

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**--🙣🕮🙡--**

**BÁO CÁO**

**MÔN KIỂM THỬ XÂM NHẬP**

**LAB 1**

**Tìm hiểu, nhận diện và khai thác lỗ hổng MS17-010**

**Giảng Viên: *Huỳnh Thanh Tâm***

**Sinh Viên thực hiện:**

***Chế Công Hậu N17DCAT023 – D17CQAT01-N***

**TPHCM – Ngày 16/4/2021**

1. **Tìm hiểu lỗ hổng MS17-010 trên hệ điều hành Windows**

Lỗ hổng này xuất hiện trên dịch vụ chia sẻ file SMB, được công khai bởi ShadowsBrowkers, nó cho phép kẻ tấn công có thể khai thác và chạy các mã lệnh thực thi từ xa trên máy tính nạn nhân. Lỗ hổng này được đánh giá là cực kỳ nghiêm trọng do SMB là dịch vụ chia sẻ file được khởi chạy cùng hệ thống trên nhiều phiên bản của hệ điều hành Windows.

**Phiên bản bị ảnh hưởng**:  
– Người dùng cá nhân: Windows XP, 7, 8, 8.1, 10  
– Máy chủ: Windows Server 2003, 2008, 2012, 2016

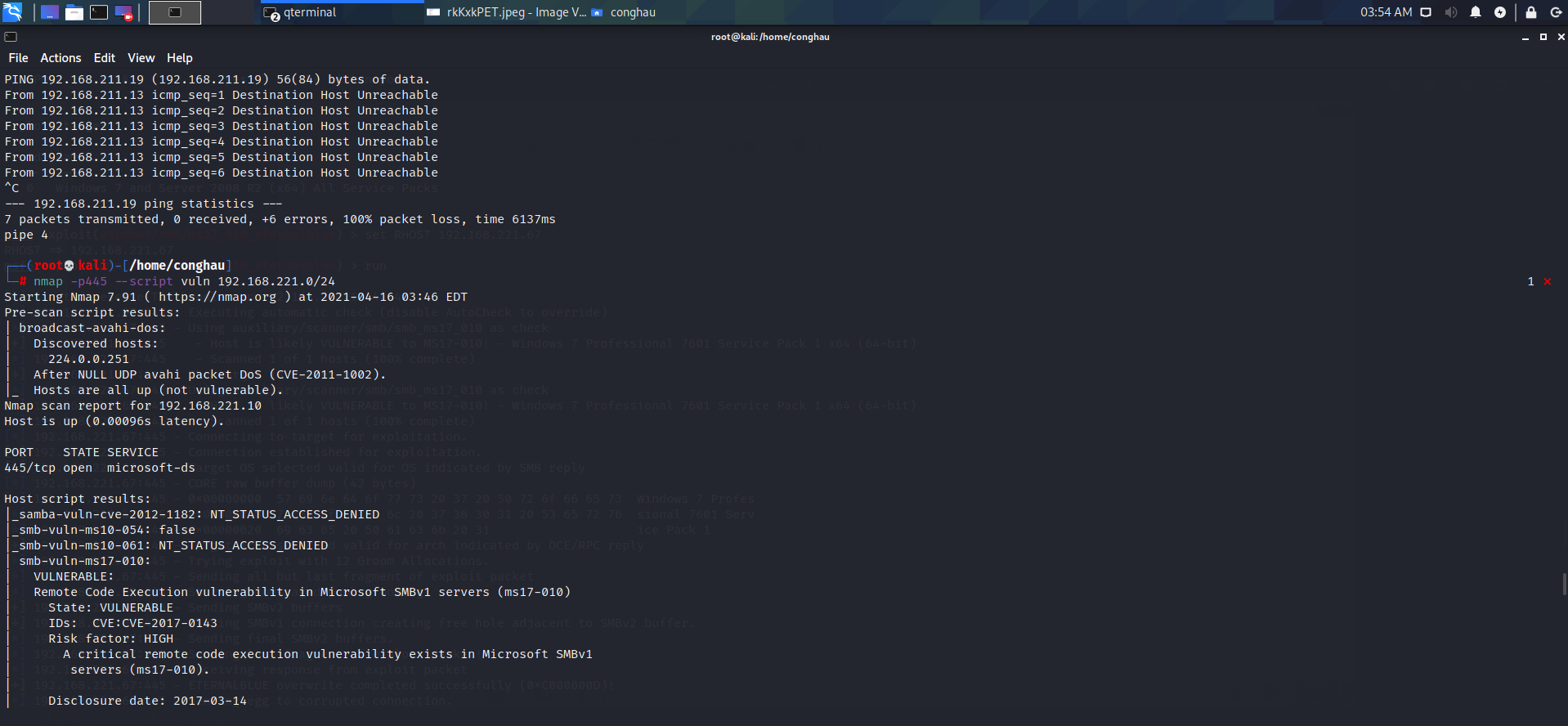
**Chú ý**: Lỗ hổng MS17-010 chỉ có thể được **khai thác trực tiếp từ Internet đối với mục tiêu là các máy chủ chạy Windows Server**, còn đối với các máy tính cá nhân thì MS17-010 **chỉ có thể thực hiện được trong mạng nội bộ.**

