**Cài đặt và sử dụng IDS Zeek**

Quá trình cài đặt Zeek gôm các bước sau

Môi truờng thực nghiệm :

- Máy host cài hê điều hành ubuntu 18.04 LTS

- Máy ảo chạy hệ điều hành ubuntu 18.04 LTS

- Chương trình VMware Workstation 16 pro

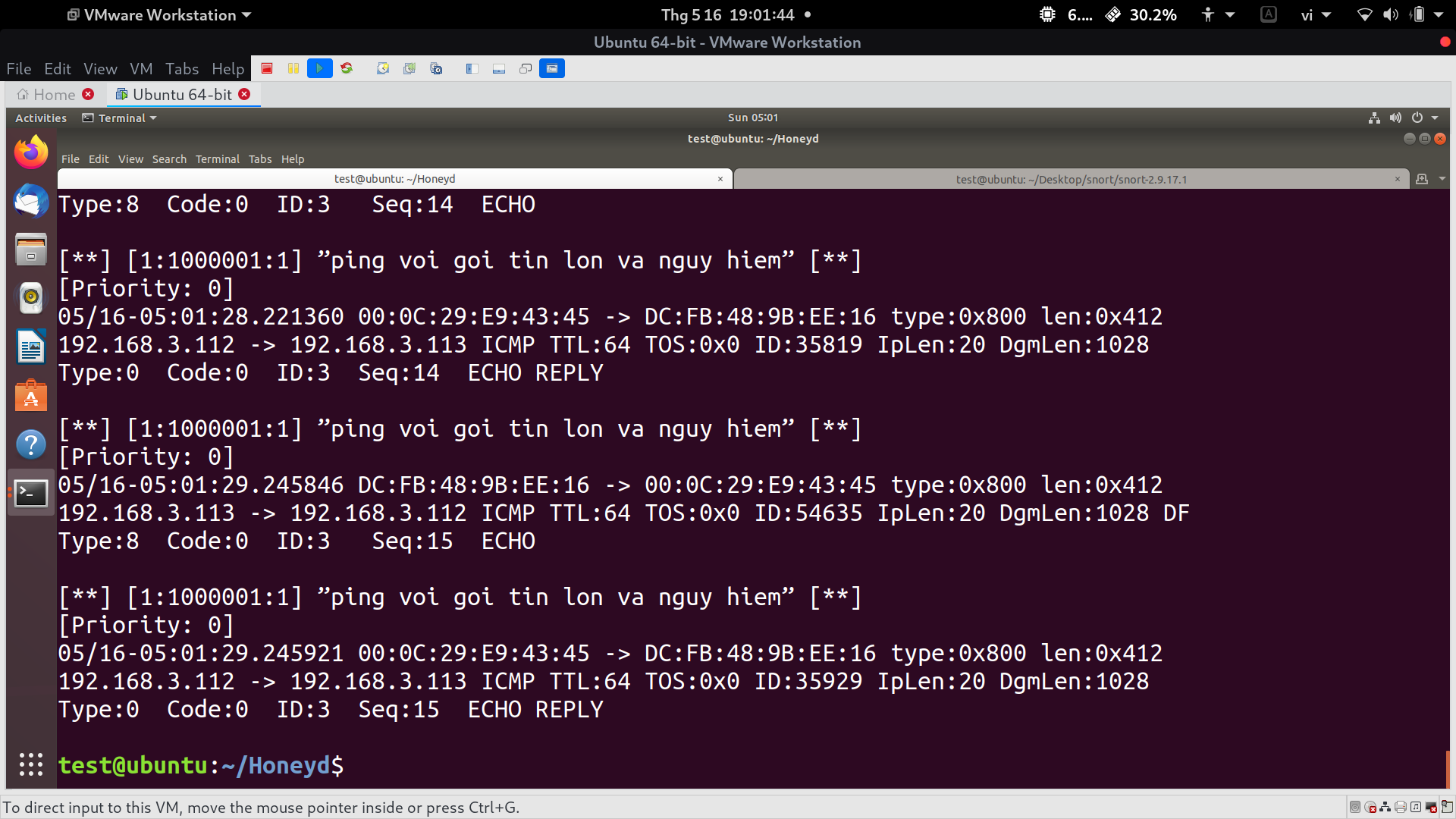
**Bước 1:** Thực hiện cài Zeek trên máy host Ubuntu 18.04 LTS

