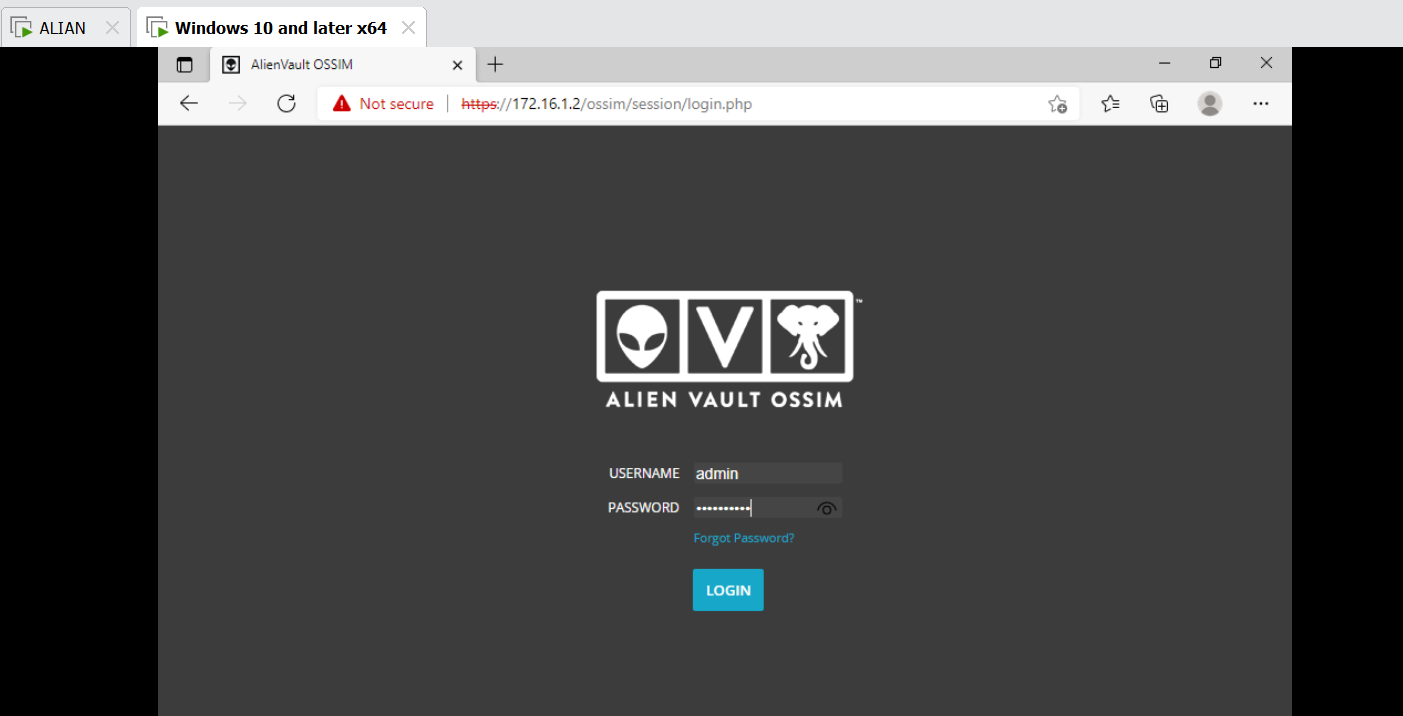
- Tiếp tục cấu hình địa chỉ IP của Interface này, đây là địa chỉ IP trong mạng quản lý. Theo mô hình mạng trên nó có IP là: 172.16.1.

- SubnetMask: 255.255.255.0, Gateway: 172.16.1.1

- Tiếp theo nhập mật khẩu cho tài khoản quản trị root

Với giao diện này người quản trị có thể cấu hình các chức năng của máy theo dòng lệnh với tùy chọn số 3 (Jailbreak System).

Giao diện sau khi cài đặt thành công và truy cập bằng trình duyệt web từ máy quản lý



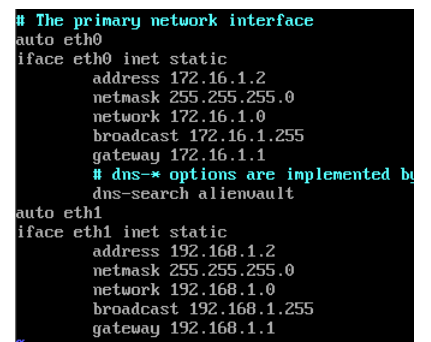
**1.5. Cấu hình máy chủ AlienVault**

**1.5.1. Cấu hình mạng giám sát**

Trong mục này cần phải cấu hình giao diện mạng cho máy chủ AlienVault để nhận thông tin gửi về từ các máy trạm cài bộ cảm biến (OSSEC client).

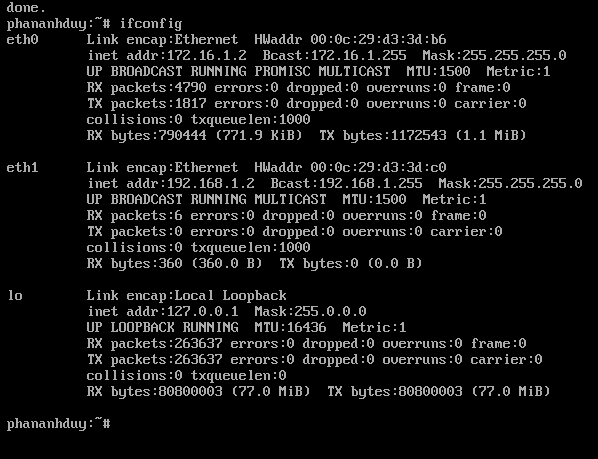
- Chọn mục 3 (Jailbreak System) như hình trên để vào giao diện cấu hình mạng bằng dòng lệnh.