**Cách thức lây nhiễm của WannaCry**

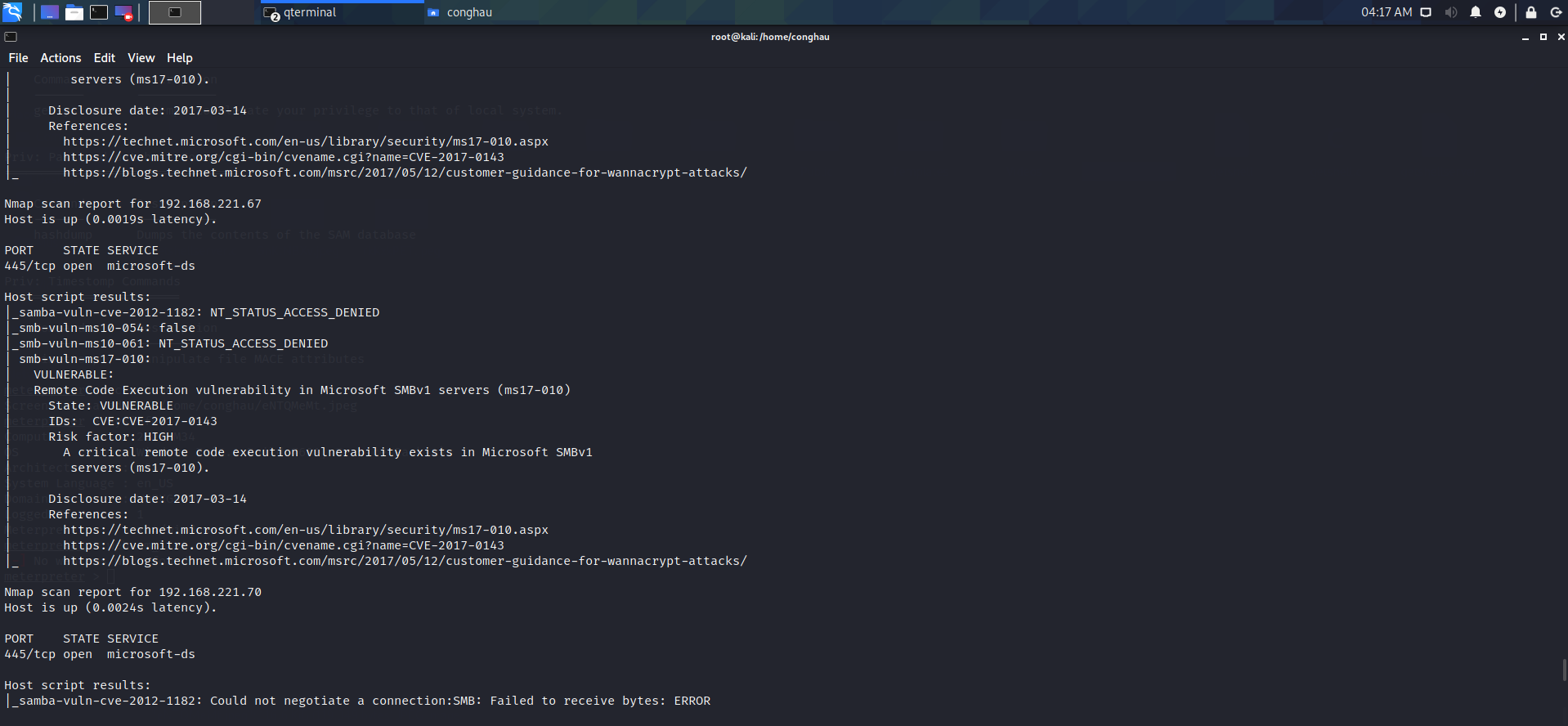
WannaCry lây nhiễm vào các máy chủ chạy hệ điều hành Windows Server sử dụng trực tiếp lỗi MS17-010 hoặc các lỗi khác nếu hệ thống chưa được cập nhật đầy đủ các bản vá.- Đối với các máy tính cá nhân, WannaCry không thể trực tiếp lây nhiễm sử dụng lỗi MS17-010 từ Internet, thông thường WannaCry sẽ lây nhiễm qua các con đường: Phishing hoặc HTA, Phishing kết hợp mã khai thác các tệp tin PDF, DOC, DOCX,…. Sau khi thành công cài đặt vào máy tính người dùng, WannaCry sẽ tiếp tục lây nhiễm các máy tính trong mạng nội bộ qua lỗi MS17-010.

1. **Cách nhận diện lỗ hổng MS17-010**

Nhập lệnh : **nmap -p445 --script vuln <IP Target>** (ở đây là đang scan dãy mạng 192.168.221.0/24).

