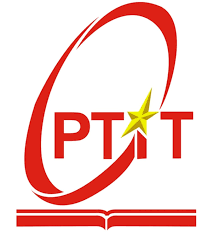
**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

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



**BÁO CÁO TIẾN ĐỘ**

**GV :** TS. NGUYỄN HỒNG SƠN

**Sinh viên thực hiện :** Ngô Nhựt Minh

**Mã số sinh viên :** N19DCAT050

**Lớp :** D19CQAT01-N

**Khóa :** 2019 - 2024

**Hệ :** ĐẠI HỌC CHÍNH QUY

**TP. HCM, Tháng 10 / 2023**

# 1. Lỗ hổng CVE-2017-7494

*1.1 Giới thiệu*

Samba là phần mềm mã nguồn mở chạy trên phần lớn các hệ điều hành: Windows, Linux, UNIX, IBM System 390 và OpenVMS. Samba cho phép chia sẻ các thư mục, chia sẻ mạng và máy in.

Lỗ hổng SambaCry là lỗ hổng thực thi mã lệnh từ xa CVE-2017-7494 ảnh hưởng đến tất cả các phiên bản sau Samba 3.5.0 được phát hành vào ngày 1/3/2010. Lỗ hổng được đặt tên là SambaCry do sự tương đồng của nó với WannaCry: cả hai đều nhằm đến giao thức SMB và có khả năng lây lan từ hệ thống này sang hệ khác qua giao thức SMB.

Theo công cụ tìm kiếm máy tính Shodan, gần 485.000 máy tính sử dụng phần mềm Samba có nguy cơ bị tấn công trên mạng Internet. Các nhà nghiên cứu dự đoán rằng các cuộc tấn công dựa trên lỗ hổng SambaCry cũng có tiềm năng lây lan giống như mã độc WannaCry.

Dự đoán này khá chính xác, vì hệ thống tài nguyên thông tin được xây dựng với mục đích giả dạng (honeypots) do nhóm các nhà nghiên cứu của Kaspersky Lab thiết lập đã phát hiện một chiến dịch mã độc đang khai thác lỗ hổng của SambaCry để lây nhiễm các máy tính Linux bằng phần mềm khai thác cryptocurrency.

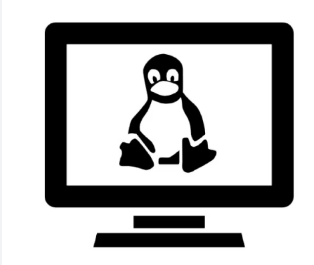
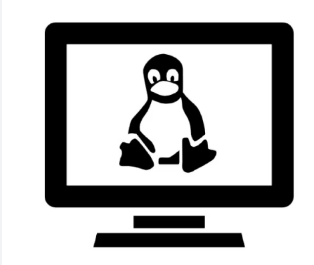
Theo các nhà nghiên cứu, một nhóm tin tặc đã bắt đầu tấn công các máy tính Linux khi lỗ hổng trong phần Samba được tiết lộ công khai và cài đặt một phiên bản nâng cấp của CPUminer, phần mềm khai thác mật mã cryptocurency và Monero.

*1.2* ***Cách thức tấn công lỗ hổng SambaCry***

Tin tặc thực hiện hai payload trên các hệ thống mục tiêu: INAebsGB.so - một đoạn mã đảo ngược (reverse-shell) cung cấp truy cập từ xa cho kẻ tấn công và CblRWuoCc.so - một backdoor bao gồm các tiện ích khai thác giao thức mật mã CPUminer. Các nhà nghiên cứu của Kaspersky Lab cho biết, thông qua đoạn mã đảo ngược trong hệ thống, tin tặc có thể thay đổi cấu hình hoặc lây nhiễm các loại phần mềm độc hại khác vào máy tính người dùng.

