Mình sẽ học một công cụ mới giúp liệt kê máy chủ SMB tốt hơn.

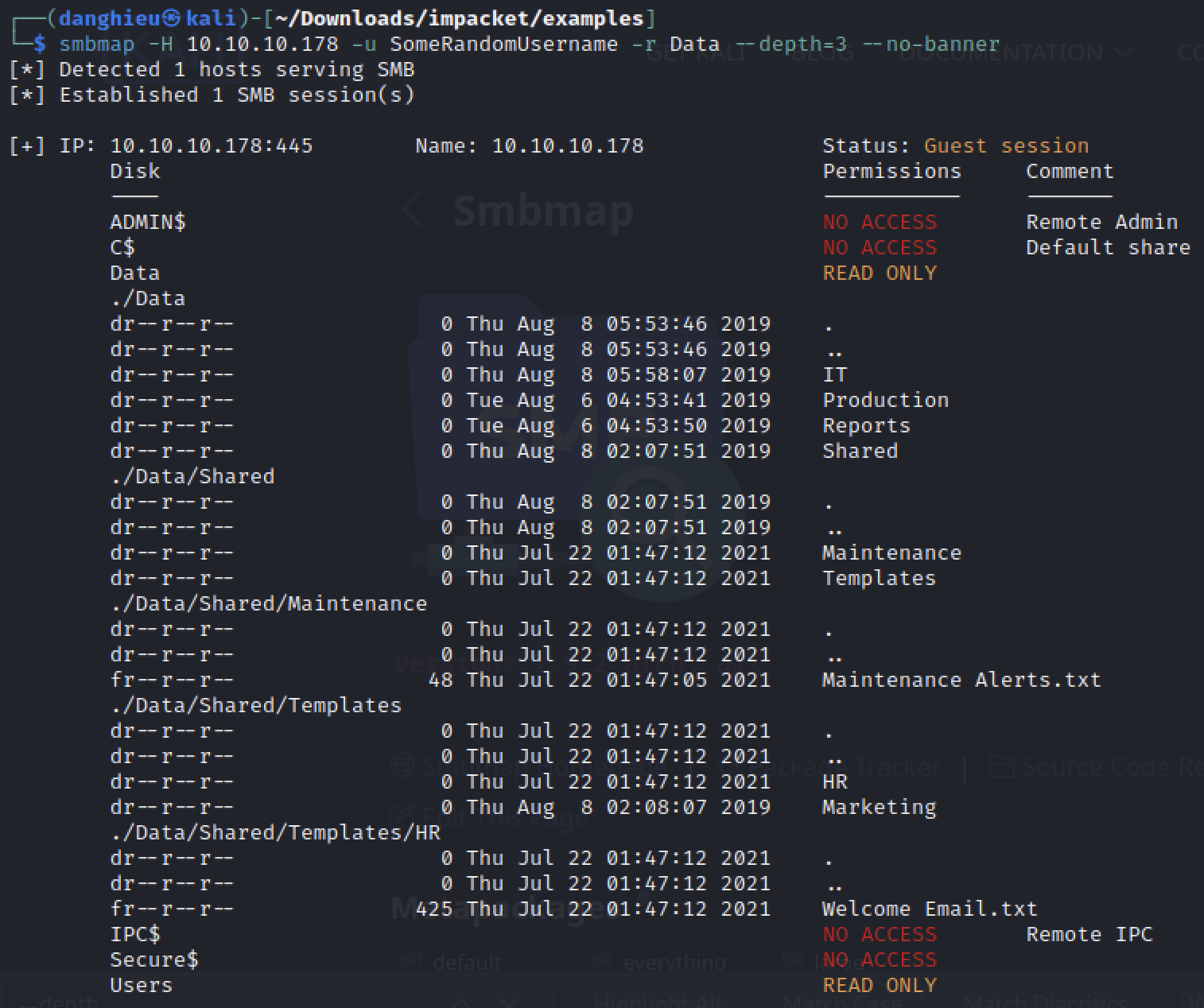
Kiểm tra SMB cho phép phiên anonymous:

python3 smbmap.py -H target-ip -u SomeRandomUsername --no-banner



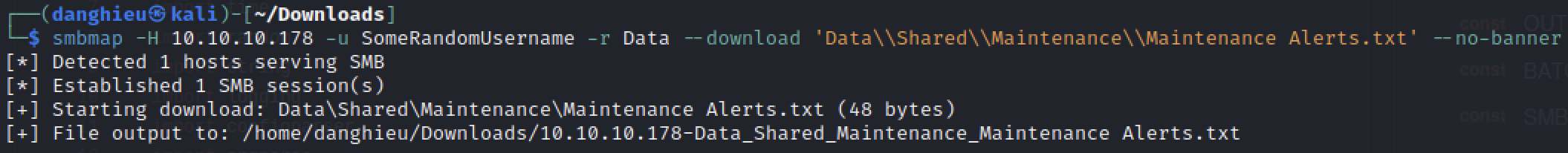
Chúng ta có thể kết nối thành công và khám phá được 3 shares không phải là mặc định: Secure$, Users và Data. Guest có quyền đọc Data và Users share. Thử liệt kê nội dung của chúng.

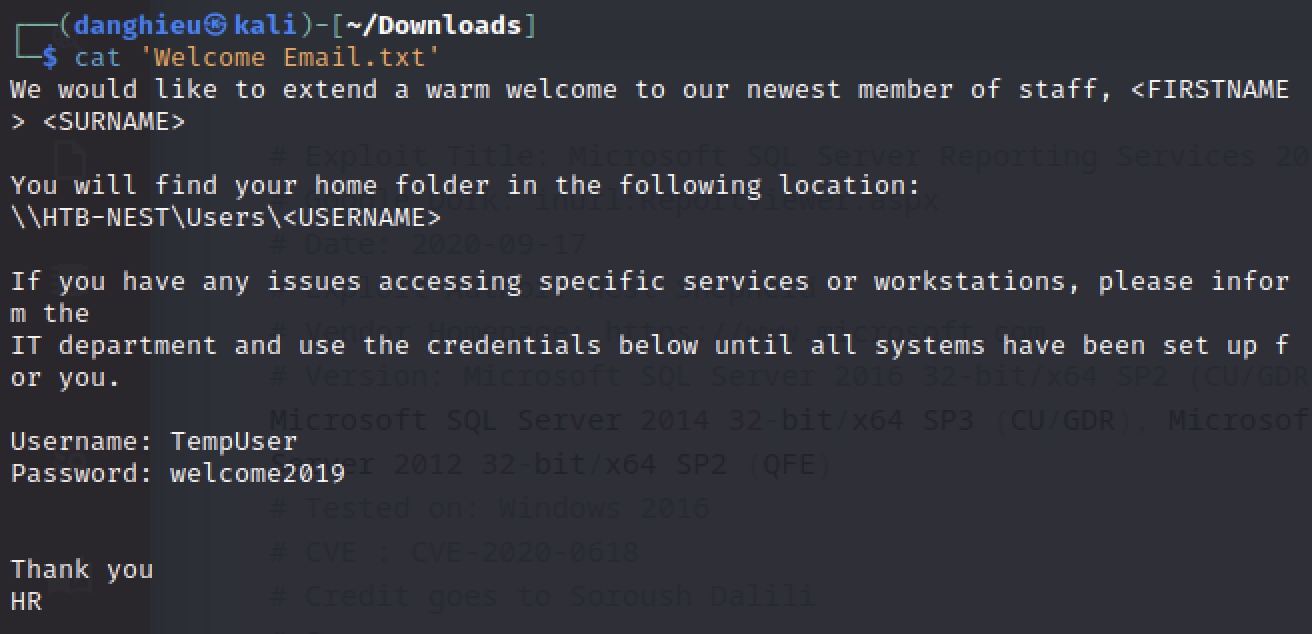
python3 smbmap.py -H target-ip -u SomeRandomUsername -r Data --depth=3 --no-banner



