Taller 2021:
Atacando Kerberos de 0 a 100

Presentada por Antonio Alvarado,
CTO, Greenfence Security

Antonio Alvarado (@antonixp21)
https://greenfencesec.com
@greenfencesec

About

- **Ingeniero en Sistemas de Información (primera Generación)**
- **Magister en Seguridad Informática y egresado de la Universidad Tecnológica de Panamá (UTP).**

Antonio Alvarado

GFS
GreenFence Security

¿Qué es Kerberos?

- En primer lugar, Kerberos es un protocolo de autenticación, pero no de autorización. Esto quiere decir que el protocolo se encarga de validar la identidad de un usuario a través de una contraseña solo conocida por este, pero no determina a qué recursos o servicios puede acceder o no dicho usuario.
- Protocolo utilizado para la autenticación en un directorio activo de Windows

GreenFence Security

Introducción a Kerberos: Elementos que forman parte de Kerberos

- En Kerberos intervienen varios servicios encargados de realizar la autenticación del usuario. Entre estos se encuentran los siguientes:
  - El **cliente** o usuario que quiere acceder al servicio.
  - El **AP** (Application Server) donde se expone el servicio al que el usuario quiere acceder.
  - El **KDC** (Key Distribution Center), el servicio de Kerberos encargado de distribuir los tickets a los clientes, instalado en el DC (Controlador de dominio). Cuenta con el AS (Authentication Service), que se encarga de expedir los TGTs

GreenFence Security

Introducción a Kerberos: Claves de cifrado

- Varias estructuras manejadas por Kerberos, como los tickets, se transmiten cifradas o firmadas. Esto evita que sean manipuladas por terceros. Las claves de cifrado utilizados por Kerberos, en Active Directory, son las siguientes:
  - Clave del KDC o krbtgt: clave derivada del hash NTLM de la cuenta krbtgt.
  - Clave de usuario: clave derivada del hash NTLM del propio usuario.
  - Clave de servicio: clave derivada del hash NTLM del propietario del servicio, que puede ser una cuenta de usuario o del servidor.
  - Clave de sesión: clave negociada por el cliente y el KDC.
  - Clave de sesión de servicio: clave negociada para utilizar entre el cliente y el AP.

GreenFence Security

Introducción a Kerberos: Tickets

- Kerberos maneja unas estructuras llamadas «Tickets», que son entregados a los usuarios autenticados para que estos puedan realizar ciertas acciones dentro del dominio de Kerberos. Se distinguen 2 tipos:
  - **El TGS (Ticket Granting Service)** es el ticket que se presenta ante un servicio para poder acceder a sus recursos. Se cifra con la clave del servicio correspondiente.
  - **El TGT (Ticket Granting Ticket)** es el ticket que se presenta ante el KDC para obtener los TGS. Se cifra con la clave del KDC.

GreenFence Security

Introducción a Kerberos: Kerberos SPN

- Service principal Name (SPN)
  - identifica de forma única el nombre de un servicio
- ServiceType/HostName:Port/DistinguishedName
  - MSSQL/server.dojo.local
  - HTTP/server01.dojo.local
  - TERMSRV/server02.dojo.local
- setspn.exe maps AD accounts to SPN
  c:\>setspn -A http/myhost.dojo.local:1433 dojo\websvc

GreenFence Security

Introducción a Kerberos: Common Service type

- TERMSVR - Remote Desktop
- WSMAN - WinRM
- ExchangeAB, ExchangeRFR & ExchangeMDM - MS Exchange
- POP/POP3 - POP3 mail service
- IMAP/IMAP4 - IMAP service
- MSSQLSvc - Microsoft SQL Server
- GC - Global Catalog
- DNS - DNS Server
- HTTP - Web Server
- LDAP - LDAP
- Dfsr - File Server participating in DFRS

GreenFence Security

Introducción a Kerberos:
El PAC (Privilege Attribute Certificate)

- El PAC (Privilege Attribute Certificate) es una estructura incluida en la mayoría los tickets. Esta estructura contiene los privilegios del usuario y está firmada con la clave del KDC.

- Es posible para los servicios verificar el PAC comunicándose con el KDC, aunque esto no es común. No obstante, la verificación del PAC solo consiste en comprobar su firma, sin comprobar si los privilegios son correctos.

