bloodyAD and Kerberos

cravaterouge.github.io/ad/privesc/2022/05/05/bloodyad-and-kerberos.html

CravateRouge May 5, 2022

5 May 2022
by CravateRouge

Most of the time I use NTLM authentication, but in some situations, we only have a kerberos TGT or ST and it would be a shame to not use it to attempt to elevate our privileges in the AD. So let's see how we can do this with bloodyAD.

Linux

```
# Get a TGT (For GSSAPI the server name must be the FQDN)
$ getTGT.py -dc-ip 192.168.10.2 bloody.local/Administrator:p@ssw0rd
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

2022-05-05 10:11:19.028227
[*] Saving ticket in Administrator.ccache

# Get a ST (For GSSAPI the spn is case sensitive)
$ getST.py -no-pass -k -dc-ip 192.168.10.2 -spn ldap/win-ij5b521uo5l.bloody.local
"BLOODY.LOCAL/Administrator"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Using TGT from cache
[*] Getting ST for user
[*] Saving ticket in Administrator.ccache

# Use bloodyAD with Kerberos auth (using a TGT or a ST)
## Add the credential cache generated in the default path
$ export KRB5CCNAME="Administrator.ccache"

## Check if the ticket is in default path, not expired, for the right
client/server
$ klist
Ticket cache: FILE:Administrator.ccache
Default principal: Administrator@BLOODY.LOCAL

Valid starting       Expires              Service principal
05/05/2022 19:42:54  06/05/2022 05:42:54  krbtgt/BLOODY.LOCAL@BLOODY.LOCAL
        renew until 06/05/2022 19:42:55

## If your DNS doesn't resolve
## Note: second level domain name with ".local" added to /etc/hosts doesn't
resolve on some Manjaro versions
# see https://forum.manjaro.org/t/mapping-for-etc-hosts-entries-with-local-as-tld-
isnt-working/116021
$ sudo echo "192.168.10.2 win-ij5b521uo5l.bloody.local bloody.local" >> /etc/hosts

## And now the magic happens
$ python bloodyAD.py -k -d bloody.local -u Administrator --host WIN-
IJ5B521UO5L.bloody.local get object 'DC=bloody,DC=local' --attr msDS-Behavior-
Version

distinguishedName: DC=bloody,DC=local
msDS-Behavior-Version: DS_BEHAVIOR_WIN2016
```

Windows

The following code demonstrates how to generate kerberos TGT and ST and how they are used by bloodyAD on a Windows environment. Of course in most of the cases you'll already have an available ticket. In this case jump directly to the bloodyAD part.

```
# Get a TGT
(venv) PS > python .\venv\Scripts\getTGT.py -dc-ip 192.168.10.2
bloody/Administrator:p@ssw0rd
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Saving ticket in Administrator.ccache

# Get a ST from the TGT
(venv) PS > ren Administrator.ccache adminTGT.ccache
(venv) PS > $env:krb5ccname="adminTGT.ccache"
(venv) PS > python .\venv\Scripts\getST.py -no-pass -k -dc-ip 192.168.10.2 -spn
ldap/WIN-IJ5B521UO5L.bloody.local "BLOODY/Administrator"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Using TGT from cache
[*] Getting ST for user
[*] Saving ticket in Administrator.ccache

# Use bloodyAD with Kerberos auth (using a TGT or a ST)
## First convert ccache in kirbi if necessary
(venv) PS > python .\venv\Scripts\ticketConverter.py Administrator.ccache
Administrator.kirbi
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] converting ccache to kirbi...
[+] done

## Inject the ticket in memory if needed
(venv) PS > .\mimikatz.exe "kerberos::ptt
d:\gold\documents\bloodyAD\Administrator.kirbi"

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "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(commandline) # kerberos::ptt
d:\gold\documents\bloodyAD\Administrator.kirbi

* File: 'd:\gold\documents\bloodyAD\Administrator.kirbi': OK

## Check if the ticket is in memory, not expired, for the right client/server
(venv) PS > klist

Current LogonId is 0:0x75af1

Cached Tickets: (1)

#0>     Client: Administrator @ BLOODY.LOCAL
        Server: ldap/WIN-IJ5B521UO5L.bloody.local @ BLOODY.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x804a0000 -> reserved initial 0xa0000
        Start Time: 5/4/2022 18:56:50 (local)
        End Time:   5/5/2022 4:54:52 (local)
```

```
        Renew Time: 0
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called:

## Install winkerberos > 0.9.0
(venv) PS > pip install --upgrade --force-reinstall winkerberos

## And now the magic happens
## (Don't forget to add an entry in C:\Windows\System32\drivers\etc\hosts for WIN-
IJ5B521UO5L.bloody.local if needed)
(venv) PS > python bloodyAD.py -k -d bloody.local -u Administrator --host WIN-
IJ5B521UO5L.bloody.local get object 'DC=bloody,DC=local' --attr msDS-Behavior-
Version

distinguishedName: DC=bloody,DC=local
msDS-Behavior-Version: DS_BEHAVIOR_WIN2016
```

Note

Since commit 54babd7 exchange of sensitive information without LDAPS is supported.

tags: - *privesc* - *bloodyad* - *kerberos* - *authentication*