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

**VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**BÁO CÁO THỰC HÀNH SỐ 3**

**RÀ QUÉT VÀ KHAI THÁC CÁC LỖ HỔNG CHUYÊN SÂU**

Họ và tên: Lục Nguyễn Trang Nhi

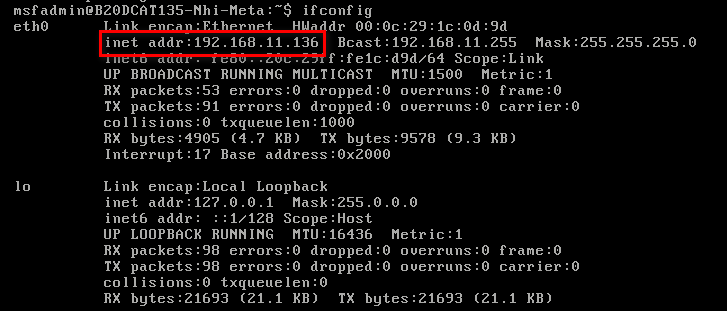
Mã sinh viên: B20DCAT135

Tổ 2 – Nhóm 2

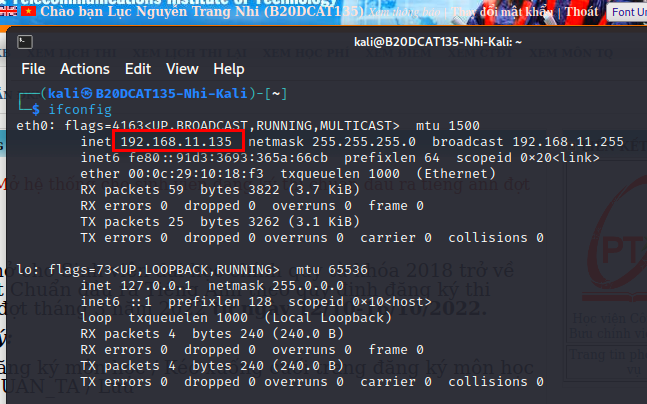
Giảng viên: Hoàng Xuân Dậu

1. **Cài đặt các công cụ, nền tảng**

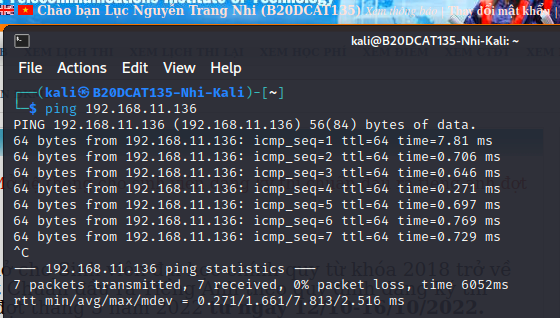
* Địa chỉ IP máy victim (Metaspoitable2): 192.168.11.136



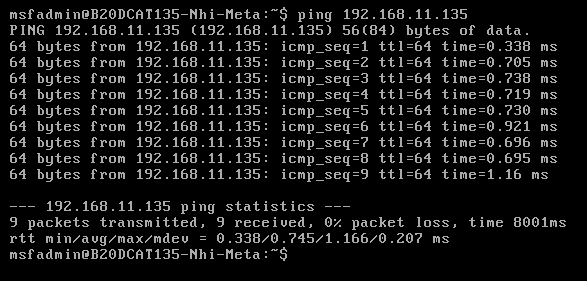
* Địa chỉ IP máy Kali: 192.168.11.136



* Kiểm tra kết nối mạng giữa các máy:
  + Màn hình ping của máy kali:

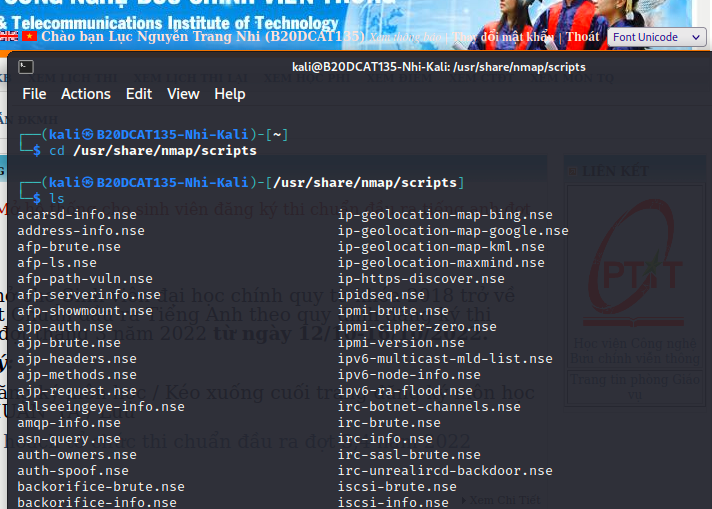


* + Màn hình ping của máy metasploitable2:

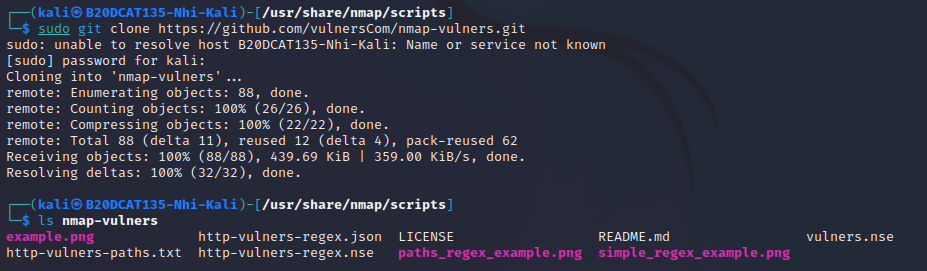


1. **Kiểm tra và cài đặt các NSE scripts cho nmap**

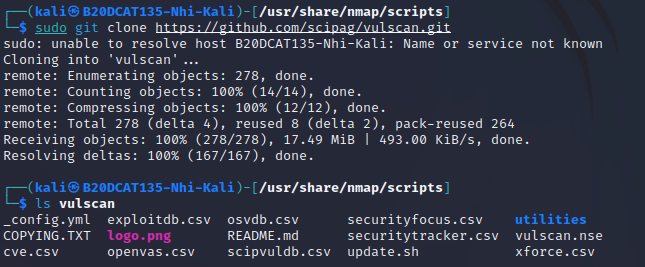
* Kiểm tra các NSE scripts có sẵn cho nmap



* Cài đặt CSDL nmap-vulners:

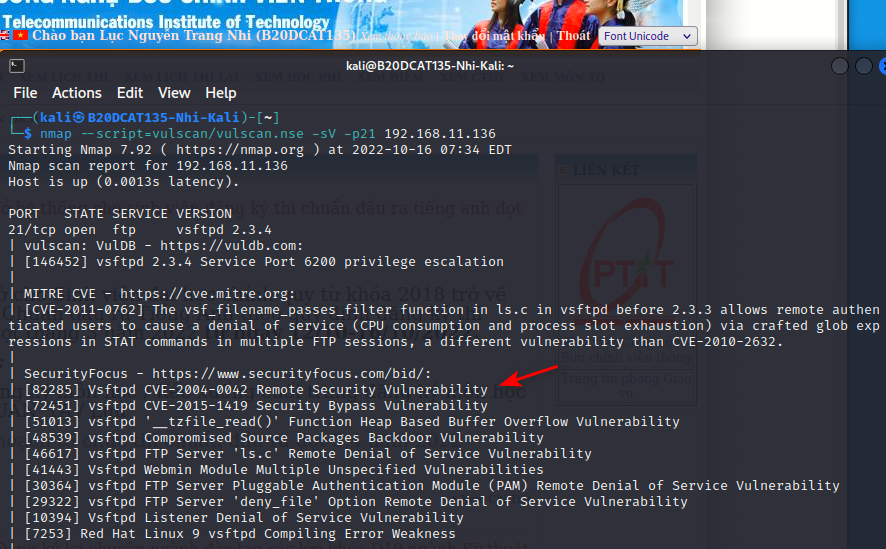


* Cài đặt CSDL vulscan

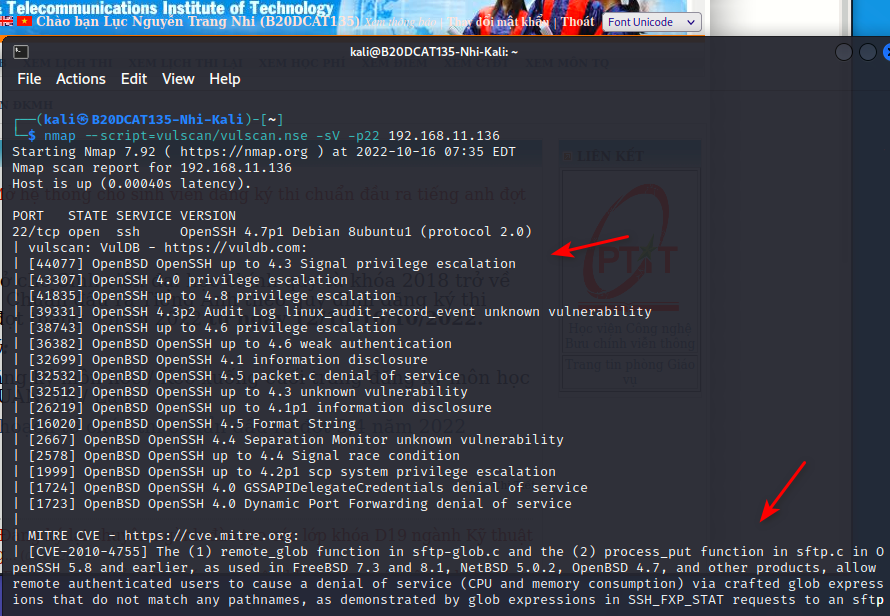


1. **Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại sử dụng NSE script với nmap**

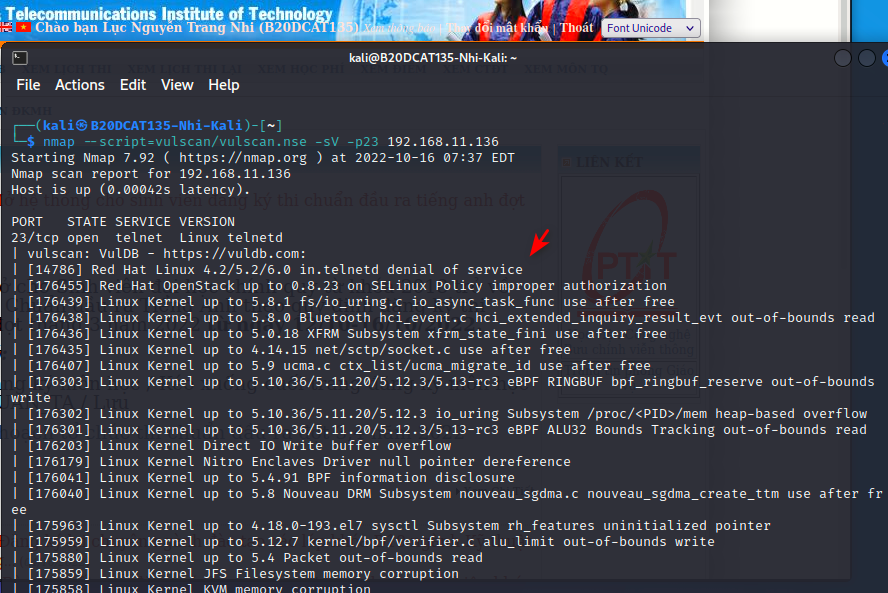
nmap --script=vulscan/vulscan.nse –sV –p21 192.168.11.136



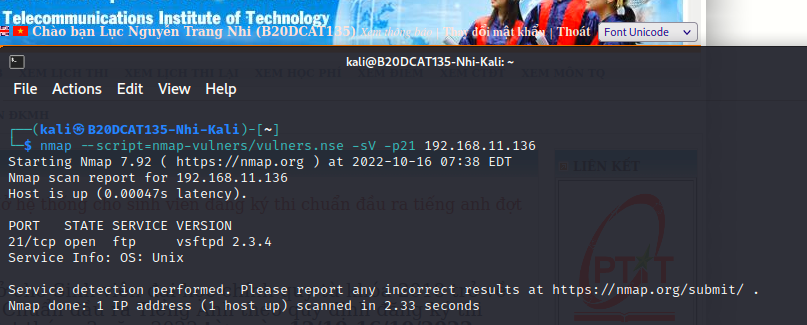
nmap --script=vulscan/vulscan.nse -sV -p22 192.168.11.136