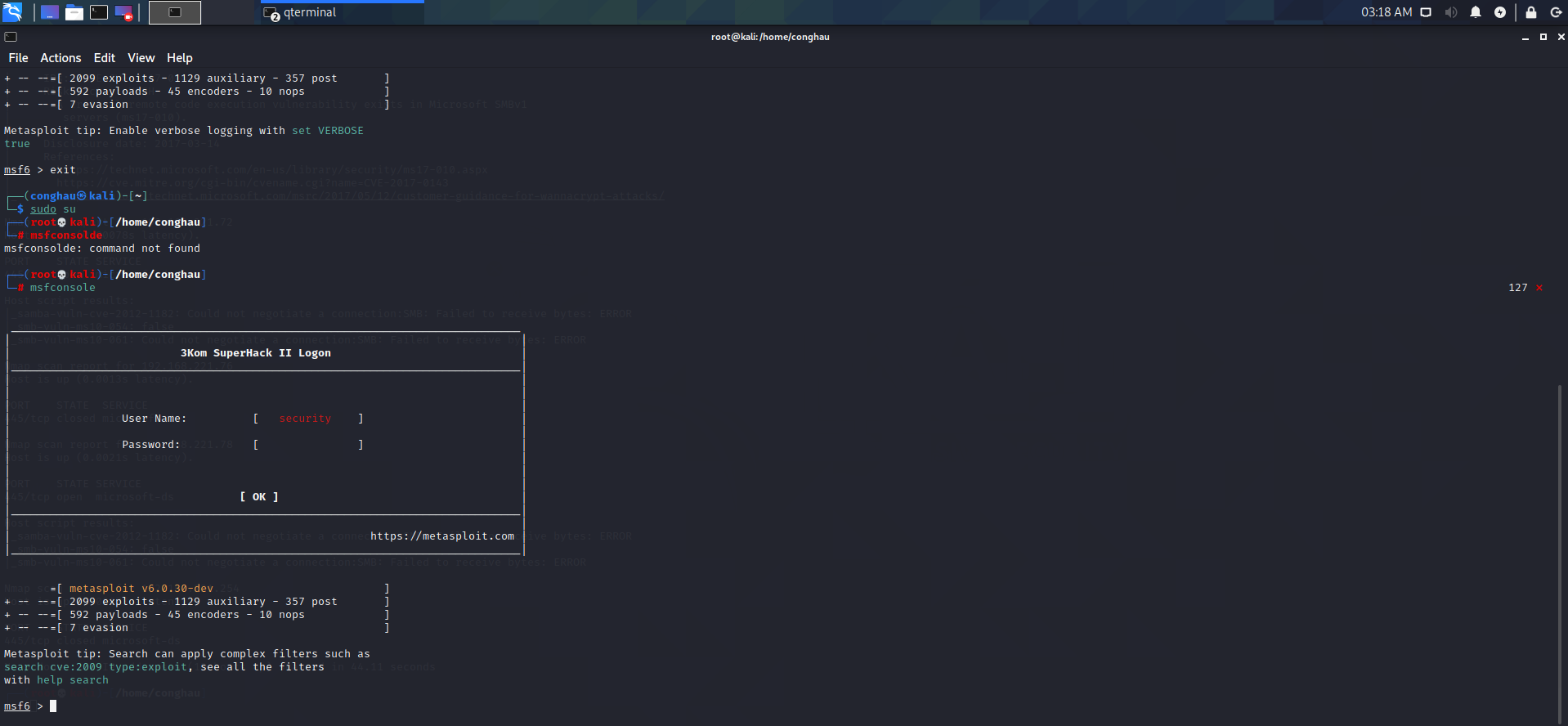


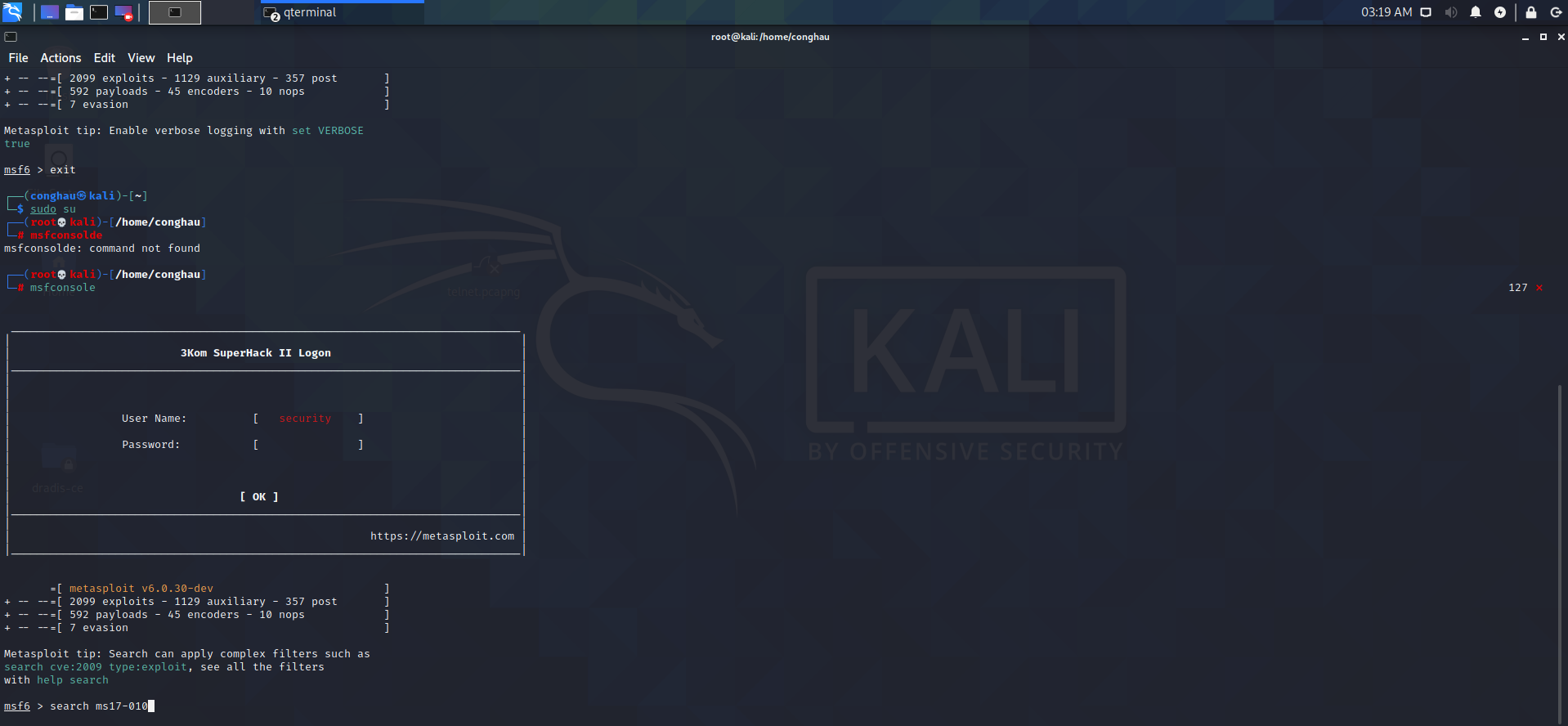
Đã phát hiện lỗ hổng MS17-010 ở máy IP **192.168.221.67**

