BÁO CÁO BÀI THỰC HÀNH SỐ 2

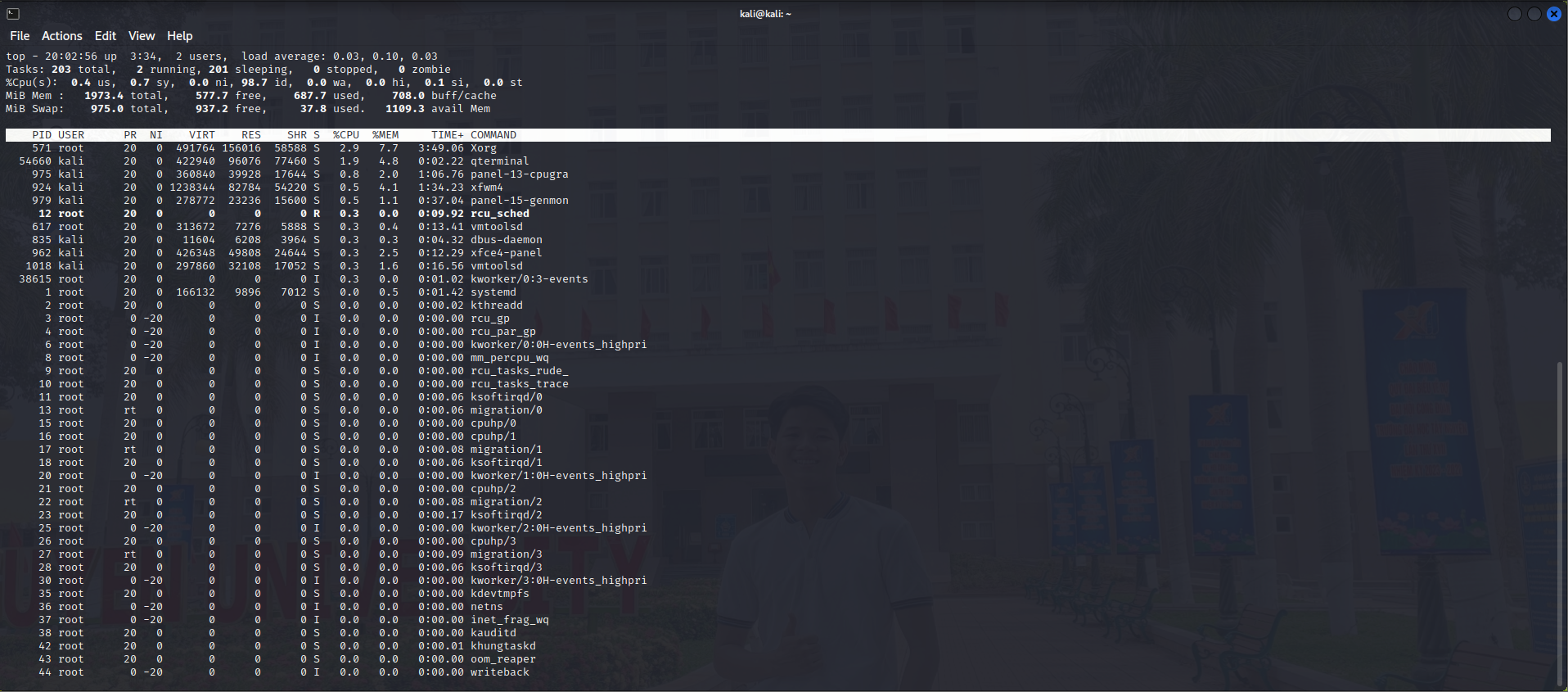
PHÂN TÍCH MỘT SỐ KỸ THUẬT TẤN CÔNG DoS

***Họ tên Sinh viên : Nguyễn Thanh Ý***

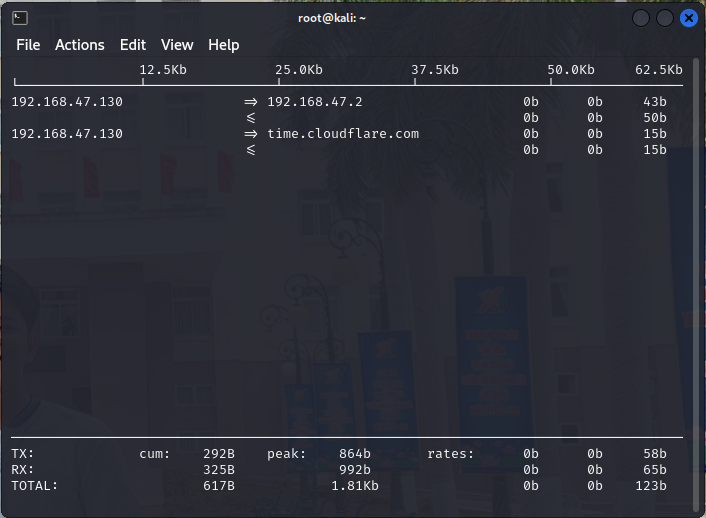
