Authentification sous Windows

Les attaques

Authentification avec des empreintes

- Objectifs
  - Utiliser les empreintes des mots de passe pour s'authentifier sur un server ou un poste de travail sans connaître les mots de passe !
- Techniques
  - Méthode Pass the hash
    - Disposer des empreintes de mot de passe (SAM, mémoire, cache)
    - Accéder à un serveur/service acceptant l'authentification NTLM
- Outils
  - Metasploit :
    - exploit/windows/smb/psexec
  - Pass The Hash Toolkit
    - C:\> iam.exe <identifiant> <domain> <empreinte_LM> <empreinte_NT>
  - Msvctl (<Seven et 2K08)
    - C:\> msvctl <domain>\<user> [lm <lm hash>] [ntlm <ntlm hash>] run <cmd>
  - Wce