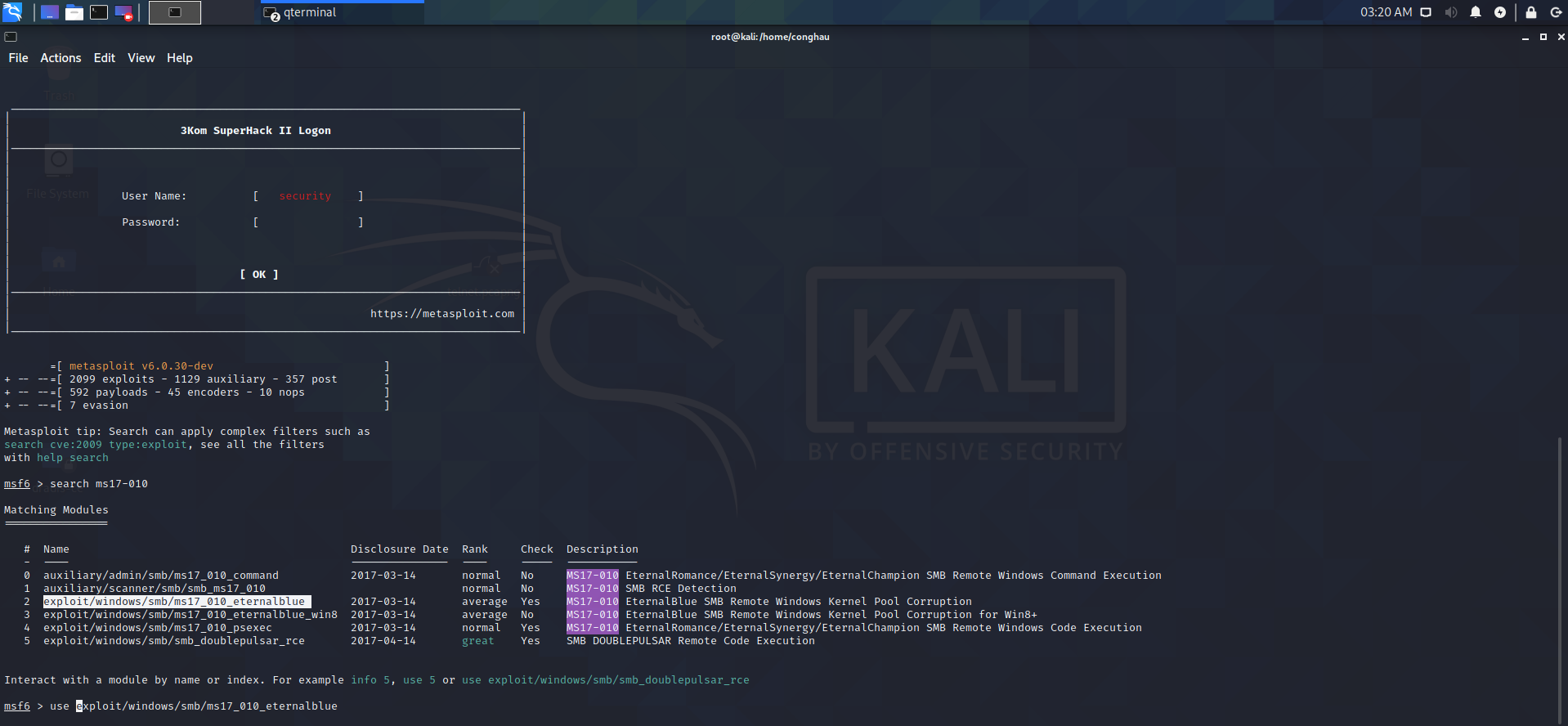


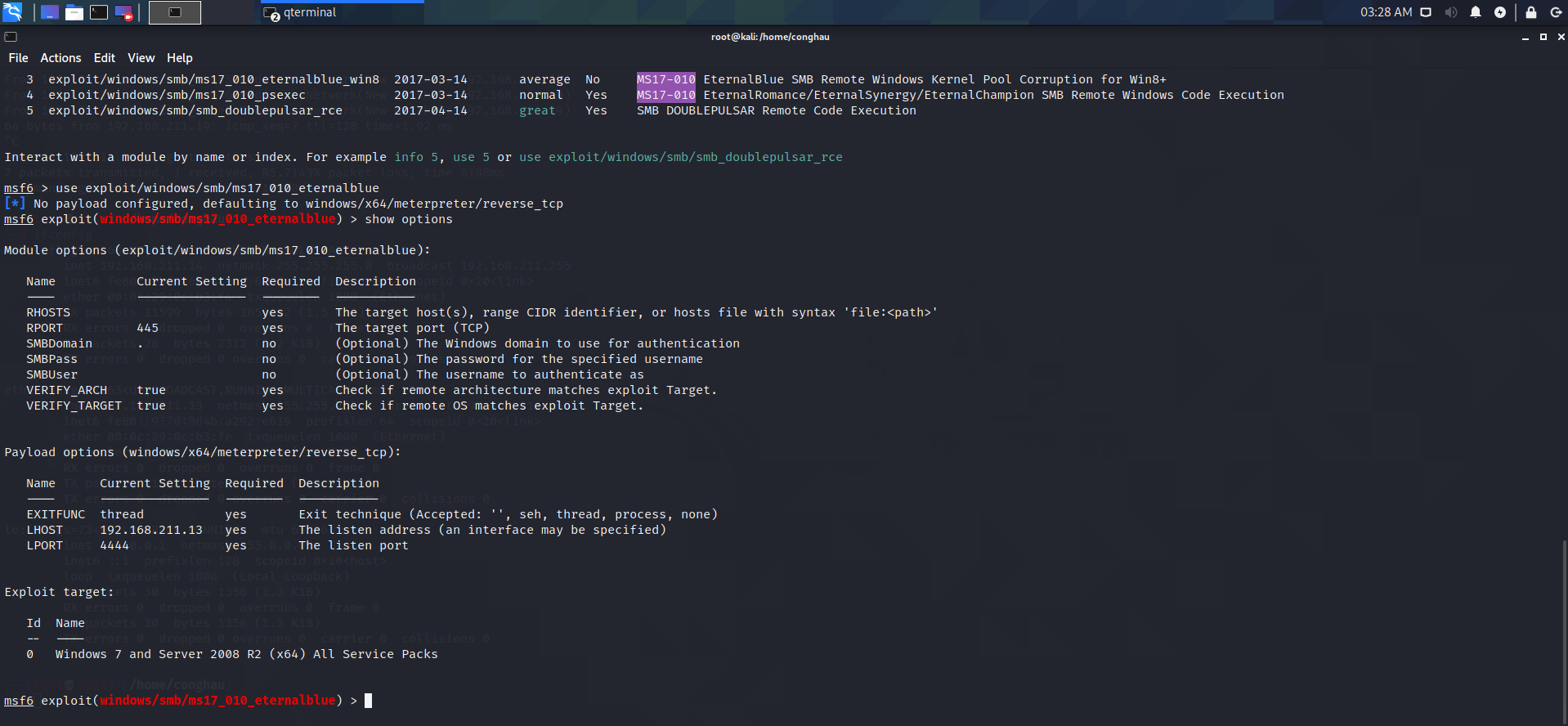
