BÁO CÁO THỰC HÀNH

**Môn học: Cơ chế hoạt động của mã độc**

**Kỳ báo cáo: Buổi 03 (Session 03)**

**Tên chủ đề: Worm**

*GVHD: Nghi Hoàng Khoa*

*Ngày báo cáo: 3/07/2021*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT230.L21.ANTT.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Hoàng Đông | 16520222 | 16520222@gm.uit.edu.vn |

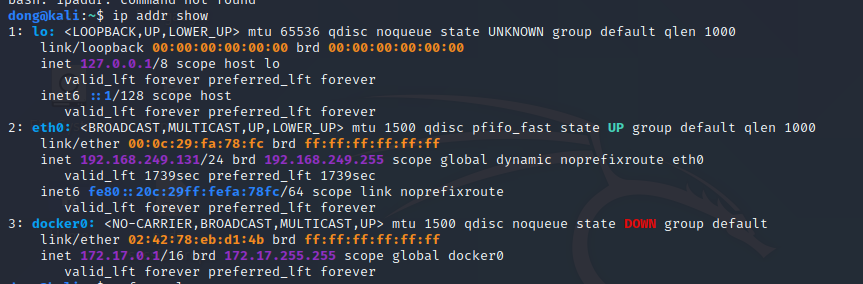
**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

