Inspecting Kerberos Ticket Requests

ZERODAYLAB®

Version:	1.0
Date:	2020
Confidentiality class:	Public

whoami?

cname: Charlie Clark

realm: Security Consultant @ ZeroDayLab

rtime: IT ~15 years, InfoSec ~5 years

authenticator: OSCP, CRTE, CRT, …

AuthorizationData: Rubeus, PowerUpSQL, impacket, …

Twitter: @exploitph GitHub: @0xe7 Blog: https://exploit.ph

Agenda

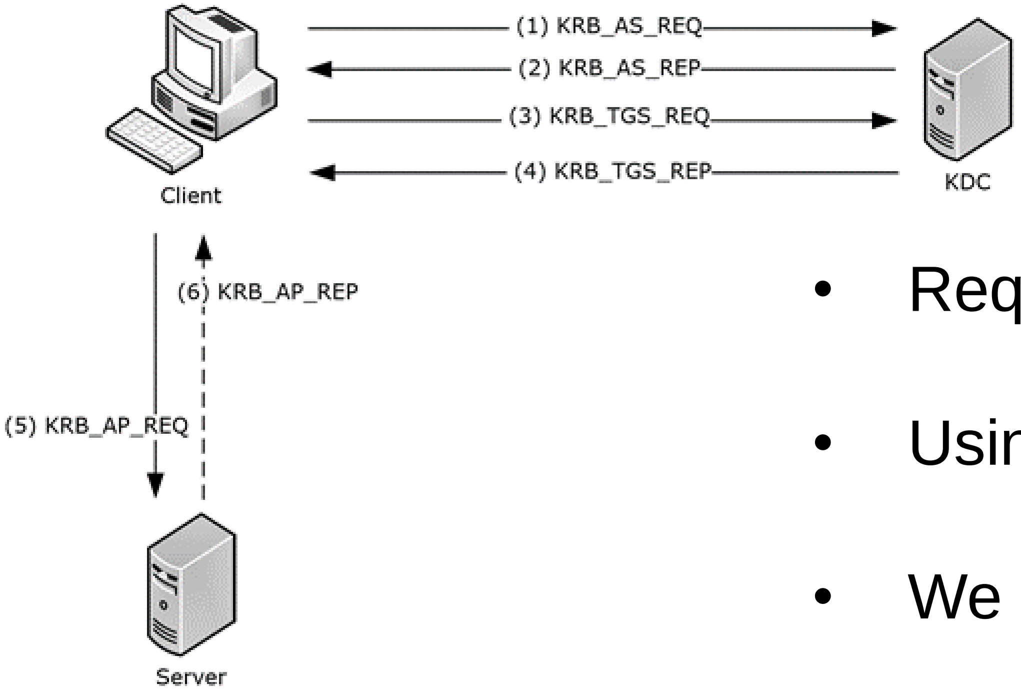
1. Kerberos 101
2. Common abuses / tools
3. A look at genuine traffic
4. Comparison with Rubeus
5. Fingerprinting abuse tools
6. Making Kerberos tickets great again
7. Looking forward

What is Kerberos?

The primary method of authentication between Windows computers on an Active Directory domain.

Used to share a session key for further communication.

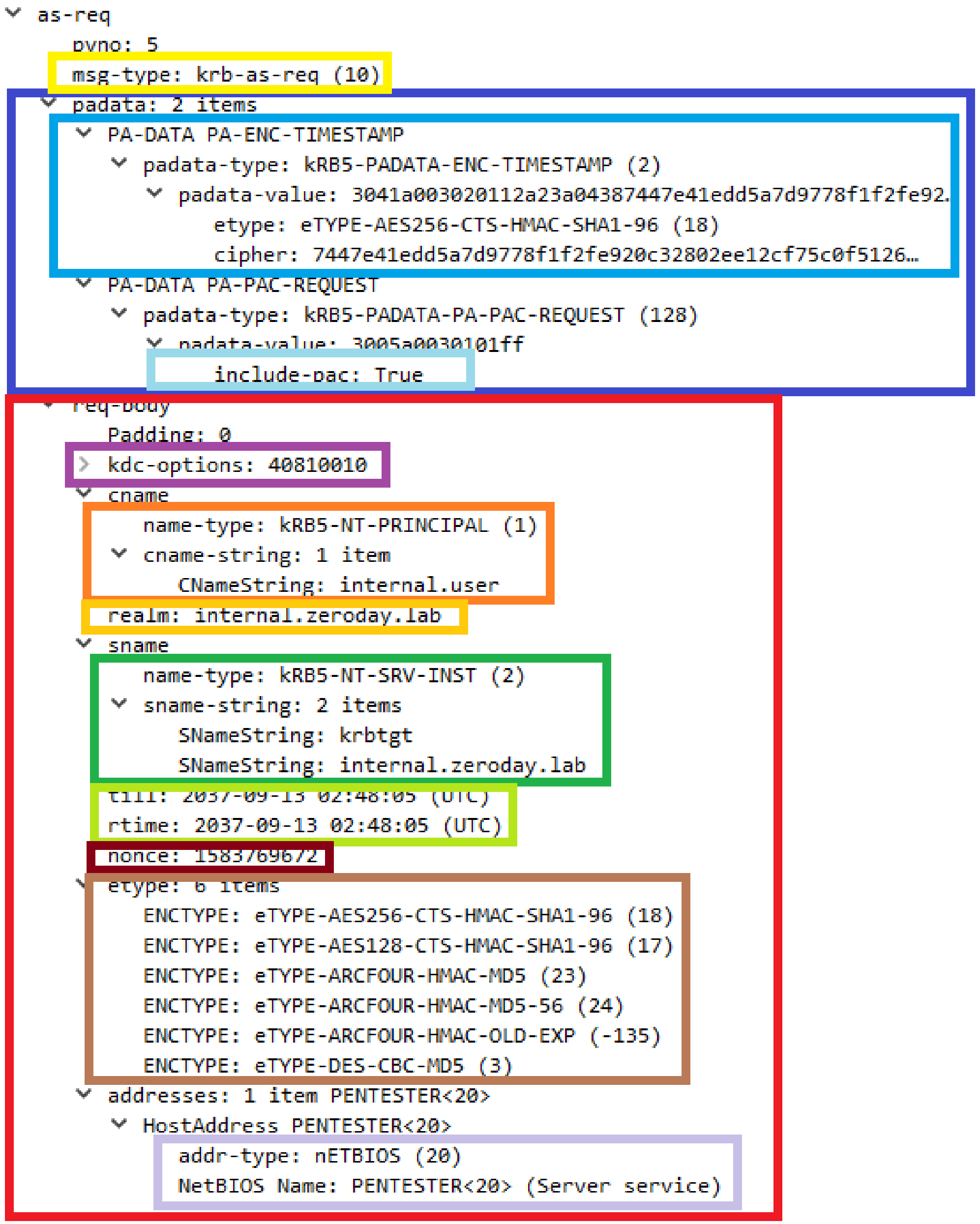
Kerberos Most Basic Usage



- Requesting a Ticket Granting Ticket (TGT)
- Using TGT to request service tickets
- We only care about 1 and 3 for this talk

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/b4af186e-b2ff-43f9-b18e-eedb366abf13

AS-REQ



```
⌄ as-req
    pvno: 5
    msg-type: krb-as-req (10)
  ⌄ padata: 2 items
    ⌄ PA-DATA PA-ENC-TIMESTAMP
      ⌄ padata-type: kRB5-PADATA-ENC-TIMESTAMP (2)
        ⌄ padata-value: 3041a003020112a23a04387447e41edd5a7d9778f1f2fe92…
            etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            cipher: 7447e41edd5a7d9778f1f2fe920c32802ee12cf75c0f5126…
    ⌄ PA-DATA PA-PAC-REQUEST
      ⌄ padata-type: kRB5-PADATA-PA-PAC-REQUEST (128)
        ⌄ padata-value: 3005a0030101ff
            include-pac: True
  ⌄ req-body
      Padding: 0
    > kdc-options: 40810010
    ⌄ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ⌄ cname-string: 1 item
          CNameString: internal.user
      realm: internal.zeroday.lab
    ⌄ sname
        name-type: kRB5-NT-SRV-INST (2)
      ⌄ sname-string: 2 items
          SNameString: krbtgt
          SNameString: internal.zeroday.lab
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 1583769672
    ⌄ etype: 6 items
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
        ENCTYPE: eTYPE-DES-CBC-MD5 (3)
    ⌄ addresses: 1 item PENTESTER<20>
      ⌄ HostAddress PENTESTER<20>
          addr-type: nETBIOS (20)
          NetBIOS Name: PENTESTER<20> (Server service)
```

● AS-REQ message type (10)

● PA Data section, for pre-authentication and extensions

● Kerberos pre-authentication

● Include PAC in AS-REP (TGT)

● Request body

● Various options for the different message types

● Client name (requesting user)

● Domain name

● Server name (with AS-REQ's always *krbtgt/domain.com*)

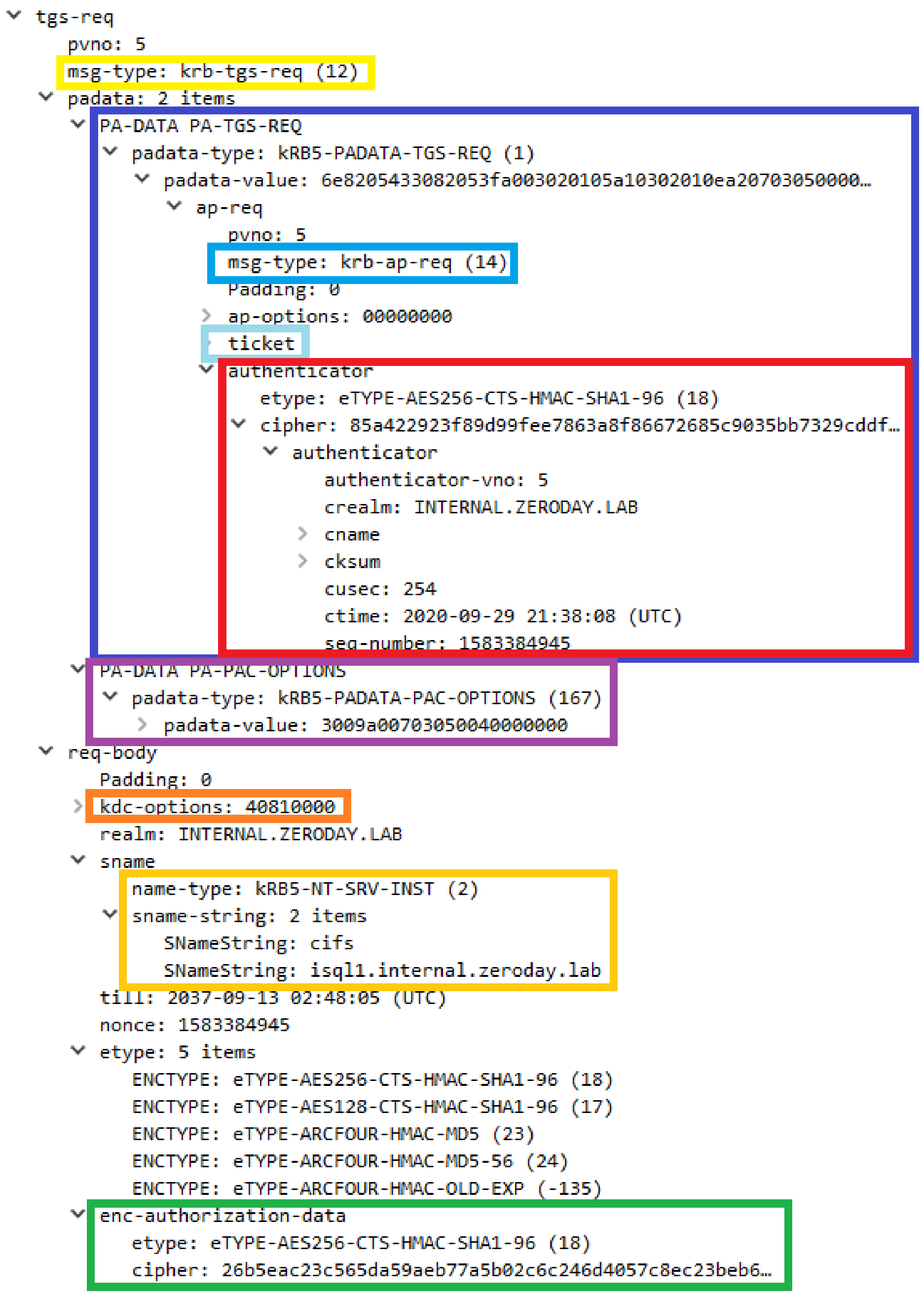
● Valid until and renew times for the resulting TGT

