**PHÂN TÍCH MỘT LINUX LOG**

{

"@timestamp": [

"2025-03-19T13:26:17.063Z"

],

"@version": [

"1"

],

"@version.keyword": [

"1"

],

"agent.ephemeral\_id": [

"d2b9d69e-5780-4a46-b5a8-7db3b1e72774"

],

"agent.ephemeral\_id.keyword": [

"d2b9d69e-5780-4a46-b5a8-7db3b1e72774"

],

"agent.id": [

"66168684-adf4-407c-8211-8d97194c00cf"

],

"agent.id.keyword": [

"66168684-adf4-407c-8211-8d97194c00cf"

],

"agent.name": [

"ubuntu-2"

],

"agent.name.keyword": [

"ubuntu-2"

],

"agent.type": [

"filebeat"

],

"agent.type.keyword": [

"filebeat"

],

"agent.version": [

"8.17.3"

],

"agent.version.keyword": [

"8.17.3"

],

"ecs.version": [

"8.0.0"

],

"ecs.version.keyword": [

"8.0.0"

],

"event.original": [

"Mar 19 20:26:09 ubuntu-2 pkexec[73931]: wanthinnn: Executing command [USER=root] [TTY=unknown] [CWD=/home/wanthinnn] [COMMAND=/usr/lib/update-notifier/package-system-locked]"

],

"event.original.keyword": [

"Mar 19 20:26:09 ubuntu-2 pkexec[73931]: wanthinnn: Executing command [USER=root] [TTY=unknown] [CWD=/home/wanthinnn] [COMMAND=/usr/lib/update-notifier/package-system-locked]"

],

"host.name": [

"ubuntu-2"

],

"host.name.keyword": [

"ubuntu-2"

],

"input.type": [

"filestream"

],

"input.type.keyword": [

"filestream"

],

"log.file.device\_id": [

"2051"

],

"log.file.device\_id.keyword": [

"2051"

],

"log.file.inode": [

"5507088"

],

"log.file.inode.keyword": [

"5507088"

],

"log.file.path": [

"/var/log/auth.log"

],

"log.file.path.keyword": [

"/var/log/auth.log"

],

"log.offset": [

250

],

"message": [

"Mar 19 20:26:09 ubuntu-2 pkexec[73931]: wanthinnn: Executing command [USER=root] [TTY=unknown] [CWD=/home/wanthinnn] [COMMAND=/usr/lib/update-notifier/package-system-locked]"

],

"message.keyword": [

"Mar 19 20:26:09 ubuntu-2 pkexec[73931]: wanthinnn: Executing command [USER=root] [TTY=unknown] [CWD=/home/wanthinnn] [COMMAND=/usr/lib/update-notifier/package-system-locked]"

],

"tags": [

"beats\_input\_codec\_plain\_applied"

],

"tags.keyword": [

"beats\_input\_codec\_plain\_applied"

],

"\_id": "35qVrpUB1lPr3AWbgYqg",

"\_index": "system\_logs",

"\_score": null

}

# 1. Thông tin chung của log

* **@timestamp:** "2025-03-19T13:26:17.063Z"  
  → Thời điểm log được ghi lại (hoặc được đưa vào Elasticsearch). Lưu ý rằng thời gian ghi trong log gốc là "Mar 19 20:26:09", có thể khác do múi giờ hoặc thời gian xử lý (ingest time).
* **@version:** "1"  
  → Phiên bản của event schema trong hệ thống (theo ECS - Elasticsearch Common Schema).
* **ECS Version:** "8.0.0"  
  → Phiên bản của Elasticsearch Common Schema mà log này tuân theo.

# 2. Thông tin từ agent Filebeat

* **agent.ephemeral\_id & agent.id:**  
  → Các định danh tạm thời và duy nhất của agent Filebeat gửi log (ví dụ: "d2b9d69e-5780-4a46-b5a8-7db3b1e72774" và "66168684-adf4-407c-8211-8d97194c00cf").  
  → Giúp theo dõi các log được gửi từ cùng một instance của Filebeat.
* **agent.name:** "ubuntu-2"  
  → Tên máy chủ (hoặc hostname) nơi Filebeat được cài đặt, cho biết log đến từ máy ubuntu-2.
* **agent.type:** "filebeat"  
  → Chỉ ra rằng nguồn log đến từ Filebeat.
* **agent.version:** "8.17.3"  
  → Phiên bản Filebeat được sử dụng.

