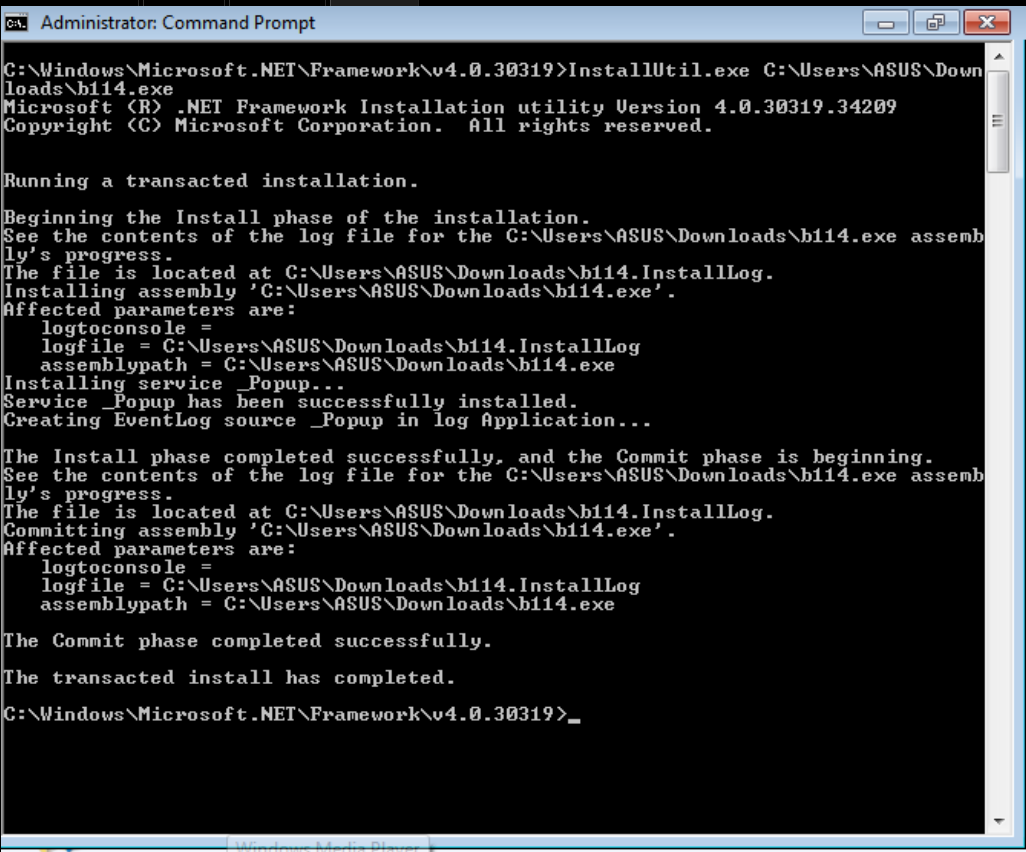
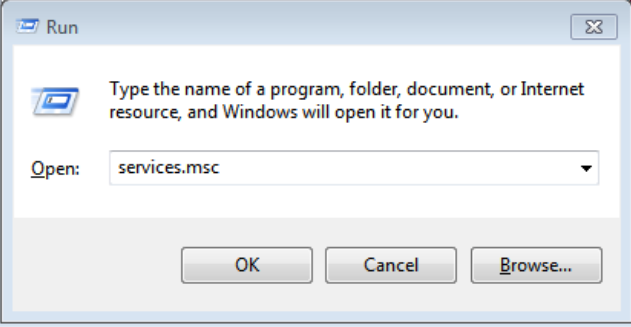
1. Viết một ứng virus đơn giản bằng dịch vụ trên C#, hiện pop-up MSSV trên máy nan nhân mỗi khi user thực hiện đăng nhập thành công.