**KẾT QUẢ THỰC HÀNH**

1. **Kịch bản 1**

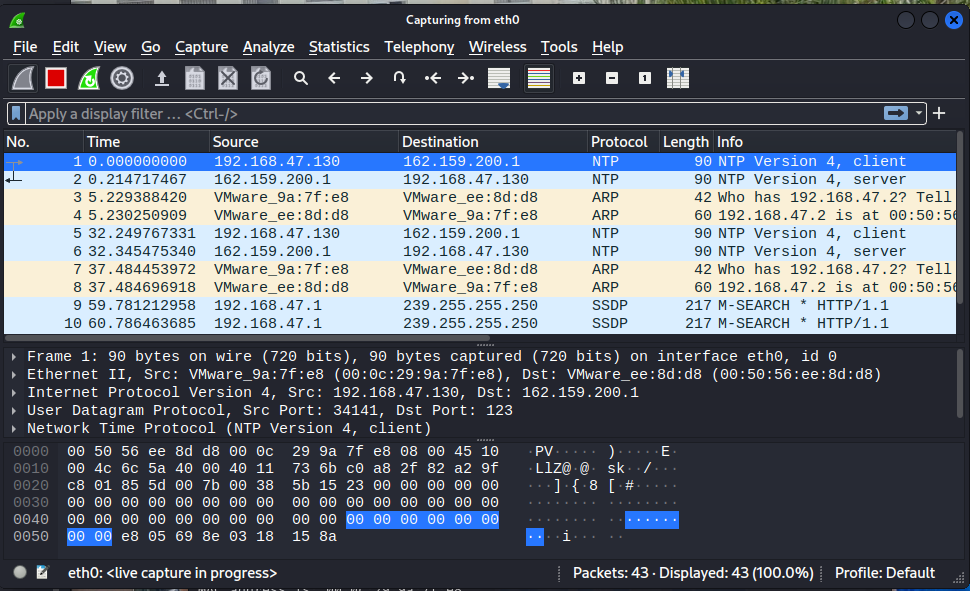
* kết quả thực hiện lệnh **top** và mức tiêu thụ tài nguyên của CPU và RAM của máy trước khi bị tấn công là khá thấp và ổn định

