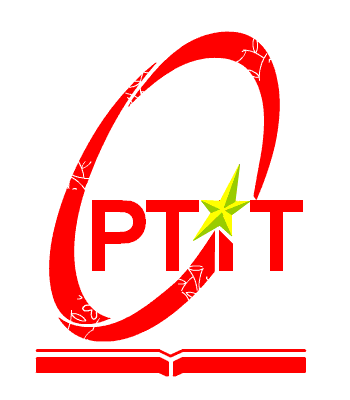
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



Môn: An toàn hệ điều hành

BÀI BÁO AN TOÀN HỆ ĐIỀU HÀNH

**Bài thực hành số 2**

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

**Sinh viên thực hiện:** Nhóm 02

**Họ và tên:** Nguyễn Thái Hưng

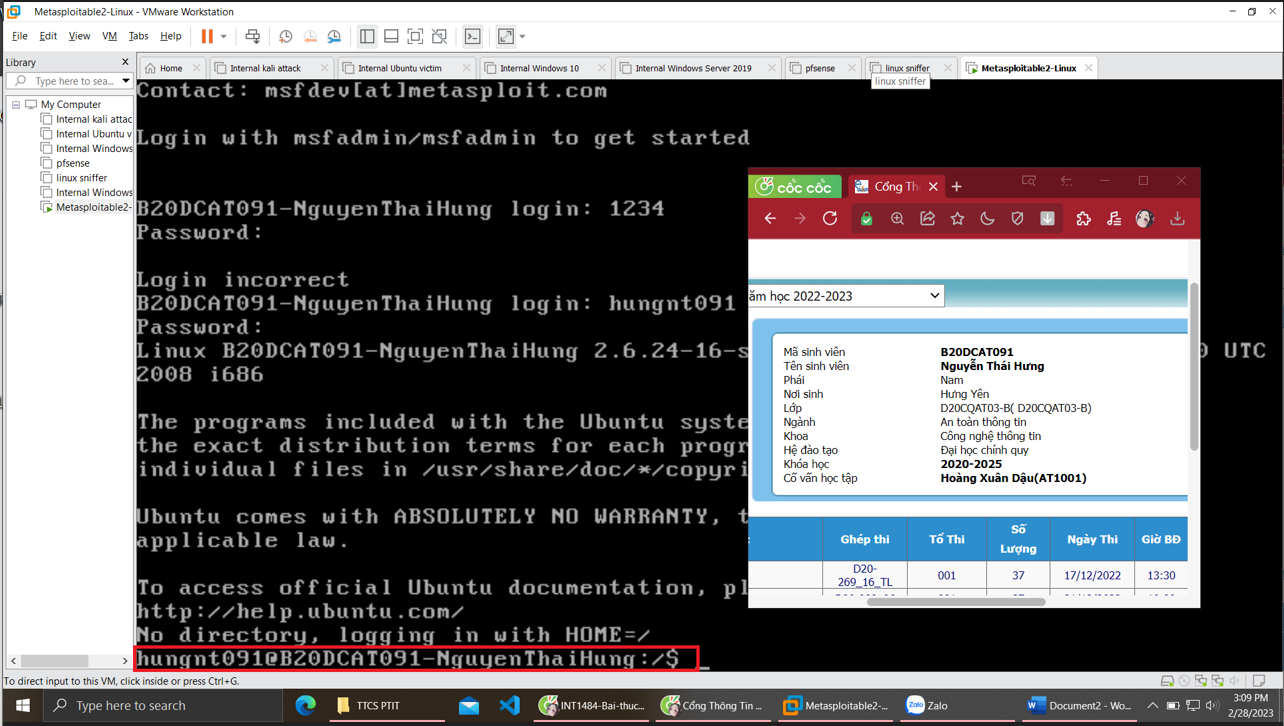
**Mã sinh viên:** B20DCAT091

