

HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO THỰC HÀNH

**TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG**

**Bài thực hành số 1:**

**DÒ QUÉT LỖ HỔNG VÀ**

**KHAI THÁC MỘT SỐ LỖ HỔNG PHỔ BIẾN**

***Nhóm sinh viên thực hiện:*** Vũ Tiến Đạt AT170609

**Lớp:** AT17G

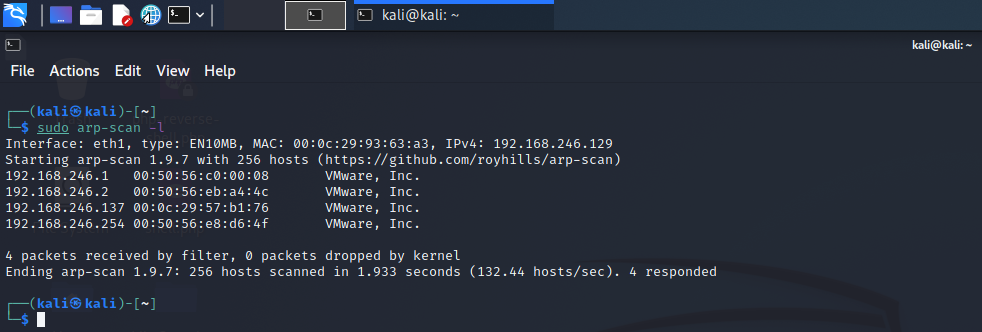
