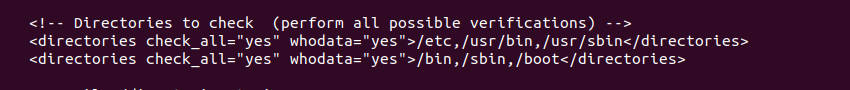
**Báo cáo Wazuh: Thực hiện theo dõi các hoạt động của file và thư mục**

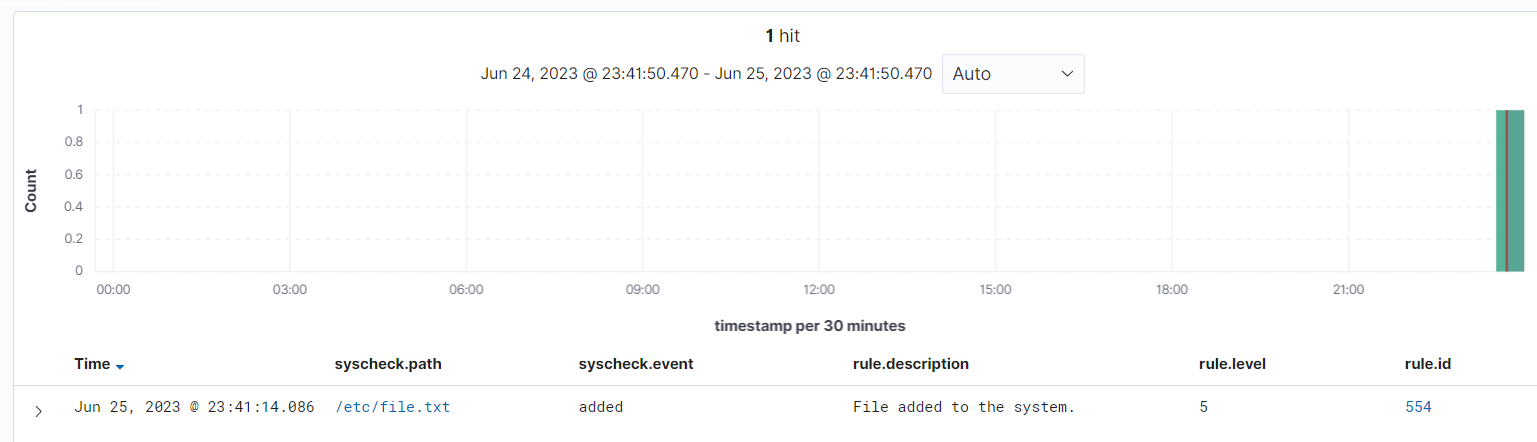
# Cấu hình File Integrity monitoring để theo dõi các hoạt động của file

* Ở Wazuh Server ta vào /var/ossec/etc/ossec.conf

Thực hiển sửa đổi directory:



* Tương tự ở Wazuh Agent ta cũng vào /var/ossec/etc/ossec.conf làm tương tự
* Sau đó tiến hành restart Wazuh Agent với câu lệnh : sudo systemctl restart wazuh-manager
* Kết quả ta thu được các log như sau:
  + Tạo file



* + Sửa file

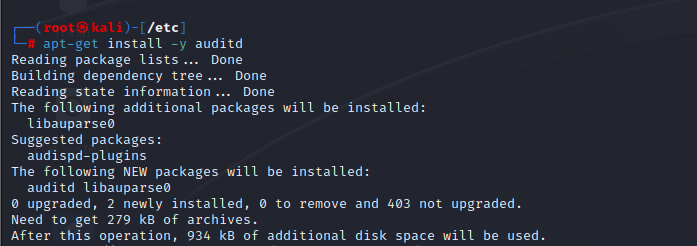


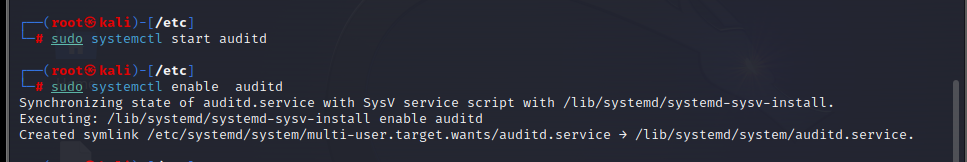
* + Xóa file



# Cấu hình system auditing để giám sát việc sử dụng lệnh liên quan file , thư mục:

* Ở Wazuh agent tiến hành sử dụng câu lệnh apt install -y auditd để cài auditd và khởi động

