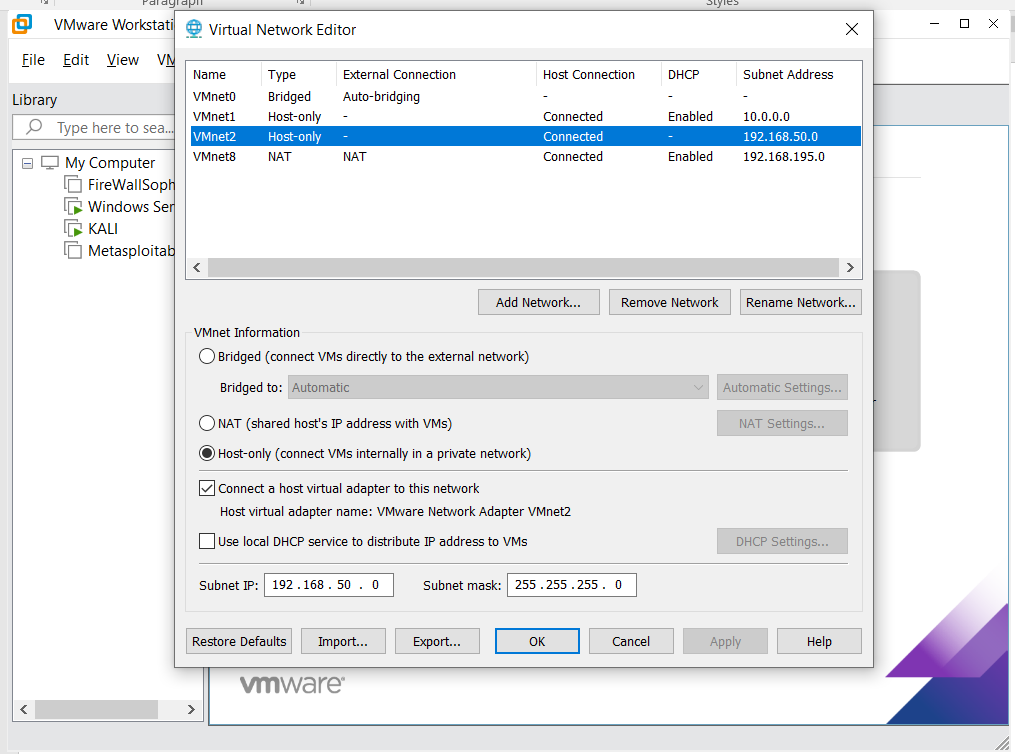
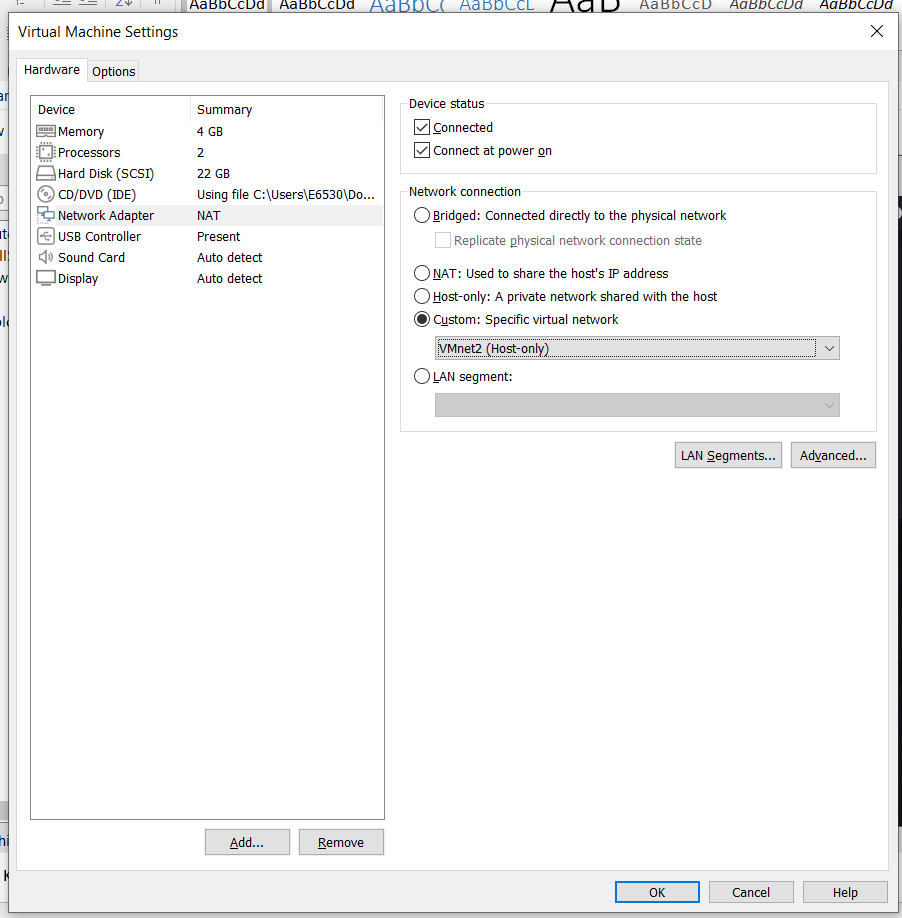
Chỉnh sửa ip

