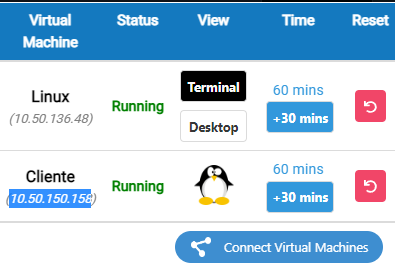
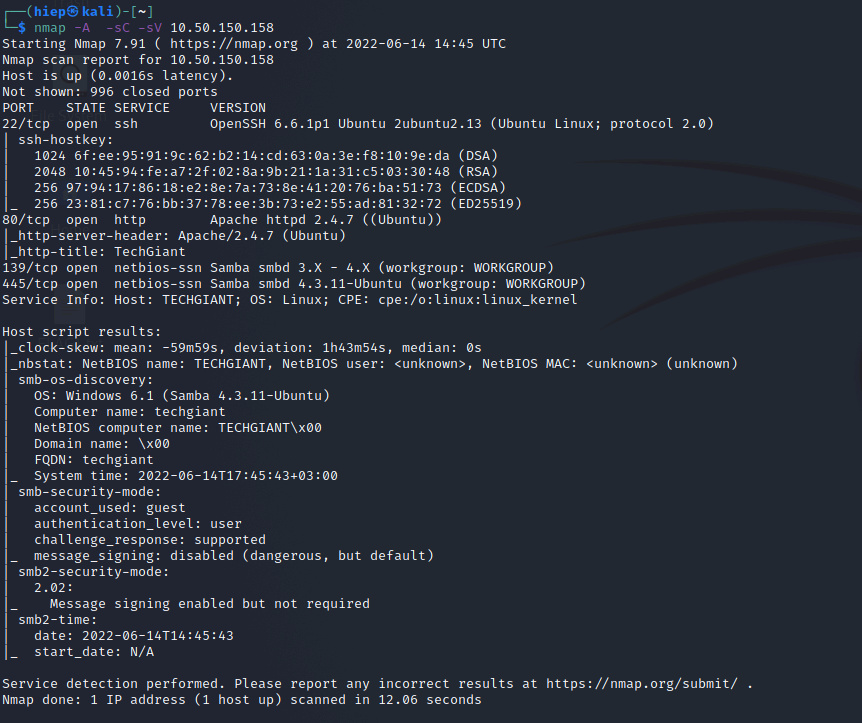
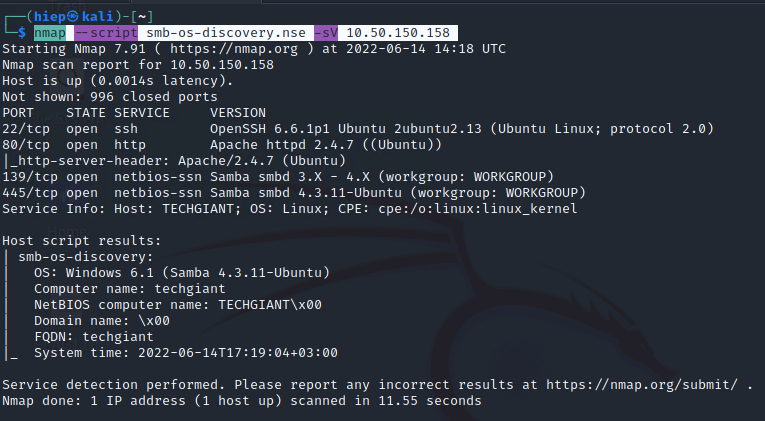
SMB ENUM



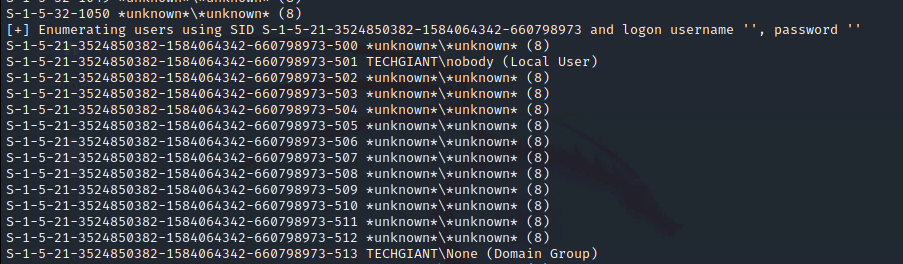
SCAN SERVICE:

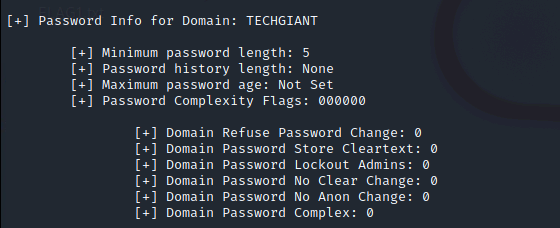
SCAN HDH CỦA MÁY CLIENT:

nmap --script smb-os-discovery.nse -sV 10.50.150.158

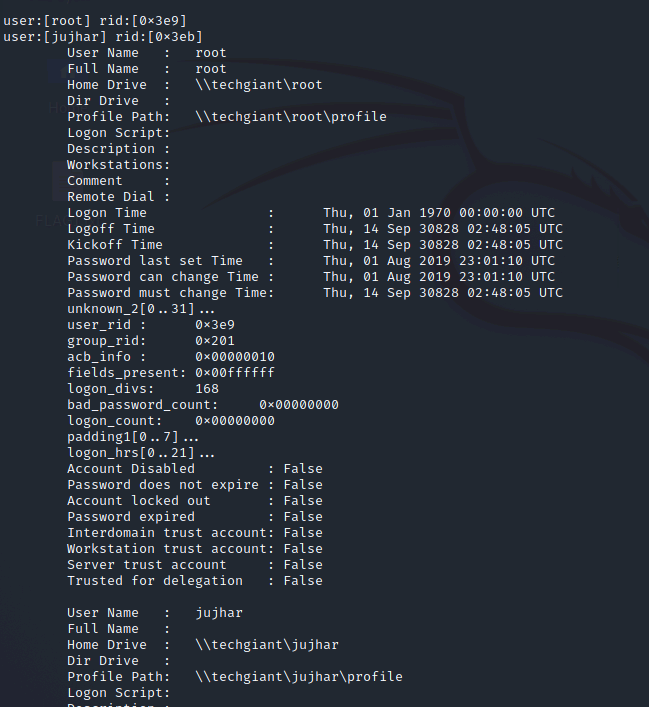


Enum user thông qua rid: enum4linux -r 10.50.150.158



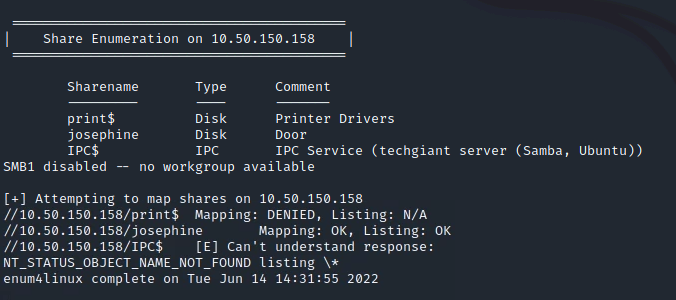
get password policy information: enum4linux -P 10.50.150.158 

Get user list and detail: enum4linux -U -d 10.50.150.158



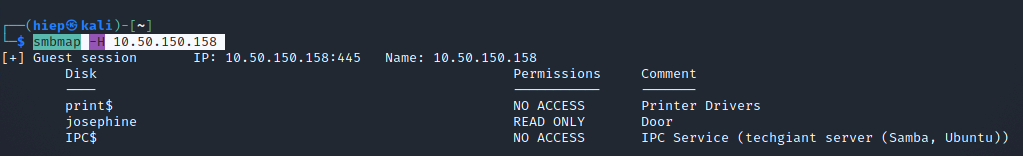
Từ cái này thấy được tài khoản 0 bị khóa, pass 0 hết hạn, có thể bruteforce được

Get share list: enum4linux -r 10.50.150.158



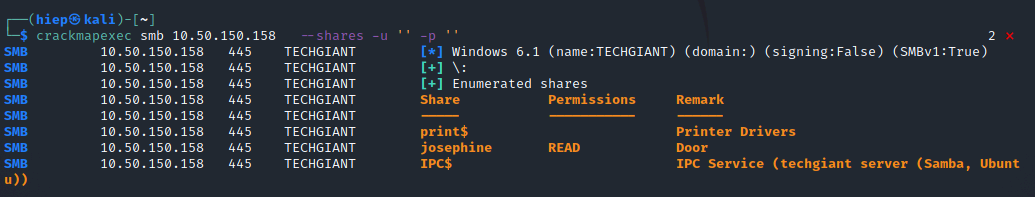
Ở đây share Josephine đáng chú ý. Có thể có khả năng truy cập 0 cần mk

Dùng smbmap để xem quyền : smbmap -H 10.50.150.158

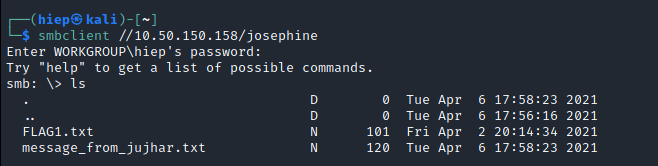


Giờ chúng ta có thể xem được quyền smb. Có thể crack acc smb bằng:

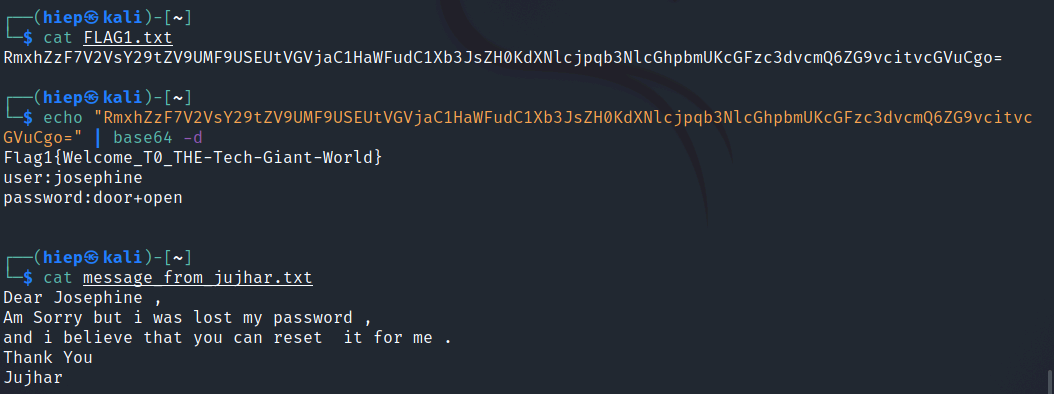
crackmapexec smb 10.50.150.158 --shares -u ‘’ -p ‘’



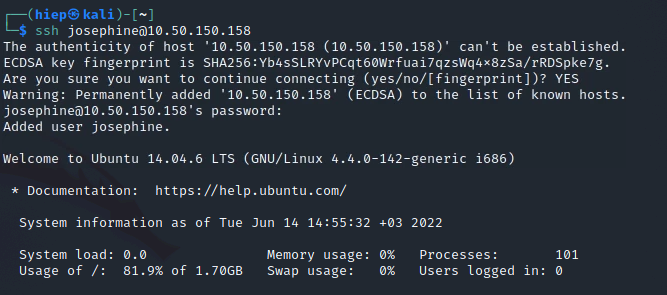
Truy cập vào thư mục được share: smbclient //10.50.150.158/osephine



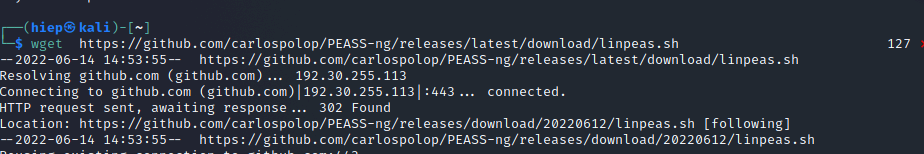
Sau đó get file về



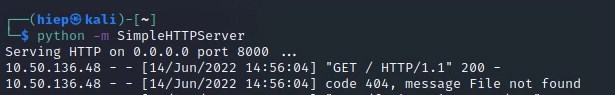
Tài khoản này có thể là tk ssh:



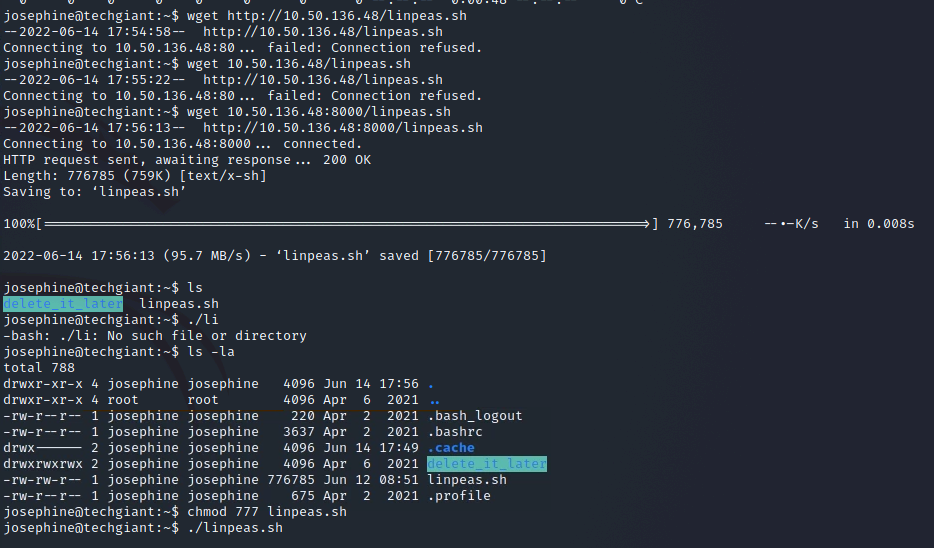
Sau đó, tải linpeas về máy tấn công



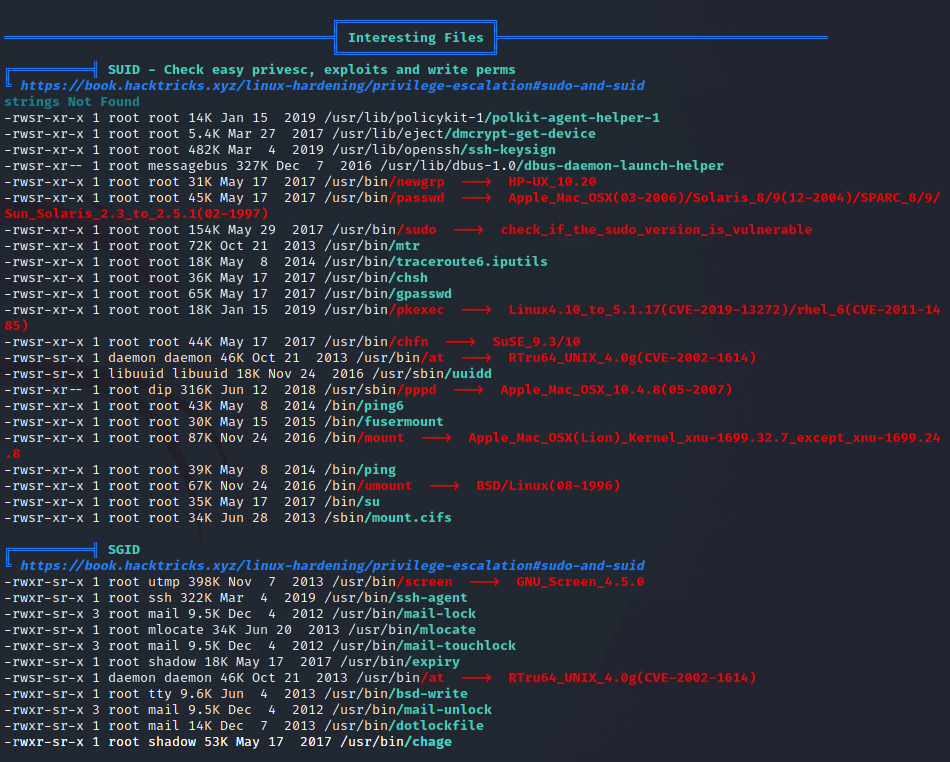
Rồi tạo web server: python -m SimpleHTTPServer



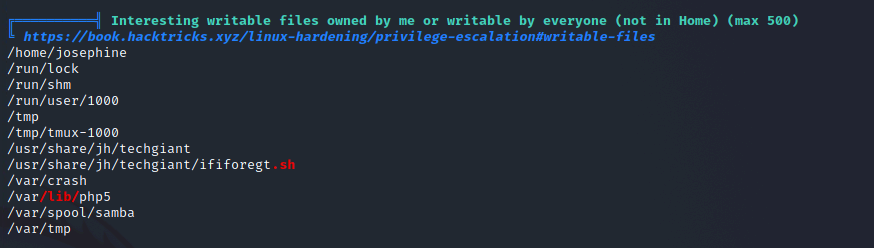
Bên máy ssh thì rồi wget tải linpeas từ máy tấn công về rồi chạy.



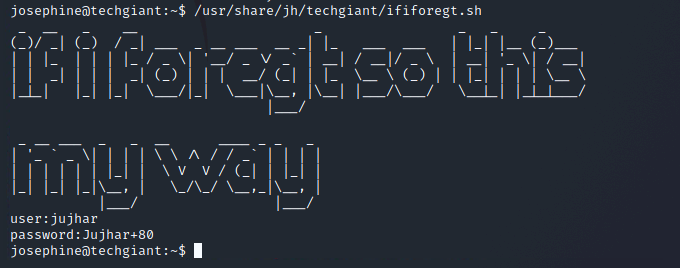
Tìm thấy được khá nhiều thứ có thể khai thác



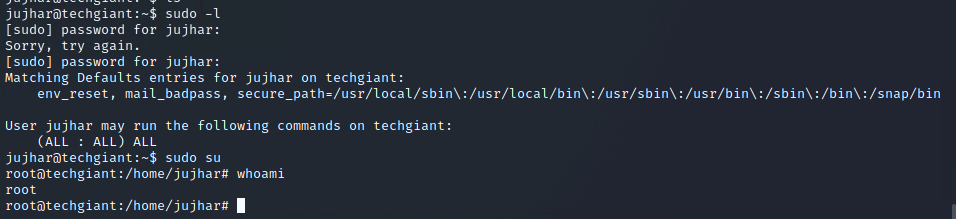
Bài này dễ nên sẽ dùng cách đơn giản hơn