1. **Cách khai thác MS17-010**

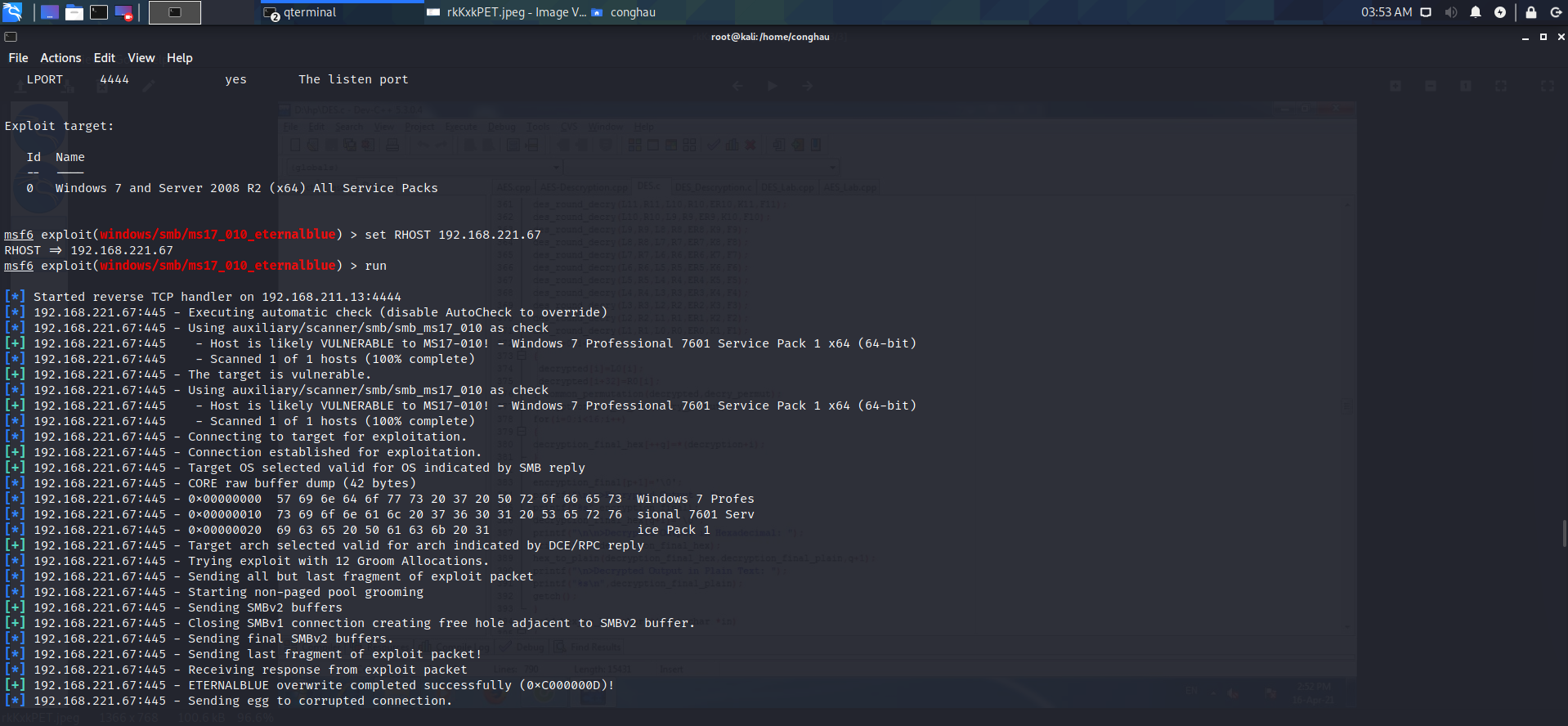
Sử dụng **Metasploit**