**2. Quá trình thu thập dữ liệu tấn công**

*2.1 Mô hình triển khai*

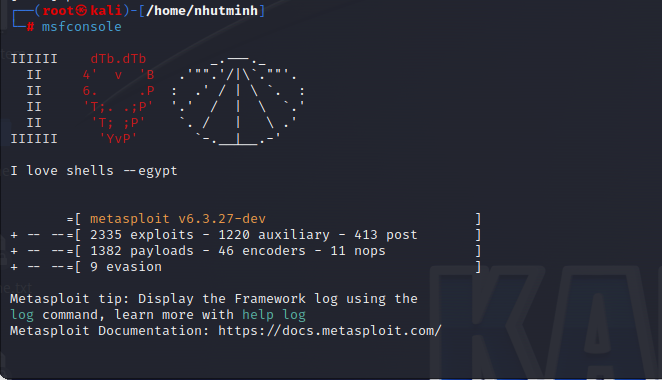
Sử dụng Vmware

Máy Attacker Kali\_2023 Máy Victim Kali\_2016

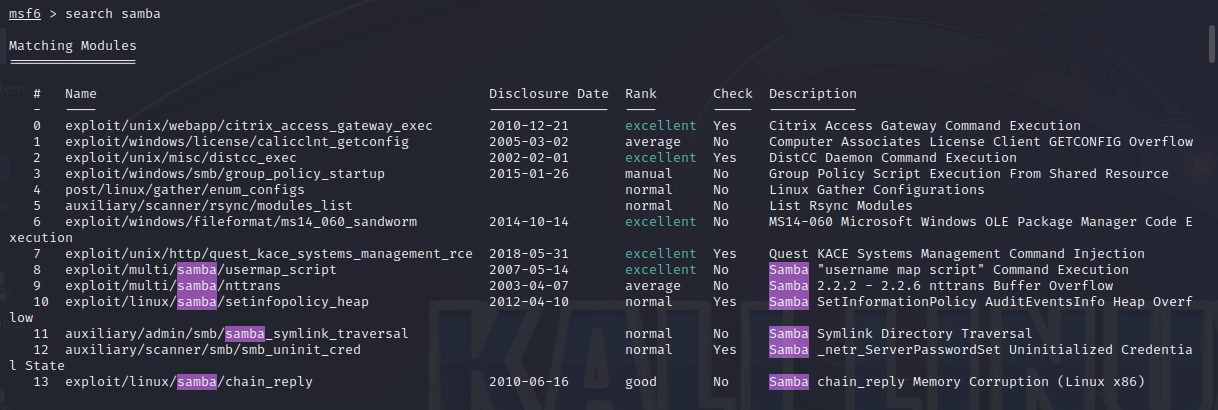
IP:172.16.1.134 IP: 172.16.1.135

*2.2 Các bước triển khai*

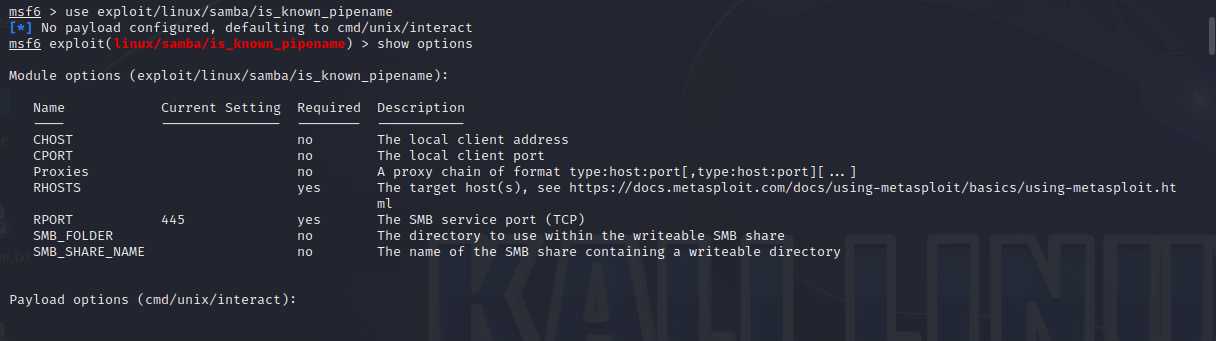
- B1: Khởi động Metaploit



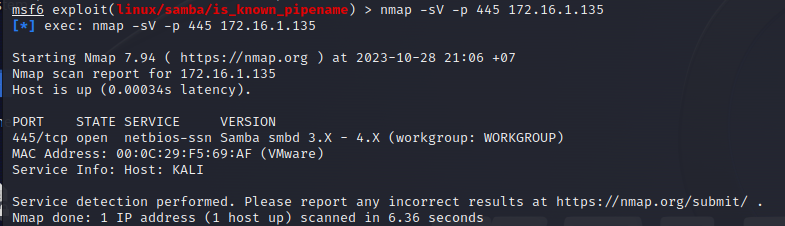
- B2: Tìm kiếm công cụ khai thác Samba. Công cụ này đã được cài đặt sẵn trong Kali-2023