GreenFence Security

PAC
PRIVILEGE ATTRIBUTE CERTIFICATE

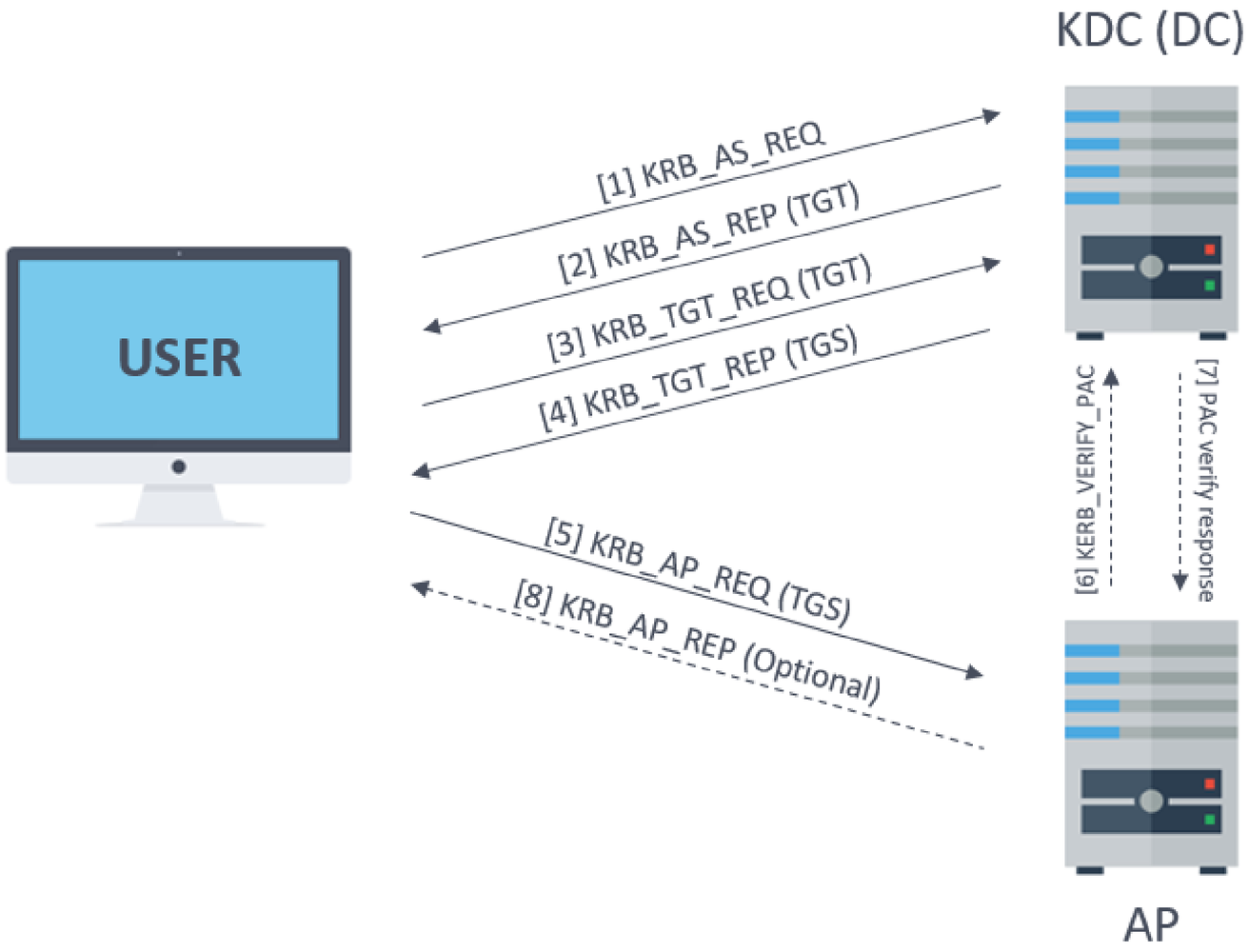
Contiene toda la información relevante para el usuario.

```
▽ IF_RELEVANT AD-Win2k-PAC
    Type: AD-Win2k-PAC (128)
  ▽ Data: 0500000000000000010000000b00100005800000000000000...
      Num Entries: 5
      Version: 0
    ▷ Type: Logon Info (1)
    ▷ Type: Client Info Type (10)
    ▷ Type: UPN DNS Info (12)
    ▽ Type: Server Checksum (6)
        Size: 20
        Offset: 608
      ▷ PAC_SERVER_CHECKSUM: 76ffffff8caf7c2d8866ed805fe6b0d498eb1bf9
    ▽ Type: Privsvr Checksum (7)
        Size: 20
        Offset: 632
      ▷ PAC_PRIVSVR_CHECKSUM: 76ffffffff93284bbc94abefbc28b97da09d4467
```

```
▽ IF_RELEVANT AD-Win2k-PAC
    Type: AD-Win2k-PAC (128)
  ▽ Data: 0500000000000000010000000b00100005800000000000000...
      Num Entries: 5
      Version: 0
    ▽ Type: Logon Info (1)
        Size: 432
        Offset: 88
      ▽ PAC_LOGON_INFO: 01100800ccccccccca001000000000000000020070b38abd...
        ▷ MES header
        ▽ PAC_LOGON_INFO:
            Referent ID: 0x00020000
            Logon Time: Sep  2, 2014 06:12:10.414987200 CDT
            Logoff Time: Infinity (absolute time)
            Kickoff Time: Infinity (absolute time)
            PWD Last Set: Sep  2, 2014 06:07:20.706869800 CDT
            PWD Can Change: Sep  3, 2014 06:07:20.706869800 CDT
            PWD Must Change: Infinity (absolute time)
          ▷ Acct Name: tm
          ▷ Full Name: tm
          ▷ Logon Script
          ▷ Profile Path
          ▷ Home Dir
          ▷ Dir Drive
            Logon Count: 167
            Bad PW Count: 1
            User RID: 1106
            Group RID: 513
            Num RIDs: 1
          ▽ GROUP_MEMBERSHIP_ARRAY
```