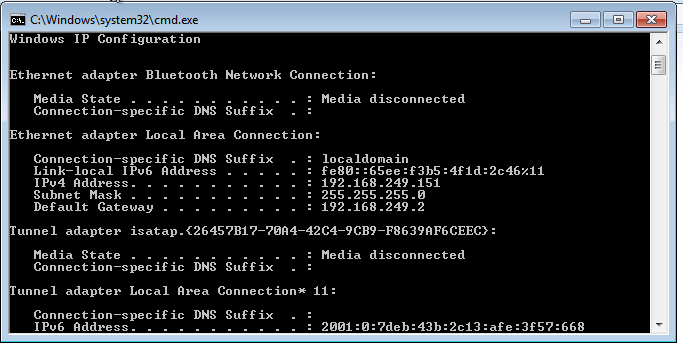
**Bài tập về nhà**

**B.1 Khai thác lỗ hổng MS17-010 sử dụng Metasploit**

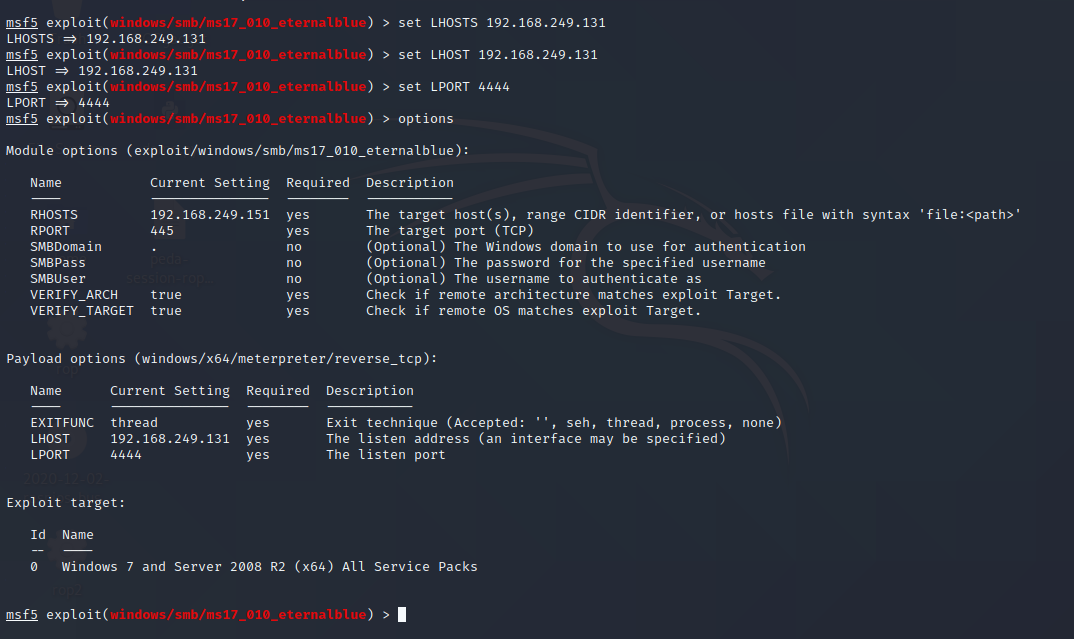
**- ip máy attacker: 192.168.249.131**



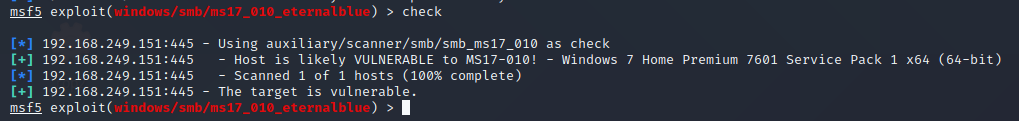
* Ip máy nạn nhân: 192.168.249.151



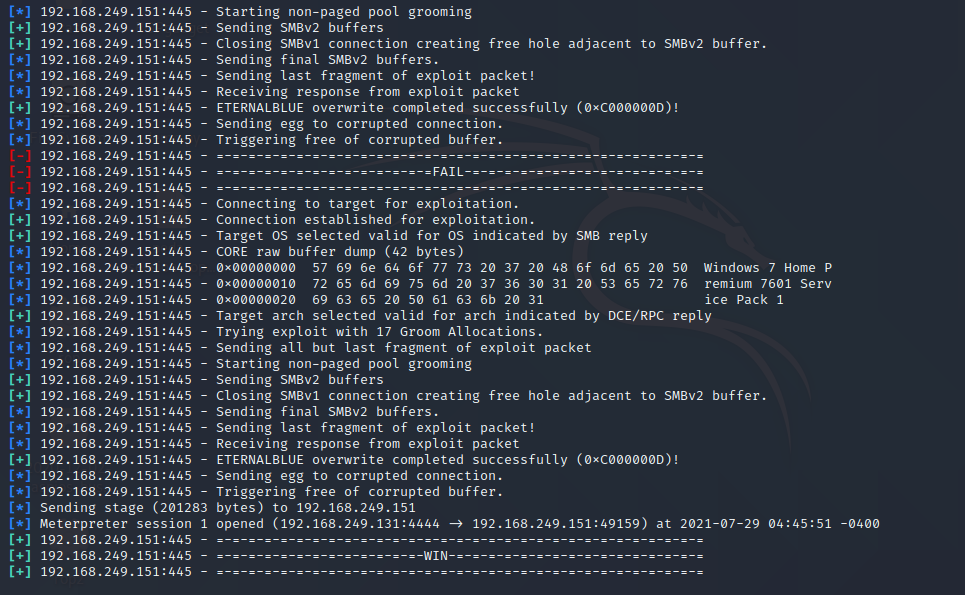
* Chọn module exploit/windows/smb/ms17\_010\_eternalblue
* Thiết lập IP máy nạn nhân là 192.168.249.151
* Payload reverse shell mặc định sẽ là windows/x64/meterpreter/reverse\_tcp



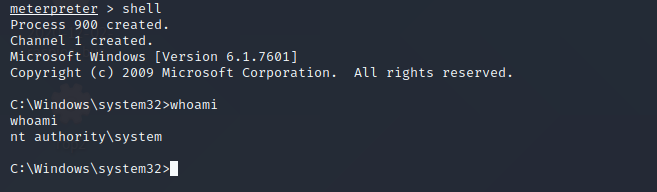
* Sử dụng lệnh check để đảm bảo máy nạn nhân tồn tại lỗ hổng này



* Thực hiện khai thác lỗ hổng này bằng lệnh **exploit**



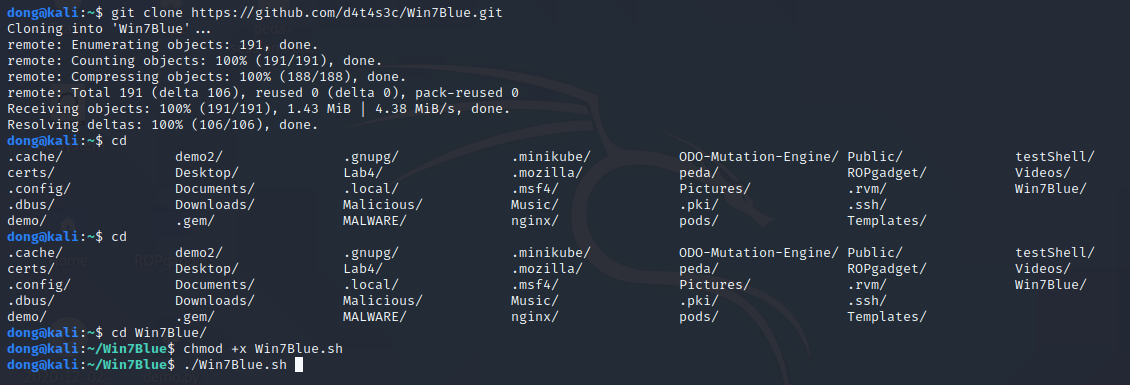
* Sau khi có được meterpreter shell, có thể chuyển sang cmd bằng lệnh shell





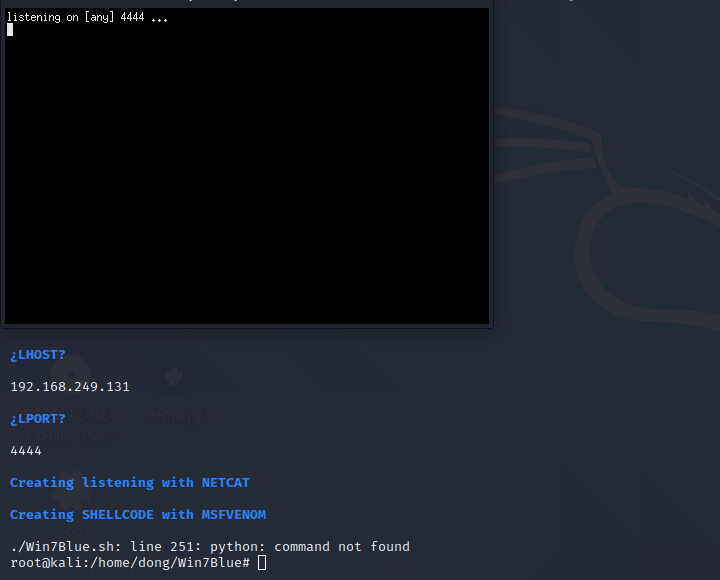
**B.2 Khai thác lỗ hổng MS17-010 không sử dụng Metasploit**

* Trên máy kẻ tấn công, thực hiện các lệnh sau để tải về exploit không sử dụng Metasploit Framework



* Xuất hiện giao diên Win7Blue





* Đến đây em có gặp phải lỗi. mặc dù đã cài cả python2 và python3

--------------------------HẾT----------------------------

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-SessionX\_ NT330.K21.1. (trong đó X là Thứ tự buổi Thực hành).

*Ví dụ: [*NT101.K11.ANTT*]-Session1\_13520401-13520387.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài Lab.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**