● Nonce – random number

● Supported encryption types

● Addresses, a list, normally just the NetBIOS name of the requesting machine

TGS-REQ

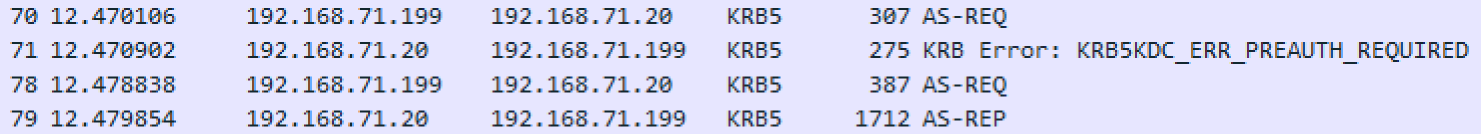


```
tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 2 items
        PA-DATA PA-TGS-REQ
        padata-type: kRB5-PADATA-TGS-REQ (1)
            padata-value: 6e8205433082053fa003020105a10302010ea20703050000…
                ap-req
                    pvno: 5
                    msg-type: krb-ap-req (14)
                    Padding: 0
                    ap-options: 00000000
                    ticket
                    authenticator
                        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                        cipher: 85a422923f89d99fee7863a8f86672685c9035bb7329cddf…
                            authenticator
                                authenticator-vno: 5
                                crealm: INTERNAL.ZERODAY.LAB
                                cname
                                cksum
                                cusec: 254
                                ctime: 2020-09-29 21:38:08 (UTC)
                                seq-number: 1583384945
        PA-DATA PA-PAC-OPTIONS
        padata-type: kRB5-PADATA-PAC-OPTIONS (167)
            padata-value: 3009a00703050040000000
    req-body
        Padding: 0
        kdc-options: 40810000
        realm: INTERNAL.ZERODAY.LAB
        sname
            name-type: kRB5-NT-SRV-INST (2)
            sname-string: 2 items
                SNameString: cifs
                SNameString: isql1.internal.zeroday.lab
        till: 2037-09-13 02:48:05 (UTC)
        nonce: 1583384945
        etype: 5 items
            ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
            ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
            ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
            ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
        enc-authorization-data
            etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            cipher: 26b5eac23c565da59aeb77a5b02c6c246d4057c8ec23beb6…
```

- ● TGS-REQ message type (12)
- ● TGS-REQ PA Data section
- ● AP-REQ message type (14)
- ● Requesting users TGT
- ● Authenticator (Encrypted using the TGT session key)
- ● PA PAC Options (Always the same)
- ● Various options for the different message types
- ● Server name (contains the service and host the ticket is for)
- ● Encrypted authorization data – used when requesting service tickets for services on remote hosts

Pre-Authentication

- Genuine AS-REQ’s always first send an AS-REQ without pre-authentication

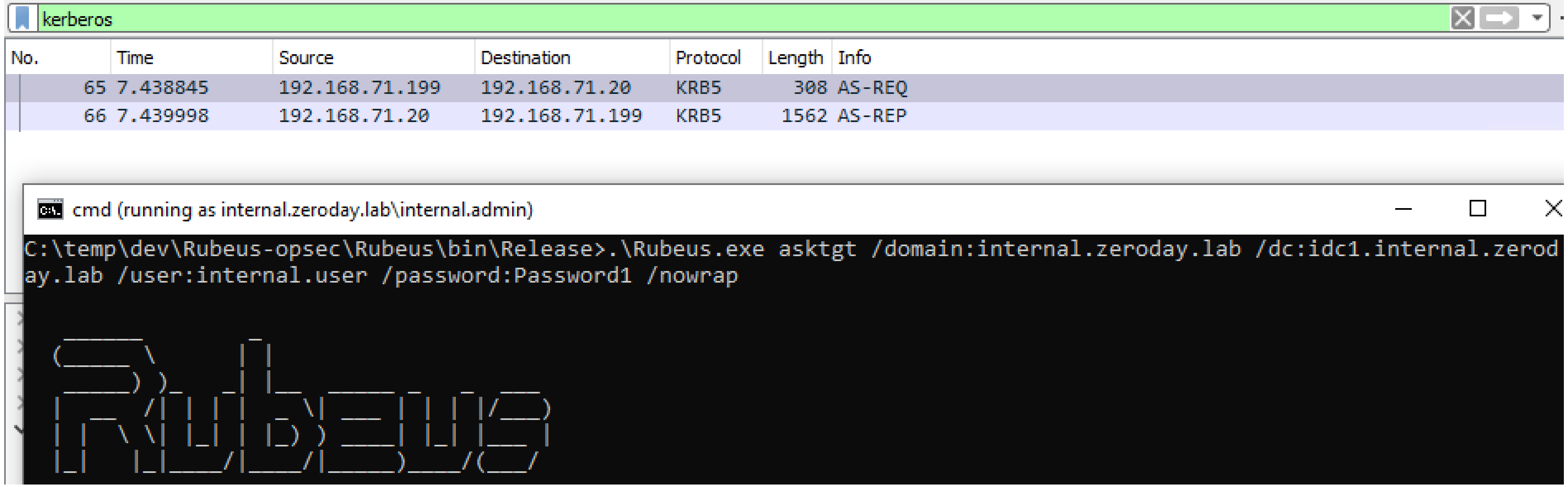


```
70 12.470106     192.168.71.199   192.168.71.20    KRB5       307 AS-REQ
71 12.470902     192.168.71.20    192.168.71.199   KRB5       275 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
78 12.478838     192.168.71.199   192.168.71.20    KRB5       387 AS-REQ
79 12.479854     192.168.71.20    192.168.71.199   KRB5      1712 AS-REP
```

- If the account requires pre-authentication, a second AS-REQ is sent with the PA-ENC-TIMESTAMP PA-DATA section, which is encrypted with the accounts password hash

Pre-Authentication – Abuse Tools

- While impacket's getTGT.py automatically sends the first AS-REQ without pre-authentication, neither Rubeus or kekeo do



No.	Time	Source	Destination	Protocol	Length	Info
65	7.438845	192.168.71.199	192.168.71.20	KRB5	308	AS-REQ
66	7.439998	192.168.71.20	192.168.71.199	KRB5	1562	AS-REP

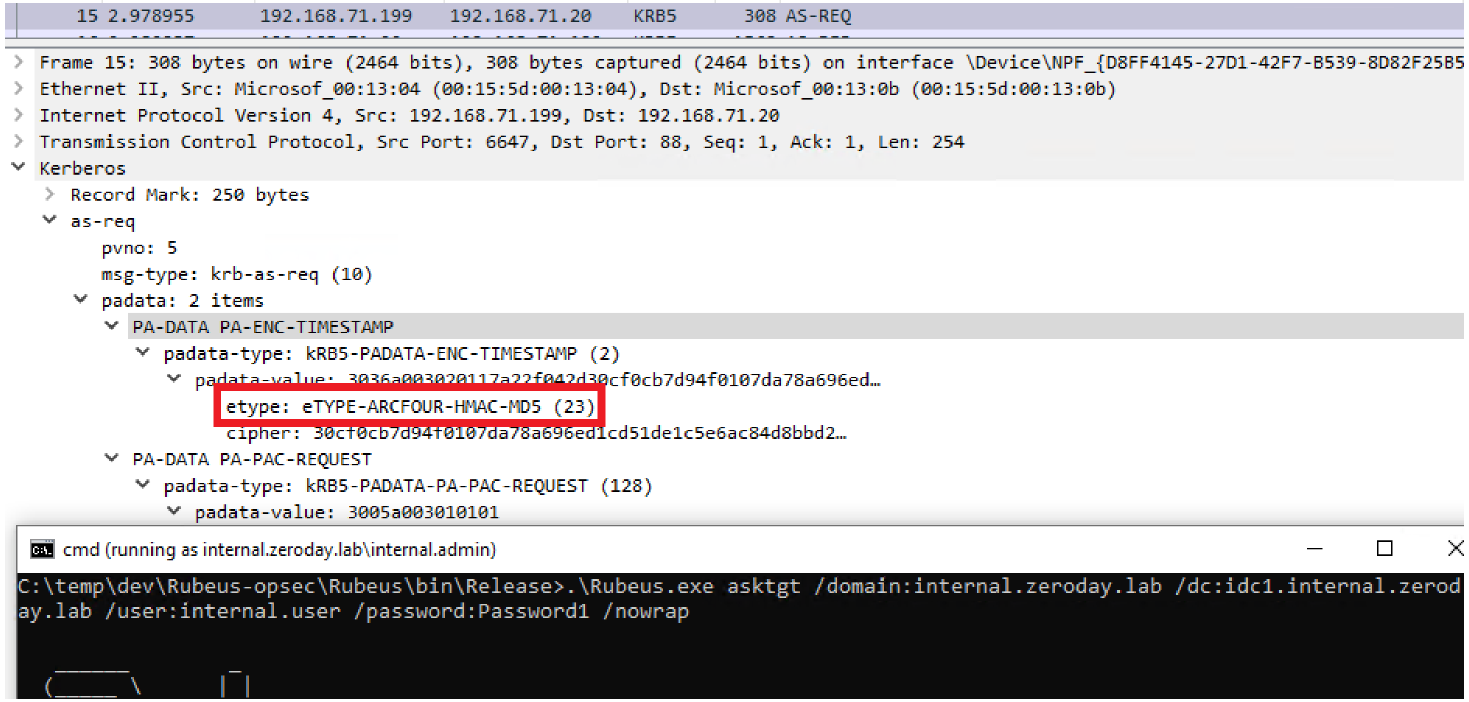
```
C:\temp\dev\Rubeus-opsec\Rubeus\bin\Release>.\Rubeus.exe asktgt /domain:internal.zeroday.lab /dc:idc1.internal.zeroday.lab /user:internal.user /password:Password1 /nowrap

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/
```

