Exploitation

Attaques des interfaces d'administration

Plusieurs méthodes

- Recherche de comptes par défaut
  - Dans la documention (`cisco/cisco`)
  - Google : `default password list`
- Attaque par dictionnaire
  - Risque de blocage des comptes
  - Outils : `medusa, hydra`
- Attaque exhaustive (« `brute force` »)
  - Risque de blocage de compte également ;
  - Essai de toutes les combinaisons login/mdp possibles par rapport à un jeu de caractères ;
  - La réussite dépend du temps d'attaque et de la complexité du mot de passe.

Exploitation

Attaques des interfaces d'administration

Plusieurs méthodes

- Objectif
  - Construire un dictionnaire de « brute force » à partir de mots clés relatifs à une cible.
- Outils
  - `Cewl` à partir d'une URL
  - `Crunch`
  - `JTR`
    - `./john -wordlist=passw.lst —stdout -rules`
  - `rsmangler`
    - `./rsmangler.rb -f wordlist.txt -x 12 -m 7 -drlTulseiyac —pna —pnb —na —nb —space > output.txt`