****

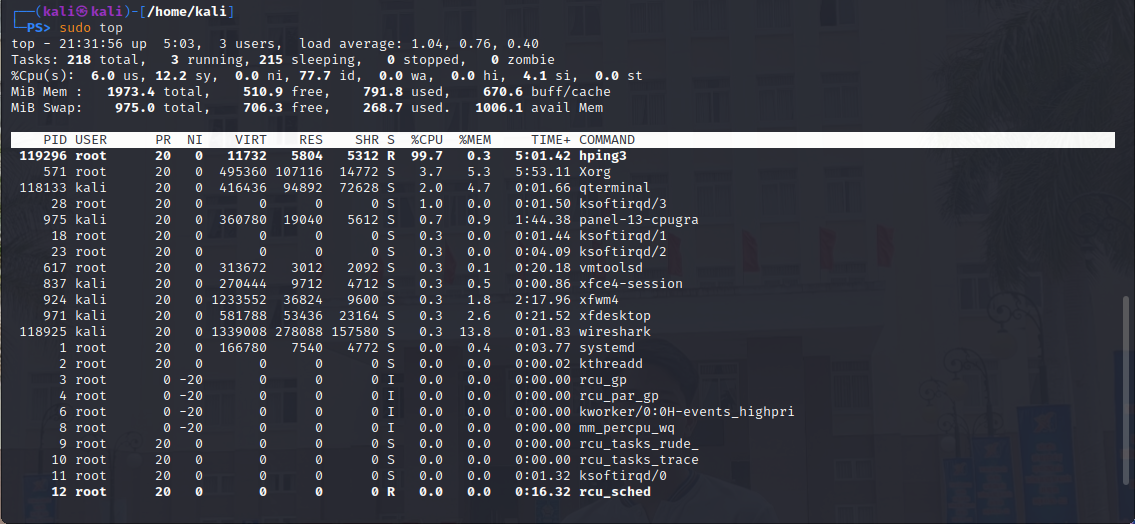
* lưu lượng máy chủ nạn nhân trước khi bị tấn công khá là thấp, gần như bằng 0

****

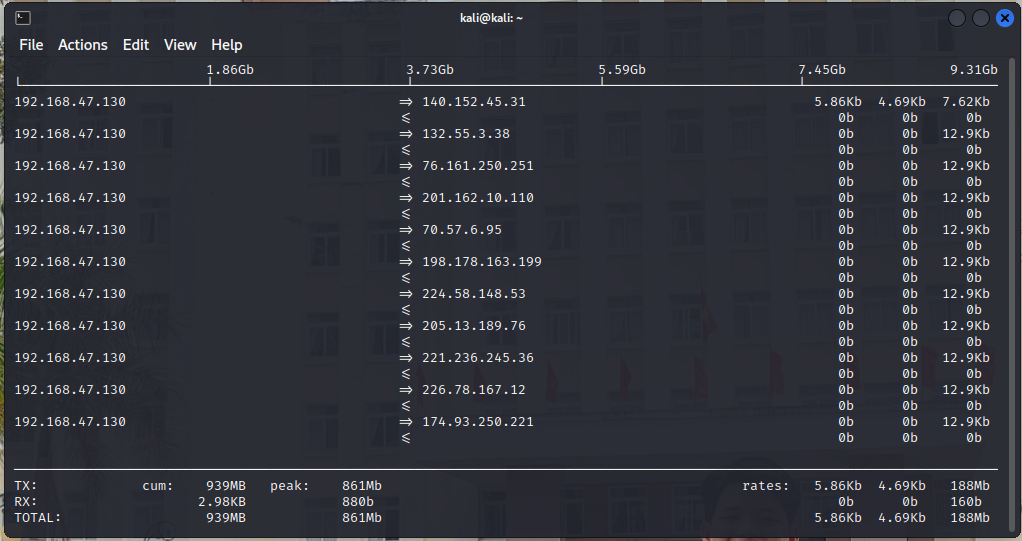
* Khởi động wireshark để bắt gói tin trên cạc mạng eth0