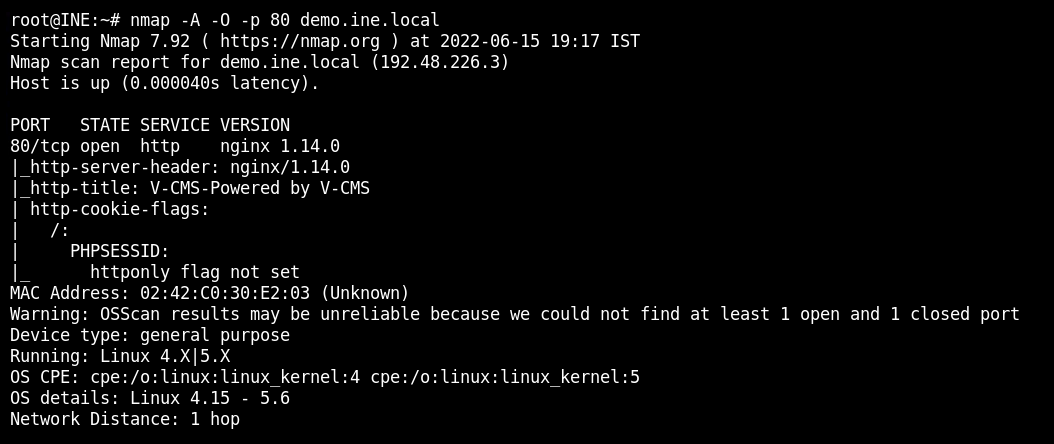
Có tài khoản root



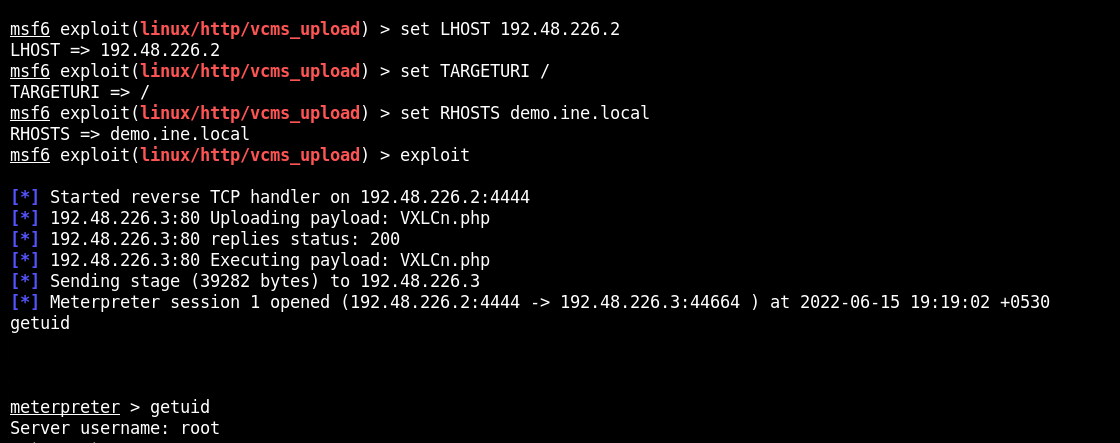
Lên quyền root



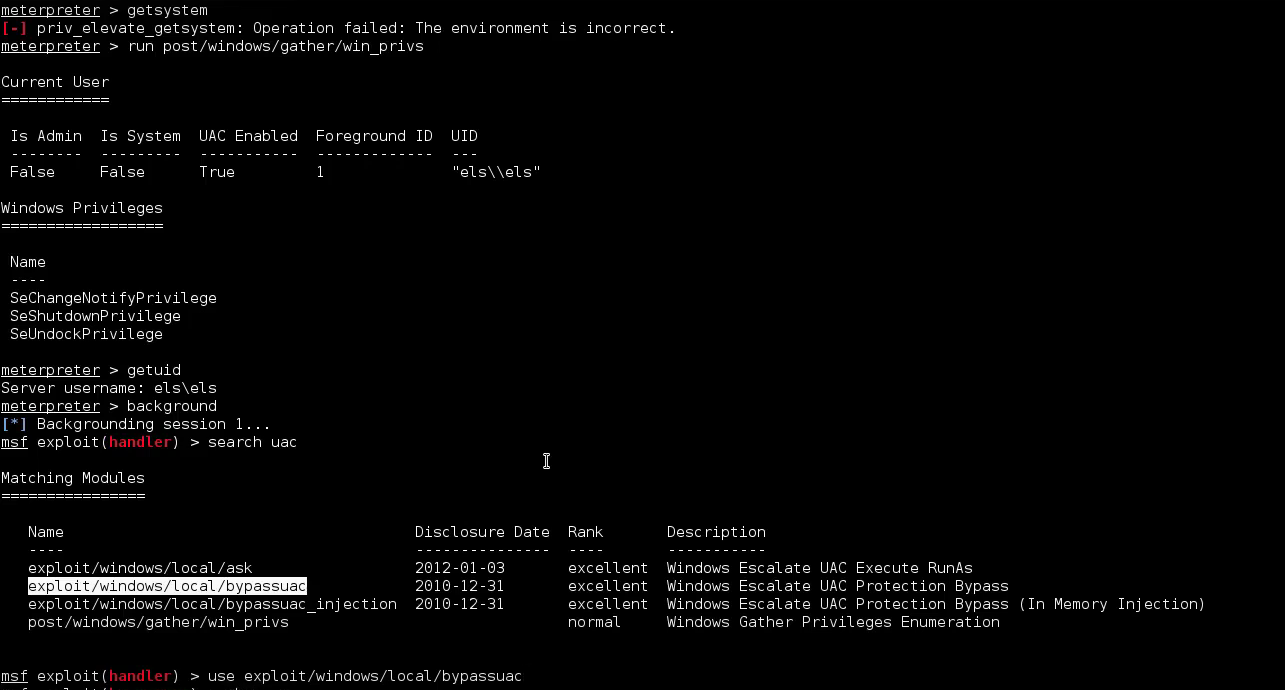
PIVOTING

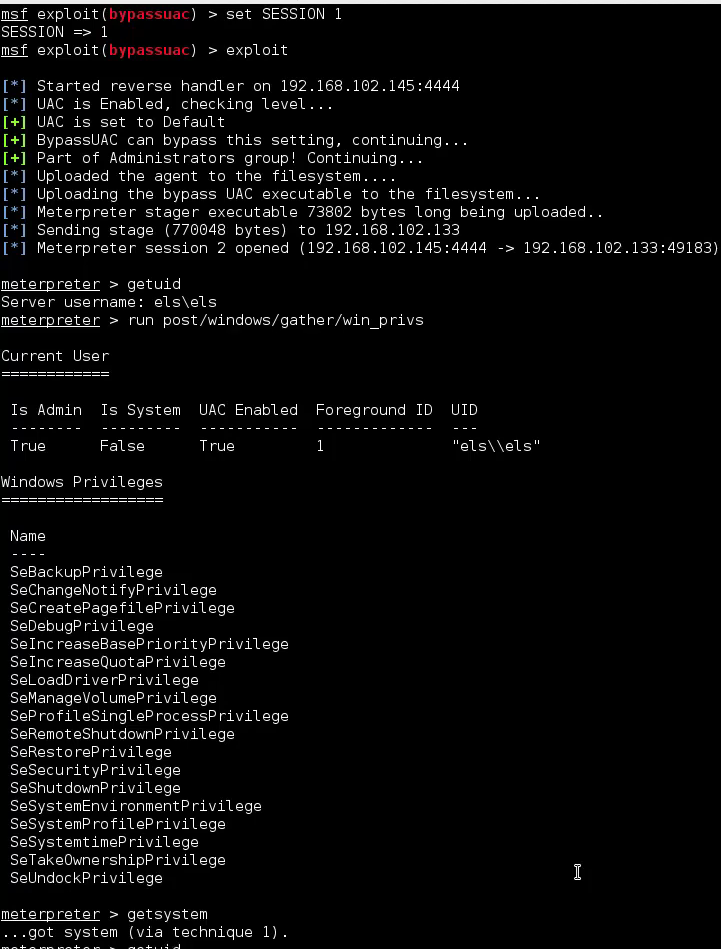


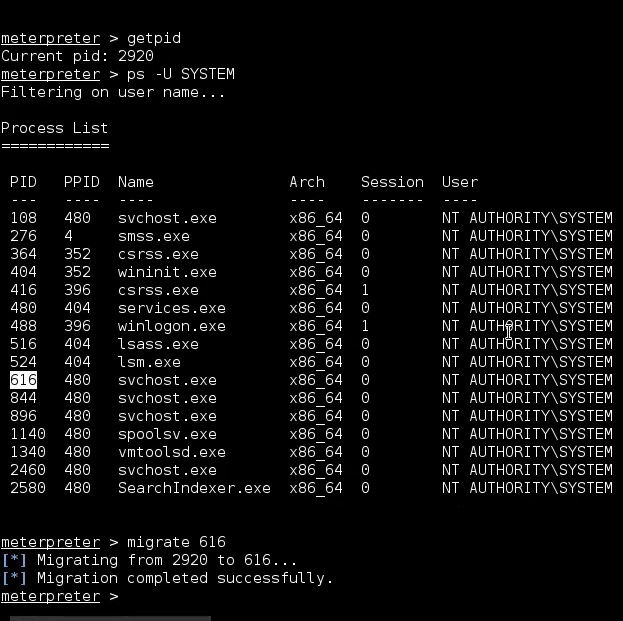
Sau khi biết có vcms thì search trên msf



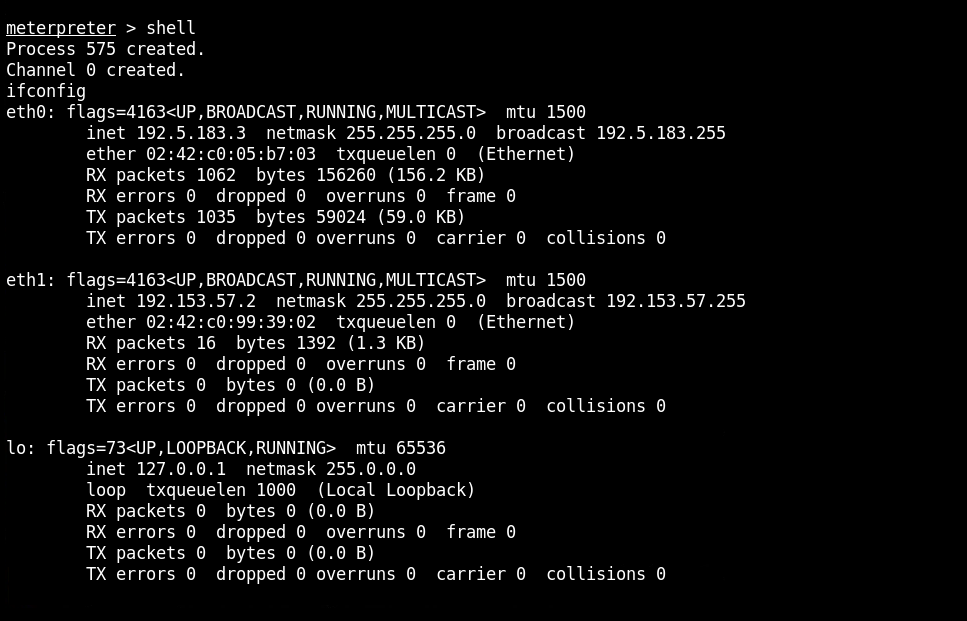
Leo thang nếu chiếm quyền thấp



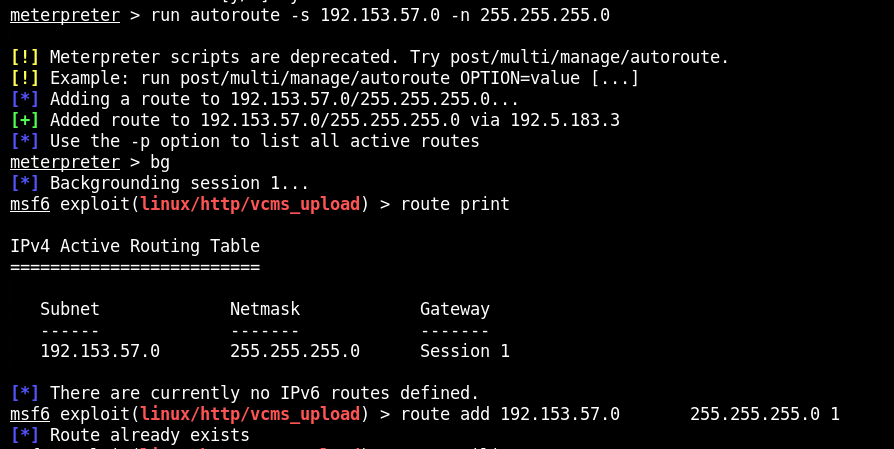




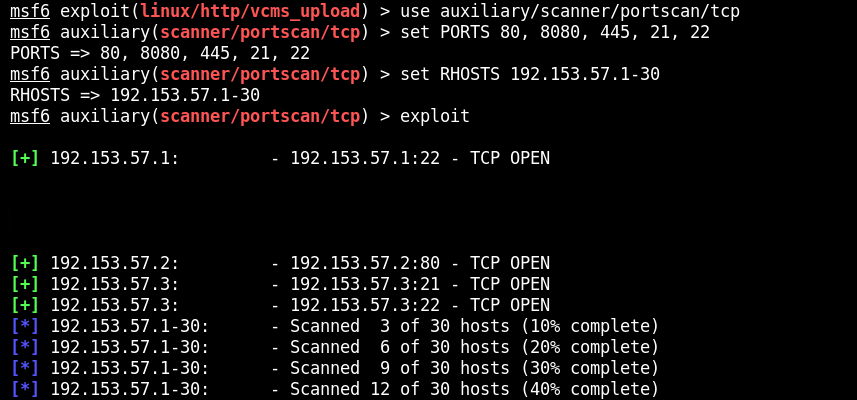
Xem ip



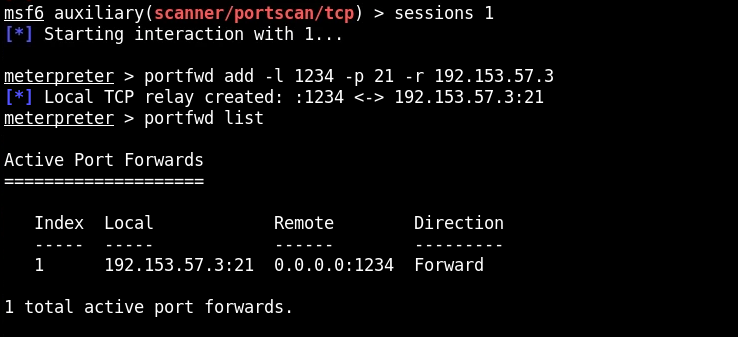
Autoroute



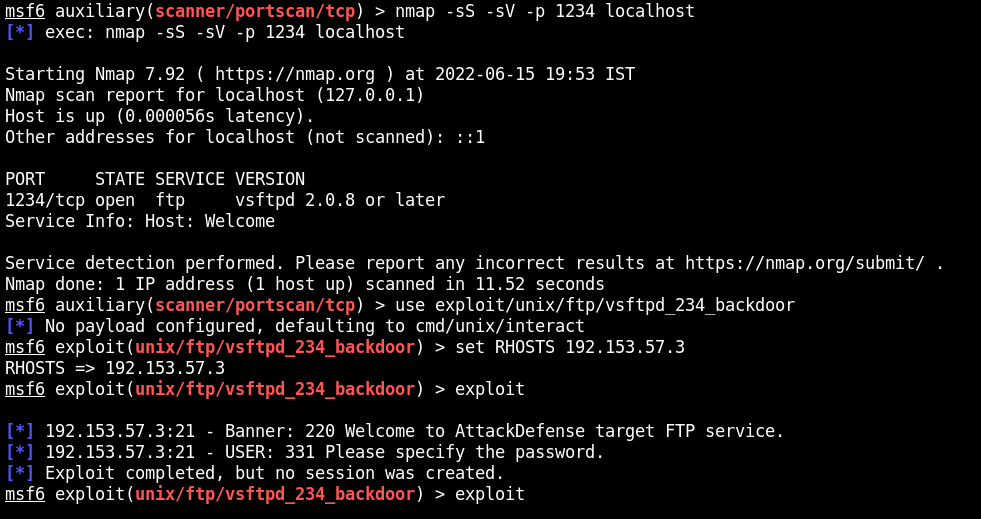
Tiến hành scan các port trên network mới



Tạo portfw



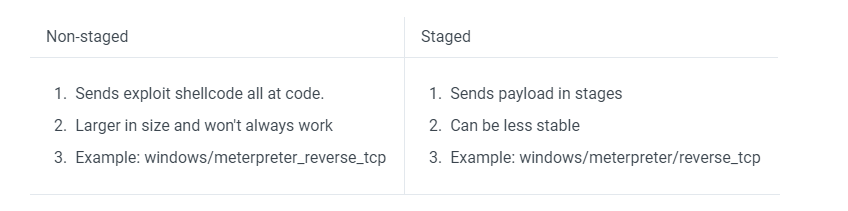