Update hệ điều hành

$ sudo apt update && sudo apt upgrade -y

Thực hiện cài đặt các thư viện cần thiết

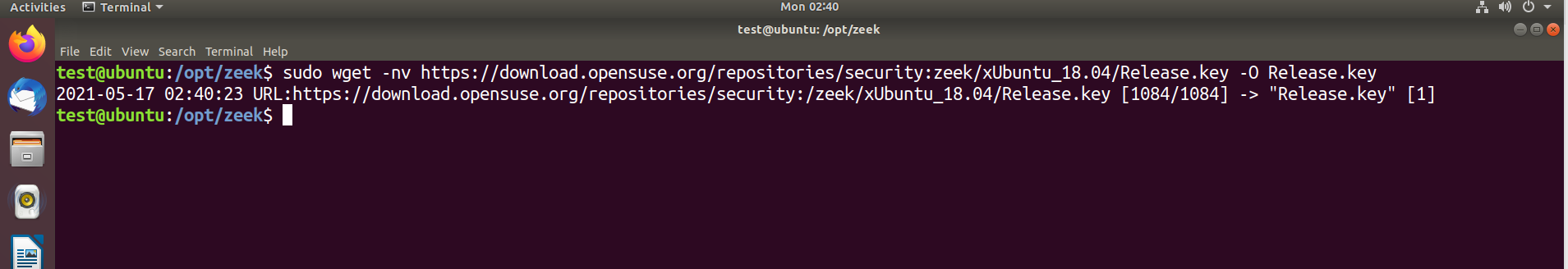
$ sudo apt install -y gcc libpcre3-dev zlib1g-dev libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev bison flex libdnet



**Bước 2 :** Thực hiện cài Zeek bằng kho lưu trữ trên Ubuntu

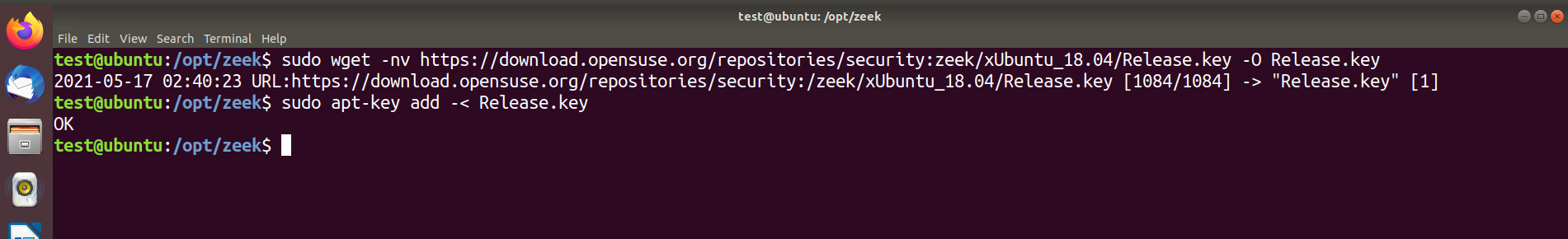
Thực hiện tải khóa trao đổi về (phiên bản cài đặt dành cho Ubuntu 18.04x)

$ wget -nv https://download.opensuse.org/repositories/security:zeek/xUbuntu\_18.04/Release.key -O Release.key



