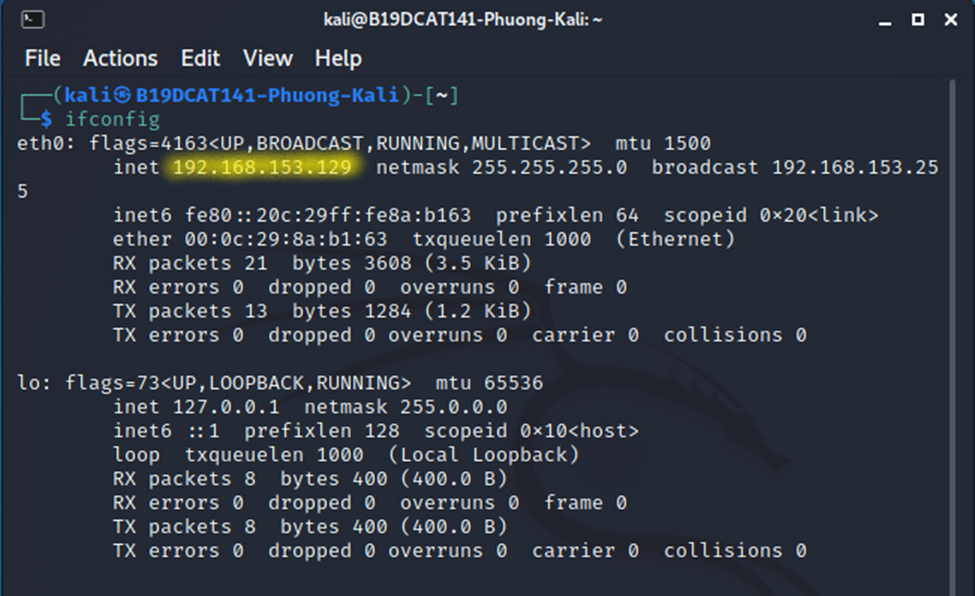
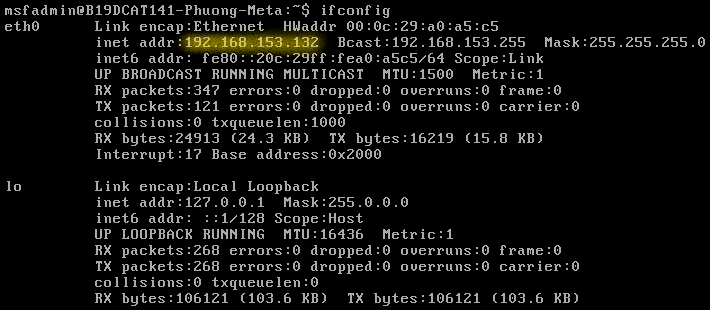
**Nguyễn Minh Phương – B19DCAT141**