- Truy cập theo đường dẫn và điền các thông tin như sau vào giao diện mạng Eth1: phananhduy:~# vi /etc/network/interfaces

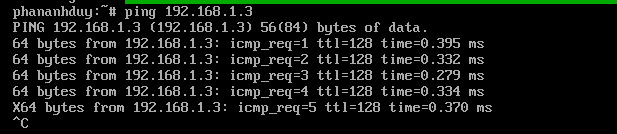


Khởi động lại cấu hình mạng

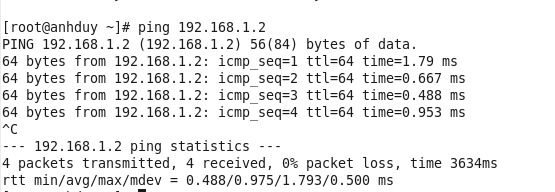
Kiểm tra lại cấu hình địa chỉ IP của các giao diện mạng



Kiểm tra kết nối với các máy tính Windows Server 2003 và Linux CentOS bằng lệnh Ping



Cấu hình mạng cho máy Linux Ubuntu

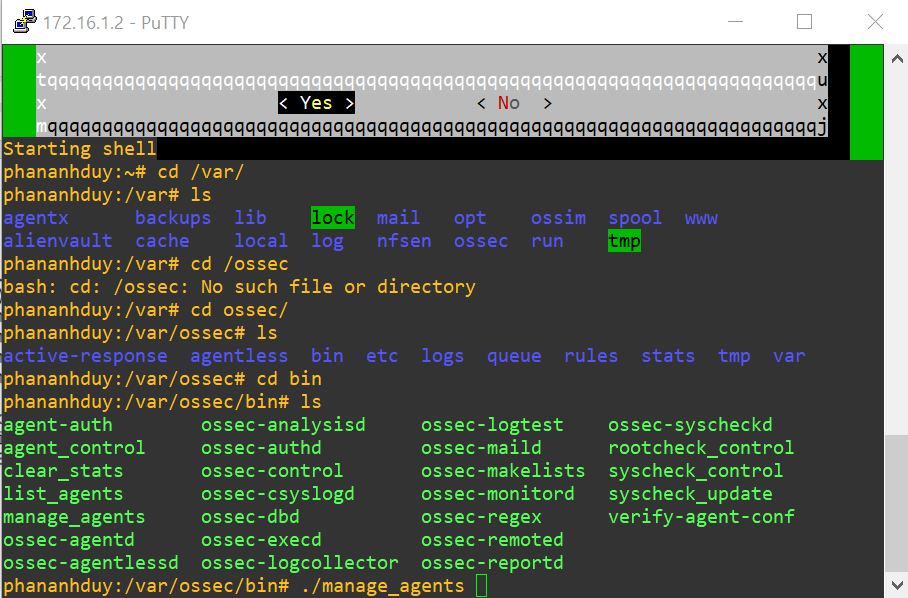


Kết quả kết nối thành công.

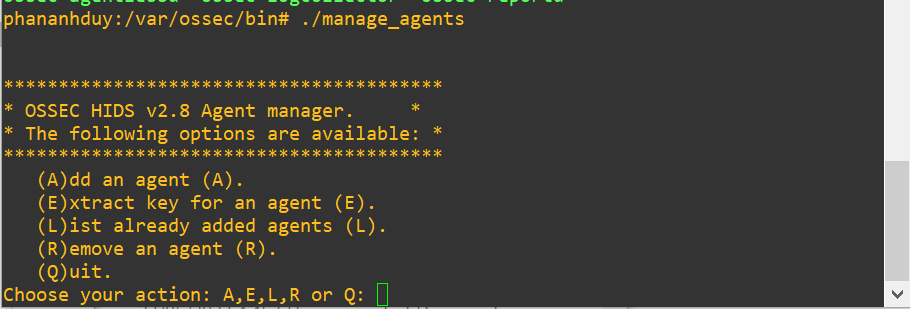
**1.5.2. Cấu hình bộ cảm biến OSSEC**

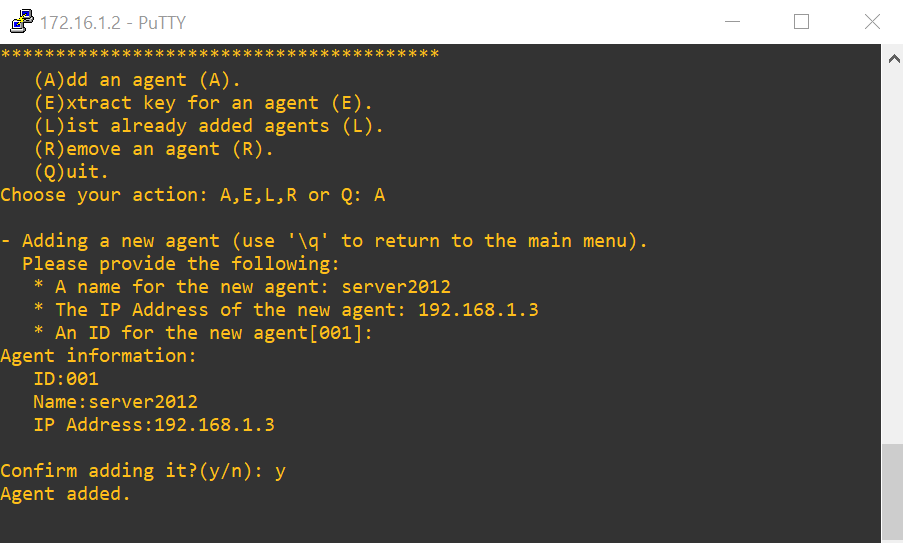
Sau khi cấu hình mạng hoàn tất, tiếp theo phải cấu hình các thông số về máy tính được giám sát bao gồm: tên máy, địa chỉ IP. Sau đó phải tạo khóa xác thực giữa máy chủ AlienVault và máy được giám sát.