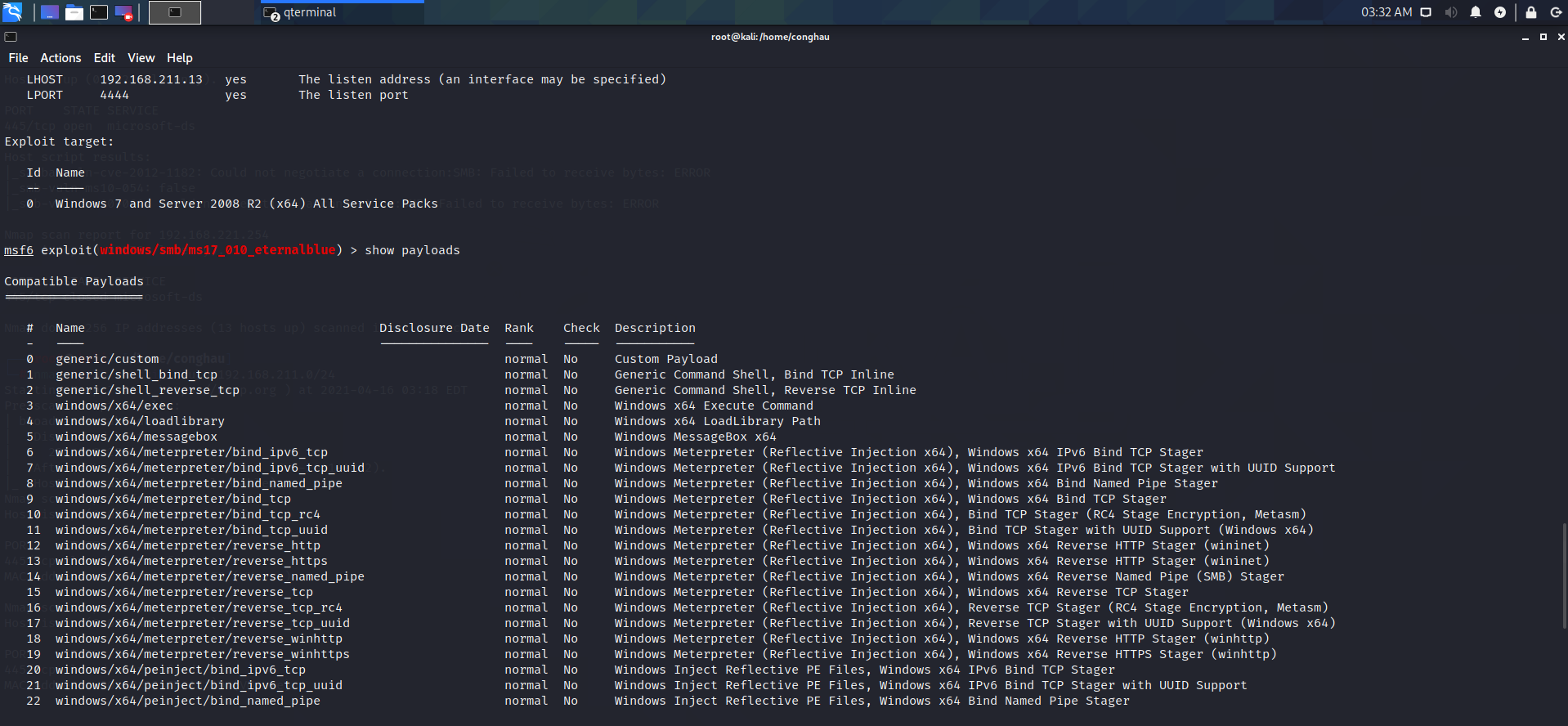


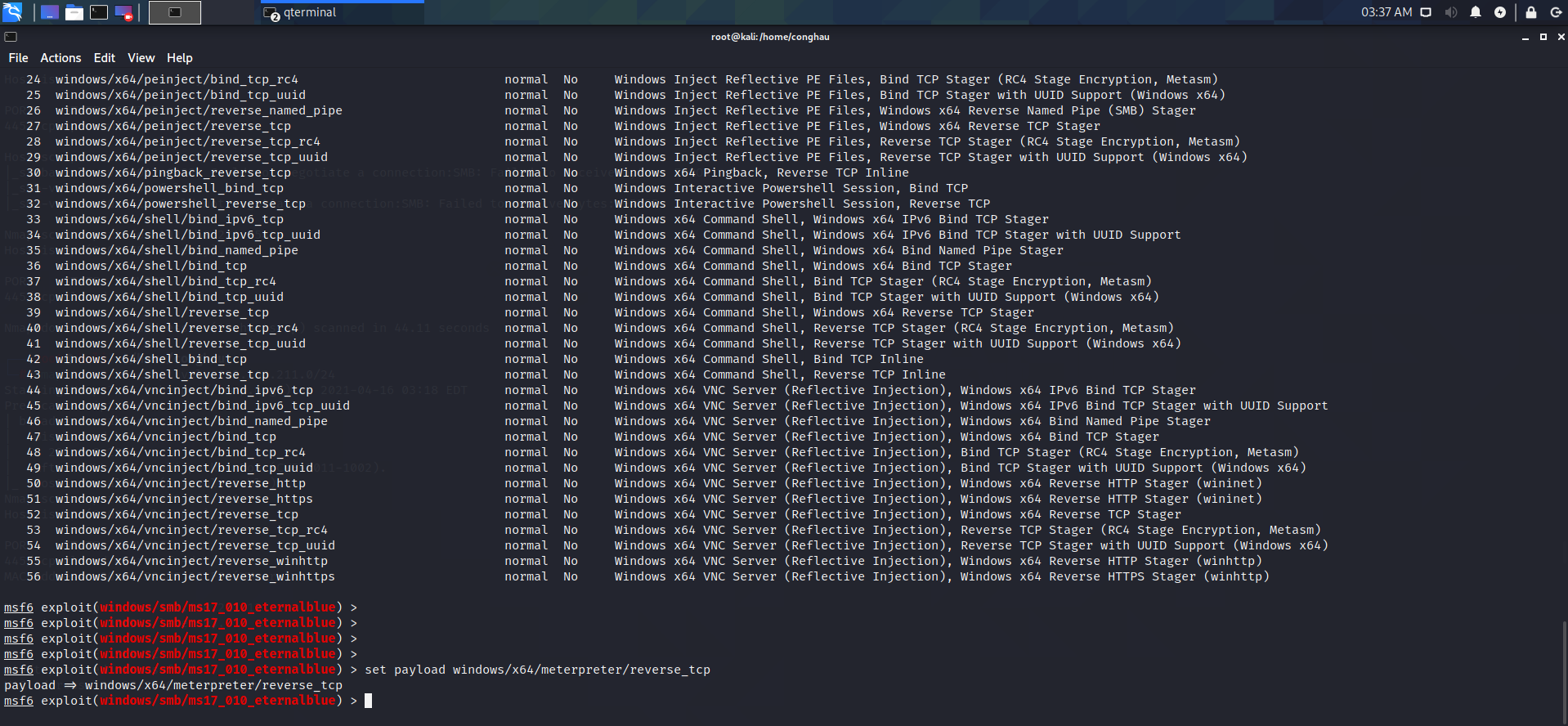


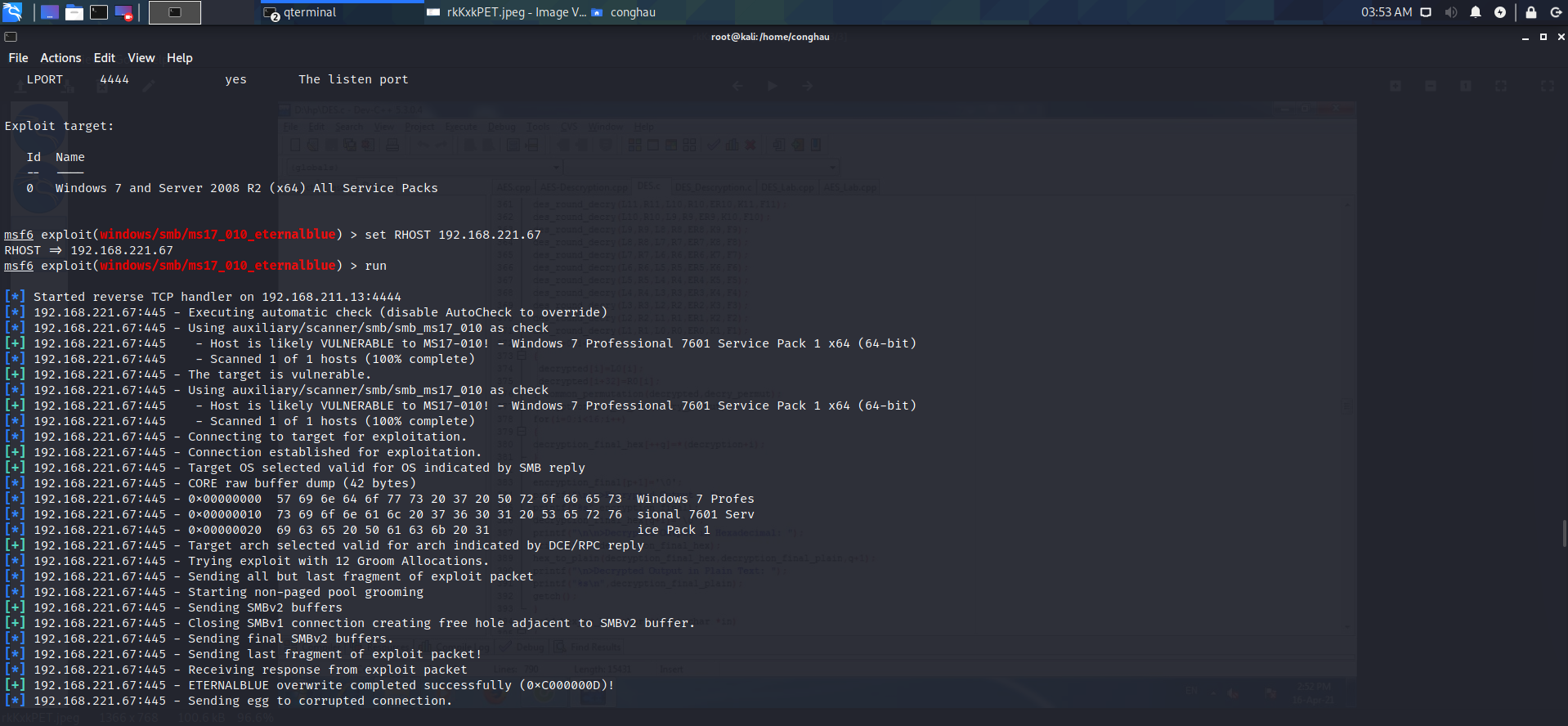