GreenFence Security

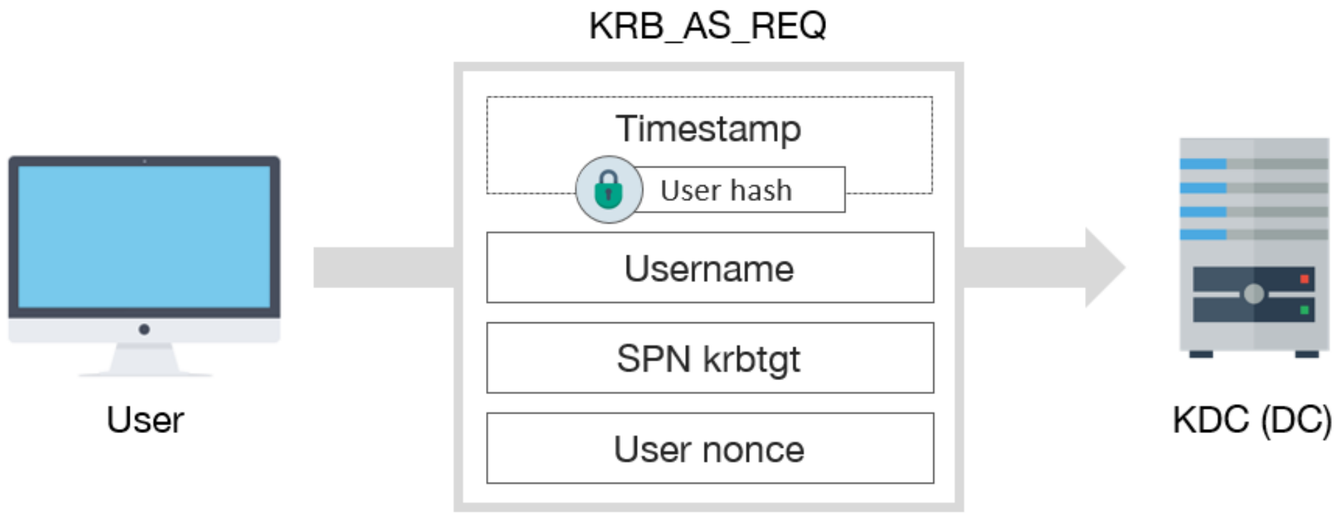
Proceso de comunicación de Kerberos



- **KRB_AS_REQ**: Utilizado por el usuario para solicitar el TGT al KDC.
- **KRB_AS_REP**: Respuesta del KDC para enviar el TGT al usuario.
- **KRB_TGS_REQ**: Utilizado por el usuario para solicitar el TGS al KDC, utilizando el TGT.
- **KRB_TGS_REP**: Respuesta del KDC para enviar el TGS solicitado al usuario.
- **KRB_AP_REQ**: Utilizado por el usuario para identificarse contra el servicio deseado, utilizando el TGS del propio servicio.
- **KERB_VERIFY_PAC_REQUEST** para enviar la firma del PAC al KDC, y verificar si ésta es correcta.
- **KRB_AP_REP**: (Opcional) Utilizado por el servicio para autenticarse frente al usuario.

GreenFence Security

Proceso de autenticación: KRB_AS_REQ

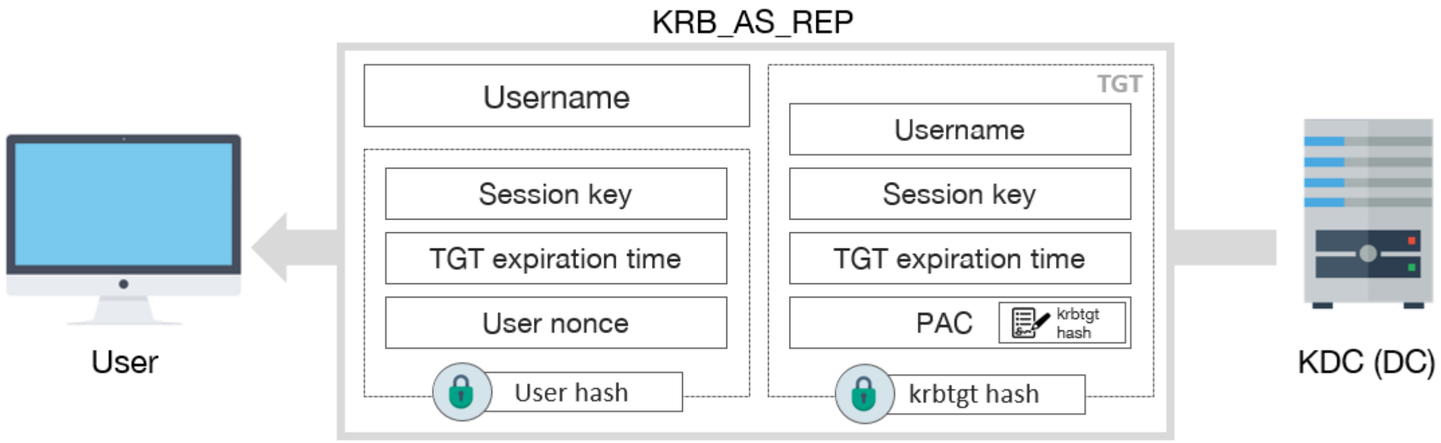


Step 1: User authenticates to KDC by encrypting current UTC timestamp with user's long-term key.

- El usuario inicia sesión con nombre de usuario y contraseña.
  - El usuario se autentica contra el KDC cifrando el tiempo actual en formato UTC utilizando la clave a largo plazo del usuario (contrasena del usuario convertida a hash NTLM) para solicitarle al KDC un TGT.
  - En KRB_AS_REQ se encuentran, entre otros, los siguientes campos:
    - Un **timestamp** cifrado con la clave del cliente, para autenticar al usuario y prevenir ataques de replay
    - El **nombre del usuario** que se está autenticando
    - El **SPN del servicio** asociado a la cuenta krbtgt
    - Un **nonce** generado por el usuario