**Báo cáo bài Thực hành số 3**

1. **Màn hình tìm được địa chỉ IP máy Kali**

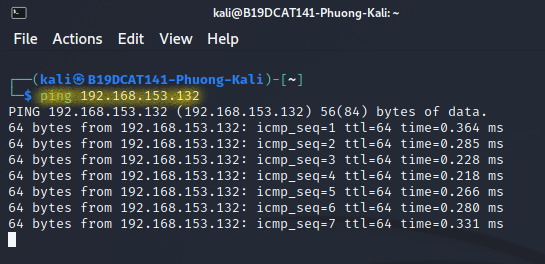


1. **Màn hình tìm được địa chỉ IP máy Metasploiatble2**

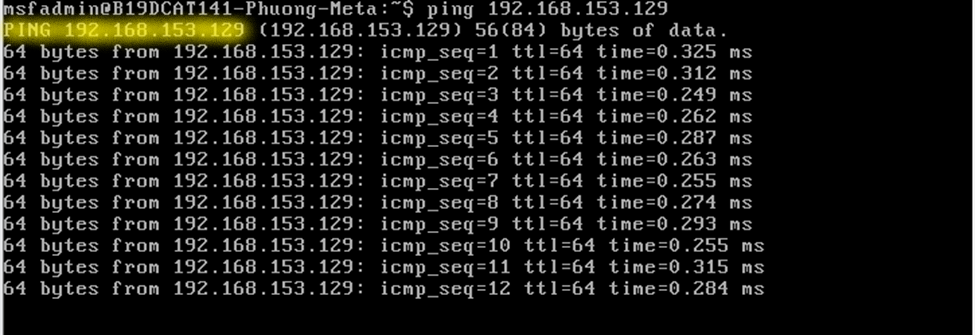
****

1. **Màn hình các máy ping nhau**

Máy Kali ping đến Metasploiatble2

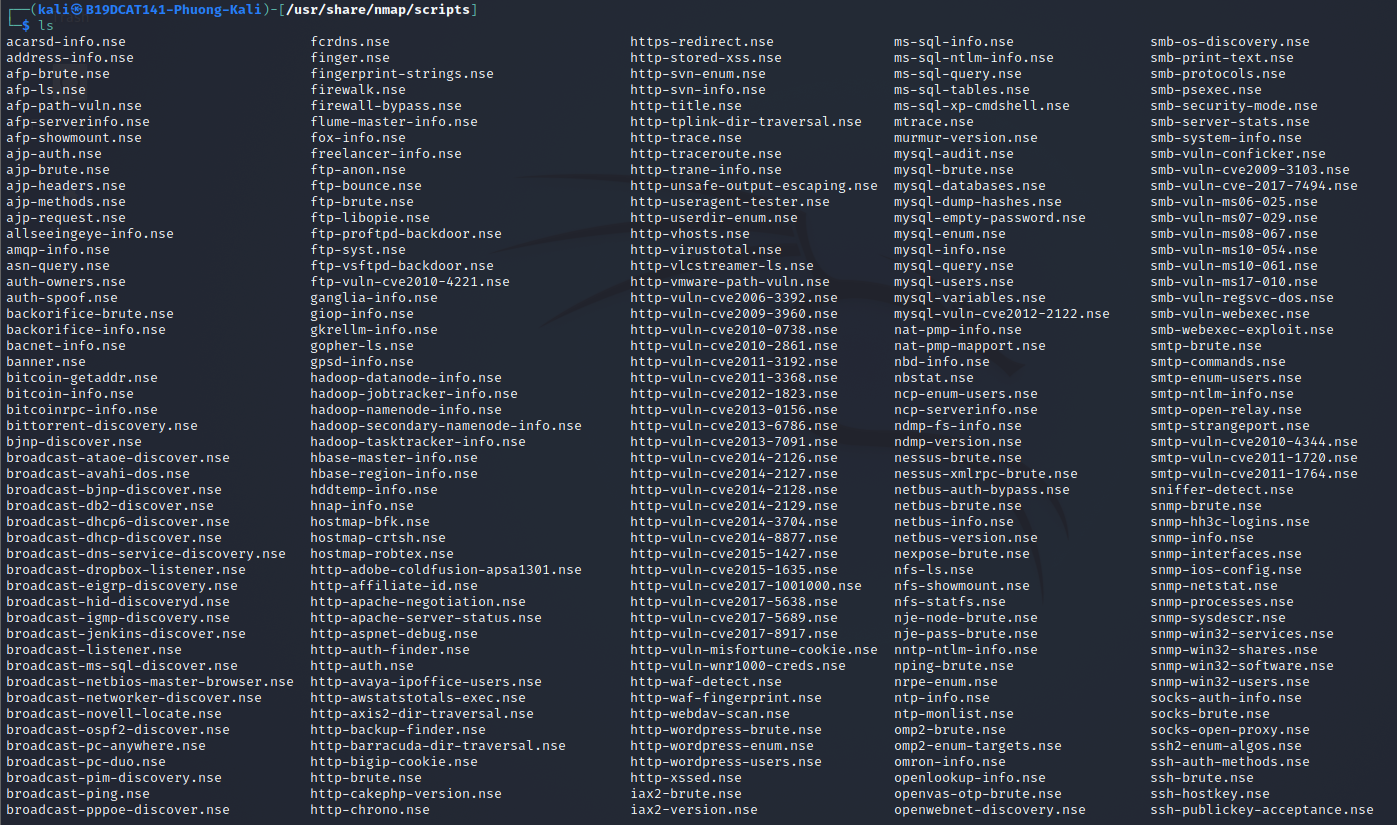
****

Máy Metasploiatble2 ping đến máy Kali

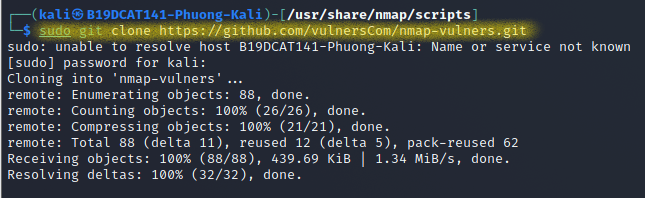


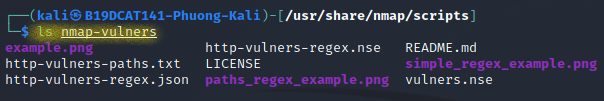
1. **Kiểm tra và cài đặt các NSE scripts cho nmap**