**Thời gian nộp bài:** 15/12/2023

***Giảng viên hướng dẫn****:* Phạm Minh Thuấn

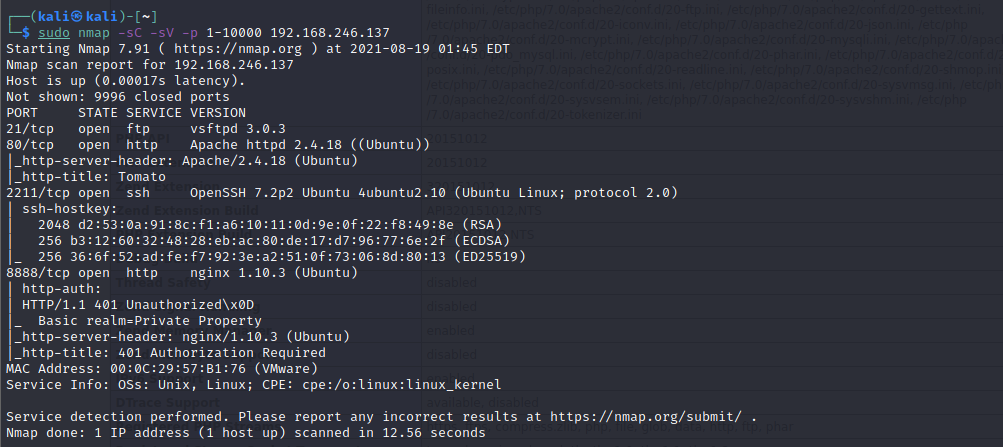
Hà Nội, 15-12-2023

Khai thác

-Sử dụng arp-scan để tìm ip target => 192.168.246.137



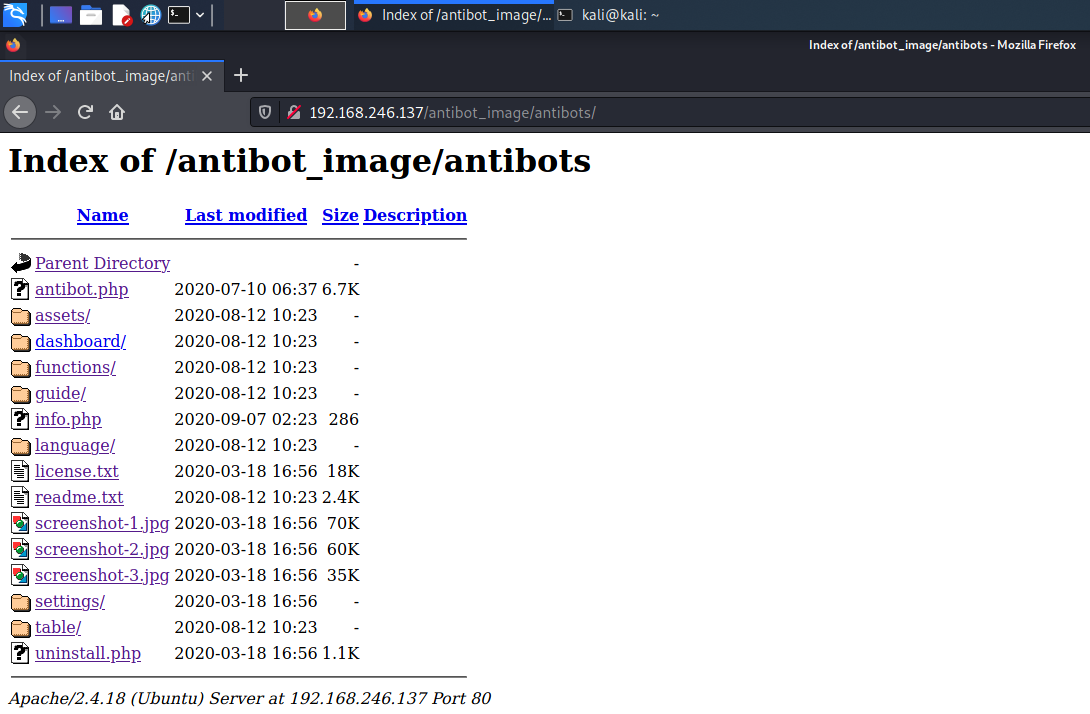
-Sử dụng nmap để quét cổng



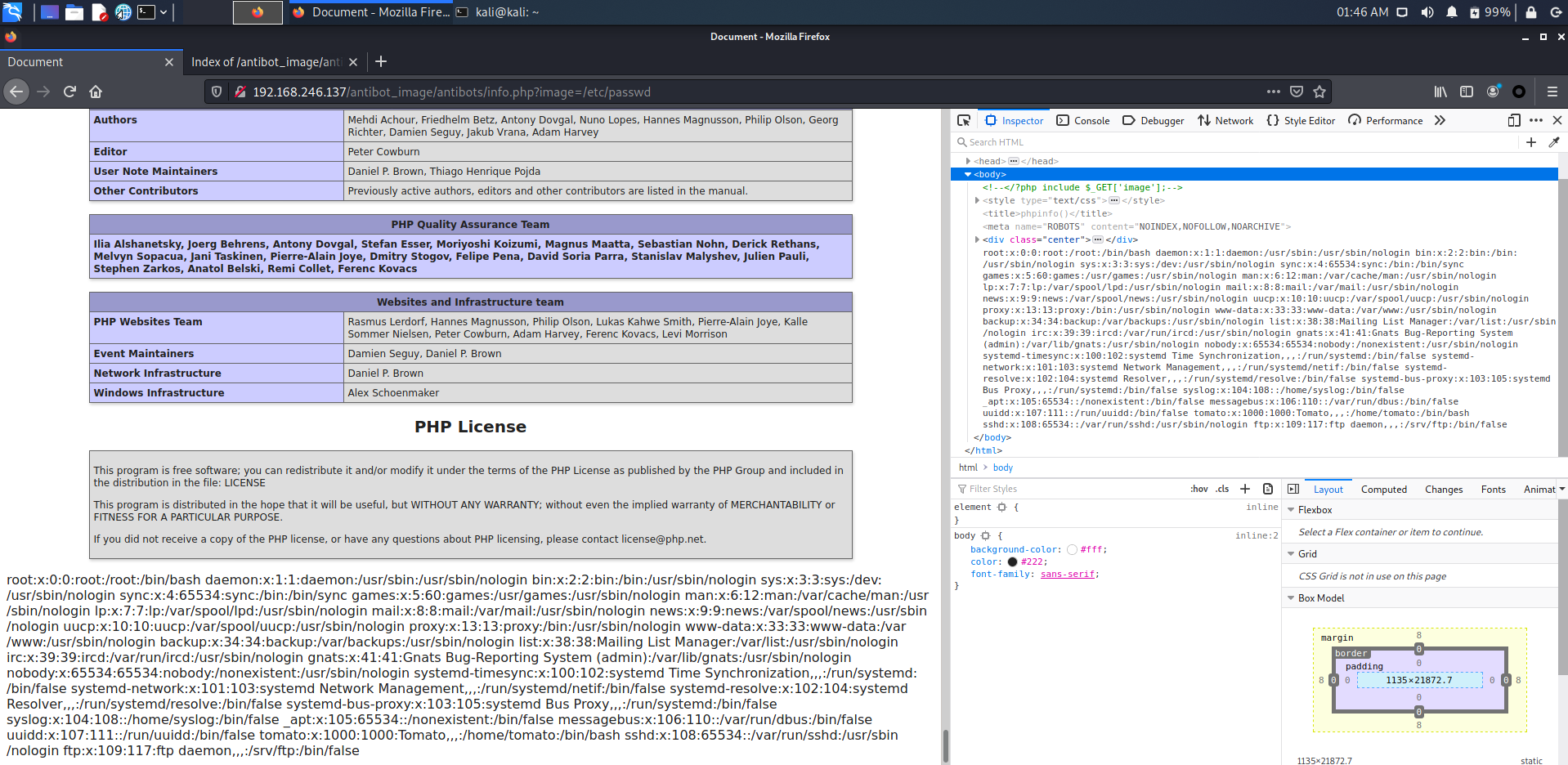
-Sử dụng tính năng quét các cổng đang mở thấy đường dẫn



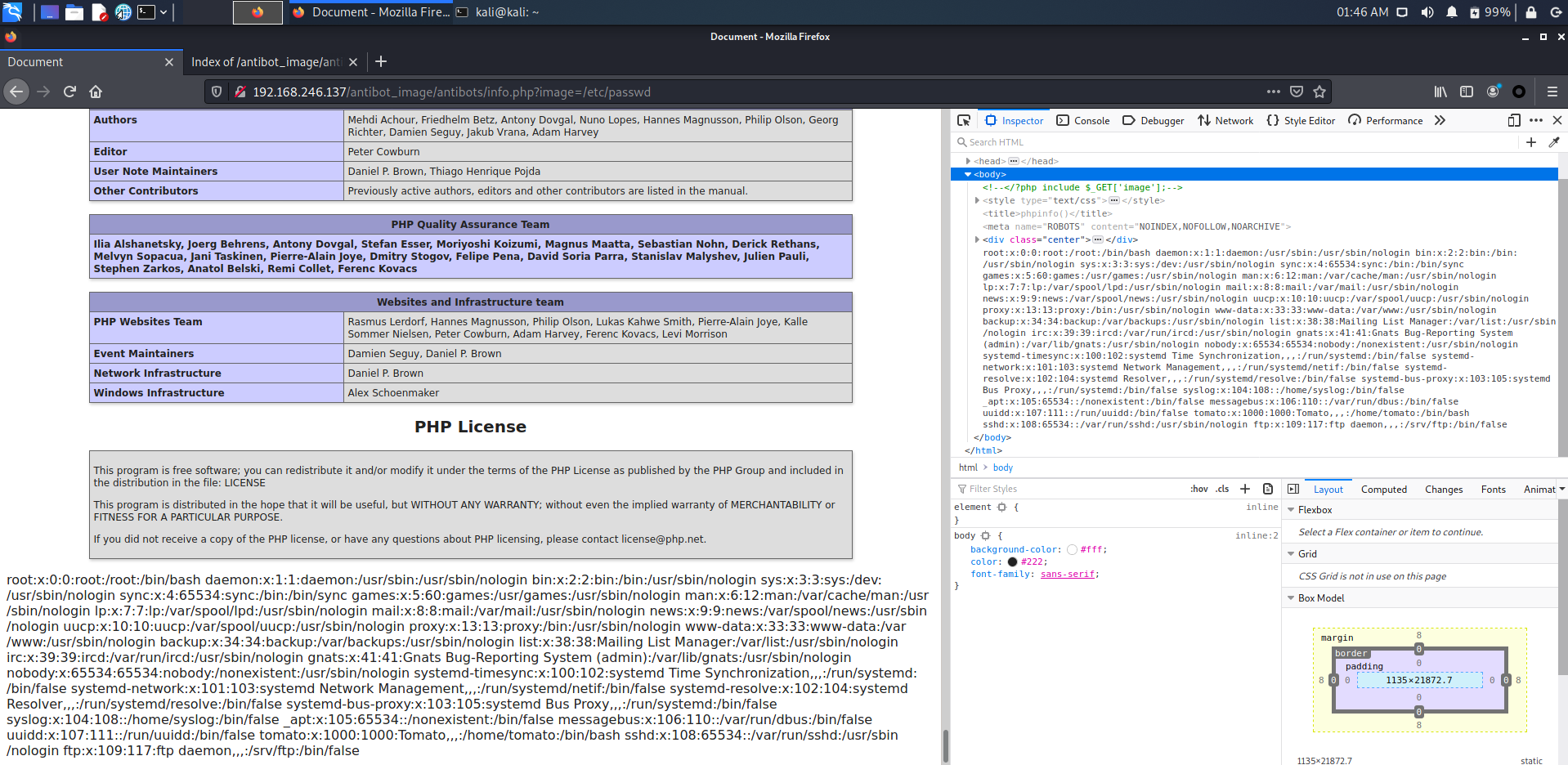
-Truy cập đường dẫn của tomato



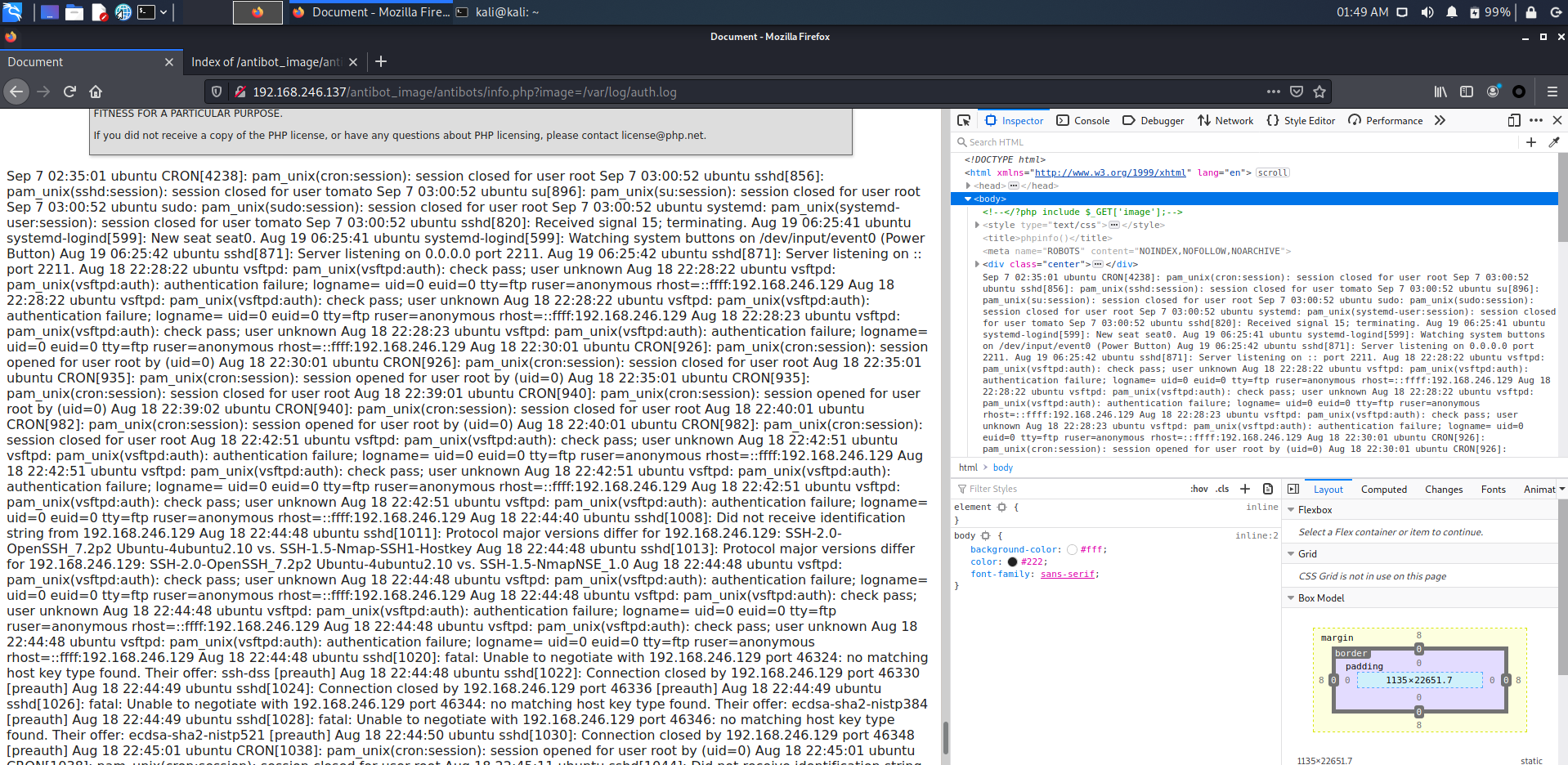
-Thêm ?image=/etc/passwd để xem lỗ hổng