Scan service vào khai khác



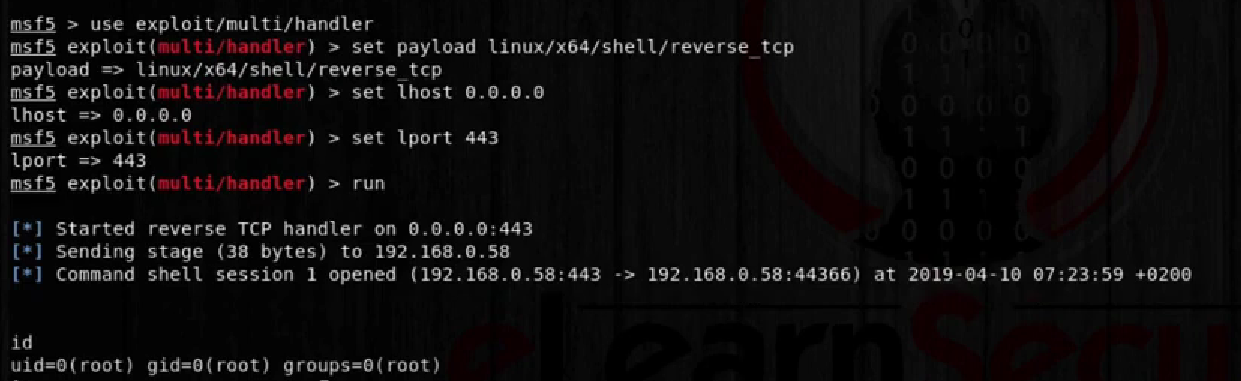
TẠO SHELL VỚI MSFVENOM



VỀ REVERSE\_TCP LÀ STAGED PAYLOAD. VÌ VẬY CẦN THÊM 1 LISTENER RIÊNG. Tham khảo hình dưới



Sau đó, chạy file backdoor vừa tạo để lấy reverse shell



Stageless như hình dưới thì netcat có thể bắt được. còn staged thì nc không bắt được.