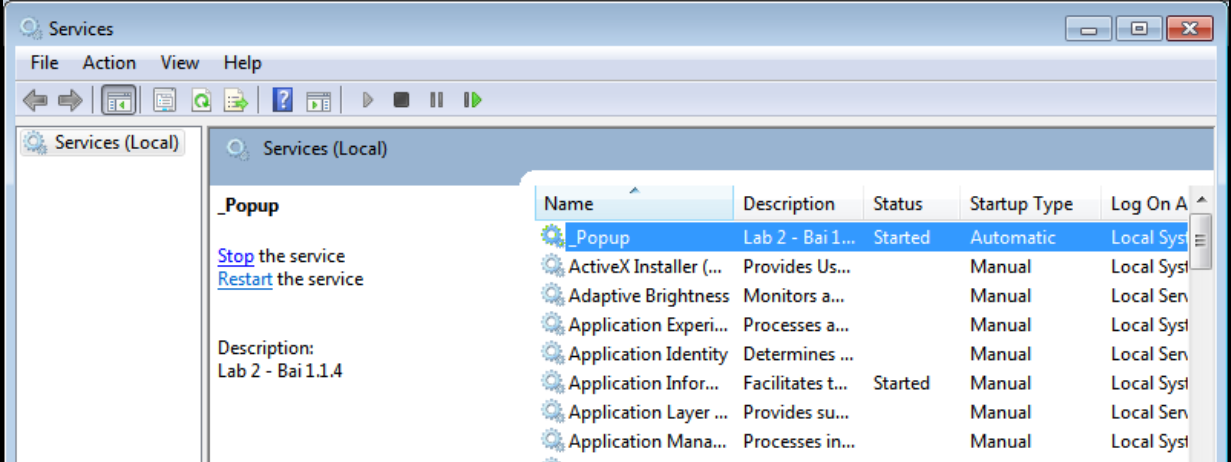
Thực hiện cài đặt service



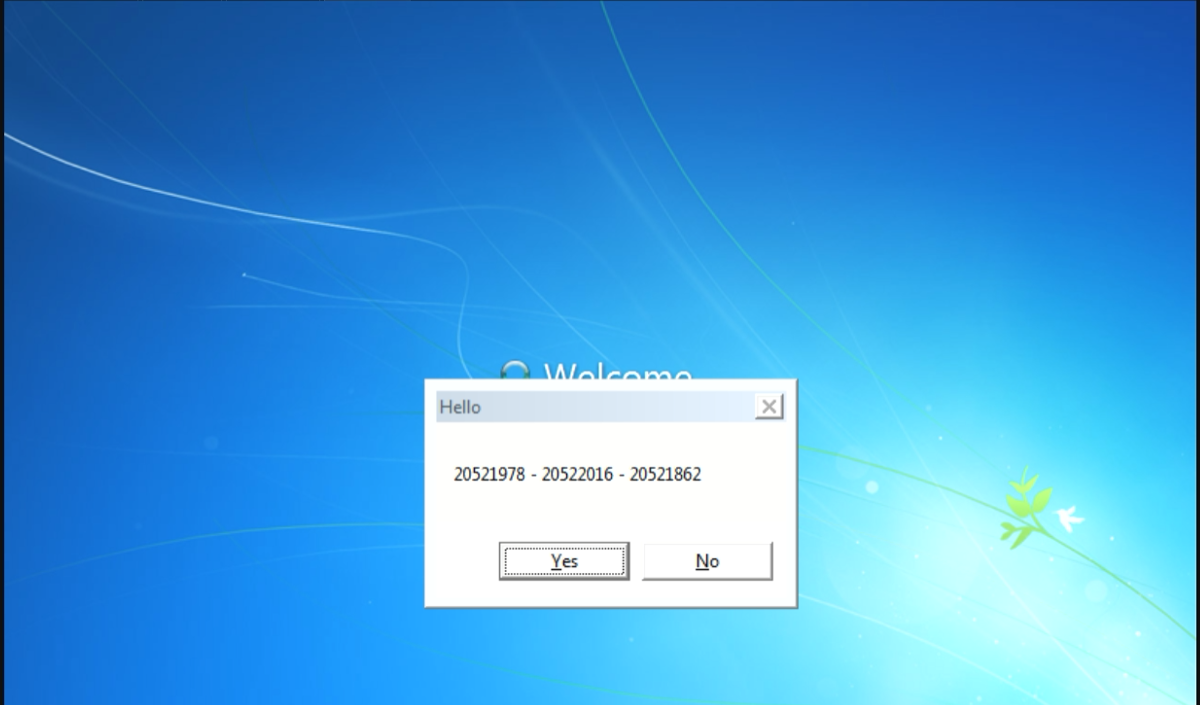
Ấn Windows+R và nhập service.msc để bật services manager



Start sevice vừa cài.



Thử sign out và sign in để kiểm tra. Kết quả là xuất hiện popup với nội dung mong muốn

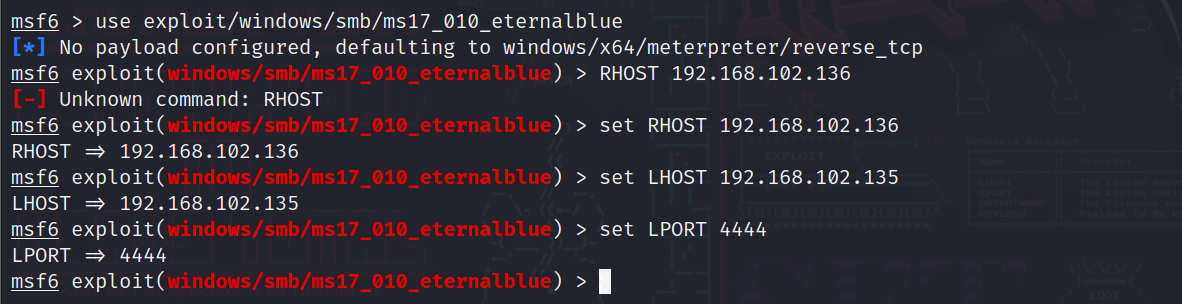


5. So sánh giữa việc viết virus bằng dịch vụ trên C# so với việc tao bằng MSF (quyền, khả  
năng phát hiện, …)

**B.2 Sâu máy tính**

**B.2.1 Khai thác lỗ hổng MS17-010 sử dụng Metasploit**

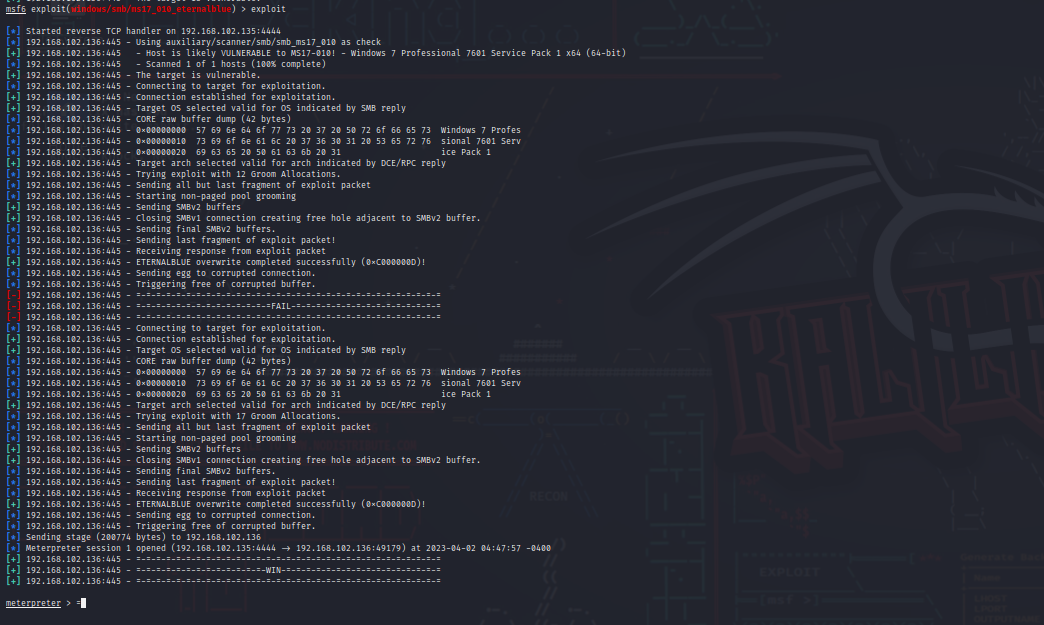
Khởi chạy mã khai thác lỗ hổng MS17-010



Dùng lệnh check để đảm bảo máy nạn nhân có lỗ hổng



Dùng lệnh exploit để khai thác lỗ hỗng tìm được

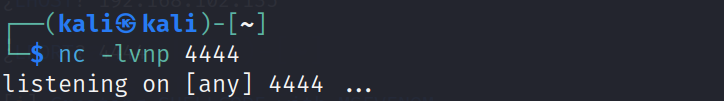


Sau khi có được parameter shell, dùng lệnh shell để mở một cmd trên máy victim

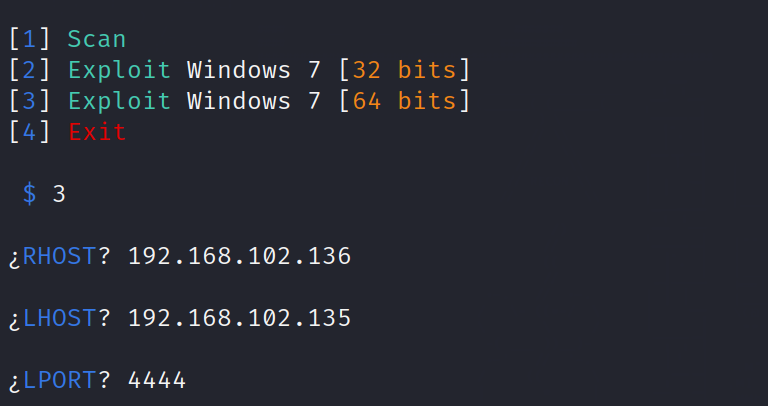


**B.2.2 Khai thác lỗ hổng MS17-010 không sử dụng Metasploit**

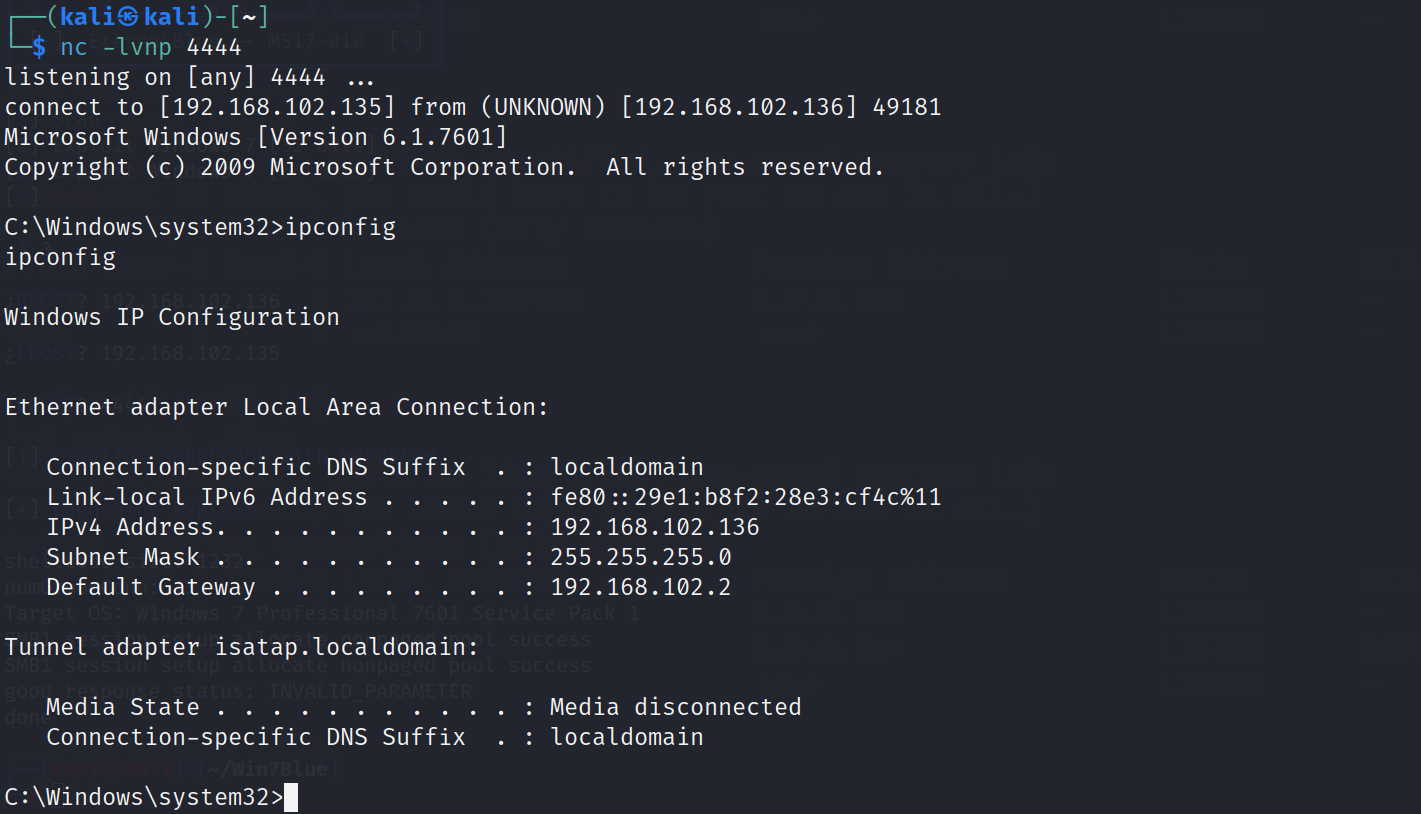
Thực hiện lắng nghe trên port 4444 trước khi thực hiện exploit



Thực hiện exploit với tool vừa tải về



Sau khi thực hiện explot, nhận được connect back tại terminal thực hiện lắng nghe trên port 4444.

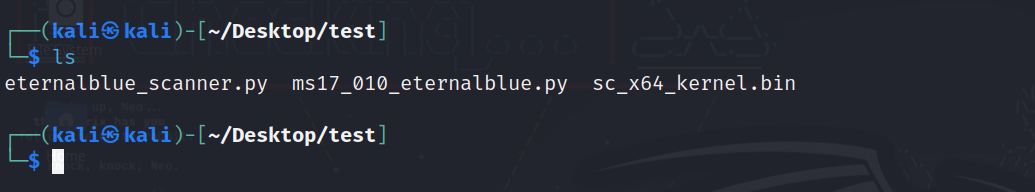


**B.2.2.1 Bài tập về nhà (YÊU CẦU LÀM)**

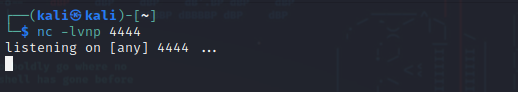
**1. Thực hiện lai nhưng không được sử dụng script .sh. Giải thích chi tiết từng bước mà script**

**đã làm (KHÔNG CẦN GIẢI THÍCH MÃ KHAI THÁC LỖ HỔNG)**

Thực hiện copy eternalblue\_scanner.py, ms17\_010\_eternalblue.py và sc\_x64\_kernel.bintừ Win7Blue sang 1 thư mục khác



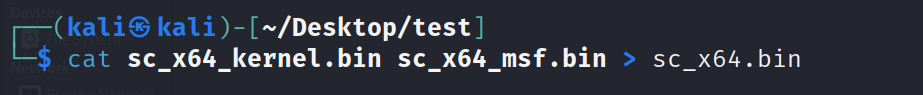
Bắt đầu lắng nghe trên port 4444



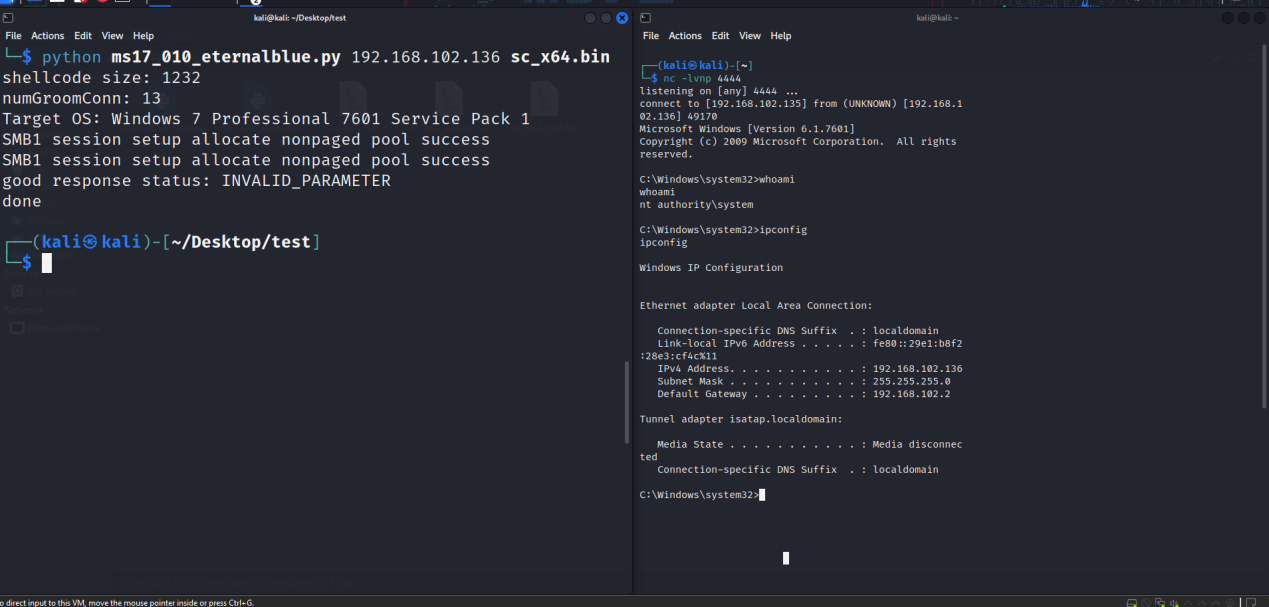
Sử dụng msfvenom để tạo payload thực hiện reverse shell



Gộp payload và sc\_x64\_kernel.bin thành 1



Thực thi ms17\_010\_eternalblue.py với payload là file vừa gộp, ta có một reverse shell trả về từ victim trên terminal thực hiện netcat



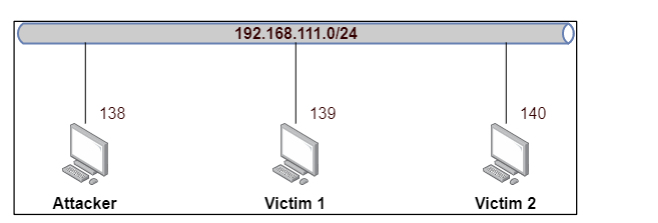
Script hoạt động như sau:

Đầu tiên sẽ thực hiện quét máy victim có lỗ hổng hay không bằng eternalblue\_scanner.py.

Tiếp theo scrip sẽ dùng msfvenom để tạo một payload tạo reverse shell(như đã làm ở trên) và gộp nó với sc\_x64\_kernel.bin để tạo thành payload hoàn chỉnh

Cuối cùng, sẽ thực hiện attack bằng cách thực thi ms17\_010\_eternalblue.py cùng payload hoàn chỉnh để có được reverse shell trên terminal đang thực hiện netcat.

1. **Thực hiện các yêu cầu với mô hình sau**

****a. Trên máy Attacker, mở 2 cổng lắng nghe là 4444 và 4445  
b. Trên máy Attacker, thực hiện khai thác lỗ hổng MS17-010 trên máy Victim 1 và thực hiện connect back về máy Attacker trên port 4444  
c. Sau khi có được connect back từ máy Victim 1, trong session shell đó, thực hiện tải về exploit từ máy Attacker và khai thác lỗ hổng MS17-010 trên máy Victim 2, để máy  
Victim 2 thực hiện connect back về máy Attacker trên port 4443

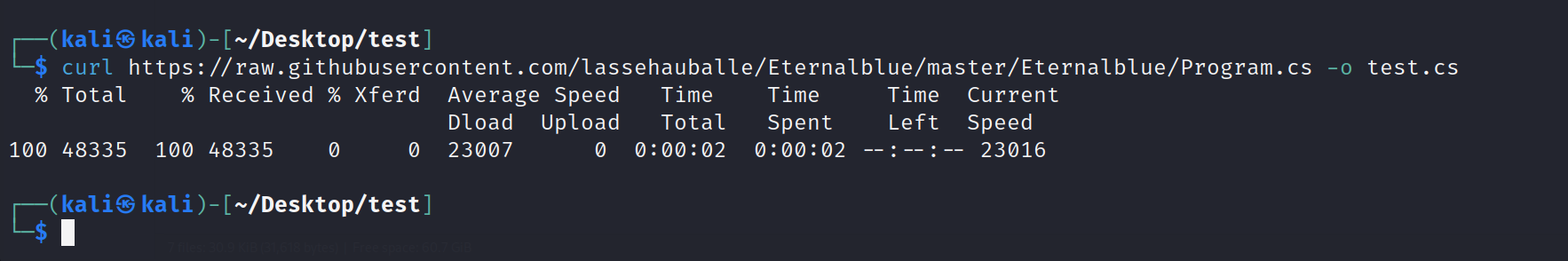
134

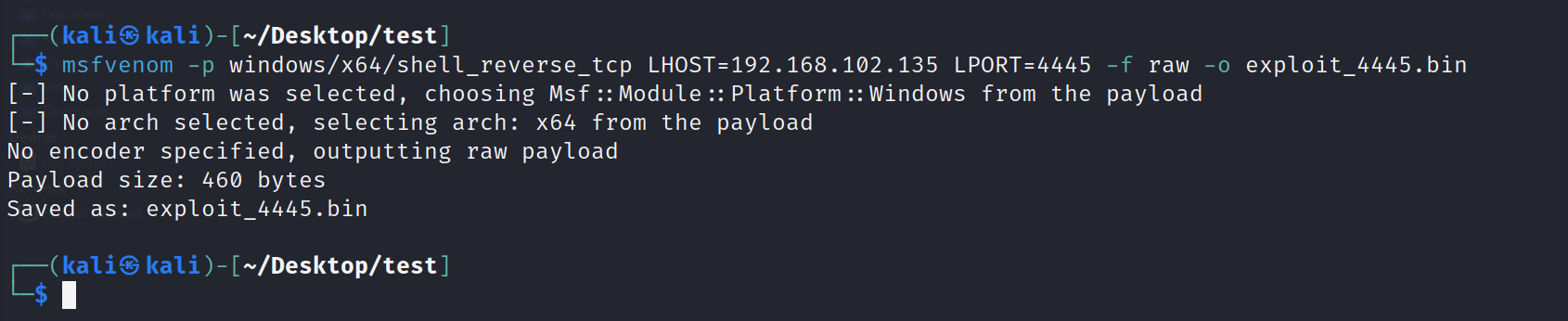
136

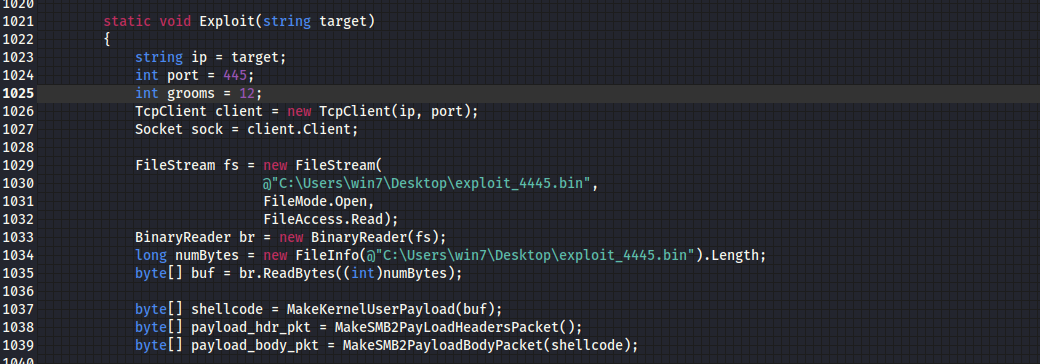
135

192.168.102.x

Tải source của EternalBlue về máy tấn công

  
Dùng msfvenom để tạo payload thực hiện reverse shell từ máy victim 2 về máy attacker trên port 4445

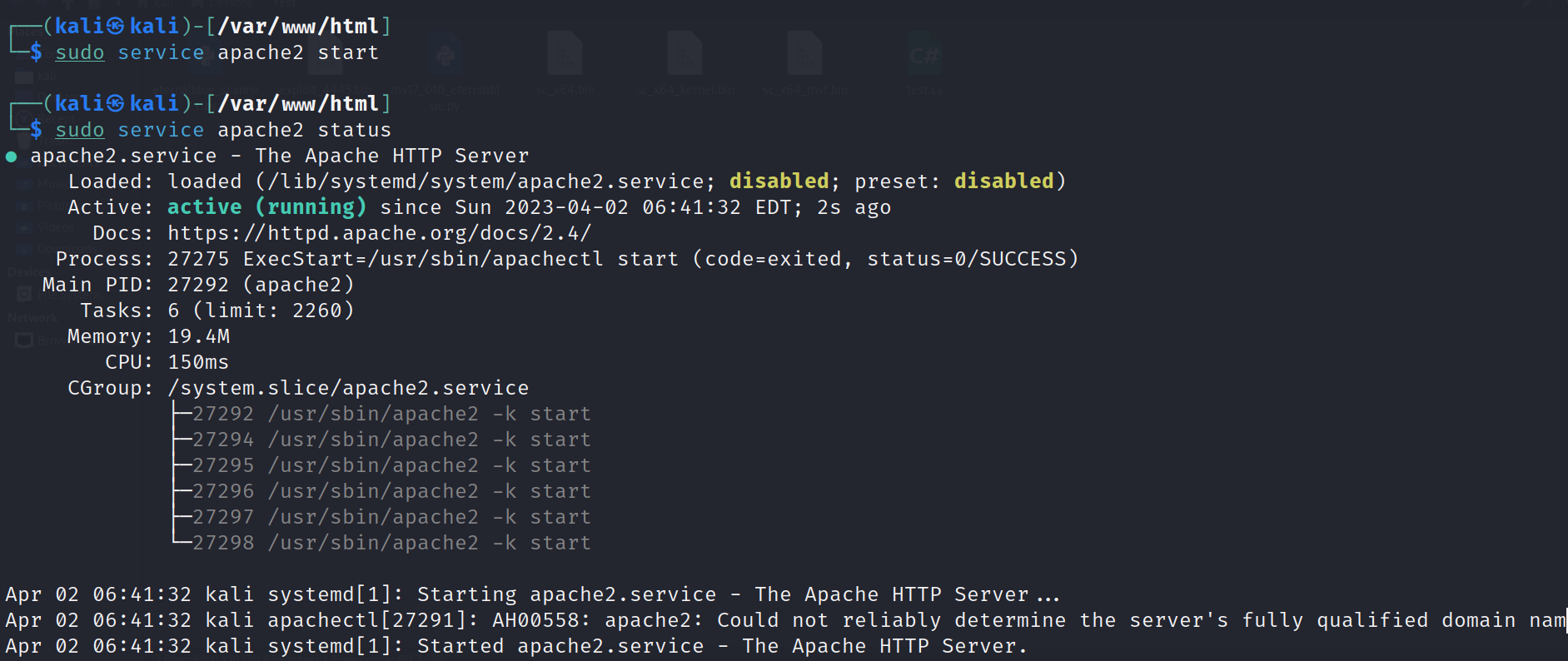
Chỉnh sửa source code EternalBlue cho phù hợp



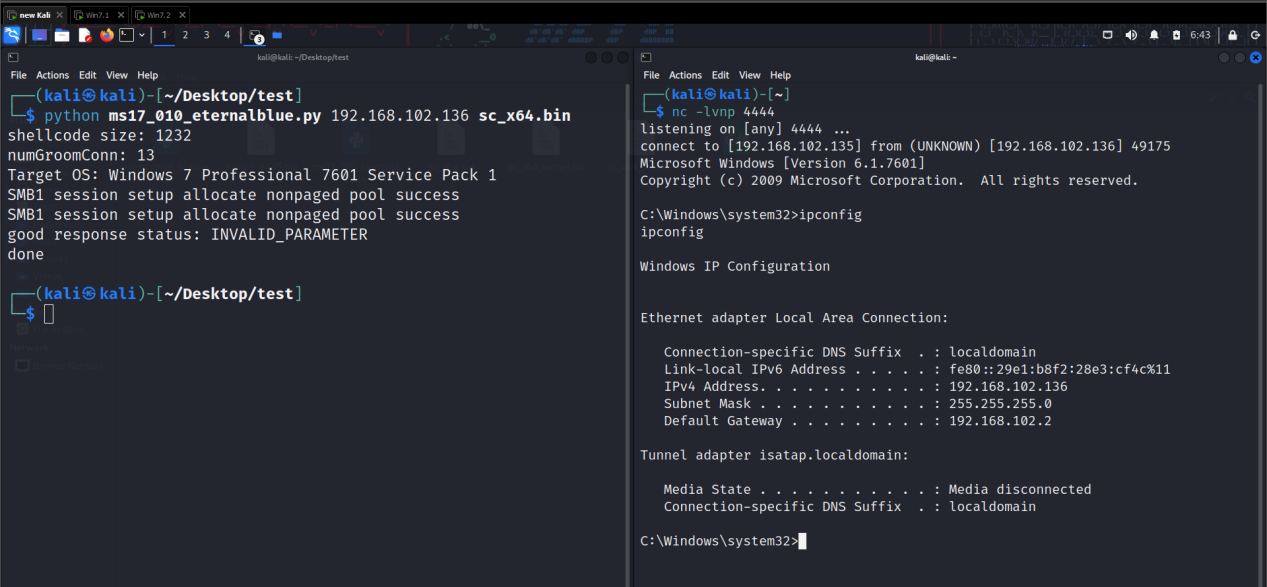
Đẩy source code EternalBlue và payload lên apache2



