Silver ticket là 1 Kerberos Service Ticket giả mạo được tạo ra cho 1 dịch vụ cụ thể trong môi trường Active Directory. Silver ticket chỉ có thể sử dụng để truy cập vào 1 dịch vụ cụ thể trong domain. Ví dụ như SQL Server

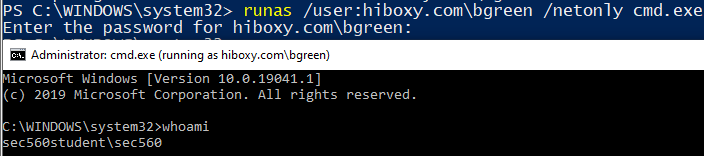
1. Preparation

Cấu hình hệ thống Window để sử dụng máy chủ DNS chỉ để tra cứu DNS



1. Testing bgreen’s access

Kiểm tra truy cập bằng cách đăng nhập vào tài khoản bgreen



Lệnh này sẽ giúp ta mở ra 1 cửa sổ mới. Tại cửa sổ này thực hiện liệt kê các tệp trên file01.hiboxy.com



Có thể thấy bgreen không có quyền truy cập vào

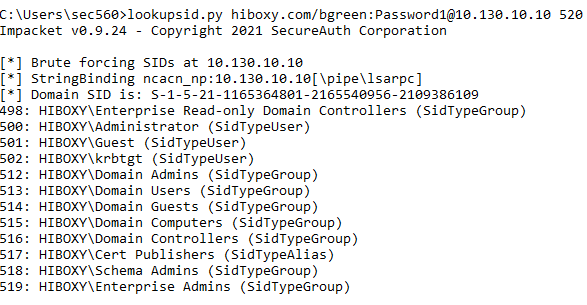
1. Getting the information to build a ticket

Chúng ta sẽ tắt cửa sổ cmd chạy dưới bgreen. Ta sẽ thực hiện tấn công dưới tư cách 1 người dung thông thường.

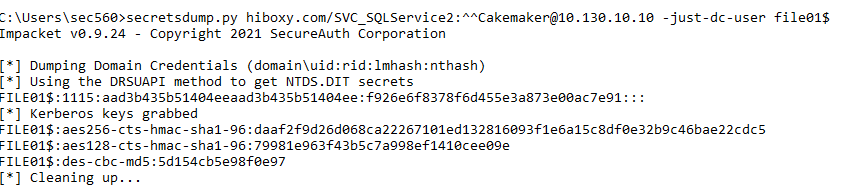
Để có thể tạo Silver ticket bằng Rubeus, ta cần vài thứ

* NT Hash từ dịch vụ cần
* SID của Domain

Đầu tiên, thực hiện lấy được SID của Domain. Sử dụng lookupsid.py trong Impacket



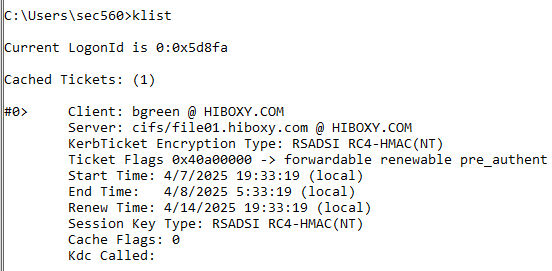
Thu được SID của Domain. H thì mục tiêu ta hướng đến là FILE01. Vì thế ta cần những NT hash từ những tài khoản FILE01.

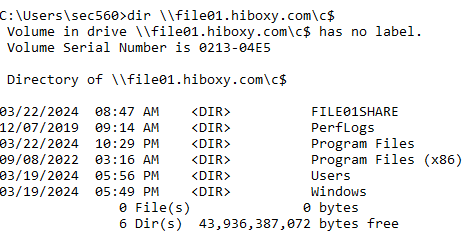
Sử dụng secretsdump để dump NTHash

1. Creating the Ticket with Rubeus



Xem thông tin ticket



’

Thành công kết nối được đến file01 bằng ticket vừa tạo

1. A Second Forged Ticket

Tạo 1 ticket mới nhưng hãy biến đổi nó đi 1 chút

Với ticket trước, ta đã cấp quyền admin cho bgreen. Bây giờ ta sẽ fake username và RID

Xóa ticket vừa tạo