GreenFence Security

Proceso de autenticación: KRB_AS_REP

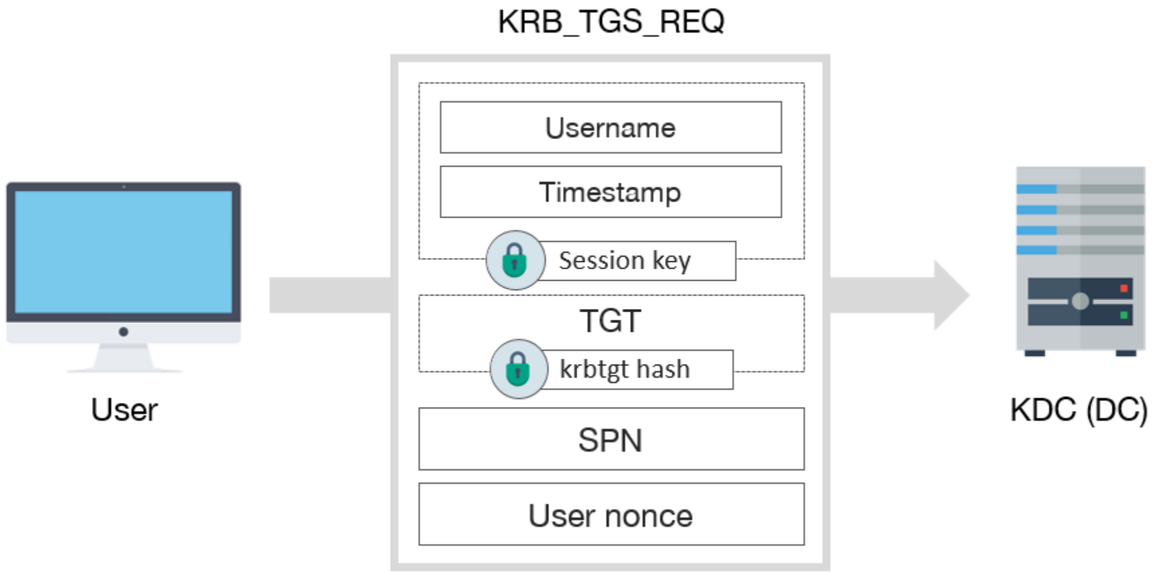


Step 2: If KDC can decrypt the timestamp with the user's key stored in AD, and time is within allowed skew (5-min by default), authentication succeeds. KDC creates a TGT, encrypted with the 'krbtgt' user's long-term key. The TGT is really just a special service ticket. Like all service tickets, it includes user identity information, such as group membership, in a Privilege Attribute Certificate (PAC).

- Al recibir el mensaje el KDC verifica la identidad del usuario descifrando el timestamp. Si el mensaje recibido es correcto entonces responde con un KRB_AS_REP:
  - El controlador de dominio (KDC) verifica la información del usuario (restricciones de inicio de sesión, pertenencia a grupos, etc.) y crea un ticket de concesión de tickets (TGT).
  - En KRB_AS_REP se envía la siguiente información:
    - Nombre de usuario
    - El TGT, que incluye:
      - Nombre de usuario
      - Clave de sesión
      - Fecha de expiración del TGT
      - PAC con los privilegios del usuario, firmado por el KDC
    - Una serie de datos cifrados con la clave del usuario, que incluyen:
      - Clave de sesión
      - Fecha de expiración del TGT
      - Nonce del cliente, para evitar ataques de replay

GreenFence Security

Proceso de autenticación: KRB_TGS_REQ



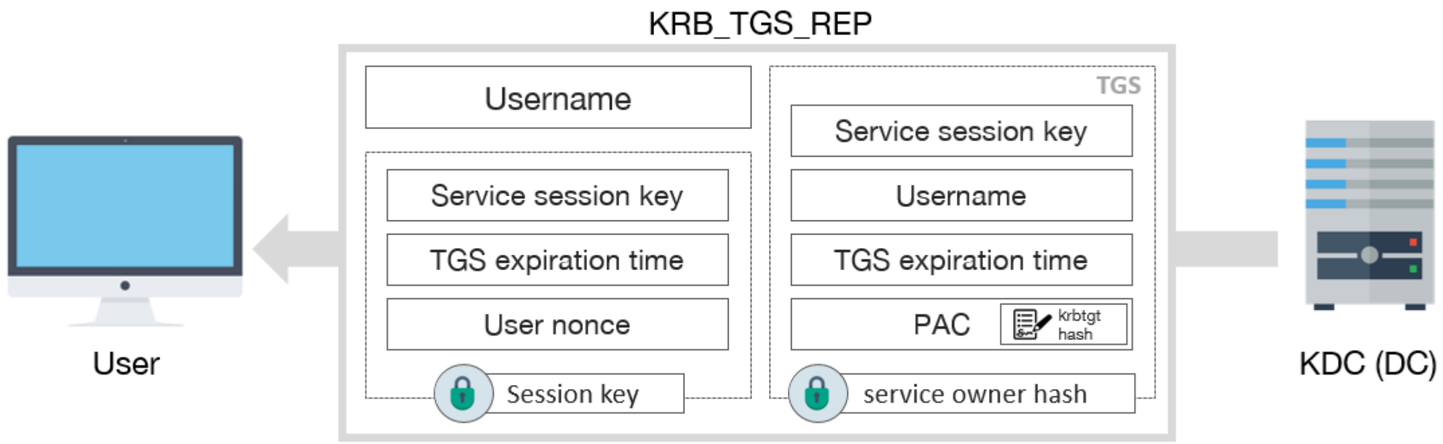
Step 3: User requests service ticket from the KDC. Request includes the user's TGT, encrypted with 'krbtgt' account's long-term key.

- El Usuario presenta el TGT al DC cuando solicita un ticket Granting Service (TGS) . El DC abre el TGT y valida el PAC mediante un checksum - Si el DC puede abrir el ticket y el PAC checksum es verificado entonces considera el TGT como válido. Los datos del TGT se copian de forma eficaz para crear el ticket TGS.

- En KRB_TGS_REQ se pueden apreciar estos apartados, entre otros:
  - Datos cifrados con la clave de sesión:
    - Nombre de usuario
    - Timestamp
  - TGT
  - SPN del servicio solicitado
  - Nonce generado por el usuario