Encryption Type

- The encryption type used to encrypt most encrypted sections of genuine Kerberos messages is AES256 (18)

- Rubeus, kekeo and impacket all support multiple encryption types but are often used with RC4 (23)

- This is the easiest indicator that one of these tools is likely in use



```
   15 2.978955      192.168.71.199    192.168.71.20    KRB5      308 AS-REQ
> Frame 15: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface \Device\NPF_{D8FF4145-27D1-42F7-B539-8D82F25B5
> Ethernet II, Src: Microsof_00:13:04 (00:15:5d:00:13:04), Dst: Microsof_00:13:0b (00:15:5d:00:13:0b)
> Internet Protocol Version 4, Src: 192.168.71.199, Dst: 192.168.71.20
> Transmission Control Protocol, Src Port: 6647, Dst Port: 88, Seq: 1, Ack: 1, Len: 254
v Kerberos
  > Record Mark: 250 bytes
  v as-req
      pvno: 5
      msg-type: krb-as-req (10)
    v padata: 2 items
      v PA-DATA PA-ENC-TIMESTAMP
        v padata-type: kRB5-PADATA-ENC-TIMESTAMP (2)
          v padata-value: 3036a003020117a22f042d30cf0cb7d94f0107da78a696ed…
              etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
              cipher: 30cf0cb7d94f0107da78a696ed1cd51de1c5e6ac84d8bbd2…
      v PA-DATA PA-PAC-REQUEST
        v padata-type: kRB5-PADATA-PA-PAC-REQUEST (128)
          v padata-value: 3005a003010101
```

cmd (running as internal.zeroday.lab\internal.admin)

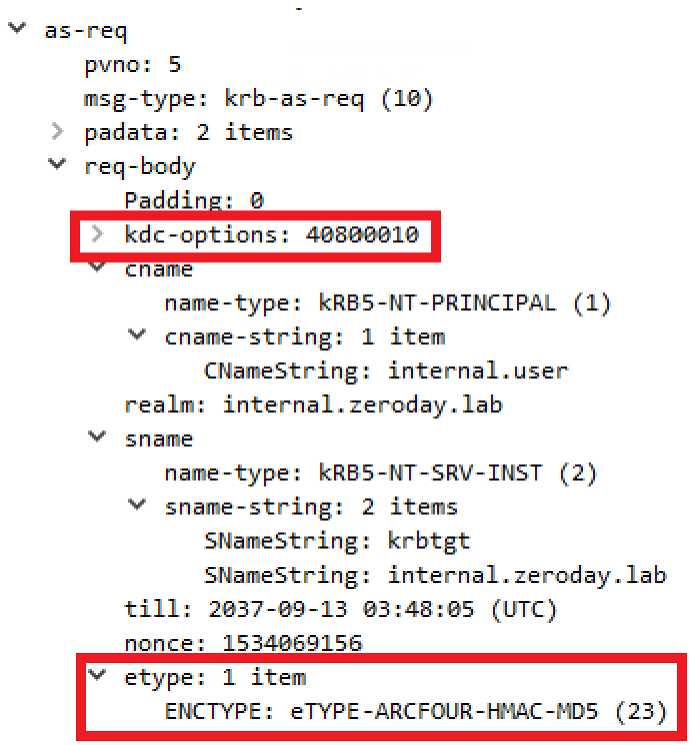
```
C:\temp\dev\Rubeus-opsec\Rubeus\bin\Release>.\Rubeus.exe asktgt /domain:internal.zeroday.lab /dc:idc1.internal.zerod
ay.lab /user:internal.user /password:Password1 /nowrap
```

Rubeus AS-REQ Indicators

- KDC options differ from real traffic with canonicalize disabled
- Incorrect supported etypes specified, genuine AS-REQ’s includes 6 supported etypes

Missing

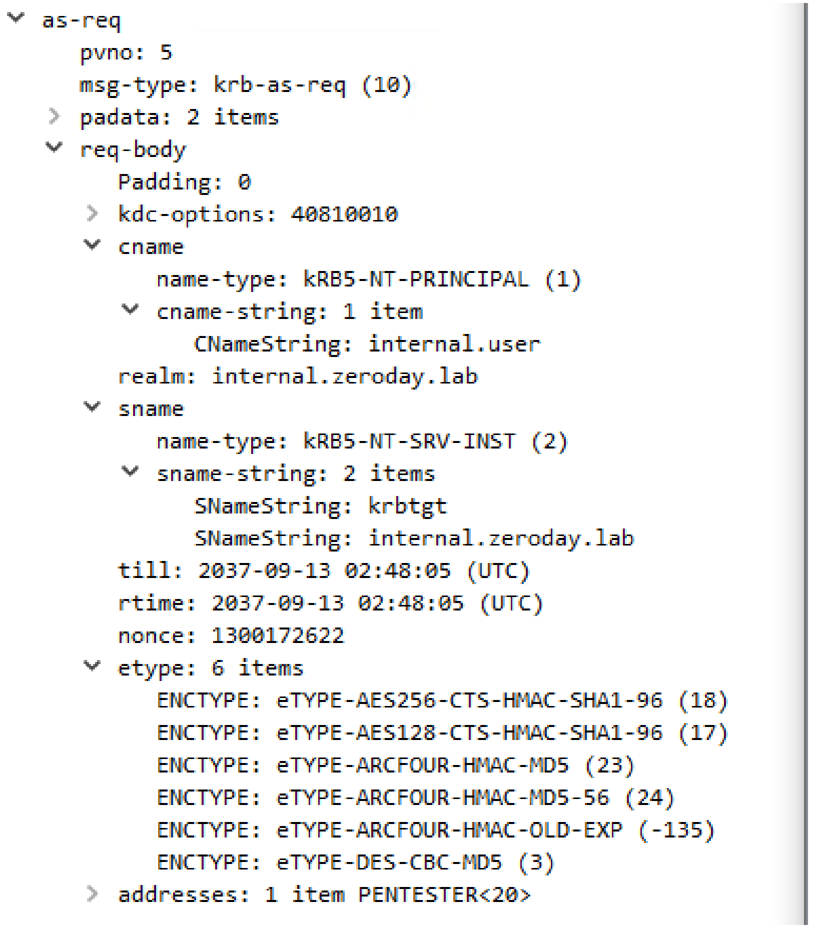
- rtime (renew time) field
- addresses field



```
as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 2 items
    req-body
        Padding: 0
        kdc-options: 40800010
        cname
            name-type: kRB5-NT-PRINCIPAL (1)
            cname-string: 1 item
                CNameString: internal.user
        realm: internal.zeroday.lab
        sname
            name-type: kRB5-NT-SRV-INST (2)
            sname-string: 2 items
                SNameString: krbtgt
                SNameString: internal.zeroday.lab
        till: 2037-09-13 03:48:05 (UTC)
        nonce: 1534069156
        etype: 1 item
            ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

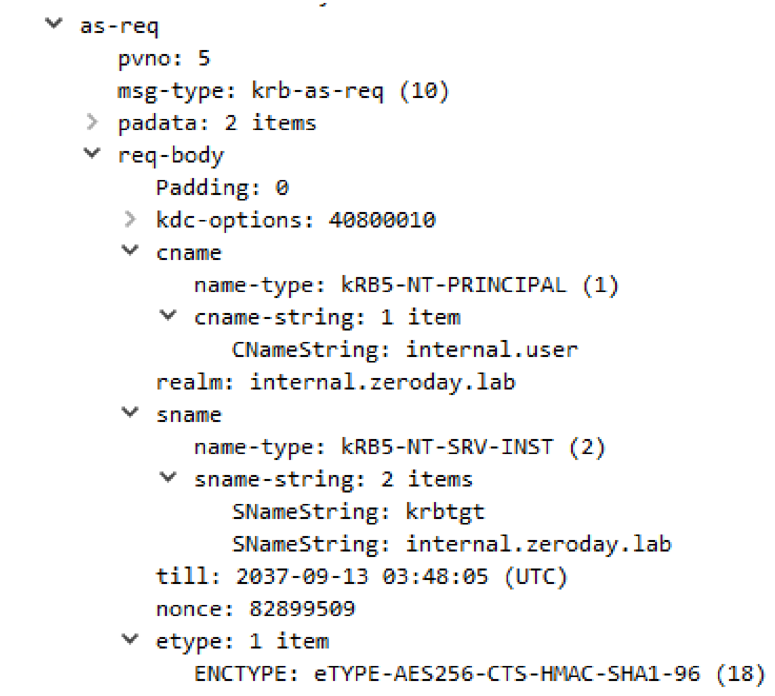
Rubeus AS-REQ Indicators – Continued

Genuine AS-REQ



```
˅ as-req
    pvno: 5
    msg-type: krb-as-req (10)
  > padata: 2 items
  ˅ req-body
      Padding: 0
    > kdc-options: 40810010
    ˅ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ˅ cname-string: 1 item
          CNameString: internal.user
      realm: internal.zeroday.lab
    ˅ sname
        name-type: kRB5-NT-SRV-INST (2)
      ˅ sname-string: 2 items
          SNameString: krbtgt
          SNameString: internal.zeroday.lab
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 1300172622
    ˅ etype: 6 items
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
        ENCTYPE: eTYPE-DES-CBC-MD5 (3)
    > addresses: 1 item PENTESTER<20>
```

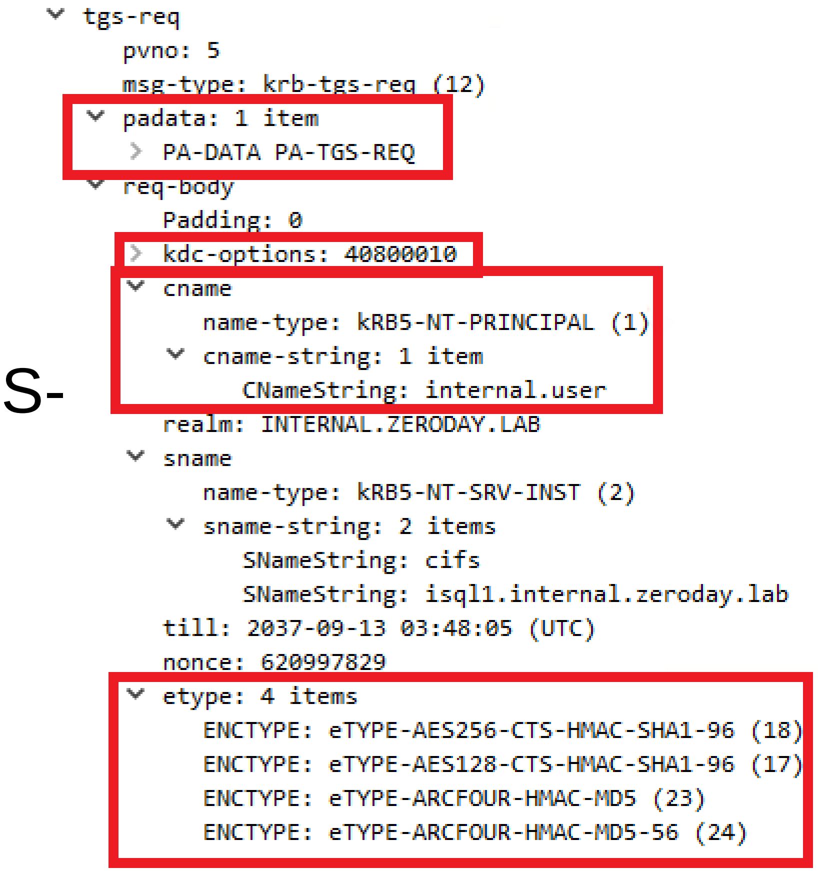
Rubeus AS-REQ



