# [Énumération] RpcClient

### Introduction

**RpcClient** est un outil en ligne de commande permettant d'interagir avec les services **RPC** ( *Remote Procedure Call*) dans les systèmes basés sur Windows ou Samba.

## Manuel

#### Syntaxe globale

rpcclient [OPTIONS] -U <USERNAME>%<PASSWORD> //<IP|HOSTNAME>

#### Exemples d'utilisation

• Connexion à un serveur :

rpcclient -U user%password //192.168.1.1

• Lister les partages accessibles :

rpcclient -U user%password -c "enumprinters" //192.168.1.1

Exécuter des commandes spécifiques :

rpcclient -U user%password -c "querydispinfo" //192.168.1.1

Connexion anonyme:

rpcclient -N //192.168.1.1

# **Options** courantes

Options	Descriptions
-U	Spécifie le nom d'utilisateur et le mot de passe pour l'authentification.
-C	Exécute une commande spécifique après la connexion.
-N	Spécifie un nom d'utilisateur mais n'effectue pas d'authentification (utilisé pour les connexions anonymes).
-W	Spécifie le domaine Windows à utiliser.
-1	Spécifie l'adresse IP du serveur DNS.

Revision #1 Created 6 November 2023 14:35:19 by Elieroc Updated 3 May 2024 14:28:42 by Elieroc