GreenFence Security

Proceso de autenticación: KRB_TGS_REP

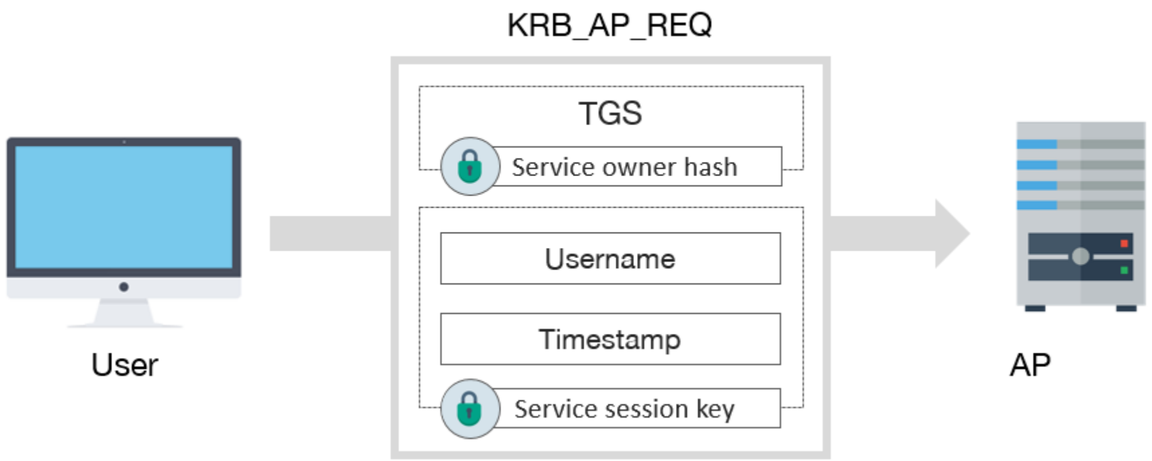


Step 4: KDC decrypts TGT and creates the new service ticket. User's PAC information is copied from TGT to the new ticket. KDC sends service ticket to user, who will then pass it on to the target service. The ticket is encrypted with the target service account's long-term key.

- El TGS se cifra utilizando el hash de contraseña NTLM de las cuentas de servicio de destino y se envía al usuario (TGS-REP)
- En KRB_TGS_REP se pueden apreciar estos apartados, entre otros:
  - Nombre de usuario
  - TGS, que contiene:
    - Clave de sesión de servicio
    - Nombre de usuario
    - Fecha de expiración del TGS
    - PAC con los privilegios del usuario, firmado por el KDC
  - Datos cifrados con la clave de sesión:
    - Clave de sesión de servicio
    - Fecha de expiración del TGS
    - Nonce del cliente, para evitar ataques de replay

GreenFence Security

Proceso de autenticación: KRB_AP_REQ

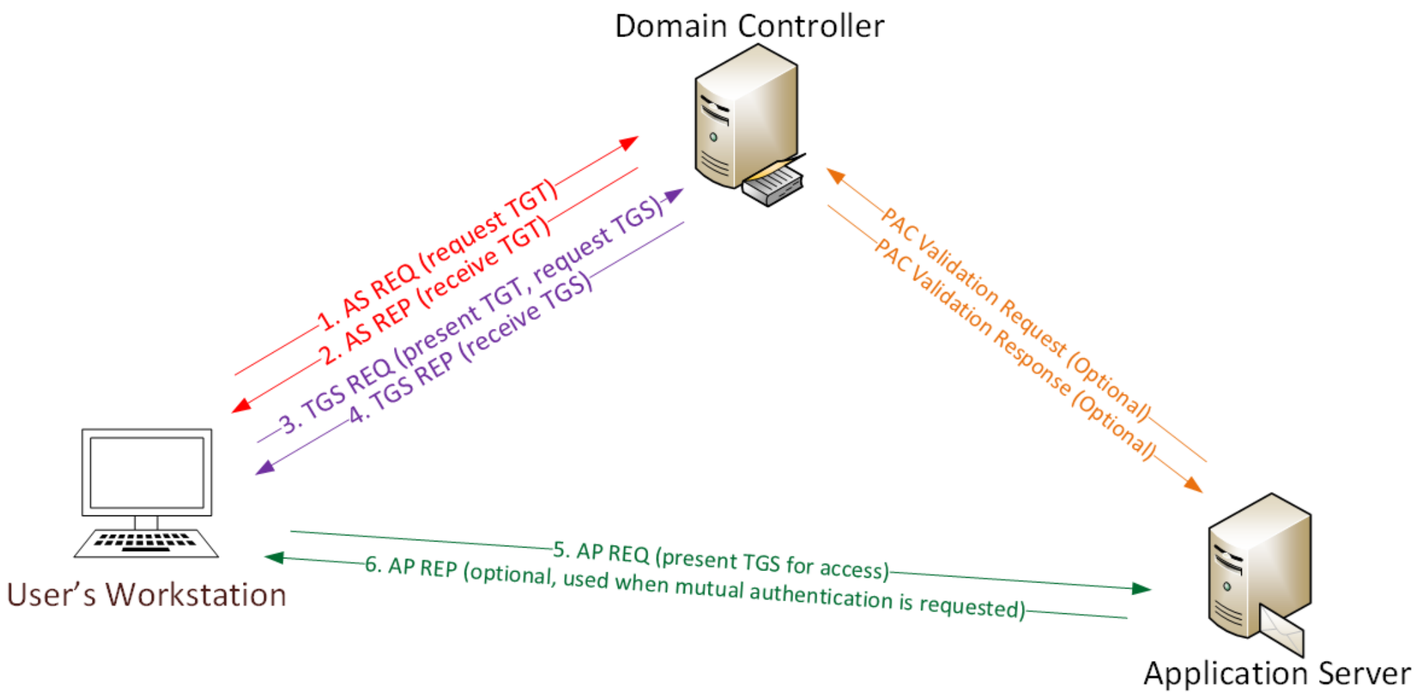


Step 5: User sends service ticket. Service decrypts ticket with its long-term key. The user's identity information (PAC) is included in the encrypted ticket, allowing the service to determine user's authorization level for the service.

- El usuario se conecta al servidor que aloja el servicio en el puerto apropiado y presenta el TGS (AP-REQ). El servicio abre el ticket TGS usando su hash de contraseña NTLM
- En KRB_AP_REQ se especifica:
- Nombre de usuario
  - TGS
  - Datos cifrados con la clave de sesión del servicio:
    - Nombre de usuario
    - Timestamp, para evitar ataques de replay
- Tras esto, si los permisos del usuario son correctos, este ya puede acceder al servicio. Para esto, si está configurado, el AP verificará contra el KDC el PAC. Y en caso de requerir autenticación mutua, responderá con un mensaje KRB_AP_REP al usuario.

