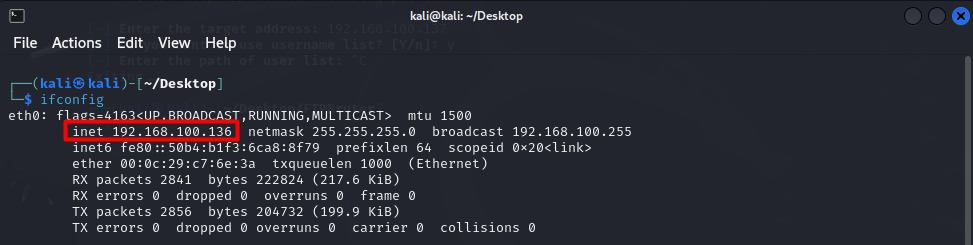
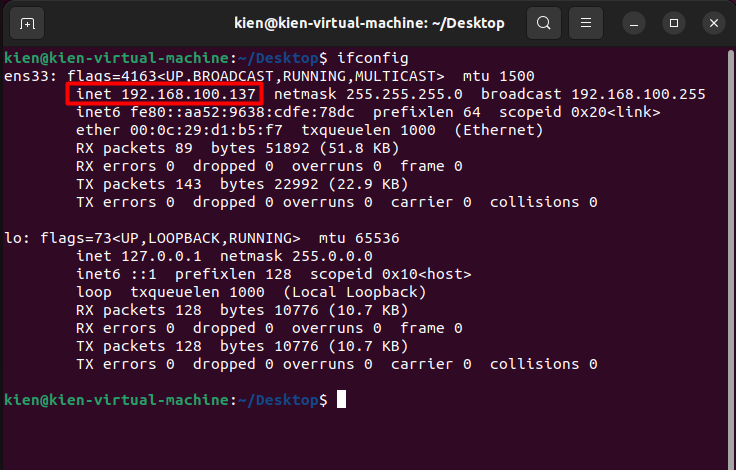
4. Demo

Kịch bản sử dụng máy kali để tấn công brute force dịch vụ ftp. Sử dụng Zeek Scripting để phát hiện Brute-force.