Để làm được điều này cần sử dụng phần mềm kết nối thông qua giao thức SSH tới AlienVault. Sử dụng PuTTY để kết nối:

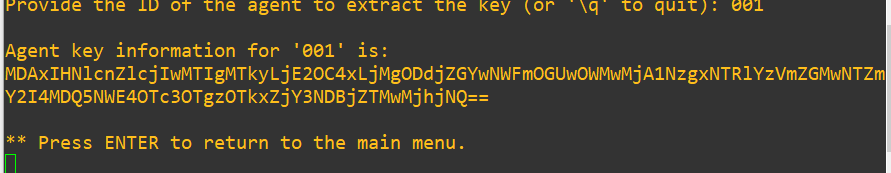
****

Chọn A để thêm thông tin về máy tính được giám sát

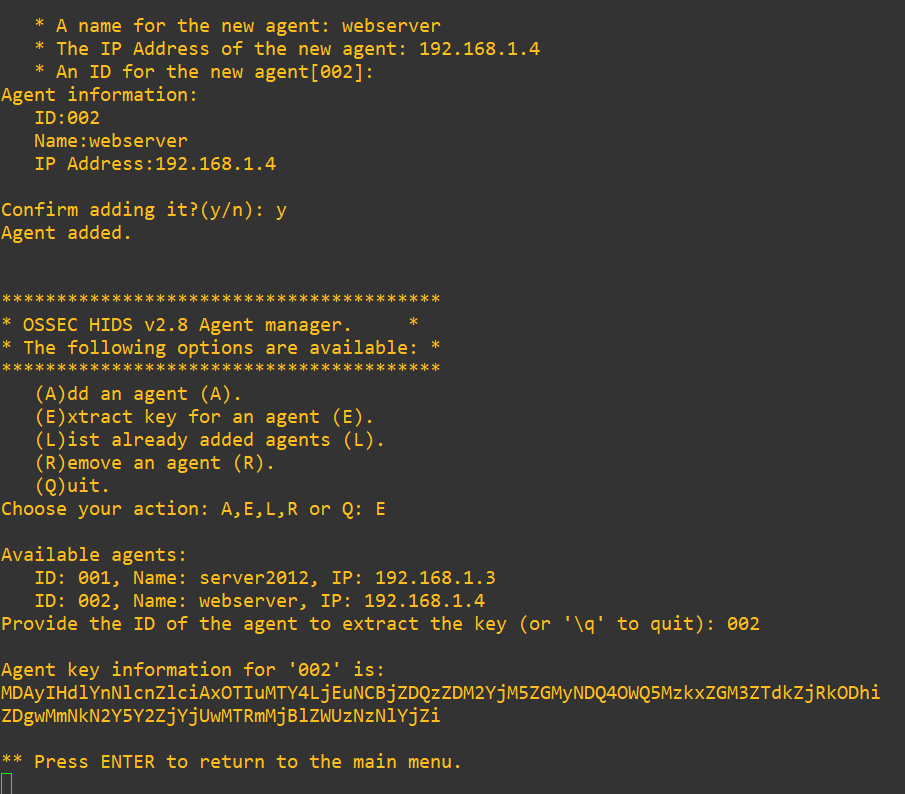
****

****

Tiếp tục chọn E để trích xuất khóa xác thực sử dụng cho máy Windows 2012

****

**Tương tự với Linux Ubuntu**

****

* 1. **Cài đặt và cấu hình OSSEC trên máy tính được giám sát**

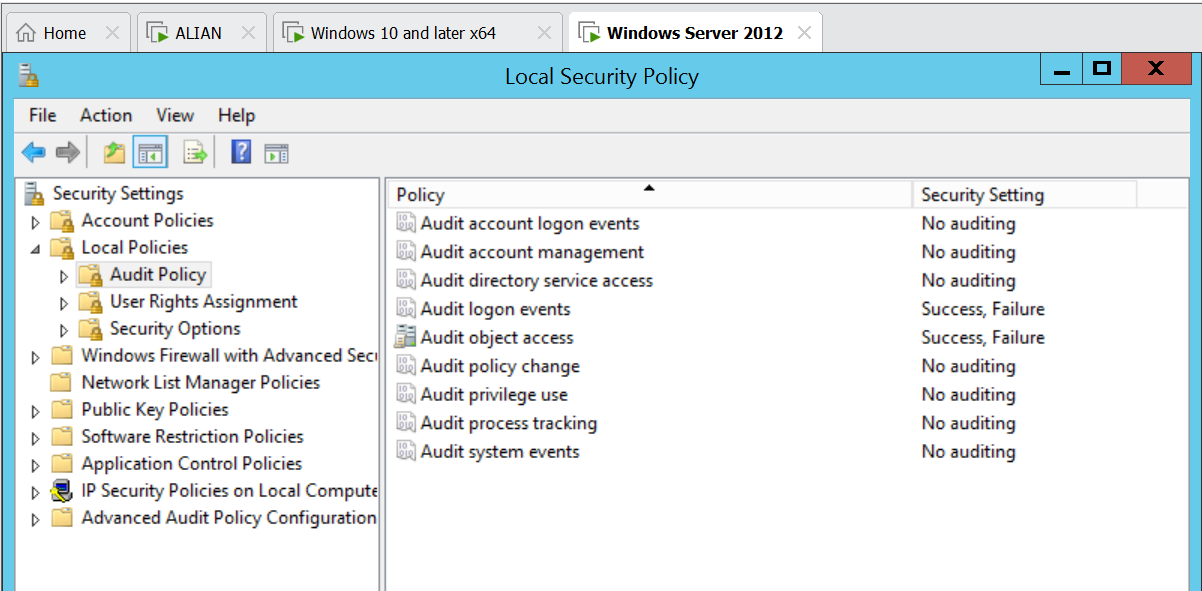
**1.6.1. Cài đặt và cấu hình OSSEC trên máy Windows**

Để thực hiện giám sát các hành vi tấn công tại các máy tính chạy Windows phải cài đặt công cụ phần mềm OSSEC client trên các máy đó. Khi có sự kiện xảy ra trên máy này OSSEC client sẽ gửi thông tin về máy chủ OSSEC (AlienVault) để phân tích và phát hiện hành vi tấn công.