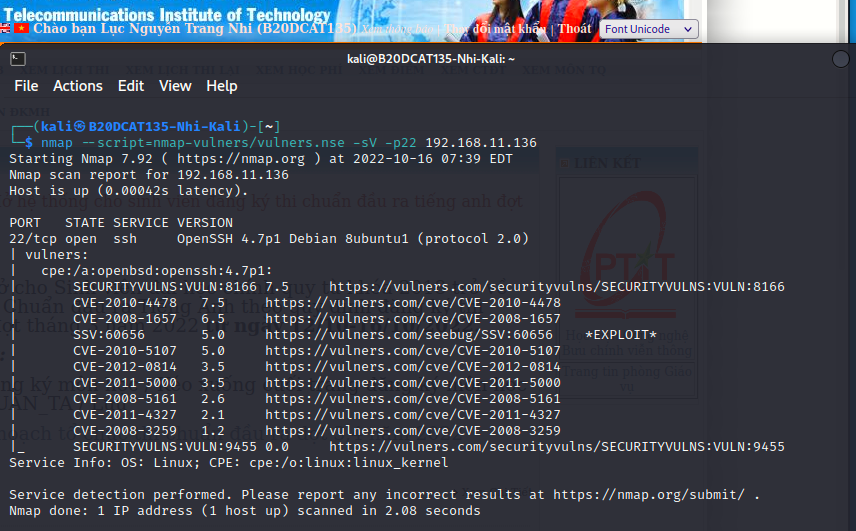
nmap --script=vulscan/vulscan.nse -sV -p23 192.168.11.136



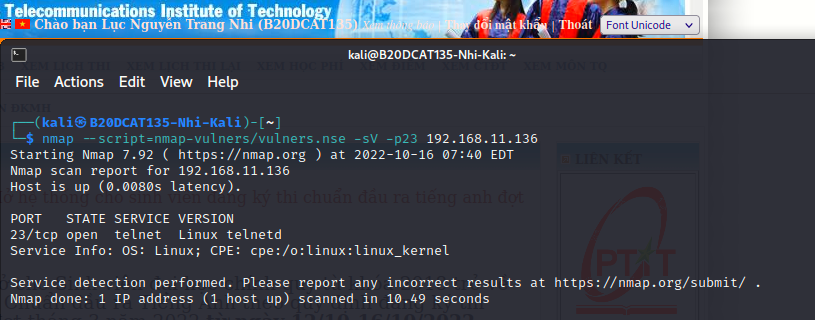
nmap --script=nmap-vulners/vulners.nse -sV -p21 192.168.11.136



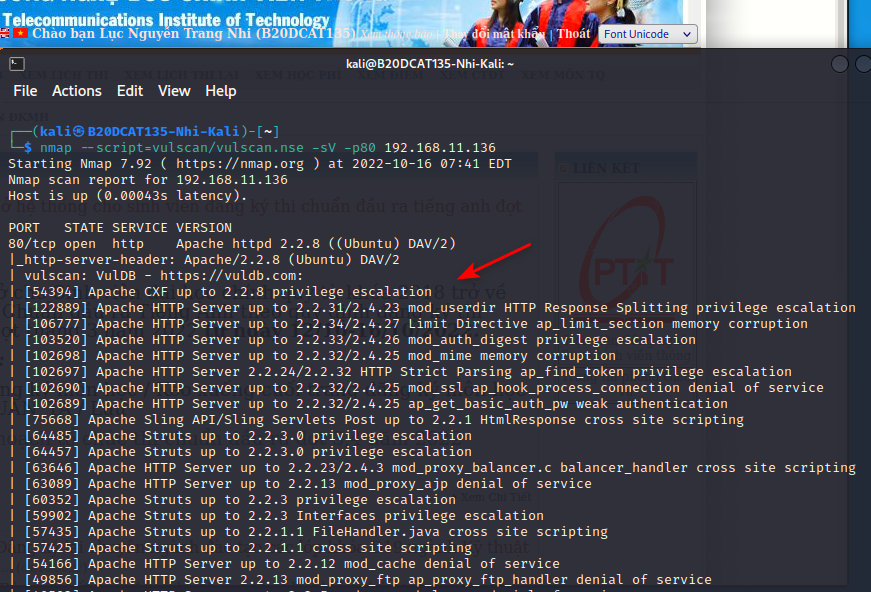
nmap --script=nmap-vulners/vulners.nse -sV -p22 192.168.11.136