GreenFence Security

Proceso de autenticación: Validación de PAC (poco común)



- A menos que se requiera la validación de PAC (poco común), el servicio acepta todos los datos en el ticket TGS sin comunicación con el DC.

- Algunas palabras más sobre el PAC
- El PAC no siempre es verificado o validado:
  - Para TGT: el PAC solo se valida cuando el TGT tiene más de 20 minutos de antigüedad
  - Para TGS: el PAC generalmente no es validado para servicios en Windows modernos.

Step 6 (Optional): Service requests KDC to verify 'krbtgt' signature for the PAC data

GreenFence Security

Ataques de Kerberos

Resumen de ataques que estaremos viendo

- Overpass The Hash/Pass The Key (PTK)
- Golden Ticket y Silver Ticket
- Kerberoasting
- ASREPRoast

GreenFence Security

Overpass The Hash/Pass The Key (PTK)

Si un atacante consigue obtener el hash de un usuario podría suplantar a este frente al KDC, y acceder a los servicios del dominio disponibles para dicho usuario.

Funciona incluso si la autenticación NTLM está deshabilitada en todas partes

Active Directory utiliza el hash NTLM como clave para Kerberos
Si tenemos el hash (o contraseña), aún podemos realizar el AS-REQ (

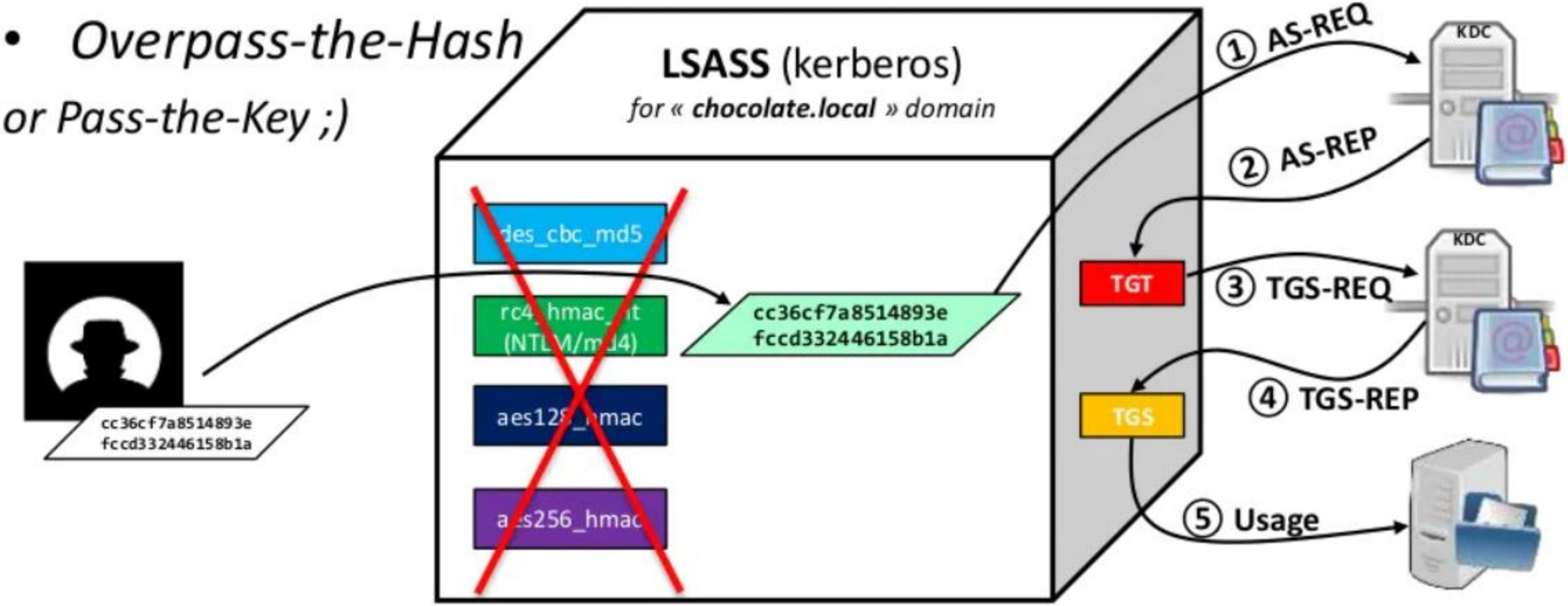
> **Overpass-the-Hash (Step 1):** For RC4 encryption, a user's Kerberos long-term key is the user's NT hash. By "choosing" RC4 encryption, an attacker can intiate a Kerberos logon with the NT hash, providing the capaiblity to perform privileged actions only available via Kerberos logons (such as changing the password).

GreenFence Security

Overpass The Hash/Pass The Key (PTK)

- *Overpass-the-Hash*

or Pass-the-Key ;)