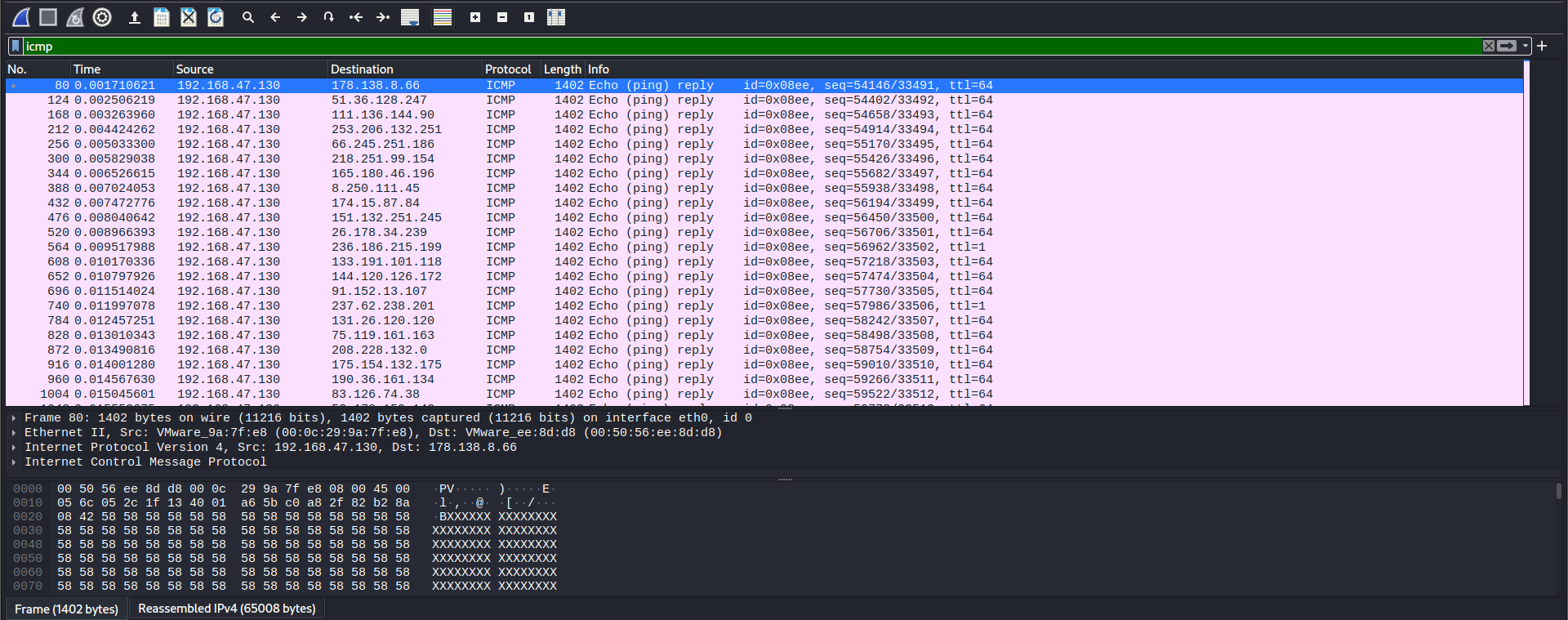
* Máy chủ nạn nhân trong khi bị tấn công thì CPU gần như là 100% user root có port 119296 đã chiếm 99.7%



* Iftop



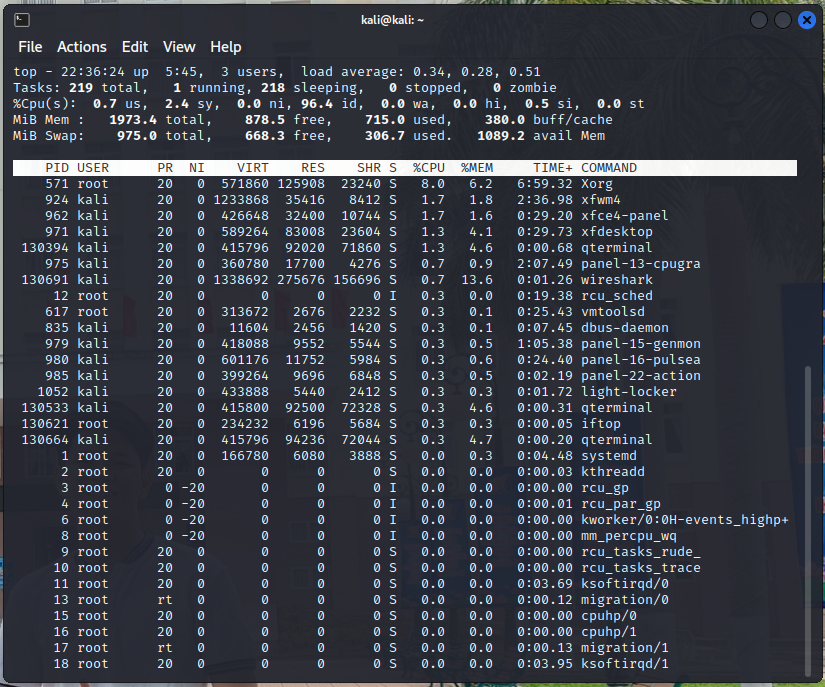
* Đặc điểm lưu lượng bằng Wireshark trên máy nạn nhân là icmp liên tục nhận được yêu cầu ping từ phía máy tấn công.



