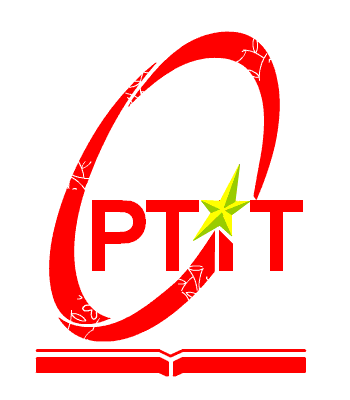
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



Môn: An toàn hệ điều hành

BÀI BÁO AN TOÀN HỆ ĐIỀU HÀNH

**Bài thực hành số 1**

**Họ và tên giảng viên**: TS.Hoàng Xuân Dậu

**Sinh viên thực hiện:** Nhóm 02

**Họ và tên:** Nguyễn Thái Hưng

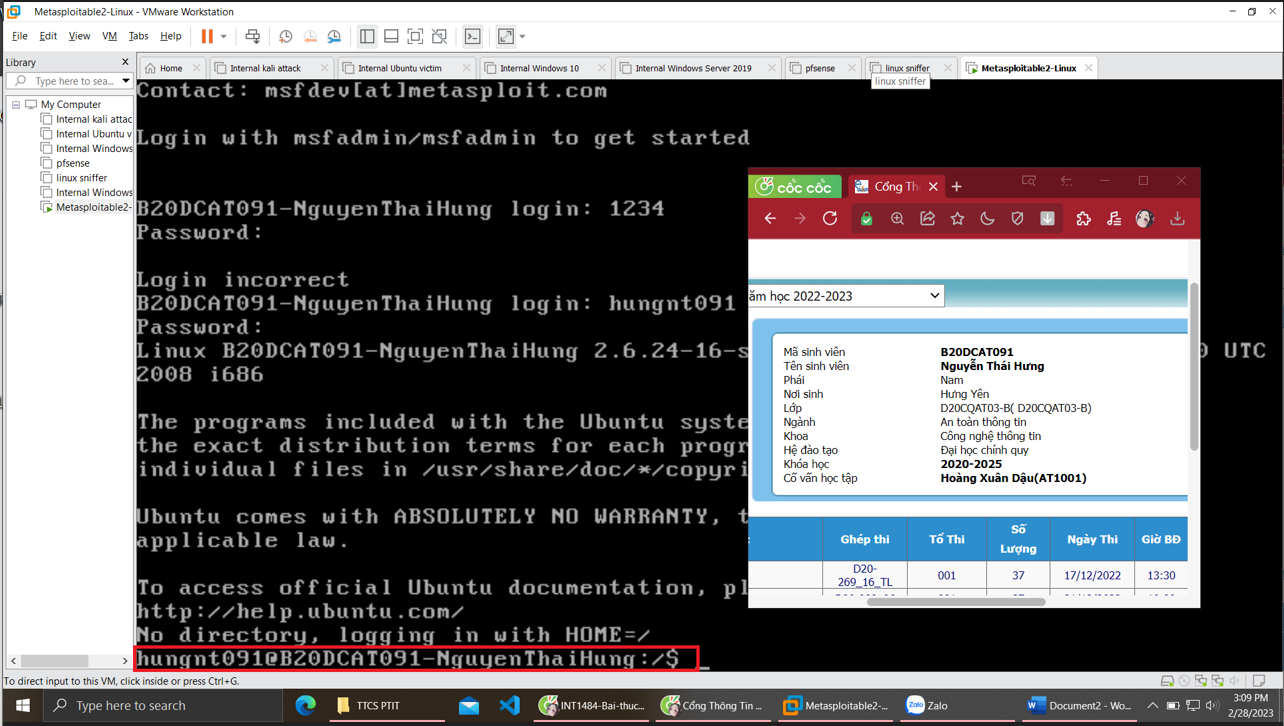
**Mã sinh viên:** B20DCAT091

**Lớp:** D20CQAT03-B

**Số điện thoại:** 0823226644

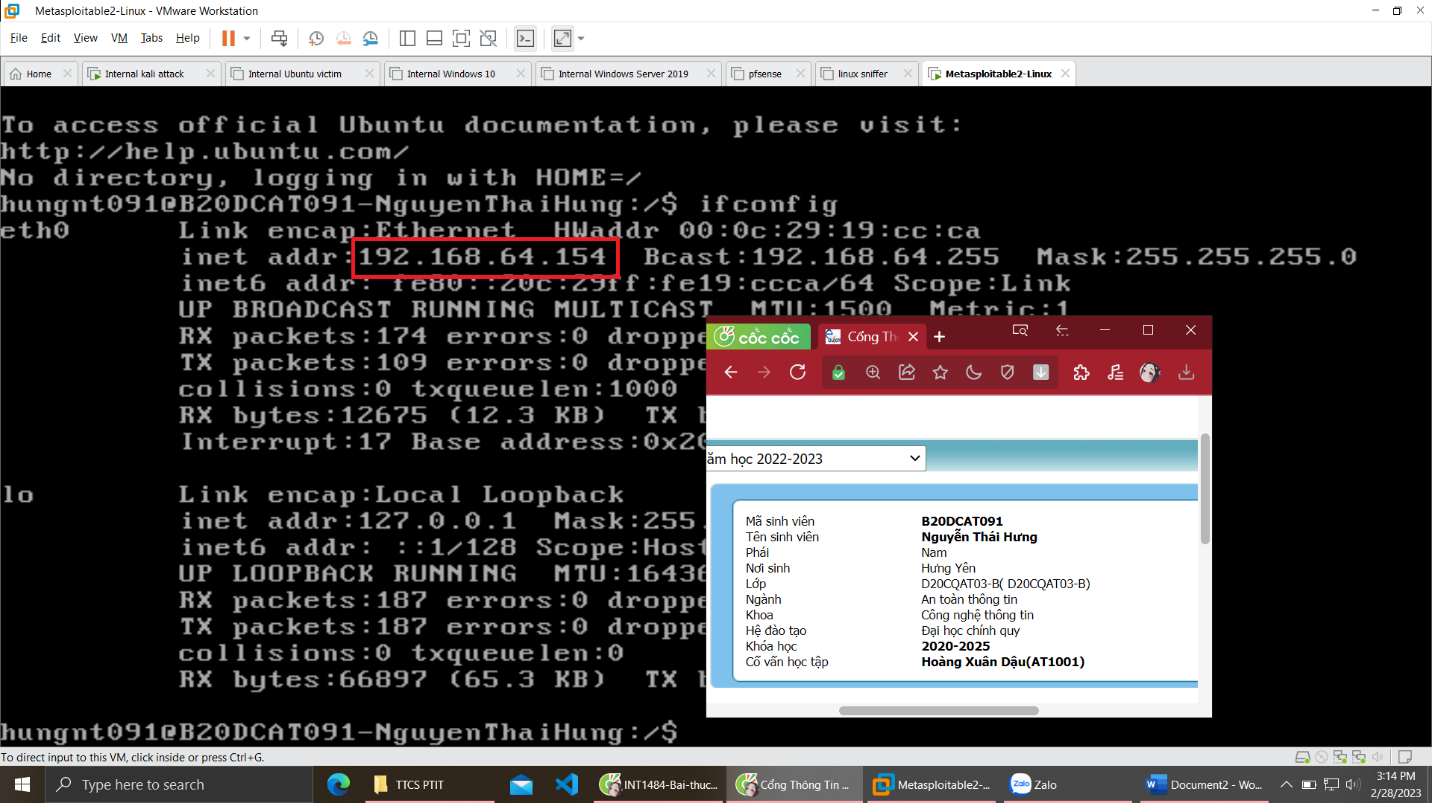
Hà Nội 2023

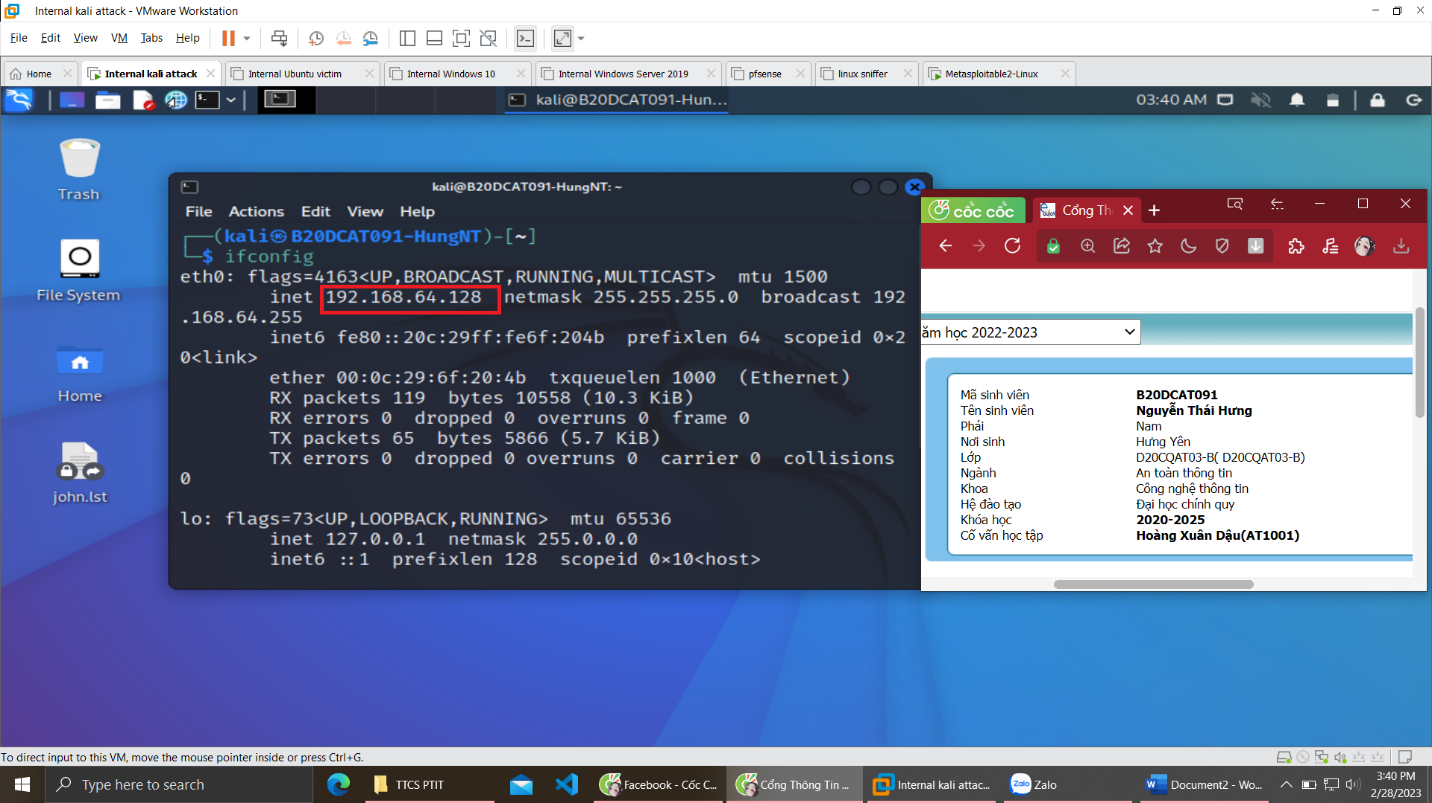
1.Đổi tên máy và tạo người dùng thành công



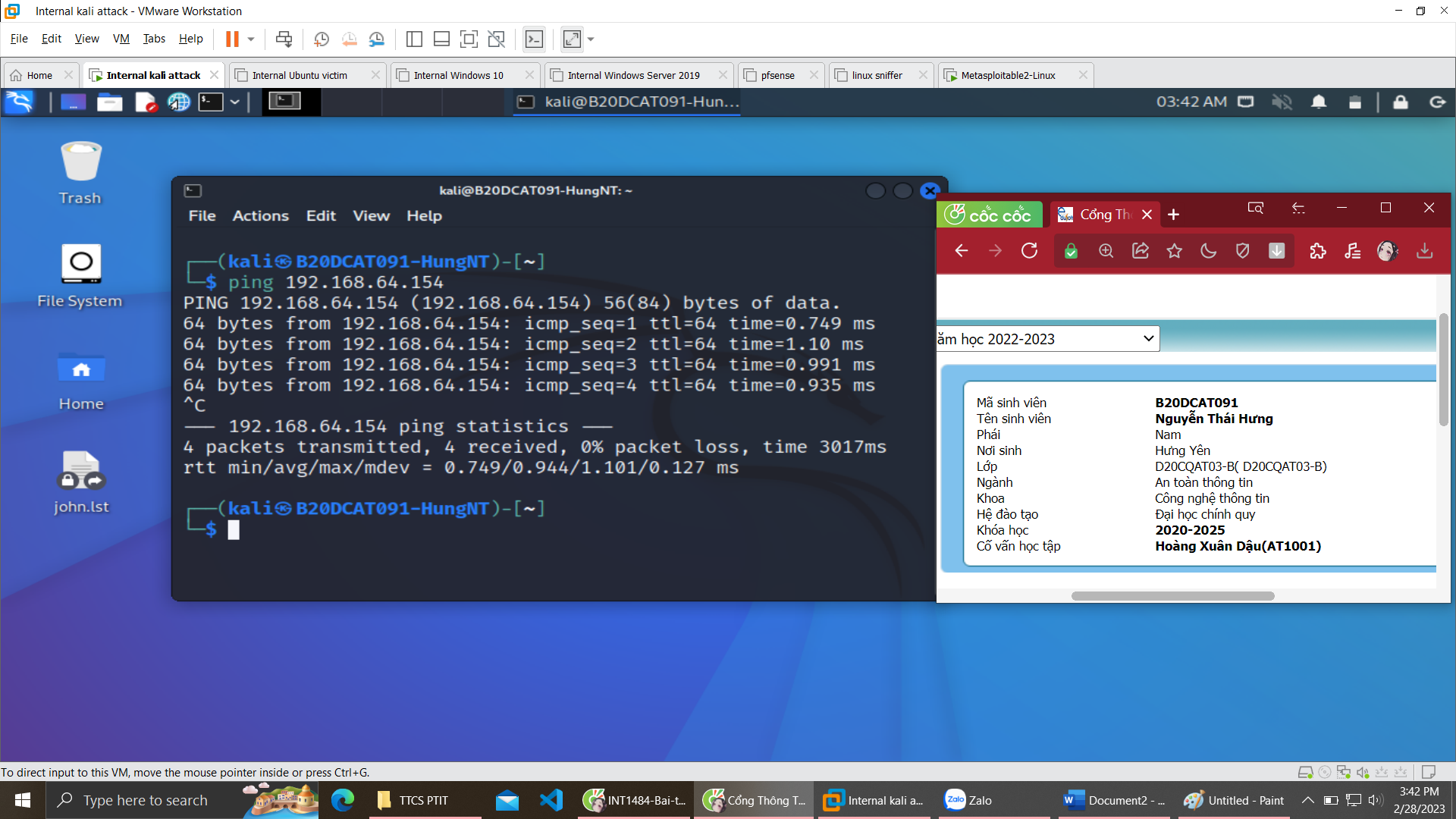
2.Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

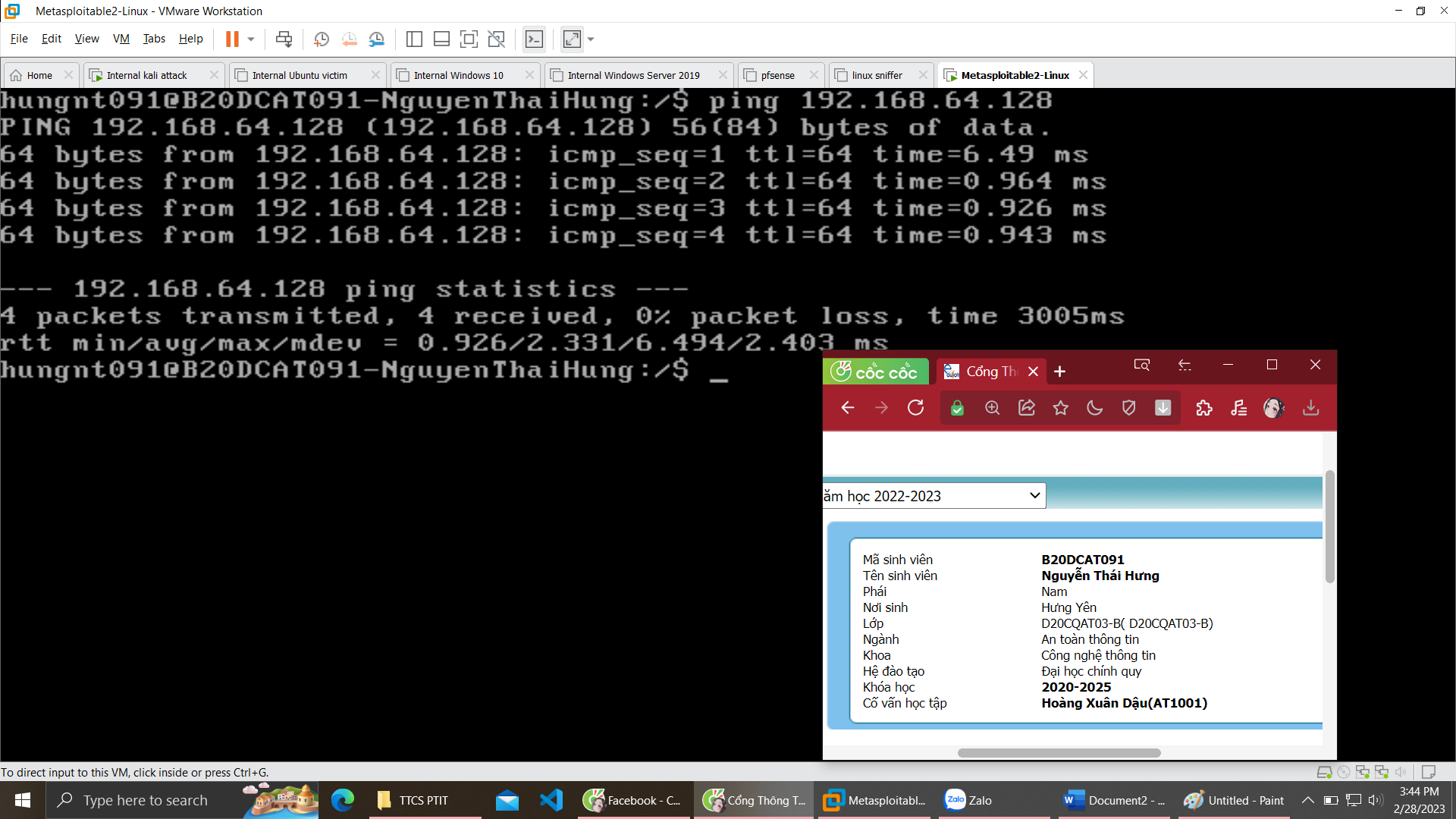
Tìm địa chỉ IP của máy victim, kali:





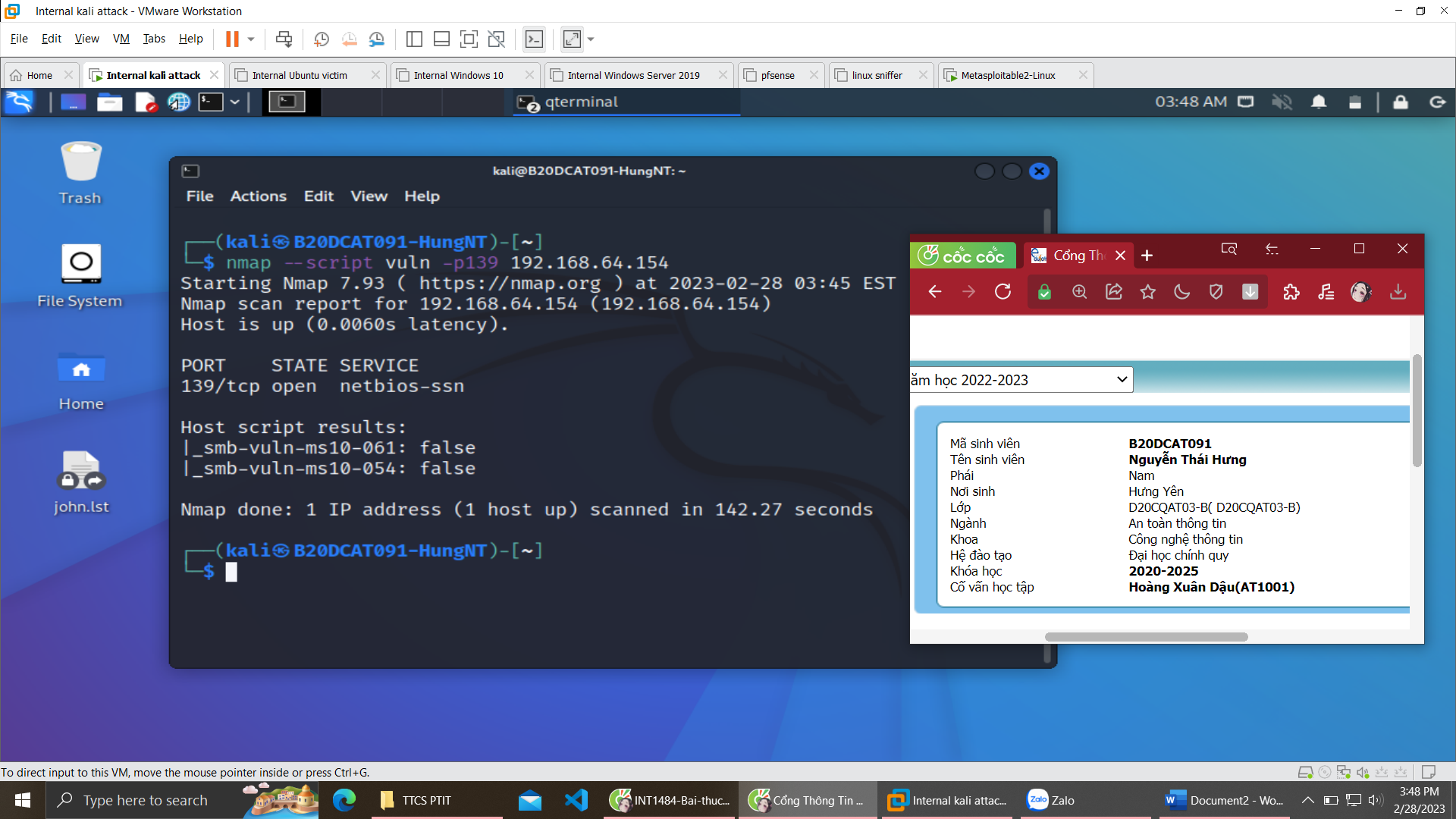
Kiểm tra kết nối mạng giữa các máy:



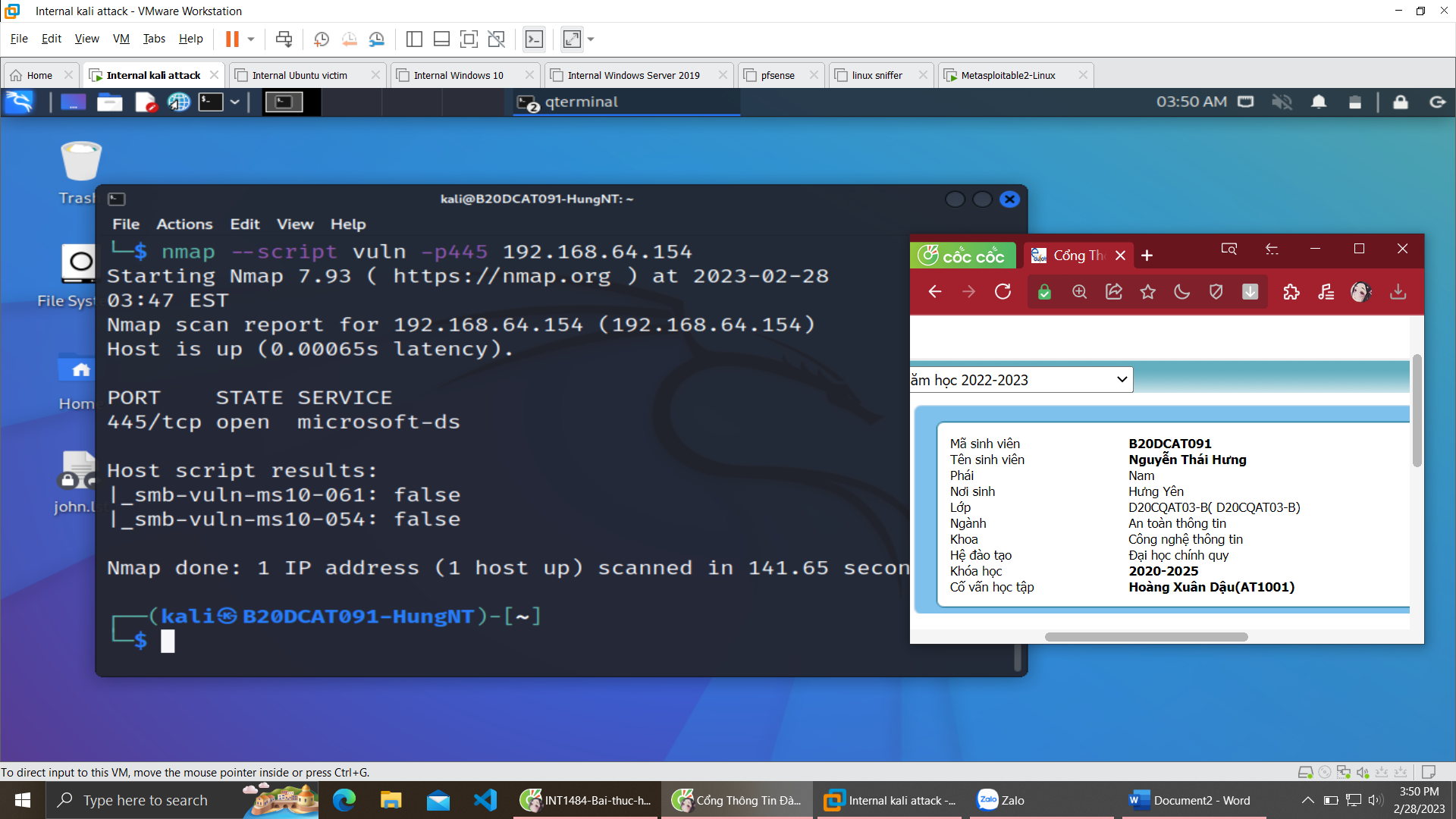


- Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:

o Quét cổng dịch vụ netbios-ssn cổng 139:

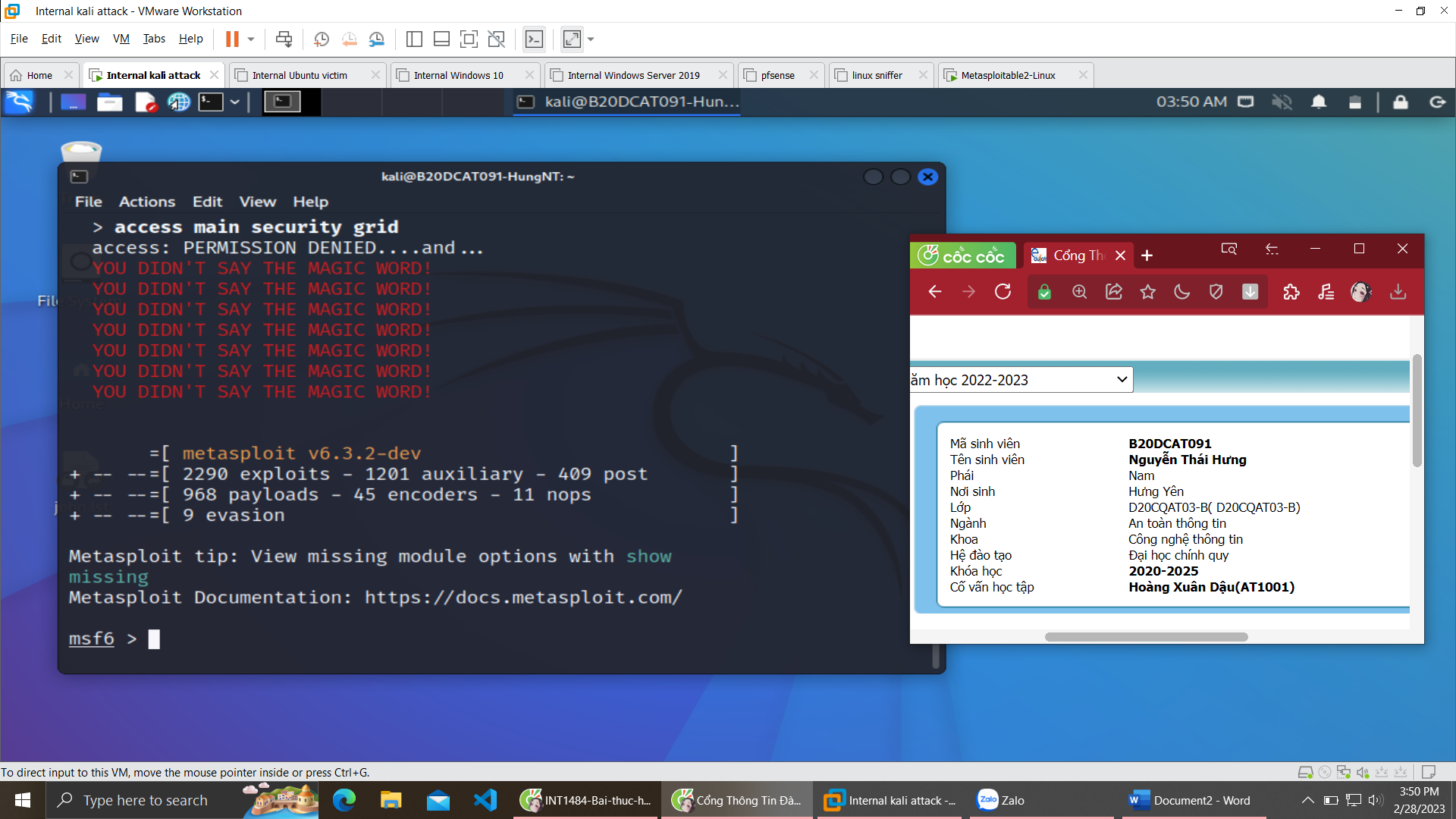


o Quét cổng dịch vụ microsoft-ds cổng 445:



3. Khai thác tìm phiên bản Samba đang hoạt động:

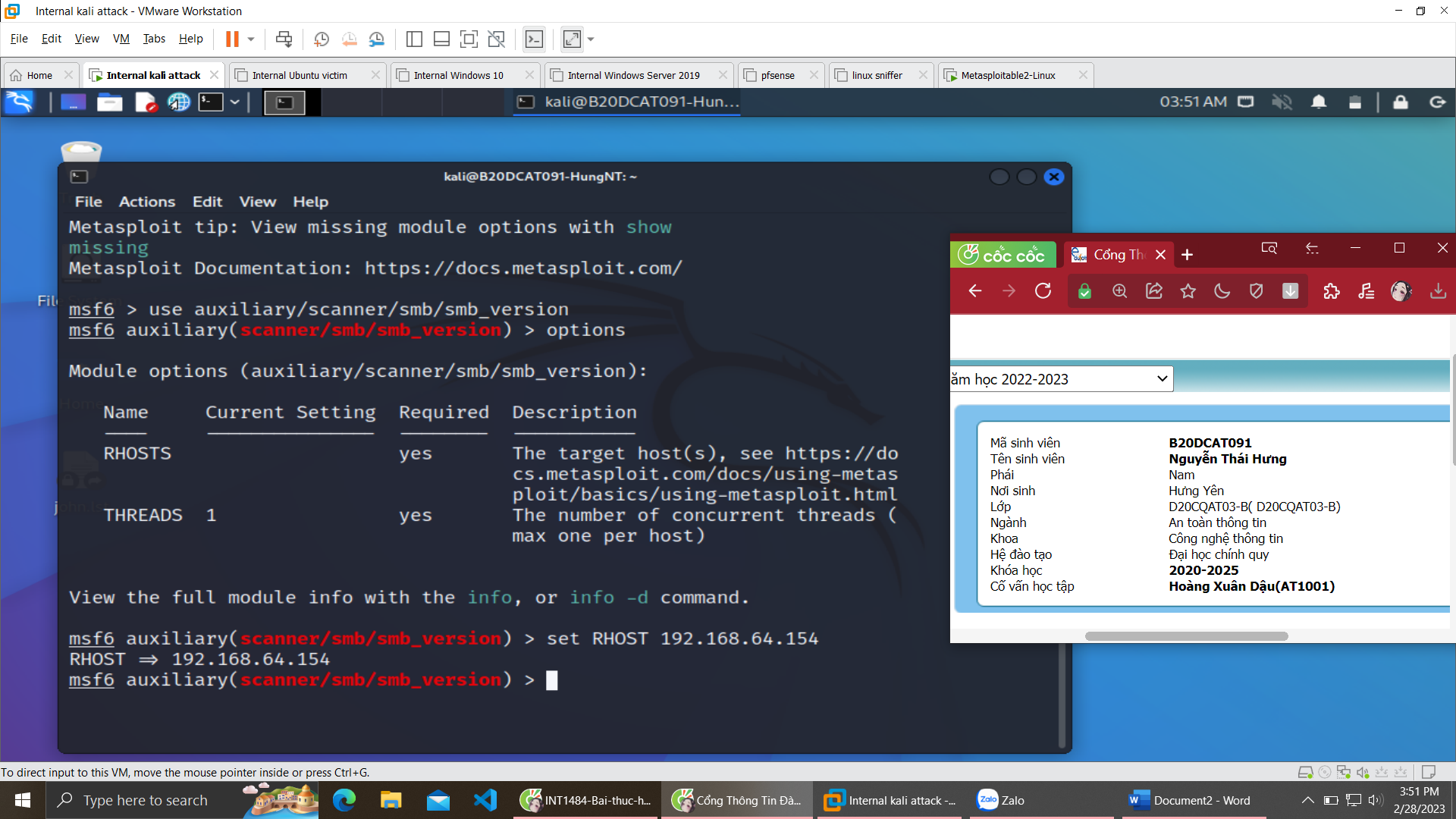
- Khởi động Metasploit



- Khai báo sử dụng mô đun tấn công:

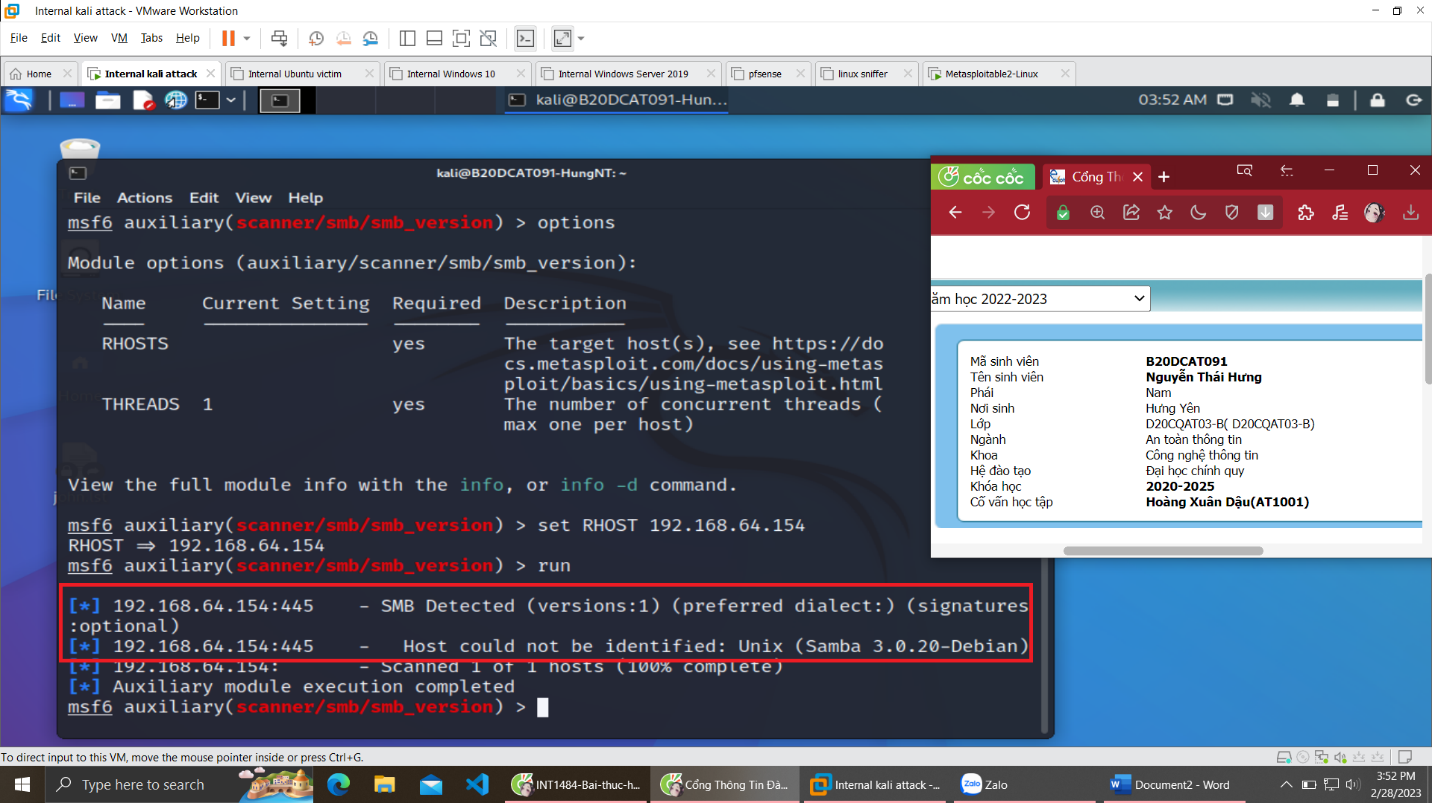
- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

- Đặt địa chỉ IP máy victim:

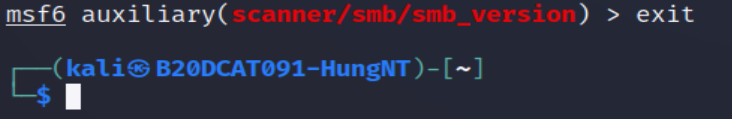


- Thực thi tấn công:

Máy victim sẽ liệt kê tên dịch vụ Samba và phiên bản



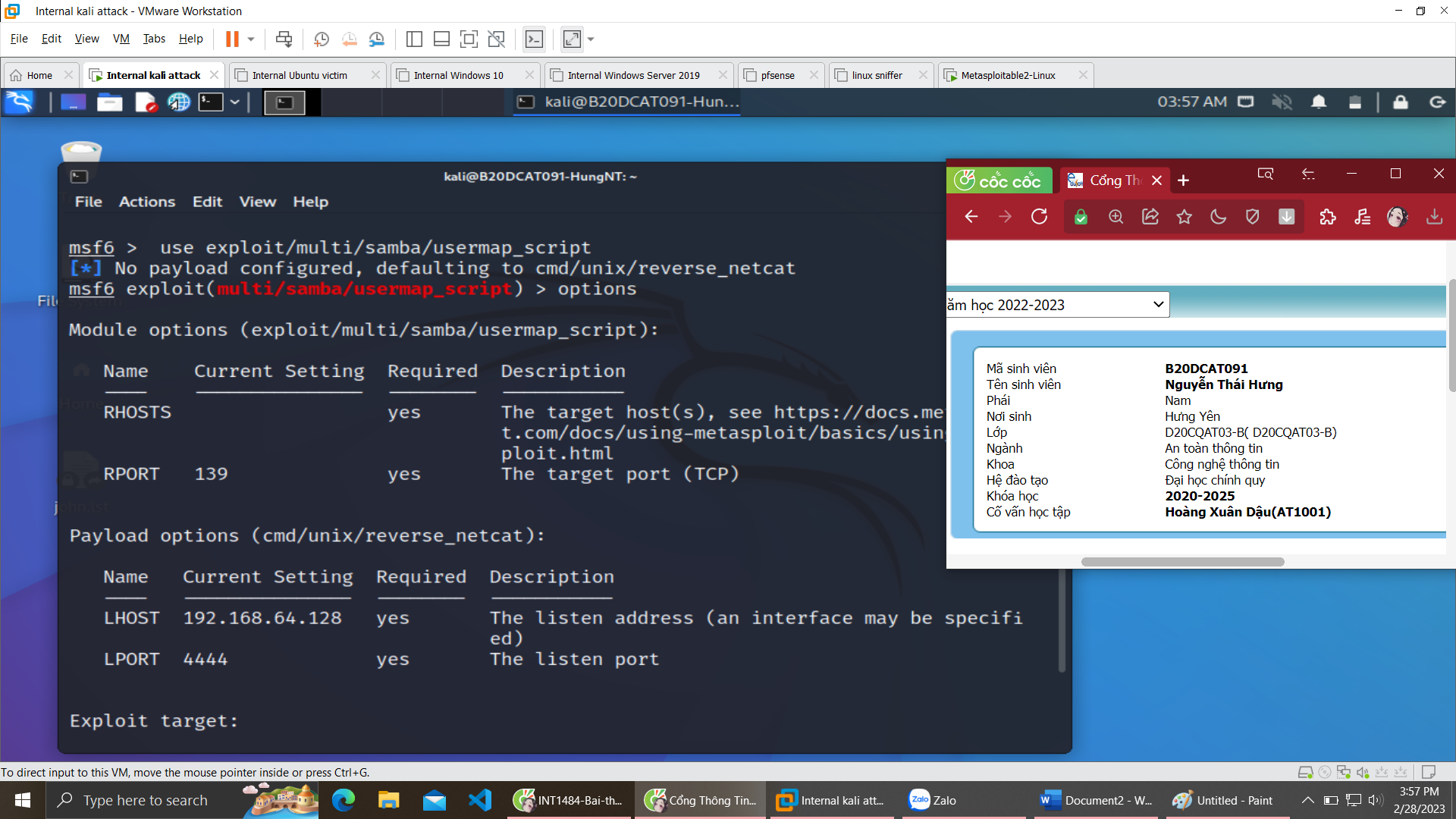
- Gõ lệnh exit để kết thúc



4 Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

- Khai báo sử dụng mô đun tấn công:

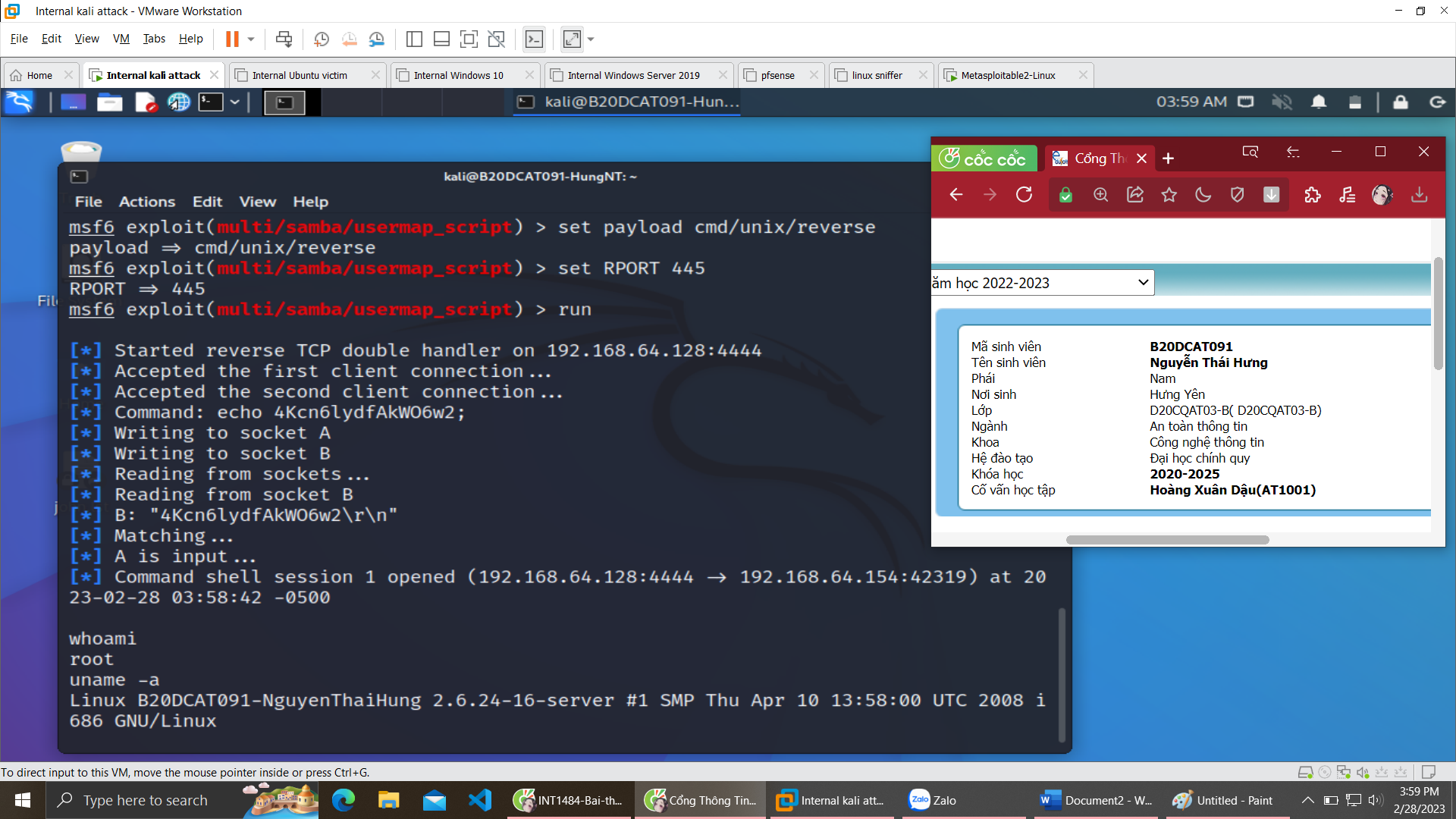
-Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng



Đặt địa chỉ IP máy victim

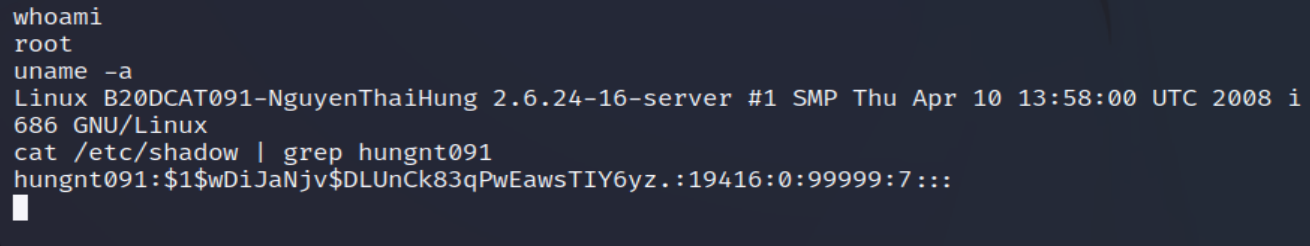
Chọn payload cho thực thi (mở shell):

Đặt 445 là cổng truy cập máy victim:

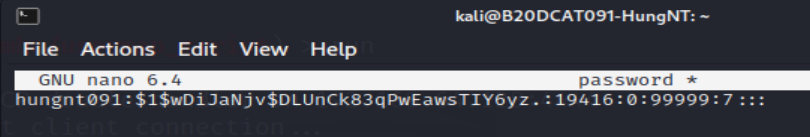


Lấy tên người dùng và mật khẩu đã tạo ở mục 3.1

Chọn và sao chép cả dòng tên người dùng và mật khẩu băm vào clipboard



Mở một cửa sổ Terminal mới, chạy lệnh: nano password sau đó paste thông tin tên người dùng và mật khẩu băm từ clipboard vào file password



Sử dụng công cụ john để crack mật khẩu