- B3: Sử dụng Module exploit/linux/samba/is\_known\_pipename được tích hợp sẵn trong công cụ Samba



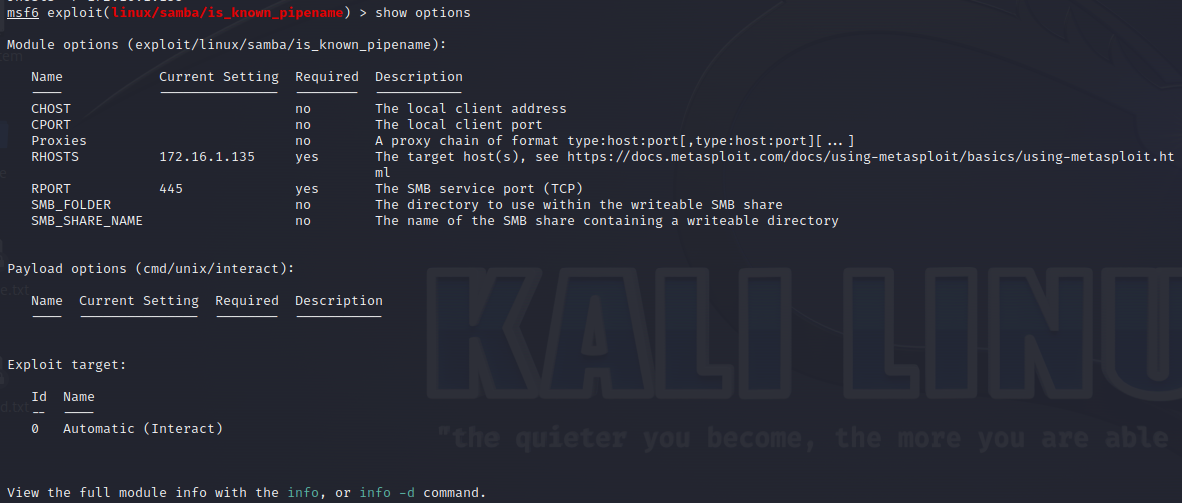
- B4: Dùng lệnh nmap để quét cổng và địa chỉ của máy Victim xem đã lắng nghe được chưa



- B5: Đặt Rhost chính là IP của máy Victim



- B6: Sau khi hoàn tất các bước trên ta show options



- B7: Trêm máy Victim ta khởi động công cụ Samba bằng câu lệnh sau



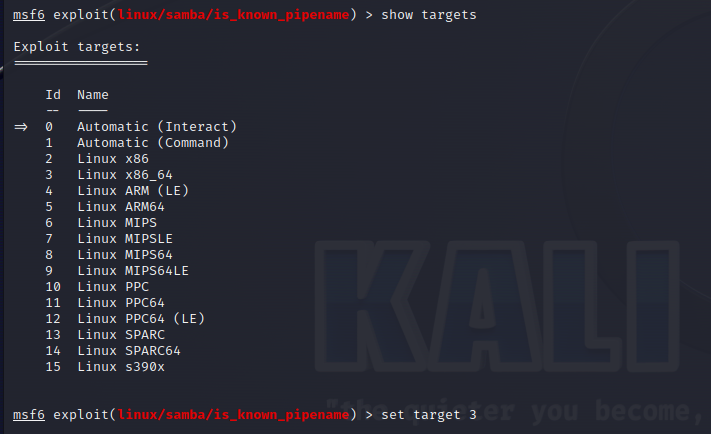
- B8: Chỉnh sửa file theo đường dẫn /etc/samba/smb.conf với nội dung như hình bên dưới