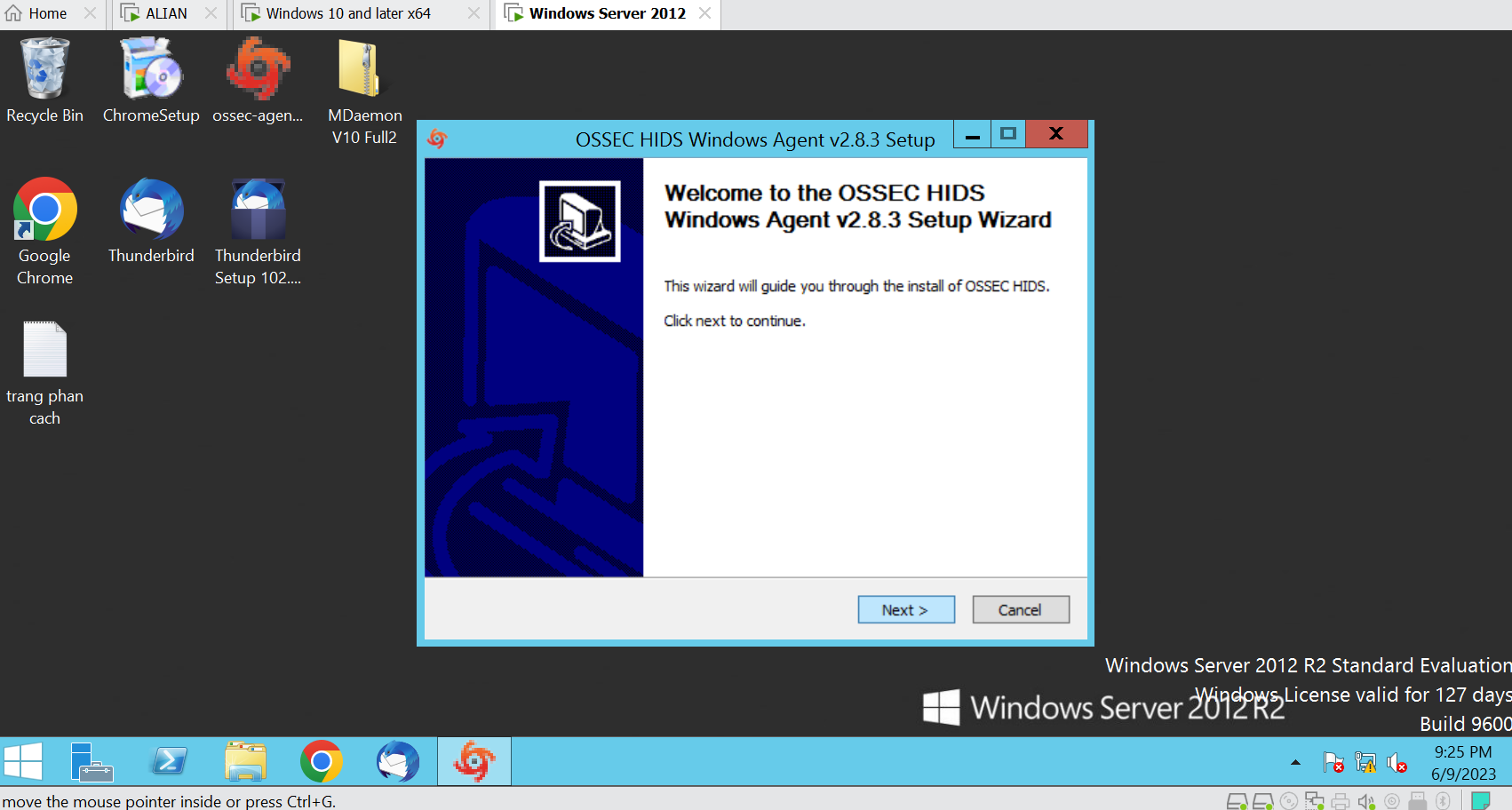
Kích hoạt chức năng ghi lại hành động đăng nhập bằng tài khoản của Windows Server 2003 bằng cách:

Start → Administrative Tools → Local Security Policy.

Trong mục Audit Policy kích hoạt ghi lại hành động đăng nhập cả thành công và thất bại

****

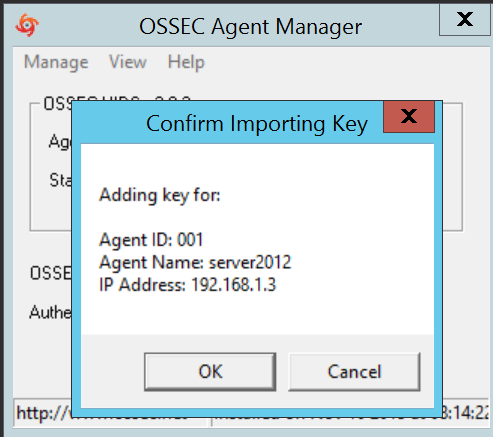
Tiếp theo cài đặt phầm mềm Ossec agent: Sao chép phần mềm ossec-agent-win32-2.8 vào máy Windows 2003 và cài đặt

****

Nhấn Next và cài đặt theo mặc định.

Sau khi cài đặt thành công nhập thông tin về máy chủ OSSEC: IP, Key Authention đã trích xuất ở bước trên.

Nhấn Save để lưu thông tin và truy cập vào Tab Manage → Start OSSEC để chạy ứng dụng.

