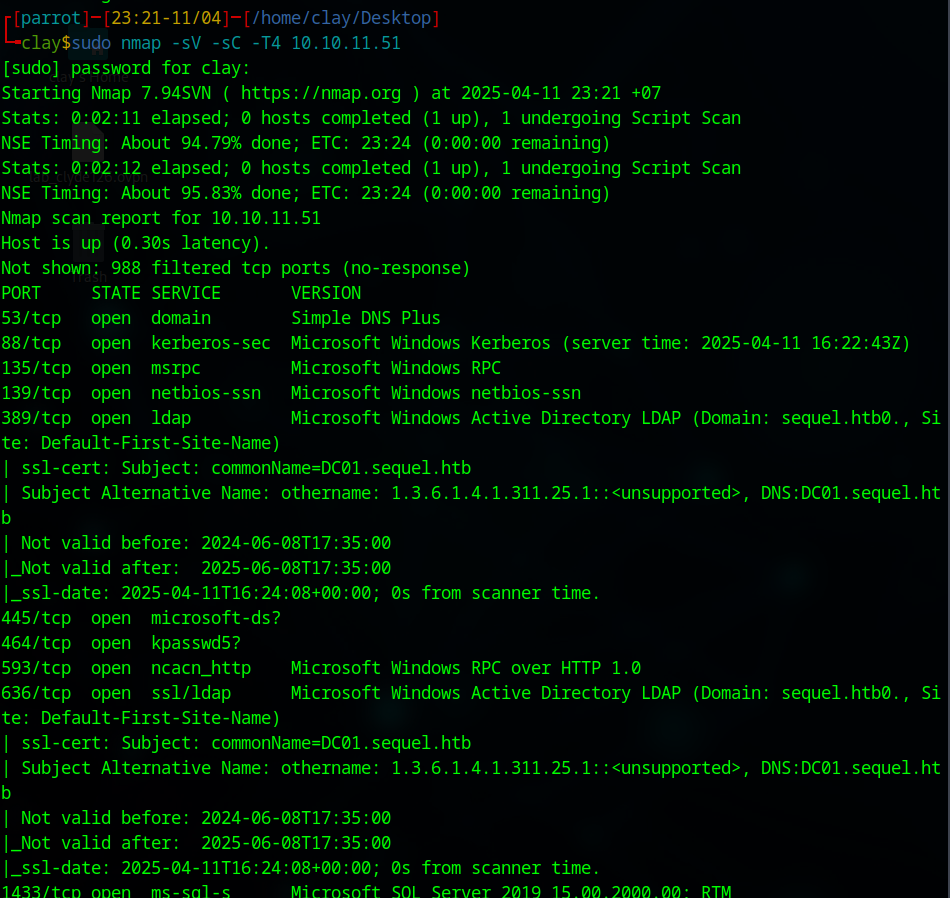
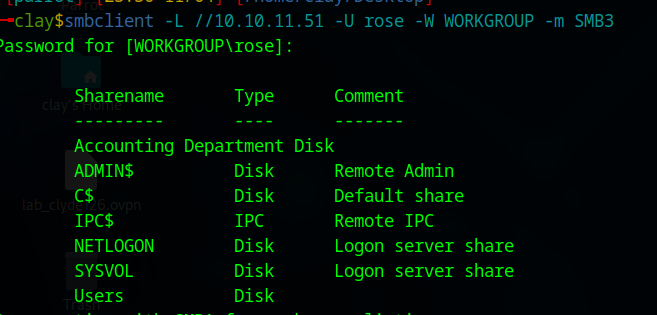
B1 Scanning



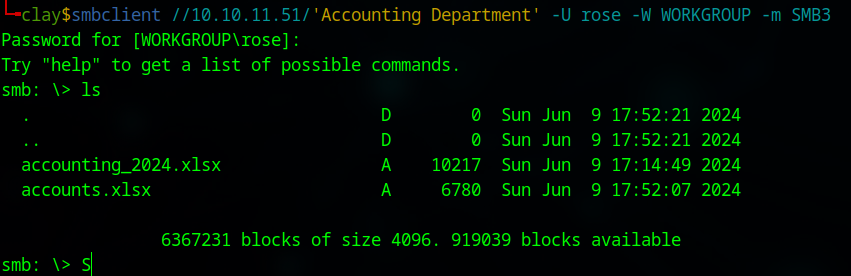
Ta có thể thấy đây là 1 AD khi mở cổng 88 cho keberos và cả cổng 1433 cho sql-server

Ta được cho thông tin như sau: rose / KxEPkKe6R8su

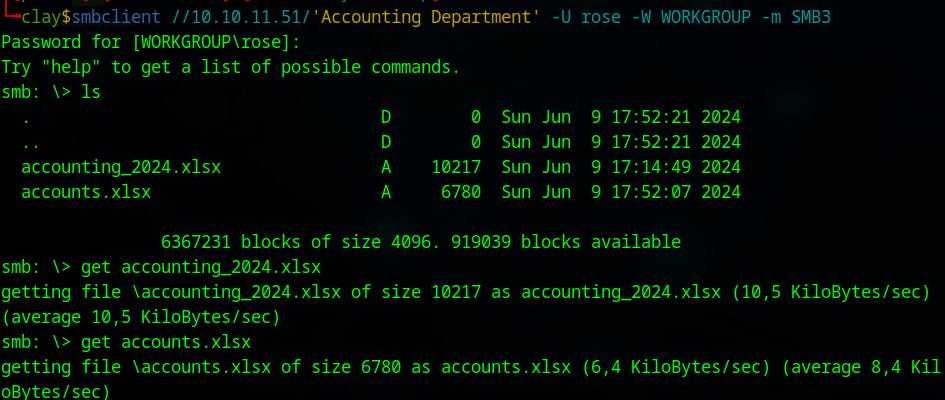
Sử dụng smbclient



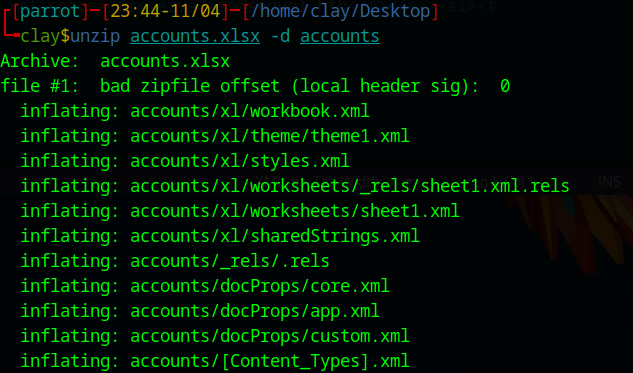
Có 1 thư mục accounting hay ho để ta tới thử xem



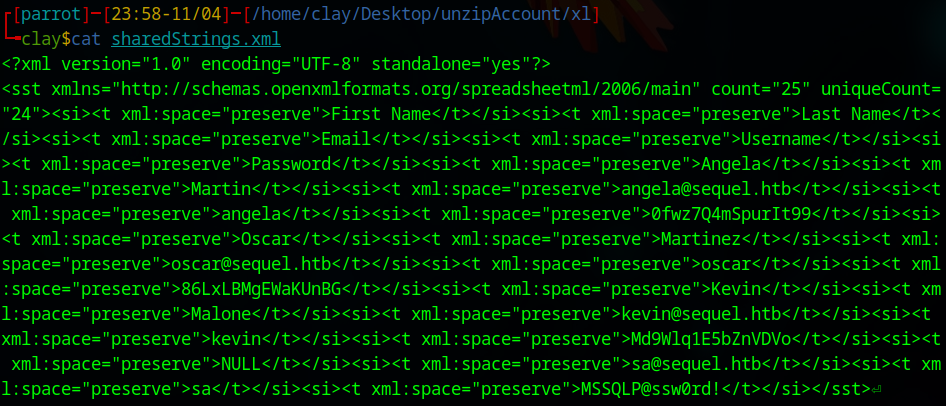
Ta lấy 2 file đó về



Ta unzip file accounts



Ta xem thông tin của 1 file xml trong đó có nói về password và email

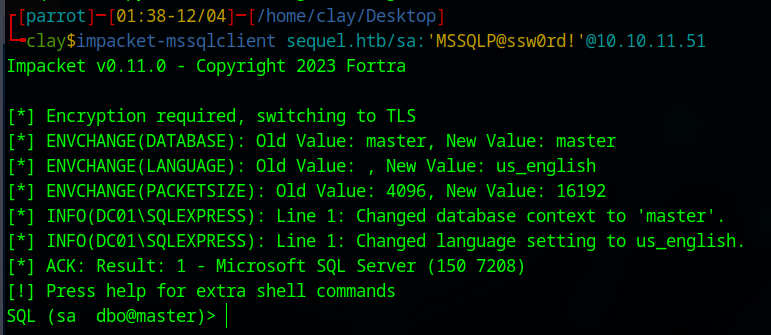


Nhờ chatgpt đổi qua dạng bảng cho dễ đọc



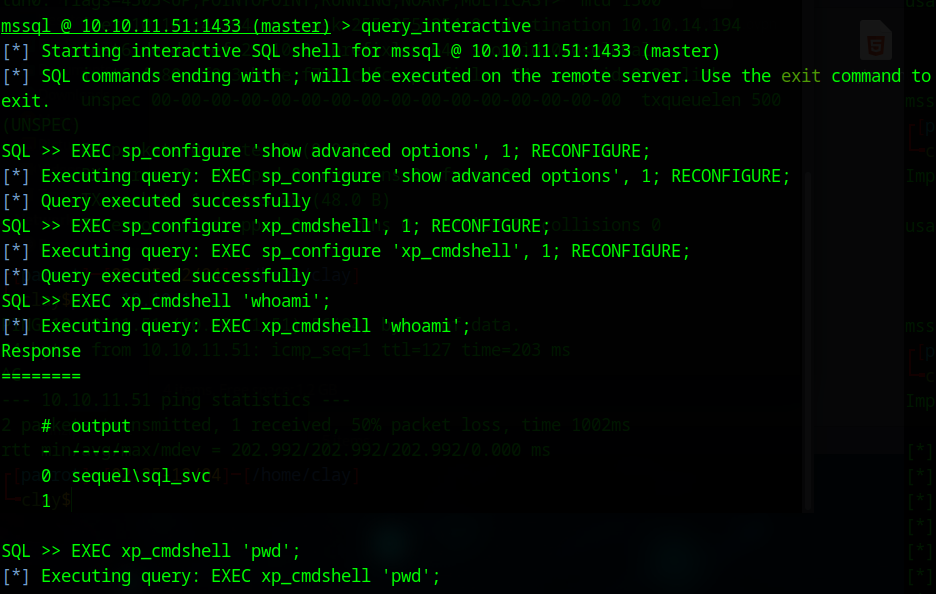
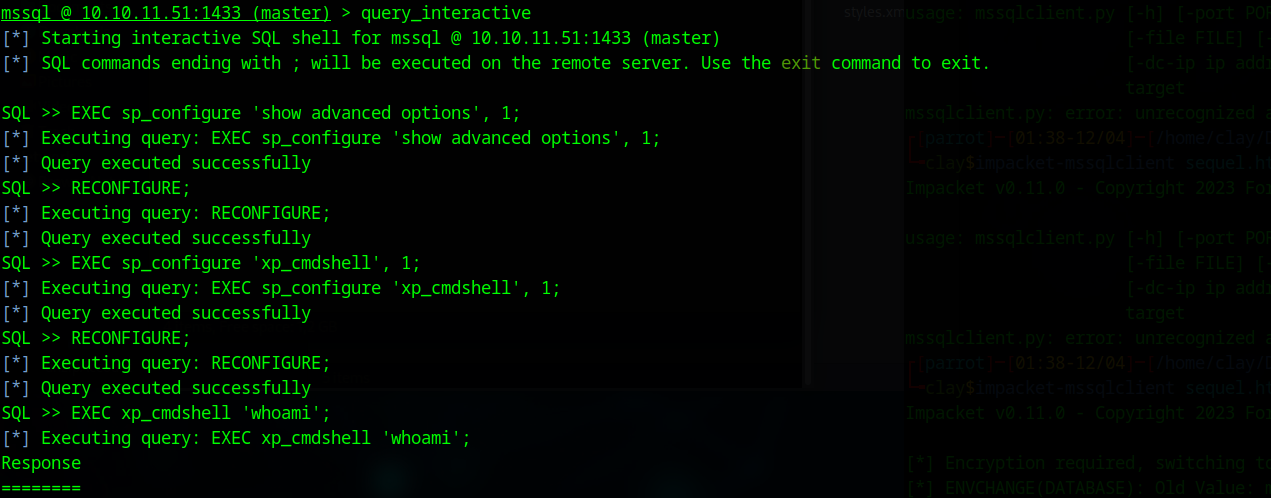
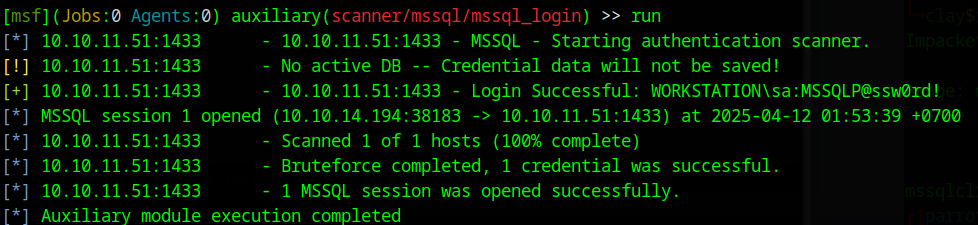
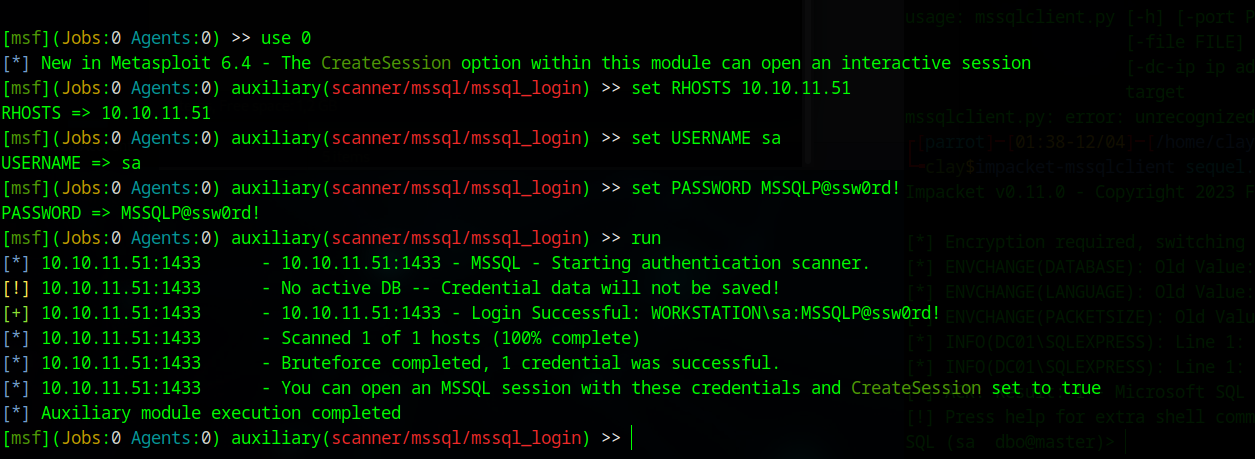
Ta thấy ở cuối cùng có thông tin đây là mssql

C1 dùng msqclient



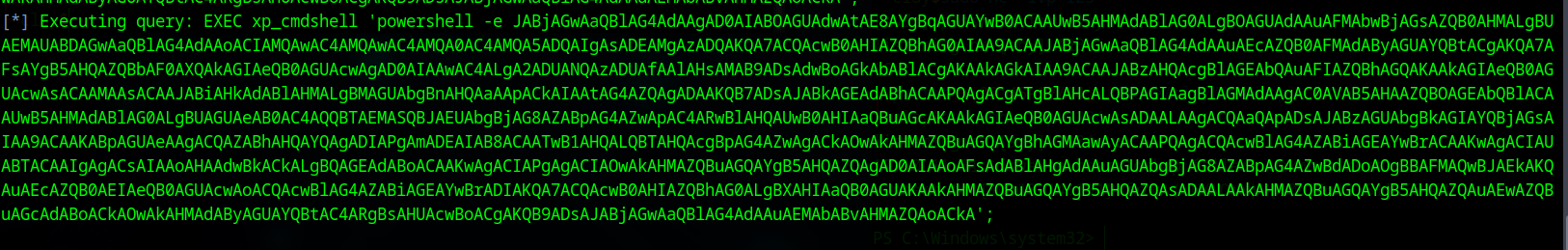
Sử dụng thông tin đăng nhập đó ta có thể dùng mssqlclient trong impacket để tấn công vào

C2: Có thể sử dụng metasploit để tấn công

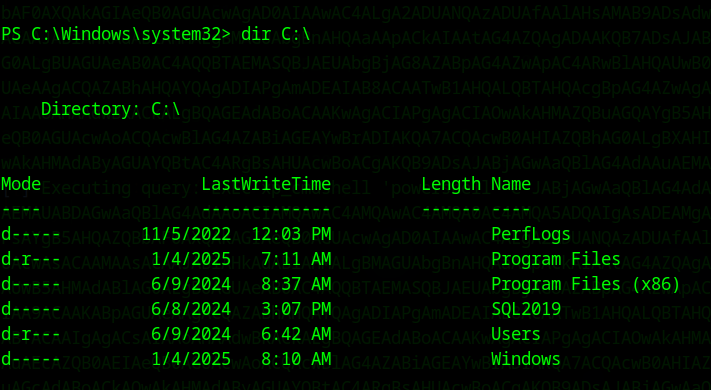
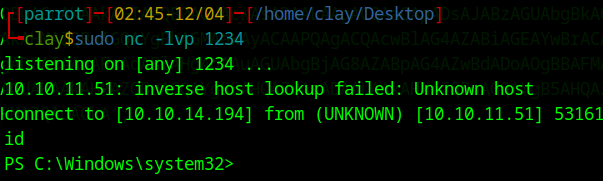


Ta bật chế độ xp\_cmdshell lên để có thể tương tác với shell

Ta tạo 1 payload reverse\_shell [tại đây](https://www.revshells.com/) và dùng xp\_cmdshell để thực thi



Có kết nối trả về



Có 1 folder sql 2019 ta truy cập sâu hơn vào file configuration.INI thì sẽ thấy



Có thông tin sqlsvaccount và mk

PS C:\SQL2019\ExpressAdv\_ENU> type sql-Configuration.INI

[OPTIONS]

ACTION="Install"

QUIET="True"

FEATURES=SQL

INSTANCENAME="SQLEXPRESS"

INSTANCEID="SQLEXPRESS"

RSSVCACCOUNT="NT Service\ReportServer$SQLEXPRESS"

AGTSVCACCOUNT="NT AUTHORITY\NETWORK SERVICE"

AGTSVCSTARTUPTYPE="Manual"

COMMFABRICPORT="0"

COMMFABRICNETWORKLEVEL=""0"

COMMFABRICENCRYPTION="0"

MATRIXCMBRICKCOMMPORT="0"

SQLSVCSTARTUPTYPE="Automatic"

FILESTREAMLEVEL="0"

ENABLERANU="False"

SQLCOLLATION="SQL\_Latin1\_General\_CP1\_CI\_AS"

SQLSVCACCOUNT="SEQUEL\sql\_svc"

SQLSVCPASSWORD="WqSZAF6CysDQbGb3"

SQLSYSADMINACCOUNTS="SEQUEL\Administrator"

SECURITYMODE="SQL"

SAPWD="MSSQLP@ssw0rd!"

ADDCURRENTUSERASSQLADMIN="False"

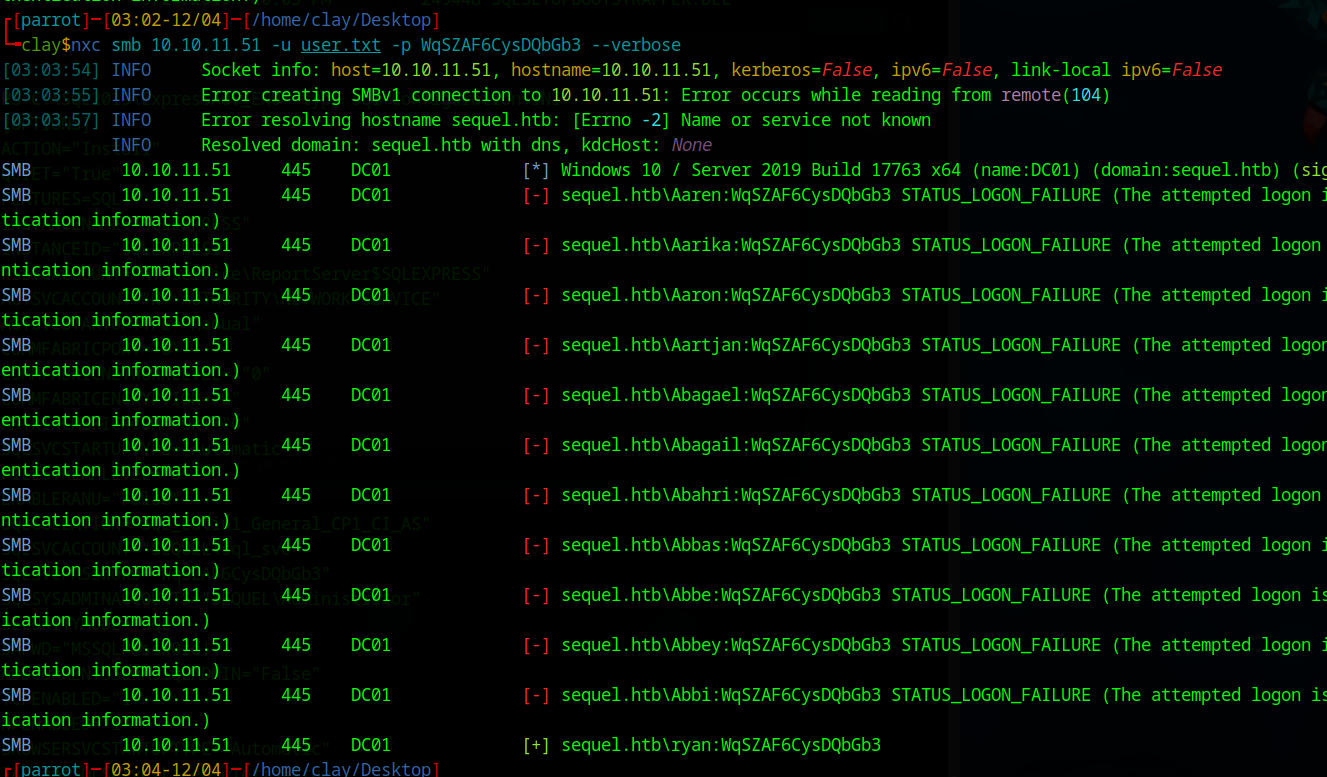
TCPENABLED="1"

NPENABLED="1"

BROWSERSVCSTARTUPTYPE="Automatic"

IAcceptSQLServerLicenseTerms=True

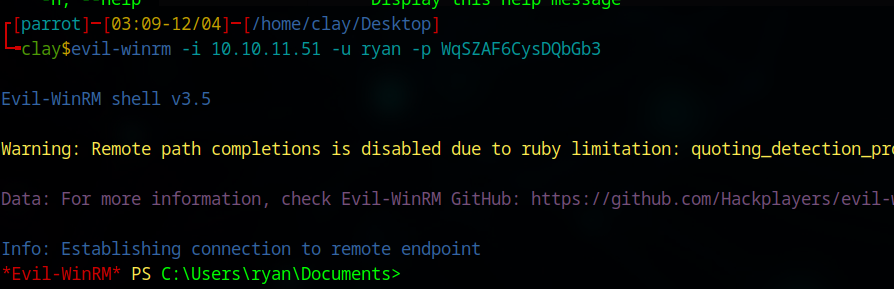
Từ thông tin mật khẩu đó ta dùng password spraying để tìm tk



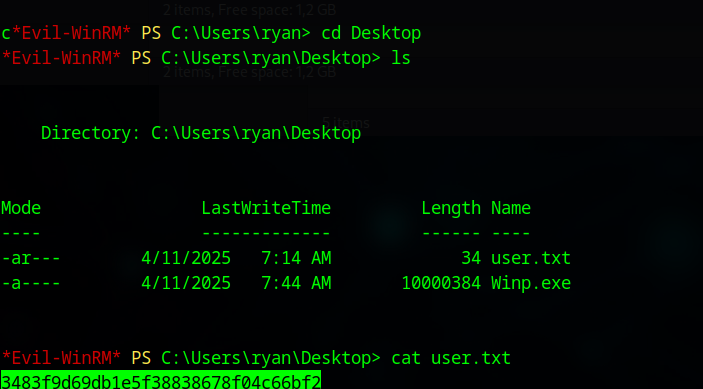
Ta dùng công cụ nxc để thực hiện tấn công

-> tìm ra tk ryan mk: WqSZAF6CysDQbGb3

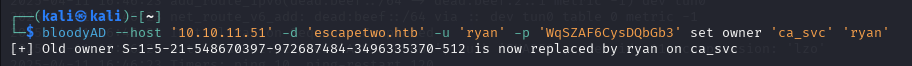
Ta dùng công cụ evil-winrm để kết nối tới máy mục tiêu



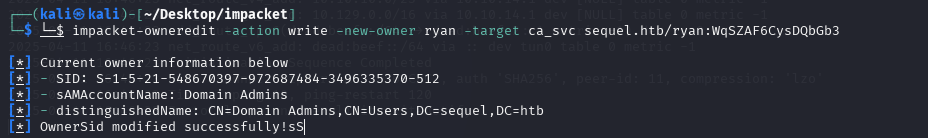
Lấy được flag



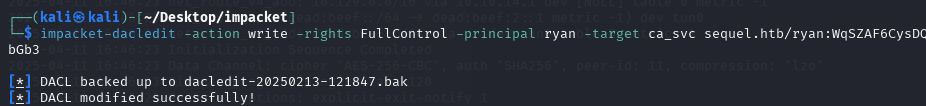
B4: leo thang đặc quyền



Sử dụng impacket-owner edit để đổi quyền sở hữu của tk ca\_svc cho ryan.

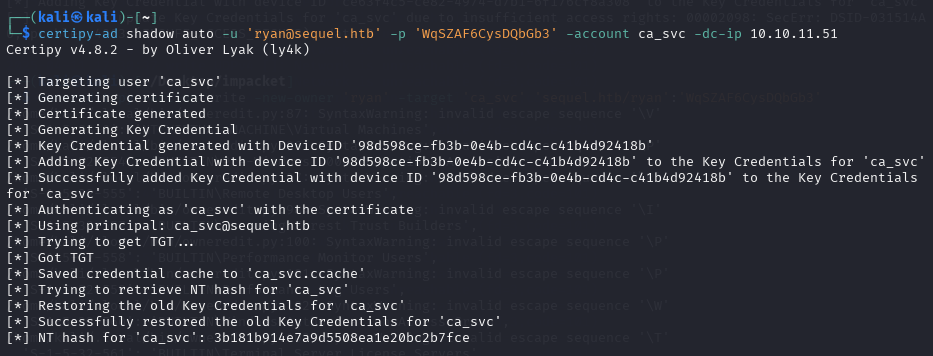


Dùng công cụ dacledit để cấp full quyền

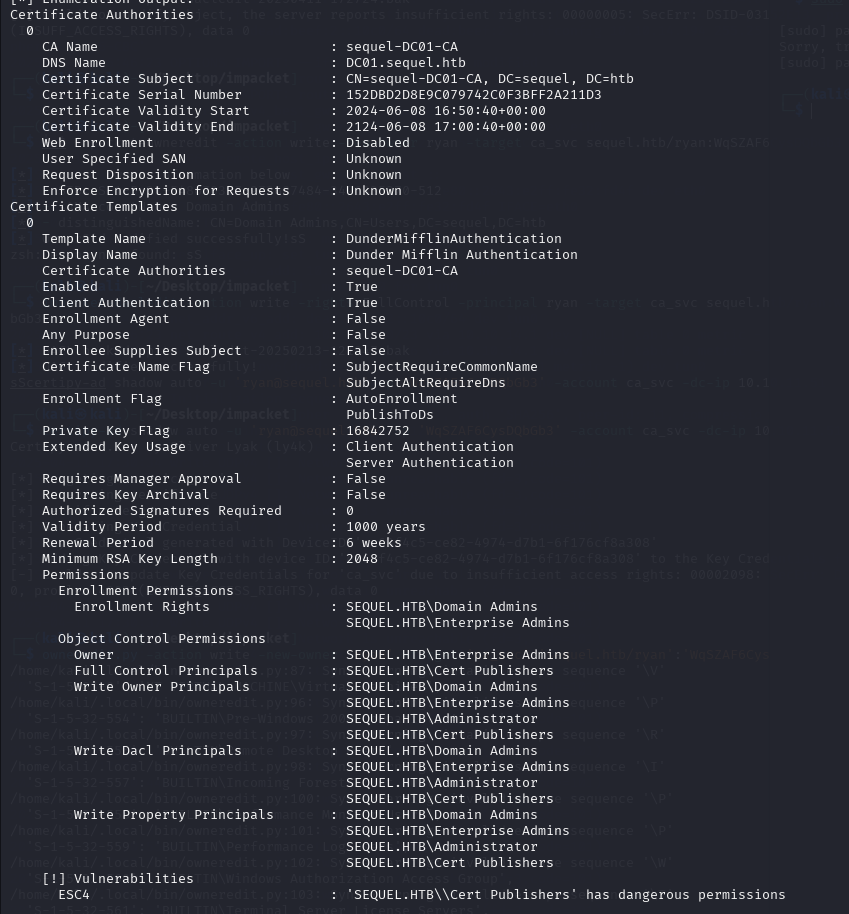
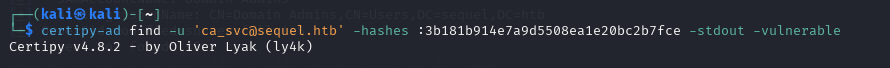


Ta dùng shadow credential Attack, ta add 1 malicious key cho ca\_svc giúp tk ryan có thể được xác thực dưới quyên fcuar ca\_svc mà chỉ cần certificate mà k cần password

Lấy NT hash cảu ca\_svc

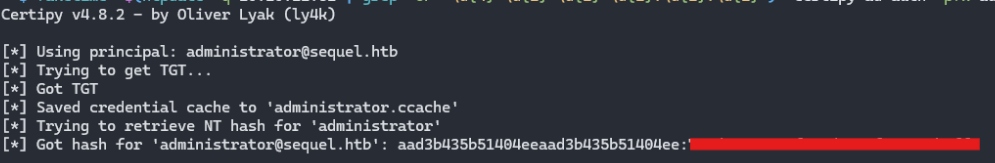


Dùng câu lệnh này certipy-ad find -u 'ca\_svc@sequel.htb' -hashes :3b181b914e7a9d5508ea1e20bc2b7fce -stdout -vulnerable



Có hash của tk sa\_svc rồi ta dùng câu lệnh certipy-ad auth -pfx administrator.pfx

Để lấy được hash của admin



Dùng hash và đăng nhập vào lấy flag

