Découverte de mots de passe

- Objectifs
  - Découvrir le clair d'une empreinte
  - Identifier des comptes et mots de passe valides
- Techniques
  - Cassage d'empreinte
    - Par dictionnaire
      - Test des mots de passe usine
      - Constitution d'un dictionnaire (noms communs, multilingues ...)
    - Par force-brute
      - Test des possibilités en direct, selon un jeu de caractères prédéterminé (charset)
    - Par les tables « rainbow »
      - Génération de tables de hash et de mots de passe selon un algorithme "optimisé",
      - Nécessite une table par type d'algorithme, en fonction du nombre de caractères, et du charset composant le mot de passe recherché.
    - Attaque sur l'authentification SMB
      - Attention à la politique de blocage des comptes
      - Penser à vérifier avec rpcclient ou wmi
- Outils
  - `John` (formats : LM, NT et mscash)
  - `Rcrack` (formats : LM et NT)
  - `Cain` (formats : LM, NT et mscash)
  - `Medusa` (`medusa -h <adresse_de_la_cible> -U <fichier_identifiants> _P <dictionnaire> -M smbnt`)

Protocoles d'authentification

- Challenge fixe + Rainbow table
  - Outils : `Cain, OphCrack`
- Prédiction des nombres pseudo-aléatoires/défi
  - Corrigé par le patch MS10-012
- SMB Relay et NTLM Reflection
  - Corrigé par le patch MS08-068
  - Outils : `Metasploit`