* Kiểm tra các NSE scripts có sẵn cho nmap:

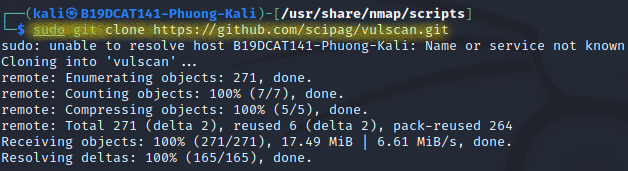
****

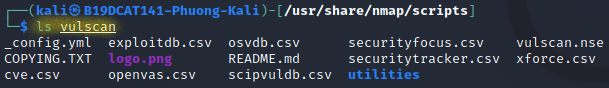
* Cài đặt CSDL nmap-vulners:





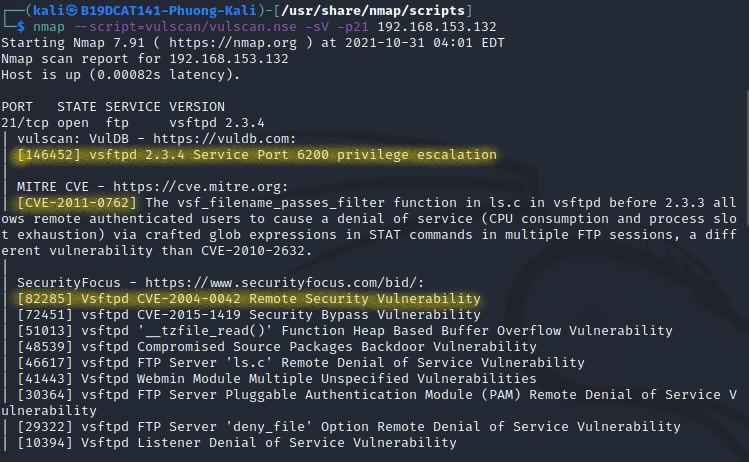
* Cài đặt CSDL Vulscan:



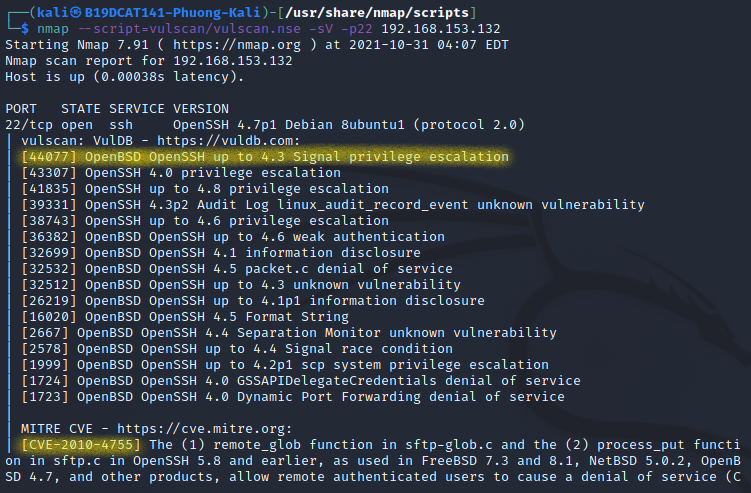


1. **Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại sử dụng NSE script với nmap**

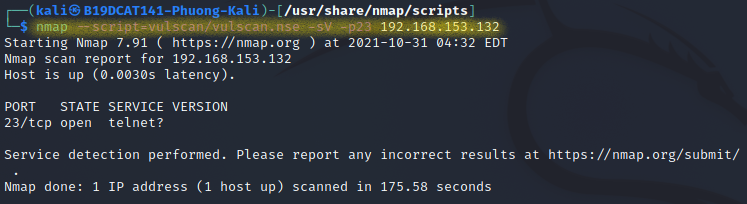
nmap --script=vulscan/vulscan.nse -sV -p21 192.168.153.132

****

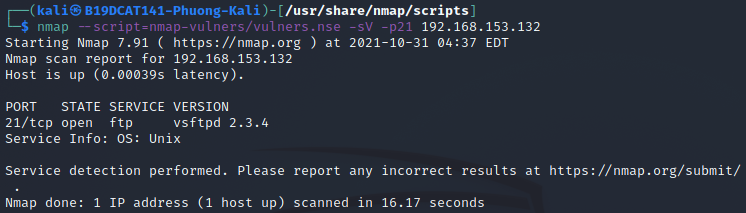
nmap --script=vulscan/vulscan.nse -sV -p22 192.168.153.132