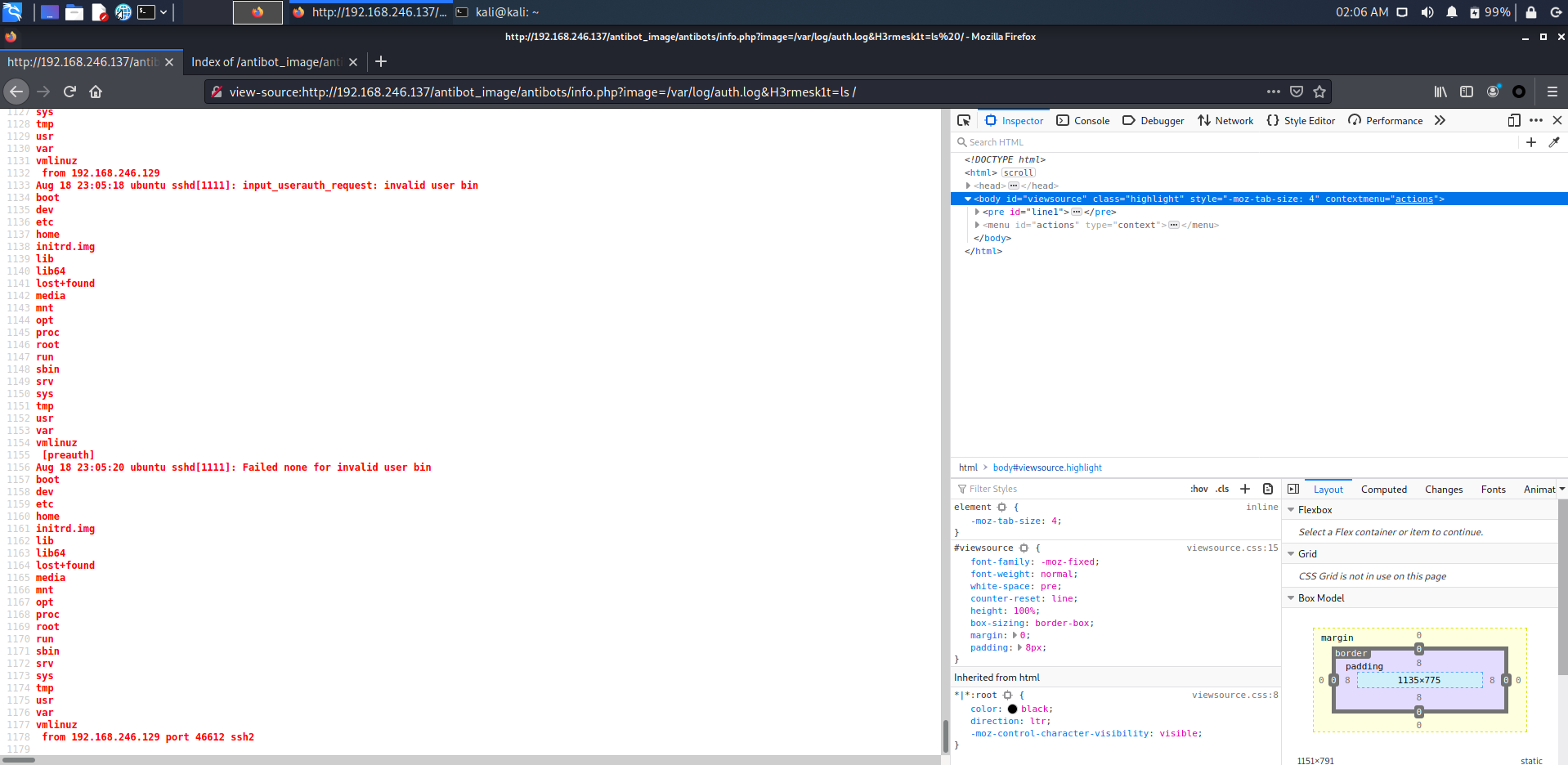
-Xem source để xem gợi ý lỗ hổng



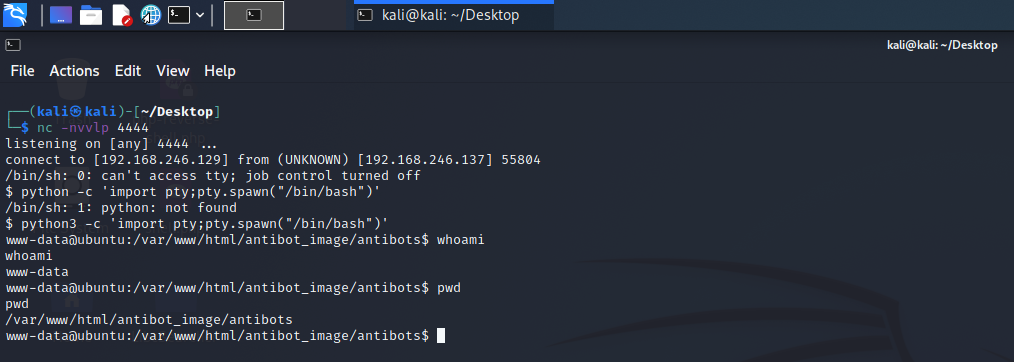
-Kiểm tra nhật ký