Trong vmw, mở edit -> virtual network editor -> change setting -> thêm vmnet2

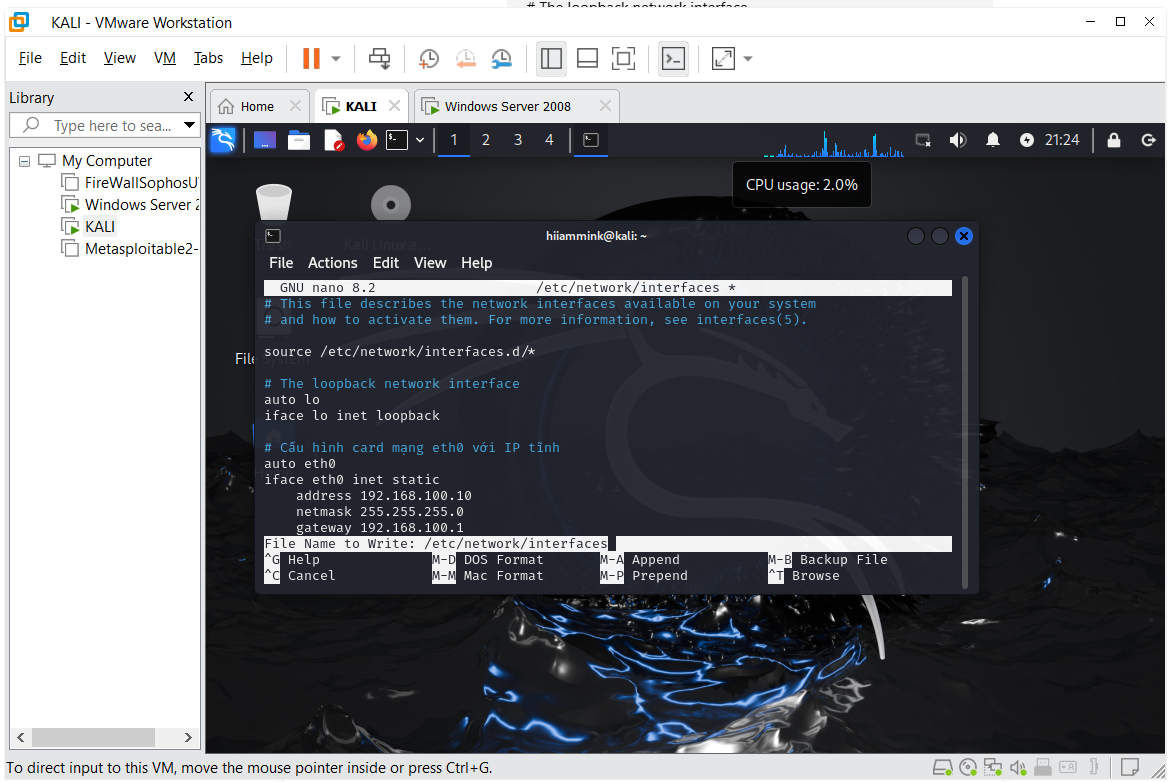
Chỉnh host-only -> tắt dchp để set ip tĩnh cho máy ảo