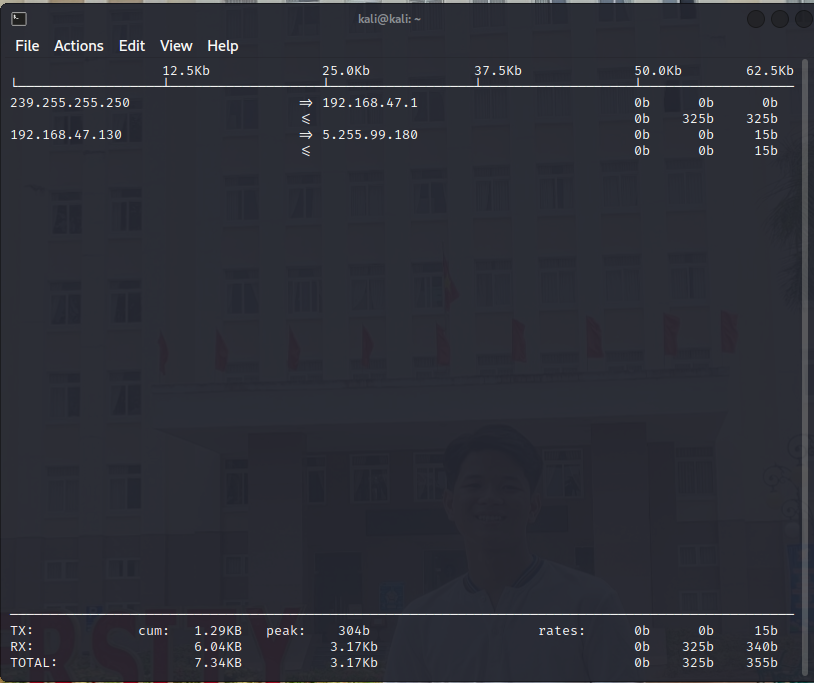
* Kỹ thuật DoS (Denial of Service) khi sử dụng lệnh sudo hping3 --icmp 192.168.47.130 -d 65000 --flood --rand-source được gọi là ICMP flood attack (tấn công lũy tiến ICMP).
* Kỹ thuật ICMP flood attack này nhằm mục đích làm quá tải và làm ngập lụt (flood) hệ thống mạng mục tiêu bằng việc gửi một lượng lớn gói tin ICMP liên tục. Điều này có thể làm cho hệ thống mục tiêu trở nên không thể phản hồi đúng và dẫn đến tình trạng từ chối dịch vụ (DoS).