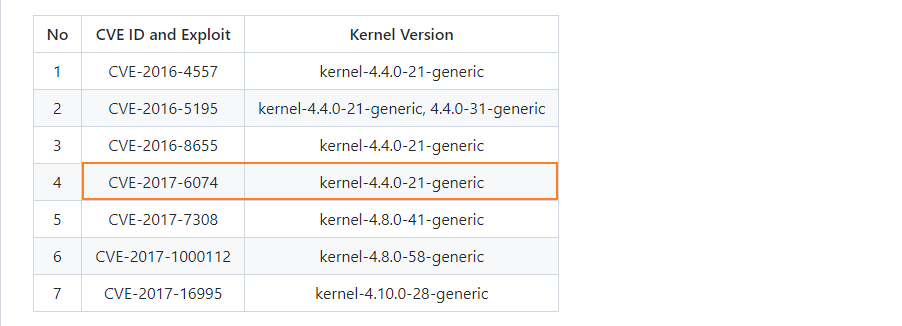
-Sử dụng connect, viết 1 đoạn trojan

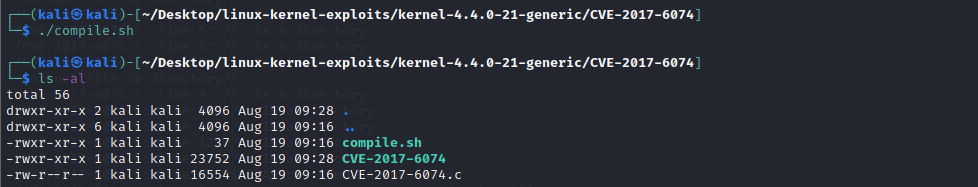