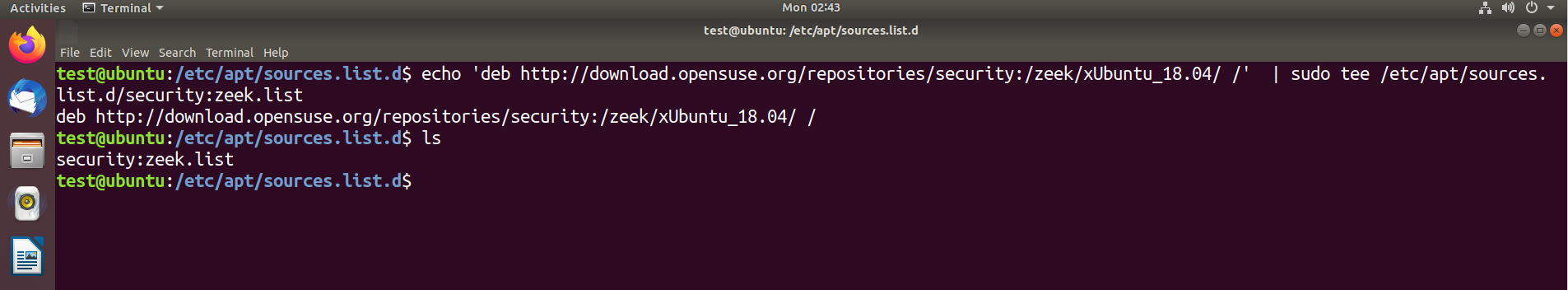
Thêm khóa

$ sudo apt-key add -< Release.key



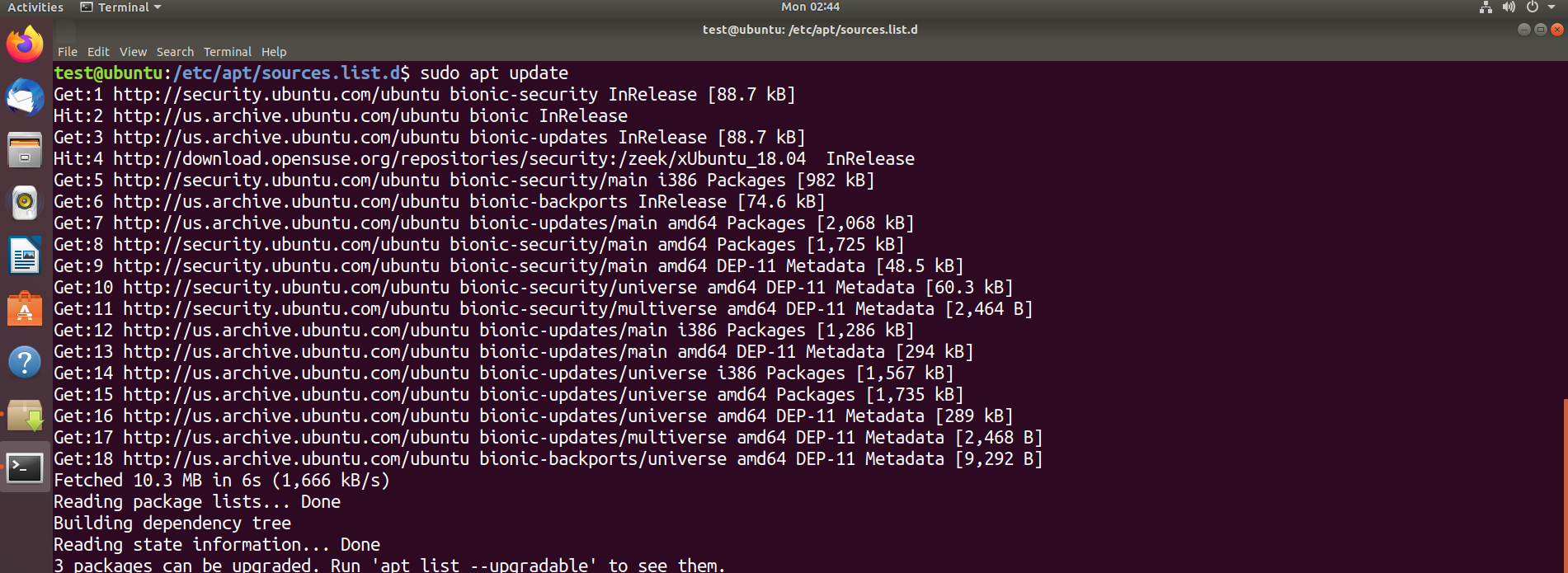
Thêm kho lưu trữ cá nhân APT :

$ echo 'deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu\_18.04/ /' | sudo tee /etc/apt/sources.list.d/security:zeek.list