1. **Kịch bản 2**

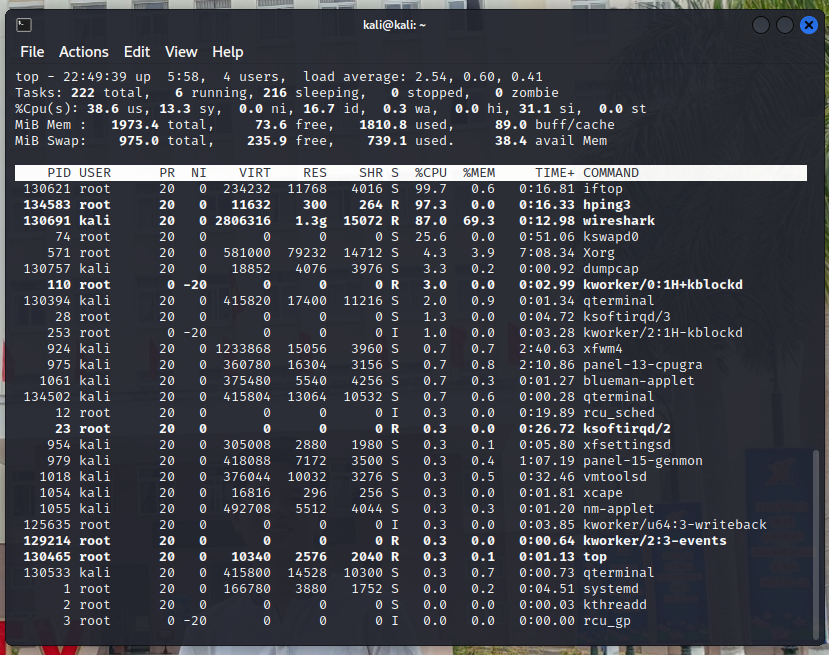
* Cpu và Ram trên máy chủ khi chưa bị tấn công rất ít khoản 3-5%

****

* Lưu lượng mà máy chủ nạn nhân phải nhận trước khi bị tấn công khá là ít, gần như bằng 0



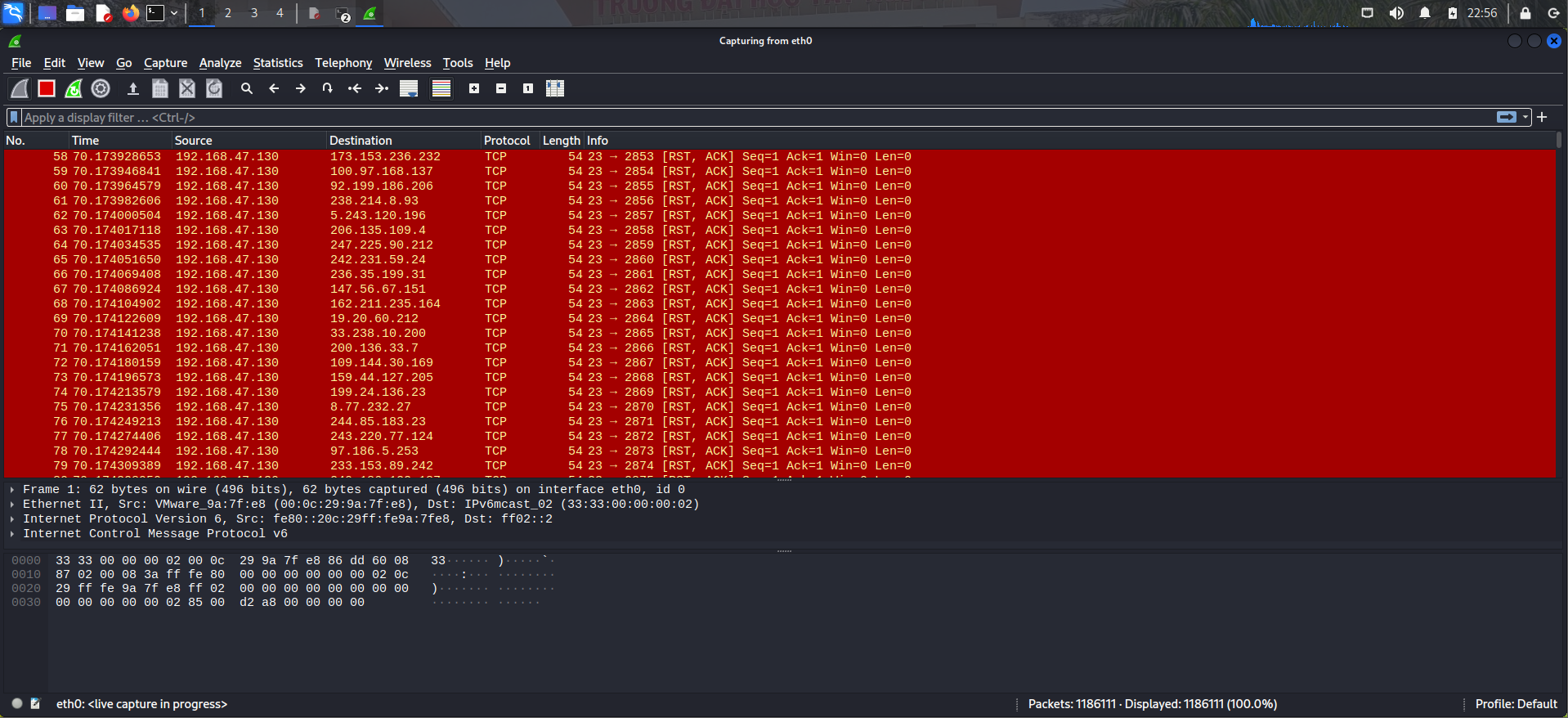
* Khi bị tấn công bằng kịch bản 2 thì CPU và RAM cũng gần như ở mức tối đa