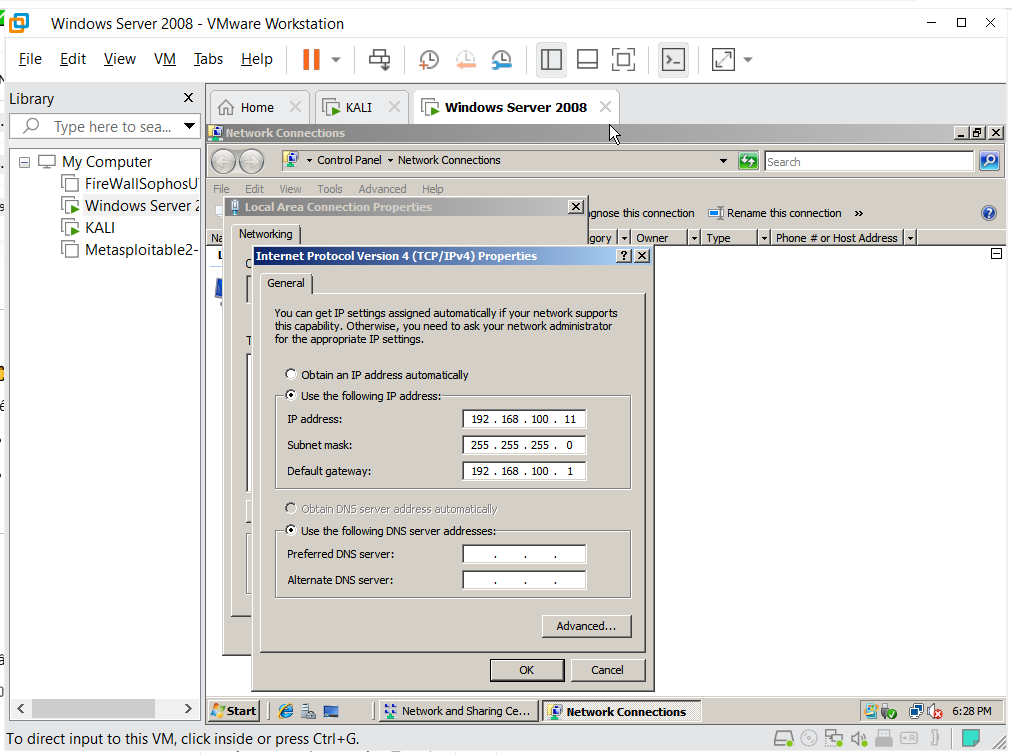
Gán card mạng cho máy ảo:



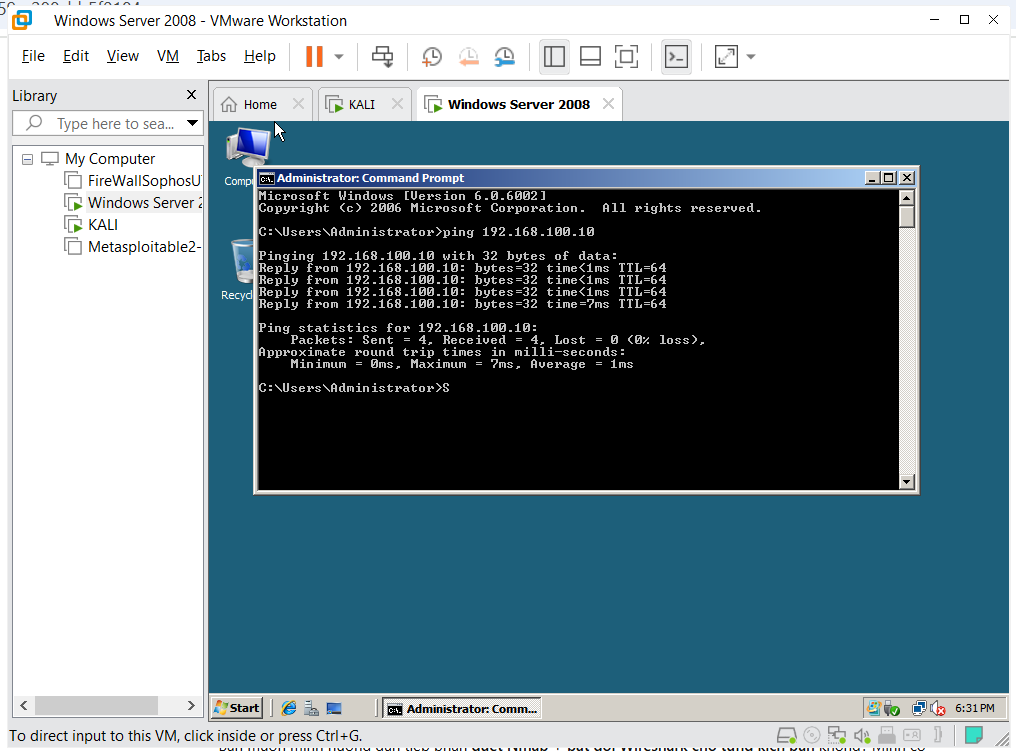
Chỉnh ip tĩnh cho máy ảo kali:



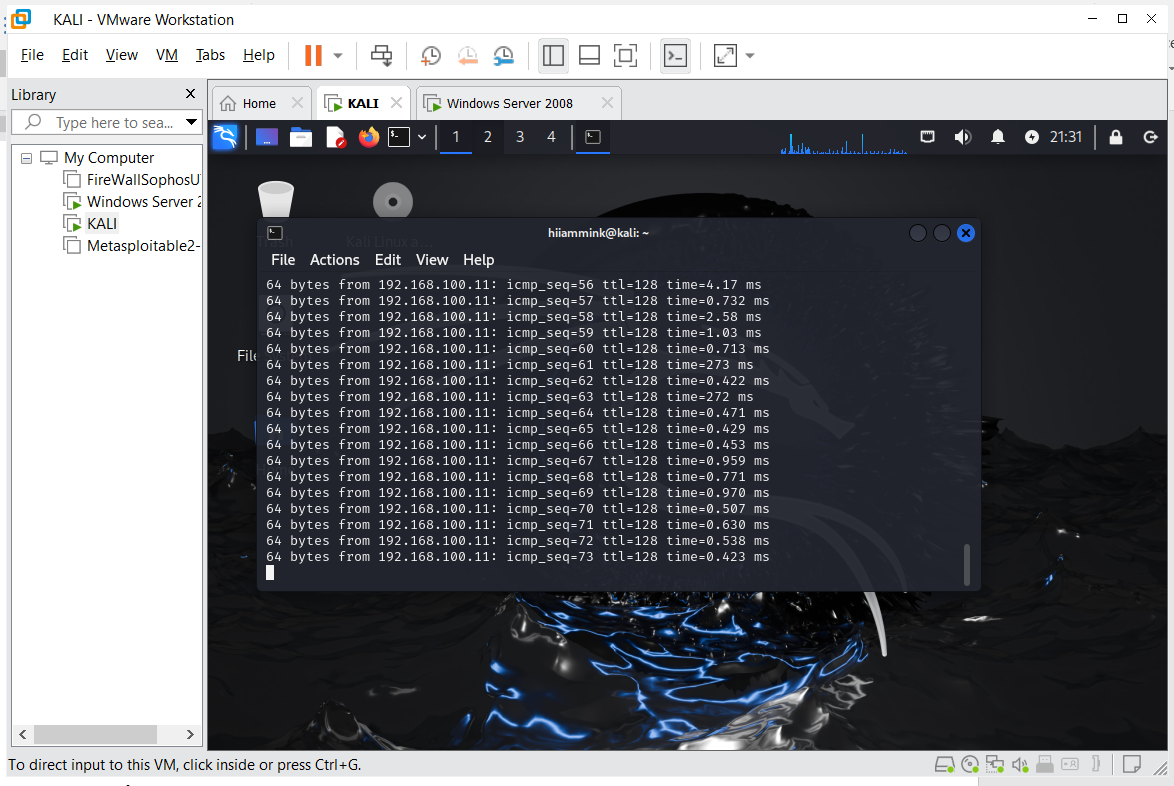
Chỉnh ip tĩnh cho máy ảo window 2008:



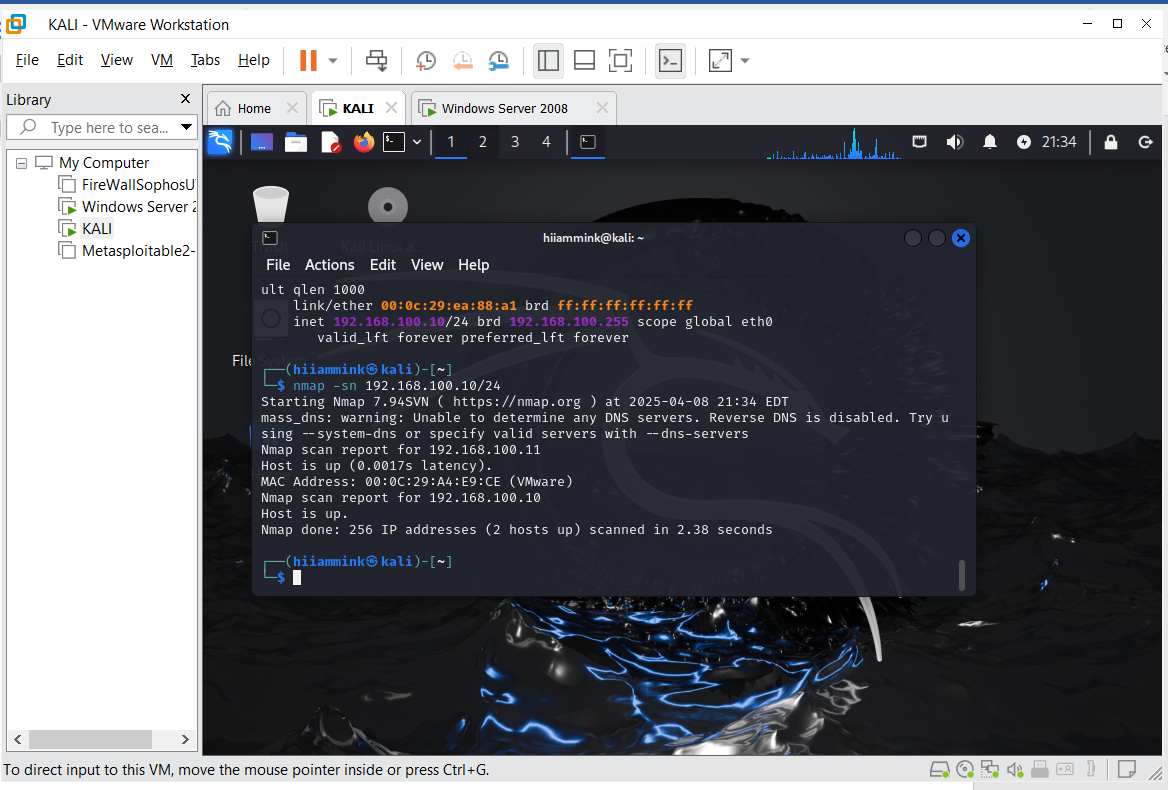
Kiểm tra kết nối ping trên window

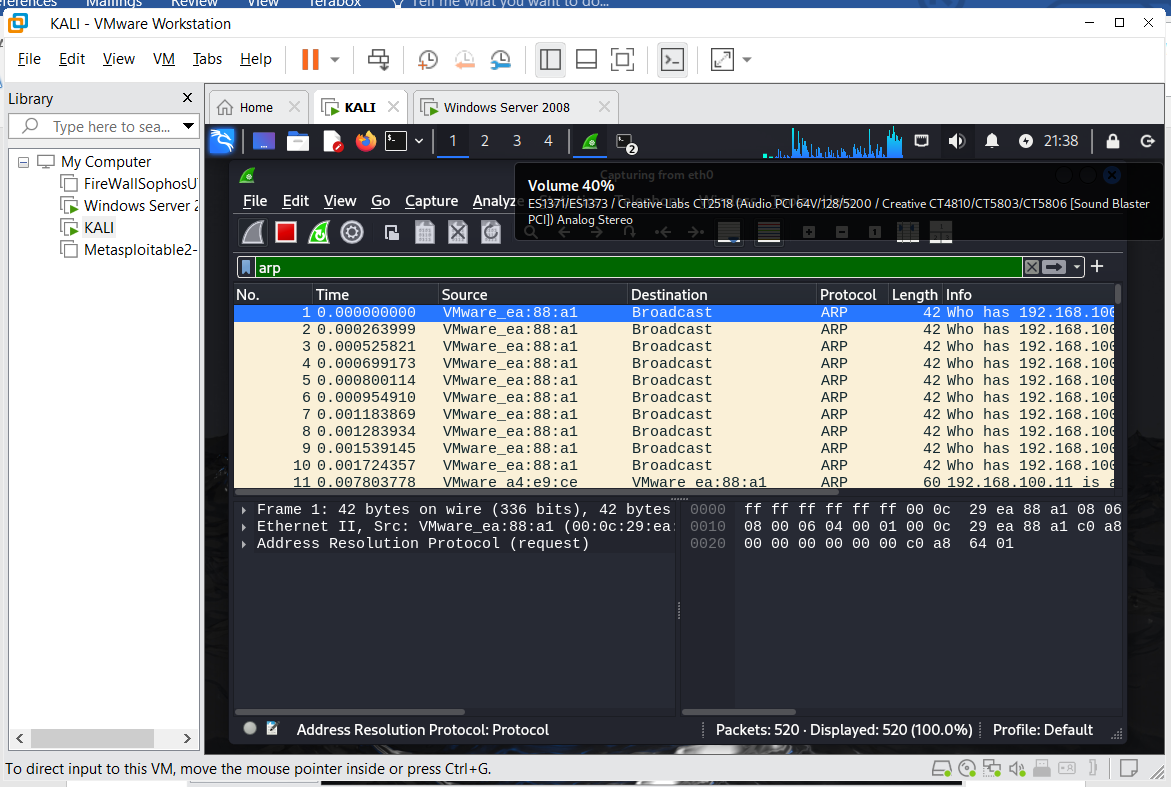


Kiểm tra trên kali



Kịch bản 1: nmap –sn 192.168.100.10/24