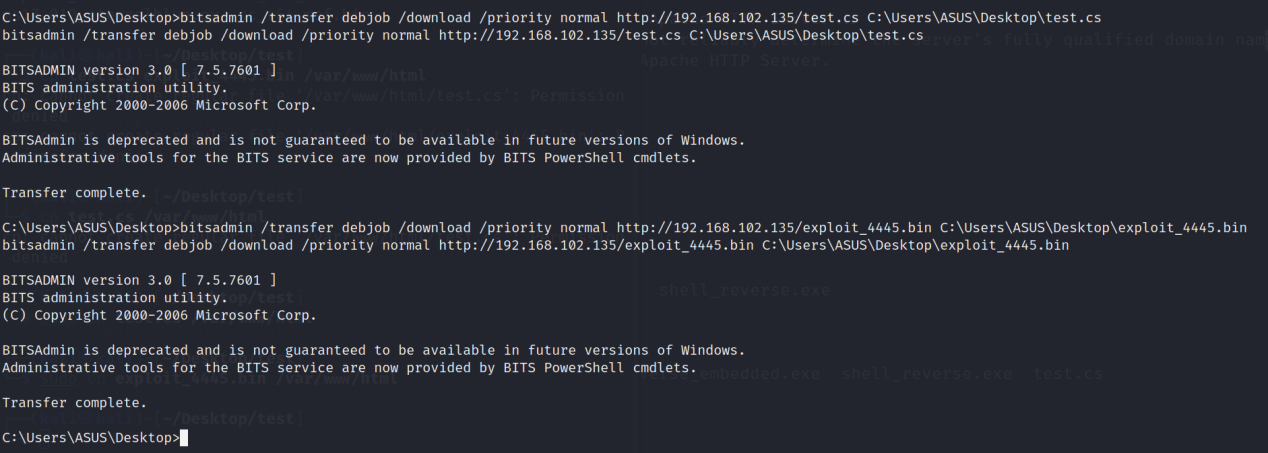
Khởi động apache2

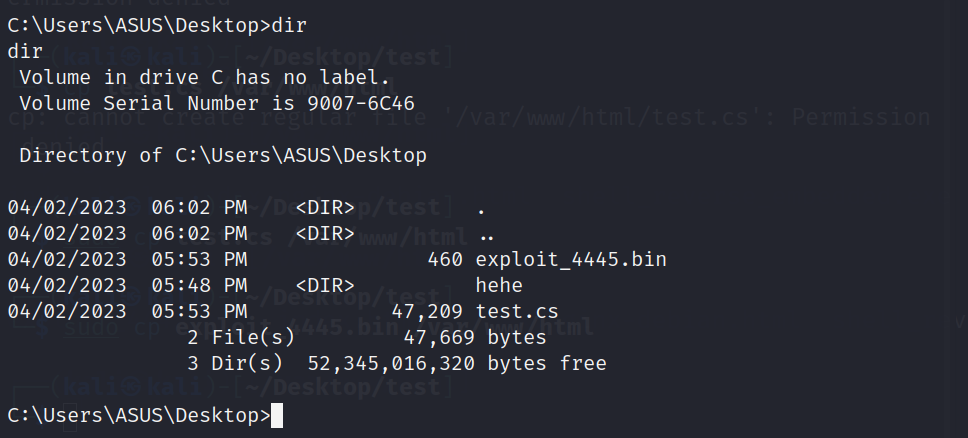


Thực hiện tấn công victim 1 như bài 1



Trên reverse shell vừa mở ta tải về EternalBlue và payload đã tạo ban đầu

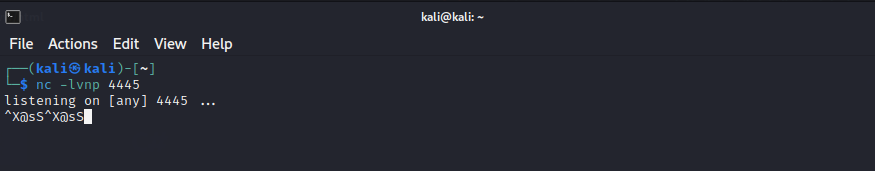




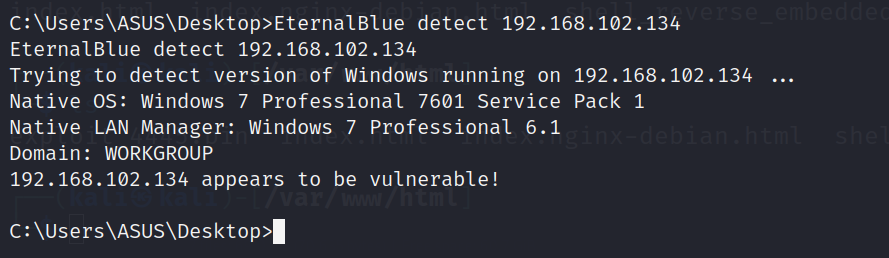
Compile code EternalBlue thành file exe



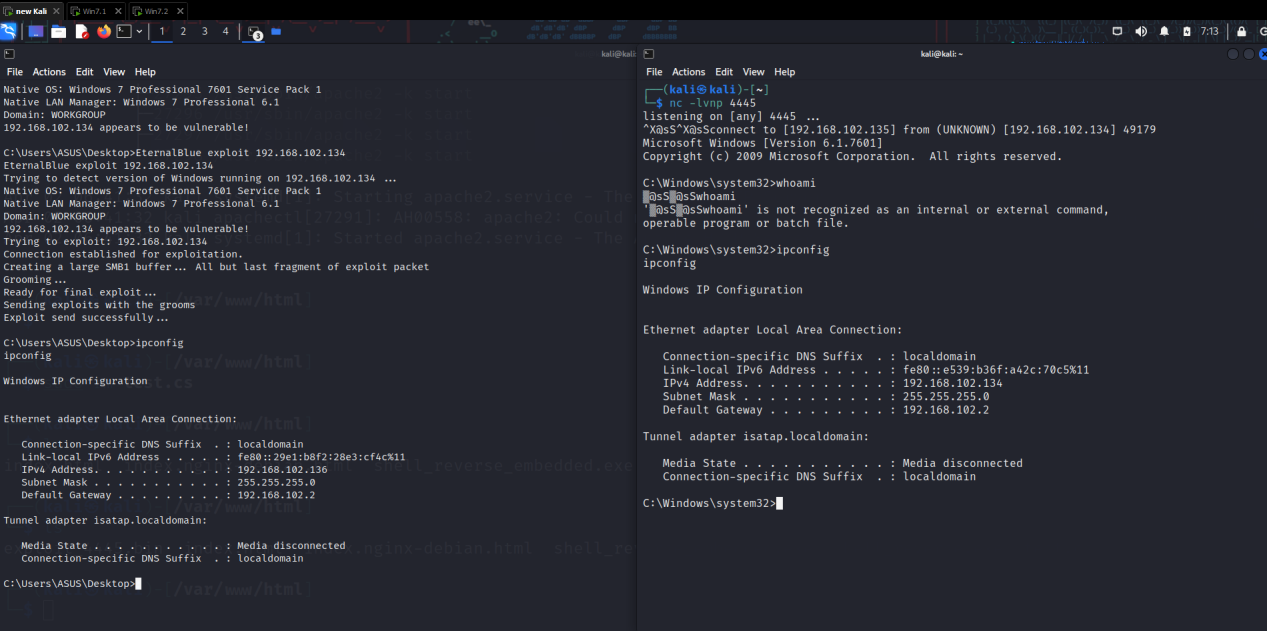
Attacker bắt đầu lắng nghe trên port 4445



Bây giờ dùng victim 1 để exploit victim 2. Check xem victim 2 có lỗ hổng không



Tấn công victim 2 bằng lệnh exploit



Kết quả thành công khi có được reverse shell từ victim 2 trả về máy attacker trên terminal đang lắng nghe trên port 4445