Les permissions NTFS

À chaque ouverture de session, les informations d'identification employées par l'utilisateur (nom d'utilisateur et mot de passe) sont transmises à un moniteur de sécurité locale qui accède au Gestionnaire de sécurité (SAM pour *Security Account Manager*). Ce dernier accorde un jeton d'accès (token) qui va déterminer les droits d'accès que possède cet utilisateur pour tout objet "sécurisable" (clé du Registre, fichier, dossier, service, processus, etc.). Ce descripteur de sécurité vérifie deux informations :

- Le SID de l'utilisateur.
- La liste DACL de l'objet auquel tente d'accéder l'utilisateur.

Ces deux notions vont être expliquées dans la suite de ce chapitre.

1. Les SID utilisateurs

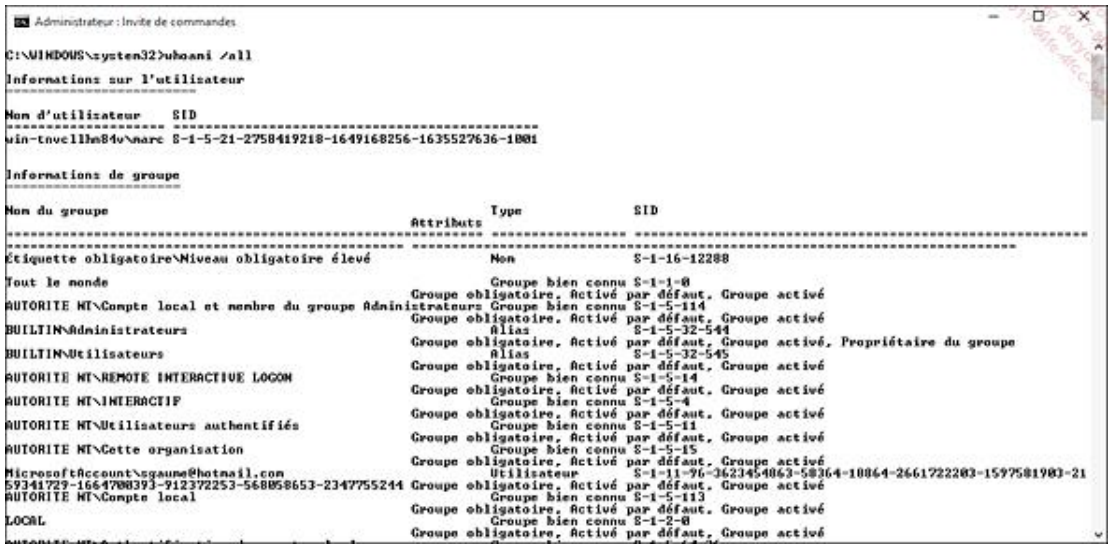
Un SID (*Security IDentifier*) est une manière unique d'identifier un utilisateur ou un groupe d'utilisateurs. Nous retrouvons ces identifiants dans les jetons d'accès, dans les ACL (*Access Control List*) et dans les bases de sécurité des comptes. Reportez-vous à la section suivante pour une description complète du mécanisme des ACL.

Les SID sont des données de longueur variable formant une représentation hiérarchique de l'acteur désigné. La syntaxe est la suivante : S-R-I-XXX-XXX-XXX.

- S : la lettre S (pour rappeler qu'il s'agit d'un SID).
- R : numéro du format binaire du SID.
- I : nombre entier identifiant l'autorité ayant émis le SID.
- XXX-XXX-XXX : suite de longueur variable, formée d'identifiants de sous-autorités ou d'identifiants relatifs (*Relative IDentifier* ou RID).

Vous pouvez afficher les SID de cette manière :

→ Depuis une invite de commandes, tapez : `whoami /all`.



Les informations suivantes sont visibles :