**Lớp:** D20CQAT03-B

**Số điện thoại:** 0823226644

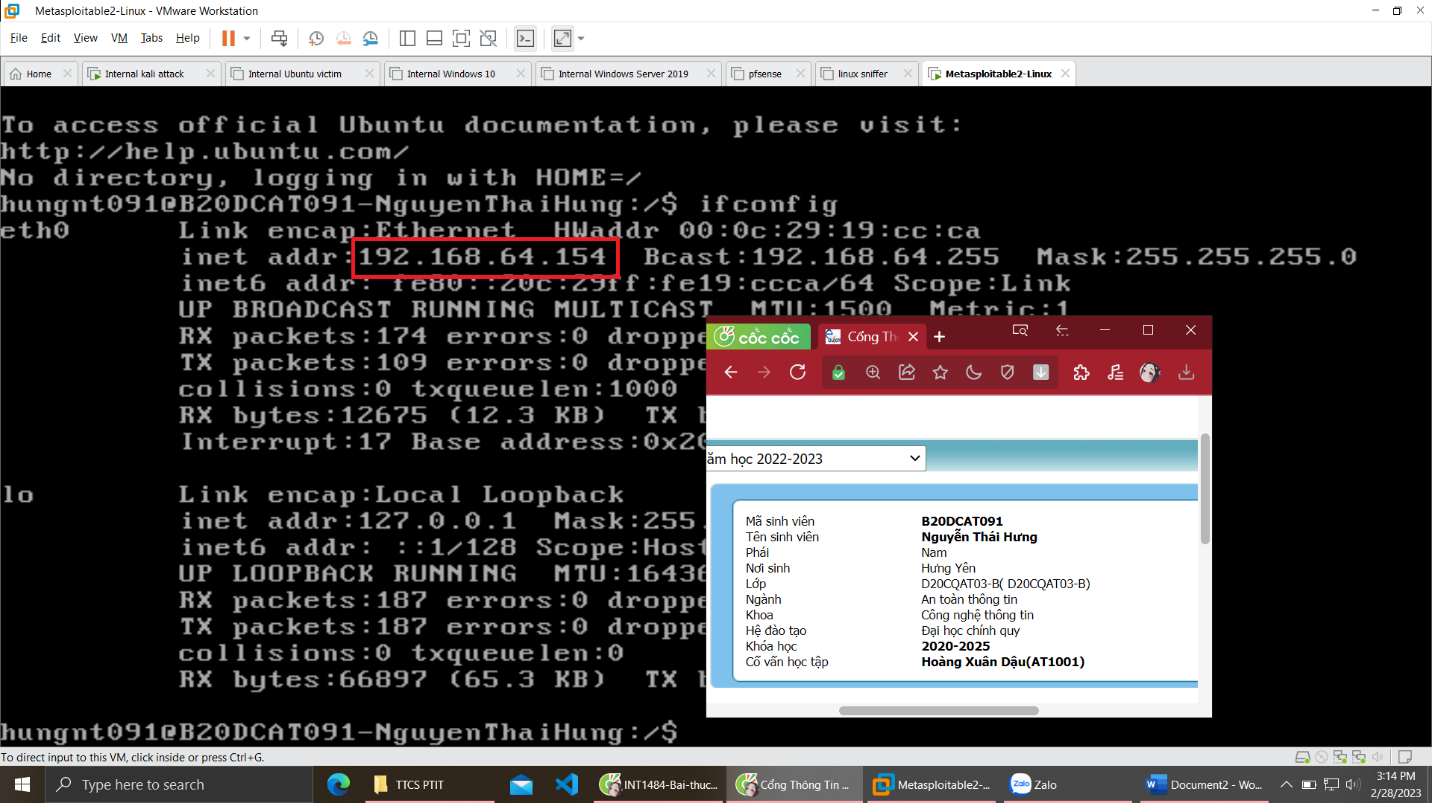
Hà Nội 2023

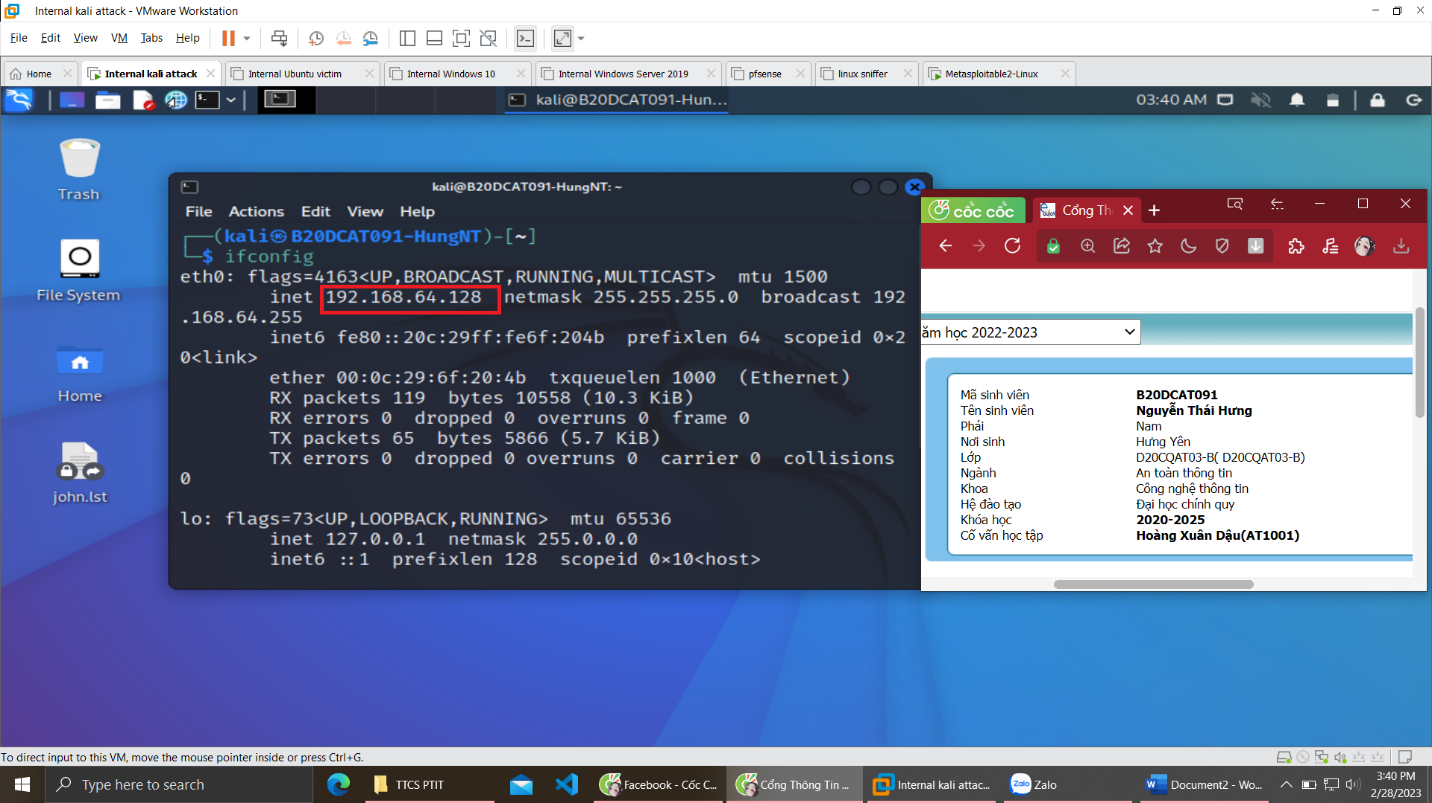
1.Đổi tên máy và tạo người dùng thành công