Các tập tin có thể được tải bằng flag --download:

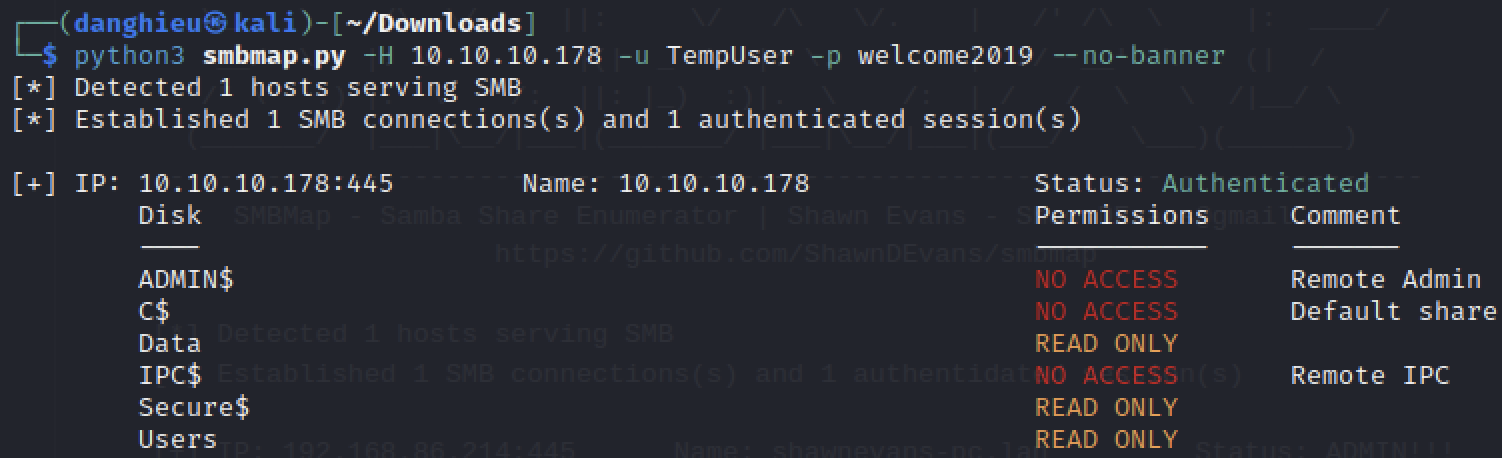
python3 smbmap.py -H target-ip -u SomeRandomUsername -r Data --download 'Data\\Shared\\Maintenance\\Maintenance Alerts.txt' --no-banner





