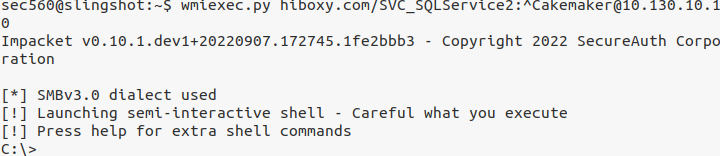
1. Establishing a shell on DC01

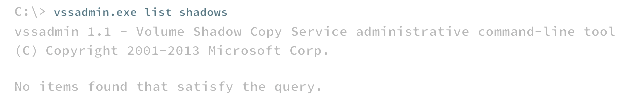
Truy cập vào DC01 bằng tài khoản SVC\_SQLService2



1. Looking at shadow copies

Sử dụng vssadmin để tạo bản sao cho ổ C

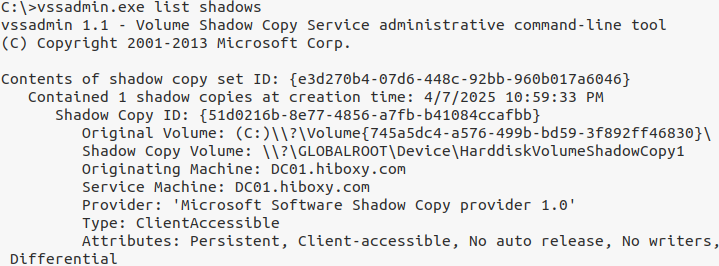
Liệt kê danh sách các bản sao



Đảm bảo ko có 1 bản sao nào

1. Create a Shadow Copy

Tạo 1 bản sao cho ổ C



1. Createing a copy of NTDT.dt and the System Hive

Hiện tại ta đã đã có được 1 bản sao. Thực hiện trích xuất file ntds.dit(là tệp csdl lưu trữ thông in về người dung, nhóm, máy tính, các đối tượng và chính sách) sang 1 file khác



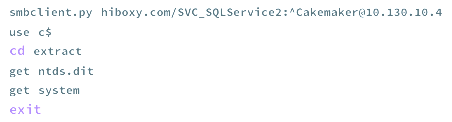
Tiếp tục lưu nhanh system của registry vào file ntds.dit

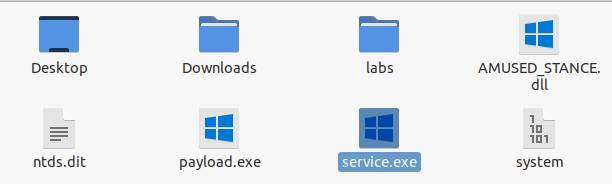


1. Copy the NTDS.dit file to your manchine

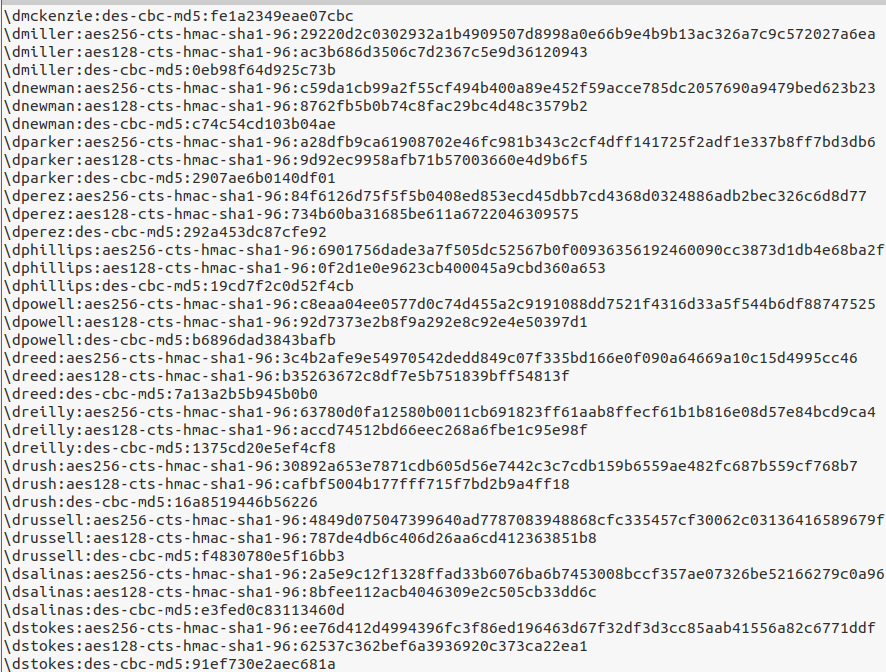
H chúng ta đã có file NTDS.dit mà mình cần. Thực hiện copy sang linux

Sử dụng smbclient





1. Extracting hashes

Sử dụng secretsdump.py để thực hiện thu thập những hash, 

Trong đó có 1 hash mà ta cần