****

* Lưu lượng máy chủ nạn nhân cũng phải nhận lượng dữ liệu lớn liên tục, khoản 100MB mỗi giây

****

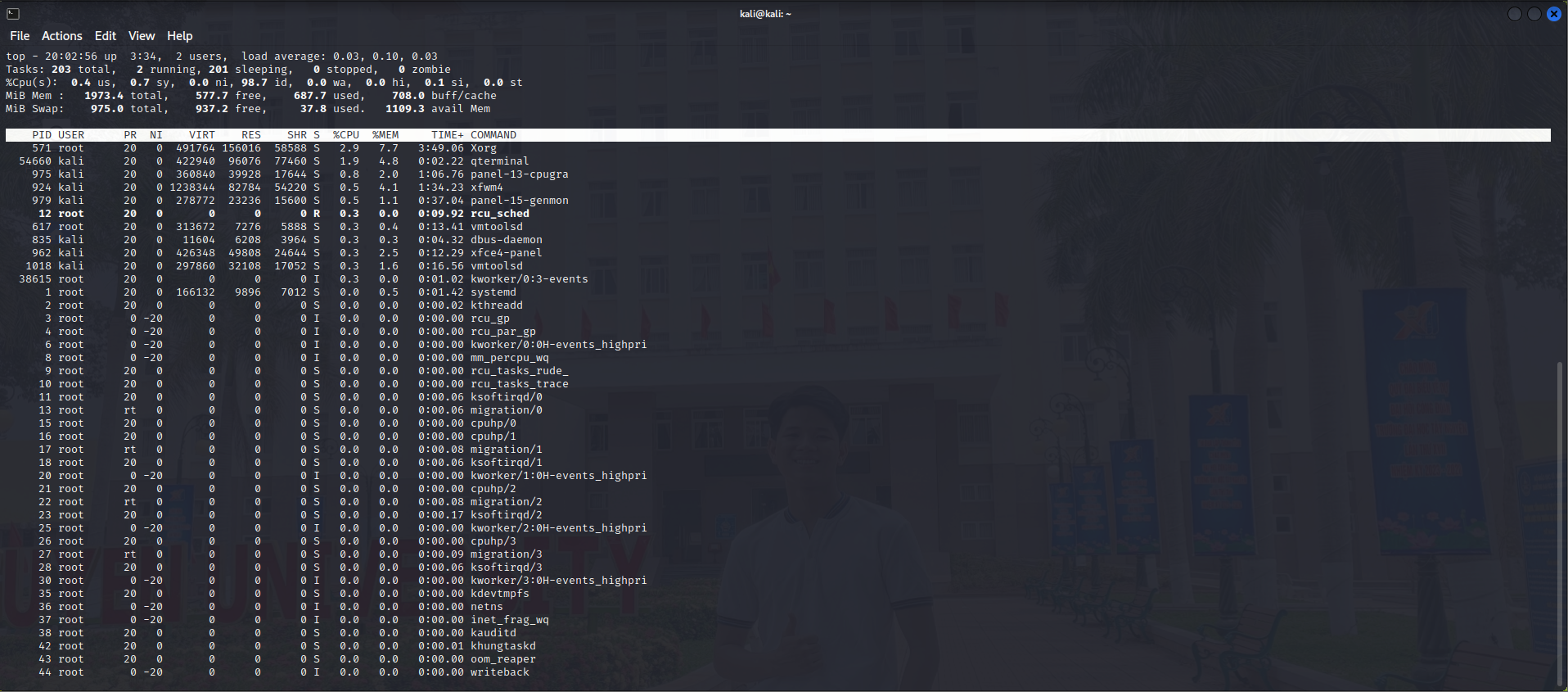
* Khi bị tấn công máy chủ nạn nân liên tục nhận các yêu cầu kết nối TCP