GreenFence Security

Golden Ticket

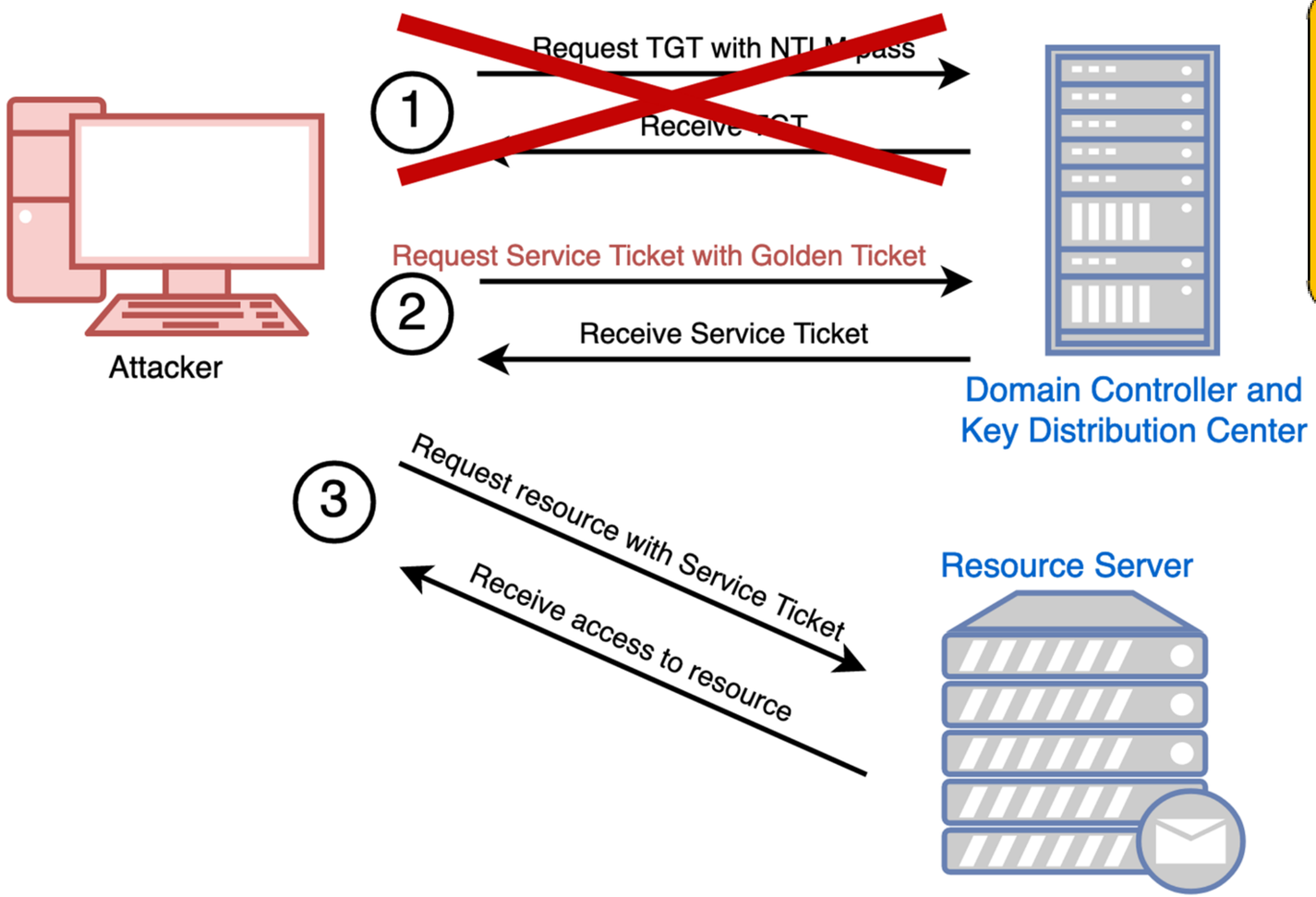
- El objetivo del ataque del Golden Ticket es construir un TGT, para lo cual se necesita la clave del krbtgt. Por tanto si se obtiene el hash NTLM de la cuenta krbtgt, es posible construir un TGT. Dicho TGT puede contar con la caducidad y permisos que se desee, consiguiendo incluso privilegios de administrador de dominio.

- Un atacante que puede crear Golden Ticket puede hacerse pasar por cualquier usuario del dominio

- El ticket continuará siendo válido aunque el usuario incluido cambie su contraseña. El TGT solo podrá ser invalidado si expira o cambia la contraseña de la cuenta krbtgt.

GreenFence Security

Golden tickets:Flujo



Golden Ticket (Step 3): The TGT is encrypted with the 'krbtgt' account's long-term key. This key rarely if ever changes. If an attacker has this long-term key, they can create a TGT that the KDC can decrypt and will assume is valid. The crafted TGT can be created for any user with any group membership, including domain admin.

- Cuando utilizamos un Golden Ticket, la primera interacción es un TGS-REQ (solicitud de un Ticket de Servicio) usando el TGT falsificado (el Golden Ticket).
- No hay presentación previa de credenciales o AS-REQ/ AS-REP!