```
˅ as-req
    pvno: 5
    msg-type: krb-as-req (10)
  > padata: 2 items
  ˅ req-body
      Padding: 0
    > kdc-options: 40800010
    ˅ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ˅ cname-string: 1 item
          CNameString: internal.user
      realm: internal.zeroday.lab
    ˅ sname
        name-type: kRB5-NT-SRV-INST (2)
      ˅ sname-string: 2 items
          SNameString: krbtgt
          SNameString: internal.zeroday.lab
      till: 2037-09-13 03:48:05 (UTC)
      nonce: 82899509
    ˅ etype: 1 item
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
```

Rubeus TGS-REQ Indicators

- PA DATA does not include the PA-PAC-OPTIONS field
- KDC options differ from real traffic with canonicalize disabled
- Incorrect supported etypes specified, genuine TGS-REQ's includes 5 supported etypes
- cname field included when not in genuine traffic



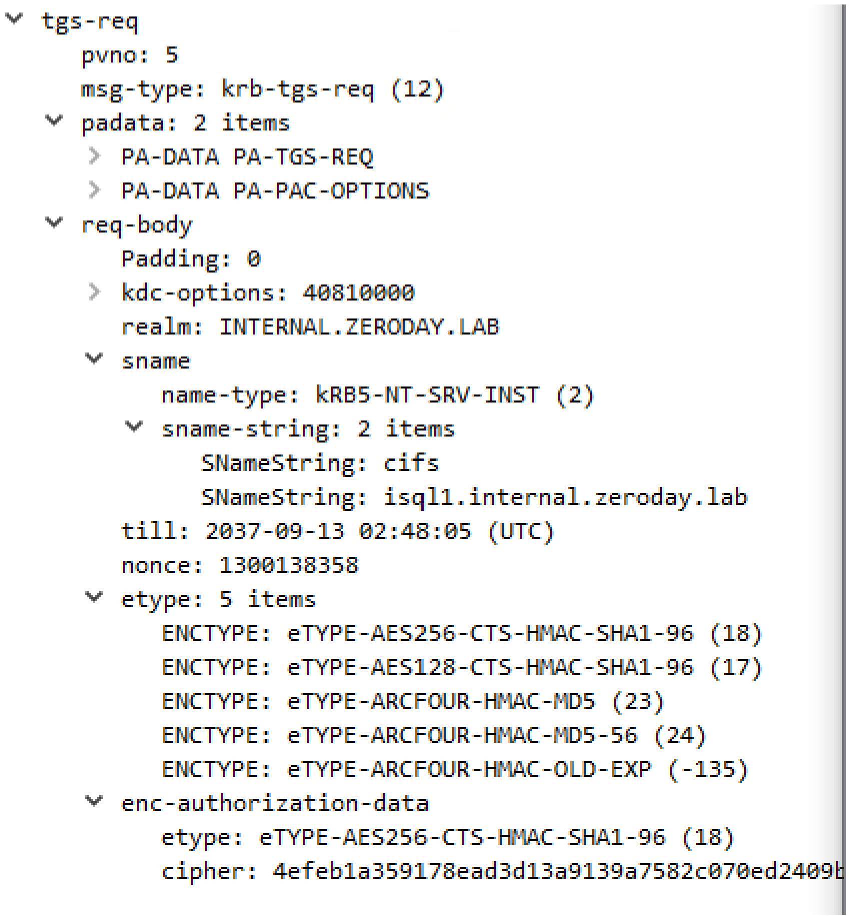
```
v tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
  v padata: 1 item
    > PA-DATA PA-TGS-REQ
  v req-body
      Padding: 0
    > kdc-options: 40800010
    v cname
        name-type: kRB5-NT-PRINCIPAL (1)
      v cname-string: 1 item
          CNameString: internal.user
      realm: INTERNAL.ZERODAY.LAB
    v sname
        name-type: kRB5-NT-SRV-INST (2)
      v sname-string: 2 items
          SNameString: cifs
          SNameString: isql1.internal.zeroday.lab
      till: 2037-09-13 03:48:05 (UTC)
      nonce: 620997829
    v etype: 4 items
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
```

Missing

- enc-authorization-data field

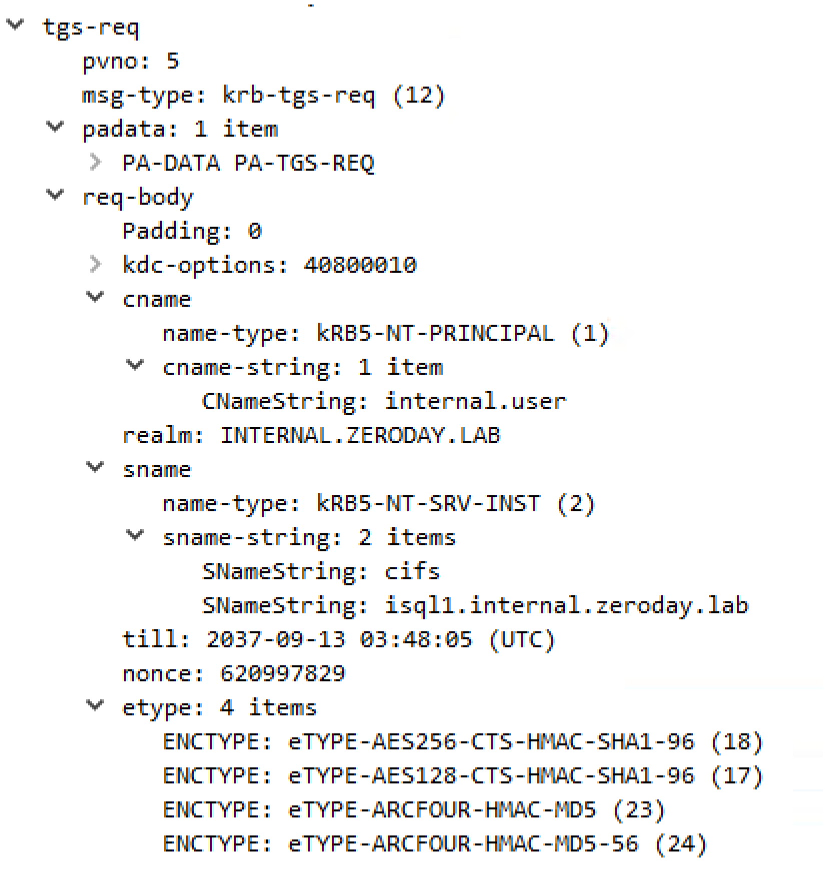
Rubeus TGS-REQ Indicators - Continued

Genuine TGS-REQ



```
⌄ tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
  ⌄ padata: 2 items
    › PA-DATA PA-TGS-REQ
    › PA-DATA PA-PAC-OPTIONS
  ⌄ req-body
      Padding: 0
    › kdc-options: 40810000
      realm: INTERNAL.ZERODAY.LAB
    ⌄ sname
        name-type: kRB5-NT-SRV-INST (2)
      ⌄ sname-string: 2 items
          SNameString: cifs
          SNameString: isql1.internal.zeroday.lab
      till: 2037-09-13 02:48:05 (UTC)
      nonce: 1300138358
    ⌄ etype: 5 items
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
    ⌄ enc-authorization-data
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        cipher: 4efeb1a359178ead3d13a9139a7582c070ed2409b
```

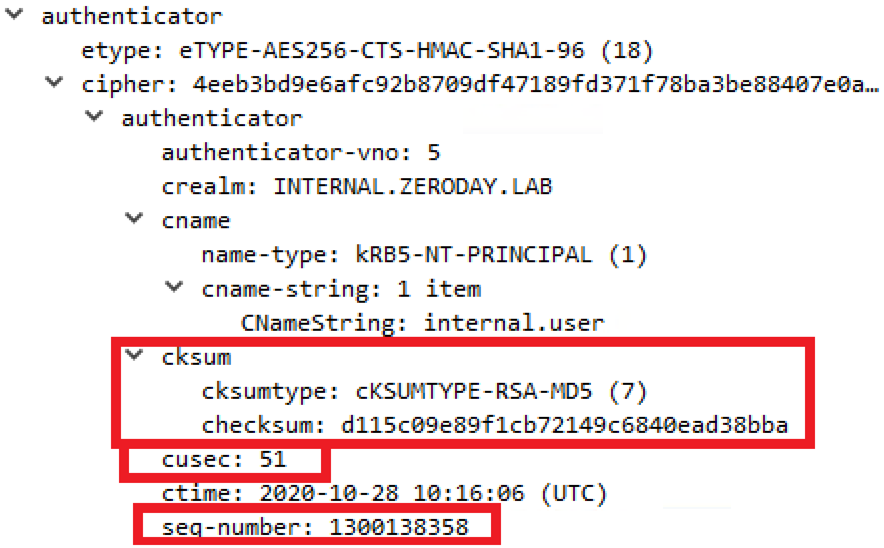
Rubeus TGS-REQ



