Kerberos là giao thức xác thực mạng. Dùng để

* Xác thực lẫn nhau: client và server
* Không gửi mk qua mạng
* Sử dụng ticket

Các thành phần:

* Client
* Service
* KDC: trung tâm phân khối khóa gồm
  + AS: cấp vé đăng nhập
  + TGS: cấp vé truy cập dịch vụ

Cách thức hoạt động

* Client gửi thông tin đăng nhập đến AS
* AS xác thực client và gửi lại TGT cho Client(TGT được mã hóa bằng khóa bí mật của TGS)
* Client gửi yêu cầu + TGT đến TGS
* TGS kiểm tra TGT và tạo vé gửi về cho Client để đến dịch vụ
* Client gửi vé dịch vụ vừa tạo đến dịch vụ của nó

SPN là viết tắt của **Service Principal Name** – là một **tên định danh duy nhất cho một dịch vụ** chạy trong môi trường **Active Directory**, giúp **Kerberos biết được tài khoản nào cung cấp dịch vụ đó và cung cho TSG cấp đúng vé dịch vụ được mã hóa bằng mật khẩu của tài khoản đso**

1. Enumerate and Request Tickets

Sử dụng GetUserSPNs để liệt kê những tài khoản người dungf có SPN được set và tự động yêu cầu vé dịch vụ cho những dịch vụ đó


Ta xác thực được 2 tài khoản dịch vụ thuộc nhóm domain admins

Sử dụng tee để ghi những thông tin vào file /tmp/spns.output

Và ta có thể nhìn thấy được những service ticket được mã hóa bằng RC4

1. Cracking the ticket

Lưu riêng các hashes vào 1 file khác



Sử dụng hashcat để crack

**hashcat -m 13100 -a 6 /tmp/tickets /opt/passwords/english-dictionary-capitalized.txt ?d**

-m 13100: Kerberos 5 TGS-REP hash

-a 6: Hybrid attack: kết hợp dictionary + mask

Thu được mật khẩu của hash thứ nhất



1. Cracking the domain admin ticket

**hashcat -m 13100 -a 7 /tmp/tickets ?s /opt/passwords/english-dictionary-capitalized.txt**

Sử dụng -a 7 thay vì 6 để thay đổi vị trí mask và dictionary

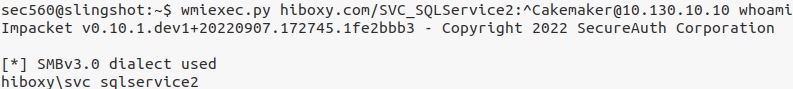


Thu được mật khẩu của hash thứ 2

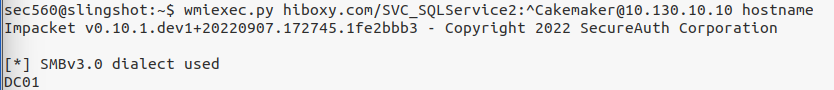
1. Use stolen credential

Sử dụng những hash được crack để truy cập vào DC

Sử dụng wmiexec.py



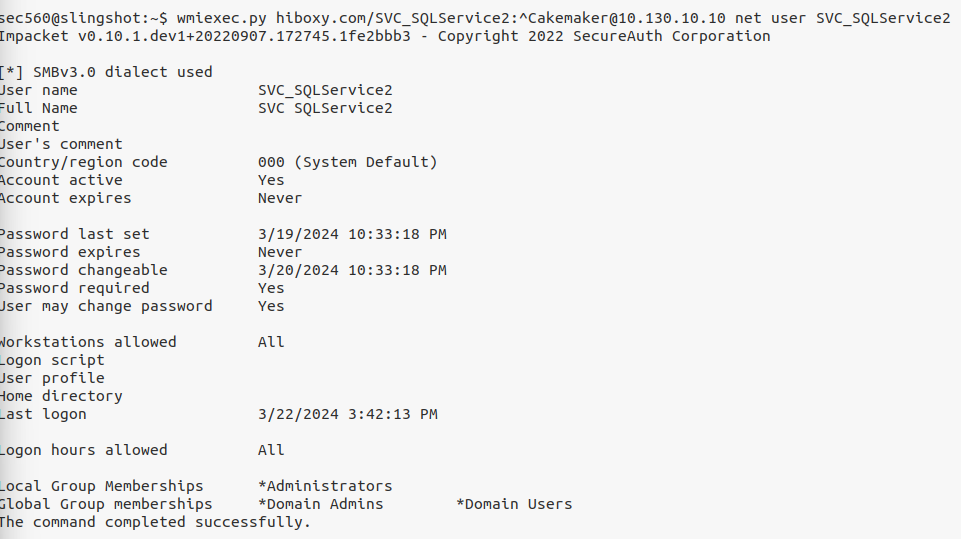
Xác nhận chúng ta đã thực hiện ở trong DC với svcsqlservice



Xem các user trong DC



Xem thông tin user SVC\_SQLService2



Có thể thấy user này thuộc group admin