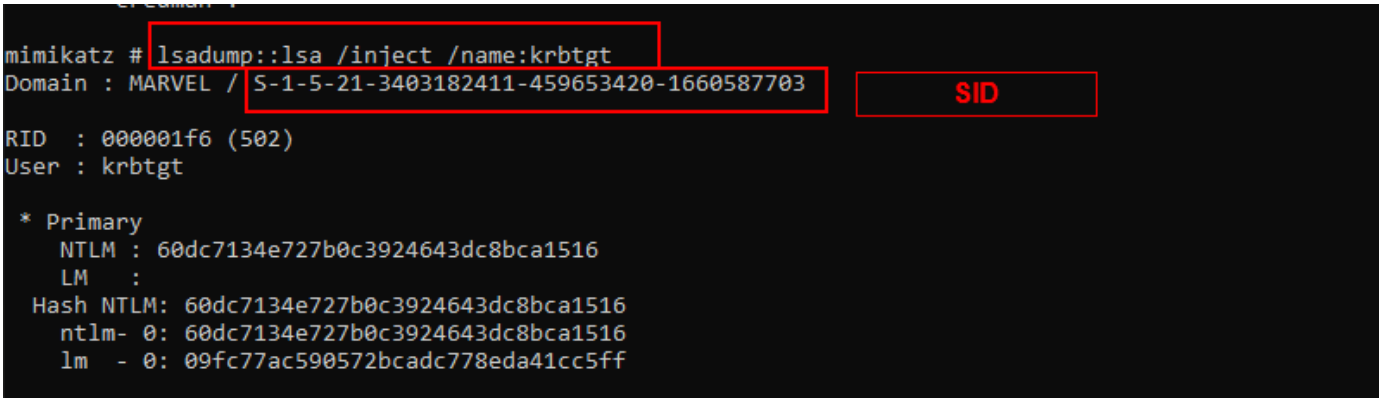
GOLDEN TICKET ATTACK

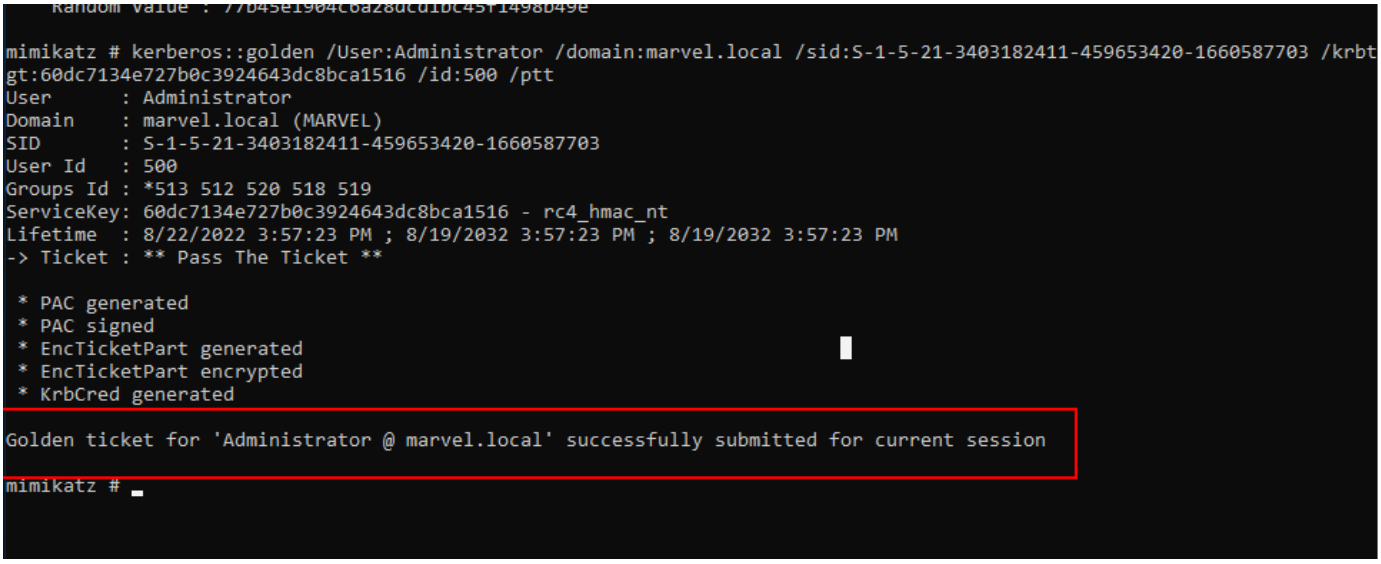
THIS ONLY WORKS IF WE CAN COMPROMISE THE KERBROAT ACCOUNT, AND THIS ATTACK ALLOWS US TO GENERATE TICKET.