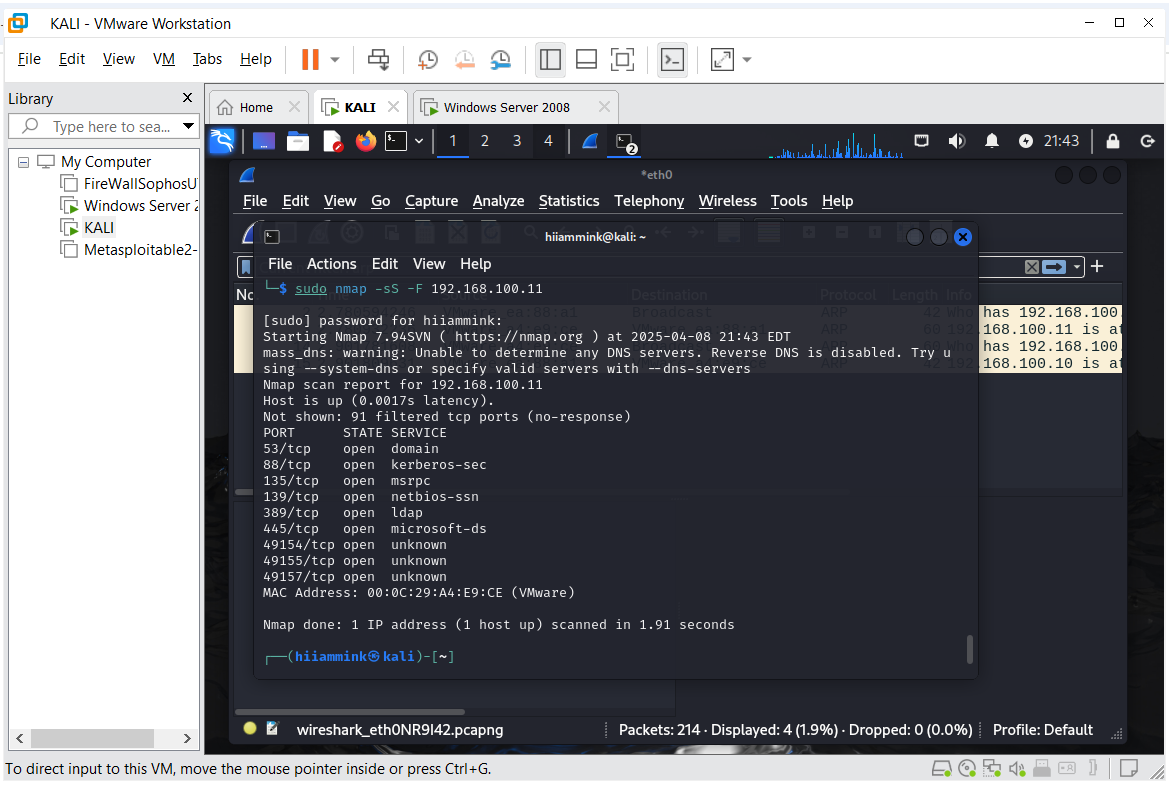


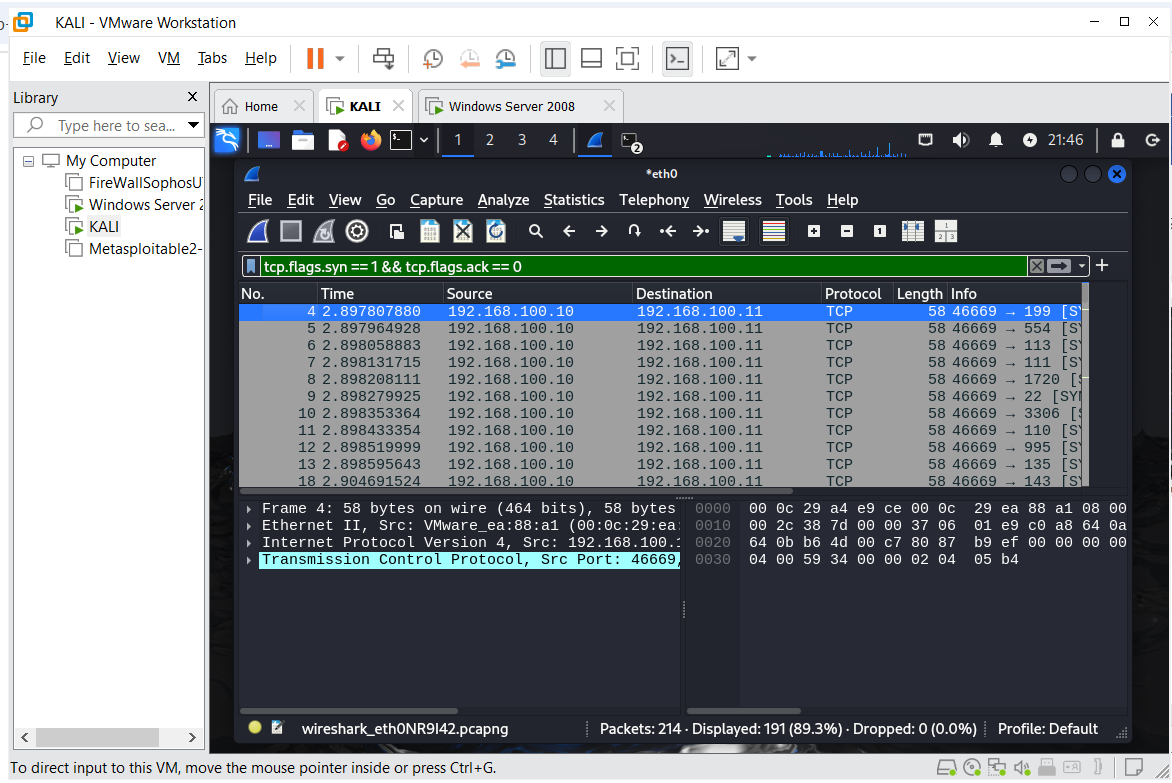


Kỹ thuật quét là: Host Discovery và sử dụng ARP request

Mục tiêu: phát hiện các host đang hoạt động

Kịch bản 2: nmap –sS –F 192.168.100.11





Kỹ thuật:

Mục tiêu: Phát hiện cổng đang mở mà **không thiết lập kết nối hoàn chỉnh**

Kịch bản 3