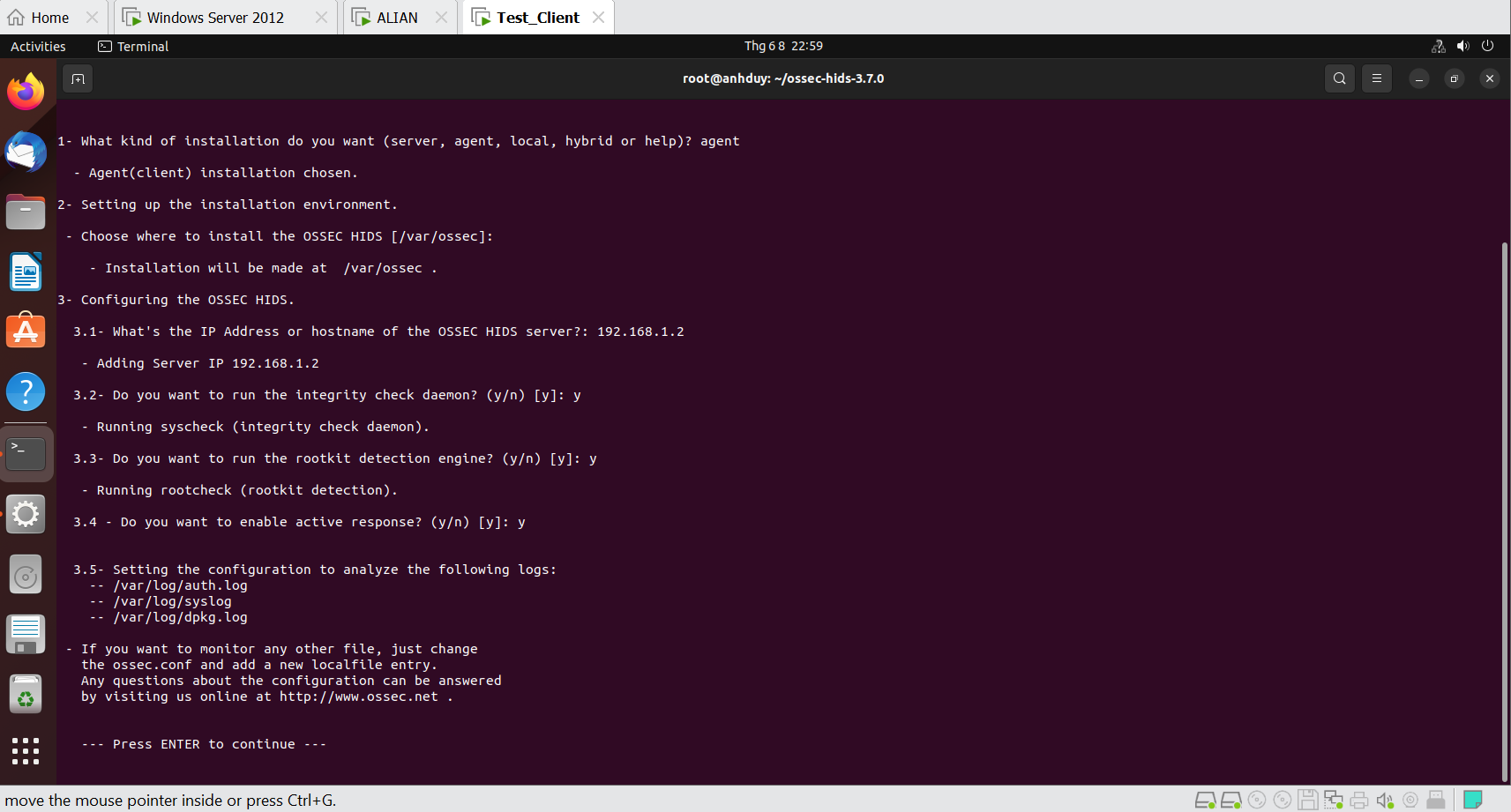
****

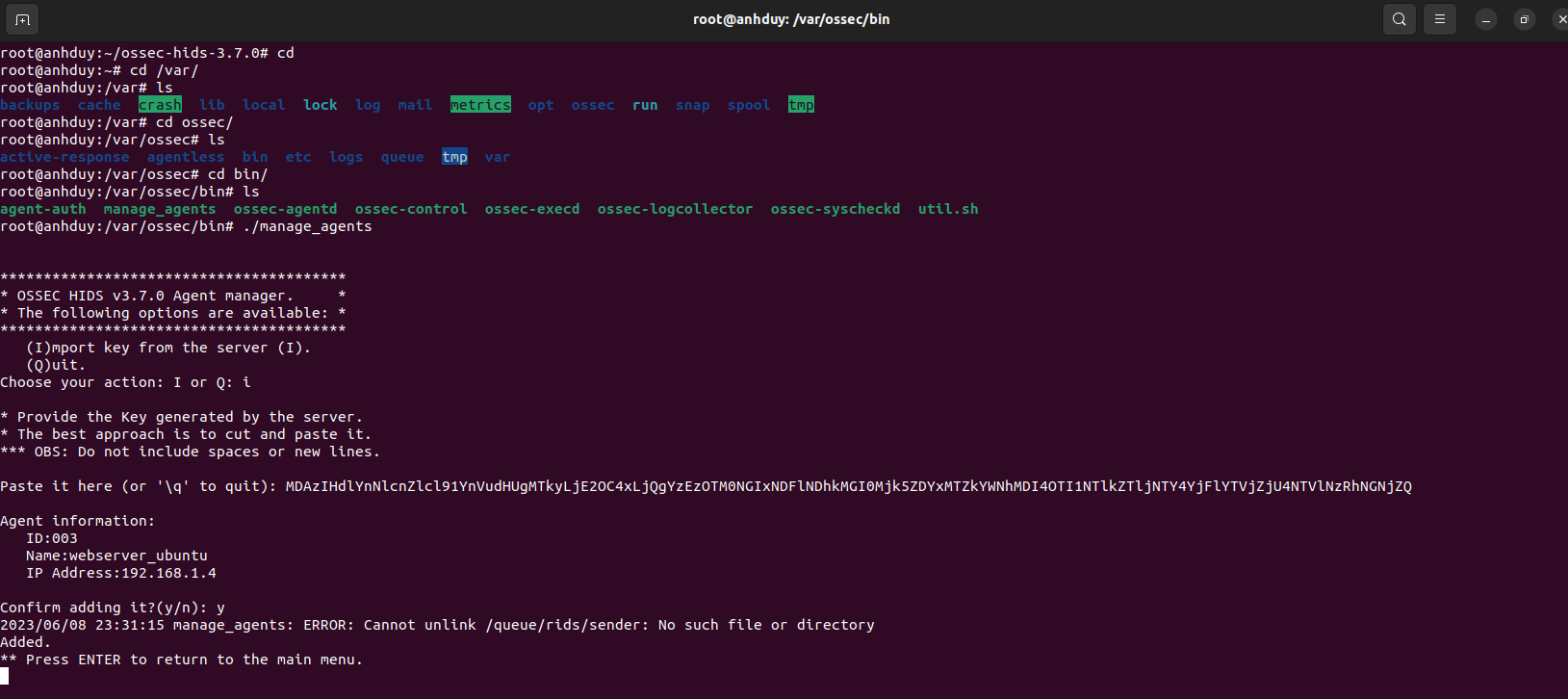
Chọn Save để lưu thông tin vừa nhập.

Truy cập vào Tab Manage chọn Start OSSEC để chạy dịch vụ

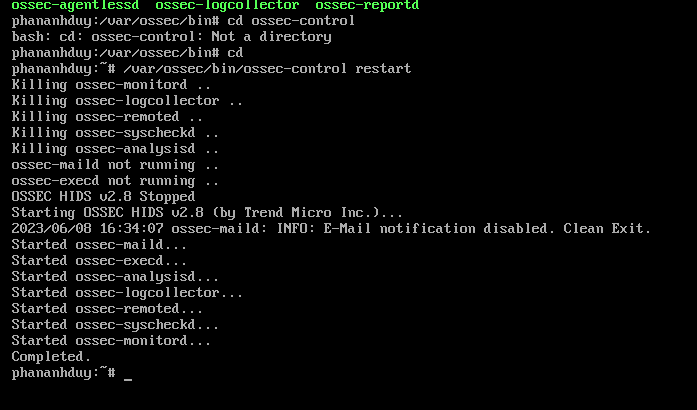
**1.6.2. Cài đặt và cấu hình OSSEC trên máy Linux**

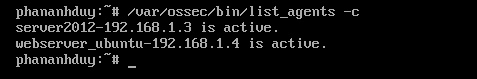
****

****

****

Sử dụng lệnh sau để khởi động lại dịch vụ trên cả máy chủ AlienVault và Linux Ubuntu: Restart lại dịch vụ và kiểm tra agent đã kết nối:

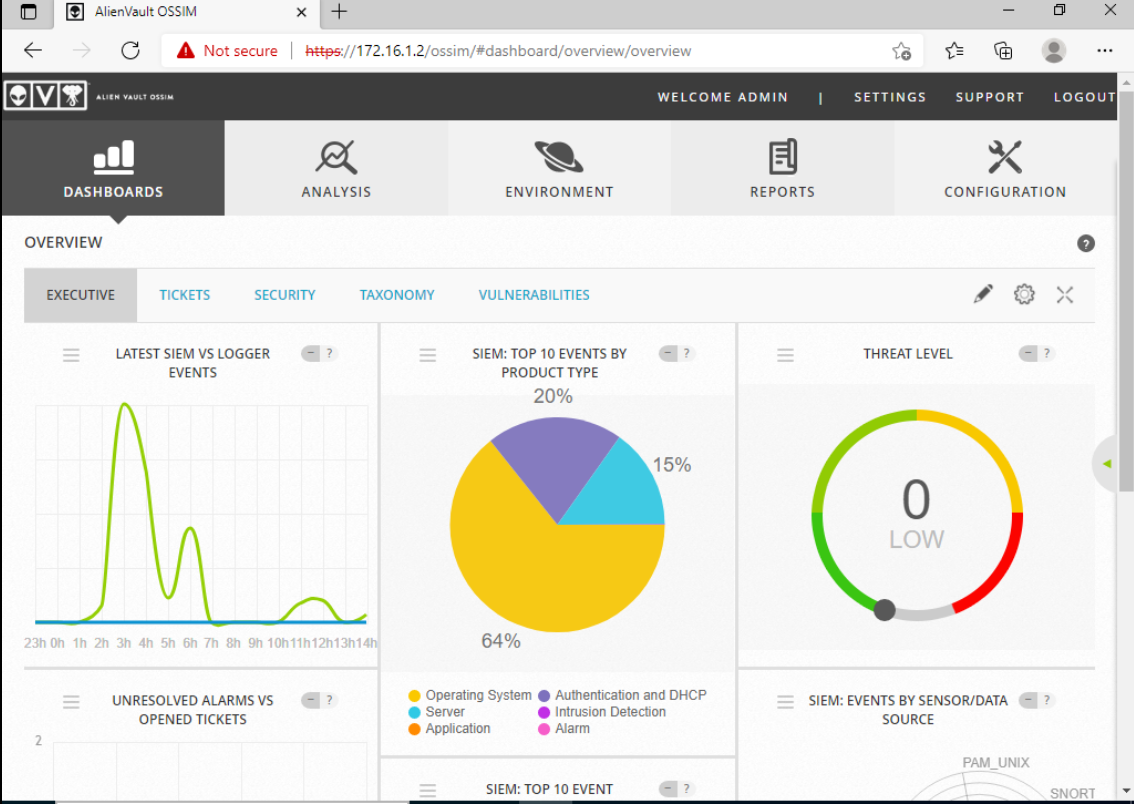
****

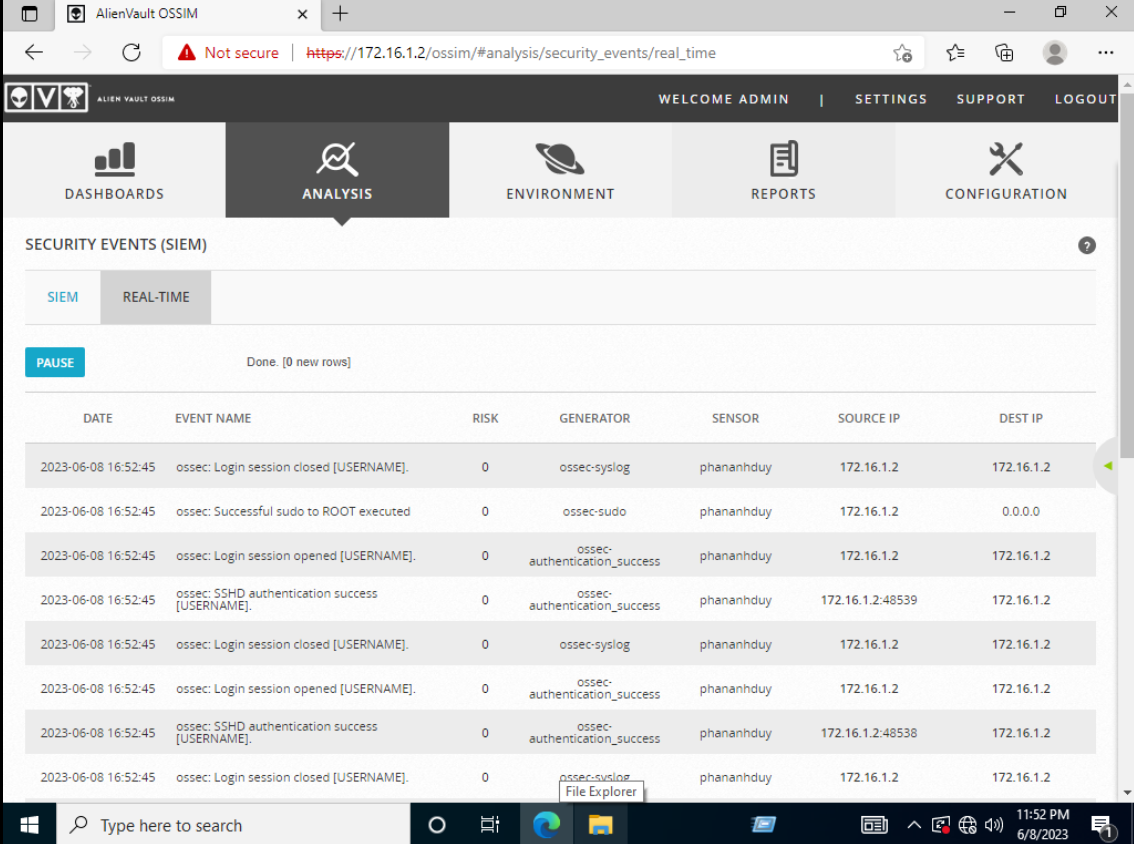
****

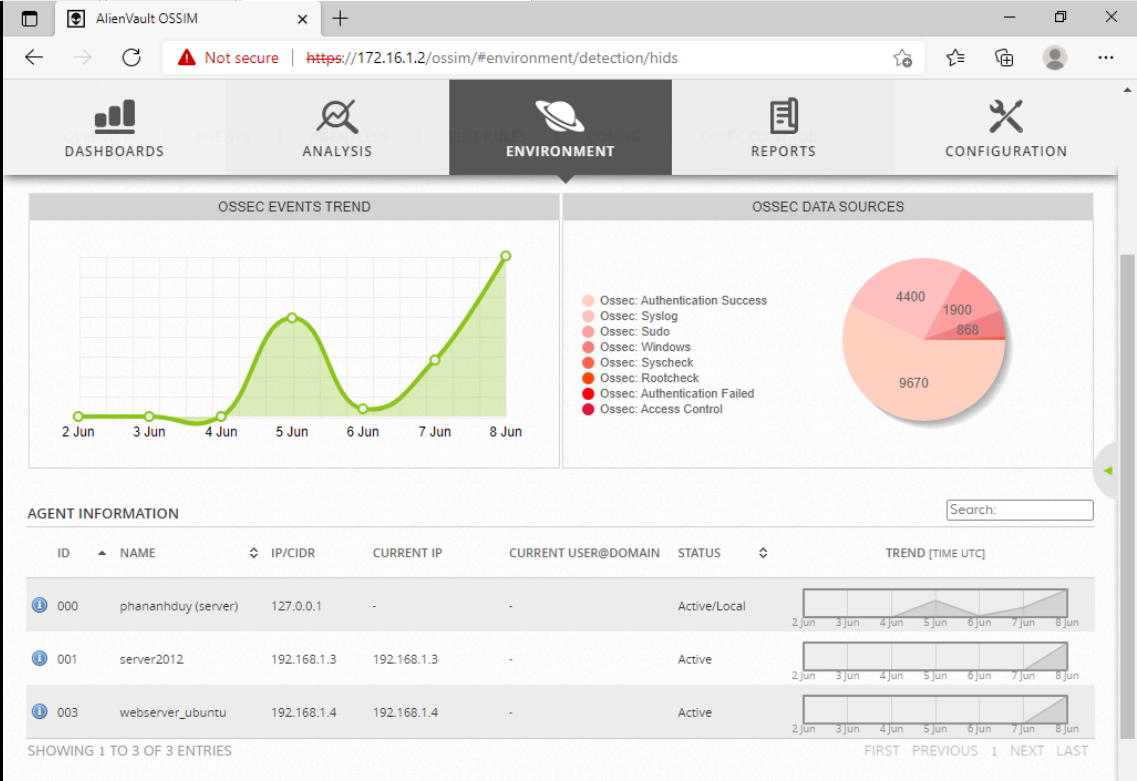
**1.7. Quản lý AlienVault thông qua giao diện web**

Sử dụng trình duyệt web truy cập theo địa chỉ IP: <https://172.16.1.2>

Giao diện tổng quát của AlienVault

****

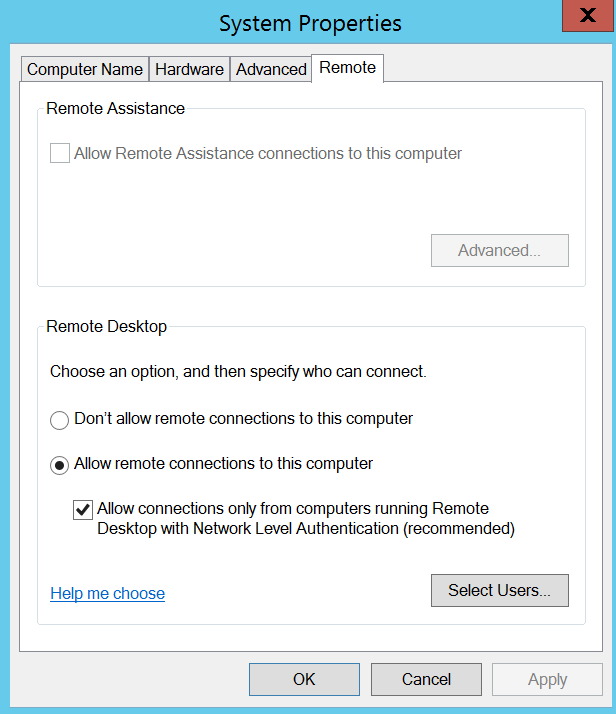
****

****

**1.8. Thực hiện tấn công vào mật khẩu trên máy Server 2003**

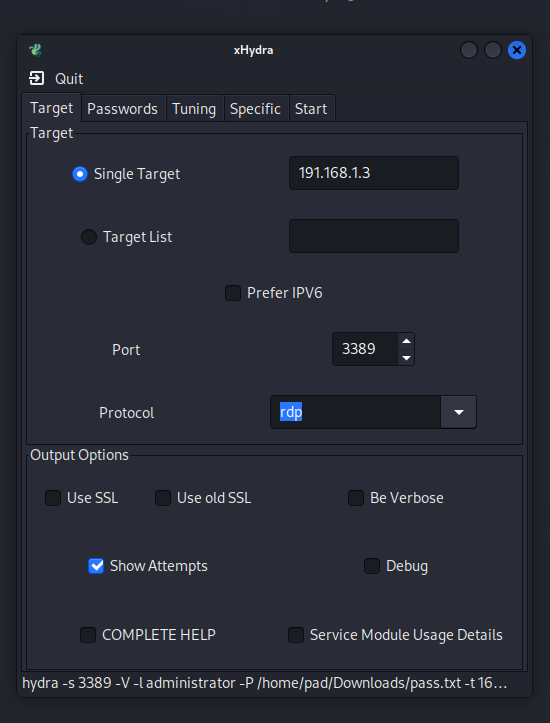
Sử dụng máy trạm Kali Linux để tấn công từ điển mật khẩu vào tài khoản Administrator trên Server 2012:

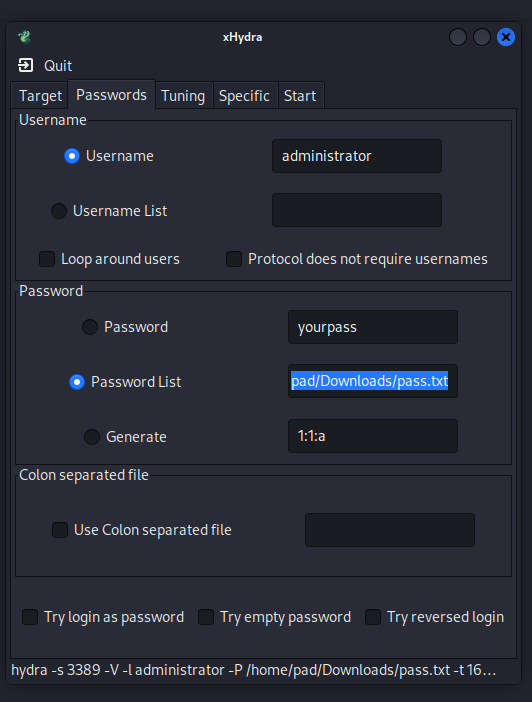
Trên máy Server 2003 bật dịch vụ truy cập từ xa Remote Desktop

****

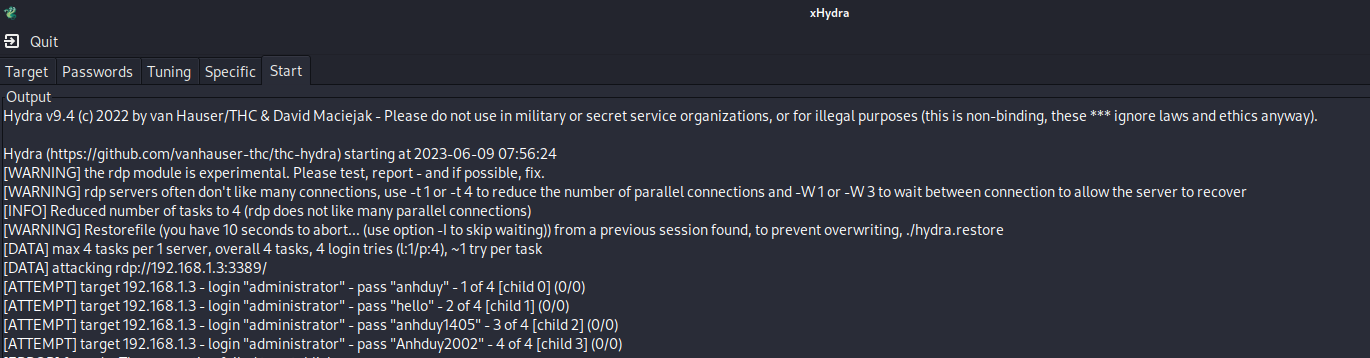
Trên máy Kali: Bật công cụ xhydra để tấn công mật khẩu bằng từ điển

Trong Tab Target nhập địa chỉ IP của máy Server 2012, nhập cổng dịch vụ Remote Desktop là 3389, giao thức rdp:

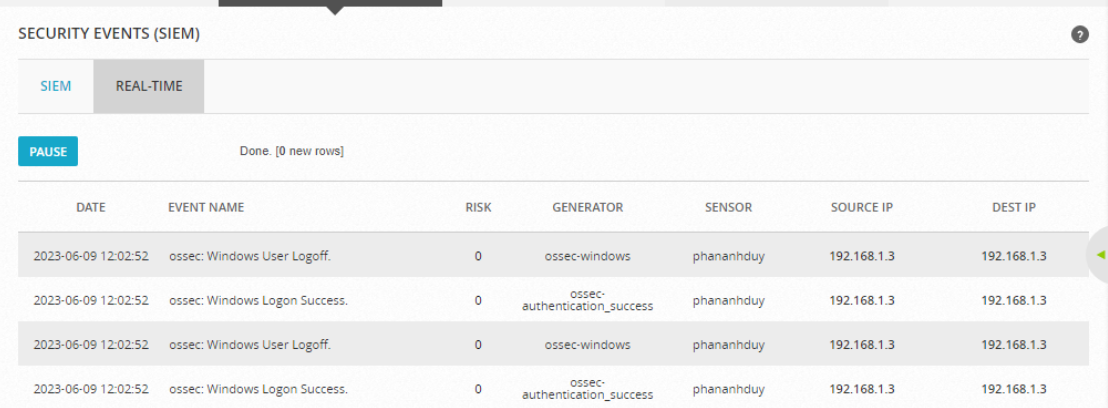
****

****

Chuyển sang Tab Start nhấn vào nút Start để bắt đầu tấn công

****

Chuyển sang giao diện web quản trị AlienVault với chức năng giám sát thơi gian thực, phát hiện sự kiện tấn công:

****

Từ sự kiện này biết được địa chỉ đích tấn công và nguồn bị tấn công. Với dấu hiệu là rất nhiều sự kiện xác thực không thành công, vì vậy có thể kết luận máy Server 2012 đang bị tấn công vào mật khẩu.

**1.9. Thực hiện tấn công quét lỗ hổng đối với mã nguồn website**

Lúc này sử dụng thêm máy ảo Windows XP để cài đặt công cụ Acunetix Web Vulnerability Scanner quét lỗ hổng website trên máy Linux Ubuntu. Sử dụng trình duyệt web để truy cập thử vào trang web có trên máy chủ Ubuntu: