**Lab 7 - Giám sát và phát hiện truy cập trái phép bằng Fail2Ban và Splunk trên Linux**

**1. Mục tiêu**

* Thiết lập môi trường theo dõi và ghi nhận các lần thử truy cập trái phép vào dịch vụ SSH.
* Cấu hình **Fail2Ban** để phát hiện và chặn các địa chỉ IP độc hại.
* Sử dụng **Splunk** để thu thập và phân tích log từ Fail2Ban nhằm phát hiện hành vi tấn công.

**2. Sơ đồ mạng**

Ubuntu Server (Victim, SplunkUniversalForwarder): 192.168.56.105/24

Ubuntu (Splunk Server): 192.168.56.104/24

Kali (Attacker): 192.168.56.101/24

**3. Kiến thức nền**

* **Splunk**: Nền tảng mạnh mẽ dùng để thu thập, phân tích và trực quan hóa log hệ thống. Splunk giúp phát hiện hành vi bất thường như thực thi tiến trình lạ, kết nối ngược (reverse shell), hay các cuộc tấn công mạng thông qua phân tích log theo thời gian thực.
* **Splunk Universal Forwarder**: Là agent nhẹ được cài đặt trên máy **Ubuntu Server** (nạn nhân), có nhiệm vụ chuyển tiếp log từ hệ thống (ví dụ: log tiến trình, log SSH) về **Splunk Server** (máy phân tích, thường là Windows hoặc Linux).
* **Fail2Ban**: Công cụ bảo mật trên Linux dùng để giám sát log và tự động **chặn các địa chỉ IP** có dấu hiệu tấn công (như đăng nhập sai nhiều lần qua SSH). Fail2Ban giúp giảm thiểu rủi ro từ các cuộc tấn công brute-force.
* **SSH (Secure Shell)**: Giao thức phổ biến để truy cập máy chủ từ xa. Do tính phổ biến và quyền truy cập cao, SSH thường là mục tiêu của các **cuộc tấn công brute-force**, nơi kẻ tấn công thử nhiều tổ hợp tên đăng nhập và mật khẩu để xâm nhập hệ thống.
* **Hydra**: Là công cụ tấn công brute-force nổi tiếng, hỗ trợ nhiều giao thức như SSH, FTP, HTTP, Telnet,… Hydra cho phép kẻ tấn công tự động thử hàng loạt mật khẩu trên một tài khoản nhằm chiếm quyền truy cập.
* **Tấn công Brute-force**: Là hình thức tấn công dò mật khẩu bằng cách thử tất cả các kết hợp có thể cho đến khi tìm ra thông tin đúng. Đây là kỹ thuật đơn giản nhưng vẫn rất hiệu quả nếu hệ thống không có cơ chế khóa tài khoản hoặc giám sát truy cập.

**4. Các bước thực hiện**

**Bước 1: Chuẩn bị môi trường**

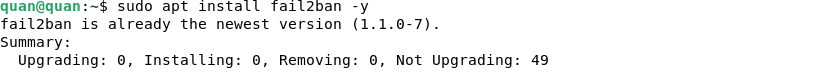
* Tải và cài đặt máy ảo Ubuntu Server 22.04 và Kali Linux 2025.1a qua VMware Player.
  + Ubuntu Server: <https://releases.ubuntu.com/jammy/ubuntu-22.04.5-live-server-amd64.iso>
  + Kali Linux: <https://cdimage.kali.org/kali-2025.1a/kali-linux-2025.1a-vmware-amd64.7z>
* Thực hiện cài đặt, cấu hình Splunk Server trên Windows và Splunk Universal Forwarder trên Ubuntu Server theo hướng dẫn tại: [https://github.com/0xrajneesh/90-days-security-challenge/blob/main/Challenge%231/LabSetup.md](https://github.com/0xrajneesh/90-days-security-challenge/blob/main/Challenge%231/Lab%20Set%20up.md)

**Bước 2: Cài đặt và cấu hình Fail2Ban trên Ubuntu Server**

1. **Cài đặt Fail2Ban**

sudo apt update

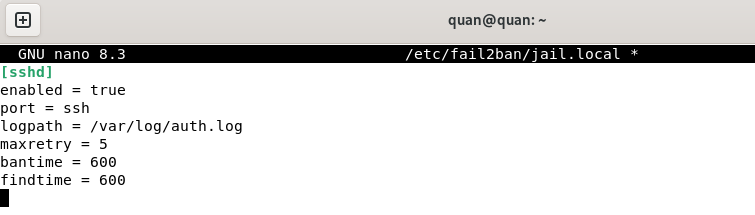
sudo apt install fail2ban -y



1. **Cấu hình bảo vệ dịch vụ SSH trên Fail2Ban**
   * Mở file cấu hình của Fail2Ban

sudo nano /etc/fail2ban/jail.local

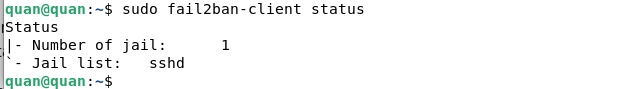
* + Thêm những dòng sau để bảo vệ dịch vụ ssh



* + Lưu và đóng file

1. **Kiểm tra trạng thái hoạt động của Fail2Ban**

sudo fail2ban-client status



**Bước 3: Cấu hình Splunk Server và Splunk Forwarder**

1. **Trên Splunk Server (Windows)**

Tạo index mới: fail2ban\_logs (Settings → Indexes → New Index).

1. **Trên Splunk Universal Forwarder (Ubuntu Server)**

Thiết lập Splunk Forwarder giám sát log của Fail2Ban:

/opt/splunkforwarder/bin/splunk add monitor /var/log/fail2ban.log

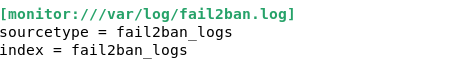
sudo systemctl restart fail2ban

Cấu hình Splunk Forwarder gửi log của Fail2Ban:

Mở fileinputs.conf

* + sudo nano /opt/splunkforwarder/etc/system/local/inputs.conf

Thêm nội dung sau



Lưu lại và khởi động lại Splunk Forwarder:

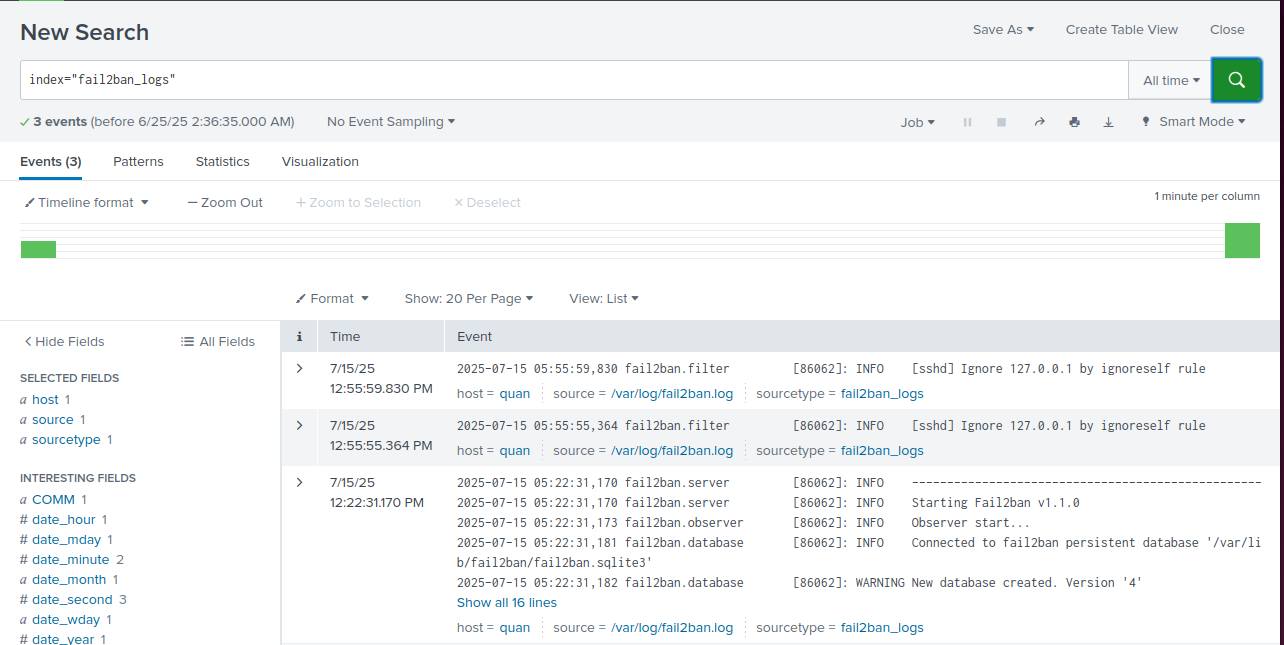
sudo /opt/splunkforwarder/bin/splunk restart

**Bước 4: Mô phỏng tấn công brute-force SSH từ Kali Linux**

1. **Kiểm tra thử hệ thống log hoạt động ổn định:**

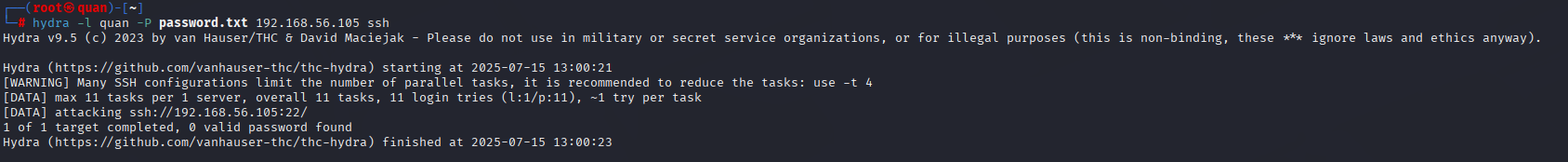
* Sau khi cấu hình Splunk Server, Splunk Forwarder thì trên máy Ubuntu Server thử đăng nhập SSH với mật khẩu sai để tạo log xem mọi thứ đã hoạt động ổn chưa



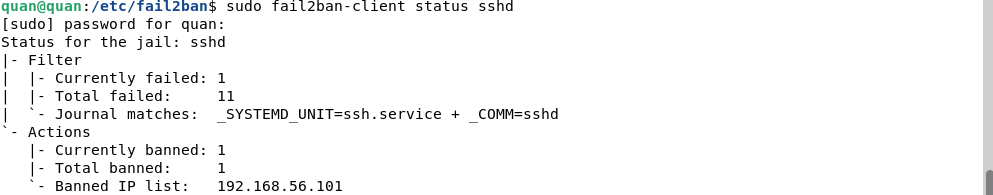


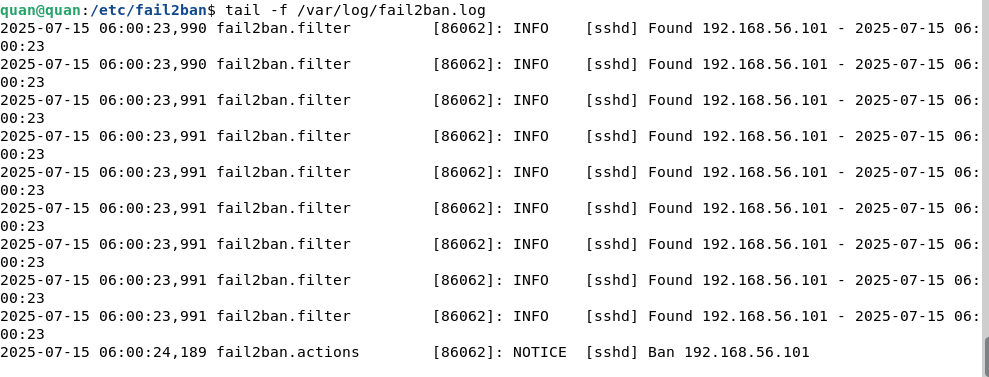
* Như trên hình thì ta đã có thể xác định được là **Fail2Ban** hoạt động và tạo log, **Splunk Forwarder** cũng đã theo dõi log của **Fail2Ban** và chuyển tiếp chúng tới **Splunk Server**, **Spunk Server** cũng đã nhận được log của **Fail2Ban**
* Bây giờ chúng ta sẽ sử dụng máy ảo Kali để mô phỏng cuộc tấn công bruteforce

1. **Tạo danh sách mật khẩu brute-force (hoặc sử dụng wordlist có sẵn)**
2. **Chạy Hydra brute-force SSH**



1. **Kiểm tra Fail2Ban trên máy Ubuntu Server đã block IP tấn công chưa**





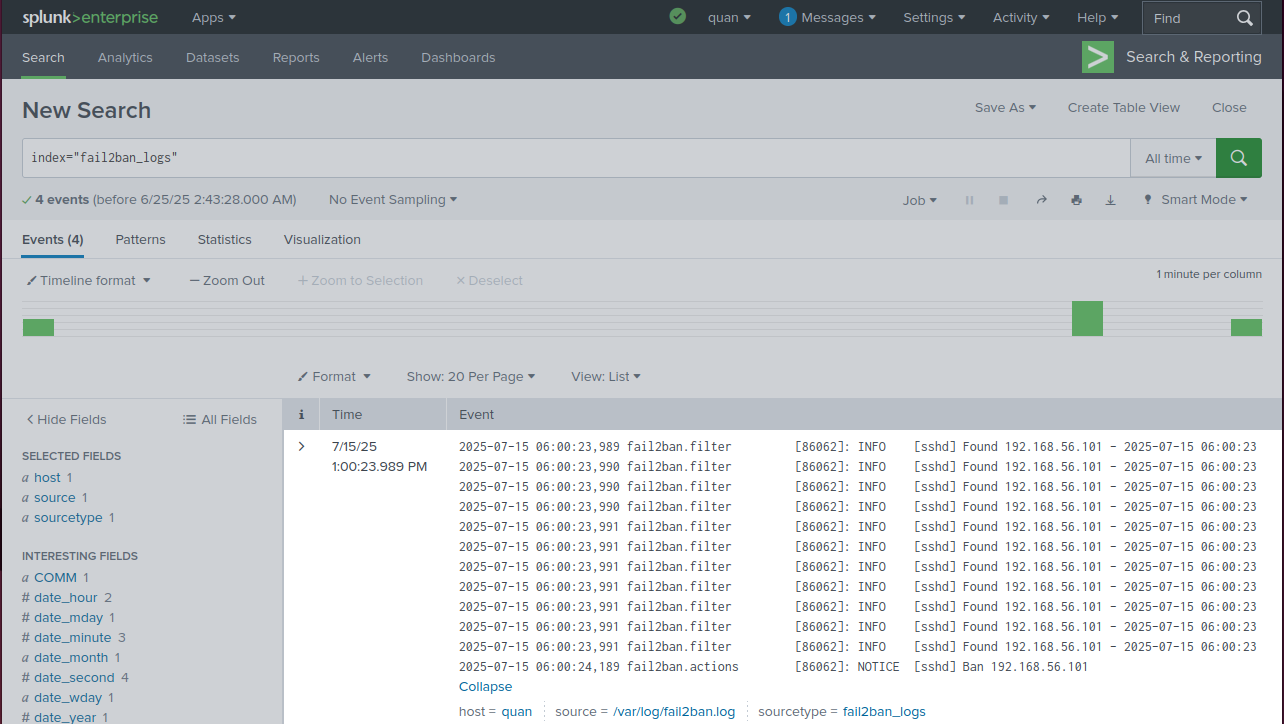
→ Nhận thấy rằng IP của kali (kẻ tấn công) đã được log lại và bị chặn

**Bước 5. Phân tích log trên Splunk**

Truy cập giao diện Splunk Server qua trình duyệt:

Vào Search → chọn index fail2ban\_logs và thực hiện truy vấn log:

Xác minh các sự kiện block IP đã được ghi nhận đúng từ Fail2Ban.



**PHÁT HIỆN VÀ CHẶN TẤN CÔNG SSH BRUTE FORCE**

**1. Thông tin sự kiện**

* **Thời gian:** 2025-07-15, khoảng 06:00:23 đến 06:00:24
* **Dịch vụ bị tấn công:** SSH (sshd)
* **Địa chỉ IP tấn công:** 192.168.56.101
* **Hành động:**
  + Fail2ban phát hiện nhiều lần truy cập thất bại từ IP trên.
  + Đã thực hiện chặn (ban) IP 192.168.56.101 vào lúc 06:00:24.
* **Cơ chế:** Fail2ban theo dõi file log /var/log/auth.log để phát hiện các hành vi đăng nhập sai và tự động chặn IP tấn công.

**2. Đánh giá**

* IP 192.168.56.101 thực hiện tấn công brute force vào dịch vụ SSH.
* Hệ thống đã phản ứng kịp thời bằng cách khóa IP, giảm nguy cơ bị xâm nhập trái phép.
* Fail2ban hoạt động hiệu quả, giúp bảo vệ dịch vụ SSH trước các tấn công phổ biến.

**3. Khuyến nghị**

* Tiếp tục giám sát log fail2ban và hệ thống để phát hiện các IP tấn công mới.
* Áp dụng các biện pháp bổ sung:
  + Sử dụng xác thực đa yếu tố (MFA) cho SSH.
  + Giới hạn truy cập SSH chỉ từ các IP tin cậy.
  + Thường xuyên cập nhật phần mềm và kiểm tra cấu hình bảo mật SSH.