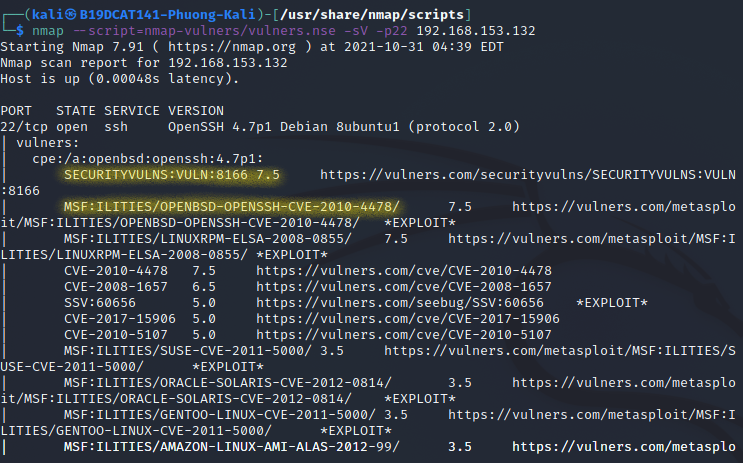
nmap --script=vulscan/vulscan.nse -sV -p23 192.168.153.132



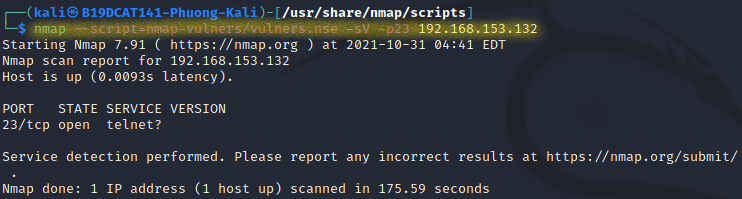
nmap --script=nmap-vulners/vulners.nse -sV -p21 192.168.153.132



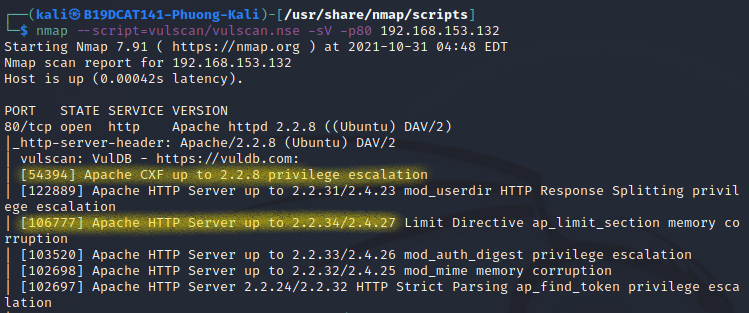
nmap --script=nmap-vulners/vulners.nse -sV -p22 192.168.153.132



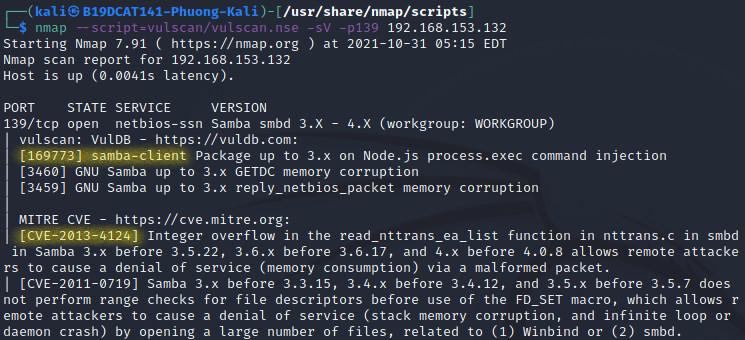
nmap --script=nmap-vulners/vulners.nse -sV -p23 192.168.153.132



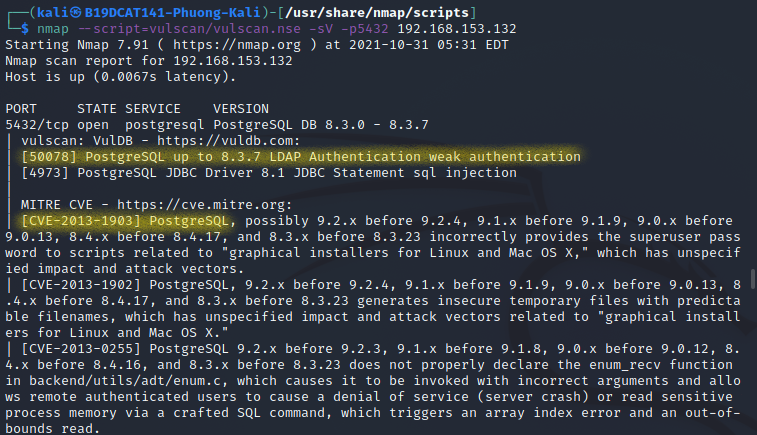
nmap --script=vulscan/vulscan.nse -sV -p80 192.168.153.132