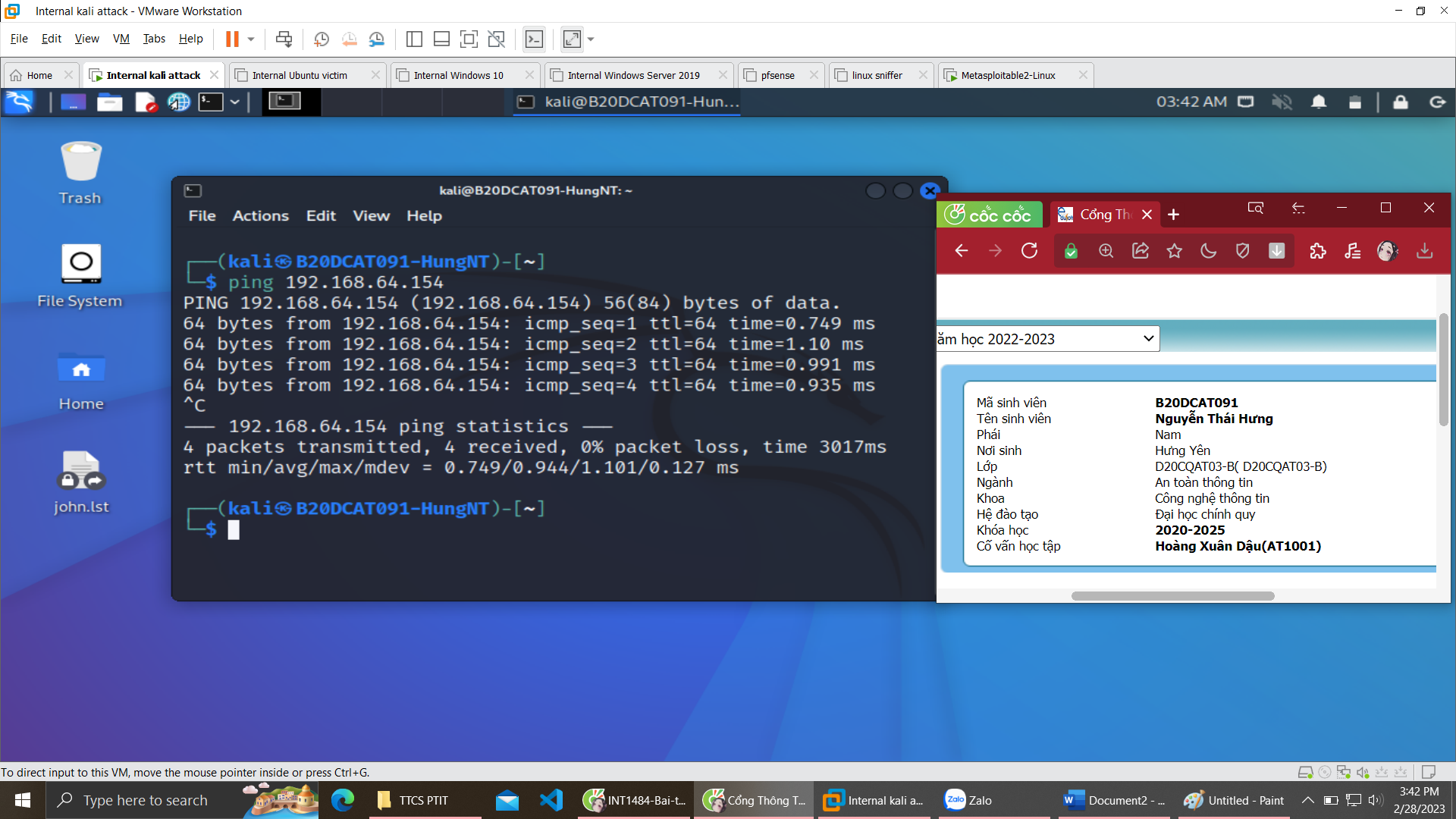
2.Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