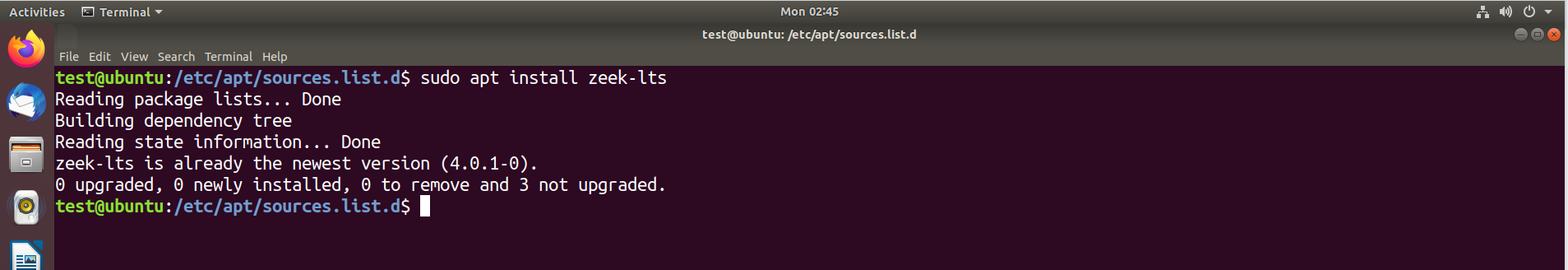
Thực hiện cập nhật kho lưu trữ

$ sudo apt update -y



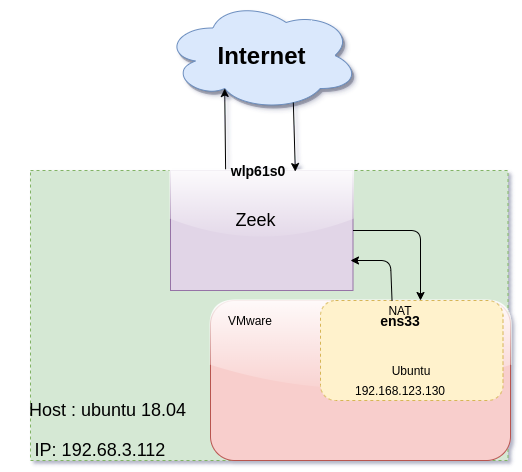
**Bước 3 :** Cài đặt Zeek

$ sudo apt install zeek-lts



II. Thực nghiệm khai thác vận hành IDS Zeek

1. Network topology

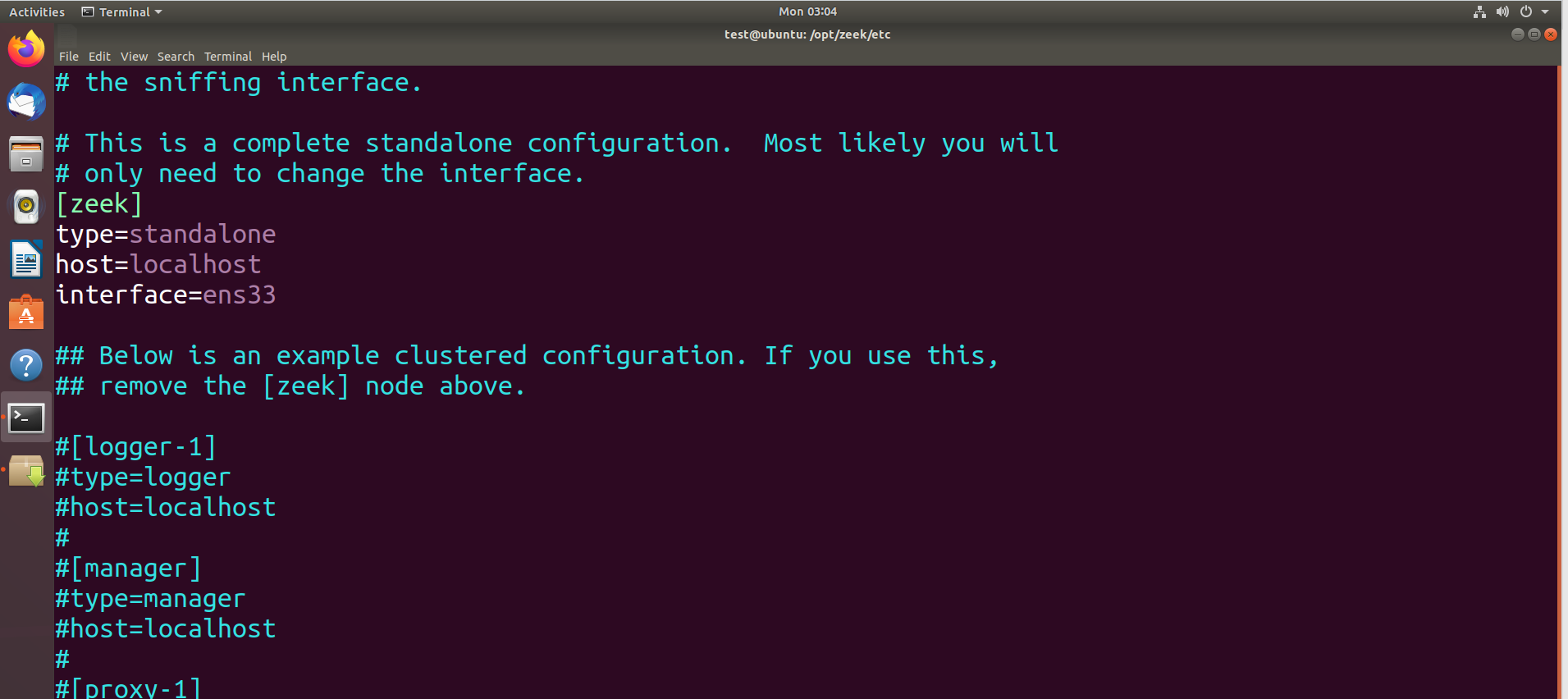
.

Trong thực nghiệm Zeek sẽ thực hiện chức năng giám sát luồng mạng như đã thể hiện trên lược đồ.

**2. Tiến hành cấu hình Zeek**

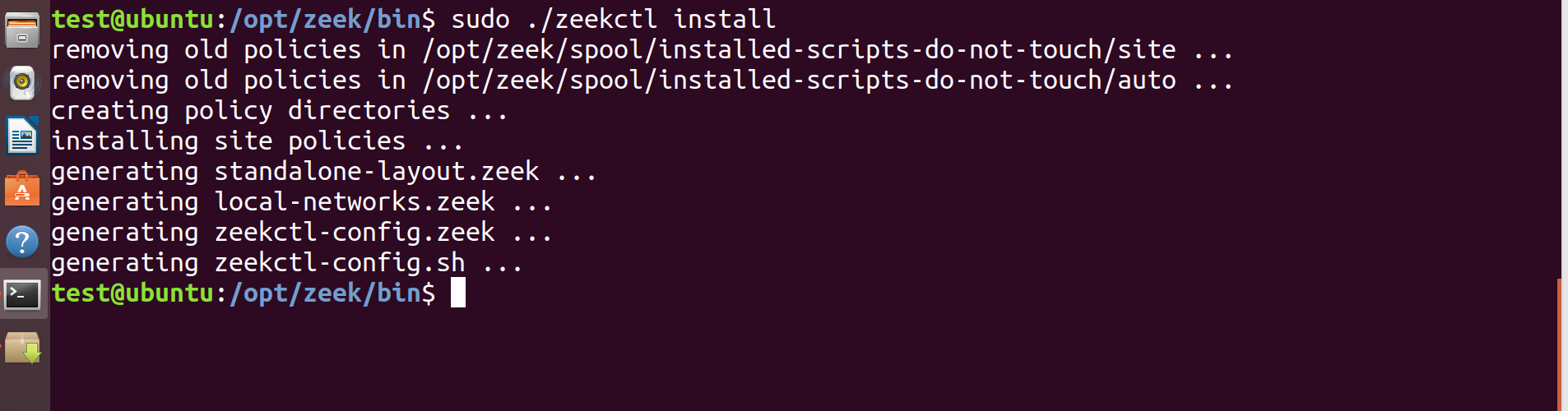
Thực hiện cấu hình lại thông tin trong file node.conf