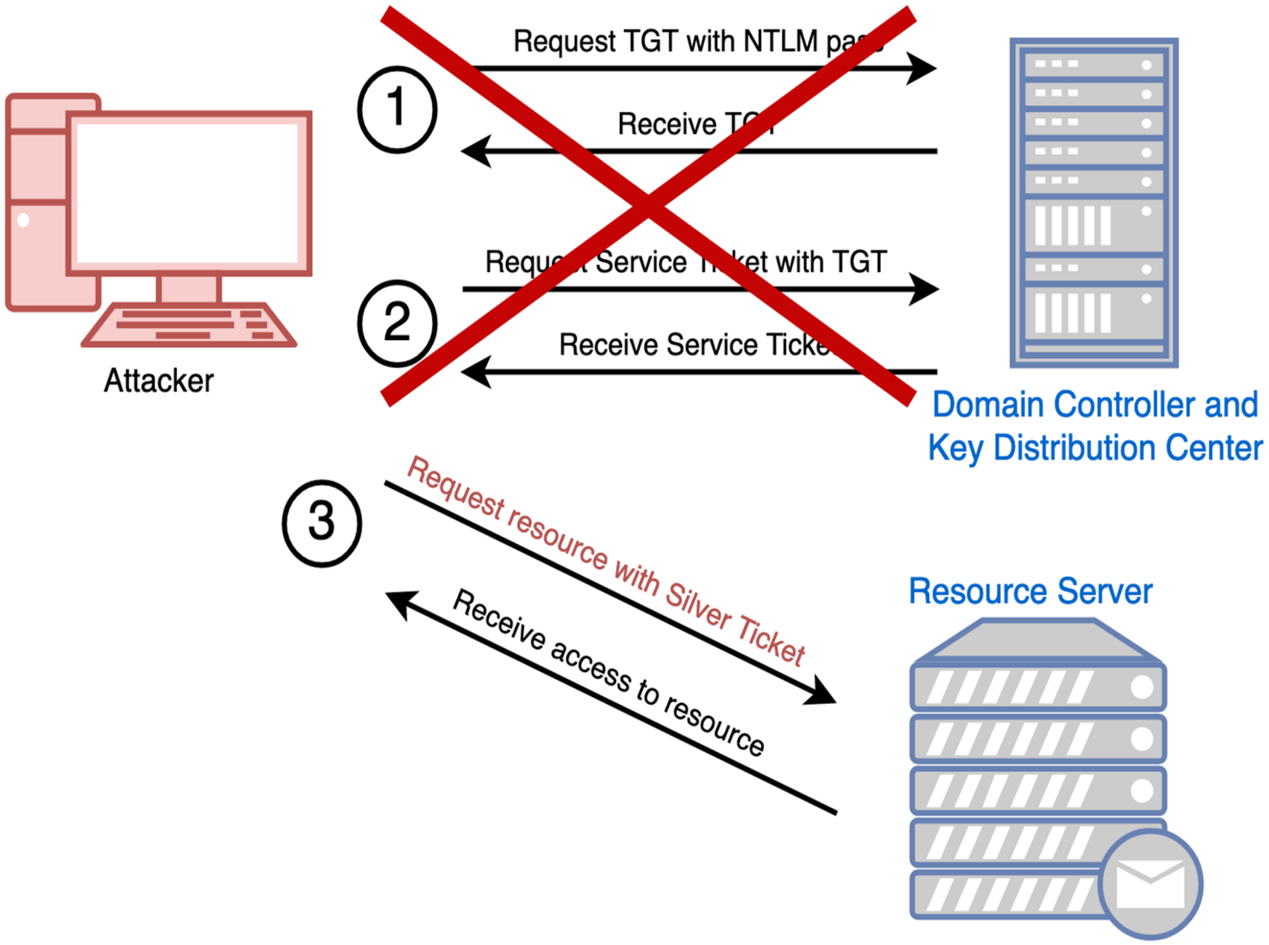
GreenFence Security

Silver Ticket

- El Silver Ticket es similar al Golden Ticket, pero esta vez se construye un TGS y lo que se requiere es la clave del servicio al que se quiere acceder. Esta clave se deriva del hash NTLM de la cuenta de computadora propietaria del servicio.
- En un ataque de Silver Ticket, se crea un Ticket de servicio (TGS) con un PAC personalizado (para escalar privilegios).
- Esta técnica no funcionará si el servicio verifica el PAC, ya que al no conocer la clave de krbtgt, no es posible firmarlo correctamente. **Sin embargo, la validación de PAC es generalmente ejecutada, lo que significa que hay una oportunidad.**

GreenFence Security

Silver Tickets:Flujo



Silver Ticket (Step 5): If an attacker has the long-term key for a service account, they can create a ticket that the service can decrypt and will assume valid. The crafted service ticket can be created for any user with any group membership, including domain admin. This usually works because most services do not take the optional Step 6 to verify the PAC information with the KDC.

GreenFence Security

Kerberoasting

- El **Kerberoasting** trata de usar los TGS para realizar cracking de las contraseñas de los usuarios offline.
- Los TGS vienen cifrados con la clave del servicio, que se deriva del hash NTLM de la cuenta propietaria del servicio.
- Las claves de servicios generalmente son de computadoras y son muy complejas para ser crackeadas pero en algunas ocasiones los propietarios de los servicios son cuentas de usuario normal. **En estos casos es más factible crackear las contraseñas. Además, este tipo de cuentas suelen ser privilegiadas.**

GreenFence Security

ASREPRoast

- El ASREPRoast es una técnica similar al Kerberoasting, que también busca el crackeo offline de las credenciales.
- Cuando un usuario está configurado con el atributo DONT_REQ_PREAUTH, no necesita preautenticación, con lo que es posible construir un mensaje KRB_AS_REQ sin conocer las credenciales del mismo.
- Una vez construído y enviado, el KDC responderá con un mensaje KRB_AS_REP que contiene datos cifrados con el hash de este usuario, pudiendo ser utilizados para el crackeo offline.

GreenFence Security

Cuando utilizar estos ataques?

- **Golden Ticket:** requiere un compromiso de dominio completo. utilizar para persistencia y movimiento lateral
- **Kerberoasting:** requiere acceso como cualquier usuario. utilizar para escalar privilegios y movimiento lateral
- **Silver Ticket:** requiere hash de servicio. utilizar para persistencia y escalar privilegios
- **Over-Pass-the-Hash:** requiere acceso como usuario. Utilizar para movimiento lateral

GFS
GreenFence Security

Controles de seguridad para mitigar

Recomendaciones para proteger su entorno:

- Usar el **principio de privilegios mínimos,** establecer contraseñas seguras y aplicar actualizaciones a tiempo contribuirá en gran medida a mantener seguro un dominio de Active Directory.
- Asegúrese de que todas **las cuentas de servicio asociadas a cuentas de usuarios privilegiados** tengan contraseñas largas y complejas de más de 25 caracteres, preferiblemente 30 o más. Esto hace que descifrar estas contraseñas sea mucho más difícil.
- Asegúrese de que todas las contraseñas de las cuentas de servicio se **cambien con regularidad** (al menos una vez al año).
- Si es posible, utilice cuentas de servicio administradas por grupos **(gMSA**) que tengan contraseñas complejas aleatorias (> 100 caracteres) y que Active Directory las administre automáticamente.
- La contraseña de la cuenta **krbtgt** debe rotarse dos veces al año como mínimo. Se recomiendan rotaciones de contraseña cada 40 días.

GitHub (Antonixp21)

antonixp

antonio-aac