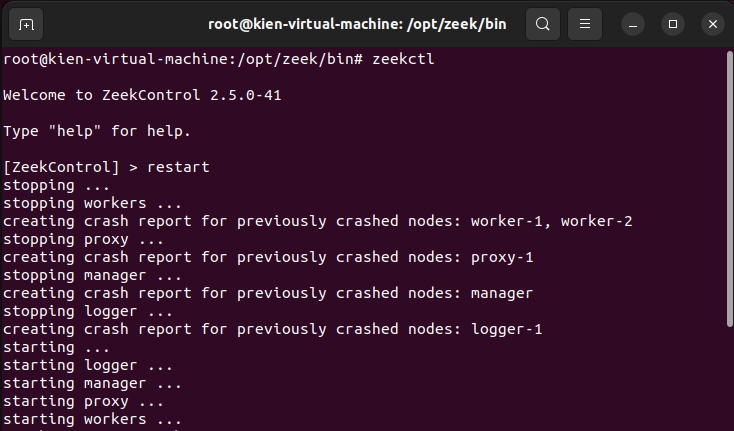
Địa chỉ Ip máy kali

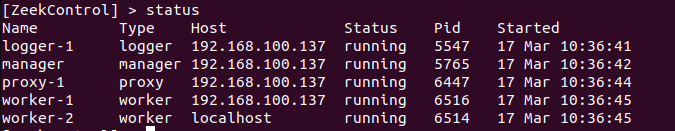


Địa chỉ Ip máy Ubuntu



Khởi động zeek

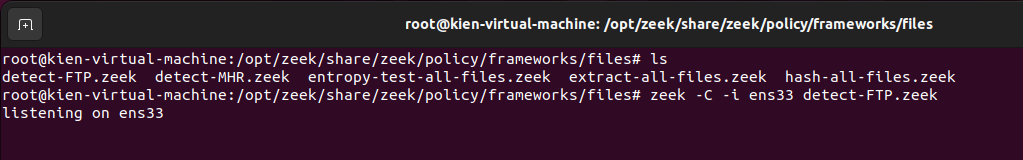




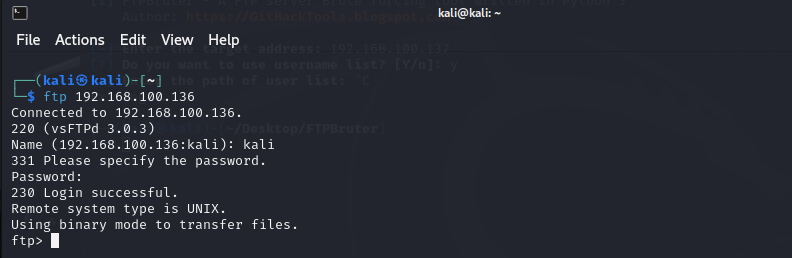
Vào đường dẫn /opt/zeek/share/zeek/policy/frameworks/files chạy file detect-FTP.zeek bằng câu lệnh:

*zeek -C -i ens33 detect-FTP.zeek*

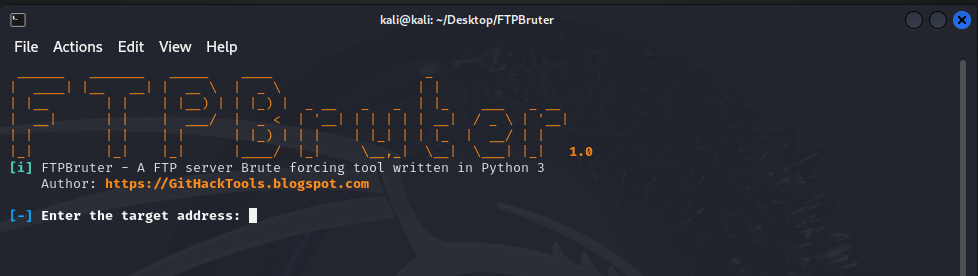
câu lệnh "zeek -C -i ens33 detect-FTP.zeek" sẽ chạy Zeek trên giao diện mạng "ens33", cho phép Zeek phân tích các gói tin có checksum không hợp lệ và sử dụng tệp script "detect-FTP.zeek" để phát hiện các hoạt động FTP trong gói tin mạng.



Kết nối đến máy ubuntu



Sử dụng công cụ FTPBruter để tấn công brute force



Địa chỉ Ip mục tiêu là địa chỉ Ip máy ubuntu



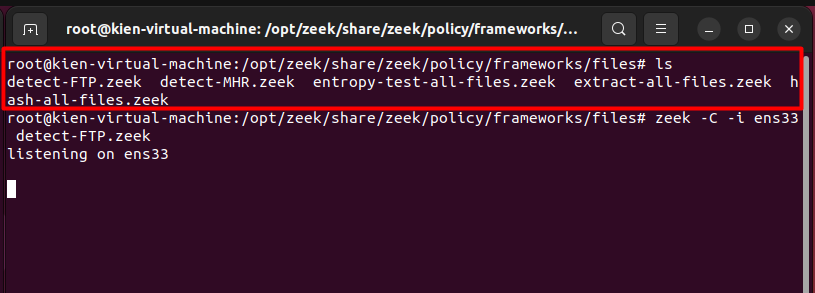
Khai thác thành công



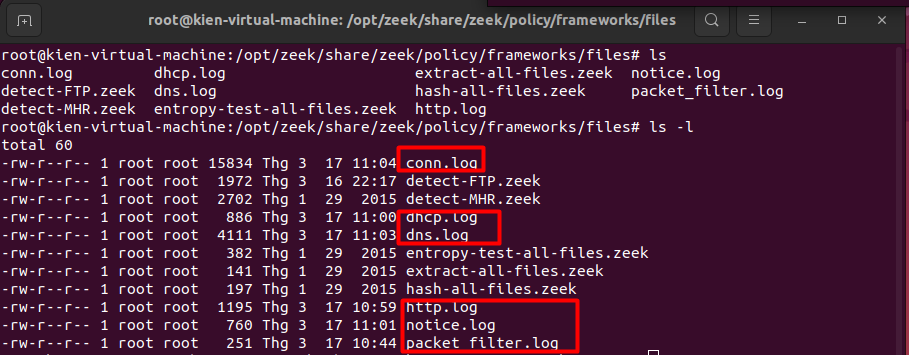
Truy cập thư mục chứa file detect-FTP.zeek:

*/opt/zeek/share/zeek/policy/frameworks/files*

Trước khi chạy file script detect-FTP.zeek

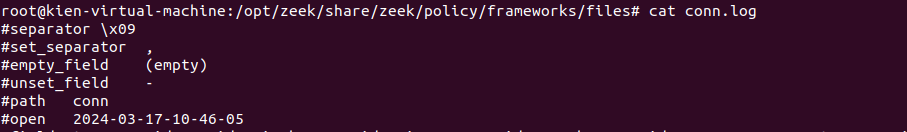


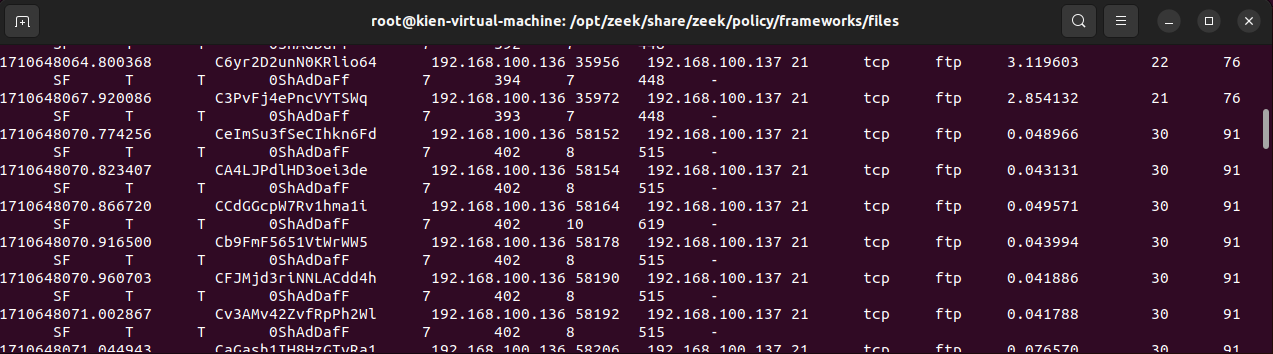
Sau khi tấn công thì trong thư mục này sẽ xuất hiện những file logs



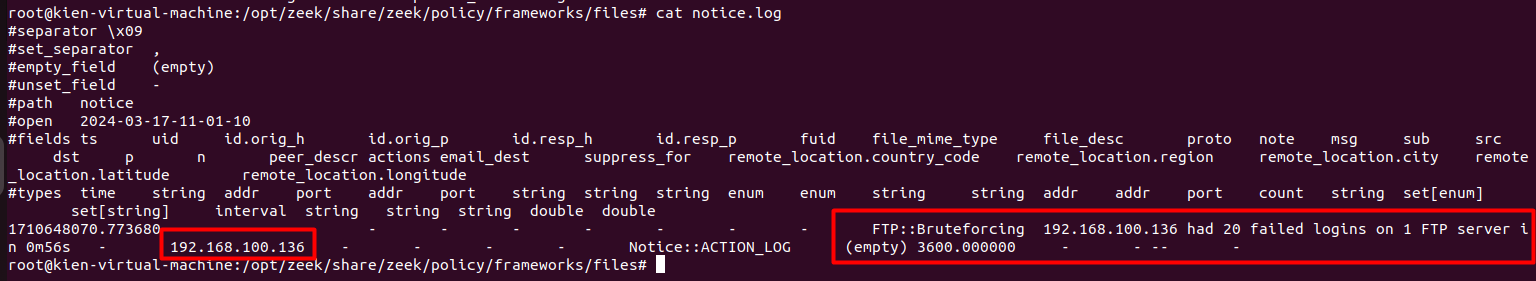
Ta xem các file logs:

File conn.log





Files notice.log



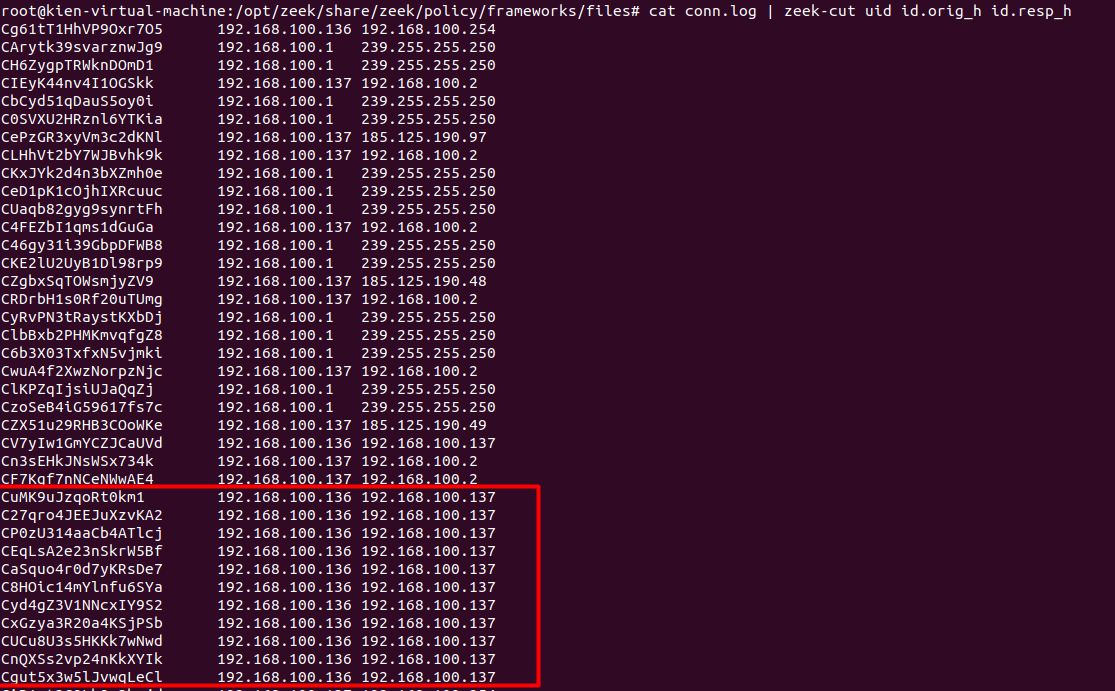
Thấy được thông báo FTP:Bruteforcing và có địa chỉ Ip từ máy kali

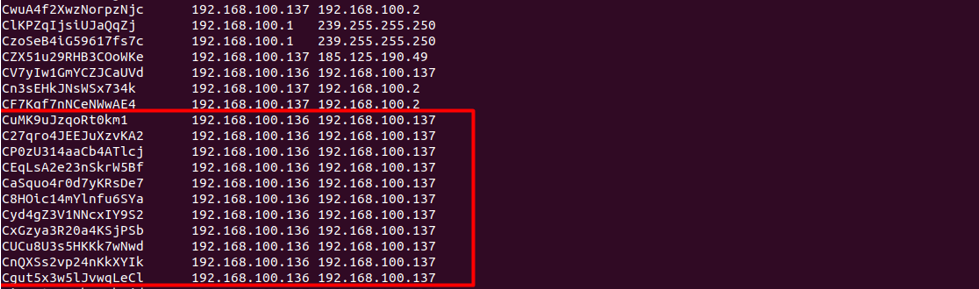
🡪 Zeek đã phát hiện được xâm nhập bất thường từ máy kali

Sử dụng câu lệnh: **cat conn.log | zeek-cut uid id.orig\_h id.resp\_h**

("zeek-cut": Đây là một công cụ dòng lệnh Zeek để cắt (cắt giảm) các trường dữ liệu từ đầu ra của Zeek logs.)

Câu lệnh **"cat conn.log | zeek-cut uid id.orig\_h(địa chỉ Ip nguồn) id.resp\_h(địa chỉ ip đích)"** sẽ hiển thị các giá trị của các trường "uid", "id.orig\_h" và "id.resp\_h" từ tệp tin "conn.log" trên màn hình.





File Script: detect-FTP.zeek