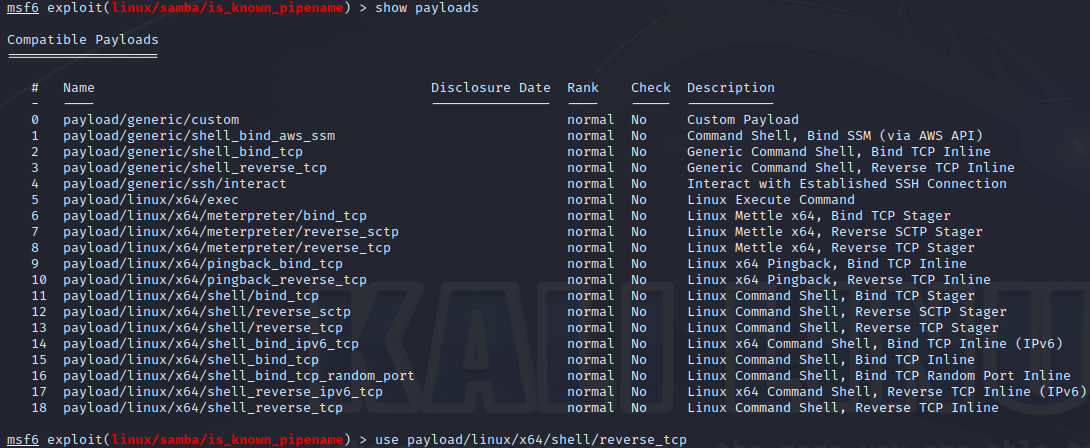
- B9: Restart lại công cụ Samba trên máy Victim



- B10: Chọn target phù hợp để tấn công, do ở đây ta tấn công máy kali\_2016 nên ta chọn target 3



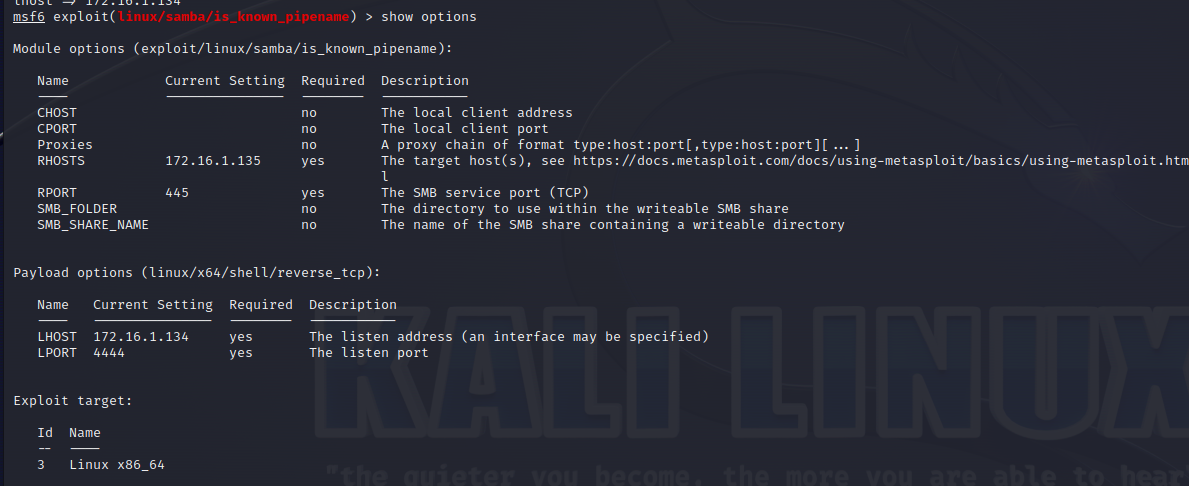
- B11: Chọn sử dụng payload như hình bên dưới



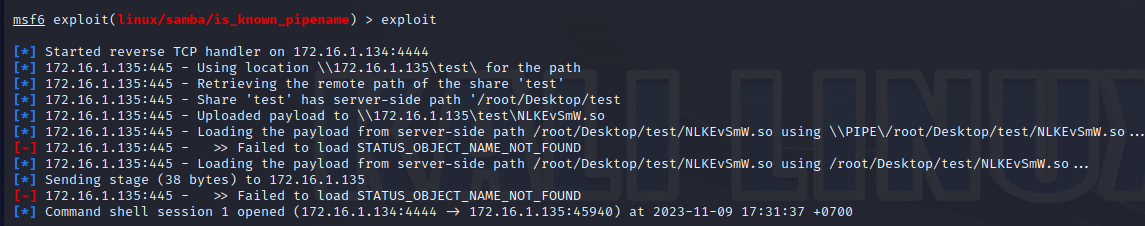
- B12: Thiết lập LHOST chính là IP của máy attack