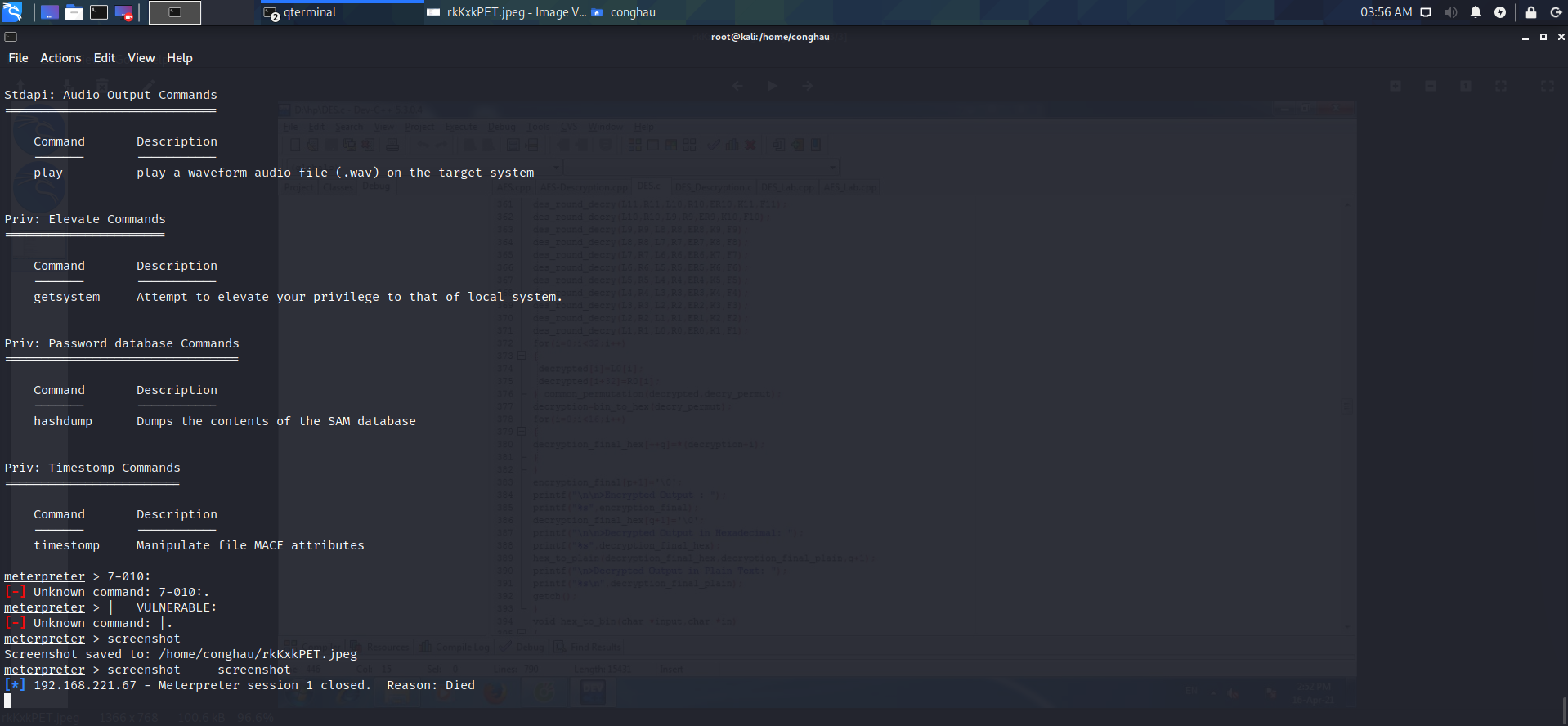


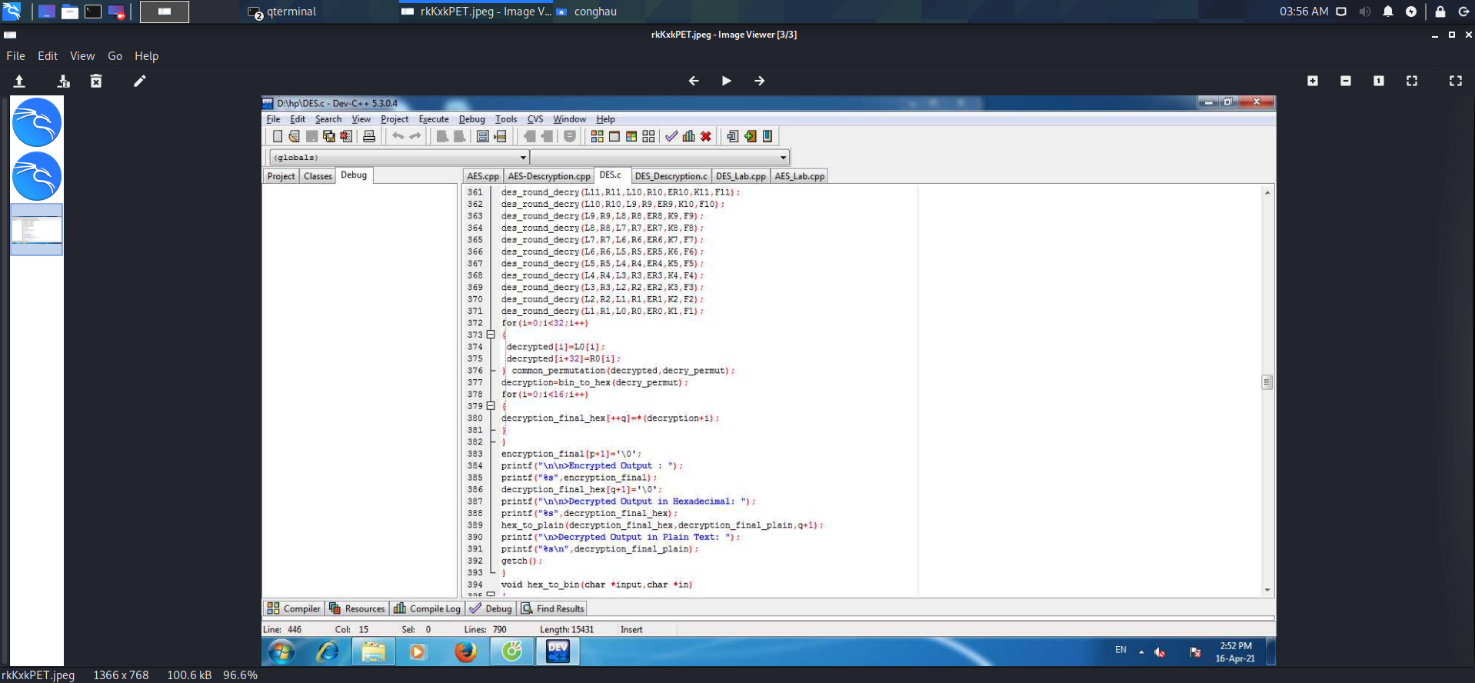


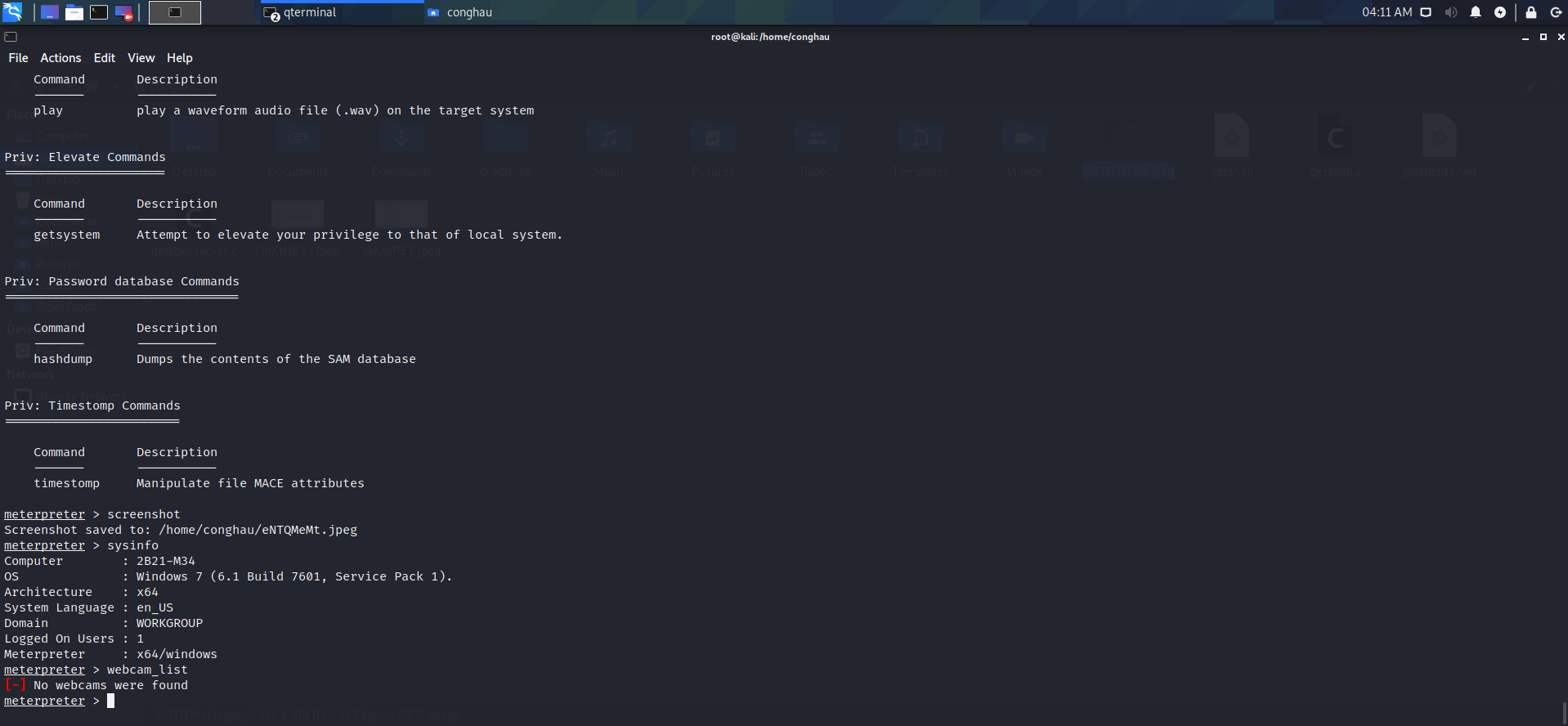












* Đã thực hiện tấn công thành công