# 3. Thông tin về nguồn log và file log

* **host.name:** "ubuntu-2"  
  → Xác định nguồn của log, cho biết log được tạo trên máy ubuntu-2.
* **input.type:** "filestream"  
  → Loại input được Filebeat sử dụng để thu thập log, trong trường hợp này là đọc từ file (filestream).
* **log.file.path:** "/var/log/auth.log"  
  → Đường dẫn đến file log gốc, ở đây là file chứa các sự kiện liên quan đến xác thực trên hệ thống Linux.
* **log.file.device\_id, log.file.inode, log.offset:**  
  → Các thông tin metadata của file log giúp định vị và theo dõi vị trí đọc log (để tránh đọc trùng hoặc bỏ sót log).
* **message & event.original:**  
  → Nội dung log gốc:

Mar 19 20:26:09 ubuntu-2 pkexec[73931]: wanthinnn: Executing command [USER=root] [TTY=unknown] [CWD=/home/wanthinnn] [COMMAND=/usr/lib/update-notifier/package-system-locked]

→ Đây là dòng log ghi lại hoạt động của pkexec trên hệ thống.

* **tags:**  
  → "beats\_input\_codec\_plain\_applied" cho biết Filebeat đã áp dụng codec plain khi xử lý log.

# 4. Phân tích nội dung log gốc

* **Context của log:**
  + Log này được ghi từ file /var/log/auth.log, file này thường chứa các sự kiện liên quan đến xác thực, truy cập, và hoạt động của các dịch vụ liên quan đến bảo mật trên Linux.
* **Thành phần của log gốc:**
  + **Thời gian:** Mar 19 20:26:09 – Thời điểm sự kiện xảy ra trên hệ thống.
  + **Hostname:** ubuntu-2 – Cho biết log đến từ máy chủ có tên ubuntu-2.
  + **Process:** pkexec[73931] – Đây là process pkexec, công cụ của PolicyKit dùng để chạy lệnh với quyền root.
  + **User thực hiện:** wanthinnn – Người dùng thực hiện lệnh thông qua pkexec.
  + **Hành động:** "Executing command [USER=root] [TTY=unknown] [CWD=/home/wanthinnn] [COMMAND=/usr/lib/update-notifier/package-system-locked]"  
    → Log này cho biết rằng người dùng wanthinnn đã sử dụng pkexec để thực hiện lệnh với quyền root, và lệnh được thực thi là /usr/lib/update-notifier/package-system-locked.  
    → Đây có thể là một hành động hợp lệ (ví dụ: một tiến trình tự động của hệ thống cập nhật trạng thái hoặc khóa gói cập nhật) nhưng cũng cần được theo dõi trong ngữ cảnh chính sách bảo mật của hệ thống.

# 5. Ý nghĩa đối với SOC

* **Theo dõi hoạt động tăng quyền:**  
  Sự kiện sử dụng pkexec luôn được chú ý trong môi trường an ninh vì nó liên quan đến việc chạy lệnh với quyền root. SOC cần kiểm tra xem hành động này có thuộc quy trình hợp lệ (ví dụ: được phép thực hiện bởi người dùng cụ thể hay không) hay có dấu hiệu bất thường.
* **Kiểm tra hành vi người dùng:**  
  Thông tin người dùng (wanthinnn) và các tham số như [TTY=unknown] cũng giúp SOC điều tra xem liệu đây có phải là hành vi đáng ngờ hay không. Nếu có nhiều log tương tự xảy ra bất thường, đó có thể là dấu hiệu của tấn công nội bộ.
* **Phân tích thay đổi hệ thống:**  
  Log từ /var/log/auth.log cung cấp thông tin quan trọng về các hành động bảo mật, từ đó giúp xác định liệu hệ thống có bị xâm nhập, thay đổi cấu hình không hợp lệ hoặc tấn công brute force không.

**Kết luận**

Log trên cho thấy một sự kiện từ file /var/log/auth.log của hệ thống Linux, ghi lại hoạt động sử dụng pkexec để thực thi lệnh với quyền root. Các trường metadata của Filebeat (agent, host, input type, v.v.) cung cấp thông tin bổ sung về nguồn gốc log, giúp SOC dễ dàng theo dõi và phân tích các sự kiện bảo mật. Đối với team SOC, log này là một nguồn dữ liệu quan trọng để phát hiện hành vi tăng quyền, kiểm tra tính hợp lệ của các hoạt động bảo mật, và đưa ra các biện pháp phản ứng kịp thời nếu phát hiện bất thường.

Nếu cần bổ sung thêm chi tiết hoặc có các câu hỏi khác, hãy cho tôi biết để tôi hỗ trợ thêm!