```
⌄ tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
  ⌄ padata: 1 item
    › PA-DATA PA-TGS-REQ
  ⌄ req-body
      Padding: 0
    › kdc-options: 40800010
    ⌄ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ⌄ cname-string: 1 item
          CNameString: internal.user
      realm: INTERNAL.ZERODAY.LAB
    ⌄ sname
        name-type: kRB5-NT-SRV-INST (2)
      ⌄ sname-string: 2 items
          SNameString: cifs
          SNameString: isql1.internal.zeroday.lab
      till: 2037-09-13 03:48:05 (UTC)
      nonce: 620997829
    ⌄ etype: 4 items
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
```

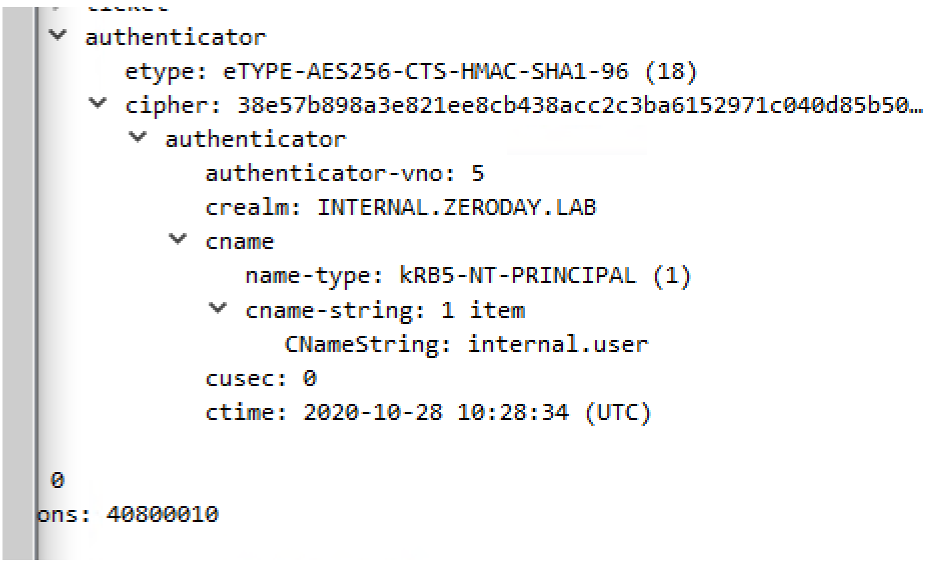
Rubeus TGS-REQ Indicators - Authenticator

Genuine Authenticator



```
⌄ authenticator
    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
  ⌄ cipher: 4eeb3bd9e6afc92b8709df47189fd371f78ba3be88407e0a…
    ⌄ authenticator
        authenticator-vno: 5
        crealm: INTERNAL.ZERODAY.LAB
      ⌄ cname
          name-type: kRB5-NT-PRINCIPAL (1)
        ⌄ cname-string: 1 item
            CNameString: internal.user
      ⌄ cksum
          cksumtype: cKSUMTYPE-RSA-MD5 (7)
          checksum: d115c09e89f1cb72149c6840ead38bba
        cusec: 51
        ctime: 2020-10-28 10:16:06 (UTC)
        seq-number: 1300138358
```

Rubeus Authenticator

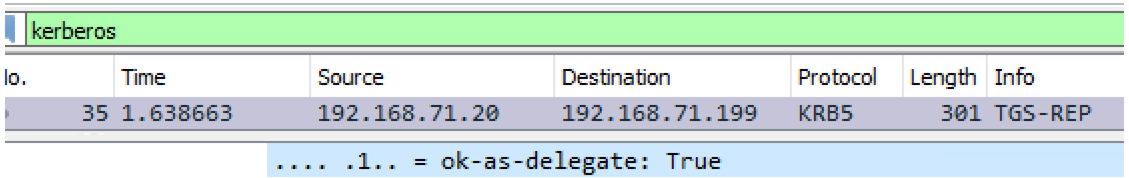


```
⌄ authenticator
    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
  ⌄ cipher: 38e57b898a3e821ee8cb438acc2c3ba6152971c040d85b50…
    ⌄ authenticator
        authenticator-vno: 5
        crealm: INTERNAL.ZERODAY.LAB
      ⌄ cname
          name-type: kRB5-NT-PRINCIPAL (1)
        ⌄ cname-string: 1 item
            CNameString: internal.user
        cusec: 0
        ctime: 2020-10-28 10:28:34 (UTC)


0
ons: 40800010
```

Unlikely to be monitored for as decrypting all authenticators on the fly would be a massive overhead

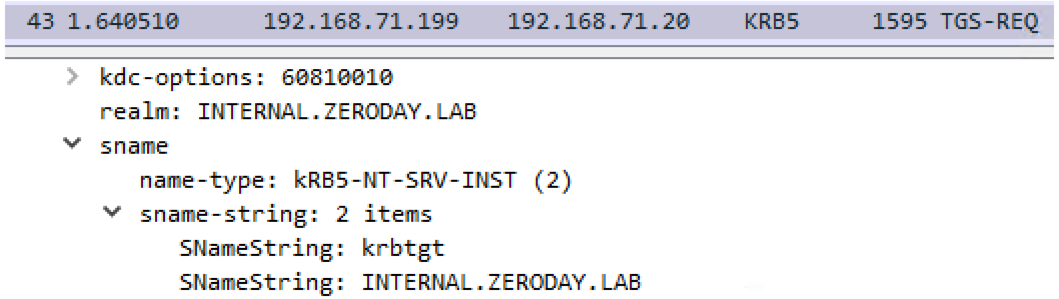
Rubeus TGS-REQ Indicators – Unconstrained Delegation

TGS-REP’s (replies to TGS-REQ’s) will set the ok-as-delegate bit within the flags field of the enc-part section if the account with the SPN is configured for unconstrained delegation



```
kerberos
lo.      Time        Source          Destination      Protocol  Length  Info
      35 1.638663    192.168.71.20   192.168.71.199   KRB5         301  TGS-REP
                .... .1.. = ok-as-delegate: True
```

This results in a second TGS-REQ for krbtgt/domain.com (a forwardable TGT) being requested (to include in the connection to the service)



```
 43 1.640510       192.168.71.199   192.168.71.20     KRB5       1595 TGS-REQ

  > kdc-options: 60810010
    realm: INTERNAL.ZERODAY.LAB
  v sname
      name-type: kRB5-NT-SRV-INST (2)
    v sname-string: 2 items
        SNameString: krbtgt
        SNameString: INTERNAL.ZERODAY.LAB
```

AS-REQ Comparison Table

Indicator	Genuine	Rubeus (asktgt)	Kekeo (tgt::ask)	Impacket
without pre-auth	✓	✗	✗	✓
kdc-options	40810010	40800010	40800010	50800000
etypes	-135, 3, 17, 18, 23, 24	18	17, 18, 23	18
rtime	✓	✗	✗	✓
addresses	✓	✗	✗	✗
till	2037-09-13 02:48:05 (UTC)	2037-09-13 02:48:05 (UTC)	2037-09-13 02:48:05 (UTC)	+ 1 day

TGS-REQ Comparison Table

Indicator	Genuine	Rubeus (asktgs)	Kekeo (tgs::ask)	Impacket
PA-PAC-OPTIONS	✓	✗	✗	✗
kdc-options	40810000	40800010	40800010	40810010
etypes	-135, 17, 18, 23, 24	17, 18, 23, 24	17, 18, 23	3, 16, 18, 23
cname	✗	✓	✓	✗
enc-authorization-data	✓	✗	✗	✗
unconstrained TGS-REQ	✓	✗	✗	✗
till	2037-09-13 02:48:05 (UTC)	2037-09-13 02:48:05 (UTC)	2037-09-13 02:48:05 (UTC)	+ 1 day
authenticator cksum	✓	✗	✗	✗
authenticator cusec	✓	Always 0	Always 0	✓
authenticator seq-number	✓	✗	✗	✗

S4U2Self TGS-REQ Comparison Table

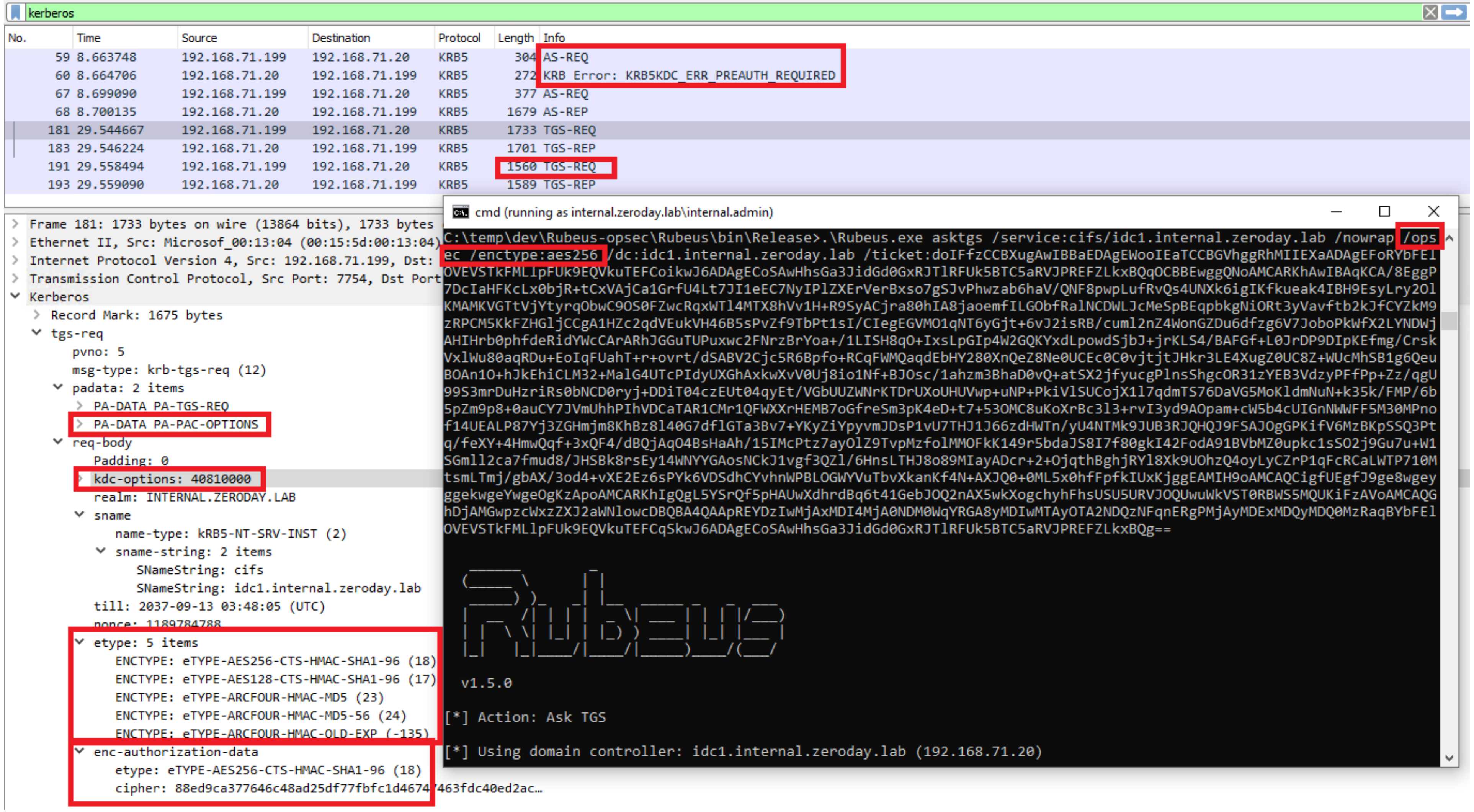
Indicator	Genuine	Rubeus	Kekeo	Impacket
PA-S4U-X509-USER	✓	✗	✗	✗
kdc-options	40810000	40800018	40800018	40810000
etypes	-135, 17, 18, 23, 24	17, 18, 23, 24	17, 18, 23	18, 23
cname	✗	✓	✓	✗
till	+ 15 minutes	2037-09-13 02:48:05 (UTC)	2037-09-13 02:48:05 (UTC)	+ 1 day
PA USER name-type	Enterprise Principal (10)	Enterprise Principal (10)	NT Principal (1)	NT Principal (1)
sname name-type	NT Principal (1)	NT Principal (1)	NT Principal (1)	Unknown (0)
authenticator cksum	✓	✗	✗	✗
authenticator cusec	✓	Always 0	Always 0	✓
authenticator seq-number	✓	✗	✗	✗

S4U2Proxy TGS-REQ Comparison Table

Indicator	Genuine	Rubeus	Kekeo	Impacket
PA-PAC-OPTIONS	✓	✓	✗	✓
kdc-options	40830000	40820010	40820010	40830000
etypes	-135, 17, 18, 23, 24	17, 18, 23	17, 18, 23	3, 16, 18, 23
cname	✗	✓	✗	✗
till	+ 15 minutes	2037-09-13 02:48:05 (UTC)	2037-09-13 02:48:05 (UTC)	+ 1 day
enc-authorization-data	✓	✗	✗	✗
authenticator cksum	✓	✗	✗	✗
authenticator cusec	✓	Always 0	Always 0	✓
authenticator seq-number	✓	✗	✗	✗

Resolving Differences

ASKTGT followed by ASKTGS both using the new */opsec* flag