****

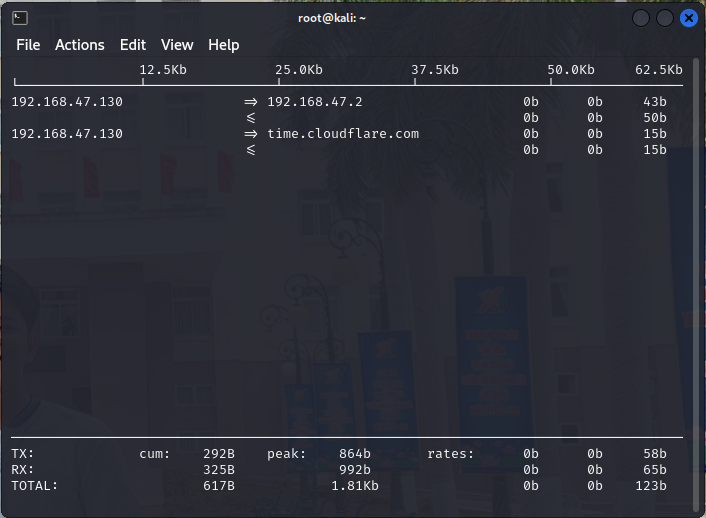
* Kỹ thuật DoS (Denial of Service) khi sử dụng lệnh sudo hping3 -S -p 23 192.168.47.130 --flood --rand-source được gọi là SYN flood attack (tấn công lũy tiến SYN).
* Kỹ thuật SYN flood attack này nhằm tạo ra một lượng lớn các yêu cầu kết nối TCP (Transmission Control Protocol) bằng cách gửi gói tin SYN đến hệ thống mục tiêu mà không hoàn thành quá trình kết nối. Điều này có thể làm cho tài nguyên của hệ thống bị tiêu tốn và không thể phục vụ các yêu cầu kết nối hợp lý, dẫn đến tình trạng từ chối dịch vụ (DoS).
* Có thể giới hạn kết nối TCP hoặc cấu hình tường lửa để chặn lưu lượng gói tin SYN từ các nguồn không xác định.

1. **Kịch bảng 3**

* kết quả thực hiện lệnh **top** và mức tiêu thụ tài nguyên của CPU và RAM của máy trước khi bị tấn công là khá thấp và ổn định

****

* lưu lượng máy chủ nạn nhân trước khi bị tấn công khá là thấp, gần như bằng 0

****

* Khởi động wireshark để bắt gói tin trên cạc mạng eth0