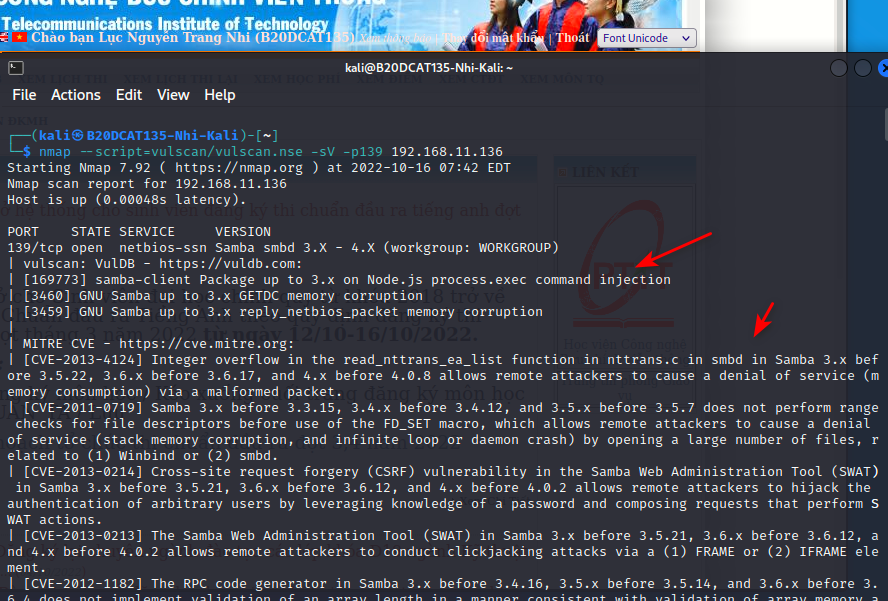
nmap --script=nmap-vulners/vulners.nse -sV -p23 192.168.11.136



nmap --script=vulscan/vulscan.nse -sV -p80 192.168.11.136



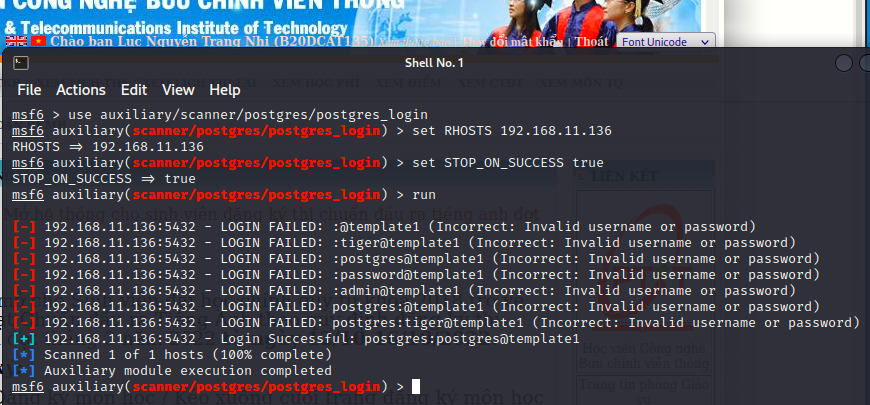
nmap --script=vulscan/vulscan.nse -sV -p139 192.168.11.136



nmap --script=vulscan/vulscan.nse -sV -p5432 192.168.11.136



1. **Khai thác lỗi đăng nhập trên PostgreSQL, cổng 5432**



1. **Khai thác lỗi trên PostgreSQL, cho phép mở shell chạy với quyền root**