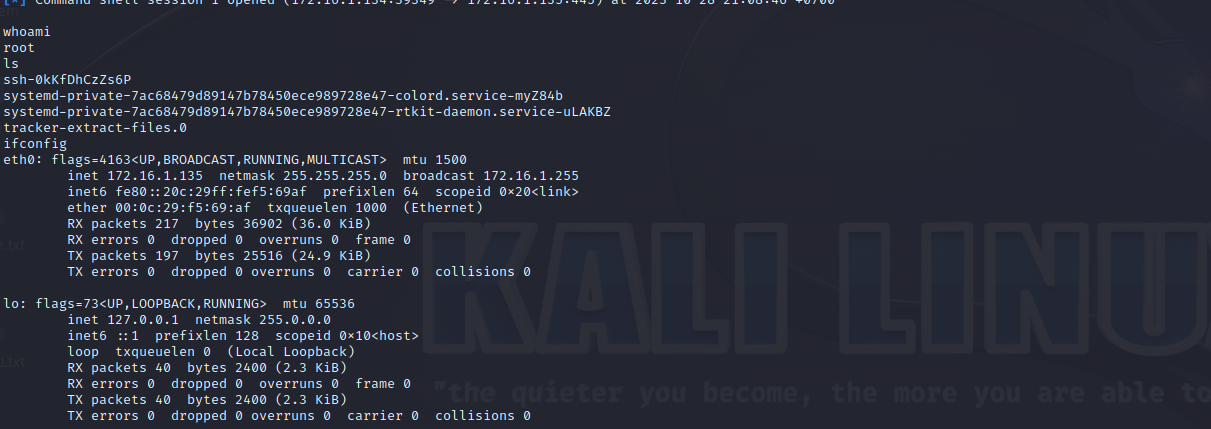
- B13: Sau khi đã thực hiện các bước trên ta show lại options để kiểm tra



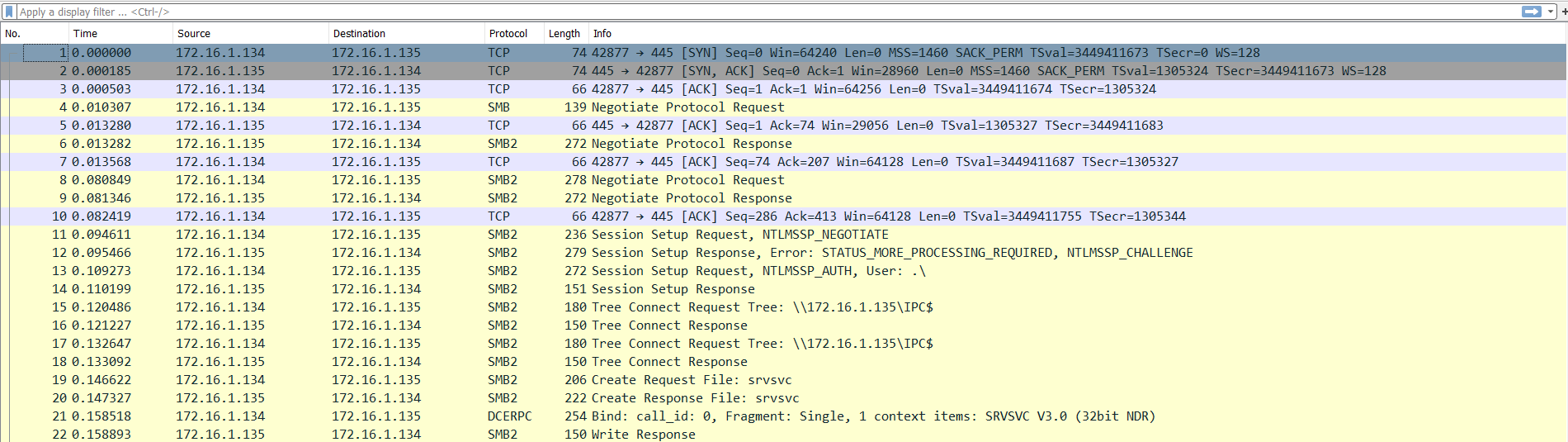
- B14: Trên máy attack thực hiện câu lệnh Exploit để tấn công