```
No.   Time        Source          Destination     Protocol  Length  Info
   59 8.663748    192.168.71.199  192.168.71.20   KRB5        304   AS-REQ
   60 8.664706    192.168.71.20   192.168.71.199  KRB5        272   KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
   67 8.699090    192.168.71.199  192.168.71.20   KRB5        377   AS-REQ
   68 8.700135    192.168.71.20   192.168.71.199  KRB5       1679   AS-REP
  181 29.544667   192.168.71.199  192.168.71.20   KRB5       1733   TGS-REQ
  183 29.546224   192.168.71.20   192.168.71.199  KRB5       1701   TGS-REP
  191 29.558494   192.168.71.199  192.168.71.20   KRB5       1560   TGS-REQ
  193 29.559090   192.168.71.20   192.168.71.199  KRB5       1589   TGS-REP
```

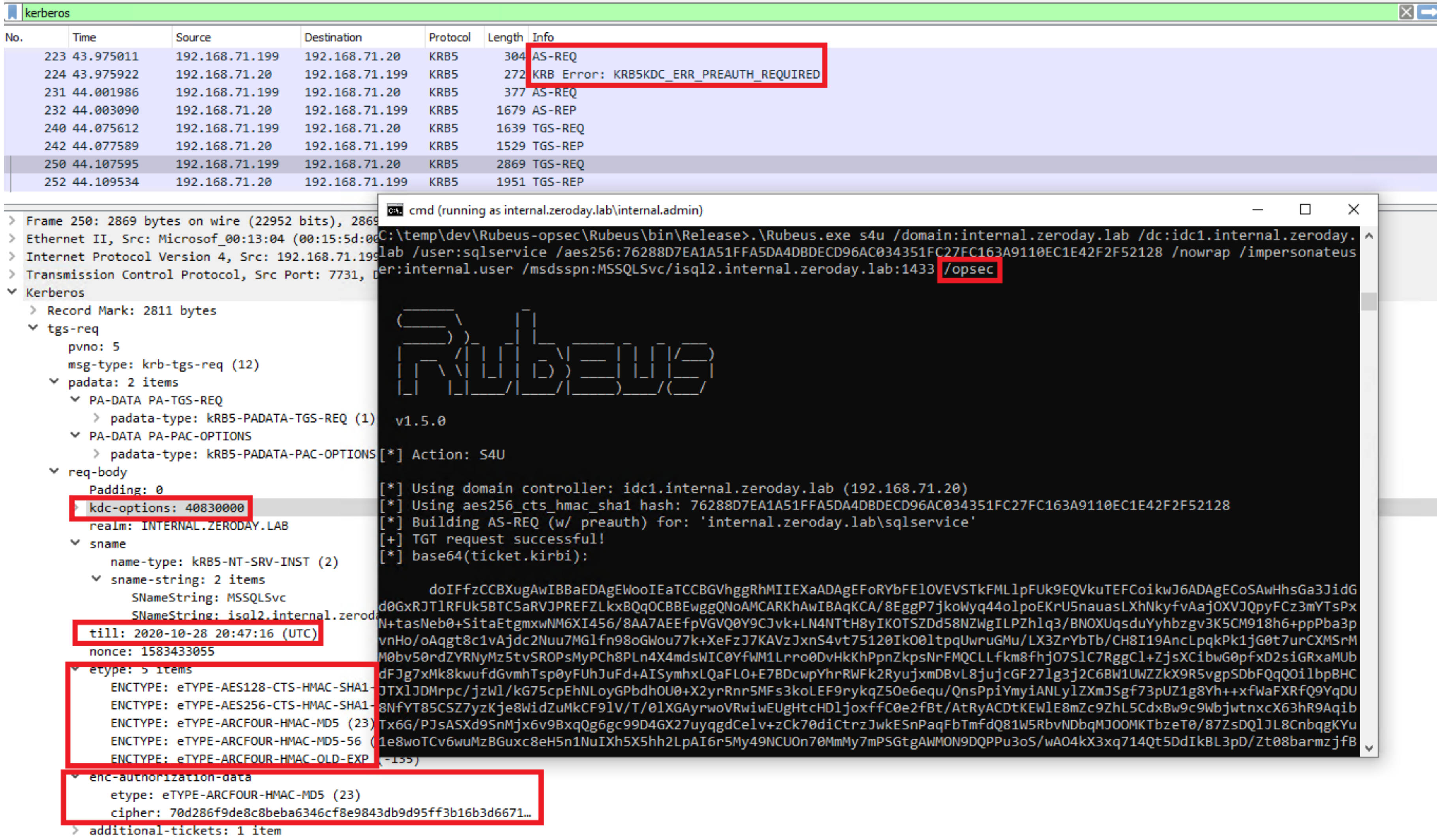
```
> Frame 181: 1733 bytes on wire (13864 bits), 1733 bytes
> Ethernet II, Src: Microsof_00:13:04 (00:15:5d:00:13:04)
> Internet Protocol Version 4, Src: 192.168.71.199, Dst:
> Transmission Control Protocol, Src Port: 7754, Dst Port
v Kerberos
  > Record Mark: 1675 bytes
  v tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    v padata: 2 items
      > PA-DATA PA-TGS-REQ
      > PA-DATA PA-PAC-OPTIONS
    v req-body
        Padding: 0
      > kdc-options: 40810000
        realm: INTERNAL.ZERODAY.LAB
      v sname
          name-type: kRB5-NT-SRV-INST (2)
        v sname-string: 2 items
            SNameString: cifs
            SNameString: idc1.internal.zeroday.lab
        till: 2037-09-13 03:48:05 (UTC)
        nonce: 1189784788
      v etype: 5 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
      v enc-authorization-data
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          cipher: 88ed9ca377646c48ad25df77fbfc1d4674f463fdc40ed2ac…
```

```
C:\temp\dev\Rubeus-opsec\Rubeus\bin\Release>.\Rubeus.exe asktgs /service:cifs/idc1.internal.zeroday.lab /nowrap /ops
ec /enctype:aes256 /dc:idc1.internal.zeroday.lab /ticket:doIFfzCCBXugAwIBBaEDAgEWooIEaTCCBGVhggRhMIIEXaADAgEFoRYbFEl
OVEVSTkFMLlpFUk9EQVkuTEFCoikwJ6ADAgECoSAwHhsGa3JidGd0GxRJTlRFUk5BTC5aRVJPREFZLkxBQqOCBBEwggQNoAMCARKhAwIBAqKCA/8EggP
7DcIaHFKcLx0bjR+tCxVAjCa1GrfU4Lt7JI1eEC7NyIPlZXErVerBxso7gSJvPhwzab6haV/QNF8pwpLufRvQs4UNXk6igIKfkueak4IBH9EsyLry2Ol
KMAMKVGTtVjYtyrqObwC9OS0FZwcRqxWTl4MTX8hVv1H+R9SyACjra80hIA8jaoemfILGObfRalNCDWLJcMeSpBEqpbkgNiORt3yVavftb2kJfCYZkM9
zRPCM5KkFZHGljCCgA1HZc2qdVEukVH46B5sPvZf9TbPt1sI/CIegEGVMO1qNT6yGjt+6vJ2isRB/cuml2nZ4WonGZDu6dfzg6V7JoboPkWfX2LYNDWj
AHIHrb0phfdeRidYWcCArARhJGGuTUPuxwc2FNrzBrYoa+/1LISH8qO+IxsLpGIp4W2GQKYxdLpowdSjbJ+jrKLS4/BAFGf+L0JrDP9DIpKEfmg/Crsk
VxlWu80aqRDu+EoIqFUahT+r+ovrt/dSABV2Cjc5R6Bpfo+RCqFWMQaqdEbHY280XnQeZ8Ne0UCEc0C0vjtjtJHkr3LE4XugZ0UC8Z+WUcMhSB1g6Qeu
BOAn1O+hJkEhiCLM32+MalG4UTcPIdyUXGhAxkwXvV0Uj8io1Nf+BJOsc/1ahzm3BhaD0vQ+atSX2jfyucgPlnsShgcOR31zYEB3VdzyPFfPp+Zz/qgU
99S3mrDuHzriRs0bNCD0ryj+DDiT04czEUt04qyEt/VGbUUZWNrKTDrUXoUHUVwp+uNP+PkiVlSUCojX1l7qdmTS76DaVG5MoKldmNuN+k35k/FMP/6b
5pZm9p8+0auCY7JVmUhhPIhVDCaTAR1CMr1QFWXXrHEMB7oGfreSm3pK4eD+t7+53OMC8uKoXrBc3l3+rvI3yd9AOpam+cW5b4cUIGnNWWFF5M30MPno
f14UEALP87Yj3ZGHmjm8KhBz8l40G7dflGTa3Bv7+YKyZiYpyvmJDsP1vU7THJ1J66zdHWTn/yU4NTMk9JUB3RJQHQJ9FSAJOgGPKifV6MzBKpSSQ3Pt
q/feXY+4HmwQqf+3xQF4/dBQjAqO4BsHaAh/15IMcPtz7ayOlZ9TvpMzfolMMOFkK149r5bdaJS8I7f80gkI42FodA91BVbMZ0upkc1sSO2j9Gu7u+W1
SGmll2ca7fmud8/JHSBk8rsEy14WNYYGAosNCkJ1vgf3QZl/6HnsLTHJ8o89MIayADcr+2+OjqthBghjRYl8Xk9UOhzQ4oyLyCZrP1qFcRCaLWTP710M
tsmLTmj/gbAX/3od4+vXE2Ez6sPYk6VDSdhCYvhnWPBLOGWYVuTbvXkanKf4N+AXJQ0+0ML5x0hfFpfkIUxKjggEAMIH9oAMCAQCigfUEgfJ9ge8wgey
ggekwgeYwgeOgKzApoAMCARKhIgQgL5YSrQf5pHAUwXdhrdBq6t41GebJOQ2nAX5wkXogchyhFhsUSU5URVJOQUwuWkVST0RBWS5MQUKiFzAVoAMCAQG
hDjAMGwpzcWxzZXJ2aWNlowcDBQBA4QAApREYDzIwMjAxMDI4MjA0NDM0WqYRGA8yMDIwMTAyOTA2NDQzNFqnERgPMjAyMDExMDQyMDQ0MzRaqBYbFEl
OVEVSTkFMLlpFUk9EQVkuTEFCqSkwJ6ADAgECoSAwHhsGa3JidGd0GxRJTlRFUk5BTC5aRVJPREFZLkxBQg==