nmap --script=vulscan/vulscan.nse -sV -p139 192.168.153.132

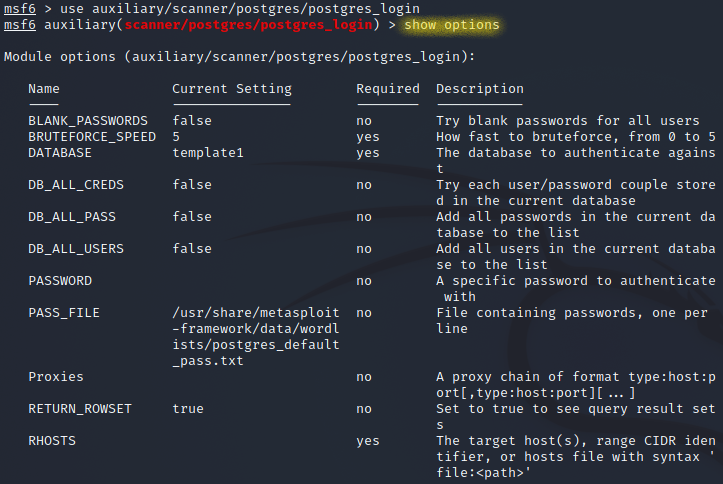


nmap --script=vulscan/vulscan.nse -sV -p5432 192.168.153.132

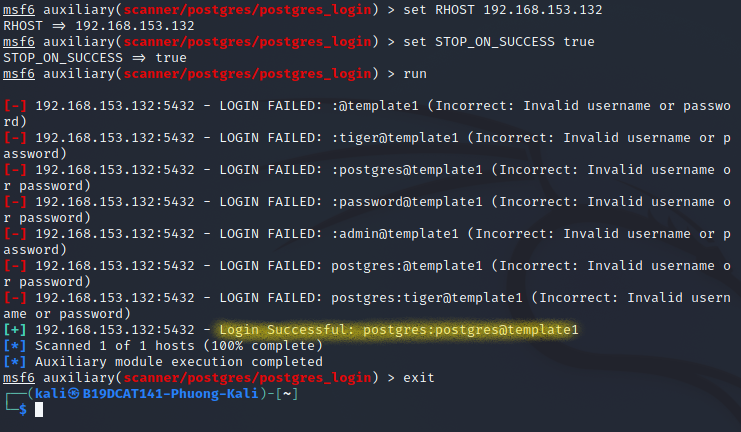


1. **Khai thác lỗi đăng nhập trên PostgreSQL, cổng 5432**

* Những modulo tấn công đang sử dụng:

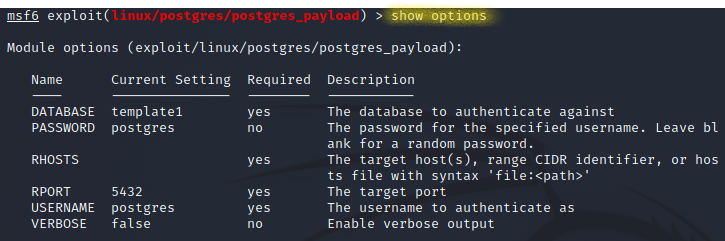


* Thực hiện tấn công:

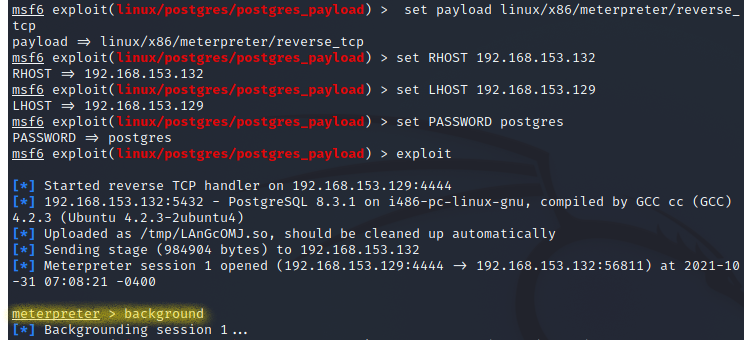
****

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

* Một số modulo tấn công đang sử dụng:



* Tạo được một phiên kết nối đến CSDL”



* Các modulo tấn công đang sử dụng:

