bloodyAD and Certificate Authentication

cravaterouge.github.io/ad/privesc/2022/05/09/bloodyad-and-certificate-authentication.html

CravateRouge May 9, 2022

9 May 2022
by CravateRouge

A few days ago I read a great article from Yannick Méheut of Almond about certificate authentication in Active Directory environment. It is especially useful when PKINIT is not supported and thus you can't use your certificate to request a TGT. This is why I wanted to extend the capabilities of bloodyAD by allowing certificate authentication. Here is an example on how to use it (the first part show how to get a certificate if you just want to try the functionality):

```
# Grab the cert
## Get the CA Authority name
$ certipy find -u Administrator@bloody -p 'Password123!' -dc-ip 192.168.10.2 -
debug
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[+] Authenticating to LDAP server
[+] Bound to ldaps://192.168.10.2:636 - ssl
[+] Default path: DC=bloody,DC=local
[+] Configuration path: CN=Configuration,DC=bloody,DC=local
[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[+] Trying to resolve 'DC01.bloody.local' at '192.168.10.2'
[*] Trying to get CA configuration for 'bloody-DC01-CA' via CSRA
[+] Trying to get DCOM connection for: 192.168.10.2
[*] Got CA configuration for 'bloody-DC01-CA'
[+] Resolved 'DC01.bloody.local' from cache: 192.168.10.2
[+] Connecting to 192.168.10.2:80

## Get the PFX
$ certipy req -u Administrator@bloody.local -p 'Password123!' -target 192.168.10.2
-ca bloody-DC01-CA -template User
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 4
[*] Got certificate with UPN 'Administrator@bloody.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'

## Convert it to pem
$ openssl pkcs12 -in administrator.pfx -out administrator.pem -nodes
Enter Import Password:

# Use cert authentication
$ bloodyAD -c ":administrator.pem" -d bloody -u Administrator --host 192.168.10.2
get object 'DC=bloody,DC=local' --attr msDS-Behavior-Version

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

Old certipy version v2.0.9

```
# Grab the cert

## Get the CA Authority name
## -debug is required in my env or it doesn't work
(venv) PS > certipy.exe find bloody/Administrator:passw0rd@192.168.10.2 -debug
Certipy v2.0.9 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[+] Authenticating to LDAP server
[+] Bound to ldaps://192.168.10.2:636 - ssl
[+] Default path: DC=bloody,DC=local
[+] Configuration path: CN=Configuration,DC=bloody,DC=local
[*] Found 33 certificate templates
[*] Finding certificate authorities
[+] Trying to resolve 'WIN-IJ5B521UO5L.bloody.local' at '192.168.10.2'
[*] Trying to get CA configuration for 'bloody-WIN-IJ5B521UO5L-CA' via CSRA
[+] Target system is 192.168.10.2 and isFQDN is False
[+] StringBinding: \\\\WIN-IJ5B521UO5L[\\pipe\\cert]
[+] StringBinding: WIN-IJ5B521UO5L[49702]
[*] Got CA configuration for 'bloody-WIN-IJ5B521UO5L-CA'
[+] Resolved 'WIN-IJ5B521UO5L.bloody.local' from cache: 192.168.10.2
[+] Connecting to 192.168.10.2:80
[*] Found 11 enabled certificate templates
[*] Saved text output to '20220506173005_Certipy.txt'
[*] Saved JSON output to '20220506173005_Certipy.json'
[*] Saved BloodHound data to '20220506173005_Certipy.zip'. Drag and drop the file
into the BloodHound GUI

## Get the PFX
(venv) PS > certipy.exe req bloody/Administrator:passw0rd@192.168.10.2 -ca bloody-
WIN-IJ5B521UO5L-CA -debug

[*] Requesting certificate
[+] Trying to connect to endpoint: ncacn_np:192.168.10.2[\pipe\cert]
[+] Connected to endpoint: ncacn_np:192.168.10.2[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 4
[*] Got certificate with UPN 'Administrator@bloody.local'
[*] Saved certificate and private key to 'administrator.pfx'
```

tags: - *privesc* - *bloodyad* - *certificate* - *authentication*