Exploitation

Attaques sur les protocoles Cisco :
Attaques d'empreinte des mots de passe

- Vulnérabilités
  - Pas de chiffrement du mot de passe
  - Ou faiblesse de l'algorithme de chiffrement
- Chiffrement type 7
  - Format reversible
  - Outils : `Cain & Abel, Ciscocrack, GetPass…`
- Chiffrement de type 5
  - Empreinte MD5 du mot de passe, unique et non réversible
  - Attaque possible par comparaison d'empreinte de mots de passe
  - Outils : `John The Ripper, Hachcat, RainbowTables…`

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