$ vi /opt/etc/node.conf



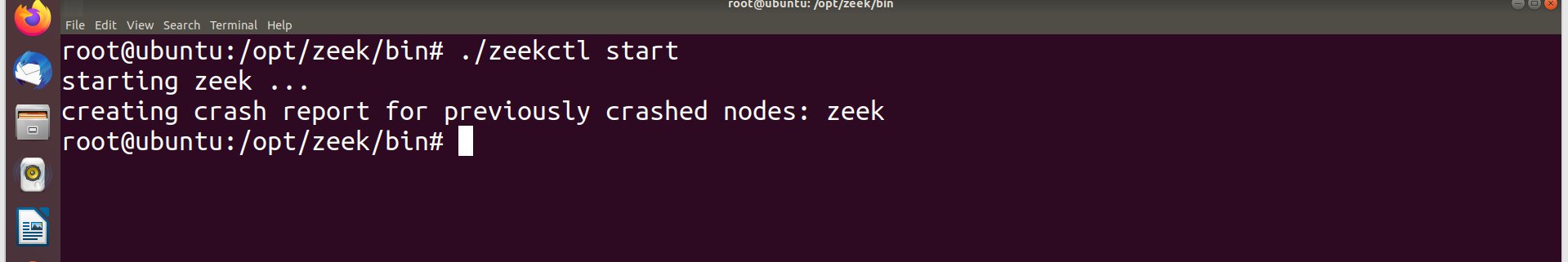
Thực hiện lệnh cài đặt lại với cấu hình đã thay đổi dùng lệnh :