RUN THE COMMAND LSADUMP::LSA /INJECT /NAME:KRBTGT TO FIND ITS SID AND ITS HASH

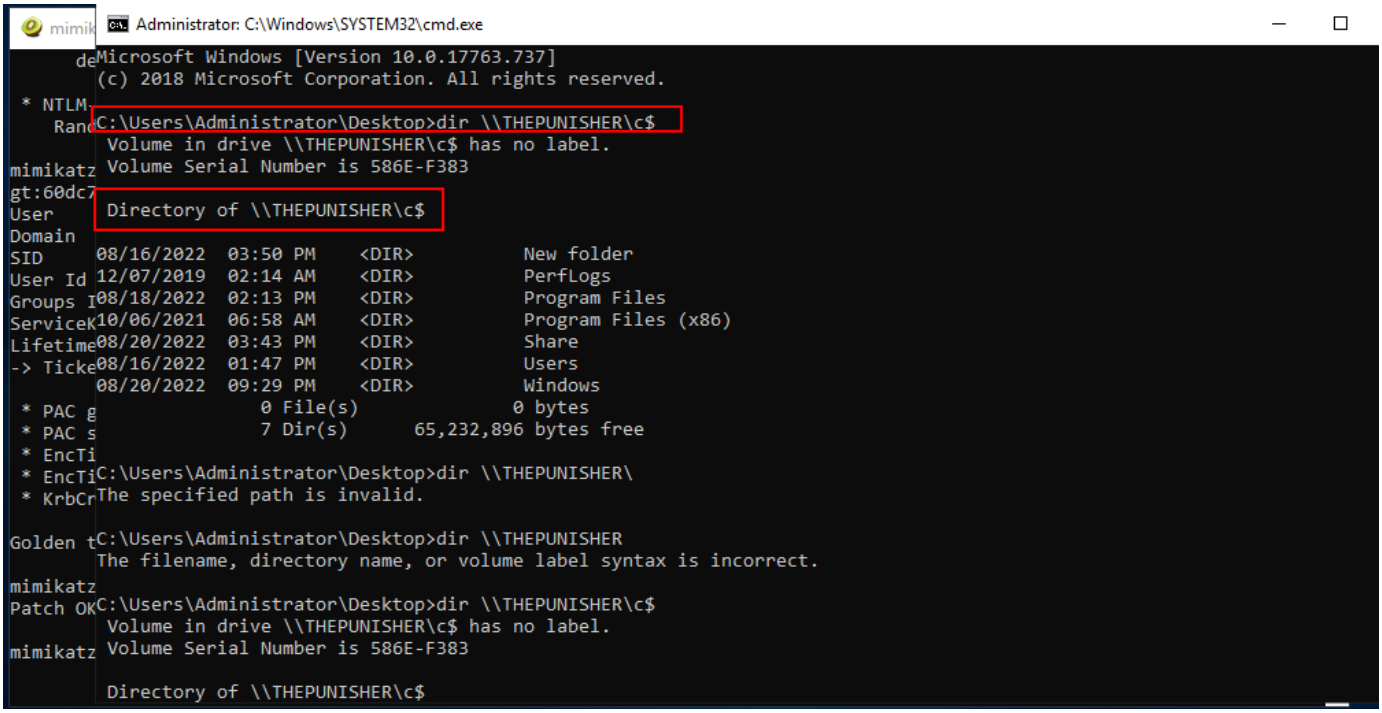


SID: SECURITY IDENTIFIER. *là* một mã định dạng cho mỗi đối tượng trong windows (user, group)

GENERATE THE TICKET TO ACCESS TO ALL THE SERVICE OR ANY ACCOUNT WE WANT



RUN THIS COMMAND TO OPEN NEW TERMINAL TO GAIN ACCESS TO OTHER MACHINES



OTHER OPTIONS:

WE CAN USE PSEXEC ON DC TO GAIN SHELL AS WELL