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.5.0

[*] Action: Ask TGS

[*] Using domain controller: idc1.internal.zeroday.lab (192.168.71.20)
```

Resolving Differences – S4U

S4U using the new */opsec* flag

PA-S4U-X509-USER for the S4U2Self is still a work in progress



```
No.  Time       Source          Destination     Protocol  Length  Info
 223 43.975011  192.168.71.199  192.168.71.20   KRB5        304  AS-REQ
 224 43.975922  192.168.71.20   192.168.71.199  KRB5        272  KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
 231 44.001986  192.168.71.199  192.168.71.20   KRB5        377  AS-REQ
 232 44.003090  192.168.71.20   192.168.71.199  KRB5       1679  AS-REP
 240 44.075612  192.168.71.199  192.168.71.20   KRB5       1639  TGS-REQ
 242 44.077589  192.168.71.20   192.168.71.199  KRB5       1529  TGS-REP
 250 44.107595  192.168.71.199  192.168.71.20   KRB5       2869  TGS-REQ
 252 44.109534  192.168.71.20   192.168.71.199  KRB5       1951  TGS-REP
```

```
> Frame 250: 2869 bytes on wire (22952 bits), 2869
> Ethernet II, Src: Microsof_00:13:04 (00:15:5d:00
> Internet Protocol Version 4, Src: 192.168.71.199
> Transmission Control Protocol, Src Port: 7731, D
v Kerberos
  > Record Mark: 2811 bytes
  v tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    v padata: 2 items
      v PA-DATA PA-TGS-REQ
        > padata-type: kRB5-PADATA-TGS-REQ (1)
      v PA-DATA PA-PAC-OPTIONS
        > padata-type: kRB5-PADATA-PAC-OPTIONS
    v req-body
        Padding: 0
      > kdc-options: 40830000
        realm: INTERNAL.ZERODAY.LAB
      v sname
          name-type: kRB5-NT-SRV-INST (2)
        v sname-string: 2 items
            SNameString: MSSQLSvc
            SNameString: isql2.internal.zeroda
        till: 2020-10-28 20:47:16 (UTC)
        nonce: 1583433055
      v etype: 5 items
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
      v enc-authorization-data
          etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
          cipher: 70d286f9de8c8beba6346cf8e9843db9d95ff3b16b3d6671…
      > additional-tickets: 1 item
```

cmd (running as internal.zeroday.lab\internal.admin)

```
C:\temp\dev\Rubeus-opsec\Rubeus\bin\Release>.\Rubeus.exe s4u /domain:internal.zeroday.lab /dc:idc1.internal.zeroday.
lab /user:sqlservice /aes256:76288D7EA1A51FFA5DA4DBDECD96AC034351FC27FC163A9110EC1E42F2F52128 /nowrap /impersonateus
er:internal.user /msdsspn:MSSQLSvc/isql2.internal.zeroday.lab:1433 /opsec

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.5.0

[*] Action: S4U

[*] Using domain controller: idc1.internal.zeroday.lab (192.168.71.20)
[*] Using aes256_cts_hmac_sha1 hash: 76288D7EA1A51FFA5DA4DBDECD96AC034351FC27FC163A9110EC1E42F2F52128
[*] Building AS-REQ (w/ preauth) for: 'internal.zeroday.lab\sqlservice'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFfzCCBXugAwIBBaEDAgEWooIEaTCCBGVhggRhMIIEXaADAgEFoRYbFElOVEVSTkFMLlpFUk9EQVkuTEFCoikwJ6ADAgECoSAwHhsGa3JidG
d0GxRJTlRFUk5BTC5aRVJPREFZLkxBQqOCBBEwggQNoAMCARKhAwIBAqKCA/8EggP7jkoWyq44olpoEKrU5nauasLXhNkyfvAajOXVJQpyFCz3mYTsPx
N+tasNeb0+SitaEtgmxwNM6XI456/8AA7AEEfpVGVQ0Y9CJvk+LN4NTtH8yIKOTSZDd58NZWgILPZhlq3/BNOXUqsduYyhbzgv3K5CM918h6+ppPba3p
vnHo/oAqgt8c1vAjdc2Nuu7MGlfn98oGWou77k+XeFzJ7KAVzJxnS4vt75120IkO0ltpqUwruGMu/LX3ZrYbTb/CH8I19AncLpqkPk1jG0t7urCXMSrM
M0bv50rdZYRNyMz5tvSROPsMyPCh8PLn4X4mdsWIC0YfWM1Lrro0DvHkKhPpnZkpsNrFMQCLLfkm8fhjO7SlC7RggCl+ZjsXCibwG0pfxD2siGRxaMUb
dFJg7xMk8kwufdGvmhTsp0yFUhJuFd+AISymhxLQaFLO+E7BDcwpYhrRWFk2RyujxmDBvL8jujcGF27lg3j2C6BW1UWZZkX9R5vgpSDbFQqQOilbpBHC
JTXlJDMrpc/jzWl/kG75cpEhNLoyGPbdhOU0+X2yrRnr5MFs3koLEF9rykqZ5Oe6equ/QnsPpiYmyiANLylZXmJSgf73pUZ1g8Yh++xfWaFXRfQ9YqDU
8NfYT85CSZ7yzKje8WidZuMkCF9lV/T/0lXGAyrwoVRwiwEUgHtcHDljoxffC0e2fBt/AtRyACDtKEWlE8mZc9ZhL5CdxBw9c9WbjwtnxcX63hR9Aqib
Tx6G/PJsASXd9SnMjx6v9BxqQg6gc99D4GX27uyqgdCelv+zCk70diCtrzJwkESnPaqFbTmfdQ81W5RbvNDbqMJOOMKTbzeT0/87ZsDQlJL8CnbqgKYu
1e8woTCv6wuMzBGuxc8eH5n1NuIXh5X5hh2LpAI6r5My49NCUOn70MmMy7mPSGtgAWMON9DQPPu3oS/wAO4kX3xq714Qt5DdIkBL3pD/Zt08barmzjfB
```

ZERODAYLAB®

Resolving Differences – Github PR

The PR has been made:

https://github.com/GhostPack/Rubeus/pull/69

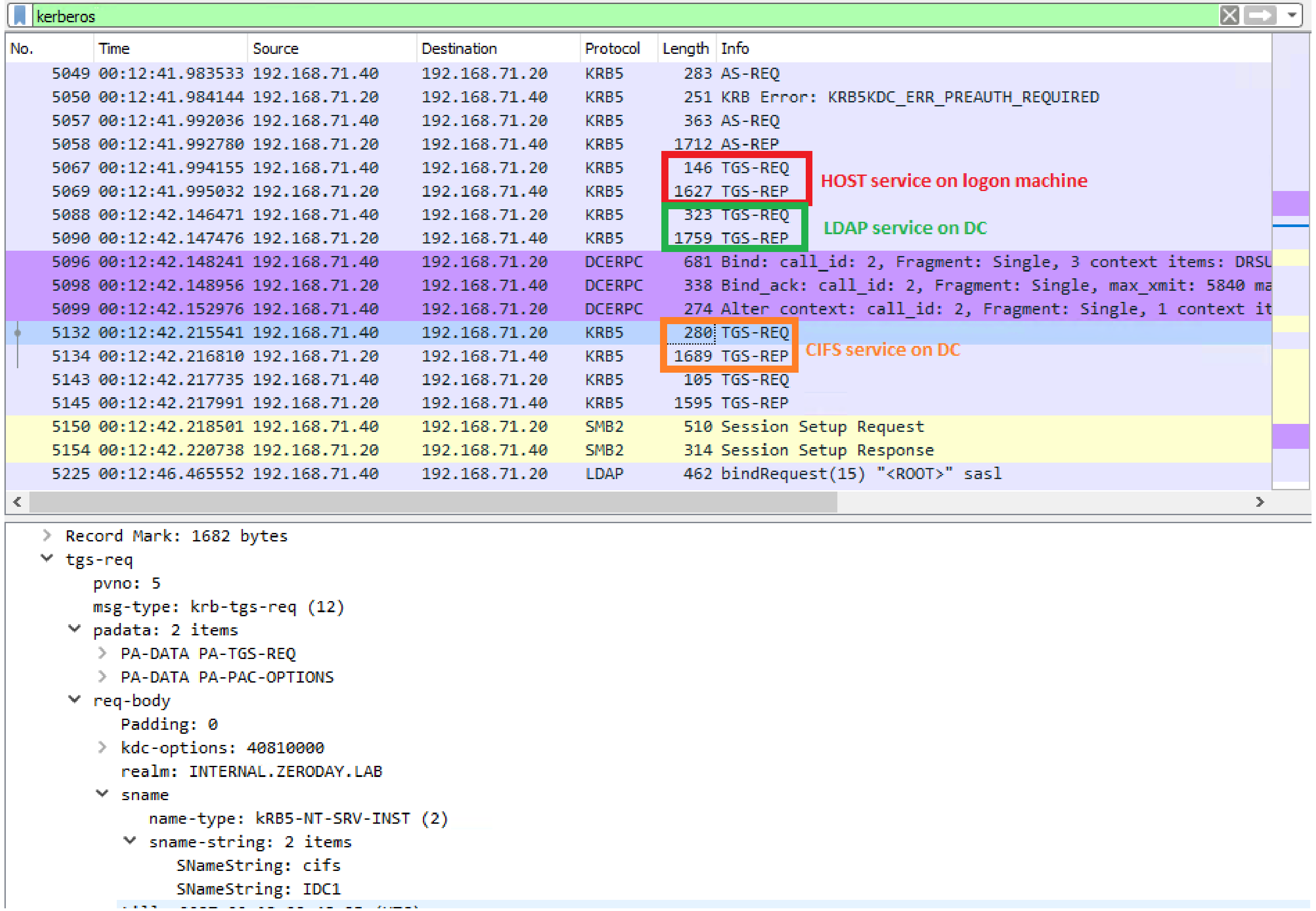
The modified version can be pulled from the “opsec” branch of my forked Rubeus:

https://github.com/0xe7/Rubeus/tree/opsec

Further Considerations

Several service tickets are requested following a genuine login

Perhaps a ***login*** command for Rubeus to implement this instead of *asktgt* for extra stealth



kerberos

