Exploitation

Attaques des interfaces d'administration

- Objectifs
  - Découvrir des comptes valides sur les équipements réseau
  - Prendre la main sur ces équipements
- Cibles : interfaces d'administration :
  - SSH
  - HTTP
  - Telnet
  - …
- Vulnérabilités :
  - Services accessibles depuis toutes les interfaces de l'équipement
  - Compte par défaut ou mot de passe triviaux
  - Failles applicatives ou de configuration de serveurs Web

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.