$ sudo /opt/etc/bin/zeekctl install

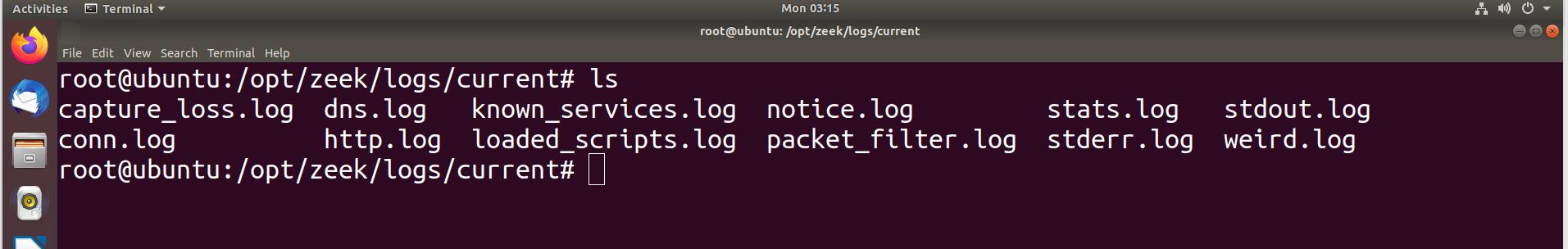


Chạy lệnh sau với quyền sudo để khởi động dịch vụ của Zeek

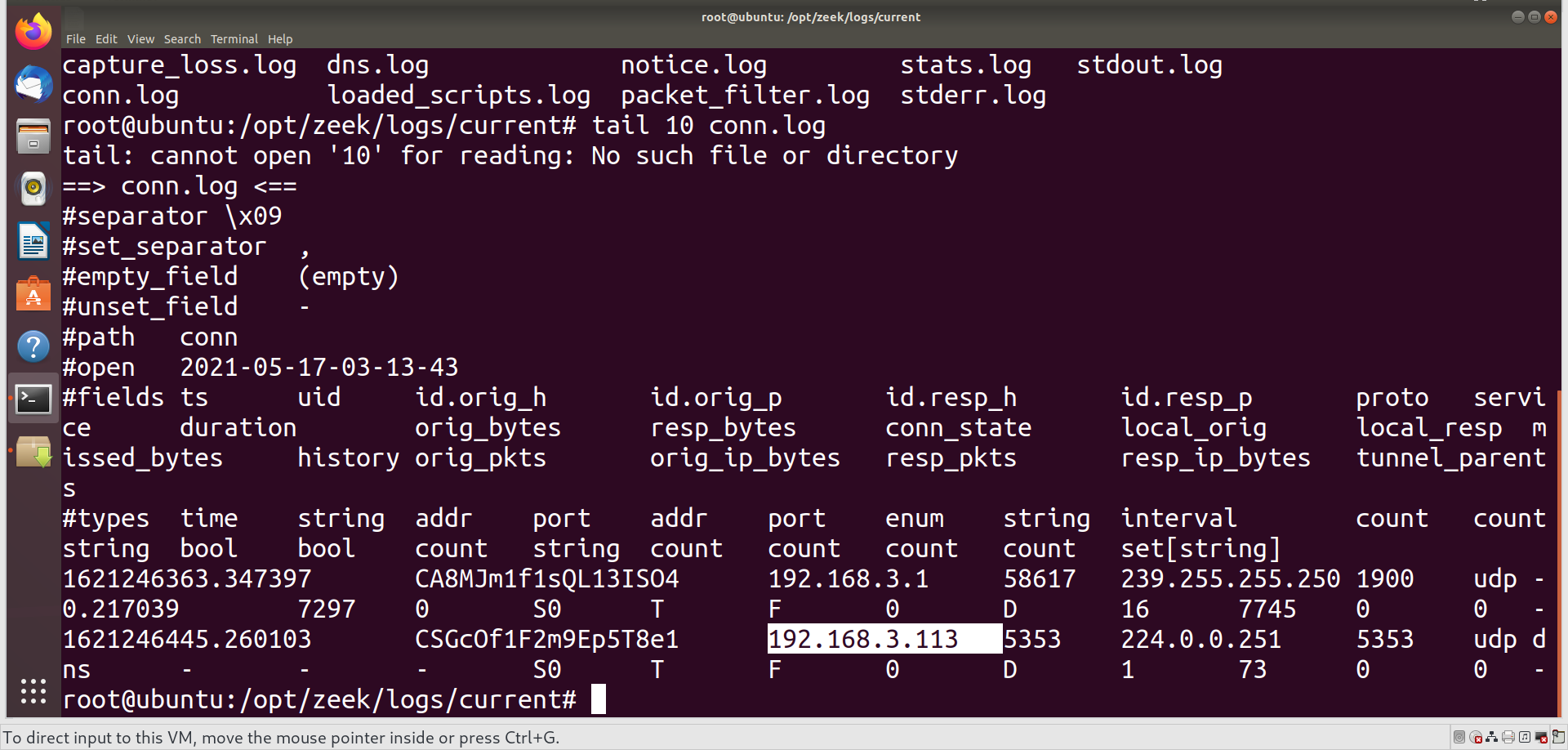
$ sudo ./opt/zeek/bin/zeekctl start



Kiểm tra log của Zeek sinh ra trong thư mục log/curent

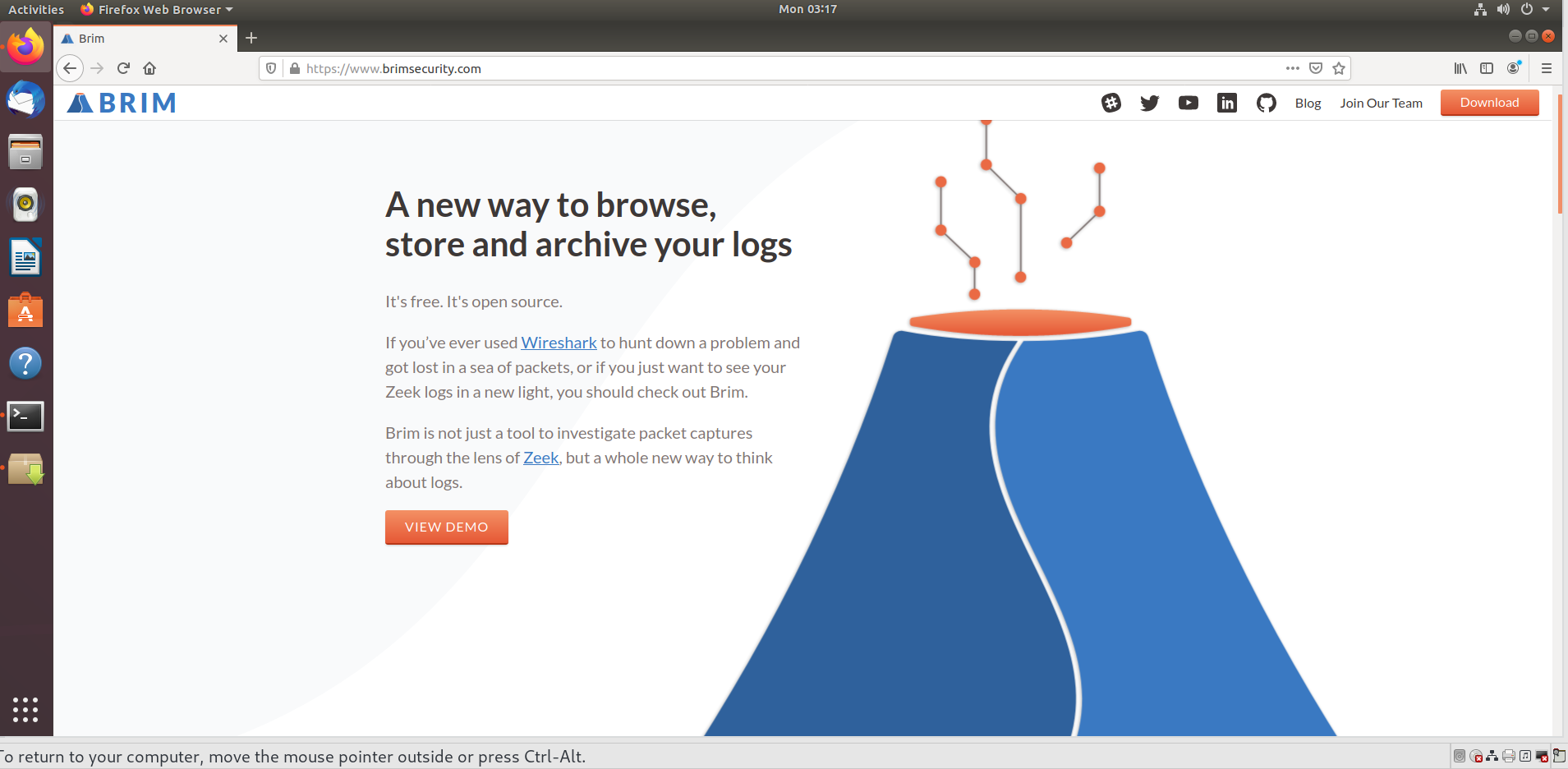


Sau khi thử kết nối internet với máy đã cài Zeek thực hiện quan sát file conn.log



Các kết nối thông qua card mạng đã được ghi nhận đầy đủ bởi Zeek .