```
No.  Time            Source         Destination    Protocol Length Info
5049 00:12:41.983533 192.168.71.40  192.168.71.20  KRB5      283 AS-REQ
5050 00:12:41.984144 192.168.71.20  192.168.71.40  KRB5      251 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
5057 00:12:41.992036 192.168.71.40  192.168.71.20  KRB5      363 AS-REQ
5058 00:12:41.992780 192.168.71.20  192.168.71.40  KRB5     1712 AS-REP
5067 00:12:41.994155 192.168.71.40  192.168.71.20  KRB5      146 TGS-REQ
5069 00:12:41.995032 192.168.71.20  192.168.71.40  KRB5     1627 TGS-REP
5088 00:12:42.146471 192.168.71.40  192.168.71.20  KRB5      323 TGS-REQ
5090 00:12:42.147476 192.168.71.20  192.168.71.40  KRB5     1759 TGS-REP
5096 00:12:42.148241 192.168.71.40  192.168.71.20  DCERPC    681 Bind: call_id: 2, Fragment: Single, 3 context items: DRSU
5098 00:12:42.148956 192.168.71.20  192.168.71.40  DCERPC    338 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 ma
5099 00:12:42.152976 192.168.71.40  192.168.71.20  DCERPC    274 Alter context: call_id: 2, Fragment: Single, 1 context it
5132 00:12:42.215541 192.168.71.40  192.168.71.20  KRB5      280 TGS-REQ
5134 00:12:42.216810 192.168.71.20  192.168.71.40  KRB5     1689 TGS-REP
5143 00:12:42.217735 192.168.71.40  192.168.71.20  KRB5      105 TGS-REQ
5145 00:12:42.217991 192.168.71.20  192.168.71.40  KRB5     1595 TGS-REP
5150 00:12:42.218501 192.168.71.40  192.168.71.20  SMB2      510 Session Setup Request
5154 00:12:42.220738 192.168.71.20  192.168.71.40  SMB2      314 Session Setup Response
5225 00:12:46.465552 192.168.71.40  192.168.71.20  LDAP      462 bindRequest(15) "<ROOT>" sasl
```

HOST service on logon machine

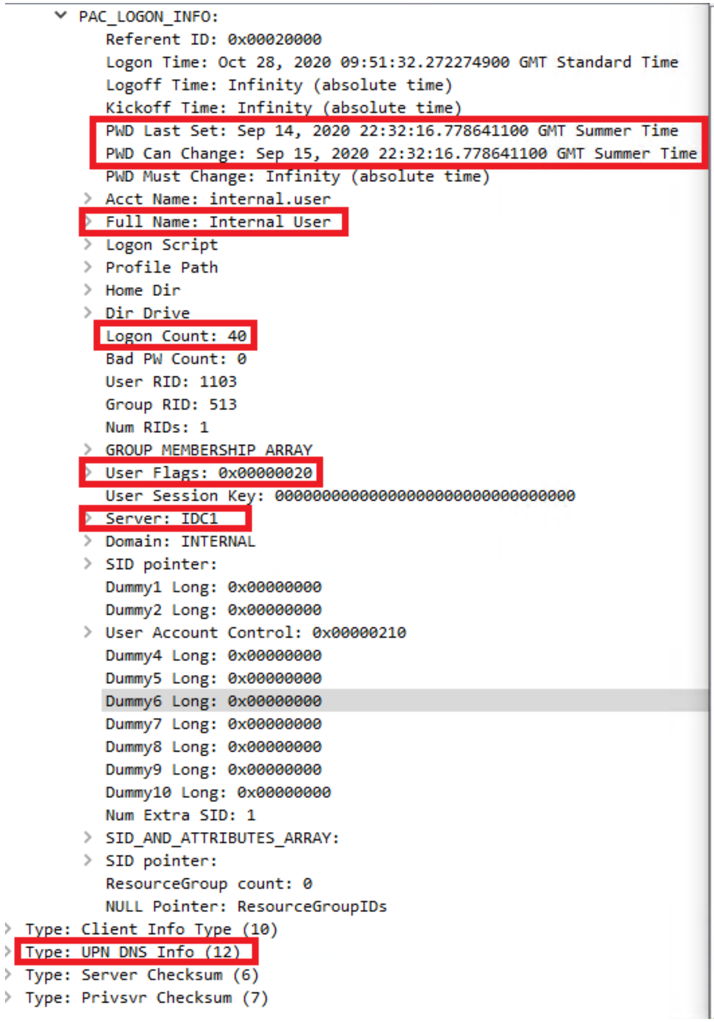
LDAP service on DC

CIFS service on DC

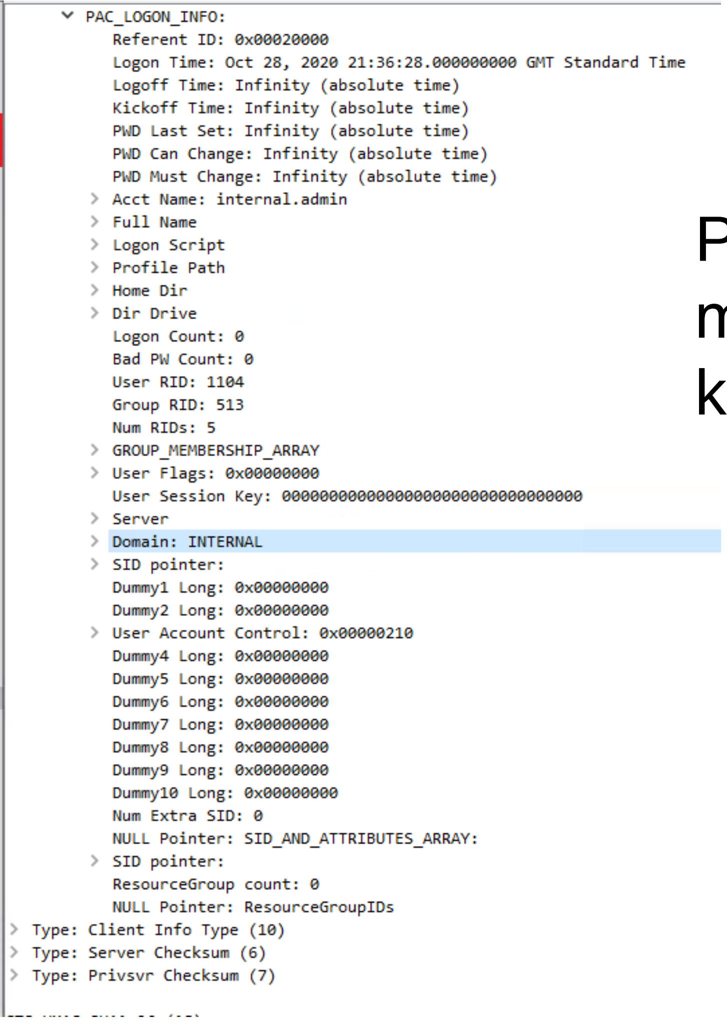
```
> Record Mark: 1682 bytes
v tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
  v padata: 2 items
    > PA-DATA PA-TGS-REQ
    > PA-DATA PA-PAC-OPTIONS
  v req-body
      Padding: 0
    > kdc-options: 40810000
      realm: INTERNAL.ZERODAY.LAB
    v sname
        name-type: kRB5-NT-SRV-INST (2)
      v sname-string: 2 items
          SNameString: cifs
          SNameString: IDC1
```

Further Considerations - Continued

Genuine PAC



```
  ˅ PAC_LOGON_INFO:
      Referent ID: 0x00020000
      Logon Time: Oct 28, 2020 09:51:32.272274900 GMT Standard Time
      Logoff Time: Infinity (absolute time)
      Kickoff Time: Infinity (absolute time)
      PWD Last Set: Sep 14, 2020 22:32:16.778641100 GMT Summer Time
      PWD Can Change: Sep 15, 2020 22:32:16.778641100 GMT Summer Time
      PWD Must Change: Infinity (absolute time)
    > Acct Name: internal.user
    > Full Name: Internal User
    > Logon Script
    > Profile Path
    > Home Dir
    > Dir Drive
      Logon Count: 40
      Bad PW Count: 0
      User RID: 1103
      Group RID: 513
      Num RIDs: 1
    > GROUP_MEMBERSHIP_ARRAY
    > User Flags: 0x00000020
      User Session Key: 00000000000000000000000000000000
    > Server: IDC1
    > Domain: INTERNAL
    > SID pointer:
      Dummy1 Long: 0x00000000
      Dummy2 Long: 0x00000000
    > User Account Control: 0x00000210
      Dummy4 Long: 0x00000000
      Dummy5 Long: 0x00000000
      Dummy6 Long: 0x00000000
      Dummy7 Long: 0x00000000
      Dummy8 Long: 0x00000000
      Dummy9 Long: 0x00000000
      Dummy10 Long: 0x00000000
      Num Extra SID: 1
    > SID_AND_ATTRIBUTES_ARRAY:
    > SID pointer:
      ResourceGroup count: 0
      NULL Pointer: ResourceGroupIDs
> Type: Client Info Type (10)
> Type: UPN DNS Info (12)
> Type: Server Checksum (6)
> Type: Privsvr Checksum (7)
```



```
  ˅ PAC_LOGON_INFO:
      Referent ID: 0x00020000
      Logon Time: Oct 28, 2020 21:36:28.000000000 GMT Standard Time
      Logoff Time: Infinity (absolute time)
      Kickoff Time: Infinity (absolute time)
      PWD Last Set: Infinity (absolute time)
      PWD Can Change: Infinity (absolute time)
      PWD Must Change: Infinity (absolute time)
    > Acct Name: internal.admin
    > Full Name
    > Logon Script
    > Profile Path
    > Home Dir
    > Dir Drive
      Logon Count: 0
      Bad PW Count: 0
      User RID: 1104
      Group RID: 513
      Num RIDs: 5
    > GROUP_MEMBERSHIP_ARRAY
    > User Flags: 0x00000000
      User Session Key: 00000000000000000000000000000000
    > Server
    > Domain: INTERNAL
    > SID pointer:
      Dummy1 Long: 0x00000000
      Dummy2 Long: 0x00000000
    > User Account Control: 0x00000210
      Dummy4 Long: 0x00000000
      Dummy5 Long: 0x00000000
      Dummy6 Long: 0x00000000
      Dummy7 Long: 0x00000000
      Dummy8 Long: 0x00000000
      Dummy9 Long: 0x00000000
      Dummy10 Long: 0x00000000
      Num Extra SID: 0
      NULL Pointer: SID_AND_ATTRIBUTES_ARRAY:
    > SID pointer:
      ResourceGroup count: 0
      NULL Pointer: ResourceGroupIDs
> Type: Client Info Type (10)
> Type: Server Checksum (6)
> Type: Privsvr Checksum (7)
```

PAC forged with mimikatz' kerberos::golden

Questions?