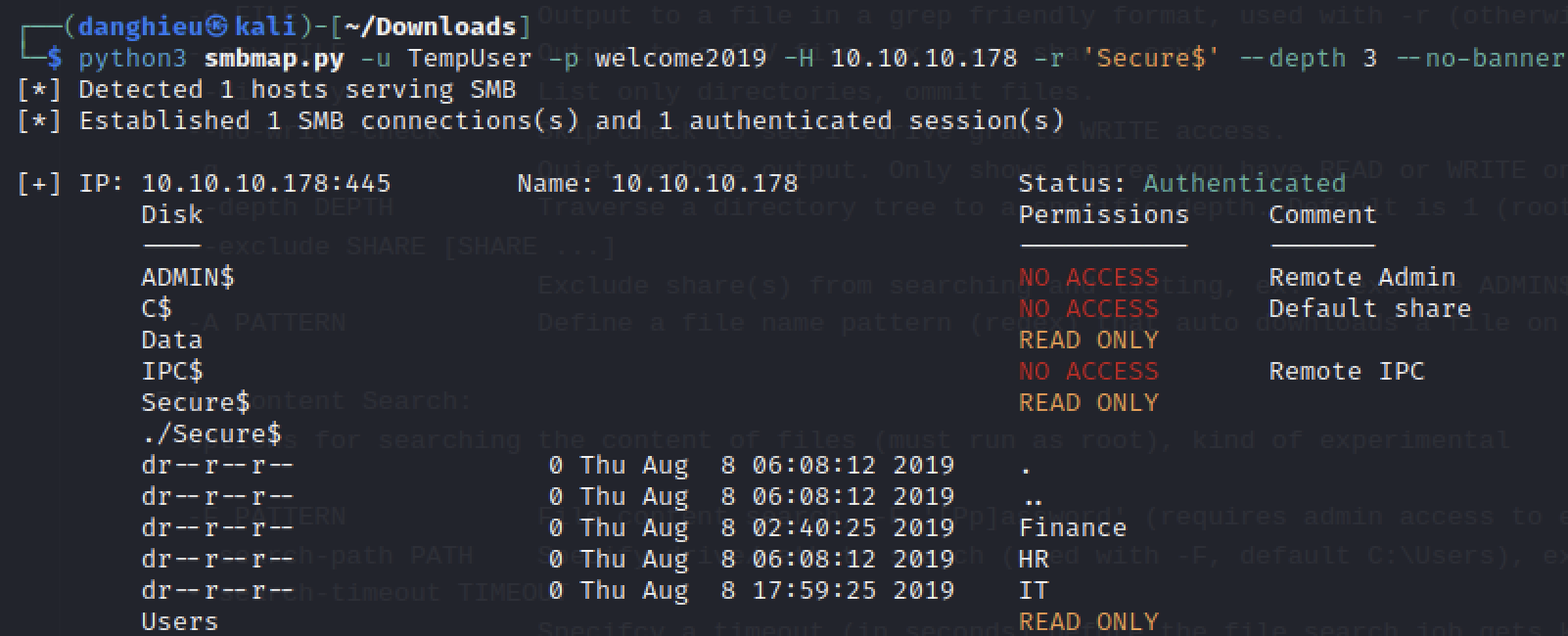
Tìm được tài khoản TempUser:welcome2019

python3 smbmap.py -u TempUser -p welcome2019 -H target-ip --no-banner



Nó cho phép chúng ta truy cập Secure$ share.

python3 smbmap.py -u TempUser -p welcome2019 -H target-ip -r Secure$ --depth=3 --no-banner

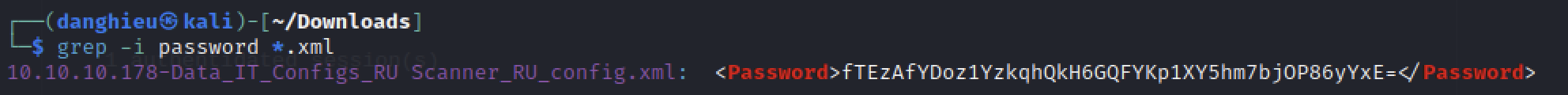


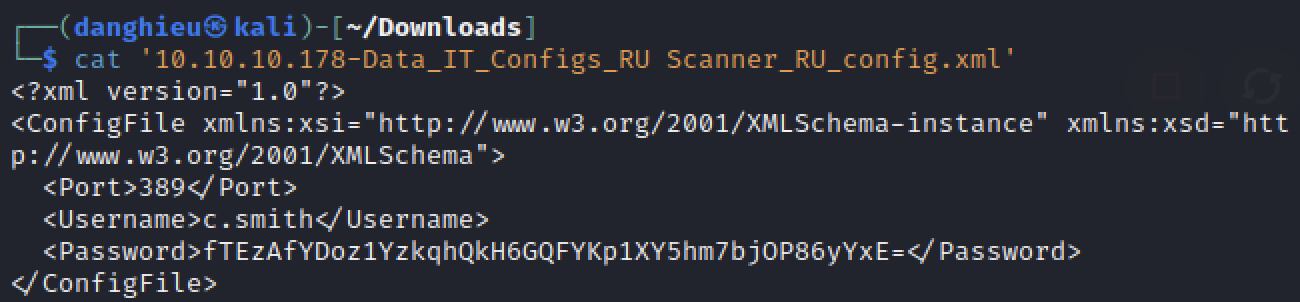
🡪 Chúng ta không có đặc quyền để liệt kê các thư mục trong Secure$

Chúng ta truy cập được nhiều tập tin và thư mục hơn trong Data share. Thư mục chứa rất nhiều tập tin XML, có thể chứa mật khẩu. Hãy tải tất cả tập tin XML bằng smbmap. Đối số -A để tải tất cả tập tin phù hợp với định dạng.

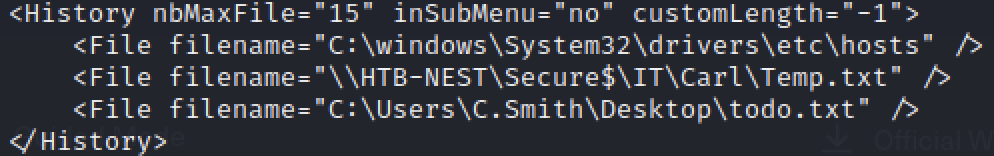
python3 smbmap.py -u TempUser -p welcome2019 -H target-ip -r Data --depth=4 -A xml --no-banner

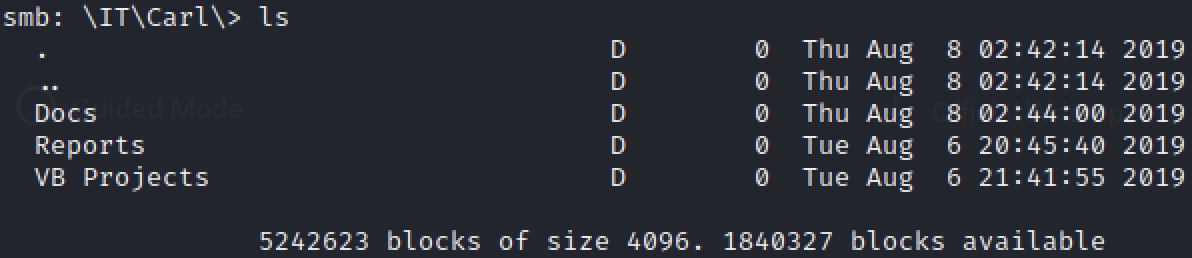
Lọc chuỗi password cho thấy tập tin RU\_Config.xml có chứa mật khẩu:

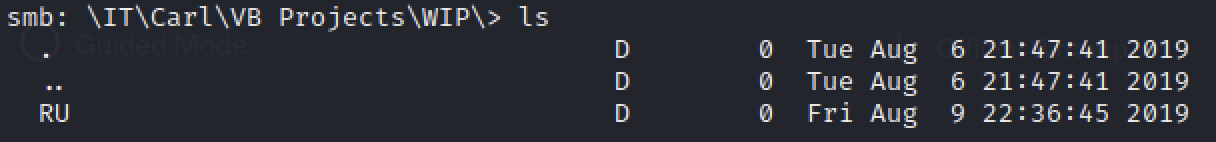


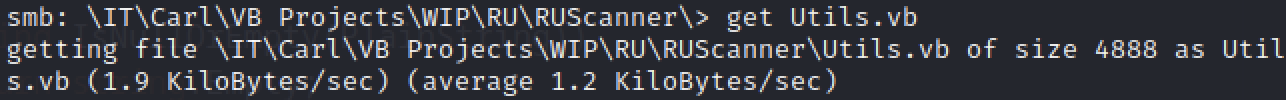


Tập tin cấu hình của notepad:

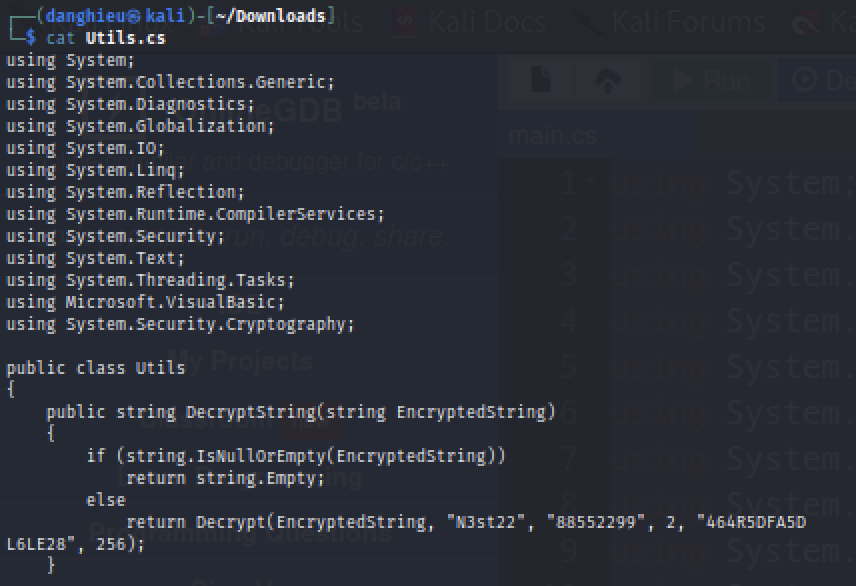


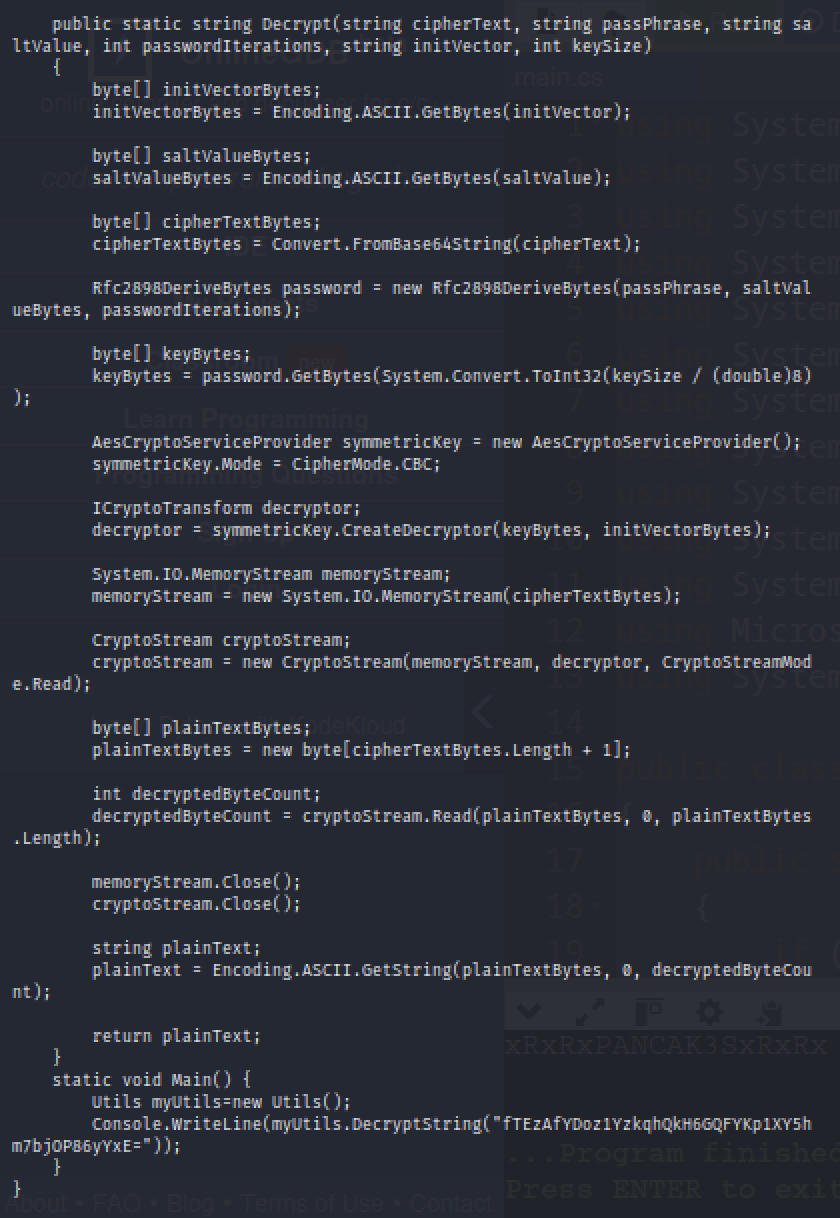




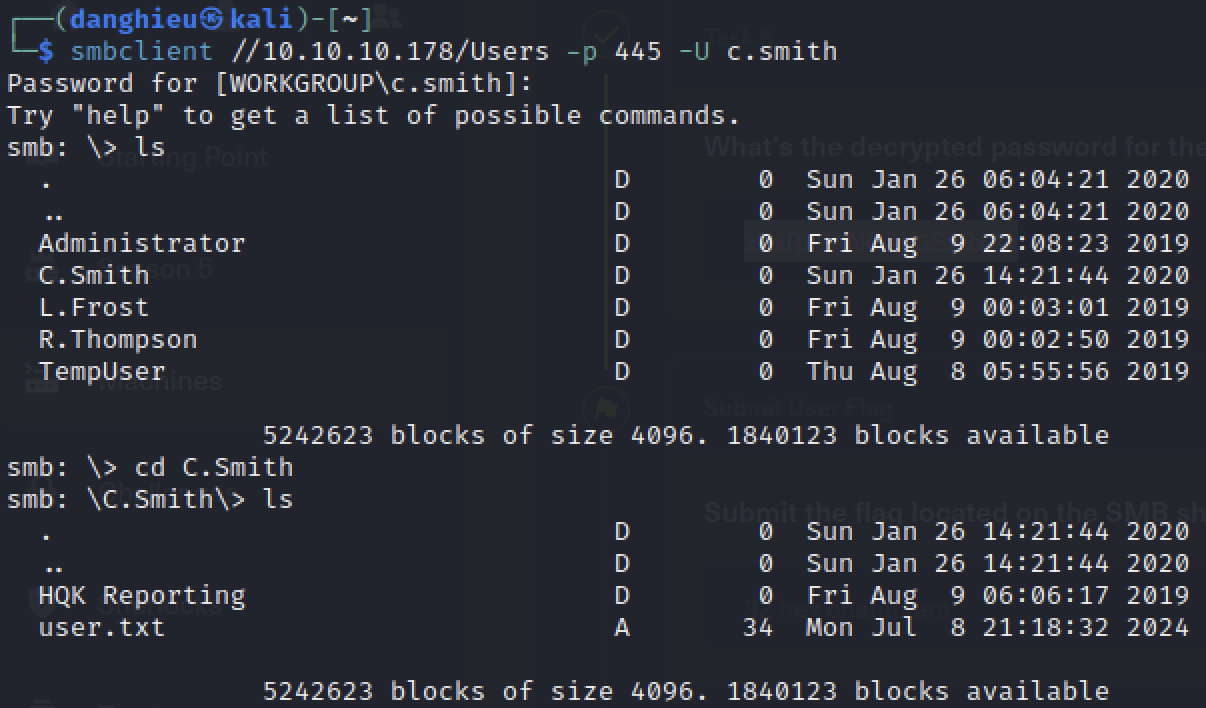


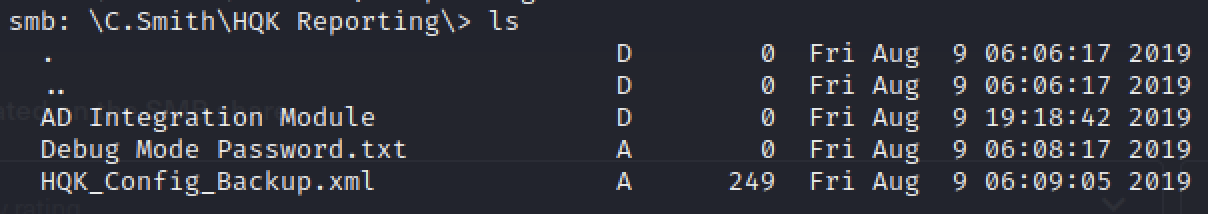
Chuyển tập tin .vb thành .cs:

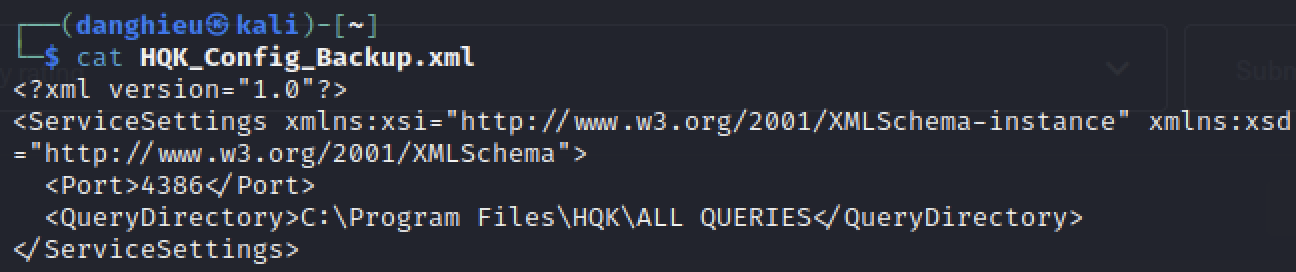


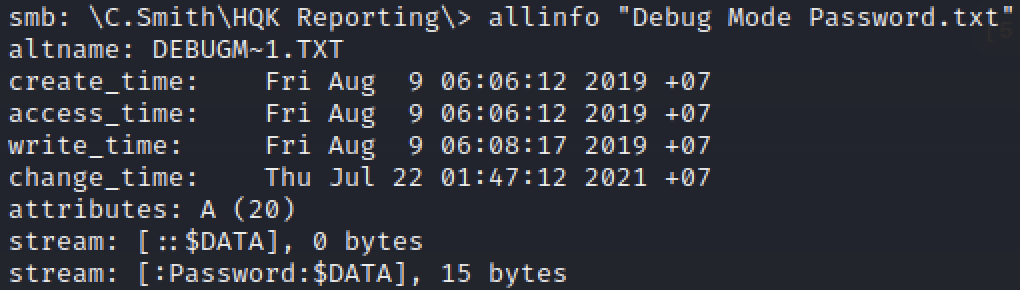


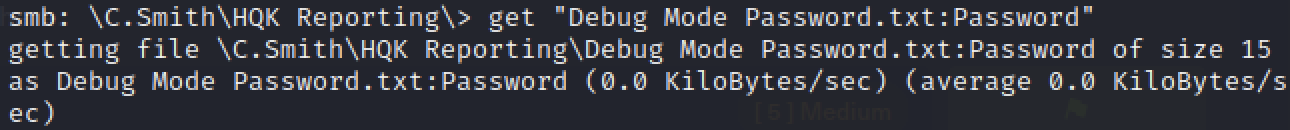
c.smith:xRxRxPANCAK3SxRxRx

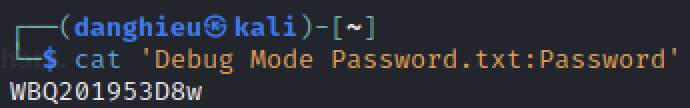












WBQ201953D8w