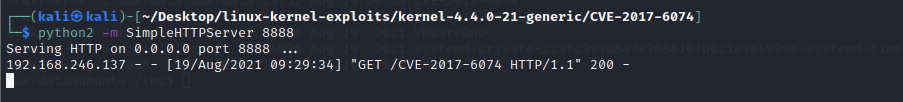
Thực hiện lệnh để biến shell thành shell tương tác

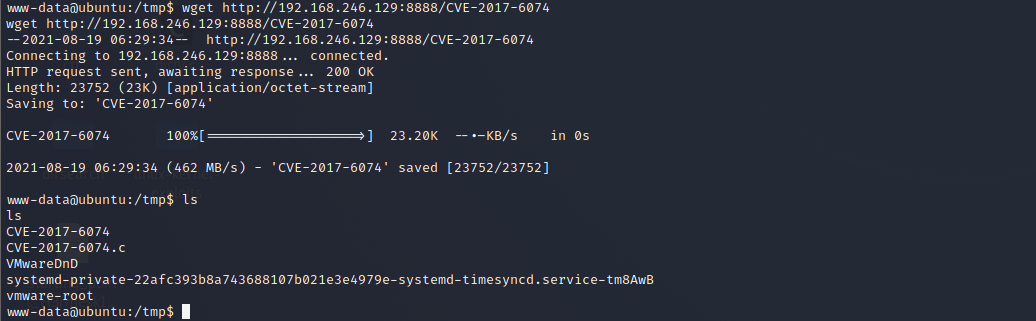


Chạy complie, thiết lập dịch vụ http và tải xuống cve 2017 6074

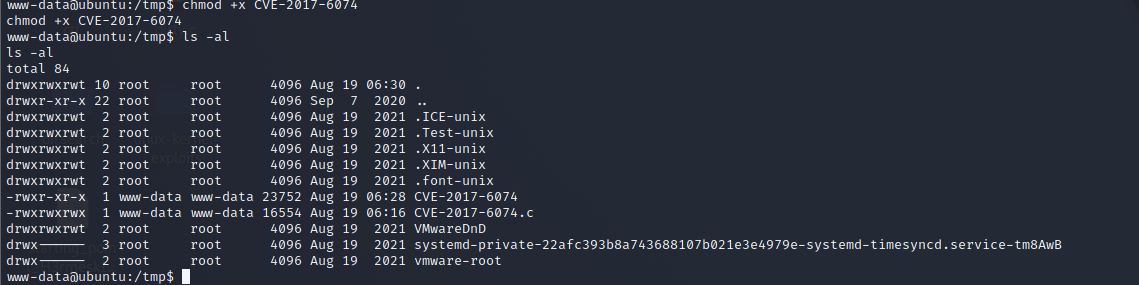








-Cấp quyền thực thi cve



-Chạy exp để nhân quyền root