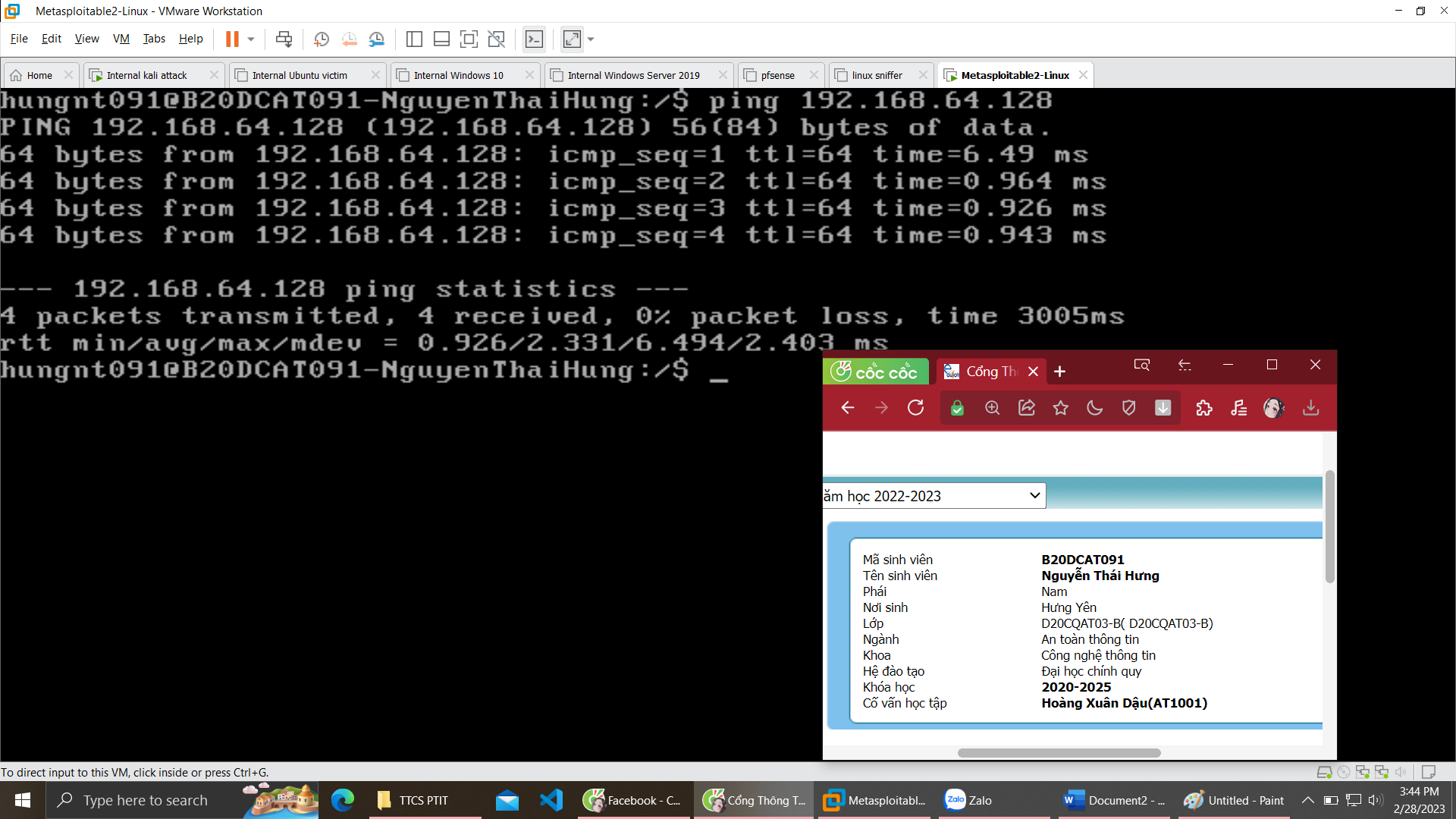
Tìm địa chỉ IP của máy victim, kali:





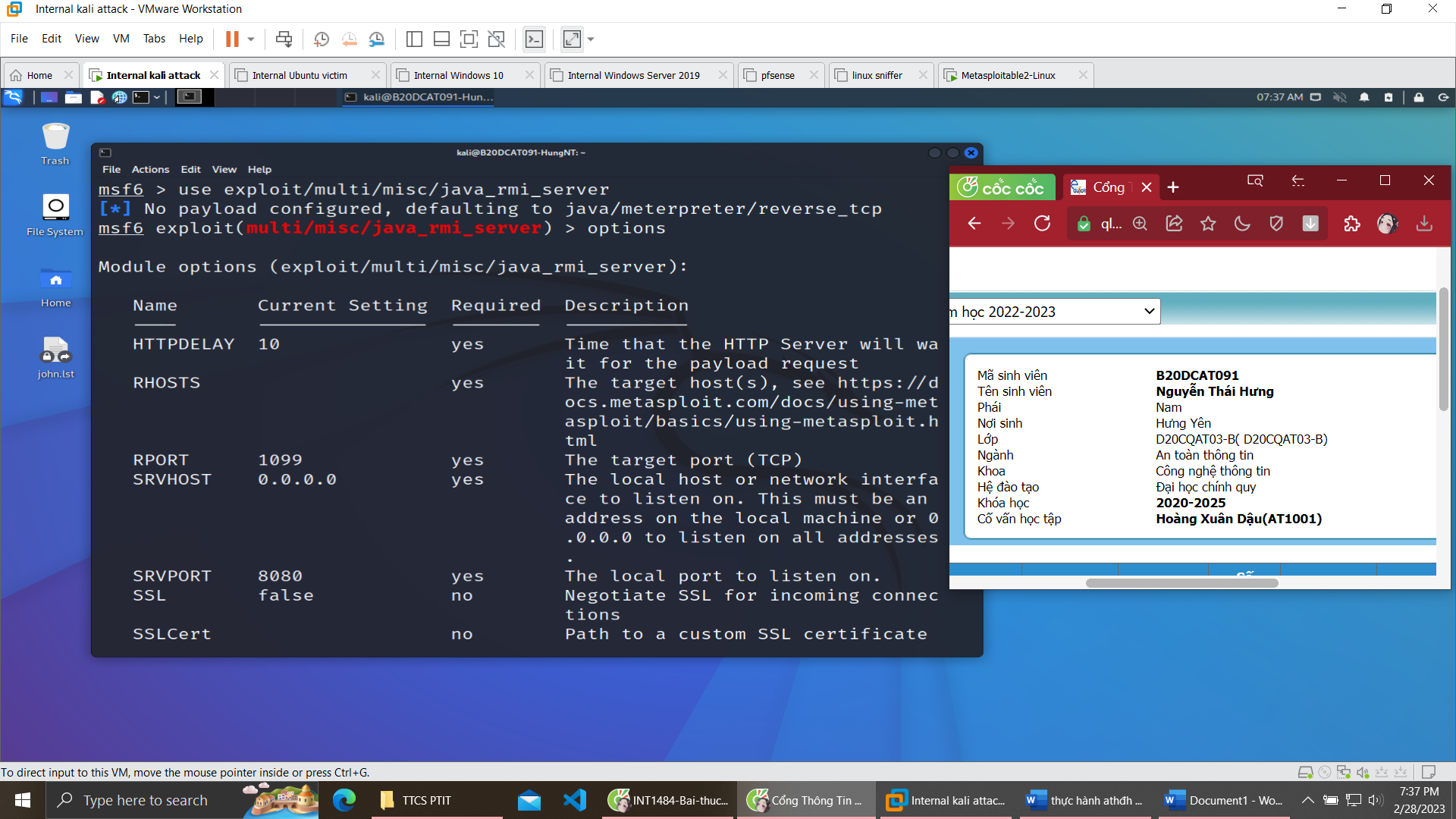
Kiểm tra kết nối mạng giữa các máy:

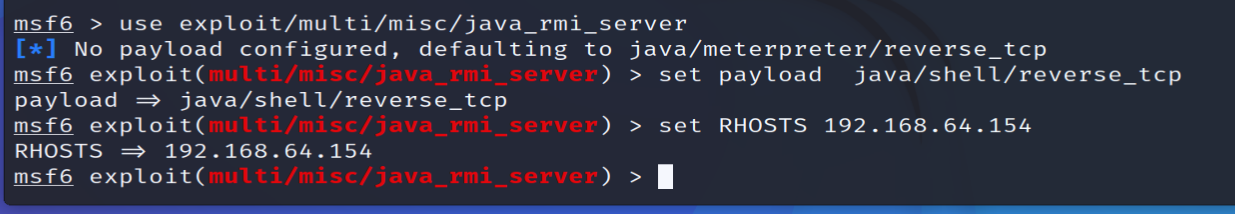


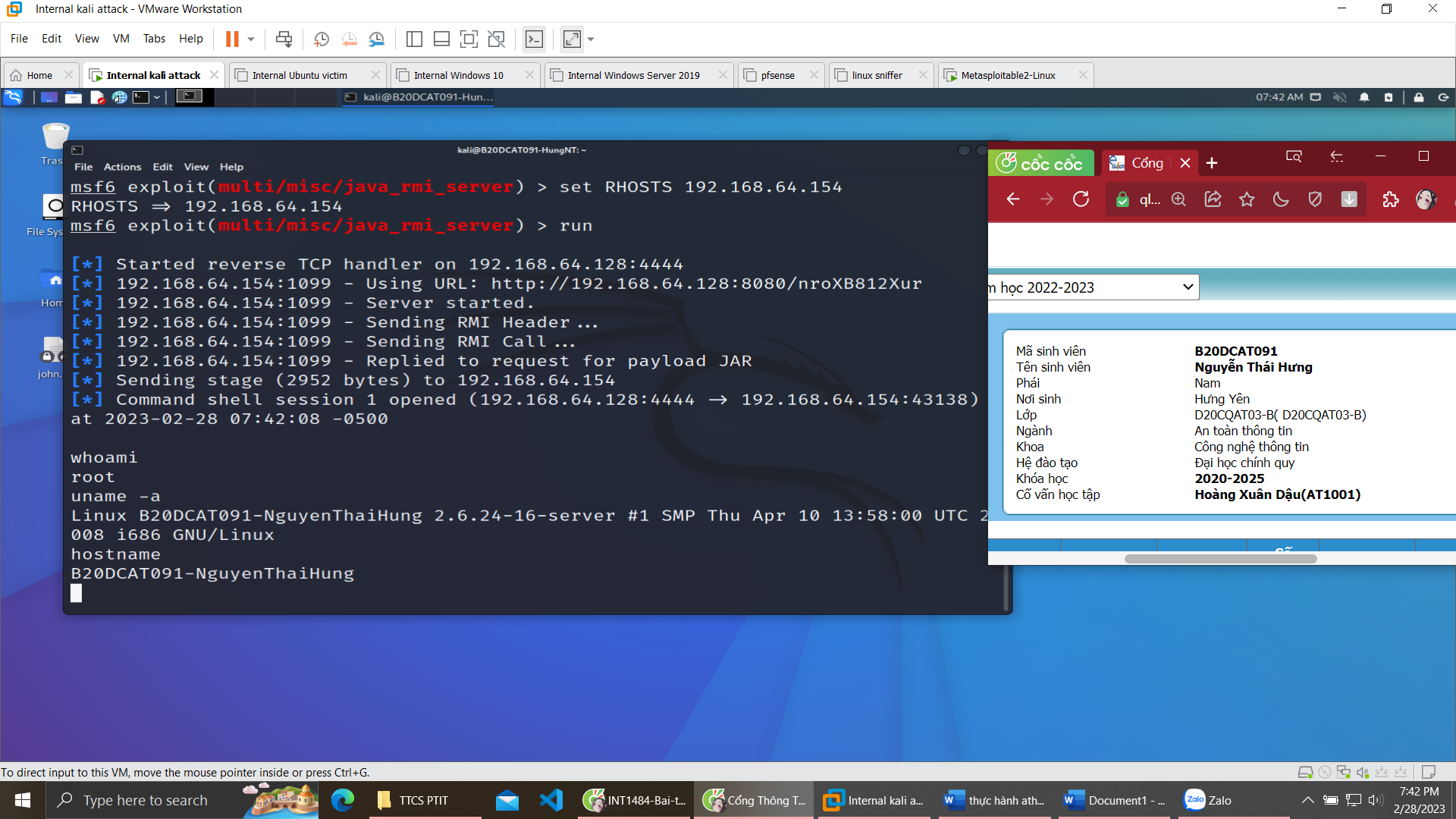


3. Khai thác lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI:

- Khai báo sử dụng mô đun tấn công->Chọn payload cho thực thi (mở shell)->Đặt địa chỉ IP máy victim->Thực thi tấn công:

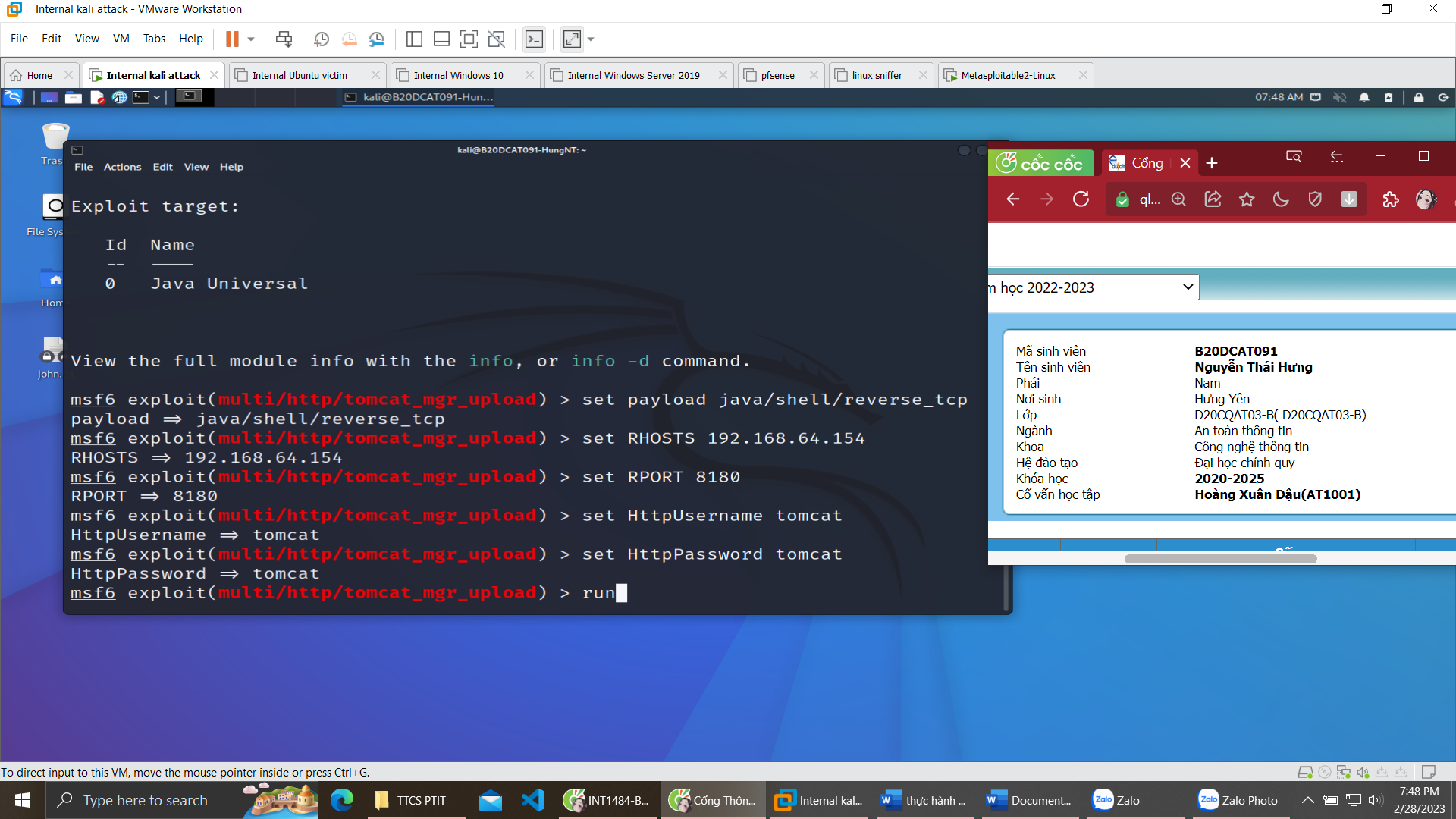






4. Khai thác lỗi trên Apache Tomcat:

- Khai báo sử dụng mô đun tấn công->- Đặt 445 là cổng truy cập máy victim->Chọn payload cho thực thi (mở shell)-> Thực thi tấn công:



➔ mở shell với người dùng tomcat55 cho phép chạy lệnh từ máy Kali

