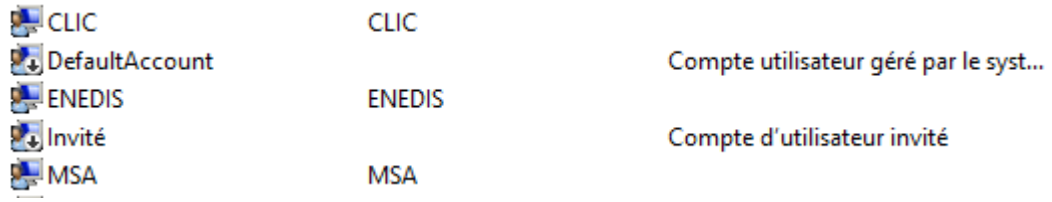
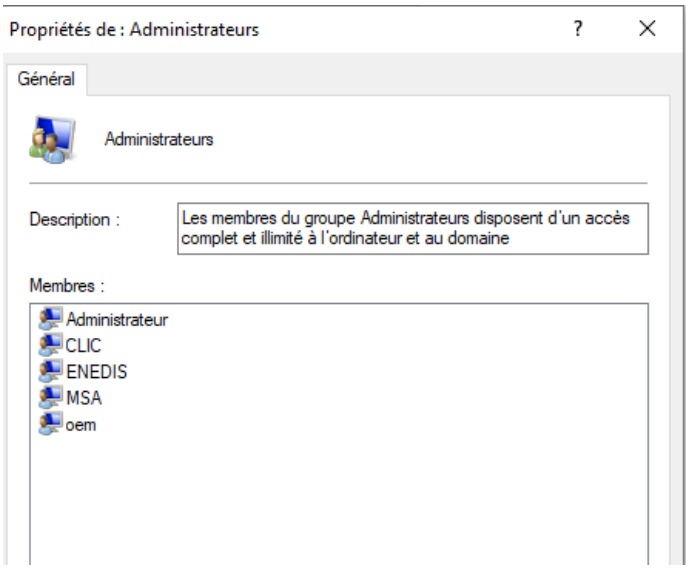
Baptiste Gaillard

TH3 : CH4 : TD1

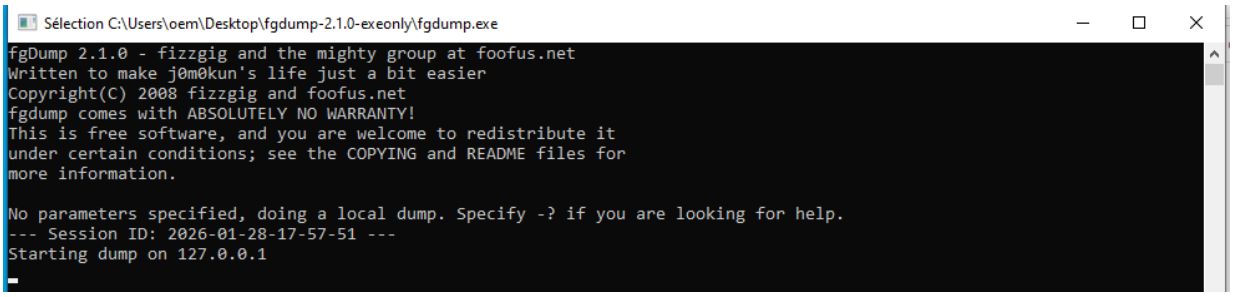
1) Préparation de la VM Windows 10





2) Extraction des hash Windows

Malheureusement je n'ai pas réussi à faire marcher fgdump. Je soupçonne le fait que windows 10 soit un os trop récent pour un outil dont la dernière version a été édité en 2008 même si le tp indique d'utiliser une vm windows 10.



pareil pour son concurrent pwdump7. Je vais donc utiliser un dump fictif pour poursuivre le tp

3) Tests avec John the Ripper

La table rockyou a été insuffisante j'ai donc choisi d'ajouter les mots de passe à une wordlist spécifique pour avoir un résultat avec johntheripper:

```
┌──(stan㉿Stanprout)-[/mnt/c/Users/Stan/Desktop/tp kali]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16
x3])
Warning: no OpenMP support for this hash type, consider --fork=12
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2026-01-28 19:18) 0g/s 36778Kp/s 36778Kc/s 110335KC/s  _
09..*7¡Vamos!
Session completed.
```

Worldlist personnalisé :

```
stan@Stanprout: /mnt/c/Users/Stan/Desktop/tp kali
Session  Actions  Edit  View  Help
  GNU nano 8.6              /usr/share/john/password.lst *
#!comment: This list has been compiled by Solar Designer of Openwall Project
#!comment: in 1996 through 2011.  It is assumed to be in the public domain.
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Un>
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first).  It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
#!comment:
#!comment: For more wordlists, see https://www.openwall.com/wordlists/
aurillac15
judo63
test
123456
12345
password
password1
123456789
12345678
1234567890
abc123

^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

Résultat : Toujours non concluant !

Conclusion :

Je ne peut malheureusement pas effectué ce tp dans de bonnes conditions car l'utilitaire qui permet de dump les NTLM hashes n'est pas fonctionnel.
J'ai tenté à l'aide d'ia de générer un dump théorique de ce qu'aurait dû être le résultat mais c'était en vain. Néanmoins j'ai pu voir l'ensemble de la démarche théorique et l'utilisation des différents os/utilitaires.