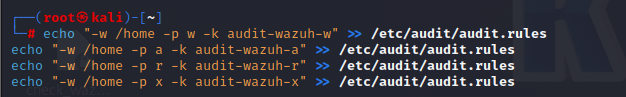




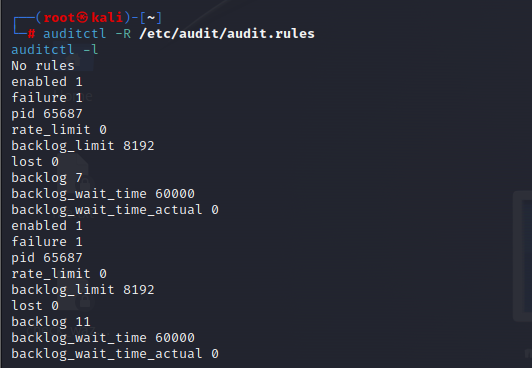
* Cấu hình thông tin dưới đây vào /vả/ossec/etc/ossec.conf. Cấu hình này sẽ giúp wazuh đọc được các log kiểm tra các thao tác , sự kiện mà hệ thống phát hiện



* Sau đó tiến hành restart wazuh-agent
* Tiếp theo ta tiến hành cấu hình rule audit như sau



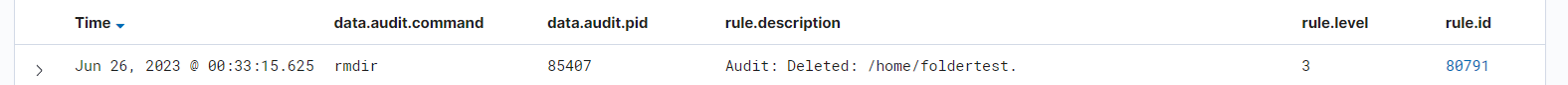
* Thực hiện reload lại rule audit để chấp nhận thay đổi



* Kết quả thu được các log như sau
  + Tạo một folder với lệnh mkdir



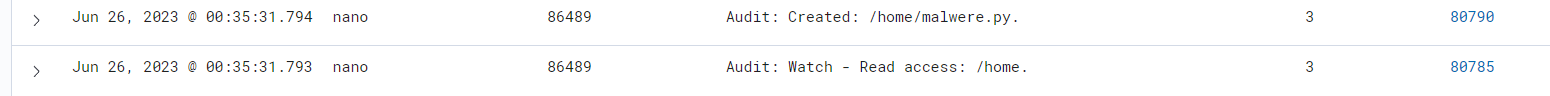
* + Xóa một folder với lệnh rmdir



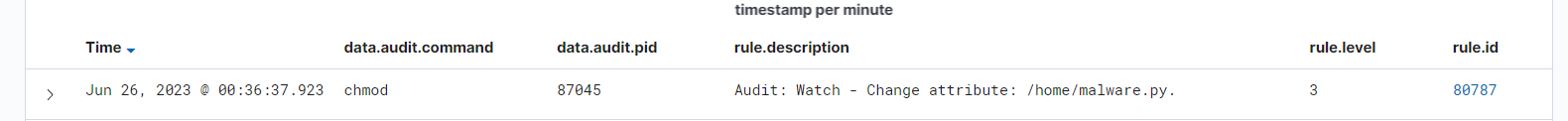
* + Tạo một file với lệnh touch



* + Ghi file với lệnh nano



* + Thay đổi quyền của file , thư mục với lệnh chmod



* + Đọc và chạy file



* + Xóa file với lệnh rm