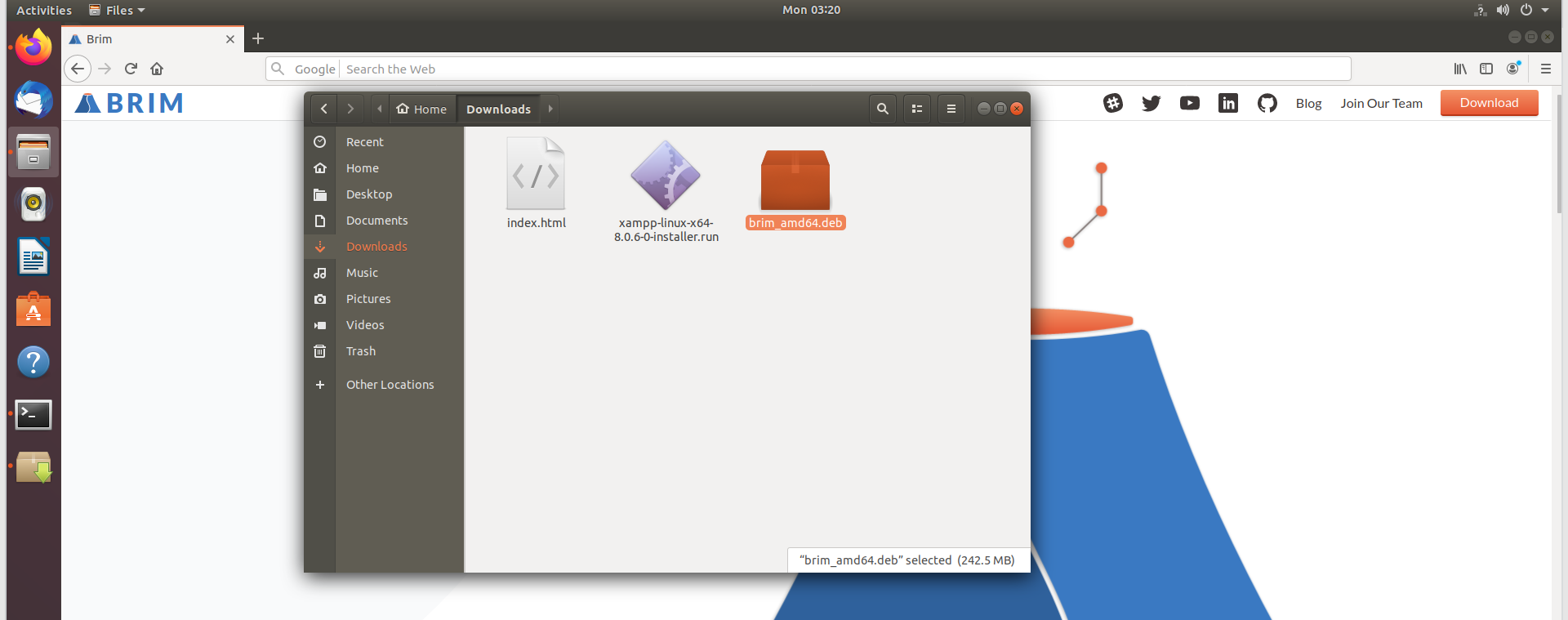
3. Thực hành quan sát và đánh giá dữ liệu thu thập bởi Zeek qua công cụ Brim



Brim là một ứng dụng phân tích và hiển thị kết quả của các file log thu được từ Zeek.

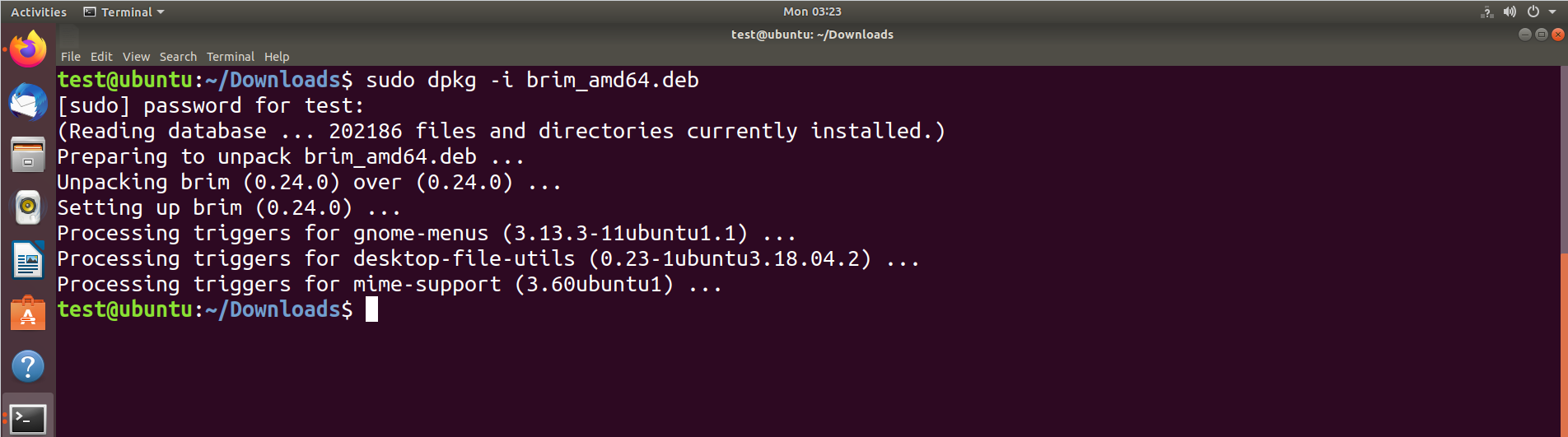
Thực hiện cài đặt Brim trên môi trường Ubuntu 18.04 LTS

Bước 1 : Tải file cài đặt của brim

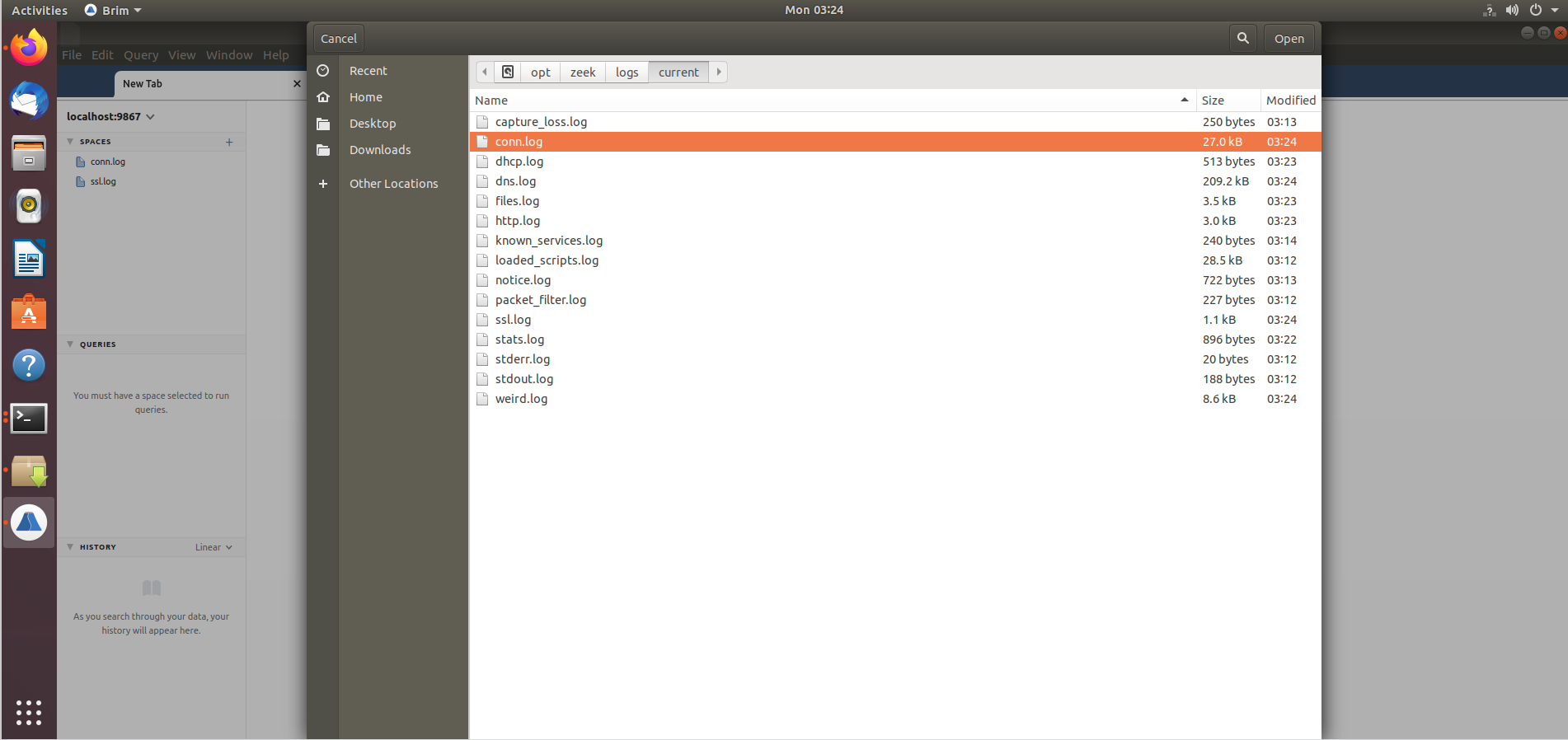


Bước 2 : Cài đặt với lệnh dpkg

$ sudo dpkg -i brim\_amd64.deb



Bước 3 : Tiến hành import log và quan sát kết quả thu được



Kết quả phân tích log từ brim