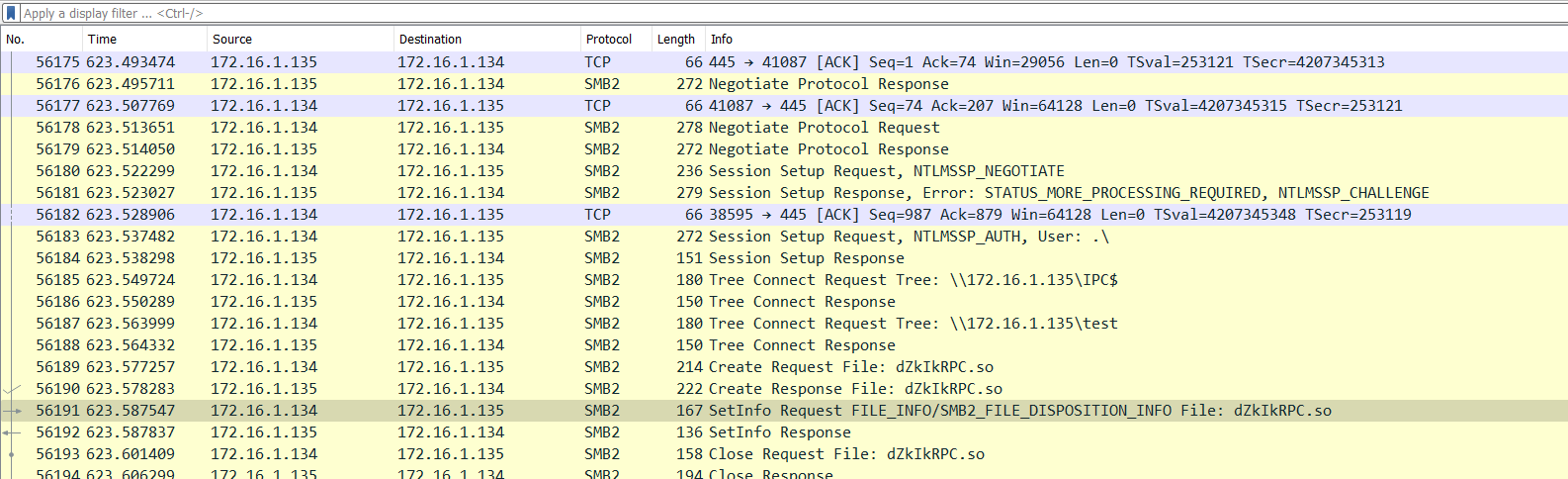
- B15: Sau khi tấn công thành công ta thực hiện các câu lệnh khi đã chiếm được quyền hệ thống file của máy Victim



**3. Trình bày dữ liệu tấn công**

*Dữ liệu khi bắt đầu chạy payload*  


*Dữ liệu khi payload chạy thành công*



*Xác định signature*

* Địa chỉ nguồn: Địa chỉ nguồn là địa chỉ IP của máy tính tấn công.
* Địa chỉ đích: Địa chỉ đích là địa chỉ IP của máy tính mục tiêu.
* Khi tấn công ta thấy có một session được tạo, trong cái session sẽ phản hồi những cái yêu cầu mà máy attack đã ra lệnh
* Khi tấn công thành công ta thấy sẽ có một file với phần đuôi .so được tạo ra, như đã được đề cập ở phần 1 thì file này là một đoạn mã đảo ngược (reverse-shell)- đây là dấu hiệu việc đã tấn công thành công
* Ngoài ra ta còn chú ý thêm là protocol của hình thức này chính là SMB hoặc là SMB2
* Chiều dài của gói packet lúc nào cũng lớn, thường chiều dài của nó sẽ vượt quá 100.

